Financial Services Sector Protection and Homeland Security

FRANK R. SPELLMAN

Financial Services Sector Protection and Homeland Security

ALSO IN THE CRITICAL INFRASTRUCTURE AND HOMELAND SECURITY SERIES

Chemical Infrastructure Protection and Homeland Security
Nuclear Infrastructure Protection and Homeland Security
Water Infrastructure Protection and Homeland Security
Energy Infrastructure Protection and Homeland Security
Food Supply Protection and Homeland Security
Dam Sector Protection and Homeland Security
Transportation Protection and Homeland Security
Government Facilities Protection and Homeland Security
Information Technology Protection and Homeland Security

Financial Services Sector Protection and Homeland Security

Frank R. Spellman

Homeland Security Series

Bernan Press

Lanham • Boulder • New York • London

Published by Bernan Press
An imprint of The Rowman & Littlefield Publishing Group, Inc.
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706
www.rowman.com
800-462-6420

6 Tinworth Street, London SE11 5AL, United Kingdom

ISBN: 978-1-64143-340-2
E-ISBN: 978-1-64143-341-9

♾™ The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Printed in the United States of America

Contents

Acronyms and Abbreviations

ACH	Automated Clearing House
APEC	Asia-Pacific Economic Cooperation
APM	Asset Prioritization Model
ATM	Automated Teller Machine
ATM	Asynchronous Transfer Mode
BIS	Bureau of Industry and Security
BSS	Broadcast Satellite Service
CATV	Cable Television
CERT	Computer Emergency Readiness Team
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CHIPS	The Clearing House Interbank Payments System
CII	Critical Infrastructure Information
CIKR	Critical Infrastructure and Key Resources
CINS	FS-ISAC's Critical Infrastructure Notification System
CIP	Critical Infrastructure Protection
CLEC	Competitive Local Exchange Carrier
CME	Chicago Mercantile Exchange
CSBS	Conference of State Bank Supervisors
CS/IA	Cybersecurity/Information Assurance
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOC	Department of Commerce
DOD	Department of Defense
Dodd	Department of Defense Directive
Dodin	Department of Defense Instruction

DOJ	Department of Justice
DOS	Department of State
DOT	Department of the Treasury
DPAS	Defense Priorities and Allocations System
E.O.	Executive Order
FBIIC	Financial and Banking Information Infrastructure Committee
FCA	Farm Credit Administration
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FOIA	Federal of Information Act
GDP	Gross Domestic Product
GPS	Global Positioning System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IP	Office of Infrastructure Protection
IT	Information Technology
IXC	Interexchange Carrier
LEC	Local Exchange Carrier
NASD	National Association of Securities Dealers
NCIP	National Critical Infrastructure Protection
NCS	National Communications System
PSTN	Public Switched Telephone Network
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
TSA	Transportation Security Administration

To the Reader

I am going to make you wake up scared; that is, if you sleep at all.

I am going to make you go through your day looking over your shoulder, to each side of you, in front of you and above you and aware of anyone and everyone you see or come into contact with.

I am going to make you shop at the mall in fear.

I am going to make you sit in your school desk ill at ease.

I am going to make you finish your day wondering when I will come after you and destroy you.

I will make your smartphone inoperative; you will not be able to use your favorite signoff: CUL8R.

When you go to bed, you will take a loaded heater, a fully loaded Dirty Harry Special with you because you will shoot into the darkness if necessary.

I am not a Muslim. I am not crazy. I am not afraid. My goal is to scare the hell out of you . . . constantly . . . all the time . . . any time . . . now and forever.

What I am is a terrorist . . . plain and simple.

Live in terror.

—Your Friendly Radical Terrorist

Preface

The twelfth volume of a well-received series on critical infrastructure and homeland security, *Financial Services Sector Protection and Homeland Security* is an eye-opening account and an important reference source of a diverse and complex sector. This book was designed and written to serve and advise U.S. financial planners, project designers, engineers, communications technicians, law enforcement and security specialists, managers, and superintendents and/or supervisors and responsible-managers-in-charge of protecting the multifaceted nature of this U.S. critical infrastructure.

Currently, the financial services sector critical infrastructure sector includes underlying components that allow for the operations of all business, public safety organizations, and government. Basically, the Financial Services Sector, according to Presidential Policy Directive 21, is critical because it provides an "enabling function" across all critical infrastructures. Moreover, the Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.

Well, this part of the description is easy to understand. But even though it can deal with complex digital transmission technology such as cloud computing, it does not take a "cloud" scientist to comprehend the complexity of this sector. This sector has evolved from the simplicity of the small town or stand-alone bank into a diverse, competitive, and interconnected industry. Varying widely in size and presence, the financial services sector ranges from some to the world's largest global companies with thousands of employees and many billions of dollars in assets to community banks and credit unions with a small number of employees serving individual communities. In short, the financial services sector provides the financial infrastructure of the nation.

This book is organized to simplify and present in a logical and sequential manner a discussion of not only the elements comprising the financial services sector in the United States but also many of the security measures employed to protect the various entities and equipment involved.

Let's face today's reality, those who want quick answers to complicated questions—to help employers and employees handle security threats—must be prepared to meet and deal with the threat of terrorism on a 24/7 basis. It is important to point out that this book does not discuss and focus on security concerns related to natural disasters; on the contrary, the focus here is on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, specifically from malicious actors. This focus includes the added dimension of preventing misuse and malicious behavior. In the post–September 11, 2001, world, the possibility of financial services sector infrastructure terrorism—the malicious use of weapons and cyber intrusion to cause devastating damage to financial services sector infrastructure and its associated subsectors along with—literally—its cascading effects—is very real. Thus, the need is clear and real and so is the format and guidelines presented in this text to improve protection and resilience of financial services sector infrastructure.

This book describes the sector- and subsector-wide processes required to identify and prioritize assets, assess risk in the sector, implement protective programs and resilience strategies, and measure their effectives. This book and the complete sixteen volumes (expanded from the original 14 volumes) of the critical infrastructure sector series were written as a result of 9/11 to address these concerns. It is important to point that our financial services sector infrastructure (as is the case with the other 15 critical infrastructures) cannot be made absolutely immune to all possible intrusions/attacks; thus, it takes a concerted, well-thought-out effort to incorporate security upgrades in the retrofitting of existing systems and careful security planning for all new facility infrastructure components. These upgrades or design features need to address issues of monitoring, response, critical infrastructure redundancy, and recovery to minimize risk to the facility infrastructure. However, based on personal experience none of these approaches is or can be effective unless financial services sector staff members at all levels of the chain of command are cognizant of the threats.

Financial Services Sector Protection and Homeland Security presents common-sense methodologies in a straightforward, almost blunt manner. Why so blunt? At this particular time, when dealing with security of employees, family members, citizens, and society in general—actually, with our very way of life—politically correct presentations on security might be the norm, might be expected, and might be demanded, but my view is that there is nothing normal or subtle about killing innocent people—the right and need

to communicate and the right to live in a free and safe environment is a reasonable demand.

This text is accessible to those who have no experience with or knowledge of the financial services sector. If you work through the text systematically, you will gain an understanding of the challenge of domestic preparedness—that is, an immediate need for a heightened state of awareness of the present threat facing the financial services sector members as potential terrorist targets. Moreover, you will gain knowledge of security principles and measures that can be implemented—adding a critical component not only to your professional knowledge but also give you the tools needed to combat terrorism in the homeland—our homeland, both by outsiders and insiders.

One final word to readers is this: This book is written in the conversational and engaging and reader-friendly style that is the author's trademark. Why? Well, I never apologize for attempting to communicate.

Frank R. Spellman
Norfolk, Virginia

Prologue

No Honor among Terrorists

Note: The following fictitious account is included here in order to set the stage for what follows in the text and to continue the sordid saga of the Williams family (chronicled in the other volumes of the critical infrastructure and homeland security series). The Williams are homegrown, radicalized terrorists (smart and brutal and not Muslim; you might say they are clones of Timothy McVeigh) who have done whatever they could do to bring about the death and destruction of innocents in the United States, with particular attention being paid to attacking, impacting, and/or destroying sectors of critical infrastructure.

*****

I just love it when banks, credit unions, and the other money-grubbing institutions lose money, fold up, go bankrupt, go belly up, get caught breaking the law, or get a little hand up with their *total* destruction (that is where I come into the picture, so to speak)! Don't you just love it too? Moreover, watching all those bank and money managers do a perp walk in handcuffs and leg chains and trying to hide their Botox-injected faces just turns me on…totally!

So, okay, not by my choice, this is going to be one of those one-way conversations—me to you—about those nightmarish financial services organizations and some of the other ills (there are so many to choose from) contaminating this country. They need to be changed and/or eradicated…one way or the other…I prefer the other way, thank you very much.

I blame our present country's decline on all the phony financial practices perpetrated on us by those greedy and heartless money changers … and those foreclosure clowns who smile while they devastate, destroy, and eviscerate

you. Where has all the decency gone today? And have you noticed those frog-faced goonies out protesting every day? And when you ask them what their complaint is…they cannot answer. Wow! It is amazing to me and my fellow patriots how messed up today's young people are. Anyway, I think it is okay to melt or kill all those Snowflakes (the wackoes destroying all of us).

Let's cut the baloney—you know all that pretentious nonsense—and get down to brass tacks, so to speak. I'm in the slammer. I am here because I am and continue to be unlucky. Yes, it's because one of my fellow patriots ratted me out.

Anyway, I will get to that disastrous caper and exactly what happened in due time. For now, I am presently locked up in this cell in King County Lock-Up here in Seattle…my home town…where all them bleeding heart ultra-brain-dead liberal dumb bunny snowflakes live. Oh well, as I look around at the bars on the cell door and the three windowless walls painted sickening pea green, my gaze settles on those initials and short, pithy statements carved there (I can't repeat those statements here, folks, even I have some degree of modesty). I am familiar with most of the initials—many belong to my family members, my blood. I am part of that famous—excuse, me, infamous—family, the Williams. I am B. M. Williams VII…and I'm proud of it. I know you have heard of our infamous and patriotic exploits, which unfortunately end with so many of us inhabiting this isolation cell…sooner or later…usually sooner…before we have a chance to kill as many of you sickening no-loads as possible. With us, failure is not an option…but unfortunately it is a common happening. But be advised, we are a large family and are just beginning our cleansing of America and the melting of all you snowflakes…and others who dare get in the way…our way—remember, collateral damage is good…very good.

You want to know all? You are writhing and sweating all over in anticipation, aren't you? You want to know me better…you can't wait…I have you poor souls hooked, addicted. Well, I do not blame you one tiny bit: besides being young, extremely talented, and 10 times smarter than the average genius, I am rather appealing…and a good-looking redhead (like all my 11 blood sisters and hundreds of my want-to-be sisters) too. Well, okay, let's get down to it…*it* being why I have joined many of my other bloods in occupying this horrible, inhumane cell…and having been sentenced to 10 years in the Big House…federal, of course.

It began after my first course in advanced finance administration at a northwest university. In that class and others that followed, I learned how easy it is to part people from their money and turn those funds into my personal gains. My family was already wealthy with almost unlimited wealth…so I had little need to fill my pockets with others' money. What a horrible awakening it was for me…to realize that this country runs on figuring out how to tear

folks from their money and other assets to increase the fortunes of a handful of greedy jerks. I found out that it is so easy to do…to take peoples' money on the pretext of making them richer (because people are suckers and greedy, too). Anyway, when I turned 21, after years of "maybe" spiking old growth trees so those commie lumber people could not cut them down without chopping themselves up…and maybe (I can't say for sure, the commie prosecutors are probably listening in) setting aflame all those gas-guzzlers in the those sleazebag car lots and doing other despicable things that, again, I can't comment on … otherwise those liberal pigs will prosecute me and my patriotic family members for trying to save the country from the money grubbers…and for glorious things I might have accomplished in the past.

Anyway, my plan was conceived while I was in lockup for stealing and burning up some of those leftwing political signs. My plan? Well, it was brilliant. First, you need to understand the two things that me and my blood share: our innate hatred for anything federal or state or local government that has anything to do with enforcing the stupid laws those commies put into effect and… our genius, of course. Einstein, Newton, Aristotle, Stonewall Jackson, Patton, and da Vinci, well, they were pretty smart, but the Williams are just a whole lot smarter. Our only problem is bad luck…lots of bad luck… and, when employed, our incompetent coconspirators.

A few years ago, I came up with a plan to destroy as many banks as possible. I was particularly interested in small-town banks (those big-city banks are too risky…at least for the time being…their day is coming…). The small-city banks themselves are relatively easy targets even though they are so widespread and there are so many of them…my research in 2016 enabled me to discover that at that time there were almost 6,000 small-city banks or credit unions in the United States. My view of banks is that they are instruments of extortion of the worst sort and rip off innocent people. Ah, but there is more to my hate-filled and disgusting views of those rip-off systems…yes, more. How about the poor taxpayers who have to subsidize and bail out those rip-off banks?

My targets had to be fairly remote banks. I had to whittle down to a specific number of targets…ones that were doable, destroyable. I came up with a brilliant plan to attack and destroy a large number of remote, small-city banks. This was my "Blow Up the Small Banks Caper."

There were a few things I knew based on experience and research. First, I knew I had to work alone, but I knew that I could not inflict a large amount of damage to the financial services sector without help…lots of help. I am not a lone wolf…more like a lone Utah raptor, thank you very much! But when planning on the destruction of large numbers of targets, it is important to have as much help as possible. Still, I knew my family's past experience with "partners in crime": they found out the hard way that adding people to

a plan is like adding weak links to an extensive chain. Never work as a team; instead, work alone. I knew all this and the risks of adding weak links to my killing chain. I am a genius for sure but also a realist…I knew I could not act alone.

The only way to work alone is, for example, when you rob a bank … and if you work alone, all you have to worry about is the bank teller and the video cameras…and if you have to you can destroy both…but if you get away scot-free then the only one who knows what you accomplished is you.

The other thing I knew is this: never stick to the eight signs of terrorism that the commie homeland security and other law guys look for. Today, after 9/11, more people are paying attention to those eight signs…and those can give you away before you even destroy. What are the eight signs? Gee, thought you would never ask. Actually, the eight signs are published and described by that Big Brother agency known as FEMA…I did my homework, important. You remember FEMA don't you? Well, just think Hurricane Katrina…ya, you got it…a real mess by an incompetent political agency. Ok, here we go...I will bulletize them…I just love bullets—and bombs, A-bombs, H-bombs, Mother of all Bombs (MOABs), and even firebombs included:

- Surveillance
- Elicitation
- Testing security
- Funding
- Acquiring supplies
- Suspicious persons
- Rehearsal phase
- Deployment

Okay, humor me and let me go down the list and tell you what I did and did not do. With regard to surveillance, I already knew my targets from my research. My targets were all small banks and credit unions in small towns and cities throughout the country…50 of them. Now, in regard to elicitation (what a stupid word, why not just say entice information from dumb-dumb clowns), it was not necessary for me to spend any time in this area because of all the information that is readily available via the Internet.

Testing security is another key step in terrorist planning…no kidding! But…however…there is no security that I knew of at any of the selected bank locations that could handle or prevent the type of attack that I had planned… at least this is what I *thought* at the time.

It is expensive to accomplish a terrorist mission….but…without going into detail, funding has never ever been an issue for the Williams family…enough

said. I had all the supplies I needed for this caper: a huge cache of military-grade explosives and 50 used sedan-type cars.

Suspicious persons or impersonation? Wow, really? Simply, this did not apply to me or my co-patriots because there was nothing suspicious about me and them. And, who would I impersonate? No one on Earth that I can think of is suitable to impersonate.

In my case there was no rehearsal needed. I knew the targets (again, so I thought) and how to reach them and that they were mostly in secluded areas off the highway where few people would be around. The exact and precise plan to blow up the banks in each of their locations was clearly imprinted in my mind. I knew what had to be done and how to accomplish it (again, so I told myself).

It was the employment of my co-patriots that turned out to be my Achilles' heel…my downfall. What happened was this. I had a ton of female followers to choose from…fairly smart and determined woman who knew that something had to be done to this country to make it straight again. I never work with men; remember, it was men that screwed up the country in the first place. However, even with all my brilliance and attention to detail and my unmatched ability to get the job done, I ran into the same problem my other family members encountered: bad luck…poor selection of people…well, poor selection with regard to one young woman, anyway. She was Sally B. Grade…actually, she turned out to be an F grade … big-time.

I began my caper in Seattle…it was easy to put together my 50 bombers in Seattle because the place is full of our kind…which I will not describe in detail here…to protect the guilty, so to speak. Anyway, I planned on loading up the 50 used sedans with enough explosives to completely destroy the banks and everyone in them and around them. The idea was to send the sedans fully loaded with explosives at very high speeds right into the banks and blow them to smithereens. I intended to have my co-patriots guide their explosives-loaded vehicles right into each bank and let them blow… and blow… and destroy…and maim and kill. No, it was not my intent to have the drivers in the sedans when they plowed into the banks…we are patriots and not martyrs…only a fool would be a martyr for anything. Because of technology…you know those gadgets that when properly installed in autos make them self-drivable … well, I had my ace mechanics install those figamajigs and we tested them…to my surprise, they actually worked—funny: I could not believe we could use a rotten society's toys to destroy it!

Now some of you are probably wondering why I just did not take the modern approach to destroying banks by just hacking them out of business. Well, that's too easy! Any fool can hack a bank and drain some fool's bank account or all the accounts…but how do you get to those hidden riches in them safe

deposit boxes…oh, gee, I know…you blow them to smithereens…yup…my big bang(k) theory. Those safe deposit boxes hide many secrets from the IRS, police, relatives, and others and they needed to go the way of the *Titanic*.

Anyway, I thought Sally B. Grade would do just fine attacking a small bank in Lummus, Texas…she was from that area and said she knew the bank and surrounding neighborhood like the back of her hand. Wrong! Anyway, as you might expect, Sally had only one type of car in mind to do her dirty work…a Mustang, of course….Sally without a Mustang is like bread without butter…that is, according to Sally and all those other Mustang Sallies out there.

So, I had them retrofit a 2006 Mustang GT just for Mustang Sally…ha… seems funny now…I guess it was then too … . Anyway, I can't criticize her taste in autos….I like that model, too. However, the problem with a Mustang is limited space….great car and sporty and love those deep throaty sounds from the exhaust pipes…but when you are trying to blow something up, you need space for the explosives…so I had the seats removed in the back and that helped….I should have had the passenger side front bucket seat removed also…my mistake.

Mustang Sally was assigned to direct her fully explosives-loaded Mustang into the S&W Bank of Lumus, Texas. Huge mistake… HUGE. Anyway, on the Friday before Memorial Day all my co-patriots were directed to strike their targets. I picked that last working day before the holiday because I wanted to ensure there were civilians of all types inside those banks so we could kill them all…and send the ultimate message to all the Snowflakes and Bleeders out there in la-la land that we will eventually find and kill you all.

But on the day before the Friday before Memorial Day, Mustang Sally was whacked out on drugs of one type or another…we will never know for sure because there was so little left of her or the Mustang to determine anything… NO…there was little evidence left.

Mustang Sally, hopped up on drugs, allowed one of her friends to ride shotgun in the Mustang the day before she was supposed to drive, by remote control, the Mustang into the S&W Bank of Lumus, Texas. But Mustang Sally had a secret. Apparently she had a death wish: instead of directing the explosives-loaded Mustang into the bank remotely and by herself alone, Sally removed some of the explosives from the passenger side of the car…to make room for her passenger…and then she just drove the Mustang at high speed toward the bank. And into the bollards and high curb. She never even reached the bank's front, which had security doors, reinforced windows, and a double-bricked façade—all security measures she hadn't planned on. The car exploded on impact, immediately killing Mustang Sally.

And how about Sally's friend, you ask? Good question. We now know most of the details because Sally's friend did *not* have a death wish: she was able to open the passenger-side door and jump out into the street before impact. She was bruised up but she survived—and was almost immediately arrested by a group of Texas Rangers. Turns out that right next to the bank was a Texas Ranger district office with a dozen Rangers and others within. Their office building was destroyed and took the brunt of the damage. Two Rangers were killed and a few others that were present received assorted injuries. It was Sally's friend who ratted me and my co-patriots out.

Now, what I am relating to you is based on court testimony given by Sally's friend—she was given complete immunity for her testimony—who talked on the stand in court for three days. From what this witness said we now know that Mustang Sally had talked to her about going to the bank and that the Mustang was loaded with unmarked boxes. Sally had a small electronic transmitter (the detonator) to ignite the explosives, if the crash did not. The witness said she had no idea what Sally's intentions were until about a block or so before they reached the bank's location. Sally had told her to get ready to meet again in heaven…that is when Sally's friend jumped from the car. "A quick trip to heaven was not really on my agenda," she said. Interestingly, during the friend's testimony, when asked why Sally picked a bank that was so well prepared for such a terrorist attack she replied that she thought Sally had not actually visited the bank for several years and was not familiar with the bank's security upgrades. It then made sense to me because there is no way anyone with a brain, even one on drugs, who had the knowledge of the bank's great security upgrades would attack that particular bank. The bank employees testified they stated upgrading after 9/11 (the Texas Ranger office next to the bank did likewise)—otherwise, the bank employees believed that none of them would have survived.

Well, you know what they say about the best laid plans… My plan failed right after I placed my faith in coconspirators and in particular in Mustang Sally, who literally blew the whole thing up. This caper was all about bad luck. The bad luck was twofold: Mustang Sally herself, of course, did not use good judgment in her drug abuse and in not following directions from me … simply, she did not allow me to accomplish my mission. Also, when I made the decision not to be a lone Utah Raptor, it was a big mistake on my part. It is hard to say how many weak links were in my chain, because the plan never came off. After Sally's friend survived and mentioned to the investigators that Sally was in contact with me—me, a person from a family of infamous terrorists—I was a cooked raptor, for sure.

Months after the Texas fiasco I had my trial, and after that two unsuccessful appeals, I was totally shocked, to say the least, that someone like me who was as guilty as they come was actually found guilty; hard to believe in this day and age of liberal juries and judges…especially in Seattle. Oh well, I was involved with a couple of killings of Texas Rangers and with the severe injury of several others, but I had made a plea deal that shortened my sentence considerably. I say, isn't the American justice system great!

Remember that famous movie line: "I'll be back!"…my final comment here is "ditto to that!"

Chapter 1

Introduction

> Fear is the emotion that makes us blind.
>
> —Stephen King

> Financial markets in the United States are the largest and most liquid in the world.
>
> —U.S. Commerce Department

SETTING THE STAGE

The Financial Services Critical Infrastructure Sector faces a complex and evolving risk environment that has the potential to disrupt the sector's ability to deliver services that are critical to the nation's economy. To manage this risk, a diverse set of stakeholders—including financial services sector companies; sector trade associations; federal government agencies; financial regulators; state, local tribal, and territorial governments; and other government and private sector partners in the United States and around the world—collaborate to enhance the sector's security and resilience—resilience being the key goal (USDOT/DHS 2015).

SECTOR OVERVIEW

The primary entity responsible for protecting financial services sector infrastructure and assets is split between three entities: the U.S. Treasury Department, Homeland Security, and the private sector. In conjunction with

the federal government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to continue financial services during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

The financial services sector is closely linked to other sectors. Specifically, using a simple analogy we can say that just as one needs arteries and veins to move blood in our circulatory system, in the same way financial services ensure that we transfer, invest, or spend our money effectively with least amount of loss and risk. Simply, financial services are not only the circulatory system but also the backbone for much of the critical infrastructure within the United States. And many of the other infrastructure components are completely dependent on financial services systems to perform their missions. As such, financial sector systems serve part in parcel with other key national security and emergency preparedness resources and are an important component of our overall national critical infrastructure. The financial services sector is closely linked to other critical sectors (each of which is covered or are in production in separate editions of this series), including, for example (DHS 2017):

- The *Energy Sector*, which provides the flow of energy in different forms to run the engines of industry and just about everything else we have come to count on to maintain the so-called good life. Without the flow of finances to maintain the flow of energy, the engines of industry would come to a screeching halt.
- The *Information Technology Sector*, which provides critical control systems and services, physical architecture, and internet infrastructure, and which also relies on communication to deliver distribution applications and services.
- The *Emergency Services Sector*, which depends on the other sectors for resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls.
- The *Transportation Systems Sector*, which provides the fuel needed to power backup generators and relies on financing to maintain monitoring and control of the flow of ground, sea, and air traffic.

It is safe to say that none of the other 12 critical infrastructure sectors could function without the financing provided by the financial services sector.

At this point you have probably surmised that the one way of investigating the interdependence of the financial services sector architecture is to look at them from a critical financial services infrastructure perspective. The National

Infrastructure Protection Plan (NIPP) is intended to meet the requirements set forth by the president in Homeland Security Presidential Directive 7 (HSPD-7). The Treasury Assistant Secretary for Financial Institutions implements the Treasury Department's responsibilities under HSPD-7. To meet objectives set forth by HSPD-7 for collaboration with the private sector, the Treasury Department works closely with the private sector. Further, NIPP utilizes Critical Infrastructure Identification, Prioritization, and Protection which is an overarching approach for integrating the nation's Critical Infrastructure and Key Resources (CIKR) protection initiatives.

It is clear from figure 1.1 that there is a great deal of interdependency between the financial services sector and a number of the functionaries within the critical infrastructure community. Figure 1.1 illustrates that all of the critical infrastructures have critical requirements for financial services of some form. Alternatively, the financial services community has a number of instances where they are dependent on the other critical infrastructures. The remainder or this section will provide profile for the financial sector services, which will also demonstrate the interdependencies between the nation's CIKR.

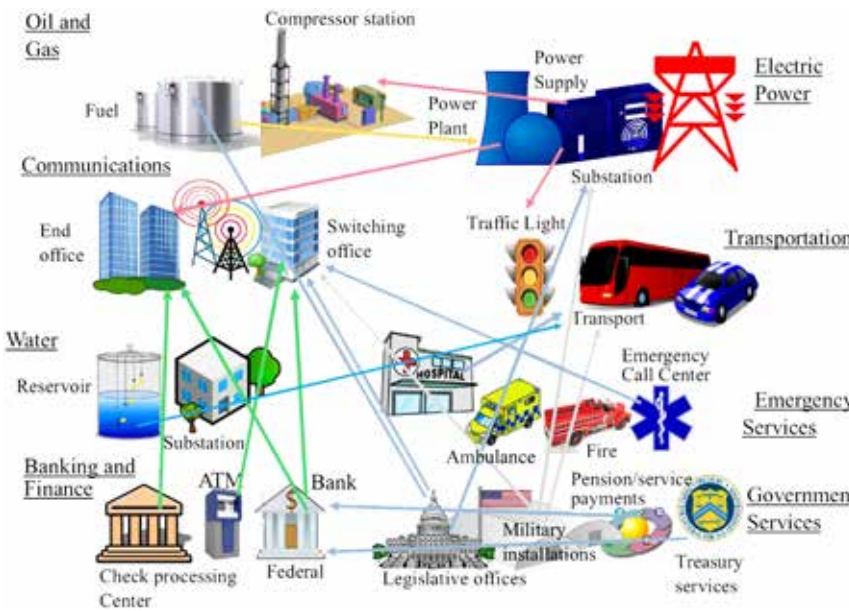

Figure 1.1 Partial Illustration of the Interdependencies between Critical Infrastructures.
Source: Adapted from FCC (2017) and illustrated by F. R. Spellman and Kathern Welsh.

SECTOR PROFILE

The financial services sector profile is best described by defining the services offered. In fact, financial institutions are organized and regulated based on the services the institutions provide. These services include the following: (1) deposit and payment systems and products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products. All aforementioned critical services are executed upon, or delivered through, information technology (IT)–based platforms and channels; therefore, cybersecurity components are factored into all critical infrastructure protection–related activities performed by the sector.

The financial services sector is both large in assets and in the number of individual businesses. For example, in the sector there are almost 19,000 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,500 broker-dealers, investment advisers, and investment company complexes; providers of risk transfer products, including almost 8,000 domestic U.S. insurers; and many thousands of other credit and financing organizations (DHS 2010).

Deposit, Consumer Credit, and Payment Systems Products

The primary providers of wholesale and retail payment services, such as wire transfers, checking accounts, and credit and debit cards are provided by depository institutions such as banks, thrifts, and credit unions. These institutions use and/or operate the payments infrastructure, which includes electronic large value transfer systems automated clearinghouse (ACH) and automated teller machines (ATM). Note that these institutions are the primary point of contact with the sector for many individual customers. Additionally, these institutions may be federal or state-chartered banks or credit unions; however, in most instances, the federal financial regulators have at least some authority over the institutions (DHS 2010).

In addition to the aforementioned payment systems, the depository institutions provide customers with various forms of extensions of credit, such as mortgages and home equity loans, collateralized and uncollateralized loans, and lines of credit, including credit cards. Consumers have multiple ways of accessing these services. For example, customers can make deposits in person at a depository institution's branch office, through the mail, at an ATM, or via direct deposit using ACH transactions. Customers can make withdrawals at a branch office, at an ATM, or by using a debit card or check. Customers also can access credit lines through other retail banking services using the telephone or the Internet. In the United States, customers typically have deposit, checking, and loan accounts with more than one depository institution. The

average household may have up to 18 account relationships spread among 12 financial institutions (DHS 2010).

Credit and Liquidity Products

When an individual seeks a mortgage to purchase a house, when a business obtains a line of credit to expand its operations, and when a government issues sovereign debt obligations, these are examples of seeking liquidity and credit for a wide variety of needs. Many financial institutions, such as depository institutions, finance and lending firms, securities firms, and Government Sponsored Enterprises (GSEs) meet customers' long- and short-term needs through a multitude of financial products. Some of these entities provide credit directly to the end customers, while others do so indirectly by providing wholesale liquidity to those financial services firms that provide these services on a retail basis.

Integrity and fairness are essential to the credit and liquidity markets. The law provides for consumer protections against fraud involving these products, as well as certain other consumer protections, many of which are tired directly to the specific type of credit and liquidity product. Further, credit and liquidity products are governed by a complex body of laws. These laws include federal and state securities laws, banking laws, and laws that are tailored to the specifics of a particular class of lending activity (DHS 2010).

Investment Products

The global competitiveness of U.S. financial markets depend on and is promoted by the diversity of investment-service providers and products. These products provide opportunities for both short- or long-term investments and include debt securities (such as bonds and bond mutual funds) and equities (such as stocks or stock mutual funds), and derivatives (such as options and futures). Security firms, depository institutions, pension funds, and GSEs all offer financial products that are used for investing needs. These investment products are issued and traded in various organized markets, from physical trading floors to economic markets. U.S. Treasuries and equities (securities) are traded around the globe. Certain U.S. Treasuries and equities of some multinational companies are traded around the glove, 24 hours a day. Financial regulation for certain investment products are provided by the Treasury Department, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), banking regulators, and insurance regulators. The SEC and CFTC have legally designated Self-Regulatory Organizations (SROs). Notably, the SEC has the power to delegate authority to its SROs, national stock exchanges, and National Association of Security

Dealers (NASD) to enforce certain industry standards and requirements related to securities trading and brokerage. Similarly, the CFTC oversees exchanges and the industry SRO, that is, designated futures exchanges and the National Futures Association (NFA), which have regulatory authority to enforce industry standards and requirements related to futures trading and participants. These regulatory requirements are directed toward consumer protection, fair and orderly markets, and the ongoing capability of financial services firms to meet financial obligations (DHS 2010).

Risk Transfer Products and Insurance

A wide variety of financial institutions provide risk transference products to meet market needs. For example, the transfer of financial risks, such as the financial loss due to theft or the destruction of physical or electron property resulting from a fire, cyberattack, or other loss event, or the loss of income due to a death or disability in a family, is an import tool for the sustainability of businesses and economic vitality of individuals and their families.

Measuring in the trillions of dollars, the U.S. market for financial risk transfer products is among the largest in the world. These products range from straightforward to exceedingly complex. For example, insurance companies, futures firms, and forward market participants offer financial products that allow customers to transfer various types of financial risks under a myriad of circumstances. Marketplace efficiency often requires that market participants engage in both financial investments as well as in financial risk transfers that enable risk hedging (i.e., employing a strategy to offset potential for loss). Financial derivatives including futures and security derivatives can provide both of these functions for market participants (DHS 2010).

Regulation of Financial Services Firms

All financial services firms are subject to the constraints of the financial market, and these markets have certain, though often informal, market constraints and self-regulation. Additionally, many of these financial firms are subject to additional governmental and legally mandated regulation and self-regulation. Such regulation is designed to provide reasonable assurance that consumers are protected, and that the financial services firm is able to meet its financial obligations on an ongoing basis. The U.S. financial regulatory system includes federal and, in some cases, SROs concerned among other responsibilities with institutional and systemic ability to withstand operational disruptions (DHS 2010).

State Regulation of Financial Services Firms

Insurance services are unique in that they are primarily regulated by states (however, other financial services may be regulated at both the federal and state levels). With regard to insurance services in particular, under the McCarran-Ferguson Act of 1945, Congress affirmed the right of the stated exclusively to regulate the insurance industry. Except for a few federal laws and regulations, state insurance commissioners general have regulatory authority over all aspects of a firm's business, including rates and terms of policies, qualifications for licensing, market conduct, and financial structures and practices.

The chief insurance regulatory officials from each state collaborate through the National Association of Insurance Commissioners (NAIC). Many of the state insurance regulators review the disaster response and business continuity plans of insurers and conduct periodic examinations of these plans. The NAIC developed a handbook for state insurance regulatory response to disasters entitled, *The State Disaster Response Plan.*

In addition to the insurance industry, state agencies regulate banks, thrifts, and credit unions that are state-chartered. Although membership in the Federal Reserve System is optional for state-chartered banks, all of the banks are insured by the Federal Deposit Insurance Corporation (FDIC). State agencies also regulate the purchase and sale of securities and the provision of investment advice regarding securities (DHS 2010).

THE BOTTOM LINE

In addition to the critical dependencies for the financial services sector mentioned to this point it is important to note that physical security of financial services sector facilities (covered in the prologue and in detail later) is important but, actually, the focus of security of this sector is a different kind. Much of the financial services infrastructure is vulnerable to cyberattack from either inside or outside of the network. Cybersecurity is addressed later. Also, financial services infrastructure is extremely dependent on the IT sector (covered in detail in another of the volumes in this series).

The bottom line is that from this discussion, it is clear that any number of interdependencies could threaten one of the key components of our critical national infrastructure, the financial services sector. These factors are the "realities" of the financial services sector and go beyond just the core precepts of good system development and design. Cleary, there is a great deal of interdependence on other outside factors that could threaten financial services and other key resources. Without the active participation of each of

these sectors, the key and essential facilities of the financial services industry could be very vulnerable, a fact that is not acceptable for the protection of our national interests.

REFERENCES AND RECOMMENDED READING

DHS. 2010. *Banking and Finance Sector-Specific Plan—An Annex to the National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security.

DHS. 2017. *Financial Services Sector*. Washington, DC: Department of Homeland Security. Accessed May 6, 2017 @ https://www.dhs.gov/financial-services-sector.

DOT/DHS. 2015. *Financial Services Sector-Specific Plan*. Washington, DC: U.S. Department of Treasury and Department of Homeland Security.

Haimes, Y. Y. 2004. *Risk Modeling, Assessment, and Management*, 2nd Edition. New York: John Wiley & Sons, p. 699.

Henry, K. 2002. New Face of Security. *Government Security*, April, pp. 30–37.

NSHS. 2006. *National Strategy for Homeland Security*. Accessed May 13, 2006 @ www.whitehouse/homeland.

Sauter, M. A. and J. J. Carafano. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York: McGraw-Hill.

Spellman, F. R. 1997. *A Guide to Compliance for Process Safety Management/ Risk Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.

Chapter 2

Terrorist Attacks against Americans and United States Financial Services

> America is no longer protected by vast oceans. We are protected from attack only by vigorous action abroad, and increased vigilance at home.
>
> —President George W. Bush, 2002

> Cyber criminals can significantly threaten the finances and reputations of United States businesses and financial institutions. Given the abundance of potential victims and profits, cyber criminals will likely continue to target these entities.
>
> —Gordon M. Snow, former assistant director FBI, Cyber Division

It was not that far in America's distant past that the threats we dealt with mostly were the ramifications of natural disasters. Although never welcomed, these natural occurrences were expected, planned for, guarded against, and recovered from. Of course, there have always been the human-made or human-caused disasters that we also had to contend with. The sinking of the *Titanic* prompted new safety regulations for passenger ships; a fire at New York City's Triangle Shirtwaist Factory in 1911 caused the deaths of 146 young women and was the catalyst for the development of workplace safety and fire regulations. But the ultimate wake-up call for Americans came in the form of the events that we now summarize as "9/11": On September 11, 2001, terrorists struck at the heart of America—on American soil in a way that is unforgettable. Airplanes filled with people and fuel were turned into guided missiles of death and destruction.

What the 9/11 terrorists provided us with was a wake-up call. It was a wake-up call that alerted us to a new type of hateful venom—coldly delivered by groups or individuals to kill massive numbers of people, cause substantial

property damage, and affect economic stability. Most importantly, for the public and emergency responders the events of 9/11 brought to the forefront knowledge and awareness that just about anything unthinkable is possible. The bottom line: security of the homeland is vital to all of us.

As noted by that great philosopher (Bob Dylan, of course) in the song "Times They Are A Changing"—recent terrorist events have made this well-worn statement certainly the case. For example, with the manifestation of the Islamic State of Iraq and Syria (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL) and by its Arabic language acronym Daesh, and other terrorist groups—including inside and outside fanatics—there are many out there that who would kill us all. It is important to point out with the advent of insider threats, that is, domestic terrorism. The message of this book is the same as in the other books in this series where the focus has been shifted to the Lone Wolf (or as Williams VII stated in the prologue, lone Utah Raptor) terrorist. The fact is that there are homegrown terrorists, plotting, quivering in the glory of mass murder and destruction and the attended glory of making the headlines in the sickest sense possible. Again, remember, these are people who live among us, who shop in our stores, who use the benefits of our free society to grow their hate and to enhance their total disgust for all those things that we value in life.

Before 9/11 terrorism was not previously seen as a significant threat to the United States. However, while the United States has not experienced continuous 9/11-type terror events in the past, the current climate suggests that the United States is at significant risk of further terror activity in the future. Forecasting the future is impossible, but we can look at the past and learn from it. Table 2.1 summarizes past acts of sabotage/terrorism carried out in the United States, or against U.S. citizens overseas.

WHAT IS TERRORISM?

A few terms often are not only poorly defined but also defined from different and conflicting points of view. The definition of *terrorism* is an example.

Standard Dictionary Definition of Terrorism

After reviewing several dictionaries (too many to list here), we have found this fairly standard definition of terrorism:

> The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons.

Table 2.1 Selected Terror Attacks since 1993 (Within the United States or against Americans Abroad)*

Date/Location	*Summary of Attacks*
February 26, 1993, New York City	World Trade Center truck bomb in garage. Six deaths and 1,042 injuries. Intended structural collapse did not occur. Several members of Middle Eastern extremist organizations convicted of roles in the bombing.
April 19, 1995, Oklahoma City	Truck bomb exploded outside Alfred P. Murrah Federal Building, collapsing walls and floors which killed 168 people. More than 300 other buildings sustained damage. Timothy McVeigh and Terry Nichols later convicted in the anti-government plot to avenge the Branch Davidian standoff in Waco, TX, exactly two years earlier.
November 13, 1995, Riyadh, Saudi Arabia	Car bomb exploded at U.S. military training facility, killing six, including five U.S. military servicemen.
October 9, 1995, Hyder, Arizona	Amtrak Sunset Limited passenger train traveling from New Orleans to Los Angeles carrying 248 people derailed, killing 1 and injuring 78. Investigations indicated that tracks had been deliberately tampered with by one or more who left anti-government notes at the site.
June 25, 1996, Dhahran, Saudi Arabia	Truck bomb exploded outside Khobar Towers housing complex, killing 20, including 19 American servicemen, and injuring hundreds of others. Alleged members of Hezbollah were indicted on charges relating to the attack in June 2001.
July 27, 1996, Atlanta, Georgia	Bomb exploded at Centennial Olympic Park during the 1996 Summer Olympics killing one and injuring 111. Domestic terrorist convicted.
August 7, 1998, Nairobi, Kenya and Dar es Salaam, Tanzania	Truck bombs exploded almost simultaneously near two U.S. embassies, killing 224 (213 in Kenya and 11 in Tanzania) and injuring about 4,500. Attributed to al Qaeda. Indictments were brought against 22 men—including Osama bin Laden—but only four men were convicted of the killings in May 2001 and later sentenced to life in prison.
September 11, 2001, New York City, Washington, DC, and Pennsylvania	Al Qaeda terrorists hijacked four commercial jet airlines. Two aircraft used against World Trade Center Towers in NYC, third against Pentagon. Fourth aircraft brought down by passenger intervention. Approximately 3,000 killed.
September 18–October 9, 2001, United States	U.S. postal system used as delivery vehicle for anthrax spores contained in letters. News organizations and government representatives were targeted. Five people died and 17 suffered effects.
May 12, 2003, Riyadh, Saudi Arabia	Suicide bombers killed 35, including nine Americans, at housing compounds for Westerners. Al Qaeda suspected.

(*Continued*)

Table 2.1 (Continued)

Date/Location	*Summary of Attacks*
December 6, 2004, Jeddah, Saudi Arabia	Terrorists stormed the U.S. consulate, killing nine consulate employees.
November 9, Amman, Jordan	Coordinated bombings hit three hotels—Radisson SAS Hotel, Grand Hyatt Hotel, and Days Inn—in Amman, Jordan, killing more than 60 people and injuring 115. Al Qaeda claimed responsibility.
September 13, 2006, Damascus, Syria	Syrian terrorists attacked the U.S. embassy, but Syrian security forces intervened to stop it.
January 12, 2007, Athens, Greece	The U.S. embassy was fired on by an anti-tank missile causing damage but no injuries.
December 11, 2007, Algiers, Algeria	About 41 people were killed, including 17 United Nations staff members, when al Qaeda terrorists detonated two car bombs near the Constitutional Court and United Nations offices.
July 13, 2008, Quam, Afghanistan	Nine U.S. soldiers died when Taliban militants boldly attacked an American base bordering Pakistan.
September 16, 2008, Sana, Yemen	A car bomb and rocket struck the U.S. embassy in Yemen as staff arrived to work, killing 12 people. At least 25 suspected al Qaeda militants were arrested for the attack.
November 26–29, 2008, Mumbai, India	Pakistani terrorists targeting sites popular with Americans and other foreign tourists attacked two five-star hotels, a hospital, a train station, and a cinema. More than 300 people were wounded and 161 people died, including at least 5 Americans.
June 1, 2009, Little Rock, Arkansas	Abdulhakim Muhammed, a convert to Islam from Memphis, Tennessee, shot two soldiers outside a military recruiting center, killing one. He pled allegiance to al Qaeda.
December 25, 2009	A Nigerian man on a flight from Amsterdam to Detroit ignited a hidden chemical explosive but the fire was suppressed by two other passengers. The would-be bomber claimed allegiance to al Qaeda.
December 31, 2009, Afghanistan	A suicide bomber killed eight CIA employees at a military base in Khost Province, Afghanistan. The Taliban claimed responsibility.
May 1, 2010, New York City	A car bomb was discovered in Times Square that failed to detonate. Faisal Shahzad pled guilty to 10 terrorism and weapons charges.
May 10, 2010, Jacksonville, Florida	A pipe bomb exploded while approximately 60 Muslims were praying in the Islamic Center of Northeast Florida. The attack caused no injuries.
September 11, 2012, Benghazi, Libya	Militants armed with antiaircraft weapons and rocket-propelled grenades fired upon the American consulate, killing U.S. ambassador to Libya Christopher Stevens and three other embassy officials.

(*Continued*)

Table 2.1 (Continued)

Date/Location	*Summary of Attacks*
April 15, 2013, Boston, Massachusetts	Pressure cooker bombs exploded near the finish line of the Boston Marathon. Three people were killed and more than 260 people were injured. Three days later, the two suspects—brothers from Chechnya—went on a shooting/robbing spree in an attempt to escape arrest, killing two police officers.
August 19–September 2, 2014	ISIS murdered two American journalists—James Foley and Steven Sotloff—by decapitation after holding them hostage.
December 2, 2015, San Bernardino, California	Fourteen people were killed and more than 20 wounded when husband and wife Syed Rizwan Farook and Tashleen Malik opened fire at an employee holiday partly at the Inland Regional Center, San Bernardino, California. The suspects, killed later in a shootout, claimed to be inspired by ISIS.
June 12, 2016, Orlando, Florida	A gunman who claimed allegiance to ISIS in a 911 call opened fire at an Orlando nightclub, leaving 49 people dead and injuring 58. He was targeting the LGBT community. The gunman died at the scene.
October 31, 2017, New York City	A "self-radicalized" terrorist supporting ISIS ran a van down the Hudson River Park bike path, killing 8 people and injuring 11.

*Adapted from *Terrorist Attacks in the U.S. or Against Americans*. @http://www.infoplease.com/ipa/A0001454.html.

America's *National Strategy for Homeland Security* defines terrorism as follows:

> Any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments. (White House 2006)

The U.S. State Department defines terrorism thus:

> Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. (U.S. Congress 2005)

The FBI definition of terrorism is as follows:

> The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (FBI 2006).

Note that the FBI divides terrorism into two categories: domestic (homegrown), involving groups operating in and targeting the United States without

foreign direction; and international, involving groups that operate across international borders and/or have foreign connections.

Well, at this point the obvious question is this: Do you now know what terrorism is? That is, can you definitively define it? If you can't define it, you are not alone—not even the U.S. government can definitively define it. Maybe we need to look at other sources—views from the real experts on terrorism.

Osama bin Laden's View on Terrorism

> Wherever we look, we find the U.S. as the leader of terrorism and crime in the world. The U.S. does not consider it a terrorist act to throw atomic bombs at nations thousands of miles away [Japan during World War II], when those bombs would hit more than just military targets. Those bombs rather were thrown at entire nations, including women, children, and elderly people. (Bergen 2002, 21–22)

Another View

This view is from court testimony on terrorism from Ramzi Ahmed Yousef, who helped organize the first terrorist attack on the World Trade Center in 1993:

> You keep talking also about collective punishment and killing innocent people to force governments to change their policies; you call this terrorism when someone would kill innocent people or civilians in order to force the government to change its policies. Well, when you were the first one who invented this . . . .
>
> You were the first one who killed innocent people, and you are the first one who introduced this type of terrorism to the history of mankind when you dropped an atomic bomb which killed tens of thousands of women and children in Japan and when you killed over a hundred thousand people, most of them civilians, in Tokyo with fire bombings.
>
> You killed them by burning them to death. And you killed civilians in Vietnam with chemicals as with the so-called Orange Agent. You killed civilians and innocent people, not soldiers, innocent people every single war you went. You went to wars more than any other country in this century, and then you have the nerve to talk about killing innocent people.
>
> And now you have invented new ways to kill innocent people. You have so-called economic embargo which kills nobody other than children and elderly people, and which other than Iraq you have been placing the economic embargo on Cuba and other countries for over 35 years.
>
> The government in its summations and opening said that I was a terrorist. Yes, I am a terrorist and I am proud of it. And I support terrorism so long as it was against the United States government and Israel, because you are more than

> terrorists; you are the one who invented terrorism and using it every day. You are butchers, liars and hypocrites. (excerpts from court 1998)

And finally, here is an old cliché on a terrorist:

> One man's terrorist is another man's freedom fighter.

Again, from the preceding points of view, it can be seen that defining terrorism or the terrorist is not straightforward and never easy. Even the standard dictionary definition leaves us with the vagaries and ambiguities of other words typically associated with terrorism, such as in the definitions of *unlawful* and *public welfare* (Sauter and Carafano 2005).

Raphael Perl (2004) in a Congressional Research Service (CRS) report points out that one definition widely used in U.S. government circles, and incorporated into law, defines *international terrorist* as terrorism involving the citizens or property of more than one country.

Terrorism is broadly defined as politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. For example, kidnapping of U.S. birdwatchers or bombing of U.S.-owned oil pipelines by leftist guerrillas in Columbia would qualify as international terrorism. In 22 U.S.C. 2656f, a *terrorist group* is defined as a group which practices terrorism or has significant subgroups that practice terrorism. Perl points out that one of the shortfalls of this traditional definition is its focus on groups and its exclusion of individual ("lone wolf") terrorist activity, which has recently risen in frequency and visibility.

At this point, readers may wonder, "Why should we care what the definition of terrorist or terrorism is?" Definitions are important because in order to prepare for the terrorism contingency, domestic or international, we must have some feel, as with any other problem, for what it is we are dealing with. We are fighting a war of ideas. We must attempt to understand both sides of the argument, even though the terrorist's side makes no sense to an American or other freedom-loving occupant of the globe.

The Washington Times (2009) reported that in an interview with German magazine *Der Spiegel*, then secretary of Homeland Security Napolitano said that she rejected the word *terrorism*, and has instead renamed terrorist acts using the euphemism "man-caused disasters," because "it demonstrates that we want to move away from the politics of fear, toward a policy of being prepared for all risks that can occur." This is analogous to stating that we should refer to serial killers, serial rapists, and serial arsonists as man-caused afflictions. After all, we do not want to create fear about serial offenders. Get real! The author of this text suggests that former secretary Napolitano read the remarks we mentioned earlier by Ramzi Ahmed Yousef:

> Yes, I am a terrorist and I am proud of it. And I support terrorism as long as it was against the United States Government and Israel.

Finally, while it is difficult to pinpoint an exact definition of terrorism (but not difficult to rename it and call it something else), we certainly have little difficulty in identifying it when we see it, when we feel it, when we suffer from it. By any other name terrorism is best summed up as an absolute feeling of Terror—nothing judgmental about that—just Terror with a capital *T*.

For my purposes, probably the best definition of terrorism is given in U.S. Department of Homeland Security's *Defense Industrial Base Sector-Specific Plan* (2010):

> Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate [instill] fear, intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Ok, you say, several definitions of terror have been presented. The question is which definition will be used in this book and in all 16 volumes of the Critical Infrastructure and Homeland Security series? Probably the best definition of terrorism is given in the U.S. Department of Homeland Security's *Defense Industrial Base Sector-Specific Plan* (2010). DHS's definition is

> Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate [instill] fear, intended to coerce of intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Other Important Definitions

In addition to the definition of terrorism I include a few of the important definitions related to this discussion of critical infrastructure in the following (DHS 2010). (See also the Appendix for more terms.)

All hazards—a grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects.

Asset (Infrastructure)—a distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated

by domestic, foreign, public, or private sector organizations. DHS states an asset is a person, structure, facility, information, material, or process that has value.

Business continuity—strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions and continue business operations at an acceptable predefined level. DHS states business community is the ability of an organization to continue to function before, during, and after a disaster.

Consequence—the effect of an event, incident, or occurrence. For the purposes of this book, consequences are divided into four main consequences: public health and safety, economic, psychological, and governance impacts.

Control systems—computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurements and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include Supervisory Control and Data Acquisition systems, Process Control Systems, and Distributed Control Systems.

Critical infrastructure—systems and assets, whether physical or virtual, so vital that the incapacity of destruction of them may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these factors, across any federal, state, regional, territorial, or local jurisdiction.

Critical infrastructure information (CII)—information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems, CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computed-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law; harms the interstate commerce of the united States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical

infrastructure of a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
- Any planned or past operation problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation.

Cybersecurity—the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communication systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wire line, wireless, satellite, public-safety answering points, and 911 communication systems and control systems.

Defense critical asset—an asset of such extraordinary important to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of DoD to fulfill its mission.

Defense Production Act of 1950 (DPA)—under Title 1 of the act, as amended (50 U.S.C. App. 2061 et seq.), the president is authorized to require preferential acceptance and performance of contracts or orders supporting certain approved national defense and energy programs, and to allocate materials, services, and facilities in such a manner as to promote these approved programs. Under Title VII, the president is authorized to conduct mandatory surveys and analyses, and prepares reports on specific subsectors of the U.S. DIB. The DPA's current definition of "national defense" includes programs for military and energy production or constructions, military or critical infrastructure assistance to any foreign nation, homeland security, stockpiling, space, and any directly related activity. The DPA authority has also been extended to support emergency preparedness activities under Title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act), as amended (42 U.S.C 5195 et seq.), and critical infrastructure protection and restoration (Public Law 111-67).

Dependency—the one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly. It is a relationship or connection whereby one entity is influenced or controlled by another (Department of Defense Directive [DoDD] 3020.40, August 19, 2005).

- *Interdependency*—relationships or connections between entities of different functions, networks, sectors, or service (DoDD 30020.40, August 19, 2005).

- *Intra-dependency*—relationships or connections between entities within a common function, network, sector, or service (DoDD 3020.40, August 19, 2005).

DIB Critical Asset—an asset determined by DoD to be critical to successful execution of its missions.

Government Coordinating Council (GCC)—the government counterpart to the SCC for each sector established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the security and operational landscape of each individual sector.

Incident—an occurrence caused by either human action or natural phenomena that requires action to prevent or minimize loss of life or damage to property and/or natural resources (JP 3-18).

Infrastructure—(1) It is the framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities that enable continued flow of goods and services (DoDD 3020.40); all building and permanent installations necessary for support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations) (JP 3-35). (2) It is the framework of interdependent networks and systems comprising identifiable industries, institutions (include people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act of 2002, infrastructure includes physical, cyber, and/or human elements.

Key resources—publicly or privately controlled resources essential to the minimal operation of the economy and government.

Mitigation—actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure (DoDD 3020.40).

Network—a group or system of interconnected or cooperating entities, normally characteristic as being nodes (assets), and the connections that link them (DoDD 3020.40). The DHS definition of network is a group of components that share information or interact with each other in order to perform a function.

Owners and operators—those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness—activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts at all levels of government, and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents.

Prevention—the security procedures undertaken by the public and private sectors to discourage terrorist acts (JP 3-07.2).

Prioritization—In the context of this presentation, prioritization is the process of using risk assessment results to identify where risk-reduction or mitigation efforts are most needed, and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection—preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (JP 3-0). DHS states that protection is an action or measure taken to cover or shield from exposure, injury, or destruction. In the context of this book, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resilience and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercise, and implementing cybersecurity measures, among various others.

Recovery time objective—target time set for resumption of product, service, or activity delivery after an incident. Note: The recovery time objective must be less than the maximum tolerable period of disruption.

Resilience/resiliency—the adaptive capacity of an organization in a complex and changing environment (ISO 31000).

Note 1: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period after being affected.
Note 2: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when it must.
Note 3: There are three levels of resilience: National, Continuous Integration (CI System), and Individual.

(A) National—willpower to bounce back
(B) CI Systems—identify critical nodes for protection and planning prioritization; create, adaptive grids to ensure redundancy
(C) Individual

Response—activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increasing security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity and apprehending actual perpetrators and bringing them to justice.

Risk—probability and severity of loss linked to threats or hazards (DoDD 3020.40). DHS states risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk management framework—a planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks, assessing risks; prioritizing and implementing protection programs and resilience strategies, measuring performance, and taking corrective action. Public and private sector entities often include risk management frameworks in the business continuity plans.

Sector—a sector is a logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.

System—a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements forming a unified whole (JP 3-0). DHS states a system is any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

Threat—an adversary having the intent, capability, and opportunity to cause loss or damage (DoDD 3020.40). DHS definition of threat is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Value proposition—a statement that outlines the national and homeland security interest in protecting the nation's critical infrastructure and articulates benefits gained by all partners through the risk management framework.

Vulnerability—the characteristic of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation (or incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard (DoDD 3020.40). The DHS definition of vulnerability is a physical feature or operational attribute that renders an entry open to exploitation or susceptible to a given hazard.

REFERENCES AND RECOMMENDED READING

Bergen, P. L. 2002. *Holy War, Inc: Inside the Secret World of Osama bin Laden*. New York: Touchstone Press, pp. 21–22.

CRS. 2006. *Chemical Facility Security. CRS Report for Congress*. Washington, DC: Congressional Research Service—The Library of Congress.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2010. *Banking and Finance Sector-Specific Plan—An Annex to the National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security.

DHS. 2017. *Financial Services Sector*. Washington, DC: Department of Homeland Security. Accessed May 6, 2017 @ https://www.dhs.gov/financial-services-sector.

DOT/DHS. 2015. *Financial Services Sector-Specific Plan*. Washington, DC: U.S. Department of Treasury and Department of Homeland Security.

FEMA. 2015. *Protecting Critical Infrastructure against Insider Threats.* Accessed April 17, 2015 @ http://emilms.fema.gov/IS0915/IABsummary.htm.

Gurr, T. R. 1968. Psychological Factors in Civil Violence. *World Politics*, 20, No. 32, January, 245–78.

Haimes, Y. Y. 2004. *Risk Modeling, Assessment, and Management*, 2nd Edition. New York: John Wiley & Sons, p. 699.

Henry, K. 2002. New Face of Security. *Government Security*, April, pp. 30–37.

Lindsey, H. 2001. *Vocabulary of Hate*. Accessed April 18, 2008 @ www.wordnetdaily.com.

NSHS. 2006. *National Strategy for Homeland Security*. Accessed May 13, 2006 @ www.whitehouse/homeland.

New York Times. 1998. Excerpt from Court Testimony. January 9, 1998, p. B4.

Old Dominion University. 2000; 2002. *Violence in the Workplace: Security Concerns*. From a series of lectures presented to environmental health students. Norfolk, VA.

Perl, R. 2004. *Terrorism and National Security: Issues and Trends*. CRS Issue Brief IB10119. Washington, DC.

Sauter, M. A. and J. J. Carafano. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York: McGraw-Hill.

Spellman, F. R. 1997. *A Guide to Compliance for Process Safety Management/ Risk Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.

The Washington Times. 2009. Napolitano Tells It Like It Isn't. Accessed March 29, 2009 @ www.washingtontimes.com/news/2009/mar/29/tell-it-like-it-is-man-casued-disasters-is-mapolit/.

United States Congress. 2005. *Annual Country Reports on Terrorism*. 22 USC, Chapter 38, Section 2656f.

Chapter 3

Critical Infrastructure

> In providing a secure environment, the key function is to connect the dots. In designing and building infrastructure to withstand terrorism, the mantra is Resilience, Resilience, Resilience.
>
> —Frank R. Spellman

> While it is not so easy to definitively define terrorism and/or the terrorist, we have less difficulty identifying the likely targets of terrorists. In America, we call these likely targets our critical infrastructure; that is, they are the essential services that underpin American society and serve as the backbone of our Nation's economy, security, and health.
>
> —U.S. Department of Homeland Security

WHAT IS CRITICAL INFRASTRUCTURE?

For the United States of America, 9/11 was a slap in the face, a punch in the gut (actually, the ultimate sucker punch), and the most serious wake-up call. The 9/11-wake-up call generated several reactions on our part—obviously, protecting ourselves from further attack became (and hopefully still is) priority number one. In light of this important need, the Department of Homeland Security was created. As described by Tom Ridge, the first secretary of the new department, "You may say homeland security is a Y2K problem that doesn't end January 1 of any given year" (Henry 2002). And, according to Barack Obama (2007), the Department of Homeland Security does "the work that ensures no other family members have to lose a loved one to a terrorist who turns a plane into a missile, a terrorist who straps a bomb around her

waist and climbs aboard a bus, a terrorist who figures out how to set off a dirty bomb in one of our cities."

Among other things, the new emphasis on homeland security pointed the need to protect and enhance the security of the nation's critical infrastructure. Critical infrastructure can be defined or listed in many ways. Generally, governments use the term to describe material assets, systems, and services that are essential for the functioning of an economy and society and maintaining public confidence. Destruction or compromise of any of these systems or services would have a debilitating impact on the area either directly, through interdependencies or from cascading effects. For the purpose of this text, critical infrastructure is defined as those assets of key physical resources and computer-/service-based systems that are essential to the minimum operations of economy and government. The 16 critical infrastructures (in author's opinion and making up the volumes in this series) are the following:

- Critical manufacturing
- Food and agriculture
- Financial (banking and finance)
- Chemical and hazardous materials
- Defense industrial base
- Emergency services
- Energy
- Public health
- Communications
- Transportation
- Water and wastewater
- Dams
- Information technology
- Commercial facilities
- Government facilities
- Nuclear power plants

DID YOU KNOW?

More than 85 percent of the critical infrastructure within the United States are owned and operated by the private sector.

Although we did not list cyberspace and all ancillaries (excluding, of course, the listing of information technology [IT]) involved in or with digital operations (e-technology), in this current era we can state without

equivocation or ambiguity that the digital communication connection is the glue that holds all critical infrastructure together. This is the case, of course, because all separate infrastructures are interconnected (lots of crossover; refer to figure 1.1) in one way or another. This may surprise you to some degree, but think about it—we are speaking about present reality of e-technology. It would be hard to imagine that any of the above listed infrastructure sectors could operate today without e-technology.

CLICKS-AND-BRICKS

Virtual banking, also known as *online banking, e-banking*, or *internet banking* is an electronic payment system that enables customers of a bank or other financial services institution to conduct a range of financial transactions through the institution's website. Online banking is the business model also known as *clicks-and-bricks* (aka *bricks and clicks, click and mortar,* or *bricks, clicks, and flips*); the online part of the business model is *clicks* and the offline is *bricks*. The clicks-and-bricks model allows customers to conduct financial transactions online or physically in one of their financial institutions. Virtual banking allows customers to perform various tasks, including the following:

- Download periodic account statements
- Order check books
- View recent transactions
- View account balances
- View record of paid checks
- Transfer funds between customer's linked accounts
- Apply for loan
- Pay utility bills
- Obtain personal financial management support

Online banking offers the customer advantages, including the following:

- Universal access
- Time savings
- Quick transfer of funds
- Permanent access to bank account
- Cost savings

The most prominent factor involved in online banking is security. Not only is the customer's funds important to protect, guard, and guarantee but also the security of the customer's financial information is important. The importance

of ensuring security of e-banking and other digital business transactions is discussed in detail later in the text.

THE BOTTOM LINE

Again, it is important to point out that the financial services sector provides services that are essential to U.S. defense, offense, security, and economy to protect and ensure the standard of living we presently enjoy. The financial services sector is well aware of its vulnerabilities and is leading a significant, mandated, and voluntary effort to increase its planning and preparedness. Cooperation through industry groups has resulted in substantial information sharing of effective and best practices across the sector. Many sector owners and operators have extensive experience with infrastructure protection and have more recently focused their attention on cybersecurity. In addition to the economic consequences of a successful homegrown or foreign terrorist attack against financial services sector facilities, there is also the potential of a threat to public health and safety and the environment. I hope that this book and the others in the critical infrastructure series will aid in the prevention and mitigation of deliberate attacks.

REFERENCES AND RECOMMENDED READING

CBO. 2004. *Homeland Security and the Private Sector*. Washington, DC: Congressional Budget Office.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2010. *Banking and Finance Sector-Specific Plan—An Annex to the National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security.

DHS. 2017. *Financial Services Sector*. Washington, DC: Department of Homeland Security. Accessed May 6, 2017 @ https://www.dhs.gov/financial-services-sector.

DOT/DHS. 2015. *Financial Services Sector-Specific Plan*. Washington, DC: U.S. Department of Treasury and Department of Homeland Security.

FAO. 2005. *Bridging the Rural Digital Divide*. New York: United Nations. Accessed April 19, 2008 @ www.fao.org/rdd.

FEMA. 2015. *Protecting Critical Infrastructure against Insider Threats.* Accessed April 17, 2015 @ http://emilms.fema.gov/IS0915/IABsummary.htm.

FR. 2003. Notice of Proposed Rulemaking. *Federal Register*, 68, No. 90.

Henry, K. 2002. New Face of Security. *Government Security*, April, pp. 30–37.

Horn, F. P. 1999. *Statement Made Before the United States Senate Emerging Threats and Capabilities Subcommittee of the Armed Services Committee*. Accessed June 27, 2007 @ www.Senate.gov/~armed_servies/statement/1999/991027fh.pdf.

Lane, J. 2002. Sworn Testimony, Congressional Field Hearing, House Committee on Government Reform, Abilene, KS.

Obama, B. 2007. *Homeland Security*. http://www.whitehouse.gov/agenda/homeland_security/.

Techopedia. *Enterprise Network*. Accessed April 10, 2017 @ https://www.technopedia.com/defintion/7044/enterprise-network.

Chapter 4

Critical Infrastructure Security and Resilience

The flow of providing security protection, from data to understanding:

DATA → INFORMATION → KNOWLEDGE → UNDERSTANDING

> In the prevention of and preparation for terrorism, ending well is the best revenge.
>
> —F.R. Spellman

> The emergence of amorphous and largely unknown terrorist individuals and groups operating independently (freelancers) and the new recruitment patterns of some groups, such as recruiting suicide commandos, female and child terrorists, and scientists capable of developing weapons of mass destruction, provide a measure of urgency to increasing our understanding of the psychological and sociological dynamics of terrorist groups and individuals.
>
> —R.A. Hudson, 1999

> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.
>
> —Gene Spafford

From several terrorism incidents on financial sector critical infrastructure in the United States, South America, the Middle East, and Africa, it is apparent that financial services infrastructure is a preferred target of the terrorists. Moreover, al Qaeda, ISIS, homegrown terrorists, and others have made it clear via documented actions or threats that it has an interest in attacking the American financial services sector.

Beyond the obvious the question might be this: What makes the financial services sector such an attractive terrorism target? The financial services sector is an attractive target because of the following:

- It is easy to infiltrate and, like other lifeline functions—which include energy, transportation, and water, and other resources essential to the operations of most critical infrastructure partners and communities financial—it is a target of choice.
- Financial services sector components or assets are spread throughout the nation with little definition of boundaries.
- Much of the financial services sector business is conducted using equipment that is one-of-a-kind technical electronics (ATM machines) and computer systems which are difficult to replace in the short term.
- Initially, several financial sector components were designed and constructed without concern for terrorist intrusion or destructive activities.
- Many financial services systems are monitored and operated using underprotected computer systems.
- As with many of the industries attempting to economize, many financial services segments and subsegments assign responsibility for safety and security as a collateral duty to a line employee instead of employing a fulltime certified cyber and safety of IT safety and security professional.

FINANCIAL SERVICES SECTOR SECURITY GOALS AND ATTRIBUTES

The Department of Homeland Security (DHS) has identified eight general security goals and attributes.

- *Critical Asset Reduction Goal*: Sector resiliency will be most assured if no particular asset can be assessed as more critical than any other. While the ultimate ideal goal would be zero critical financial services assets, the sector will strive to reduce the number of critical assets whenever and wherever possible within fiscal and legal constraints. Sound risk management practices including asset resiliency, mitigation of risks, and redundancy will be shared and advanced throughout the sector.
- *Cyber Goals and Attributes*: Like physical attributes, these assist the financial services sector to evaluate consequences and vulnerabilities, and develop protective strategies. Cyber systems that link and help monitor

and control the financial services systems are increasingly recognized as a potential vulnerability. All information that identifies or otherwise describes characteristics of a critical financial services asset that is created, held, and maintained by the government or the private sector will be protected from unauthorized disclosure according to established procedures, appropriate to the particular level of information.

- *Volumetric or Throughput Attributes*: These define the extent of any damage, depending on the utilized capacity of the systems, or points where the system may be capacity constrained.
- *Personnel Security Goals and Human Attributes*: Ensure all personnel directly associated with a critical financial services asset are vetted for employment suitability, reliability, and trustworthiness using established processes commensurate with requirements of the respective positions held, in conformance with pertinent security policy. Highly trained and skilled personnel are key factors in a comprehensive financial services sector security plan. The availability of skilled and experienced technical talent is a concern in the financial services sector. Sustaining essential technical knowledge is critical to maintaining the sector's safety, reliability, and security.
- *Physical Security Goal*: Determines the impact or consequence of critical financial services asset loss its mission(s) supported, the known or perceived threat, and the susceptibility to exploitation of vulnerabilities the threat is capable of perpetuating; identify specific financial services assets, the destruction or disruption of which could result in human casualties or economic disruption similar to the effects of weapons of mass destruction; compile a composite of facility physical security risk assessments.
- *Insider Threat Goal and Attributes*: Responsible parties in charge provide security education and training aids to financial services asset owners/operators not having security program so that they may implement provisions for the vetting of system and network administrators commensurate with the consequences of the loss of sensitive or classified information, production or provisioning capability, and supply chain integrity.
- *Monitoring and Reporting Goals and Attributes*: Ongoing determination of the effectiveness of government threat reporting to officials, owners, and operators responsible for critical financial services assets, and to local law enforcement officials and other first-responders including, as appropriate, the medical and mass transportation communities.
- *Training and Education Goal and Attributes*: Develop and provide continuous specific security education and training materials for critical financial services asset owner/operators.

HOMELAND SECURITY DIRECTIVES

As a result of 9/11, the DHS was formed. On matters pertaining to homeland security, Homeland Security Presidential Directives (HSPDs) are issued by the president. Each directive has specific meaning and purpose and is carried out by the U.S. DHS. Table 4.1 lists HSPDs.

Table 4.1 Homeland Security Presidential Directives

HSPD—1: Organization and Operation of the Homeland Security Council. (White House) Ensures coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.
HSPD—2: Combating Terrorism through Immigration Policies. (White House) Provides for the creation of task force which will work aggressively to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.
HSPD—3: Homeland Security Advisory System. (White House) Establishes a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people.
HSPD—4: National Strategy to Combat Weapons of Mass Destruction. Applies new technologies, increased emphasis on intelligence collection and analysis, strengthens alliance relationships, and establishes new partnerships with former adversaries to counter this threat in all of its dimensions.
HSPD—5: Management of Domestic Incidents. (White House) Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
HSPD—6: Integration and Use of Screening information. (White House) Provides for the establishment of the Terrorist Threat Integration Center.
HSPD—7: Critical Infrastructure Identification, Prioritization, and Protection. (White House) Establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks.
HSPD—8: National Preparedness. (White House) Identifies steps for improved coordination in response to incidents. This directive describes the way federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident. This directive is a companion to HSPD-5.

(*Continued*)

Table 4.1 (Continued)

HSPD—8 Annex 1: National Planning. Further enhances the preparedness of the United States by formally establishing a standard and comprehensive approach to national planning.

HSPD—9: Defense of U.S. Agriculture and Food. (White House) Establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

HSPD—10: Biodefense for the 21st century. (White House) Provides a comprehensive framework for our nation's Biodefense.

HSPD—11: Comprehensive Terrorist-Related Screening Procedures. (White House) Implements a coordinated and comprehensive approach to terrorist-related screening that supports homeland security, at home and abroad. This directive builds upon HSPD – 6.

HSPD—12: Policy for a Common Identification Standard for Federal Employees and Contractors. (White House) Establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).

HSPD—13: Maritime Security Policy. Establishes policy guidelines to enhance national and homeland security by protecting U.S. maritime interests.

HSPD—14: Domestic Nuclear Detection established a Domestic Nuclear Detection Office (DNSO) to coordinate efforts to protect the domestic United States against dangers from nuclear or radiological materials. EPA supports the detection, response, law enforcement, and information sharing aspects of the DNDO's mission.

HSPD—16: Aviation Strategy. Details a strategic vision or aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans.

HSPD—18: Medical Countermeasures against Weapons of Mass Destruction. (White House) Establishes policy guidelines to draw upon the considerable potential of the scientific community in the public and private sectors to address medical countermeasure requirements relating to CBRN threats.

HSPD—19: Combating Terrorist Use of Explosives in the United States. (White House) Establishes a national policy, and calls for the development of a national strategy and implementation plan, on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

HSPD—20: National Continuity Policy. (White House) Establishes a comprehensive national policy on the continuity of federal government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of federal continuity policies.

(*Continued*)

Table 4.1 (Continued)

HSPD—21: Public Health and Medical Preparedness. (White House) Establishes a national strategy that will enable a level of public health and medical preparedness sufficient to address a range of possible disasters.
HSPD—23: Cybersecurity requires federal agencies to monitor cyber activity toward federal agencies' computer systems and, where necessary, provide action to eliminate sources of hostile action. EPA has a robust security program for both personnel and cybersecurity as mandate by the directive.

Source: USEPA (2016).

Note: HSPD-7 was revoked by the Presidential Policy Directive 21 (PPD-21) on critical infrastructure security and resilience on February 12, 2013. PPD-21 states that "Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded" (DHS 2013). Multiple changes came out of PPD-21, including six actions with specific deadlines. One of those actions was to update the National Infrastructure Protection Plan within 240 days.

Note: The significance of PPD-21 is that it deals specifically with critical infrastructure security and resilience; it defines security as reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters. Examples of security measures (DHS 2016) are listed:

- Badge entry at doors
- Using antivirus software
- Fencing around buildings
- Locking computer screens

PRD-21 defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly form disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Examples of resilience measures are listed:

- Developing a business continuity plan
- Having a generator for back-up power
- Using building materials that are made more durable

ASSESSING CHALLENGES

In its *Banking and Finance Sector-Specific Plan* (2016), DHS determined that there were many challenges facing the financial services sector; in particular

it has listed and detailed seven challenges, each of which is covered in this section.

Challenge 1: Advancing the State of the Art in Designing and Testing Secure Applications

Software flaws and inadequate patching and configuration practice are two of the sources of IT vulnerabilities; therefore, they require two different threads of thinking about research. Current research has shown that across the entire financial services industry, the information protection and risk management community is generally not well equipped to accurately or completely define, specify, estimate, calculate, and measure how to design and test secure application software. Experience has shown that continued mitigation against network vulnerabilities are ongoing and remain important; however, an increasing number of attacks are against software applications, which are not the focus of many financial institutions. The fact is business requirements and risk assessments should drive resource allocations. Risks are driven by complex applications developed in-house and by partners, extension of powerful business applications to vulnerable customers, and increasingly organized criminal attacks (e.g., SQL injections to steal copies of data bases, cross-site scripting). To be effective, application security strategies must incorporate development standards and training, automated and manual code reviews, and penetration testing with and without design specifications or source code of the applications being tested. Some financial regulators have issued supervisory guidance on risks associated with web-based applications, urging banks to focus adequate attention on these risks and appropriate risk management practices (U.S. Treasury 2008).

The testing of financial institution applications for security vulnerabilities stemming from software flaws is often inadequate, incomplete, or nonexistent. Important to financial institutions is the gaining of confidence; that is, financial institutions need to gain the confidence that is needed to deploy business-critical software with some proof of evaluation for obvious application security flaws (e.g., un-validated user input, buffer-overrun conditions). Without this confidence, financial institutions are forced to develop countermeasures and compensating controls to counter these unknown potential threats and undocumented features of the software. Without explicit security assurance testing and corresponding evidence of testing results, functional testing by development teams and outside software developers is insufficient. Financial institutions need a robust, effective, affordable, and timely security testing methodology and practice to gain the confidence required to deploy application software into sometimes hostile environments for purposes of practical and appropriate risk management.

Financial institutions, to minimize vulnerability, have urged major software providers to improve the quality of their software development and testing processes for utility software, such as operating systems, but are only beginning to urge application software developers to do the same. Major software companies and outsourcing providers are responding by developing more secure code. However, while there are important and worthwhile efforts, the financial services industry (and other users of software) remains at risk from fundamental software development practices that produce vulnerable software in the very beginning stages of development. This vulnerable software has, in turn, resulted in substantial increase in application-level attacks. Risk managers in financial institutions continue to look for solutions.

The bottom line: The financial services sector needs research on how to specify, design, and implement secure software and measure its associated life-cycle costs and the benefits of the various information security technologies and processes. The sector would benefit from better understanding of how to develop, test, and measure secure application software.

Challenge 2: More Secure and Resilient Financial Transaction Systems

The financial services sector relies on an IT infrastructure, including computing hardware, software, and telecommunications networks. Some of this infrastructure is owned and operated by financial institutions and some is provided by third-party service providers in the United States and around the globe. This infrastructure is probed and attacked by a variety of adversaries, including criminal elements and nation-states. These adversaries exploit vulnerabilities in people, processes, and technologies and perpetuate attacks for financial gain, to steal proprietary information, or to undermine consumer confidence in the financial services industry and U.S. economy. Threats from adversaries are increasing, raising concerns over the integrity of devices, networks, and applications. The infrastructure is also vulnerable to natural disasters, pandemics, and other outages. The financial services, IT, and telecommunications industries have responded to these challenges with initiatives to address security, integrity, and resilience; however, significant risks remain in terms of security breaches, fraud (including identity theft), service disruptions, and data integrity.

More secure and resilient financial transaction systems are the key to maintaining the integrity of the financial services industry. Because the trustworthiness of networks and devices is uncertain, they must resist interception and tampering over an increasingly vulnerable environment. One facet is ensuring that networks and devices are “clean” when restoring services after an interruption. Reconstitution of data after an attack requires an additional step:

Decontamination, which is the process of distinguishing a clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer as little good data as possible be discarded, this problem is quite difficult. Also of primary importance is the retention and reconstruction of transaction history while simultaneously being fully engaged in business continuity operations and executing a recovery plan. Other sectors have expressed concerns about extending their continuity plans to include vital information found on remote workstations. The possibility of this dislocation of normal corporate boundaries could be strained when relying on a distributed computing model.

As a tool for business continuity planning purposes, remote access is necessary for enhancing productivity. For example, financial institutions have developed business continuity plans to ensure employees can access networks if core facilities are not available.

The bottom line: The challenge is in finding the right mix of hardware and software that gives employees the ability to conduct their work off-site while still adhering to excessive incremental risk. It should also provide employees the ability to seamlessly move from one location to another while retaining their "session state" and desktop customization (U.S. Treasury 2008; DHS 2010).

Challenge 3: Enrollment and Identity Credential Management

A secure financial services sector infrastructure requires reliable and unambiguous identification of all parties involved in a transaction and non-repudiation of authorized transactions. Current technologies offer "spot" solutions that secure an aspect of identity management; however, much vulnerability remains. Although strong authentication credentialing technology exists, the initial identification of and linkage to an individual's identity to an authentication credential and the need to replace lost or stolen credentials remain weak links. Financial institutions rely on the individual's possession of knowledge that can be stolen, or by biometrics that can be spoofed, and may not scale up to millions of individuals without sacrificing performance. Moreover, the lack of mutual authentication allows for, among other things, the ability for the launching of successful man-in-the middle attacks (i.e., active eavesdropping attacks). Financial institutions typically rely on "spot" authentication in which the financial institution authenticates customers before a transaction. Research is needed to develop more continuous authentication and credentialing.

Challenge 4: Understanding the Human Insider Threat

Financial services institutions grant access to confidential information to authorized parties. To establish and maintain trust in this access-granting

process, financial institutions use a variety of tools and controls to identify, verify, authenticate, and authorize trustworthy individuals and contractors. Measures include background checks, credit history checks, and other historical data checks. The insider threat problem (discussed in detail later) is particularly difficult because of the interplay between technical, legal, managerial, and ethical issues. Financial institutions recognize that current measures provide only a "coarse-grained" screening for obvious human threats to begin the access-granting process; individuals are granted access to networks, systems, databases, applications, and ultimately customer and business information based on their job or role in the institution. The process is enforced via a highly complex set of overlapping operational and technical controls, which requires that a large percentage of each financial institution's total information protection budget is dedicated to access management, control, and reporting.

Financial services institutions continue to experience damage from the unprofessional, malicious, or criminal activities committed by individuals with authorized access, sometimes in coordination with external individuals, criminal organizations, or terrorists; this trend continues even through preemployment/engagement checking processes, and the layering of costly operational and technical controls are actively employed. Current approaches suggest adding additional layers—technological or procedural—of surveillance processes to detect, identify, and help stop the unwanted activities of authorized individuals. However, such approaches, while they may reduce undesirable activities, add substantial operating costs to an already costly access management approach.

Financial institutions currently have tools that could be useful in determining improper behavior of insiders. Many of these tools are based on physical and logical access but are typically not integrated. Improvements in security information management are needed to detect and prevent improper insider behavior. A critical component of improving security information management is ensuring that appropriate controls are in place to address privacy and other human resource protections.

Challenge 5: Data Centric Protection Strategies

With regard to the financial services industry, protective measures are put in place to build a more secure and resilient infrastructure to protect financial transactions; vulnerability still exists because sensitive information can be stolen by criminal elements and other adversaries who attack less secure systems connected to merchants and third-party vendors. Preserving the integrity of each transaction involves identification, authentication, and authorization of each transaction to ensure that counterparties are not criminals or money

launderers, and that sensitive information is protected and its loss, copying, or tampering is detected. While financial institutions have tools that protect data while it resides in a certain environment, these tools are not effective when the data is taken out of that controlled environment (e.g., when a user cuts and pastes in another form). A key challenge is focusing on metadata to understand when data is accessed, updated, or copied.

Challenge 6: Better Measures of the Value of Security Investments

The financial services sector seeks research on the life-cycle costs of security technologies that support critical infrastructure protection, and the creation of cost-benefit models that can be adopted within institutions and across the industry. One of the key issues in the adoption of improved protective technologies and processes is the ability of the purchasing organizations to fully understand the costs and benefits of security technologies. Inflation protection organizations, as part of their regular business, can effectively evaluate specific cost elements for various protective programs in terms of operating cost, contracting costs, and the cost of purchasing the needed technology for an organization. However, information protection organizations typically do not have good estimates of the total life-cycle costs of the protective programs on the businesses lines that are asked to implement, own, and manage these protective programs over the long term. Across the entire Banking and Finance Sector, the information protection and risk management community is generally not well equipped to accurately or completely define, estimate, calculate, measure, or communicate the benefits that result from protective programs. Further exacerbating this issue is that the "benefits" of security are often intangible and often related more to loss avoidance, making traditional return on investment (ROI) calculations difficult. There needs to be a stronger correlation between security investment and the reduction of risk and subsequent loss. Some methods used today to justify security investments may not align or be equivalent with methodologies under Generally Accepted Accounting Principles (GAAP). Research is needed to establish a baseline risk and to understand changes from the baseline that result from investment. This research also could benefit the broader risk management community.

Challenge 7: Development of Practical Standards

Practical standards and suggested practices is one of the prevailing techniques for closing the gap between state-of-the-art and state-of-the-practice. In an attempt to further the protection of the banking and finance critical infrastructures, numerous documents outlining suggested practices have

been developed, most addressing a closely circumscribed segment of banking and finance systems and practices. Unfortunately, the problem is that, to date, the industry has been unable to quantitatively correlate best practices with reduced risk. If such a relationship could be determined and quantified, financial institutions would have the tools needed to justify risk management and risk reduction measures. This analysis could, in turn, assist the industry in agreeing on a common and consistent set of practices. A related question is how practitioners and regulators should adopt or consider these in developing robust and resilient infrastructures vis-à-vis the confusion caused by so many different best practices guides and standards.

ASSESSING CONSEQUENCES

The potential physical and cyber consequences of any incident, including terror attacks and natural or human-made disasters, are the primary consideration in risk assessment. In the context of this text, consequence is measured as the range of loss or damage that can be expected. The consequences that are considered for the national-level comparative risk assessment are based on the criteria as set forth in HSPD-7. These criteria can be divided into four main categories:

- *Human Impact*: Effect on human life and physical well-being (e.g., fatalities, injures).
- *Economic Impact*: Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage).
- *Impact on Public Confidence*: Effect on public morale and confidence in national economic and political institutions.
- *Impact on Government Capability*: Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Moreover, HSPD-7 is important to the financial services sector in that it required the DHS to "serve as the focal point for the security of cyberspace" with a mission that included "analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." This directive established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks. In addition, it required heads of all federal agencies to

"develop . . . plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate." Hence, the federal government began to directly address issues of cyber security within the federal government systems (FCC 2017).

DID YOU KNOW?

The DHS has the mission to provide a common baseline of security across the federal civilian executive branch and to help agencies manage their cyber risk. The common baseline is provided in part through the EINSTEIN system. EINSTEIN services two key roles in federal government cybersecurity. First, EINSTEIN detects and blocks cyberattacks form compromising federal agencies. Second, EINSTEIN provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself (DHS 2017b).

As a result of HSPD-7, the DHS established the National Cybersecurity Division (NCSD). The objectives of this division are "to build and maintain an effective national cyberspace response system, and to implement a cyber-risk management program for protection of critical infrastructure." The primary operational arms of the division are first the Cybersecurity Preparedness and National Cyber Alert System, and secondly the U.S. Computer Emergency Response Team (US-CERT). The National Cyber Alert System was created by US-CERT and the DHS to help protect computers. One of US-CERT's overarching goals is to ensure that individuals and agencies have access to timely information through tips and alerts about security topics and events. The US-CERT has become the national first line of defense for the war of cybersecurity. The CERT's Cyber Risk Management Program assesses risk, prioritizes resources, and executes protective measures in order to secure the cyber infrastructure. It includes such things as current risk assessments and vulnerabilities that are maintained in their vulnerability database, the National Cyber Alert System, for information dissemination, and a number of other references for cybersecurity measures.

In addition to the importance of HSPD-7 providing guidance and direction in cybersecurity and financial services sector protection objectives, as a further shot in the security arm, so to speak, HSPD-23 was signed in January 2008 by President George W. Bush; this directive was necessary due to increased cyber activity on an international scale and attacks targeted at U.S. computers and networks—including computer-controlled systems. HSPD-7

established a Comprehensive National Cybersecurity initiative (CNCI). Although the document is classified, public sources have indicated that in addition to establishing the National Cyber Security Center within the DHS, the initiative had 12 other objectives (FCC 2017):

- Move toward managing a single federal enterprise network
- Deploy intrinsic detection systems
- Develop and deploy intrusion prevention tools
- Review and potentially redirect research and funding
- Connect current government cyber operations centers
- Develop a government-wide cyber intelligence plan
- Increase the security of classified networks
- Expand cyber education
- Define enduring leap-ahead technologies
- Define enduring deterrent technologies and programs
- Develop multipronged approaches to supply chain risk management
- Define the role of cybersecurity in private sector domains

DID YOU KNOW?

The federal enterprise network depends on IT systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems (DHS 2017a).

REFERENCES AND RECOMMENDED READING

Crayton, J. W. 1983. Terrorism and the Psychology of the Self. In Lawrence Zelic Freedman and Yonah Alexander, eds., *Perspectives on Terrorism*, pp. 33–41. Wilmington, DE: Scholarly Resources.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

DHS. 2016. *What is Security and Resilience?* Accessed @ https//www.dhs.gov/what-security and-resilience.

DHS. 2017a. *Securing Federal Networks*. Accessed April 15, 2017 @ https:/www .dhs.gov/topic/securing-federal-networks.

DHS. 2017b. *EINSTEIN*. Accessed April 14, 2017 @ https://www.dhs.gov/einstein.

FCC. 2017. *Public Safety Tech Topic #20—Cyber Security and Communications*. Accessed April 14, 2017 @ https://www.fcc.gov/help/public-safety-tech-topic-20-cyber-security-and-communiicaitons.

FEMA. 2015. *Protecting Critical Infrastructure Against Insider Threats.* Accessed April 17, 2015 @ http://emilms.fema.gov/IS0915/IABsummary.htm.

Ferracuti, F. 1982. A Sociopsychiatric Interpretation of Terrorism. *The Annals of the American Academy of Political and Social Science,* 463, September, 129–41.

FR. 2007. *Federal Register*, 17688–17745.

Hudson, R. A. 1999. *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why*? Washington, DC: Library of Congress.

Lees, Frank. 1996. *Loss Prevention in the Process Industries*, 3: A5.1–A5.11. New York: Butterworth-Heinemann.

Long, D. E. 1990. *The Anatomy of Terrorism*. New York: Free Press.

Margolin, J. 1977. Psychological Perspectives on Terrorism. In Y. Alexander and S. M. Finger, eds., *Terrorism: Interdisciplinary Perspectives*. New York: John Jay Press.

Olson, M. 1971. *The Logic of Collective Action.* Boston: Harvard University Press.

OMB. 1998. *Federal Conformity Assessment Activities, Circular A-119*. Washington, DC: White House.

Pearlstein, R. 1991. *The Mind of the Political Terrorist*. Wilmington, DE: Scholarly Resources, Inc.

Sullivant, J. 2007. *Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-Solving*. New York: Wiley & Sons.

USEPA. 2016. *Homeland Security Presidential Directives*. Accessed @ https://www. epa.gov/emeergency-resposne/horelamnd -security-presidential-directives.

U.S. Treasury. 2008. *Guidance on Application Security*. Accessed http://www.occ. treas.gov/ftp/bulletin/2008-16.html.

Wilkinson, P. 1974. *Political Terrorism*. London: Macmillan.

Chapter 5

Vulnerability Assessment (VA)

> Vulnerability means different things to different people . . . many associate vulnerability with a specific set of human activities.
>
> —S. S. D. Foster, 1987

> But there's one thing we must all be clear about: terrorism is not the pursuit of legitimate goals by some sort of legitimate means. Whatever the murderers may be trying to achieve, creating a better world certainly isn't one of their goals. Instead they are out to murder innocent people.
>
> —Salman Rushdie

One consequence of the events of 9/11 was Department of Homeland Security's (DHS) directive to establish a Critical Infrastructure Protection Task Force to ensure that activities to protect and secure vital infrastructure are comprehensive and carried out expeditiously. Another consequence is a heightened concern among citizens in the United States over the security of their energy infrastructure (i.e., the uninterrupted supply of electrical power and fuel to power vehicles, homes, and vital communications systems). As mentioned previously, the financial services sector is classified as "vulnerable" in the sense that inherent weaknesses in its operating environment could be exploited to cause harm to the system. There is also the possibility of a cascading effect—a chain of events—due to a terrorist act affecting financial services sector providers, which could cause corresponding damage (collateral damage) to other nearby users. In addition to significant damage to the nation's financial services sector, entities using and needing financial services to function can result in loss of life due to a lack of proper emergency response; shutdown of other industries; loss of electronic communication operational control; and other long-term impacts.

Public and private members of the financial services sector conduct risk assessments. These assessments look at issues and potential vulnerabilities both within individual organizations and sector-wide. Since risk management is part of the banking and finance culture, both regulators and private organization have a long history of conducting regular risk assessments. In the private sector some of these risk assessments are mandated through regulation and validated by the examination process. Furthermore, the private sector institutions conduct voluntary risk assessments to meet their business needs as part of their continuity planning and/or in conjunction with trade associations' recommendations and self-regulatory requirements (DHS 2007).

The Treasury Department has created a process to identify and assess vulnerabilities within the sector. The following sections refer to the efforts of the Treasury Department to identify sector vulnerabilities and assess the risks across the Banking and Finance Services Sector. Again, the following information is based on its *Banking and Finance Sector-Specific Plan* (2016).

ASSESSING VULNERABILITIES

What is a vulnerability assessment (VA)? For the purpose of this text and according to FEMA 2008, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. In addition, according to the Department of Homeland Security (DHS 2009), vulnerabilities are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Vulnerabilities may be associated with physical (e.g., a broken fence), cyber (e.g., lack of a firewall), or human (e.g., insider threats; untrained guards) factors.

VAs estimate the odds that a characteristic, of, or flaw in, an infrastructure could make it susceptible to destruction, disruption, or exploitation based on its design, location, security posture, processes, or operations. Vulnerabilities typically are identified through internal assessments and information sharing with customers, vendors, and suppliers.

A VA methodology was developed as part of the complete Financial Services Sector-Specific Plan risk assessment methodology. The methodology examined physical, cyber, and human vulnerabilities and considered relevant national preparedness threat scenarios. The process varied depending on the architecture elements being studied and included subject matter expert interviews, site visits, and modeling and analysis.

The vulnerabilities of financial services architecture elements may vary depending on whether they are operational or implementation specific. Operational vulnerabilities may include those that result from the inherent principles of network design, unanticipated network congestion caused by external factors,

or collateral consequences from major disasters or events. Implementation-specific vulnerabilities may be very particular in nature—from bugs in application software and protocol deficiencies to "backdoors" in vendor equipment firmware or software. The magnitude of the implementation vulnerabilities also varies depending on the exposure of the vulnerable equipment. While embedded firmware, for example, may have only limited exposures to configuration and maintenance functions, systems such as the Domain Name Service require a high degree of exposure in order to provide service to customers (DHS 2010).

VAs are conducted on many levels. These VAs include examinations into the potential risks resulting from cross-sector dependency, sector-specific vulnerabilities and dependencies on key assets, systems, technologies, and processes. Moreover, DHS has instituted a process to provide awareness training to financial services asset owner/operators. The purpose of the awareness training is to provide financial services sector personnel with information about the place of their asset within the overall financial services mission requirements and acquisition process so they will understand their rules and importance to the entities at the corporate level (DHS 2010). This training focuses on the following:

- Protection of financial services interests
- Protection of federal interests
- Importance of facilities fostering relationships with local responders and federal, state, and local law enforcement/civil authorities for business recovery planning.

The awareness training also informs the asset owner/operators of the protection measures applied to their proprietary and business-sensitive information provided by and to the financial services sector. Once critical financial services assets are identified and prioritized, the next step is to conduct standardized assessments. DHS, working through and with various agencies, has established a standardized mission assurance assessment for application to critical financial services assets. These assessments consider impact, vulnerability, and threat/hazard (whether from natural disaster, technological failure, human error, criminal activity, or terrorist attack). This approach to risk assessment ensures consideration of relevant factors for each financial services asset and a relative prioritization of risks to support military operations.

INSIDER THREAT VULNERABILITY

The insider threat to a financial services organization and criminal cyber activities is about malicious software (malware) and the variety of forms

of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and others. The insider threat is … a human, a person, a mammal, Homo sapiens, a breathing organism, a heartbeat. To protect an organization from insider threats the organization must "use tools to monitor the traffic in or out of the networks and be able to focus that monitoring on specific people who do something concerning or suspicious; moreover, nontechnical employee behavior must be monitored" (INSA 2017).

"Behavior must be monitored" … yes, for sure. What monitoring really comes down to, however, is awareness. An important part of any successful vulnerability assessment process is awareness. Security and risk managers (and all employees in general) working in or with the critical infrastructure sectors must be aware of the potential for insider threat vulnerability. Again, the key word is *awareness*. Awareness means that personnel within the critical infrastructure sectors must know how to identify and take action against insider threats. To achieve this critical goal, safety and security personnel must be provided with an overview of and be cognizant of common characteristics and indicators associated with malicious insiders and effective measures to counter insider threats.

Protecting against Insider Threats (FEMA 2015)

As mentioned earlier, when analyzing threats to our nation's critical infrastructure, we tend to focus on malicious actions from outside actors. Of equal concern (and even more so in the author's view) are threats from an insider—someone we have given legitimate access to information, systems, and resources. The measures we take to detect and protect against external threats may not be sufficient to address threats from insiders.

A malicious insider has access and inside knowledge of the organization and uses that knowledge with the intent to cause harm. The insider may be a current employee, a former employee, a service provider, or, especially in the current era, a planted person who has been radicalized into a terrorist who waits for the right moment to unleash maximum impact to people and property.

Given the importance of our nation's critical infrastructure, the actions taken by a malicious employee or service proceed could have devastating consequences. Let's look at some actual examples.

- A service provider employee at a nuclear facility stole two 5-gallon containers of low-enriched uranium dioxide and then attempted to extort $100,000 by threatening to disperse the material in an unnamed U.S. city.

- A power company field engineer, angry with his supervisor, disabled protection systems at a substation and forced the shutdown of the entire network. More than 800,000 customers lost power as a result.
- Two municipal employees used their access credentials to sabotage the system controlling the traffic lights of a major city, causing widespread traffic delays. The damage took four days to repair.
- A disgruntled supermarket meat packaging employee intentionally contaminated hamburger meat with a pesticide, causing various levels of illness in 92 consumers.

Insider threats endanger the integrity and security of our workplaces and our communities. This section helps you become aware of threat indicators and actions you can take.

Insider Threat Defined

The President's National Infrastructure Advisory Council (2008) defines the insider threat as follows:

> The insider threat to critical infrastructure is one or more individuals with the access or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of the entity's security, systems, services, products, or facilities with the intent to cause harm.

A person who takes advantage of access or inside knowledge in such a manner is commonly referred to as a "malicious insider."

The Scope of Insider Threats

Insider threats can be accomplished through either physical or cyber means and may involve any of the following:

- *Physical or information-technology sabotage*—Involves modification or damage to an organization's facilities, property, assets, inventory, or systems with the purpose of harming or threatening harm to an individual, the organization, or the organization's operations.
- *Theft of intellectual property*—Involves removal or transfer of an organization's intellectual property outside the organization through physical or electronic means (also known as economic espionage).
- *Theft of economic fraud*—Involves acquisition of an organization's financial or other assets through theft or fraud.
- *National security espionage*—Involves obtaining information or assets with a potential impact on national security through clandestine activities.

DID YOU KNOW?

The FBI testified in June 2012 that in the preceding year, economic espionage losses to the American economy totaled more than $13 billion. In the previous four years, the number of arrests the FBI made had doubled; indictments increased by a factor of five; and convictions increased by a factor of eight (FBI 2012). In another survey, security professionals found that 43.2 percent of respondents attributed some loss at their organization to insiders. 46 percent of respondents said the damage caused by insider attacks was more damaging than outside attacks (CSI 2011).

Common Characteristics of Malicious Insiders

Based on research conducted by the Software Engineering Institute at Carnegie Mellon University and the U.S. Secret Service National Threat Assessment Center, malicious insiders often are perceived or known to be difficult or high-maintenance employees who are categorized as follows:

- Obviously unhappy or extremely resentful.
- Having financial, performance, or behavioral problems.
- At risk (or perceived to be) for layoff or termination.

Keep in mind that not all malicious insiders fit this characterization. Insiders involved in national security espionage, for example, may exhibit few outward signs. In the majority of cases, however, management and/or human resources personnel were well aware of the employees and their issues prior to an incident.

Personal Factors Associated With Insiders

The following motives and personal situations frequently are linked with malicious insiders:

- *Personal or Behavioral Problems*
  - Vulnerable to blackmail
  - Experiencing family or financial problems
  - Prone to compulsive or destructive behavior
  - Subject to ego or self-image issues

- *Personal Desires*
  - Seeking adventure or thrill
  - Seeking approval and returned favors
  - Professing allegiance
- *Workplace Issues*
  - Experiencing problems at work
  - Feeling anger or need for revenge

Organizational Factors That Embolden Malicious Insiders

The following organizational factors have been known to encourage or present opportunities to potential malicious insiders.

- *Access and Availability*
  - Ease of access to materials and information
  - Ability to exit the facility or network with materials or information
- *Policies and Procedures*
  - Undefined or inadequate policies and procedures
  - Inadequate training
  - Lack of training
- *Time Pressure and Consequences*
  - Rushed employees
  - Perception of lack of consequences

Insider Activities and Behavior You May See

Insider threats may be detected through particular activities and behavior on the part of the insider. These activities and behaviors often will appear unusual or suspicious. Keep in mind there may be several explanations for a particular activity or behavior identified here, but when combined with other factors, certain activity or behavior point toward a possible insider threat. A combination or confluence of indicators should not be ignored.

Types of Insider Activities and Behavior

Unusual or suspicious insider activities and behavior can be described using the following categories:

- Inappropriate Interest or Acquisition
- Unauthorized or Unusual Computer Use
- Unusual Hours, Contacts, or Travel
- Secretive or Peculiar Behavior
- Personal or Financial Issues

Employer Actions

- Clearly communicating and consistently enforcing security policies and controls.
- Ensuring that proprietary information and materials are adequately, if not robustly, protected.
- Routinely monitoring computer networks for suspicious activity.
- Ensuring security (to include computer network security) personnel have the tools they need.
- Consulting with legal and law enforcement experts as needed to ensure compliance with the law.

Employee Actions

Critical infrastructure organizations today employ a number of security measures to reduce the risk of insider threats. The measures involving employees include, but are not limited to

- using appropriate screening processes to select new employees;
- educating employees about security or other protocols;
- encouraging and providing non-threatening, convenient ways for employees to report suspicious in a confidential manner;
- becoming familiar with behavior and activities associated with malicious insiders;
- documenting and evaluating incidents of suspicious or disruptive behavior; and
- consulting with legal and law enforcement experts as needed to ensure compliance with the law.

THE VULNERABILITY ASSESSMENT (VA)[1]

A *VA* involves an in-depth analysis of the facility's functions, systems, and site characteristics to identify weaknesses and lack of redundancy and to determine mitigations or corrective actions that can be designed and implemented to reduce the vulnerabilities. A vulnerability assessment can be a standalone process or part of a full risk assessment. During this assessment, the analysis of site assets is based on the following: (a) the identified threat;

[1] Much of the information in this section is from U.S. Department of Energy (DOE 2002), *Vulnerability Assessment Methodology: Electric Power Infrastructure*. Washington, DC; U.S. Army Research Laboratory (2000), *Vulnerability Risk Assessment, ARL-TR-1045*. Washington, DC: DOD; U.S. Department of Justice (2002), *A Method To Assess the Vulnerability of U.S. Chemical Facilities*. Washington, DC.

(b) the criticality of the assets; and (c) the level of protection chosen (i.e., based on willingness or unwillingness to accept risk).

The actual complexity of VAs will range based upon the design and operation of the financial services asset. The nature and extent of the VA will differ among systems based on a number of factors, including system size or potential population. Safety evaluations also vary based on knowledge and types of threats, available security technologies, and applicable local, state, and federal regulations. Preferably, a VA is "performance-based," meaning that it evaluates the risk to the financial services assets based on the effectiveness (performance) of existing and planned measures to counteract adversarial actions. According to USEPA (2002), the common elements of vulnerability assessments are as follows:

- Characterization of the financial services sector, including its mission and objectives.
- Identification and prioritization of adverse consequences to avoid.
- Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.
- Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries.
- Evaluation of existing countermeasures.
- Analysis of current risk and development of a prioritized plan for risk reduction.

Financial services sector members should routinely perform VAs to better understand threats and vulnerabilities, determine acceptable levels of risk, and stimulate action to mitigate identified vulnerabilities. These assessments are based upon the extensive knowledge of regulators and guidance issued, and takes into account physical, cyber, and human vulnerabilities, available redundancy, and the sector's reliance on sector-sector assets, systems and processes, and cross-sector reliance on these factors. Consequence assessments include direct economic impacts and national confidence impacts, and are based on expert judgment and exercises. The direct benefits of performing a VA include the following:

- *Build and broaden awareness*—The assessment process directs senior management's attention to security. Security issues, risks, vulnerabilities, mitigation options, and best practices are brought to the surface. Awareness is one of the least expensive and most effective methods for improving the organization's overall security posture.
- *Establish or evaluate against a baseline*—If a baseline has been previously established, an assessment is an opportunity for a checkup to gauge the

improvement or deterioration of an organization's security posture. If no previous baseline has been performed (or the work was not uniform or comprehensive), an assessment is an opportunity to integrate and unify previous efforts, define common metrics, and establish a definitive baseline. The baseline also can be compared against best practices to provide perspective on an organization's security posture.

- *Identify vulnerabilities and develop responses*—Generating lists of vulnerabilities and potential responses is usually a core activity and outcome of an assessment. Sometimes, due to budget, time, complexity, and risk considerations, the response selected for many of the vulnerabilities may be non-action, but after completing the assessment process these decisions will be conscious ones, with a documented decision process and item-by-item rationale available for revisiting issues at scheduled intervals. This information can help drive or motivate the development of a risk management process.
- *Categorize key assets and drive the risk management process*—An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key asset. This ranking, combined with threat, vulnerability, and risk analysis, is at the heart of any risk management process. For many organizations, "Y2K" was the first time a company-wide inventory and ranking of key assets was attempted. An assessment allows any organization to revisit that list form a broader and more comprehensive perspective.
- *Develop and build internal skills and expertise*—A security assessment, when not implemented in an "audit" mode, can serve as an excellent opportunity to build security skills and expertise within an organization. A well-structure assessment can have elements that sever as a forum for cross-cutting groups to come together and share issues, experiences, and expertise. External assessors can be instructed to emphasize "teaching and collaborating" rather than "evaluating" (the traditional role). Whatever the organization's current level of sophistication, a long-term goal should be to move the organization toward a capability for self-assessment.
- *Promote action*—Although disparate security efforts may be underway in an organization, an assessment can crystallize and focus management attention and resources on solving specific and systemic security problems. Often the people "in the trenches" are well aware of security issues (and even potential solutions) but are unable to convert their awareness to action. An assessment provides an outlet for their concerns and the potential to surface these issues at appropriate levels (legal, financial, executive) and achieve action. A well-designed and executed assessment not only identifies vulnerabilities and makes recommendations; it also gains executive buy-in, identifies key players, and establishes a set of cross-cutting groups that can convert those recommendations into action.

- *Kick off an ongoing security effort*—An assessment can be used as a catalyst to involve people throughout the organization in security issues, build cross-cutting teams, establish permanent forums and councils, and harness the momentum generated by the assessment to build an ongoing institutional security effort. The assessment can lead to the creation of either an actual or a virtual (matrixed) security organization.

The Vulnerability Assessment (VA) Process

Table 5.1 provides an overview of the elements included in the assessment methodology. The elements included in this overview are based on actual in-field experience and lessons learned.

In Table 5.1, step 3 deals with identification of asset criticality. This is an important step in any VA. Identifying asset criticality serves several functions:

- It enables more careful consideration of factors that affect risk, including threats, vulnerabilities, and consequences of loss or compromise of the asset.
- It enables more focused and thorough consideration of loss or compromise of the asset.
- It enables leaders to develop robust methods for managing consequences of asset loss (restoration).
- It provides a means to increase awareness of a broad range of employees to protect truly critical assets and to differentiate in policies and procedures the heightened protection they require.

As previously indicated, identifying the criticality of assets is used primarily to focus the vulnerability analysis efforts. It also assists with the ranking of various recommendations for reducing vulnerabilities. As an example, let's take a look at the criticality of electric power assets and operations included in the normal operation of financial services sector assets:

Physical

- Generators
- Substations
- Transformers
- Transmission lines
- Distribution lines
- Control center
- Warehouses
- Office buildings
- Internal and external infrastructure dependencies

Table 5.1 Basic Elements in Vulnerability Assessments

Element	*Points to Consider*
1. Characterization of the communications entity, including its mission and objectives	• What are the important missions of the system to be assessed? Define the highest priority services provided by the sector. Identify the customers: o General public o Government o Military o Industrial o Critical care o Retail operations o Firefighting • What are the most important facilities, processes, and assets of the system for achieving the mission objectives and avoiding undesired consequences? Describe the following: o Industry facilities o Operating procedures o Management practices that are necessary to achieve the mission objectives o How the industry operates o Treatment processes o Storage methods and capacity o Energy use and storage o Distribution system In assessing those assets that are critical, consider critical customers, dependence on other infrastructures (e.g., transportation, communications), contractual obligations, single points of failure, and other aspects of the sector's operations, or availability of utilities that may increase or decrease the criticality of specific facilities, processes, and assets.
2. Identification and prioritization of adverse consequences to avoid	• Take into account the impacts that could substantially disrupt the ability of the system to provide a safe and reliable supply of materials. Financial services sector systems should use the vulnerability assessment process to determine how to reduce risk associated with the consequences of significant concern. • Ranges of consequences or impacts for each of these events should be identified and defined. Factors to be considered in assessing the consequences may include: o Magnitude of service disruption o Economic impact (such as replacement and installation costs for damaged critical assets or loss of revenue due to service outage)

(*Continued*)

Table 5.1 (Continued)

Element	*Points to Consider*
	○ Number of illnesses or deaths resulting from an event ○ Impact on public confidence in the material supply ○ Chronic problems arising from specific events ○ Other indicators of the impact of each event as determined by the financial services sector. Risk reduction recommendations at the conclusion of the VA strive to prevent or reduce each of these consequences.
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences	• What are the malevolent acts that could reasonably cause undesired consequences? ○ Electronic, computer, or other automated systems which are utilized by the financial sector entities (e.g., SCADA) ○ The use, storage, or handling of various financial services supplies ○ The operation and maintenance of such systems
4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries	• Determine the possible modes of attack that might result in consequences of significant concern based on critical assets of the financial services sector entity. The objective of this step of the assessment is to move beyond what is merely possible and determine the likelihood of a particular attack scenario. This is a very difficult task as there is often insufficient information to determine the likelihood of a particular event with any degree of certainty. • The threats (the kind of adversary and the mode of attack) selected for consideration during a VA will dictate, to a great extent, the risk reduction measures that should be designed to counter the threat(s). Some VA methodologies refer to this as a "Design Basis Threat" (DBT) where the threat serves as the basis for the design of countermeasures, as well as the benchmark against which vulnerabilities are assessed. It should be noted that there is no single DBT or threat profile for all financial systems in the United States. Differences in geographic location, size of the utility, previous attacks in the local area, and many other factors will influence the threat(s) that the financial services sector entity should consider in their assessments. Financial services sector entities should consult with the local FBI and/or other law enforcement agencies, public officials, and others to determine the threats upon which their risk reduction measures should be based.

(*Continued*)

Table 5.1 (Continued)

Element	*Points to Consider*
5. Evaluation of existing countermeasures (Depending on countermeasures already in place, some critical assets may already be sufficiently protected. This step will aid in identification of the areas of greatest concern and help to focus priorities for risk reduction.)	• What capabilities does the system currently employ for detection, delay and response? ◦ Identify and evaluate current detection capabilities such as intrusion detection systems, energy quality monitoring, operational alarms, guard post orders, and employee security awareness programs. ◦ Identify current delay mechanisms such as locks and key control, fencing, structure integrity of critical assets, and vehicle access checkpoints. ◦ Identify existing policies and procedures for evaluation and response to intrusion and system malfunction alarms, and cyber system intrusions. **It is important to determine the performance characteristics. Poorly operated and maintained security technologies provide little or no protection.** • What cyber protection system features does the facility have in place? Assess protective measures in place for the SCADA and business-related computer information systems such as these: ◦ Firewalls ◦ Modem access ◦ Internet and other external connections, including wireless data and voice communications. ◦ Security polices and protocols **It is important to identify whether vendors have access rights and/or "backdoors" to conduct system diagnostics remotely.** • What security policies and procedures exist, and what is the compliance record for them? Identify existing policies and procedures concerning: ◦ Personal security ◦ Physical security ◦ Key and access badge control ◦ Control of system configuration and operational data ◦ Vendor deliveries ◦ Security training and exercise records
6. Analysis of current risk and development of a prioritized plan for risk reduction	• Information gathered on threats, critical assets, financial services sector operations, consequences, and existing countermeasures should be analyzed to determine the current level of risk. The utility should then determine whether current risks are acceptable or risk reduction measures should be pursued. • Recommended actions should measurably reduce risks by reducing vulnerabilities and/or consequences through improved deterrence, delay, detection, and/or response capabilities or by improving operational policies or procedures.

(*Continued*)

Table 5.1 (Continued)

Element	*Points to Consider*
	• Selection of specific risk reduction actions should be completed prior to considering the cost of the recommended action(s). Facilities should carefully consider both short- and long-term solutions. An analysis of the cost of short- and long-term risk reduction actions may impact which actions the utility chooses to achieve its security goals. • Facilities may also want to consider security improvements. Security and general infrastructure may provide significant multiple benefits. For example, improved treatment processes or system redundancies can both reduce vulnerabilities and enhance day-to-day operation. • Generally, strategies for reducing vulnerabilities fall into three broad categories: ◦ Sound business practices—affect policies, procedures, and training to improve the overall security-related. ◦ System upgrades—including changes in operations, equipment, processes, or infrastructure itself that make the system fundamentally safer. ◦ Security upgrades—improved capabilities for detection, delay, or response.

Adapted from Spellan (2009), *The Handbook of Safety Enginerring.*

Cyber

- Supervisory Control and Data Acquisition (SCADA) systems
- Networks
- Databases
- Business systems
- Telecommunications

Interdependencies

- Single-point nodes of failures
- Critical infrastructure components of high reliance

VULNERABILITY ASSESSMENT (VA) METHODOLOGY

VA methodology consists of 10 elements. Each element along with a description of each is listed below (US DOE 2002).

1. Network architecture
2. Threat environment

3. Penetration testing
4. Physical security
5. Physical asset analysis
6. Operations security
7. Policies and procedures
8. Impact analysis
9. Infrastructure interdependencies
10. Risk characterization

Network Architecture

This element provides an analysis of the information assurance features of the information network(s) associated with the organization's critical information systems. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network.

Procedures for information assurance in the system, including authentication of access and management of access authorization, should be reviewed. The assessment should identify any obvious concerns related to architectural vulnerabilities, as well as operating procedures. Existing security plans should be evaluated, and the results of any prior testing should be analyzed. Results from the network architecture assessment should include potential recommendations for changes in the information architecture, functional areas, and categories where testing is needed, and suggestions regarding system design that would enable more effective information and information system protection.

Three techniques are often used in conduction the network architecture assessment:

1. Analysis of network and system documentation during and after the site visit
2. Interview with facility staff, managers, and chief information officer
3. Tours and physical inspections of key facilities

Threat Environment

Development of a clear understanding of the threat environment is a fundamental element of risk management. When combined with an appreciation of the value of the information assets and systems, and the impact of

unauthorized access and subsequent malicious activity, an understanding of threats provides a basis for better defining the level of investment needed to prevent such access.

The threat of a terrorist attack to financial services sector infrastructure is real and could come from several areas, including physical, cyber, and interdependency. In addition, threats could come from individuals or organizations motivated by financial gain or persons who derive pleasure from such penetration (e.g., recreational hackers, disgruntled employees). Other possible sources of threats are those who want to accomplish extremist goals (e.g., environmental terrorists, antinuclear advocates) or embarrass one or more organizations.

This element should include a characterization of these and other threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterization of the threat environment should be localized, that is, within the organization's service area.

Penetration Testing

The purpose of network penetration testing is to utilize active scanning and penetration tools to identity vulnerabilities that a determined adversary could easily exploit. Penetration testing can be customized to meet the specific needs and concerns of the financial services sector unit. In general, penetration testing should include a test plan and details on the rules of engagement (ROE). It should also include a general characterization of the access points of the critical information systems and include a general characterization of the access points to the critical information systems and communication interface connections, modem network connections, access points to principal network routers, and other external connections. Finally, penetration testing should include identified vulnerabilities and, in particular, whether access could be gained to the control network or specific subsystem or devices that have a critical role in assuring continuity of service.

Penetration testing consists of an overall process of establishing the ground rules or ROE for the test; establishing a white cell for continuous communication; developing a format or methodology for the test; conducting the test; and generating a final report that details methods, findings, and recommendations.

Penetration testing methodology consists of three phases: reconnaissance, scenario development, and exploitation. A one-time penetration test can provide the utility with valuable feedback; however, it is far more effective if performed on a regular basis. Repeated testing is recommended because new threats develop continuously, and the networks, computers, and architecture of the financial services sector unit or utility are likely to change over time.

Physical Security

A critical dependency for the financial services sector as well as the other sectors is related to the physical security of the facilities. The purpose of physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated. Physical security systems include access controls, barriers, locks and keys, badges and passes, intrusion detection devices and associated alarm reporting and display, closed-circuit television (assessment and surveillance), communications equipment (telephone, two-way radio, intercom, cellular), lighting (interior and exterior), power sources (line, battery, generator), inventory control, postings (signs), security system wiring, and protective force. Physical security systems are reviewed for design, installation operation, maintenance, and testing.

The physical security assessment should focus on those sites directly related to the critical facilities, including information systems and assets required for operation. Typically included are facilities that house critical equipment or information assets or networks dedicated to the operation of electric, oil, or gas transmission, storage, or delivery systems. Other facilities can be included on the basis of criteria specified by the organization being assessed. Appropriate levels of physical security are contingent upon the value of company assets, the potential threats to these assets, and the cost associated with protecting the assets. Once the cost of implementing/maintaining physical security programs is known, it can be compared to the value of the company assets, thus providing the necessary information for risk management decisions. The focus of the physical security assessment task is determined by prioritizing the company assets; that is, the most critical assets receive the majority of the assessment activity.

At the start of the assessment, survey personnel should develop a prioritized listing of company assets. This list should be discussed with company personnel to identify areas of security strengths and weaknesses. During these initial interviews, assessment area that would provide the most benefit to the company should be identified; once known, they should become the major focus of the assessment activities.

The physical security assessment of each focus area usually consists of the following:

- Physical security program (general)
- Physical security program (planning)
- Barriers
- Access controls/badges
- Locks/keys

- Intrusion detection systems
- Communications equipment
- Protective force/local law enforcement agency

The key to reviewing the above topics is not to just identify if they exist but to determine the appropriate level that is necessary and consistent with the value of the asset being protected. The physical security assessment worksheets provide guidance on appropriate levels of protection.

Once the focus and content of the assessment task have been identified, the approach to conduction the assessment can be either at the "implementation level" or at the "organizational level." The approach taken depends on the maturity of the security program.

For example, a company with a solid security infrastructure (staffing plans/procedures, funding) should receive a cursory review of these items; however, facilities where the security programs are being implemented should receive a detailed review. The security staff can act upon deficiencies found at the facilities, once reported.

For companies with an insufficient security organization, the majority of time spent on the assessment should take place at the organizational level to identify the appropriate staffing/funding necessary to implement security programs to protect company assets. Research into specific facility deficiencies should be limited to finding just enough examples to support any staffing/funding recommendations.

Physical Asset Analysis

The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist. Included in this element is an examination of asset utilization, system redundancies, and emergency operating procedures. Consideration should also be given to the topology and operating practices for electric and gas transmission, processing, storage, and delivery, looking specifically for those elements that either singly or in concert with other factors provide a high potential for disrupting service. This portion of the assessment determines company and industry trends regarding these physical assets. Historic trends, such as asset utilization, maintenance, new infrastructure investments, spare parts, SCADA linkages, and field personnel are part of the scoping element.

The proposed methodology for physical assets is based on a macro-level approach. The analysis can be performed with company data, public data, or both. Some companies might not have readily available data or might be reluctant to share that data.

Key output from analysis should be graphs that show trends. The historic data analysis should be supplemented with on-site interviews and visits. Items to focus on during a site visit include the following:

- Trends in field testing
- Trends in maintenance expenditures
- Trends in infrastructure investments
- Historic infrastructure outages
- Critical system components and potential system bottlenecks
- Overall system operation controls
- Use and dependency of SCADA systems
- Linkages of operation staff with physical and IT security
- Adequate policies and procedures
- Communications with other regional financial assets
- Communications with external infrastructure providers
- Adequate organizational structure

Operations Security

Operations security (OPSEC) is the systematic process of denying potential adversaries (including competitors or their agents) information about capabilities and intentions of the host organization. OPSEC involves identifying, controlling, and protecting generally nonsensitive activities concerning planning and execution of sensitive activities. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and nonsensitive information that might inappropriately aid or abet an individual's or organization's disproportionate influence over system operation. This assessment should include a review of security training and awareness programs, discussions with key staff, and tours of appropriate principal facilities. Information that might be available through public access should also be reviewed.

Policies and Procedures

The policies and procedures by which security is administered (1) provide the basis for identifying and resolving issues; (2) establish the standards of reference for policy implementation; and (3) define and communicate roles, responsibilities, authorities, and accountabilities for all individuals and organizations interface with critical systems. They are the backbone for decisions and day-to-day security operations. Security policies and procedures become particularly important at times when multiple parties must interact to effect a desired level of security and when substantial legal ramifications cold result from policy violations. Policies and procedures should be reviewed to determine

whether they (1) address the key factors affecting security; (2) enable effective compliance, implementation, and enforcement; (3) reference or conform to established standards; (4) provide clear and comprehensive guidance; and (5) effectively address the roles, responsibilities, accountabilities, and authorities.

The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of policies and procedures. Understanding and assessing this area provide a means of identifying strengths and areas for improvements that can be achieved through the following:

- Modification of current policies and procedures
- Implementation of current policies and procedures
- Development and implementation of new policies and procedures
- Assurance of compliance with policies and procedures
- Cancellation of policies and procedures that are no longer relevant, or are inappropriate, for the facility's current strategy and operations

Impact Analysis

A detailed analysis should be conducted to determine the influence that exploitation of unauthorized access to critical facilities or information systems might have on an organization's operations (e.g., market and/or physical operations). In general, such an analysis would require thorough understanding of (1) the applications and their information processing, (2) decisions influenced by this information, (3) independent checks and balances that might exist regarding information upon which decisions are made, (4) factors that might mitigate the impact of unauthorized access, and (5) secondary impacts of such access. Similarly, the physical chain of events following disruption, including the primary, secondary, and tertiary impacts of disruption, should be examined.

The purpose of the impact analysis is to help estimate the impact that detrimental impacts could have on financial services sector units. The impact analysis provides an introduction to risk characterization by providing quantitative estimates of these impacts so that the financial services sector unit can implement a risk management program and weigh the risks and costs of various mitigation measures.

Infrastructure Interdependencies

The term "infrastructure interdependencies" refers to the physical and electronic (cyber) linkages within communications and among our nation's critical infrastructures—energy (electric power, oil, natural gas), telecommunications, transportation, water supply systems, banking and finance,

emergency services, and government services. This task identifies the direct infrastructure linkages between and among the infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of an organization's functions, internal infrastructures, and how these link to external infrastructures.

The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.

Risk Characterization

Risk characterization provides a framework for prioritizing recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritize the recommendations and assist the organization in determining the appropriate course of action. It provides a framework for assessing vulnerabilities, threats, and potential impacts (determined in the other tasks). In addition, the existing risk analysis and management process at the organization should be reviewed and, if appropriate, utilized for prioritizing recommendations. The degree to which corporate risk management includes security factors is also evaluated.

VULNERABILITY ASSESSMENT (VA) PROCEDURES

VA procedures can be conducted for financial services sector assets using various methodologies. For example, the checklist analysis is an effective technology. In addition, Pareto analysis (80/20 principle), relative ranking, preremoval risk assessment (PRRA), change analysis, failure mode and effects analysis (FMEA), fault tree analysis, event tree analysis, what-if analysis and hazard and operability (HAZOP) can be used in conducting the assessment.

Based on personal experience, the what-if analysis and HAZOP seem to be the most user-friendly methodologies to use. A sample what-if analysis procedural outline is presented below, followed by a brief explanation and outline for conducting HAZOP.

What-If Analysis Procedure/Sample What-If Questions

The steps in a What-If Checklist analysis are as follows:

1. Select the team (personnel experienced in the process)
2. Assemble information (piping and instrumentation drawings [P&IDs], process flow diagrams [PFDs], operating procedures, equipment drawings, etc.)
3. Develop a list of what-if questions

4. Assemble your team in a room where each team member can view the information
5. Ask each what-if question in turn and determine:
   - What can cause the deviation from design intent that is expressed by the question?
   - What adverse consequences might follow?
   - What are the existing design and procedural safeguards?
   - Are these safeguards adequate?
   - If these safeguards are not adequate, what additional safeguards does the team recommend?
6. As the discussion proceeds, record the answers to these questions in tabular format.
7. Do not restrict yourself to the list of questions that you developed before the project started. The team is free to ask additional questions at any time.
8. When you have finished the what-if questions, proceed to examine the checklist. The purpose of this checklist is to ensure that the team has not forgotten anything. While you are reviewing the checklist, other what-if questions may occur to you.
9. Make sure that you follow up all recommendations and action items that arise from the hazards evaluation.

HAZOP Analysis

The HAZOP analysis technique uses a systematic process to (1) identify possible deviations from normal operations and (2) ensure that safeguards are in place to help prevent accidents. The HAZOP uses special adjectives (such as speed, flow, pressure, etc.) combined process conditions (such as "more," "less," "no," etc.) to systematically consider all credible deviations from normal conditions. The adjectives, called guide words, are a unique feature of HAZOP analysis (see table 5.2).

In this approach, each guide word is combined with relevant process parameters and applied at each point (study node, process section, or operating step) in the process that is being examined (see table 5.3).

Table 5.2 HAZOP Analysis Guide Words

Guide Words	*Meaning*
No	Negation of the Design Intent
Less	Quantitative Decrease
More	Quantitative Increase
Part Of	Other Material Present by Intent
As Well As	Other Materials Present Unintentionally
Reverse	Logical Opposite of the Intent
Other Than	Complete Substitution

Table 5.3 Common HAZOP Analysis Process Parameters

Flow	Time	Frequency	Mixing
Pressure	Composition	Viscosity	Addition
Temperature	pH	Voltage	Separation
Level	Speed	Information	Reaction

The following is an example of creating deviations using guide words and process parameters:

Guide Words		*Parameter*		*Deviation*
NO	+	FLOW	=	NO FLOW
MORE	+	PRESSURE	=	HIGH PRESSURE
AS WELL AS	+	ONE PHASE	=	TWO PHASE
OTHER THAN	+	OPERATION	=	MAINTENANCE
MORE	+	LEVEL	=	HIGH LEVEL

Guide words are applied to both the more general parameters (e.g., react, mix) and the more specific parameters (e.g., pressure, temperature). With the general parameters, it is not unusual to have more than one deviation from the application of one guide word. For example, "more reaction" could mean either that a reaction takes place at a faster rate, or that a greater quantity of product results. On the other hand, some combination of guide words and parameters will yield no sensible deviation (e.g., "as well as" with "pressure").

HAZOP Procedure

1. Select the team
2. Assemble information (P&IDs, PFDs, operating procedures, equipment drawings, etc.).
3. Assemble your team in a room where each team member can view P&IDs.
4. Divide the system you are reviewing into nodes (you can present the nodes, or the team can choose them as you go along).
5. Apply appropriate deviations to each node. For each deviation, address the following questions:
   - What can cause the deviation from design intent?
   - What adverse consequences might follow?
   - What are the existing design and procedural safeguards?
   - Are these safeguards adequate?
   - If these safeguards are not adequate, what does the team recommend?
6. As the discussion proceeds, record the answers to these questions in tabular format.

VULNERABILITY ASSESSMENT (VA): CHECKLIST PROCEDURE

In performing the vulnerability assessment of any financial services sector unit or facility, one of the simplest methodologies to employ is the checklist. The Building Vulnerability Assessment Checklist developed by the Department of Veterans Affairs and is part of FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings* is the reference manual that is recommended in this book and is available on online at https://www.fema.gov/media-library/assets/documents/2150. It is an excellent guide for conducting a viable Checklist-Type Vulnerability Assessment. This Checklist will help you to prepare your Threat Assessment because it allows a consistent security evaluation of designs at various levels. The Checklist can be used as screening tool for preliminary design vulnerability assessment and supports the preparation of all steps for use by the assessment teams during preparation for interviews with facility representatives to help assure that all relevant aspects of the financial services assets are considered in the survey.

The bottom line: through the VAs, the financial services sector has determined that some of its greatest challenges are its dependence on the telecommunications network and the power grid.

REFERENCES AND RECOMMENDED READING

CBO. 2004. *Homeland Security and the Private Sector*. Accessed May 2, 2018, 168 @ www.cbo.gov/ft. docs.

CSI. 2011. *2010/2011 Computer Crime and Security Survey*. Orlando, FL: Computer Security Institute.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

DHS. 2016. *What is Security and Resilience?* Accessed @ https://www.dhs.gov/what-security and-resilience.

DoDD. 2010. *DoD Policy and Responsibility for Critical Infractions –DODD 3020.40*. Washington, DC: U.S. Department of Defense.

FBI. 2012. *Insider Espionage. Report before the House Committee on Homeland Security Subcommittee on Counter Terrorism and Intelligence*. Washington, DC: Federal Bureau of Investigation.

FEMA. 2008. *FEMA 452: Risk Assessment A How to Guide*. Accessed May 1, 2016 @ fema.gov/library/file?type=published/filetofile.

FEMA. 2015. *Protecting Critical Infrastructure against Insider Threats.* Accessed April 17, 2015 @ http://emilms.fema.gov/IS0915/IABsummary.htm.

INSA. 2017. *Building a Stronger Intelligence Community*. Arlington, VA: Intelligence and National Security Alliance. Accessed @ www.insooline.org.

National Infrastructure Advisory Council. 2008. *First Report and Recommendations on the Insider Threat to Critical Infrastructure.* Washington, DC.

Spellman, F. R. 1997. *A Guide to Compliance for PSM/RMP*. Lancaster, PA: Technomic Publishing Company.

U.S. Department of Energy. 2010. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* Washington, DC: USDOE.

US DOE. 2002. *Vulnerability Assessment Methodology: Electric Power Infrastructure*. Washington, DC.

U.S. Department of the Treasury. 2016. *Banking and Finance Sector-Specific Plan.* Washington, DC.

US EPA. 2002. *Vulnerability Assessment Fact Sheet*. EPA 816-F-02-025. Accessed May 2006 @ www.epa.gov/ogwdw/security/index.html.

Chapter 6

Preparation

When is Enough, Enough?

Question: When preparing to respond to terrorist acts against people, malls, schools, sports stadiums, libraries, communications systems, government facilities and financial services assets when is enough, enough?

Answer: Until we can read the terrorists' minds, enough preparation is never enough. Simply, preparation is ongoing and never-ending.

—Frank R. Spellman

We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge.

—George W. Bush

Americans should find comfort in knowing that millions of their fellow citizens are working every day to ensure our security at every level—federal, state, county, municipal. These are dedicated professionals who are good at what they do. I've seen it up close, as Governor of Pennsylvania. . . . But there may be gaps in the system. The job of the Office of Homeland Security will be to identify those gaps and work to close them.

Now, obviously, the further removed we get from September 11, I think the natural tendency is to let down our guard. Unfortunately, we cannot do that. The government will continue to do everything we can to find and stop those who seek to harm us. And I believe we owe it to the American people to remind them that they must be vigilant, as well.

—Tom Ridge (quoted in Henry 2002)

The possibility of terrorism—attacks on U.S. financial services sector infrastructure—doesn't generate the same attention as potential nuclear, biological, or chemical terrorism. Yet, because of the seriousness of the threat of terrorism to the financial services sector and the enormous economic and security implications of such attacks, the US FCC, USDOE, USEPA, USDHS, and other agencies have worked nonstop since 9/11 in gathering and providing as much advice and guidance as possible to aid financial securities sector personnel in protecting sector assets and associated critical support infrastructure. In this chapter, we provide an overview of important tools that can be used in protecting the financial services sector to guard against the threat of terrorism. In the discussion, keep in mind that even though a financial services sector issued the guidance provided it could be used to protect the other critical infrastructure sectors.

THREATS AND INCIDENTS

Based on evidence of potential losses from past accidents, indication of the potential human and environmental losses and economic costs from an attack on a financial services sector facility or producer comes from major incidents that have occurred both abroad and in the United States. Those events indicate that the human and environmental losses could be significant (CBO 2004).

Financial services sector threats and incidents may be of particular concern due to the range of potential consequences:

- Disrupting system operations and interrupting the supply of critical financial components.
- Causing physical damage to financial system infrastructure.
- Reducing public confidence in the financial services system.
- Long-term denial of basic security and protection and the cost of replacement.

Keep in mind that some of these consequences would only be realized in the event of a successful terrorist incident; however, the mere *threat* of terrorism can also have an adverse impact on industries that depend on a safe, steady supply of financial services. In addition, the economic implications of such attacks are potentially enormous. For example, many believe that one actual reason that we are looking at high oil prices is because there is a "terror premium" factored into the price of a barrel.

While it is important to consider the range of possibilities associated with a particular threat, assessments are typically based on the probability of a particular occurrence. Determining probability is somewhat subjective, and is often based on intelligence and previous incidents. As mentioned, there are

historical accounts of accidental incidents that have caused tremendous death and destruction.

Threat Warning Signs[1]

A threat warning is an occurrence or discovery that indicates a potential threat that triggers an evaluation of the threat. It is important to note that these warnings must be evaluated in the context of typical industry activity and previous experience in order to avoid false alarms. Following is a brief description of potential warnings.

- *Security Breach*: Physical security breaches, such as unsecured doors, open hatches, and unlocked/forced gates, are probably the most common threat warnings. In most cases, the security breach is likely related to lax operations or typical criminal activity such as trespassing, vandalism, and theft. However, it may be prudent to assess any security breach with respect to the possibility of attack.
- *Witness Account*: Awareness of an incident may be triggered by a witness account of tampering. Financial services sector sites/facilities should be aware that individuals observing suspicious behavior near financial services sector facilities/offices will likely call 911 and not the facility. In this case, the incident warning technically might come from law enforcement, as described below. Note: the witness may be a sector employee engaged in their normal duties.
- *Direct Notification by Perpetrator*: A threat may be made directly to the financial services sector site, office, or facility, either verbally or in writing. Historical incidents would indicate that verbal threats made over the phone are more likely than written threats. While the notification may be a hoax, threatening a financial services sector unit is a crime and should be taken seriously.
- *Notification by Law Enforcement*: A financial services sector site/facility may receive notification about a threat directly from law enforcement, including local, country, state, or federal agencies. As discussed previously, such a threat could be a result of suspicious activity reported to law enforcement, either by a perpetrator, a witness, or the news media. Other information, gathered through intelligence or informants, could also lead law enforcement to conclude that there may be a threat to the financial services sector site/facility. While law enforcement will have to be lead in the criminal investigation, the financial services sector site/facility has primary

[1] The following is adapted from USEPA (2003), *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents* (Washington DC: United States Environmental Protection Agency).

responsibility for the safety of its equipment and processes. Thus, the unit's role will likely be to help law enforcement to appreciate the public health implications of a particular threat as well as the technical feasibility of carrying out a particular threat.

- *Notification by News Media*: A threat to destroy a financial services site/facility might be delivered to the news media, or the media may discover a threat. A conscientious reporter would immediately report such a threat to the police, and either the reporter or the police would immediately contact the financial services sector site/facility. This level of professionalism would provide an opportunity for the site to work with the media and law enforcement to assess the credibility of the threat before any broader notification is made.

RESPONSE TO THREATS

Note: This section is *not* designed to discuss what specific steps to take in responding to a terrorist threat. Rather, the questions addressed in this section are "Why is it necessary to plan to respond to financial services sector threats at all?" and "When have I done enough?"

Federal, state, and local programs already exist that—with varying degrees of effectiveness—encourage or require the operators of financial services sector sites/facilities to boost their efforts to promote safety and security and to share information that can help local governments plan for emergencies.

Proper planning is a delicate process because public health measures are rarely noticed or appreciated (like buried utility pipes, they are often hidden functions except when they fail)—then they are very visible. The result of too little action, including no response at all, can have disastrous consequences potentially resulting in public injuries or fatalities. One overriding question is "When has a financial services producer done enough?" This question may be particularly difficult to address when considering the wide range of agencies that may be involved in a threat situation. Other organizations, such as US FCC, USEPA, USDHA, USDOE, CDC, USDOT, law enforcement agencies, public health departments, and so on, will have unique obligations or interests in responding to a severe release or explosion threat.

When is Enough, Enough?

The guiding principle for responding to severe release or explosion threats is one of "due diligence" or "what is a suitable and sensible response to a threat?" As discussed above, some response to financial services sector failures is warranted due to the public health implications of an actual dangerous incident.

Ultimately, the answer to the question of "due diligence" must be decided at the local level and will depend on a number of considerations. Among other factors, local authorities must decide what level of risk is reasonable in the context of a perceived threat. Careful planning is essential to developing an appropriate response to terrorist threats, and in fact, one primary objective of the USEPA's *Response Protocol Toolboxes* (RPTBs) is to aid users in the development of their own site-specific plans that are consistent with the needs and responsibilities of the user. Beyond planning, the RPTB considers a careful evaluation of any terrorist threat, and an appropriate response based on the evaluation, to be the most important element of due diligence.

In the RPTB, the threat management process is considered in three successive stages: *possible*, *credible*, and *confirmed*. Thus, as the threat escalates through these three states, the actions that might be considered due diligence expand accordingly. The following paragraphs describe, in general terms, actions that might be considered as due diligence at these various stages.

- Stage 1: "Is the threat possible?" If a financial services facility is faced with a terrorism threat, they should evaluate the available information to determine whether or not the threat is "possible" (i.e., could something have actually happened). If the threat is possible, immediate operational response actions might be implemented, and activities such as site characterization would be initiated to collect additional information to support the next stage of the threat evaluation.
- Stage 2: "Is the threat credible?" Once a threat is considered "possible," additional information will be necessary to determine if the threat is "credible." The threshold at the credible stage is higher than that at the possible stage, and in general there must be information to corroborate the threat in order for it to be considered credible.
- Stage 3: "Has the incident been confirmed?" Confirmation implies that definitive evidence and information have been collected to establish the presence of a threat to the financial services sector. Obviously, at this stage the concept of due diligence takes on a whole new meaning since authorities are now faced with death and destruction and a potential public health crisis. Response actions at this point include all steps necessary to protect public health, property, and the environment.

PREPARATION

As an environmental/occupational safety, security, and health professional consultant for various utilities and others on the East Coast, I have performed numerous security, pre-OSHA audit inspections and audits of various plant

or facility PSM/RMP compliance programs. During these site visits, one factor always seemed to be universal. While conducting the plant/facility walk-around to gauge the organization's overall profile and status with FCC, OSHA, and USEPA compliance, I almost always find that the plant/facility manager or superintendent who accompanied us was shocked to find out what was actually going on or taking place in their facilities. They would scratch their heads and ask various workers: "What the hell are you doing? Where did that new computer come from? When was it installed? And also, why is that door broken? Who told you to paint that machine? When did that hole get in the fence? Who left the back gate open? Who left the safe open? Where is the assistant manager" and so on. Eventually, in an expression of utter consternation, the manager/superintendent asks, "Who the hell is in charge around here?" And this is basically the question I find myself asking—far too often.

In one inspection performed at a plant/facility right after 9/11, I drove up to the entrance gate and was impressed with the height and condition of the barbed-razor-wire-topped fence and gates. I could not enter through the gates until I identified myself over a speaker system while a CCTV camera focused on my face. I was let in and given instructions to sign in at the main office. Not bad, just the way it should be…or so I thought at the time. After walking most of the plant site in the company of the plant manager, we approached the back fence area, which was close to a huge chlorine storage building. At the terminal end of the plant and fence, I noticed a large gate that was propped open with ivy growing on it, through it, and around it—obviously, the gate had been in the open position for quite some time. I asked the plant manager why the gate was open. He stated that it was always open…that it led to a downhill path to a beach area below where plant personnel had constructed a picnic area, fronting the James River.

We walked the path to the bottom picnic area, looked around, and then looked back up the path toward the open gate and the prominent structure standing within, the chlorine storage building. While walking back up the path to the gate, I asked the plant manager if he was not concerned about the security and safety of the plant, because the gate was left open, and especially about the safety of the 50 tons of deadly chlorine gas stored in the chlorine storage building.

"Nah . . . no way . . . we are safe here. I really don't see anyone swimming up river just to get into the plant site, ha. Besides, we are surrounded by woods out here . . . there's nothing to attack anyway."

Once inside the plant, I asked the plant manager if he was not worried about terrorists or some disgruntled former employee using a boat filled with explosives or some other weapon(s) gaining easy access to the plant and especially the chlorine building via the James River beach landing and picnic area?

"Nah, that will never happen . . . who would be that stupid? There's nothing around here worth blowin' up!"

Later, when I checked the GIS/GPS system data and maps pertaining to and showing the plant and surrounding area, I noted that about one-half mile from the plant site was a large housing area, a brewery (with 700+ employees), and a very large theme and historical park—annually visited by more than 2,500,000 people each summer.

Know Your Financial Services Sector Systems

All financial services sector facility managers and financial services equipment operating personnel must know their facilities. For these persons, there is no excuse for not knowing every square inch of the facility site. In particular, plant workers should know about any and all construction activities underway on the site; the actual construction parameters of the facility; and especially operation of all transactional unit processes. In addition, management must not only know their operating staff but also their customers.

Construction and Operation

Each financial services sector facility is unique with respect to age, operation, and complexity. This is important, particularly in evaluating the potential of a financial services failure or malicious action causing financial services failure.

Personnel

Financial services sector employees are generally its most valuable asset in preparing for and responding to threats and incidents. They have knowledge of the system and potential problem areas. The importance of knowledgeable and experienced personnel is highlighted by the complexity of most financial services systems. This complexity makes a specific terrorist target contingent upon detailed knowledge of the system configuration and usage patterns. If perpetrators have somehow gained a sophisticated understanding of a financial services communications network system, the day-to-day experience of network production will prove an invaluable tool to countering any attacks. For instance, personnel may continually look for unusual aspects of daily operation that might be interpreted as a potential threat warning, and may also be aware of specific characteristics of the system that make it vulnerable to malware attacks or worse.

Customers

A customer's knowledge of financial services availability, functionality, and delivery is an important component of preventing and managing system intrusion incidents. Prevention is based largely on understanding potential types of malware attacks and the type of target facility. Steps taken to protect

the customer's financial services tie-ins and in addition its employees and property, such as enhancements to the physical security of the sender's and receiver's financial services system may deter the attack itself.

Financial services customers vary significantly with regard to their expectations of what constitutes acceptable service, so it is necessary to consider the manner in which financial services sector services are used in a particular system. Planning, preparation, and allocation of financial services resources should be directed toward protecting the public at large, beyond specific demographic groups or individual users.

Perform Training and Desk/Field Exercises

In addition to a lack of planning, another reason that emergency response plans fail is lack of training and practice. Training provides the necessary means for everyone involved to acquire the skills to fulfill their role during an emergency. It may also provide important "buy-in" to the response process from both management and staff, which is essential to the success of any response plan. Desk exercise (also known as "tabletops" or "sand lot" or "dry runs") along with field exercises allow participants to practice their skills. Also, these exercises will provide a test of the financial services security plan itself, revealing strengths and weakness that may be used to improve the overall plan.

Enhance Physical Security

Where possible deny physical access to key sites; within the financial services sector system this may act as a deterrent to a perpetrator. When we consider that many of the financial services sector units such as power generating and tower transmission systems are often in remote, wide-open spaces, this can be a huge challenge. Terrorists often seek the easiest route of attack, just like a burglar prefers a house with an open window or an unlocked car with keys in the ignition. Aside from deterring actual attacks, enhancing physical security has other benefits. For example, installation of fences and locks may reduce the rate of false alarms. Without surveillance equipment or locks, it may not be possible to determine whether a suspicious individual has actually entered a vulnerable area. The presence of a lock and a determination as to whether it has been cut or broken provides sound, although not definitive, evidence that an intrusion has occurred. Likewise, security cameras can be used to review security breaches and determine if the incident was simply due to trespassing or is a potential contamination threat. The costs of enhancing physical security may be justified by comparison to the cost of responding to just one "credible" munitions explosion or contamination threat involving site characterization and lab analysis for potential contaminants.

THE BOTTOM LINE

This chapter has emphasized the importance of ensuring the physical security of financial services sector facilities and equipment. But it is important to point out that true financial services sector security goes beyond the physical plant; the sector requires security of a different kind. Much of the financial services infrastructure, including control architecture, is vulnerable to cyberattack from either inside or outside of the network. The fact is that perhaps the largest vulnerability and dependency of the national financial services infrastructure as well as the infrastructure for other sectors is on cybersecurity. The control of financial services networks and all of its functional components are vulnerable to various degrees of cyberattacks on the software operating systems by either the idle hacker of the more malicious intruder participating in information warfare. This is also true of all the networks within others sectors. The bottom line, the networks must be protected and guarded from attack.

REFERENCES AND RECOMMENDED READING

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

Henry, K. 2002. New Face of Security. *Government Security*, pp. 30–37.

U.S. Department of Energy. 2010. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* Washington, DC: USDOE.

USEPA. 2001. *Protecting the Nation's Water Supplies from Terrorist Attack: Frequently Asked Questions*. Washington, DC: United States Environmental Protection Agency.

USEPA. 2004. *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents*. Washington, DC: United States Environmental Protection Agency.

USEPA. 2011. *Response Protocol Toolbox: Planning for and Responding to Wastewater Contamination Threats and Incidents*. Washington, DC: United States Environmental Protection Agency.

Chapter 7

Cybersecurity

> Unless people are injured, there is also less drama and emotional appeal.
>
> —Dorothy Denning, Fellow of the Association for Computing Machinery, "Is Cyber Terror Next?"

> In Queensland, Australia, on April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment along Australia's Sunshine Coast.
>
> Boden's arrest solved a mystery that had troubled the Maroochy Shire wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and the manicured grounds of a Hyatt Regency hotel. . . . Until Boden's capture—during his 46th successful intrusion—the utility's managers did not know why.
>
> —Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*

It's gotten commonplace to see reports of cyber "exploits" and infiltration of major companies in the news. Consider these:

- In May 2015, media sources reported that data belonging to 1.1 million health insurance customers in the Washington, DC area were stolen in a cyberattack on a private insurance company. Attackers accessed a database containing customer names, birth dates, e-mail addresses, and subscriber ID numbers.

- In December 2014, the Industrial Control Systems Cyber Emergency Response Team (or ICS-CERT), which works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies, issued an updated alert on a sophisticated malware camping compromising numerous industrial control system environments. Their analysis indicated that this campaign had been ongoing since at least 2011.
- In the January 2014 to April 2014 release of its Monitor report, ICS-CERT reported that a public utility had been compromised when a sophisticated threat actor gained unauthorized access to its control system network through a vulnerable remote access capability configured on the system. The incident highlighted the need to evaluate security controls employed at the perimeter and ensure that potential intrusion vectors are configured with appropriate security controls, monitoring, and detection capabilities.
- In December 2016, a Wisconsin couple was charged after allegedly defrauding a local credit union out of more than $300,000. One of the defendants, who managed the bank's accounts, had her coconspirator cash checks worth $980 several times each week beginning in May 2015. The charges allege that the couple used the money to buy drugs.

In 2000, the FBI identified and listed threats to critical infrastructure. These threats are listed and described in table 7.1. In 2015, the GAO described the sources of cyber-based threats. These threats are listed and described in detail in table 7.2.

DID YOU KNOW?

Presidential Policy Directive 21 (PPD-21) defined "All hazards" as a threat to an incident natural or manmade that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities.

Threats to systems supporting critical infrastructure are evolving and growing. As shown in table 7.2, cyber threats can be unintentional or intentional. Unintentional or non-adversarial threats include equipment failures, software coding errors, and the actions of poorly trained employees. They also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of its control. Intentional threats include both

Table 7.1 Threats to Critical Infrastructure Observed by the FBI

Threat	*Description*
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into websites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence, can affect the daily lives of Americans across the country.
Inside threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: FBI (2000, 2014).

targeted and untargeted attacks form a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nation engaged in espionage and information warfare, and terrorists. These threat adversaries vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include seeking monetary gain or seeking an economic, political, or military advantage (GAO 2015).

Table 7.2 Common Cyber Threat Sources

Source	*Description*
Non-adversarial-malicious	
Failure in information technology equipment	Failures in displays, sensors, controllers, and information Information technology hardware responsible for data storage, processing, and communications
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies
Software coding errors	Failures in operating systems, networking, and general-purpose and mission-specific applications
Natural or man-made disaster	Events beyond an entity's control such as fires, floods/tsunamis, tornadoes, hurricanes, and earthquakes
Unusual or natural event	Natural events beyond the entity's control that are not considered to be disasters (e.g., sunspots)
Infrastructure failure or outage	Failure or outage of telecommunications or electrical power
Unintentional user errors	Failures resulting from erroneous, accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities
Adversarial	
Hackers or hacktivists	Hackers break networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hactivists are ideologically motivated actors who use cyber exploits to further political goals
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) may not need a great deal of knowledge about computer intrusions because their position with the organization often allows them to gain unrestricted access and cause damage to the target system or to steal system data. These individuals engage in purely malicious activities and should not be confused with non-malicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
Criminal groups and organize crime	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion.
Terrorist	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.
Unknown malicious outsiders	Unknown malicious outsiders are threat sources or agents that, due to a lack of information, agencies are unable to classify as being one of the five types of threat sources or agents listed above.

Source: GAO analysis of unclassified government and nongovernmental data. GAO 16-79.

THE LANGUAGE OF CYBERWAR

Today's fast-evolving "information age" technology has intensified the importance of critical infrastructure protection, in which cybersecurity has become as critical as physical security to protecting virtually all critical infrastructure sectors. The Department of Defense (DoD) determined that cyber threats to contractors' unclassified information systems represented an unacceptable risk of compromise to DoD information and posed a significant risk to U.S. national security and economic security interests.

Many of the cyber intrusion incidents we read or hear about have added new terms or new uses for old terms to our vocabulary. For example, old terms such as botnets (short for robot networks, also called bots, zombies, botnet fleets, and many others) are groups of computers that have been compromised with malware such as Trojan Horses, worms, backdoors, remote control software, and viruses that have taken on new connotations in regards to cybersecurity issues. Relatively new terms such as scanners, Windows NT hacking tools, ICQ hacking tools, mail bombs, sniffer, logic bomb, nukers, dots, backdoor Trojan, key loggers, hackers' Swiss knife, password crackers, blended threats, Warhol Worms, Flash Threats, Targeted Attacks, and BIOS crackers are now commonly read or heard.

New terms have evolved along with various control mechanisms. For example, because many control systems are vulnerable to attacks of varying degrees, these attack attempts range from telephone line sweeps (wardialing), to wireless network sniffing (wardriving), to physical network port scanning, and to physical monitoring and intrusion. When wireless network sniffing is performed at (or near) the target point by a pedestrian (warwalking), meaning that instead of a person being in an automotive vehicle, the potential intruder may be sniffing the network for weaknesses or vulnerabilities on foot, posing as a person walking, but they may have a handheld PDA device or laptop computer (Warwalking 2003). Further, adversaries can leverage common computer software programs, such as Adobe acrobat and Microsoft Office, to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

Finally, the communications infrastructure and the utilities are extremely dependent on the information technology (IT) sector. This dependency is due to the reliance of the communications systems on the software that runs the control mechanism of the operations systems, the management software, the billing software, and any number of other software packages used by industry. Table 7.3 provides descriptions of common exploits or techniques, tactics, and practices used by cyber adversaries.

Table 7.3 Common Methods of Cyber Exploits

Exploit	*Description*
Watering hole	A method by which threat actors exploit the vulnerabilities of carefully selected websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct then to a website that requires information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cybersecurity supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Structured Query Language (SQL) injection	An exploit that involves the alteration of a database search in a web-based application can be used to obtain unauthorized across to sensitive information in a database, resulting in data loss at corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing the adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming code (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookers (data exchanged between a web server and a browser), log key stokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.

(*Continued*)

Table 7.3 (Continued)

Exploit	*Description*
Cross-site request forgery	An exploit takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified requires that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory path name in an application that does not properly neutralize special elements (e.g., '…', '/', '…/', etc.)
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally-controlled format strings in print-style functions to gain access to information and/or execute unauthorized code or commands.
Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site which may contain malware that compromises the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ( )."
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from un-functionality trusted sphere	An exploit that uses trusted, third-party executable requests (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanism are unable to determine whether functionality is from trusted sources, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit which combines elements of two or more of the aforementioned techniques.

Source: GAO (2015).

THE BOTTOM LINE

The United States Treasury, in collaboration with the financial services sector stakeholders, identified cyber risk as significant to the sector. Specifically, the 2010 financial services sector–specific plan stated that all of the sector's services rely on its cyber infrastructure, which necessitates that cybersecurity be factored into all of the sector's critical infrastructure protection activities. In addition, as a highly regulated sector, the financial services sector has been required to undergo risk assessments by financial regulators to satisfy regulatory requirements.

REFERENCES AND RECOMMENDED READING

Associated Press. 2009. Goal: Disrupt. From the 04/04/09 The Virginian-Pilot, Norfolk, Va.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

DOE. 2001. *21 Steps to Improve Cyber Security of SCADA Networks*. Washington, DC: Department of Energy.

FEMA. 2008. *FEMA452: Risk Assessment A How to Guide*. Accessed May 1, 2008 @ fema.gov/library/file?type=published/filetofile.

FEMA. 2015. *Protecting Critical Infrastructure against Insider Threats.* Accessed April 17, 2015 @ http://emilms.fema.gov/IS0915/IABsummary.htm.

FBI. 2000. *Threat to Critical Infrastructure*. Washington, DC: Federal Bureau of Investigation.

FBI. 2007. *Ninth Annual Computer Crime and Security Survey*. FBI: Computer Crime Institute and Federal Bureau of Investigations.

FBI. 2014. *Protecting Critical Infrastructure and the Importance of Partnerships*. Accessed @ https://www.fib.gov/news/speeches/protecitng-critical-infrastruce-andt-the-importantce-o.

GAO. 2003. *Critical Infrastructure Protection: Challenges in Securing Control System*. Washington, DC: United States General Accounting Office.

GAO. 2015. *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*. Washington, DC: United States Government Accountability Office.

Gellman, B. 2002. "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say." *Washington Post*, June 27, p. A01.

Minter, J. G. 1996. Prevention Chemical Accidents Still A Challenge. *Occupational Hazards*, September.

National Infrastructure Advisory Council. 2008. *First Report and Recommendations on the Insider Threat to Critical Infrastructure.* Washington, DC.

NIPC. 2002. *National Infrastructure Protection Center Report*. Washington, DC: National Infrastructure Protection Center.

Spellman, F. R. 1997. *A Guide to Compliance for PSM/RMP*. Lancaster, PA: Technomic Publishing Company.

Stamp, J. et al. 2003. *Common Vulnerabilities in Critical Infrastructure Control Systems*, 2nd ed. Sandia National Laboratories.

US DOE. 2002. *Vulnerability Assessment Methodology: Electric Power Infrastructure*. Washington, DC.

USEPA. 2005. *EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known SCADA Vulnerabilities*. Harris, J. Final Briefing Report. Washington, DC: USEPA.

Warwalking. 2003. Accessed May 9, 2008 @ http://warwalking.tribe.net.

Chapter 8

Emergency Response

> We're in uncharted territory.
>
> —Rudy Giuliani (9/11/01)

When New York Mayor Rudy Giuliani made the above statement to Police Commissioner Bernard Kerik at the World Trade Center Site, September 11, 2001, one of the first (and not to be forgotten) gross understatements of the 21st century had been uttered. Indeed, for citizens of the United States of America, the 9/11 events placed our level of consciousness, awareness, fear, and questions of what to do next in "uncharted territory." Actually, when you get right down to it, 9/11 generated more questions than anything else. Many are still asking the following questions today:

Why?
Why would anyone have the audacity to attack the United States?
What kind of cold-blooded killers would even conceive of such an event?
Who were the terrorists who perpetrated 9/11?
What were the terrorists' goal(s)?
Why?
Why were we not ready for such an attack?
Why had we not foreseen such an event?
Could anyone have prevented it?
Bottom line questions: Why us? Hell, why anyone?

These and several other questions continue to resonate today; there is no doubt that they will continue to haunt us for some time to come.

Maybe we ask post 9/11-related questions because of who we are, what we are, and what we are not. That is, because we are Americans, we are free, uninhibited thinkers who think what we say and say what we think—isn't

America great? Most Americans are soft-hearted and sympathetic to those in need—compassion is the very nature and soul of being an American. Americans are not born terrorists; they are not born into a terrorist regime; they are not raised with fear in their hearts—they are not afraid every time they leave their homes and go about their daily business. Suicide bombers and other like terrorists are those that occupy some other faraway place; definitely not America, and they are definitely not American. Right?

Notwithstanding exceptions to the rule, such as Timothy McVeigh (a so-called red-blooded American, born and raised in America) and that terrorist (whether a national or foreigner) who mailed the anthrax, terrorism on a mass scale was foreign to us then.

Today, from a safety/security point of view, based on the events of 9/11 and the anthrax events, we should no longer be asking why. Instead, we should not waste our time, money, and energy asking why or in pointing a finger of blame at our government, military, emergency responders, and/or the terrorists. We should stop asking *why* and shift our mindset to asking *what if*. The point is we need to stop feeling sorry for ourselves and except the fact that there are folks out there who do not share our view of the American way of life. Earlier, in regard to security preparedness, we pointed to the need to ask what-if questions. Simply, what-if analysis is a proactive approach used to prevent or mitigate certain disasters, extreme events—whether human- or nature-generated. Obviously, asking and properly answering what-if questions has little effect on preventing the actions of Mother Nature, such as earthquakes, tornadoes, hurricanes (like Katrina), mud slides, and others. On the other hand, it is true that what-if questions, when properly posed and answered (with results), can reduce the death toll and overall damage caused by these natural disasters. We are certainly aware that these natural events are possible, probable, and likely, and their effects can be horrendous—beyond tragic. The irony is apparent, however, especially when we ask this question: How many of us are actually willing to move away from or out of earthquake zones, hurricane and tornado allies, and floodplains to live somewhere else?

The fact is we do not possess a crystal ball to foretell the future. What-if questions prepare us to react and respond to certain contingencies. And we must respond, because there are certain events we simply can't prevent. The best response to an event we can't prevent is summed up by the Boy Scout motto: Be Prepared!

FINANCIAL SERVICES SECTOR CONTINGENCY PLANNING

Emergency response planning or contingency planning or emergency action plans (EAPs) for extreme events has long been standard practice for safety

professionals in industrial systems operations. For many years, prudent practices have required consideration of the potential impact of severe natural events (forces of nature), including earthquakes, tornadoes, floods, hurricanes, and blizzards. These possibilities have been included in financial services sector industry infrastructure emergency preparedness and disaster response planning. In addition, many financial services sector production and cyber distribution centers have considered the potential consequences of man-made disasters such as operator error and manufacturer's equipment defects. Currently, financial services sector managers and operators must also consider violence in the workplace. Moreover, at present, as this text has pointed out, there is a new focus of concern: the potential effects of intentional acts by domestic (homegrown—in-house) or international (foreign) terrorists.

As a result, the security paradigm has not necessarily changed, but instead has been radically adjusted—reasonable, necessary, and sensible accommodation for and mitigation of just about any emergency situation imaginable have been and continue to be made. Because we cannot foresee all future domestic or international acts of terrorism, we must be prepared to shift from the proactive to reactive mode on short notice—in some cases, on very short notice. Accordingly, we must be prepared to respond to, react to, and mitigate what we can't prevent. Unfortunately, there is more we can't prevent than we can prevent. In light of this, in this section we present in outline form a reactive mitigation procedure, the template example for a standard financial services sector Crisis Communications Plan (CCP), dealing with natural and man-caused disasters, which could also be applied in response to acts of terrorism.

CRISIS COMMUNICATIONS PLAN

Note: The following criteria has not been established as anything other than guidelines and are offered not as definitive or official regulations or procedures but rather as informed advice (based on more than 30 years of safety, industrial hygiene, emergency contingency planning, and security experience) insofar as to the subject matter specific to both public and private sectors.

Also, this emergency action plan applies to locations and facilities that are occupied by financial services personnel performing their designated work activities.

***

The fact is well known: when an emergency occurs, the need to communicate is immediate. The goals of CCPs are to document and understand the steps needed to

- rapidly restore financial processing activities after an emergency,
- minimize financial services sector equipment damage,
- minimize impact and loss to customers,
- minimize negative impacts on employee safety, and
- provide emergency public information concerning customer service.

Although we are concerned with the financial services sector in this text, the USEPA developed *Large Water System Emergency Response Outline: Guidance to Assist Community Water Systems in Complying with the Public Health and Bioterrorism Preparedness and Response Act of 2002* (dated July 2003), with minor adjustments, which can be applied as a template for any critical infrastructure sector, including the financial services sector. This template provides guidance and recommendations to aid facilities in the preparation of emergency response plans under the PL 107-188. The template is provided below.

CCPs do not necessarily need to be one document. They may consist of an overview document, individual EAPs, check lists, additions to existing operations manuals, appendices, and so on. There may be separate, more detailed plans for specific incidents. There may be plans that do not include particularly sensitive information and those that do. Existing applicable documents should be referenced in the CCP.

Crisis Communication Plan Template

I. Introduction

Safe and reliable operation is vital to every industrial operation. The CCP is an essential part of managing a financial services sector process or entity. The introduction should identify the requirement to have a documented CCP, the goal(s) of the plan (e.g., be able to quickly identify an emergency and initiate timely and effective response action, be able to quickly respond and repair damages to minimize system downtime), and how access to the plan is limited. Plans should be numbered for control. Recipients should sign and date a statement that includes their (1) CCP number, (2) agreement not to reproduce the CCP, and (3) they have read the CCP.

II. Emergency Planning Process

A. Planning Partnerships

The planning process should include those parties who will need to help the financial services sector in an emergency situation (i.e., first responders, law enforcement, public health officials, nearby utilities, local emergency planning committees, etc.). Partnerships should track from the financial services sector operation up through

local, state, regional, and federal agencies, as applicable and appropriate, and could also document compliance with governmental requirements.

B. General Emergency Response Policies, Procedures, Actions, Documents

A short synopsis of the overall emergency management structure, how other industrial emergency response, contingency, and risk management plans fit into the CCP for financial services sector emergencies, and applicable policies, procedures, actions plans, and reference documents should be cited. Policies should include interconnect agreements with adjacent communities and just how the CCP may affect them.

C. Scenarios

Use your Vulnerability Assessment (VA) findings to identify specific emergency action steps required for response, recovery, and remediation for applicable incident types. In Section V of this plan, specific emergency actions procedures addressing each of the incident types should be addressed.

III. Emergency Response Plan—Policies

A. System Specific Information

In an emergency, financial services sector industries need to have basic information for system personnel and external parties such as law enforcement, emergency responders, repair contractors/vendors, the media, and others. The information needs to be clearly formatted and readily accessible so the system staff can find and distribute it quickly to those who may be involved in responding to the emergency. Basic information that may be presented in the emergency response plan are the system's ID number, system name, system address or location, directions to the system, population served, number of service connections, system owner, and information about the person in charge of managing the emergency. Distribution maps, detailed plant drawings, site plans, source/storage/production energy locations, and operations manuals may be attached to this plan as appendices or referenced.

1. PWS ID, Owner, Contact Person
2. Population served and service connections
3. System Components
   (a) Conduits and constructed conveyances
   (b) Physical barriers
   (c) Electronic, computer, or other automated systems which are utilized by the financial services sector industry
   (d) Emergency power generators (onsite & portable)
   (e) The operation and maintenance of such system components

B. Chain-of-Command Chart developed in Coordination with Local Emergency Planning Committee (internal and/or External Emergency Responders, or both)
   1. Contact Name
   2. Organization and Emergency Response Responsibility
   3. Telephone number(s) (hardwire, cell phones, faxes, e-mail)
   4. State 24-hour Emergency Communications Center Telephone

C. Communications Procedures: Who, What, When

During most emergencies, it will be necessary to quickly notify a variety of parties both internal and external to the financial services sector entity. Using the Chain-of-Command Chart and all appropriate personnel from the lists below, indicate who activates the plan, the order in which notification occurs, and the members of the Emergency Response Team. All contact information should be available for routine updating and readily available. The following lists are not intended to be all inclusive—they should be adapted to your specific needs.

1. Internal Notification Lists
   (a) Operations Dispatch
   (b) Financial Services Sector Manager
   (c) Data (IT) Manager
   (d) Facility Managers
   (e) Maintenance Manager
   (f) Other
2. Local Notification
   (a) Head of local government (i.e., Mayor, City Manager, Chairman of Board, etc.)
   (b) Public Safety Officials—Fire, Local Law Enforcement (LLE), police, EMS, safety if a malevolent act is suspected, LLE should be immediately notified and in turn will notify the FBI, if required. The FBI is the primary agency for investigating sabotage.
   (c) Other Government Entities: Health, Schools, Parks, Finance, Electric, and so on.
3. External Notification Lists
   (a) State Department of Environmental Quality (DEQ)
   (b) USEPA/USDOE/DHS/FCC
   (c) State Police
   (d) State Health Department (lab)
   (e) Critical customers (special considerations for hospitals, federal, state and country government centers, etc).
   (f) Service Aid

(g) Mutual Aid
(h) Commercial customers not previously notified

4. Public/Media Notification: When and How to Communicate
Effective communication is a key element of emergency response, and a media or communications plan is essential to good communications. Be prepared by organizing basic facts about the crisis and your assets. Develop key messages to use with the media that are clear, brief, and accurate. Make sure your messages are carefully planned and have been coordinated with local and state officials. Considerations should be given to establishing protocols for both field and office staff to respectfully defer questions to the utility spokesperson.

Be prepared to list geographic boundaries of the affected area (e.g., west of highway a, east of highway b, north of highway c, and south of highway d to ensure the public clearly understands the system boundaries.)

E. Personnel Safety
This should provide direction as to how operations staff, emergency responders, and the public should respond to a potential toxic chemical release, including facility evacuation, personnel accountability, proper Personnel Protective Equipment as dictated by the Risk Management Program and Process Safety Management Plan, and whether the nearby public should be "in-place sheltered" or evacuated.

F. Equipment
The Emergency Response Plan (ERP) should identify equipment that can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and protect the safety and supply of communities and individuals. The financial services sector facility should maintain an updated inventory of current equipment and repair parts for normal maintenance work.

Because of the potential for extensive or catastrophic damage that could result from a malevolent act, additional sources should be identified for the acquisition and installation of equipment and repair parts in excess of normal usage. A certain number of "long-lead" procurement equipment should be inventoried and the vendor information for such unique and critical equipment maintained. In addition, mutual aid agreements with other industries, and the equipment available under the agreement, should be addressed. Inventories of current equipment, repair parts, and associated vendors should be indicated.

G. Property Protection

A determination should be made as to what financial services sector producing, processing, distribution operation/facility should be immediately "locked down," specific access control procedures implemented, initial security perimeter established, a possible secondary malevolent event considered. The initial act may be a divisionary act.

H. Training, Exercises, and Drills
Emergency response training is essential. The purpose of the training program is to inform employees or what is expected of them during an emergency situation. The level of training on a CCP directly affects how well a financial services sector facility's employees can respond to an emergency. This may take the form of orientation scenarios, tabletop workshops, functional exercises, and so on.

I. Assessment
To evaluate the overall CCP's effectiveness and to ensure that procedures and practices developed under the CCP are adequate and are being implemented; financial services sector industry staff should audit the program on a periodic basis.

IV. Emergency Action Plans (EAPs)
These are detailed procedures used in the event of an operation emergency or malevolent act. EAPs may be applicable across many different emergencies and are typically common core elements of the overall municipality ERP (e.g., responsibilities, notifications lists, security procedures, etc.) and can be referenced.

A. Event classification/severity of emergency
B. Responsibilities of Emergency Director
C. Responsibilities of Incident Commander
D. Emergency Operations Center (EOC) activation
E. Division internal communications and reporting
F. External communications and notifications
G. Emergency telephone list (division internal contacts)
H. Emergency telephone list (off-site responders, agencies, state 24-hr emergency phone number, and others to be notified)
I. Mutual Aid Agreements
J. Contact list of available emergency contractor services/equipment
K. Emergency equipment list (including inventory for each facility)
L. Security and access control during emergencies
M. Facility evacuation and lockdown and personnel accountability
N. Treatment and transport of injured personnel (including electrocution and petrochemical exposure)
O. Water use restrictions during emergencies
P. Protection of vital records during emergencies

Q. Record keeping and reporting (FCC, FEMA, DHS, DOT, OSHA, EPA, and other requirements) (it is important to maintain accurate financial records of expenses associated with the emergency event for possible federal reimbursement.)
R. Emergency program training, drills/and tabletop exercises
S. Assessment of emergency management plan and procedures
T. Crime scene preservation training and plans
U. Communication Plans:
    1. Police
    2. Fire
    3. Local Government
    4. Media
    5. And so forth
V. Administration and logistics, including EOC, when established
W. Equipment needs/maintenance of equipment
X. Recovery and restoration of operations
Y. Emergency event closeout and recovery

V. Incident-Specific Emergency Action Plans (EAPs)

Incident-Specific EAPs are action procedures that identify specific steps in responding to an operational emergency of malevolent act.

A. General Response to Terrorist Threats (Other than Bomb Threat and Incident-Specific Threats)
B. Incident-Specific Response to Man-Made or Technological Emergencies
    1. Contamination event (Articulated Threat with Unspecified Materials)
    2. Contamination Threat at a Major Event
    3. Notification from Health Officials of Potential Contamination
    4. Intrusion through Supervisory Control and Data Acquisition (SCADA)
C. Significant structural damage resulting from intentional act
D. Customer complaints
E. Severe weather response (snow, ice, temperature, lightning)
F. Flood response
G. Hurricane and/or tornado response
H. Fire response
I. Explosion response
J. Major vehicle accident response
K. Electrical power outage response
L. Water supply interruption response
M. Transportation accident response—barge, plane, train, semi-trailer/tanker

N. Contaminated/tampered with water treatment chemicals
O. Earthquake response
P. Disgruntled employees response (i.e., workplace violence)
Q. Vandals response
R. Bomb threat response
S. Civil disturbance/riot/strike
T. Armed intruder response
U. Suspicious mail handling and reporting

VI. Next Steps
  A. Plan Review and Approval
  B. Practice and Plan to Update (as necessary, once every year recommended)
    1. Training requirements
    2. Who is responsible for conducting training, exercises, and emergency drills?
    3. Update and assessment requirements
    4. Incident-specific requirements

VII. Annexes
  A. Facility and Location Information
    1. Facility maps
    2. Facility drawings
    3. Facility descriptions/layout
    4. And so on.

VIII. References and Links
  A. Department of Homeland Security—www.dhs/gov/dhspublic
  B. Environmental Protection Agency—www.epa.gov
  C. Federal Emergency Management Agency—www.fema.gov

THE BOTTOM LINE

Because industrial emergencies (in less than extreme conditions) can seriously affect the surrounding community and environment, and because poor planning and/or panic can only make a bad situation worse, and can also lead to additional injury and death, your role as financial services sector manager in emergency response is doubly important. A crisis out of hand can easily devastate a community—and your organization is (or should be) an active member of your community. By ensuring less than effective emergency response, financial services site managers endanger not only themselves and their organizations but also endanger their organization's community and standing as well.

REFERENCES AND RECOMMENDED READING

Brauer, R. L. 1994. *Safety and Health for Engineers.* New York: Van Nostrand Reinhold.

CoVan, J. 1995. *Safety Engineering*. New York: John Wiley and Sons.

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc _1214597989952.shtm.

Healy, R. J. 1969. *Emergency and Disaster Planning*. New York: Wiley.

Office of the Federal Register, 29 CFR 1910.120. Washington, DC: Office of the Federal Register, 1987.

Planning Guide and Checklist for Hazardous Materials Contingency Plans. Washington, DC: FEMA-10, Federal Emergency Management Agency, July 1981.

Smith, A. J. 1980. *Managing Hazardous Substances Accidents*. New York: McGraw-Hill.

Spellman, F. R. 1997. *A Guide to Compliance for Process Safety Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.

U.S. Army Corps of Engineers. *Safety and Health Requirements Manual*, rev. ed. Washington, DC: EM 385-1-1, October 1987.

USDOE. 2008. *Emergency Support Function #12—Energy Annex*. Washington, DC: United States Department of Energy.

USDOE. 2010. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* Washington, DC: United States Department of Energy.

USEPA. 2002. *Water Utility Response, Recovery & Remediation Guidance for Man-made and/or Technological Emergencies*. Washington, DC: United States Environmental Protection Agency.

USEPA. 2003. *Large Water System Emergency Response Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*. EPA 810-F-03-007. Accessed June 6 @ www.epa.gov/safewater/security. Washington, DC: United States Environmental Protection Agency.

Chapter 9

Security Techniques and Hardware

> There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind.
>
> —Napoleon Bonaparte

> If your facility still uses keyed locks, does anyone in your facility control those keys? Does anyone in your facility know who has keys? Does anyone know how many keys have been issued? Is there a recorded record of each key that has been issued?
>
> I know your password . . . therefore, you belong to me.

TELLER'S WINDOW

Whenever we walk into a bank, credit union, or other financial services entity, we usually pay little attention to our surroundings. Why? Well, we have become used to the surroundings and the ambience through frequent use of such a place. Or, more than likely, we are in a hurry, as usual, and surroundings are not that important to us; instead, the business at hand is much more important.

Let's say, on the other hand, we are part of that group of people who take it all in, no matter where or when. Well, if this is the case, when we walk into the bank there are a few things that stand out to us. First it is quiet, professional, and staffed with well-dressed, busy people. The standard teller window greets us as we stand to make our transaction. We see that the window is one of those typical bullet resistant windows with a deal tray and a voice-transmission system. When we glance to our right or left or glance above the place we are standing, we probably notice the CCTV security cameras here

and there—with some pointed right at us. And we presume that the teller behind the window has an alarm or panic button within easy reach.

These security devices are obvious to us or we assume they are present. However, it is what we do *not* see, anticipate, or comprehend is present (or should be) that is really what this chapter emphasizes. There are many devices and security systems that are available to protect financial services sector assets but that are not immediately visible.

THE MULTIPLE-BARRIER APPROACH

In a perfect world, all financial services sector physical sites/facilities would be secured in a layered fashion. Layered security (aka multiple-barrier) systems are vital. Using the "protection-in-depth" principle requiring that an adversary defeat several protective barriers or security layers to accomplish their goal, financial services sector physical infrastructure can be made more secure. "Protection-in-depth" is a term commonly used by the military to describe security measures that reinforce one another, masking the defense mechanisms from view of intruders and allowing the defender time to respond to intrusion or attack.

A prime example of the use of the multi-barrier approach to ensure security and safety is demonstrated by the practices of the bottled water industry. In the aftermath of 9/11 and the increased emphasis on Homeland Security, a shifted paradigm of national security and vulnerability awareness emerged. Recall that in the immediate aftermath of the 9/11 tragedies, emergency responders and others responded quickly and worked to exhaustion. In addition to the emergency responders, bottled water companies responded immediately by donating several million bottles of water to the crews at the crash sites in New York City, at the Pentagon, and in Pennsylvania. The International Bottled Water Association (IBWA 2004) reports that "within hours of the first attack, bottled water was delivered where it mattered most; to emergency personnel on the scene who required ample water to stay hydrated as they worked to rescue victims and clean up debris."

Bottled water companies continued to provide bottled water to responders and rescuers at the 9/11 sites throughout the post-event processes. These patriotic actions by the bottled water companies, however, begged the question: How do we ensure the safety and security of the bottled water provided to anyone? IBWA had the answer: using a multiple-barrier approach, along with other principles, will enhance the safety and security of bottled water. IBWA (2004, p. 3) describes its multiple-barrier approach as follows:

> *A multi-barrier approach*—Bottled water products are produced utilizing a multi-barrier approach, from source to finished product, that helps prevent

possible harmful contaminants (physical, chemical, or microbiological) from adulterating the finished product as well as storage, production, and transportation equipment. Measures in a multi-barrier approach may include source protection, source monitoring, reverse osmosis, distillation, filtration, ozonation, or ultraviolet (UV) light. Many of the steps in a multi-barrier system may be effective in safeguarding bottled water from microbiological and other contamination. Piping in and out of plants, as well as storage silos and water tankers are also protected and maintained through sanitation procedures. In addition, bottled water products are bottled in a controlled, sanitary environment to prevent contamination during the filling operation.

In financial services sector infrastructure security, protection-in-depth is used to describe a layered security approach. A protection-in-depth strategy uses several forms of security techniques and/or devices against an intruder and does not rely on one single defensive mechanism to protect infrastructure. By implementing multiple layers of security, a hole or flaw in one layer is covered by the other layers. An intruder will have to intrude through each layer without being detected in the process—the layered approach implies that no matter how an intruder attempts to accomplish his goal, he will encounter effective elements of the physical protection system.

For example, as depicted in figure 9.1, an effective security layering approach requires that an adversary penetrate multiple, separate barriers to gain entry to a critical TARGET at a financial services sector facility. As shown in figure 9.1, protection-in-depth (multiple layers of security) helps to ensure that the security system remains effective in the event of a failure or an intruder bypassing a single layer of security.

Again, as shown in figure 9.1, layered security starts with the outer perimeter (a wall, perhaps—the first line of physical security) of the facility and goes inward to the facility, the buildings, structures, other individual assets, and finally to the contents of those buildings—the TARGETs.

The area between the outer perimeter and structures or buildings is known as the site. This open site area provides an incomparable opportunity for early identification of an unauthorized intruder and initiation of early warning/response. This open space area is commonly used to calculate the standoff distance; that is, it is the distance between the outside perimeter (public areas to the wall) to TARGET or critical assets (buildings/structures) inside the perimeter (inside the wall line—the restricted access area).

The open area, between perimeter and TARGET (e.g., operations center), if properly outfitted with various security devices, can also provide layered protection against intruders. For example, lighting is a deterrent. Based on personal experience, I think an open area within the facility site that is almost as well lighted at night as would be expected during the day. In addition, strategically placed motion detectors along with crash barriers at perimeter gate

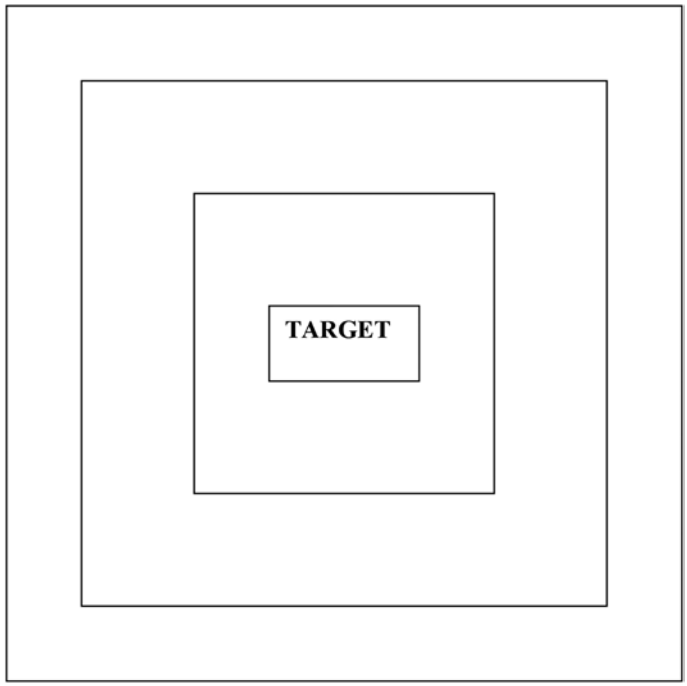

Figure 9.1 A Layered Approach to Security.

openings and in front of vital structures are also recommended. Of course, armed, mobile guards who roam the interior of the site on a regular basis provide the ultimate in security.

The next layer of physical security is the outside wall of the target structure(s) itself. Notwithstanding door, window, and/or skylight entry, walls prevent most intruders from easy entry. If doors can only be entered using card reader access, security is shored up or enhanced to an extent. The same can be said for windows and skylights that are fashioned small enough to prohibit normal human entry. These same "weak" spots in buildings can be bastioned with break-proof or reinforced security glass.

The final layer of security is provided by properly designed interior features of buildings. Examples of these types of features include internal doors and walls, equipment cages, and backup or redundant equipment.

In the preceding discussion, the features described refer to perfect world conditions; that is, to those conditions that we "would want" (i.e., the security manager's proverbial wish list) to be incorporated into the design and installation of a new financial services sector infrastructure. Post 9/11, in a not-so-perfect world, many of the peripheral (fence/wall line) measures described above are difficult to incorporate into financial services sector infrastructure.

This is not to say that financial services sector sites and facilities do not have fence lines or walls; many of them do. One problem is that many of these facilities were constructed many years ago and/or in urban settings that do not allow major hardscape security additions.

The fly in the ointment for the financial services sector assets is accessibility. People who use financial services in person need to enter the facilities to conduct their business. Thus, the multiple-barrier approach to security in a bank on a busy city street, for example, is unrealistic, at best.

Managers of financial services sector infrastructure have four primary security areas to manage. These security areas are listed and described below.

- *Physical Security*—in the financial sector, where practicable, physical security techniques and practices has the most effect at "fenced" locations. At such locations, a systems approach is best, where detection, assessment, communication, and response are planned and supported by resources, procedures, and policies.
- *Cyber/Information Technology Security*—only the use of key operating systems that have been properly vetted and scrubbed of alleged Chinese and/or Russian Trojan Horses hacked into the North American electrical grid is important. The only positive way to ensure the security of the North American Grid is to disconnect its cyber and other digital systems from the Internet. This step is impractical at the present time, but points to the need to conduct frequent audits of the system and install firewall protection in digital components and other systems to prevent hacking. Frequent third-party penetration testing is advised.
- *Employment Screening*—mitigates the threat from the "enemy at the water cooler" (inside the organization). We are always amazed whenever we conduct security audits for various companies. Often, a simple check such as reviewing an employee's driving record often reveals that the employee has no license, is driving on a suspended license, or has a horrific driving record. Hiring standards and preemployment background investigations may help ensure the trustworthiness and reliability of personnel who have unescorted access to critical facilities.
- *Protecting Potentially Sensitive Information*—the old saying that goes—a secret can best be held between three people so long as two of the three are dead—makes the point that reducing the likelihood that information could be used by those intent on disrupting operations or causing death destruction in financial services sector plants/sites is crucial. Information should only be shared within an organization on a need-to-know basis only.

For existing facilities, security upgrades should be based on the results generated from the vulnerability assessment (VA), which characterizes and

prioritizes those assets that may be targeted. Those vulnerabilities identified must be protected.

In the following sections, various security hardware and/or devices are described. These devices serve the main purpose of providing security against physical and/or digital intrusion. That is, they are designed to delay and deny intrusion and are normally coupled with detection and assessment technology. Possible additional security measures, based on the VA that may be recommended include the following (NAERC 2002):

- Electronic security
- Closing nonessential perimeter and internal portals
- Physical barriers such as bollards or highway (Jersey) walls
- Fencing
- Lighting
- Security surveys
- Availability of security resources
- General personnel and security officer training
- Law enforcement liaison
- Ensure availability of essential spare parts (machines, repair parts, wire, pipe, valves, transformers, etc.) for critical facilities

But keep in mind, no matter the type of security device or system employed, financial services sector systems cannot be made immune to all possible intrusions or attacks. Whenever a facility safety/security manager tells us that he or she has secured their site 100 percent, we are reminded of Bruce Schneier's (2000) view of security: "You can't defend. You can't prevent. The only thing you can do is detect and respond." Simply, when it comes to making "anything" absolutely secure from intrusion or attack, there is no silver bullet.

And before we describe these hardware devices, keep in mind that in addition to security hardware devices to help protect and monitor sector assets there are also a few employee practices and actions that can be taken. For example, when a bank computer system fails and must be disposed of, how is it disposed of? Is there a procedure or practice in place to prevent the valuable information on the system's hard drive from being pulled from a trash heap or from a dumpster dive and used by potential enemies? Are shredders used? Are they state-of-the-art shredders that prevent scraps from being reassembled by enemies? Are building cleaning crews properly vetted and supervised? Do you have a team that routinely inspects suspended ceilings for bugs, cameras, and listening recorders? Do you have key stroke reader capability; that is, can you record what messages are being sent by employees? Do you routinely check hardwired phone lines? Have your removed all

door signs that tell anyone what is on the other side of the room? Have you trained your employees to be slightly suspicious of just about anything and everything? Have you opened your manholes lately to see what is inside?

All of these practices just mentioned do not require security hardware such as barriers, motion detectors, fences, locks, biometric systems, video cameras, armed guards, electrified fences, and so forth. What they require instead is common sense, awareness, and alert and engaged supervisors and employees. The point is what is heard at the water cooler is sometimes more significant than any security alarm apparatus can provide.

SECURITY HARDWARE DEVICES[1]

USEPA (2005) groups infrastructure security devices or products described below into four general categories:

- Physical asset monitoring and control devices
- Cyber protection devices
- Communication/integration
- Environmental monitoring devices

Physical Asset Monitoring and Control Devices—Aboveground, Outdoor Enclosures

Financial services sector facilities and sites can consist of multiple structural components spread over a wide area and typically include a centralized production and distribution center, as well component storage facilities that are typically distributed at multiple locations throughout the area. Space restrictions often limit the amount of equipment that can be located inside. In regard to electrical power, electrical substations are not usually suited for underground installation. Therefore, many pieces of critical electrical equipment are located outdoors and aboveground in configurations that are properly fenced, insulated, or isolated to prevent accidental electrical shock or short circuits/fires in equipment.

One of the most effective security measures for protecting aboveground equipment, where feasible, is to place it inside a building or exterior fenced structure. When/where this is not possible, enclosing the equipment or parts

[1] It is important to point out that even though the following USEPA security asset and device recommendations were first made for the water/wastewater critical infrastructure; these recommendations are applicable to all other critical infrastructure sectors, including the financial services sector where practicable.

of the equipment using some sort of commercial or homemade add-on structure may help to prevent tampering with the equipment. These types of add-on structures or enclosures, which are designed to protect people and animals from electrocution and to protect equipment both from the elements and from unauthorized access or tampering, typically consist of a box-like fenced structure that is placed over or around the entire component, or over/around critical parts of the component (i.e., valves, etc.), and is then secured to delay or prevent intruders from tampering with the equipment. The enclosures are typically locked or otherwise anchored to a solid foundation, which makes it difficult for unauthorized personnel to remove the enclosure and access the equipment.

Standardized aboveground enclosures are available in a wide variety of materials, sizes, and configurations. Many options and security features are also available for each type of enclosure, and this allows system operators the flexibility to customize an enclosure for a specific application and/or price range. In addition, most manufacturers can custom-design enclosures if standard, off-the-shelf enclosures do not meet a user's needs.

Many of these enclosures are designed to meet certain standards. For example, the American Society of Sanitary Engineers (ASSE) has developed Standard #1060, *Performance Requirements for Outdoor Enclosures for Backflow Prevention Assemblies*. If an enclosure will be used to house backflow preventer, this standard specifies the acceptable construction materials for the enclosure, as well as the performance requirements that the enclosure should meet, including specifications for freeze protection, drainage, air inlets, access for maintenance, and hinge requirements. ASSE #1060 also states that the enclosure should be lockable to enhance security.

Electrical substation and electrical equipment enclosures must meet the requirements and recommendations of various OHSA Standards, National Fire Protection Association (NFPA), National Electrical Codes (NEC), Institute of Electrical and Electronic Engineers (IEEE), and local code requirements.

Equipment enclosures can generally be categorized into one of four main configurations, which include the following:

- One piece, drop-over enclosures
- Hinged or removable top enclosures
- Sectional enclosures
- Shelters with access locks

All enclosures, including those with integral floors, must be secured to a *foundation* to prevent them from being moved or removed. Un- or poorly-anchored enclosures may be blown off the equipment being protected, or

may be defeated by intruders. In either case, this may result in the equipment beneath the enclosure becoming exposed and damaged. Therefore, ensuring that the enclosure is securely anchored will increase the security of the protected equipment.

The three basic types of foundations that can be used to anchor the aboveground equipment enclosure are *concrete footers*, *concrete slabs-on-grade*, or *manufactured fiberglass pads*. The most common types of foundations utilized for equipment enclosures are standard or slab-on-grade footers; however, local climate and soil conditions may dictate whether either of these types of foundations can be used. These foundations can be either precast or poured in place at the installation site. Once the foundation is installed and properly cured, the equipment enclosure is bolted or anchored to the foundation to secure it in place.

An alternative foundation, specifically for use with smaller Hot Box® enclosures, is a manufactured fiberglass pad known as the Glass Pad™. The Glass Pad™ has the center cut out so that it can be dropped directly over the piece of equipment being enclosed. Once the pad is set level on the ground, it is backfilled over a two-inch flange located around its base. The enclosure is then placed on top of the foundation, and is locked in place with either a staple- or a slotted-anchor, depending on the enclosure configuration.

One of the primary attributes of a security enclosure is its strength and resistance to breaking and penetration. Accordingly, the materials from which the enclosure is constructed will be important in determining the strength of the enclosure, and thus its usefulness for security applications. Enclosures are typically manufactured for either fiberglass or aluminum. With the exception of the one piece, drop-over enclosure, which is typically fabricated from fiberglass, each configuration described above can be constructed from either material. In addition, enclosures can be custom-manufactured from polyurethane, galvanized steel, or stainless steel. Galvanized or stainless steel is often offered as an exterior layer, or "skin," for an aluminum enclosure. Although they are typically utilized in underground applications, precast concrete structures can also be used as aboveground equipment enclosures. However, precast structures are much heavier and more difficult to maneuver than are their fiberglass and aluminum counterparts. Concrete is also brittle, and that can be a security concern, however, products can be applied to concrete structures to add strength and minimize security risks (i.e., epoxy coating). Because precast concrete structures can be purchased from any concrete producers, this document does not identify specific vendors for these types of products.

In addition to the construction materials, *enclosure walls* can be configured or reinforced to give them added strength. Adding insulation is one option that can strengthen the structural characteristics of an enclosure; however, some manufacturers offer additional features to add strength to exterior

walls. For example, while most enclosures are fabricated with a flat wall construction, some vendors manufacture fiberglass shelters with ribbed exterior walls. These ribs increase the structural integrity of the wall and allow the fabrication of standard shelters up to twenty feet in length. Another vendor has developed a proprietary process that uses a series of integrated fiberglass beams that are placed throughout a foam inner core to tie together the interior and exterior walls and roof. Yet another vendor constructs aluminum enclosures with horizontal and vertical redwood beams for structural support.

Other security features that can be implemented on aboveground, outdoor equipment enclosures include locks, mounting brackets, tamper-resistant doors, and exterior lighting.

Physical Asset Monitoring and Control Devices—Active Security Barriers

Active security barriers (also known as crash barriers) are large structures that are placed in roadways at entrance and exit points to protected facilities to control vehicle access to these areas. These barriers are placed perpendicular to traffic to block the roadway, so that the only way that traffic can pass the barrier is for the barrier to be moved out of the roadway. These types of barriers are typically constructed from sturdy materials, such as concrete or steel, so that vehicles cannot penetrate through them. They are also designed at a certain height off the roadway so that vehicles cannot go over them.

The key difference between *active* security barriers, which include wedges, crash beams, gates, retractable bollards, and portable barricades, and *passive* security barriers, which include non-moveable bollards, jersey barriers, and planters, is that active security barriers are designed so that they can be raised and lowered or moved out of the roadway easily to allow authorized vehicles to pass them. Many of these types of barriers are designed so that they can be opened and closed automatically (i.e., mechanized gates, hydraulic wedge barriers), while others are easy to open and close manually (swing crash beams, manual gates). In contrast to active barriers, passive barriers are permanent, non-movable barriers, and thus they are typically used to protect the perimeter of a protected facility, such as sidewalks and other areas that do not require vehicular traffic to pass them. Several of the major types of active security barriers such as wedge barriers, crash beams, gates, bollards, and portable/removable barricades are described next.

Types of Active Security Barriers

Wedge barriers are plated, rectangular steel buttresses approximately two to three feet high that can be raised and lowered from the roadway. When

they are in the open position, they are flush with the roadway and vehicles can pass over them. However, when they are in the closed (armed) position, they project up from the road at a 45-degree angle, with the upper end pointing toward the oncoming vehicle and the base of the barrier away from the vehicle. Generally, wedge barriers are constructed from heavy gauge steel, or concrete that contains an impact-dampening iron rebar core that is strong and resistant to breaking or cracking, thereby allowing them to withstand the impact from a vehicle attempting to crash through them. In addition, both of these materials help to transfer the energy of the impact over the barrier's entire volume, thus helping to prevent the barrier from being sheared off its base. In addition, because the barrier is angled away from traffic, the force of any vehicle impacting the barrier is distributed over the entire surface of the barrier and is not concentrated at the base, which helps prevent the barrier from breaking off at the base. Finally, the angle of the barrier helps hang up any vehicles attempting to drive over it.

Wedge barriers can be fixed or portable. Fixed wedge barriers can be mounted on the surface of the roadway ("surface-mounted wedges") or in a shallow mount in the road's surface, or they can be installed completely below the road surface. Surface-mounted wedge barricades operate by rising from a flat position on the surface of the roadway, while shallow-mount wedge barriers rise from their resting position just below the road surface. In contrast, below-surface wedge barriers operate by rising from beneath the road surface. Both the shallow-mounted and surface-mounted barriers require little or no excavation, and thus do not interfere with buried utilities. All three barrier mounting types project above the road surface and block traffic when they are raised into the armed position. Once they are disarmed and lowered, they are flush with the road; thereby allowing traffic to pass.

Installing rising wedge barriers requires preparation of the road surface. Installing surface-mounted wedges does not require that the road be excavated; however, the road surface must intact and strong enough to allow the bolts anchoring the wedge to the road surface to attach properly. Shallow-mount and below-surface wedge barricades require excavation of a pit that is large enough to accommodate the wedge structure, as well as any arming/disarming mechanisms. Generally, the bottom of the excavation pit is lined with gravel to allow for drainage. Areas not sheltered from rain or surface runoff can install a gravity drain or self-priming pump. Table 9.1 lists the pros and cons of wedge barriers.

Crash beam barriers consist of aluminum beams that can be opened or closed across the roadway. While there are several different crash beam designs, every crash beam system consists of an aluminum beam that is supported on each side by a solid footing or buttress, which is typically constructed from concrete, steel, or some other strong material. Beams typically

Table 9.1 Pros and Cons of Wedge Barriers

Pros	*Cons*
Can be surface-mounted or completely installed below the roadway surface.	Installations below the surface of the roadway will require construction that may interfere with buried utilities.
Wedge barriers have a quick response time (normally 3.5–10.5 seconds, but barrier can be 1–3 seconds in emergency situations. Because emergency activation of the barrier causes more wear and tear on the system than does normal activation, it is recommended for use only in true emergency situations.	Regular maintenance is needed to keep wedge fully operational.
Surface or shallow-mount wedge barricades can be utilized in locations with a high water table and/or corrosive soils.	Improper use of the system may result in authorized vehicles being hung up by the barrier and damaged. Guards must be trained to use the system properly to ensure that this does not happen. Safety technologies may also be installed to reduce the risk of the wedge activating under an authorized vehicle.
All three wedge barrier designs have a high crash rating, thereby allowing them to be employed for higher security applications.	
These types of barrier are extremely visible, which may deter potential intruders.	

Source: USEPA (2005).

contain an interior steel cable (typically at least one inch in diameter) to give them added strength and rigidity. The beam is connected by a heavy duty hinge or other mechanism to one of the footings so that it can swing or rotate out of the roadway when it is open, and can swing back across the road when it is in the closed (armed) position, blocking the road and inhibiting access by unauthorized vehicles. The non-hinged end of the beam can be locked into its footing, thus providing anchoring for the beam on both sides of the road and increasing the beam's resistance to any vehicles attempting to penetrate through it. In addition, if the crash beam is hit by a vehicle, the aluminum beam transfers the impact energy to the interior cable, which in turn transfers the impact energy through the footings and into their foundation, thereby minimizing the chance that the impact will snap the beam and allow the intruding vehicle to pass through.

"Crash beam barriers" can employ drop-arm, cantilever, or swing beam designs. Drop-arm crash beams operate by raising and lowering the beam

vertically across the road. Cantilever crash beams are projecting structures that are opened and closed by extending the beam from the hinge buttress to the receiving buttress located on the opposite side of the road. In the swing beam design, the beam is hinged to the buttress such that it swings horizontally across the road. Generally, swing beam and cantilever designs are used at locations where a vertical lift beam is impractical. For example, the swing beam or cantilever designs are utilized at entrances and exits with overhangs, trees, or buildings that would physically block the operation of the drop-arm beam design.

Installing any of these crash beam barriers involves the excavation of a pit approximately 48 inches deep for both the hinge and the receiver footings. Due to the depth of excavation, the site should be inspected for underground utilities before digging begins. Table 9.2 lists the pros and cons of crash beams.

In contrast to wedge barriers and crash beams, which are typically installed separately from a fence line, *gates* are often integrated units of a perimeter fence or wall around a facility.

Gates are basically movable pieces of fencing that can be opened and closed across a road. When the gate is in the closed (armed) position, the leaves of the gate lock into steel buttresses that are embedded in concrete foundation located on both sides of the roadway, thereby blocking access to the roadway. Generally, gate barricades are constructed from a combination of heavy gauge steel and aluminum that can absorb an impact from vehicles

Table 9.2 Pros and Cons of Crash Beams

Pros	*Cons*
Requires little maintenance, while providing long-term durability.	Crash beams have a slower response time (normally 9.5–15.3 seconds, but can be reduced to 7–10 seconds in emergency situations) than do other types of active security barriers, such as wedge barriers. Because emergency activation of the barrier causes more wear and tear on the system than does normal activation, it is recommended for use only in true emergency situations.
No excavation is required in the roadway itself to install crash beams.	All three crash beam designs possess a low crash rating relative to other types of barriers, such as wedge barriers, such as wedge barriers, and thus they typically are used for lower security applications.
	Certain crash barriers may not be visible to oncoming traffic and therefore may require additional lighting and/or other warning markings to reduce the potential for traffic to accidentally run into the beam.

Source: USEPA (2005).

attempting to ram through them. Any remaining impact energy not absorbed by the gate material is transferred to the steel buttresses and their concrete foundation.

Gates can utilize a cantilever, linear, or swing design. Cantilever gates are projecting structures that operate by extending the gate from the hinge footing across the roadway to the receiver footing. A linear gate is designed to slide across the road on tracks via a rack and pinion drive mechanism. Swing gates are hinged so that they can swing horizontally across the road.

Installation of the cantilever, linear, or swing gate designs described above involve the excavation of a pit approximately 48 inches deep for both the hinge and receiver footings to which the gates are attached. Due to the depth of excavation, the site should be inspected for underground utilities before digging begins. Table 9.3 lists the pros and cons of gates.

Bollards are vertical barriers at least 3 feet tall and 0.4 to 2 feet in diameter that are typically set 4 to 5 feet apart from each other so that they block vehicles from passing between them (see figure 9.2). Smaller bollards, usually 4-inch-diameter pipe filled with concrete, are installed in parking areas to prevent vehicles from striking walls or windows or to protect walkway areas. Bollards

Table 9.3 Pros and Cons of Gates

Pros	*Cons*
All three gate designs possess an intermediate crash rating, thereby allowing them to be utilized for medium to higher security applications.	Gates have a slower response time (normally 10–15 seconds, but can be reduced to 7–10 seconds in emergency situations) than do other types of active security barriers, such as wedge barriers. Because emergency activation of the barrier causes more wear and tear on the system than does normal activation, it is recommended for use only in true emergency situations.
Requires very little maintenance.	
Can be tailored to blend in with perimeter fencing.	
Gate construction requires no roadway excavation.	
Cantilever gates are useful for roads with high crowns or drainage gutters.	
These types of barriers are extremely visible, which may deter intruders.	
Gates can also be used to control pedestrian traffic.	

Source: USEPA (2005).

Figure 9.2 Bollard Sequence Placed In Front of Store Fronts and Sidewalks in Order to Protect Store Property and Pedestrians from Rogue and/or Terrorist Drivers. *Source*: Illustration by F. R. Spellman and Kathern Welsh.

can either be fixed in place, removable, or retractable. Fixed and removable bollards are passive barriers that are typically used along building perimeters or on sidewalks to prevent vehicles from going past them, while allowing pedestrians to pass through. In contrast to passive bollards, retractable bollards are active security barriers that can easily be raised and lowered to allow vehicles to pass between them. Thus, they can be used in driveways or on roads to control vehicular access. When the bollards are raised, they protect above the road surface and block the roadway; when they are lowered, they sit flush with the road surface, and thus allow traffic to pass over them. Retractable bollards are typically constructed from steel or other materials that have a low weight-to-volume ratio so that they require low power to raise and lower. Steel is also more resistant to breaking than is a more brittle material, such as concrete, and is better able to withstand direct vehicular impact without breaking apart.

Retractable bollards are installed in a trench dug across a roadway—typically at an entrance or gate. Installing retractable bollards requires preparing the road surface. Depending on the vendor, bollards can be installed either

in a continuous slab of concrete, or in individual excavations with concrete poured in place. The required excavation for a bollard is typically slightly wider and slightly deeper than the bollard height when extended aboveground. The bottom of the excavation is typically lined with gravel to allow drainage. The bollards are then connected to a control panel which controls the raising and lowering of the bollards. Installation typically requires mechanical, electrical, and concrete work; if utility personnel with these skills are available, then the utility can install the bollards themselves. Table 9.4 lists the pros and cons of retractable bollards.

Portable/removable barriers, which can include removable crash beams and wedge barriers, are mobile obstacles that can be moved in and out of position on a roadway. For example, a crash beam may be completely removed and stored off-site when it is not needed. An additional example would be wedge barriers that are equipped with wheels that can be removed after the barricade is towed into place.

When portable barricades are needed, they can be moved into position rapidly. To provide them with added strength and stability, they are typically anchored to buttress boxes that are located on either side of the road. These buttress boxes, which may or may not be permanent, are usually filled with sand, water, cement, gravel, or concrete to make them heavy and aid in stabilizing the portable barrier. In addition, these buttresses can help dissipate any impact energy from vehicles crashing into the barrier itself.

Because these barriers are not anchored into the roadway, they do not require excavation or other related construction for installation. In contrast, they can be assembled and made operational in a short period of time. The primary shortcoming to this type of design is that these barriers may move

Table 9.4 Pros and Cons of Retractable Bollards

Pros	*Cons*
Bollards have a quick response time (normally 3–10 seconds, but can be reduced to 1–3 seconds in emergency situations).	Bollard installations will require construction below the surface of the roadway, which may interfere with buried utilities.
Bollards have an intermediate crash rating, which allows them to be utilized for medium to higher security applications.	Some maintenance is needed to ensure barrier is free to move up and down.
	The distance between bollards must be decreased (i.e., more bollards must be installed along the same perimeter) to make these systems effective against small vehicles (i.e., motorcycles).

Source: USEPA (2005).

Table 9.5 Pros and Cons of Portable/Removable Barricades

Pros	*Cons*
Installing portable barricades requires no foundation or roadway excavation.	Portable barriers may move slightly when hit by a vehicle, resulting in a lower crash resistance.
Can be moved in and out of position in a short period of time.	Portable barricades typically require 7.75 to 16.25 seconds to move into place, and thus they are considered to have a medium response time when compared with other active barriers.
Wedge barriers equipped with wheels can be easily towed into place.	
Minimal maintenance is needed to keep barriers fully operational.	

Source: USEPA (2005).

if they are hit by vehicles. Therefore, it is important to carefully assess the placement and anchoring of these types of barriers to ensure that they can withstand the types of impacts that may be anticipated at that location. Table 9.5 lists the pros and cons of portable/removable barricades.

Because the primary threat to active security barriers is that vehicles will attempt to crash through them, their most important attributes are their size, strength, and crash resistance. Other important features for an active security barrier are the mechanisms by which the barrier is raised and lowered to allow authorized vehicle entry, and other factors, such as weather resistance and safety features.

Alarm Systems

An *alarm system* is a type of electronic monitoring system that is used to detect and respond to specific types of events—such as unauthorized access to an asset or a possible fire. These types of alarms are primarily integrated with process monitoring and reporting systems (i.e., SCADA systems). Note that this discussion does not focus on alarm systems that are not related to a facility's processes.

Alarm systems can be integrated with fire detection systems, intrusion detection systems (IDSs), access control systems, or Closed Circuit Television (CCTV) systems, such that these systems automatically respond when the alarm is triggered. For example, a smoke detector alarm can be set up to automatically notify the fire department when smoke is detected, or an intrusion alarm can automatically trigger cameras to turn on in a remote location so that personnel can monitor that location.

An alarm system consists of *sensors* that detect different types of events; an *arming station* that is used to turn the system on and off; a *control panel* that receives information, processes it, and transmits the alarm; and an *annunciator* that generates a visual and/or audible response to the alarm. When a sensor is tripped it sends a signal to a control panel, which triggers a visual or audible alarm and/or notifies a central monitoring station. A more complete description of each of the components of an alarm system is provided below.

Detection devices (also called *sensors*), are designed to detect a specific type of event (such as smoke, intrusion, etc.). Depending on the type of event they are designed to detect, sensors can be located inside or outside of the facility or other asset. When an event is detected, the sensors use some type of communication method (such as wireless radio transmitters, conductors, or cables) to send signals to the control panel to generate the alarm. For example, a smoke detector sends a signal to a control panel when it detects smoke.

Alarms use either *normally closed (NC)* or *normally open (NO)* electric loops, or "circuits," to generate alarm signals. In NC loops or circuits, all of the system's sensors and switches are connected in series. The contacts are "at rest" in the closed (on) position, and current continually passes through the system. However, when an event triggers the sensor, the loop is opened, breaking the flow of current through the system and triggering the alarm. NC switches are used more often than NO switches because the alarm will be activated if the loop or circuit is broken or cut, thereby reducing the potential for circumventing the alarm. This is known as a "supervised" system.

In NO loops or circuits, all of the system's sensors and switches are connected in parallel. The contacts are "at rest" in the open (off) position, and no current passes through the system. However, when an event triggers the sensor, the loop is closed. This allows current to flow through the loop, powering the alarm. NO systems are not "supervised" because the alarm will not be activated if the loop or circuit is broken or cut. However, adding an end-of-line resistor to an NO loop will cause the system to alarm if tampering is detected.

An *arming station*, which is the main user interface with the security system, allows the user to arm (turn on), disarm (turn off), and communicate with the system. How a specific system is armed will depend on how it is used. For example, while IDSs can be armed for continuous operation (24 hours/day), they are usually armed and disarmed according to the work schedule at a specific location so that personnel going about their daily activities do not set off the alarms. In contrast, fire protection systems are typically armed 24 hours a day.

A *control panel* receives information from the sensors and sends it to an appropriate location, such as to a central operations station or to a 24-hour

monitoring facility. Once the alarm signal is received at the central monitoring location, personnel monitoring for alarms can respond (such as by sending security teams to investigate or by dispatching the fire department).

An *annunciator* responds to the detection of an event by emitting a signal. This signal may be visual, audible, electronic, or a combination of these three. For example, fire alarm signals will always be connected to audible annunciators, whereas intrusion alarms may not be.

Alarms can be reported locally, remotely, or both locally and remotely. Local and remotely (centrally) reported alarms are discussed in more detail next.

A *local alarm* emits a signal at the location of the event (typically using a bell or siren). A "local only" alarm emits a signal at the location of the event but does not transmit the alarm signal to any other location (i.e., it does not transmit the alarm to a central monitoring location). Typically, the purpose of a "local only" alarm is to frighten away intruders, and possibly to attract the attention of someone who might notify the proper authorities. Because no signal is sent to a central monitoring location, personnel can only respond to a local alarm if they are in the area and can hear and/or see the alarm signal.

Fire alarm systems must have local alarms, including both audible and visual signals. Most fire alarm signal and response requirements are codified in the National Fire Alarm Code, NFPA 72. NFPA 72 discusses the application, installation, performance, and maintenance of protective signaling systems and their components. In contrast to fire alarms, which require a local signal when fire is detected, many IDSs do not have a local alert device, because monitoring personnel do not wish to inform potential intruders that they have been detected. Instead, these types of systems silently alert monitoring personnel that an intrusion has been detected, thus allowing monitoring personnel to respond.

In contrast to systems that are set up to transmit "local only" alarms when the sensors are triggered, systems can also be set up to transmit signals to a *central location*, such as to a control room or guard post at the utility, or to a police or fire station. Most fire/smoke alarms are set up to signal both at the location of the event and at a fire station or central monitoring station. Many insurance companies require that facilities install certified systems that include alarm communication to a central station. For example, systems certified by the Underwriters Laboratory (UL) require that the alarm be reported to a central monitoring station.

The main differences between alarm systems lie in the types of event detection devices used in different systems. *Intrusion sensors*, for example, consist of two main categories: perimeter sensors and interior (space) sensors. *Perimeter intrusion sensors* are typically applied on fences, doors, walls, windows, and so on, and are designed to detect an intruder before he/

she accesses a protected asset (i.e., perimeter intrusion sensors are used to detect intruders attempting to enter through a door or window). In contrast, *interior intrusion sensors* are designed to detect an intruder who has already accessed the protected asset (i.e., interior intrusion sensors are used to detect intruders once they are already within a protected room or building). These two types of detection devices can be complementary, and they are often used together to enhance security for an asset. For example, a typical intrusion alarm system might employ a perimeter glass-break detector that protects against intruders accessing a room through a window, as well as an ultrasonic interior sensor that detects intruders who have entered into the room without using the window. Table 9.6 lists and describes types of perimeter and interior sensors.

Fire Detection/Fire Alarm Systems consist of different types of fire detection devices and fire alarm systems available. These systems may detect fire, heat, smoke, or a combination of any of these. For example, a typical fire alarm system might consist of heat sensors, which are located throughout a facility and which detect high temperatures or a certain change in temperature over a fixed time period. A different system might be outfitted with both smoke and heat detection devices. A summary of several different types of fire/smoke/heat detection sensors is provided in table 9.7.

Once a sensor in an alarm system detects an event, it must communicate an alarm signal. The two basic types of alarm communication systems are hardwired and wireless. Hardwired systems rely on wire that is run from the control panel to each of the detection devices and annunciators. Wireless systems transmit signals from a transmitter to a receiver through the air—primarily using radio or other waves. Hardwired systems are usually lower-cost, more reliable (they are not affected by terrain or environmental factors), and significantly easier to troubleshoot than are wireless systems. However, a major disadvantage of hardwired systems is that it may not be possible to hardwire all locations (for example, it may be difficult to hardwire remote locations). In addition, running wires to their required locations can be both time consuming and costly. The major advantage to using wireless systems is that they can often be installed in areas where hardwired systems are not feasible. However, wireless components can be much more expensive when compared to hardwired systems. In addition, in the past, it has been difficult to perform self-diagnostics on wireless systems to confirm that they are communicating properly with the controller. Presently, the majority of wireless systems incorporate supervising circuitry, which allows the subscriber to know immediately if there is a problem with the system (such as a broken detection device or a low battery), or if a protected door or window has been left open.

Table 9.6 Perimeter and Interior Sensors

	Description
Type of Perimeter Sensor	
Foil	Foil is a thin, fragile, lead-based metallic tape that is applied to glass windows and doors. The tape is applied to the window or door, and electric wiring connects this tape to a control panel. The tape functions as a conductor and completes the electric circuit with the control panel. When an intruder breaks the door or window, the fragile foil breaks, opening the circuit and triggering an alarm condition.
Magnetic switches (reed switches)	The most widely used perimeter sensor. They are typically used to protect doors, as well as windows that can be opened (windows that cannot be opened are more typically protected by foil alarms).
Glass-break detectors	Placed on glass and sense vibrations in the glass when it is disturbed. The two most common types of glass-break detectors are shock sensors and audio discriminators.
Type of Interior Sensor	
Passive infrared (PIR)	Presently the most popular and cost effective interior sensors. PIR detectors monitor infrared radiation (energy in the form of heat) and detect rapid changes in temperature within a protected area. Because infrared radiation is emitted by all living things, these types of sensors can be very effective.
Quad PIRs	Consist of two dual-element sensors combined in one housing. Each sensor has a separate lens and a separate processing circuitry, which allows each lens to be set up to generate a different protection pattern
Ultrasonic detectors	Emit high frequency sound waves, and sense movement in a protected area by sensing changes in these waves. The sensor emits sound waves that stabilize and set a baseline condition in the area to be protected. Any subsequent movement within the protected area by a would-be intruder will cause a change in these waves, thus creating an alarm condition.
Microwave detectors	Emit ultra-high frequency radio waves, and the detector senses any changes in these waves as they are reflected throughout the protected space. Microwaves can penetrate through walls, and thus a unit placed in one location may be able to protect multiple rooms.
Dual-technology devices	Incorporate two different types of sensor technology (such as PIR and microwave technology) together in one housing. When both technologies sense an intrusion, an alarm is triggered.

Source: USEPA (2005).

Table 9.7 Fire/Smoke/Heat Detection Sensors

Detector Type	*Description*
Thermal detector	Sense when temperatures exceed a set threshold (fixed temperature detectors) or when the rate of change of temperature increases over a fixed time period (rate-of-rise detectors).
Duct detector	Is located within the haring and ventilation ducts of the facility. This sensor detects the presence of smoke within the system's return or supply ducts. A sampling tube can be added to the detector to help span the width of the duct.
Smoke detectors	Sense invisible and/or visible products of combustion. The two principle types of smoke detectors are photoelectric and ionization detectors. The major differences between these devices are described below: • Photoelectric smoke detectors react to visible particles of smoke. These detectors are more sensitive to the cooler smoke with large smoke particles that is typical of smoldering fires. • Ionization smoke detectors are sensitive to the presence of ions produced by the chemical reactions that take place with few smoke particle, such as those typically produced by fast burning/flaming fires.
Multi-sensor detectors	Are a combination of photoelectric and thermal detectors. The photoelectric sensor serves to detect smoldering fires, while the thermal detector senses the eat give off from fast burning/flaming fires.
Carbon monoxide detectors	Are used to indicate the outbreak of fire by sensing the level of carbon monoxide in the air. The detector has an electrochemical cell which senses carbon monoxide, but not some or other products of combustion.
Beam detectors	Are designed to protect large, open spaces such as industrial warehouses. These detectors consist of three parts: the transmitter, which projects a beam of infrared light; the receiver, which registers the light and produces an electrical signal; and the interface, which processes the signal and generates alarm of fault signals. In the event of a fire, smoke particles obstruct the beam of light. Once a preset threshold is exceeded, the detector will go into alarm.
Flame detectors	Sense either ultraviolet (UV) or infrared (IR) radiation emitted by a fire.
Air-sampling detectors	Actively and continuously sample the air from a protected space and are able to sense the precombustion stages of incipient fire.

Source: USEPA (2005).

Biometric Security Systems

Biometrics involves measuring the unique physical characteristics or traits of the human body. Any aspect of the body that is measurably different from person to person—for example, fingerprints or eye characteristics—can serve as a unique biometric identifier for that individual. Biometric systems recognizing fingerprints, palm shape, eyes, face, voice, and signature comprise the bulk of the current biometric systems that recognize other biological features do exist.

Biometric security systems use biometric technology combined with some type of locking mechanism to control access to specific assets. In order to access an asset controlled by a biometric security system, an individual's biometric trait must be matched with an existing profile stored in a database. If there is a match between the two, the locking mechanisms (which could be a physical lock, such as at a doorway, an electronic lock, such as at a computer terminal or some other type of lock) is disengaged, and the individual is given access to the asset.

A biometric security system is typically comprised of the following components:

- A sensor, which measures/records a biometric characteristic or trait
- A control panel, which serves as the connection point between various system components. The control panel communicates information back and forth between the sensor and the host computer, and controls access to the asset by engaging or disengaging the system lock based on internal logic and information from the host computer
- A host computer, which processes and stores the biometric trait in a database
- Specialized software, which compares an individual image taken by the sensor with a stored profile or profiles
- A locking mechanism which is controlled by the biometric system
- A power source to power the system.

Biometric Hand and Finger Geometry Recognition

Hand and finger geometry recognition is the process of identifying an individual through the unique "geometry" (shape, thickness, length, width, etc.) of that individual's hand or fingers. Hand geometry recognition has been employed since the early 1980s and is among the most widely used biometric technologies for controlling access to important assets. It is easy to install and use, and is appropriate for use in any location requiring use of two-finger,

highly-accurate, non-intrusion biometric security. For example, it is currently used in numerous workplaces, daycare facilities, hospitals, universities, airports, refineries, and power plants.

A newer option within hand geometry recognition technology is finger geometry recognition (not to be confused with fingerprint recognition). Finger geometry recognition relies on the same scanning methods and technologies as does hand geometry recognition, but the scanner only scans two of the user's fingers, as opposed to his entire hand. Finger geometry recognition has been in commercial use since the mid-1990s and is used mainly in time and attendance applications (i.e., to track when individuals have entered and exited a location). To date the only large-scale commercial use of two-finger geometry for controlling access is at Disney World, where season pass holders use the geometry of their index and middle finger to gain access to the facilities.

To use a hand or finger geometry unit, an individual presents his or her hand or fingers to the biometric unit for scanning. The scanner consists of a Charged Coupled Device (CCD), which is essentially a high resolution digital camera; a reflective platen on which the hand is placed; and a mirror or mirrors that help capture different angles of the hand or fingers. The camera scans individual geometric characteristics of the hand or fingers by taking multiple images while the user's hand rests on the reflective platen. The camera also captures depth, or three-dimensional information, through light reflected from the mirrors and the reflective platen. This live image is then compared to a template that was previously established for that individual when they were enrolled in the system. If the live scan of the individual matches the stored template, the individual is verified, and is given access to that asset. Typically, verification takes about two seconds. In access control applications, the scanner is usually connected to some sort of electronic lock, which unlocks the door, turnstile, or other entry barrier when the user is verified. The user can then proceed through the entrance. In time and attendance applications, the time that an individual checks in an out of a location is stored for later use.

As discussed above, hand and finger geometry recognition systems can be used in several different types of applications, including access control and time and attendance tracking. While time and attendance tracking can be used for security, it is primarily used for operations and payroll purposes (i.e., clocking in and clocking out). In contrast, access control applications are more likely to be security-related. Biometric systems are widely used for access control, and can be used on various types of assets, including entryways, computers, vehicles, etc. However, because of their size, hand/finger recognition systems are primarily used in entryway access control applications.

Biometric Overview-Iris Recognition

The iris, which is the colored or pigmented area of the eye surrounded by the sclera (the white portion of the eye), is a muscular membrane that controls the amount of light entering the eye by contracting or expanding the pupil (the dark center of the eye). The dense, unique patterns of connective tissue in the human iris were first noted in 1936, but it was not until 1994, when algorithms for iris recognition were created and patented, that commercial applications using biometric iris recognition began to be used extensively. There are now two vendors producing iris recognition technology: both the original developer of these algorithms, as well as a second company, which has developed and patented a different set of algorithms for iris recognition.

The iris is an ideal characteristic for identifying individuals because it is formed *in utero*, and its unique patterns stabilize around eight months after birth. No two irises are alike; neither an individual's right or left irises, nor the irises of identical twins. The iris is protected by the cornea (the clear covering over the eye), and therefore it is not subject to the aging or physical changes (and potential variation) that are common to some other biometric measures, such as the hand, fingerprints, and the face. Although some limited changes can occur naturally over time, these changes generally occur in the iris' melanin and therefore affect only the eye's color, and not its unique patterns (in addition, because iris scanning uses only black and white images, color changes would not affect the scan anyway). Thus, barring specific injuries or certain rate surgeries directly affecting the iris, the iris' unique patterns remain relatively unchanged over an individual's lifetime.

Iris recognition systems employ a monochromatic or black and white video camera that uses both visible and near infrared light to take video of an individual's iris. Video is used rather than still photography as an extra security procedure. The video is used to confirm the normal continuous fluctuations of the pupil as the eye focuses, which ensures that the scan is of a living human being, and not a photograph or some other attempted hoax. A high resolution image of the iris is then captured or extracted from the video, using a device often referred to as a "frame grabber." The unique characteristics identified in this image are then converted into a numeric code, which is stored as a template for that user.

Card Identification/Access/Tracking Systems

A card reader system is a type of electronic identification system that is used to identify a card and then perform an action associated with that card. Depending on the system, the card may identify where a person is or where they were at a certain time; or it may authorize another action, such as

disengaging a lock. For example, a security guard may use his card at card readers located throughout a facility to indicate that he has checked a certain location at a certain time. The reader will store the information and/or send it to a central location, where it can be checked later to ensure that the guard has patrolled the area. Other card reader systems can be associated with a lock, so that the cardholder must have their card read and accepted by the reader before the lock disengages.

A complete card reader system typically consists of the following components:

- Access cards that are carried by the user
- Card readers, which read the card signals and send the information to control units
- Control units, which control the response of the card reader to the card
- A power source

A "card" may be a typical card or another type of device, such as a key fob or wand. These cards store electronic information, which can range from a simple code (i.e., the alphanumeric code on a Proximity card) to individualized personal data (i.e., biometric data on a Smartcard). The card reader reads the information stored on the card and sends it to the control unit, which determines the appropriate action to take when a card is presented. For example in a card access system, the control unit compares the information on the card vs. stored access authorization information to determine if the card holder is authorized to proceed through the door. If the information stored in the card reader system indicates that the key is authorized to allow entrance through the doorway, the system disengages the lock and the key holder can proceed through the door.

There are many different types of card reader systems on the market. The primary differences between card reader systems are different in the way that data is encoded on the cards and in the way these data are transferred between the card and the card reader, and in the types of applications for which they are best suited. However, all card systems are similar in the way that the card reader and control unit interact to respond to the card. There are several types of technologies available for card reader systems. These include the following:

- Proximity
- Wiegand
- Smartcard
- Magnetic Stripe
- Bar Code
- Infrared

- Barium Ferrite
- Hollerith
- Mixed Technologies

Table 9.8 summarizes various aspects of card reader technologies. The determination for the level of security rate (low, moderate, or high) based on the level of technology a given card reader system has and how simple it is to

Table 9.8 Card Reader Technology

Types of Card Readers	*Technology*	*Life Cycle*	*Vulnerability*	*Level of Security*
Proximity	Embedded radio frequency circuits encoded with unique information	Long	Virtually none	Moderate-high
Wiegand	Short lengths of small-diameter, special alloy wire with unique magnetic properties	Long	Low susceptibility to damage; high durability due to embedded wires	Moderate-expensive
Magnetic Stripe	Electromagnetic charges to encode information on a piece of tape attached to back of card	Moderate	Moderately susceptible to damage due to frequency of use	Low-Moderate
Bar Code	Series of narrow and wide bars and spaces	Short	High; easily damaged	Low
Hollerith	Holes punched in a plastic or paper card and read optically	Short	High; easily damaged from frequent use	Low
Infrared	An encoded shadow pattern within the card, read using an infrared scanner	Moderate	IR scanners are optical and thus, vulnerable to contamination	High
Barium Ferrite	Uses small bits of magnetized barium ferrite, placed inside a plastic card. The polarity and location of the "spots" determines the coding	Moderate	Low Susceptibility to damage; durable since spots are embedded in the material	Moderate-High
Smartcards	Patterns or series of narrow and wide bars and spaces	Short	High susceptibility to damage, low durability	Highest

Source: USEPA (2005).

duplicate that technology, and thus bypass the security. Vulnerability ratings were based on whether the card reader can be damaged easily due to frequent use or difficult working conditions (i.e., weather conditions if the reader is located outside). Often this is influenced by the number of moving parts in the system—the more moving parts, then greater the system's potential susceptibility to damage. The life cycle rating is based on the durability of a given card reader system over its entire operational period. Systems requiring frequent physical contact between the reader and the card often have a shorter life cycle due to the wear and tear to which the equipment is exposed. For many card reader systems, the vulnerability rating and life cycle ratings have a reciprocal relationship. For instance, if a given system has a high vulnerability rating it will almost always have a shorter life cycle.

Card reader technology can be implemented for facilities of any size and with any number of users. However, because individual systems vary in the complexity of their technology and in the level of security they can provide to a facility, individual users must determine the appropriate system for their needs. Some important features to consider when selecting a card reader system include the following:

- The technological sophistication and security level of the card system
- The size and security needs of the facility
- The frequency with which the card system will be used. For systems that will experience a high frequency of use it is important to consider a system that has a longer life cycle and lower vulnerability rating, thus making it more cost effective to implement
- The conditions in which the system will be used (i.e., will it be used on the interior or exterior of buildings, does it require light or humidity controls, etc.). Most card reader systems can operate under normal environmental conditions, and therefore this would be a mitigating factor only in extreme conditions
- System costs

Exterior Intrusion Sensors

An *exterior intrusion sensor* is a detection device that is used in an outdoor environment to detect intrusions into a protected area. These devices are designed to detect an intruder, and then communicate an alarm signal to an alarm system. The alarm system can respond to the intrusion in many different ways, such as by triggering an audible or visual alarm signal, or by sending an electronic signal to a central monitoring location that notifies security personnel of the intrusion.

Intrusion sensor can be used to protect many kinds of assets. Intrusion sensors that protect physical space are classified according to whether they

protect indoor, or "interior" space (i.e., an entire building or room within a building), or outdoor, or "exterior" space (i.e., a fence line or perimeter). Interior intrusion sensors are designed to protect the interior space of a facility by detecting an intruder who is attempting to enter, or who has already entered a room or building. In contrast, exterior intrusion sensors are designed to detect an intrusion into a protected outdoor/exterior area. Exterior protected areas are typically arranged as zones or exclusion areas placed so that the intruder is detected early in the intrusion attempt before the intruder can gain access to more valuable assets (e.g., into a building located within the protected area). Early detection creates additional time for security forces to respond to the alarm.

Exterior intrusion sensors are classified according to how the sensor detects the intrusion within the protected area. The three classes of exterior sensor technology include:

- Buried-line sensors
- Fence-associated sensors
- Freestanding sensors

Buried Line Sensors

As the name suggests, buried line sensors are sensors that are buried underground, and are designed to detect disturbances within the ground—such as disturbances caused by an intruder digging, crawling, walking, or running on the monitored ground. Because they sense ground disturbances, these types of sensors are able to detect intruder activity both on the surface and below ground. Individual types of exterior buried line sensors function in different ways: by detecting motion, pressure, or vibrations within the protected ground or by detecting changes in some type of field (e.g., magnetic field) that the sensors generate within the protected ground. Specific types of buried line sensors include *pressure or seismic* sensors, *magnetic field* sensors, *ported coaxial cables*, and *fiber-optic cables*. The four types of sensors are described in more detail below. Table 9.9 presents the distinctions between the four types of buried sensors.

- *Buried line pressure or seismic sensors* detect physical disturbances to the ground—such as vibrations or soil compression—caused by intruders walking, driving, digging, or otherwise physically contacting the protected ground. These sensors detect disturbances from all directions and, therefore, can protect an area radially outward from their location; however, because detection may weaken as a function of distance from the disturbance, choosing the correct burial depth from the design area will be

Table 9.9 Types of Buried Sensors

Type	*Description*
Pressure or Seismic	Responds to disturbances in the soil.
Magnetic Field	Responds to a change in the local magnetic field caused by the movement of nearby metallic material.
Ported Coaxial Cables	Responds to motion of a material with a high dielectric constant or high conductivity near the cables.
Fiber-Optic Cables	Responds to a change in the shape of the fiber that can be sensed using sophisticated sensors and computer signal processing.

Source: Adapted from M.L. Garcia (2001).

crucial. In general, sensors buried at a shallow depth protect a relatively small area but have a high probability of detecting intrusion within that area, while sensors buried at a deeper depth protect a wider area but have a lower probability of detecting intrusion into that area.

- *Buried line magnetic field sensors* detect changes in a local magnetic field that are caused by the moment of metallic objects within that field. This type of sensor can detect ferric metal objects worn or carried by an intruder entering a protected area on foot as well as vehicles being driven into the protected area.
- *Buried line ported coaxial cable sensors* detect the motion of any object (i.e., human body, metal, etc.) possessing high conductivity and located within close proximity to the cables. An intruder entering into the protected space creates an active disturbance in the electric field, thereby triggering an alarm condition.
- *Buried line fiber-optic cable sensors* detect changes in the attenuation of light signals transmitted within the cable. When the soil around the cable is compressed, the cable is distorted, and the light signal transmitted through the cable changes, initiating an alarm. This type of sensor is easy to install because it can be buried at a shallow burial depth (only a few centimeters) and still be effective.

Fence-Associated Sensors

Fence-associated sensors are either attached to an existing fence or are installed in such a way as to create a fence. These sensors detect disturbances to the fence—such as those caused by an intruder attempting to climb the fence or by an intruder attempting to cut or lift the fence fabric. Exterior fence-associated sensors include fence-disturbance sensors, taut-wire sensor fences, and electric field or capacitance sensors. Details on each of these sensor types are provided next.

- *Fence-disturbance sensors* detect the motion or vibration of a fence, such as that caused by an intruder attempting to climb or cut through the fence. In

general, fence-disturbance sensors are used on chain link fences or on other fence types where a moveable fence fabric is hung between fence posts.

- *Taut-wire sensor fences* are similar to fence-disturbance sensors except that instead of attaching the sensors to a loose fence fabric, the sensors are attached to a wire that is stretched tightly across the fence. These types of systems are designed to detect changes in the tension of the wire rather than vibrations in the fence fabric. Taut-wire sensor fences can be installed over existing fences, or as stand-alone fence systems.
- *Electric field or capacitance sensors* detect changes in capacitive coupling between wires that are attached to, but electrically isolated from, the fence. As opposed to other fence-associated intrusion sensors, both electric field and capacitance sensors generate an electric field that radiates out from the fence line, resulting in an expanded zone of protection relative to other fence-associated sensors, and allowing the sensor to detect an intruders' presence before they arrive at the fence line. Note: proper spacing is necessary during installation of the electric field sensor to detect a would-be intruder from slipping between largely spaced wires.

Freestanding Sensors

These sensors, which include active infrared, passive infrared, bistatic microwave, monostatic microwave, dual technology, and video motion detection (VMD) sensors, consist of individual sensor units or components that can be set up in a variety of configurations to meet a user's needs. They are installed above ground, and depending on how they are oriented relative to each other, they can be used to establish a protected perimeter or a protected space. More details on each of these sensor types are provided next.

- *Active infrared sensors* transmit infrared energy into the protected space, and monitor for changes in this energy caused by intruders entering that space. In a typical application, an infrared light beam is transmitted from a transmitter unit to a receiver unit. If an intruder crosses the beam, the beam is blocked, and the receiver unit detects a change in the amount of light received, triggering an alarm. Different sensors can see single- and multiple-beam arrays. Single-beam infrared sensors transmit a single infrared beam. In contrast, multiple-beam infrared sensors transmit two or more beams parallel to each other. This multiple-beam sensor arrangement creates an infrared "fence."
- *Passive infrared (PIR) sensors* monitor the ambient infrared energy in a protected area, and evaluate changes in that ambient energy that may be caused by intruders moving through the protected area. Detection ranges can exceed 100 yards on cold days with size and distance limitations

dependent upon the background temperature. PIR sensors generate a non-uniform detection pattern (or "curtain") that has areas (or "zones") of more sensitivity and areas of less sensitivity. The specific shape of the protected area is determined by the detector's lenses. The general shape common too many detection patterns is a series of long "fingers" emanating from the PIR and spreading in various directions. When intruders enter the detection area, the PIR sensor detects differences in temperature due to the intruder's body heat, and triggers an alarm. While the PIR leaves unprotected areas between its fingers, an intruder would be detected if he passed from a non-protected area to a protected area.

- *Microwave sensors* detect changes in received energy generated by the motion of an intruder entering into a protected area. Monostatic microwave sensors incorporate transmitter and a receiver in one unit, while bistatic sensors separate the transmitter and the receiver into different units. Monostatic sensors are limited to a coverage area of 400 feet, while bistatic sensors can cover an area up to 1,500 feet. For bistatic sensors, a zone of no detection exists in the first few feet in front of the antennas. This distance from the antennas to the point at which the intruder is first detected is known as the offset distance. Due to this offset distance, antennas must be configured so that they overlap one another (as opposed to being adjacent to each other), thereby creating long perimeters with a continuous line of detection.
- *Dual-technology sensors* consist of two different sensor technologies incorporated together into one sensor unit. For example, a dual-technology sensor could consist of a passive infrared detector and a monostatic microwave sensor integrated into the same sensor unit.
- *Video motion detection (VMD) sensors* monitor video images from a protected area for changes in the images. Video cameras are used to detect unauthorized intrusion into the protected area by comparing the most recent image against a previously established one. Cameras can be installed on towers or other tall structures so that they can monitor a large area.

Fences

A fence is a physical barrier that can be set up around the perimeter of an asset. Fences often consist of individual pieces (such as individual pickets in a wooden fence, or individual sections of a wrought iron fence) that are fastened together. Individual sections of the fence are fastened together using posts, which are sunk into the ground to provide stability and strength for the sections of the fence hung between them. Gates are installed between individual sections of the fence to allow access inside the fenced area.

Many fences are used as decorative architectural features to separate physical spaces for each other. They may also be used to physically mark the location of a boundary (such as a fence installed along a properly line). However, a fence can also serve as an effective means for physically delaying intruders from gaining access to a financial service sector asset. For example, many utilities install fences around their primary facilities, around remote pump stations, or around hazardous petrochemical materials storage areas or sensitive areas within a facility. Access to the area can be controlled through security at gates or doors through the fence (for example, by posting a guard at the gate or by locking it). In order to gain access to the asset, unauthorized persons could either have to go around or through the fence.

Fences are often compared with walls when determining the appropriate system for perimeter security. While both fences and walls can provide adequate perimeter security, fences are often easier and less expensive to install than walls. However, they do not usually provide the same physical strength that walls do. In addition, many types of fences have gaps between the individual pieces that make up the fence (i.e., the spaces between chain links in a chain link fence or the space between pickets in a picket fence). Thus, many types of fences allow the interior of the fenced area to be seen. This may allow intruders to gather important information about the locations or defenses of vulnerable areas within the facility.

Important security attributes of a fence include the height to which it can be constructed, the strength of the material comprising the fence, the method and strength of attaching the individual sections of the fence together at the posts and the fence's ability to restrict the view of the assets inside the fence. Additional considerations should include the ease of installing the fence and the ease of removing and reusing sections of the fence. Table 9.10 provides a comparison of the important security and usability features of various fence types.

Some fences can include additional measures to delay, or even detect, potential intruders. Such measures may include the addition of barbed wire, razor wire, or other deterrents at the top of the fence. Barbed wire is sometimes employed at the base of fences as well. This can impede a would-be

Table 9.10 Comparison of Different Fence Types

Specifications	*Chain Link*	*Iron*	*Wire (Wirewall)*	*Wood*
Height limitations	12′	12′	12′	8′
Strength	Medium	High	High	Low
Installation Requirements	Low	High	High	Low
Ability to Remove/Reuse	Low	High	Low	High
Ability to Replace/Repair	Medium	High	Low	High

Source: USEPA (2005).

intruder's progress in even reaching the fence. Fences may also be fitted with security cameras to provide visual surveillance of the perimeter. Finally, some facilities have installed motion sensors along their fences to detect movement on the fence. Several manufacturers have combined these multiple perimeter security features into one product and offer alarms, and other security features.

The correct implementation of a fence can make it a much more effective security measure. Security experts recommend the following when a facility constructs a fence:

- The fence should be at least 7 to 9 feet high.
- Any outriggers, such as barbed wire, that are affixed on top of the fence should be angled out and away from the facility, and not in toward the facility. This will make climbing the fence more difficult, and will prevent ladders from being placed against the fence.
- Other types of hardware can increase the security of the fence. This can include installing concertina wire along the fence (this can be done in front of the fence or at the top of the fence), or adding intrusion sensors, camera, or other hardware to the fence.
- All undergrowth should be cleared for several feet (typically 6 feet) on both sides of the fence. This will allow for a clearer view of the fence by any patrols in the area.
- Any trees with limbs or branches hanging over the fence should be trimmed so that intruders cannot use them to go over the fence. Also, it should be noted that fallen trees can damage fences, and so management of trees around the fence can be important. This can be especially important in areas where fence goes through a remote area.
- Fences that do not block the view from outside the fence to inside the fence allow patrols to see inside the fence without having to enter the facility.
- "No Trespassing" signs posted along fence can be a valuable tool in prosecuting any intruders who claim that the fence was broken and that they did not enter through the fence illegally. Adding signs that highlight the local ordinances against trespassing can further persuade simple troublemakers for illegally jumping/climbing the fence. Electrical substation and other electrical component installations should have clearly visible signage warning of High Voltage and the dangers of Electrical Shock.

Films for Glass Shatter Protection

Many financial services sector entities have numerous windows on the outside of buildings, in doors, and in interior offices. In addition, many facilities have glass doors or other glass structures, such as glass walls or display cases. These

glass objects are potentially vulnerable to shattering when heavy objects are thrown or launched at them, when explosions occur near them, or when there are high winds (for exterior glass). If the glass is shattered, intruders may potentially enter an area. In addition, shattered glass projected into a room from an explosion or from an object being thrown through a door or window can injure and potentially incapacitate personnel in the room. Materials that prevent glass from shattering can help to maintain the integrity of the door, window, or other glass object, and can delay an intruder from gaining access. These materials can also prevent flying glass and thus reduce potential injuries.

Materials designed to prevent glass from shattering include specialized films and coatings. These materials can be applied to existing glass objects to improve their strength and their ability to resist shattering. The films have been tested against many scenarios that could result in glass breakage, including penetration by blunt objects, bullets, high winds, and simulated explosions. Thus, the films are tested against simulated weather scenarios (which could include the high winds themselves and the force of objects blown into the glass), as well as more criminal/terrorist scenarios where the glass is subject to explosives or bullets. Many vendors provide information on the results of these types of tests, and thus potential users can compare different product lines to determine which products best suit their needs.

The primary attributes of films for shatter protection are:

- The materials from which the film is made
- The adhesive that bonds the film to the glass surface
- The thickness of the film

Standard glass safety films are designed from high strength polyester. Polyester provides both strength and elasticity, which is important in absorbing the impact of an object, spreading the force of the impact over the entire film, and resisting tearing. The polyester is also designed to be resistant to scratching, which can result when films are cleaned with abrasives or other industrial cleaners.

The bonding adhesive is important in ensuring that the film does not tear away from the glass surface. This can be especially important when the glass is broken, so that the film does not peel off the glass and allow it to shatter. In addition, films applied to exterior windows can be subject to high concentrations of UV light, which can break down bonding materials.

Film thickness is measured in gauge or mils. According to test results reported by several manufacturers, film thickness appears to affect resistance to penetration/tearing, with thicker films being more resistant to penetration and tearing. However, the appreciation of a thicker film did not decrease glass fragmentation.

Many manufacturers offer films in different thicknesses. The "standard" film is usually one 4 mil layer; thicker films are typically composed of several layers of the standard 4 mil sheet. However, newer technologies have allowed the polyester to be "microlayered" to produce a stronger film without significantly increasing its thickness. In this microlayering process, each laminate film is composed of multiple micro-thin layers of polyester woven together an alternating angles. This provides increased strength for the film, while maintaining the flexibility and thin profile of one film layer.

As described above, many vendors test their products in various scenarios that would lead to glass shattering, including simulated bomb blasts and simulation of the glass being struck by wind-blown debris. Some manufacturers refer to the Government Services Administration standard for bomb blasts, which require resistance to tearing for a 4 PSI blast. Other manufacturers use other measures and test for resistance to tearing. Many of these tests are not "standard," in that no standard testing or reporting methods have been adopted by any of the accepted standards-setting institutions. However, many of the vendors publish the procedure and the results of these tests on their websites, and this may allow users to evaluate the protectiveness of these films. For example, several vendors evaluate the "protectiveness" of their films and the "hazard" resulting from blasts near windows with and without protective films. Protectiveness is usually evaluated based on the percentage of glass ejected from the window, and the height at which that ejected glass travels during the blast (for example, if the blasted glass tends to project upward in to a room—potentially toward people's faces—it is a higher hazard than if it is blown downward into the room toward people's feet). There are some standard measures of glass breakage. For example, several vendors indicated that their products exceed the American Society for Testing and Materials (ASTM) standard 64Z-95 "Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings." Vendors often compare the results of some sort of penetration or force test, ballistic tests, or simulated explosions with unprotected glass versus glass onto which their films have been applied. Results generally show that applying films to the glass surfaces reduces breakage/penetration of the glass and can reduce the amount and direction of glass ejected from the frame. This in turn reduces the hazard from flying glass.

In addition to these types of tests, many vendors conduct standard physical tests on their products, such as tests for tensile strength and peel strength. Tensile strength indicates the strength per area of material, while the peel strength indicates the force it would take to peel the product from the glass surface. Several vendors indicate that their products exceed American National Standards Institute (ANSI) standard Z97.1 for tensile strength and adhesion.

Vendors typically have a warranty against peeling or other forms of deterioration of their products. However, the warranty requires that the films be installed by manufacturer-certified technicians to ensure that they are applied correctly and therefore that the warranty is in effect. Warranties from different manufacturers may vary. Some may cover the cost of replacing the material only, while others include material plus installation. Because installation costs are significantly greater than material costs, different warranties may represent large difference in potential costs.

Fire Hydrant Locks

Fire hydrants are installed at strategic locations throughout a community's water distribution system to supply water for firefighting. However, because there are many hydrants in a system and they are often located in residential neighborhoods, commercial/industrial districts, and other areas where they cannot be easily observed and/or guarded, they are potentially vulnerable to unauthorized access. Many municipalities, states, and EPA Regions have recognized this potential vulnerability and have instituted programs to lock hydrants. For example, EPA Region 1 has included locking hydrants as number 7 on its "Drinking Water Security and Emergency Preparedness" Top Ten List for small groundwater suppliers.

A "hydrant lock" is a physical security device designed to prevent unauthorized access to the water supply through a hydrant. They can also ensue water and water pressure availability to fire fighters and prevent water theft and associated lost water revenue. These locks have been successfully used in numerous municipalities and in various climates and weather conditions.

Fire hydrant locks are basically steel covers or caps that are locked in place over the operating nut of a fire hydrant. The lock prevents unauthorized persons from accessing the operating nut and opening the fire hydrant valve. The lock also makes it more difficult to remove the bolts from the hydrant and access the system that way. Finally, hydrant locks shield the valve from being broken off. Should a vandal attempt to breach the hydrant lock by force and succeed in breaking the hydrant lock, the vandal will only succeed in bending the operating valve. If the hydrant's operating valve is bent, the hydrant will not be operational, but the water asset remains protected and inaccessible to vandals. However, the entire hydrant will need to be replaced.

Hydrant locks are designed so that the hydrants can be operated by special "key wrenches" without removing the lock. These specialized wrenches are generally distributed to the fire department, public works department, and other authorized persons so that they can access the hydrants as needed. An inventory of wrenches and their serial numbers is generally kept by a municipality so that the location of all wrenches is known. These operating key wrenches may only be purchased by registered lock owners.

The most important features of hydrant are their strength and the security of their locking systems. The locks must be strong so that they cannot be broken off. Hydrant locks are constructed from stainless or alloyed steel. Stainless steel locks are stronger and are ideal for all climates; however, they are more expensive than alloy locks. The locking mechanisms for each fire hydrant locking system ensure that the hydrant can only be operated by authorized personnel who have the specialized key to work the hydrant.

Ladder Access Control

Financial services sector facilities have a number of assets that are raised above ground level, including electrical substations, transmitting stations, raised conduit systems, and roof access points into buildings. In addition, communications equipment, antennas, or other electronic devices may be located on the top of these raised assets. Typically, these assets are reached by ladders that are permanently anchored to the asset. Controlling access to these raised assets by controlling access to the ladder can increase security at a financial services sector facility.

A typical ladder access control system consists of some type of cover that is locked or secured over the ladder. The cover can be a casing that surrounds most of the ladder, or a door or shield that covers only part of the ladder. In either case, several rungs of the ladder (the number of rungs depends on the size of the cover) are made inaccessible by the cover, and these rungs can only be accessed by opening or removing the cover. The cover is locked so that only authorized personnel can open or remove it and use the ladder. Ladder access controls are usually installed at several feet above ground level, and they usually extend several feet up the ladder so that they cannot be circumvented by someone accessing the ladder above the control system.

The important features of ladder access control are the size and strength of the cover and its ability to lock or otherwise be secured from unauthorized access.

The covers are constructed from aluminum or some type of steel. This should provide adequate protection from being pierced or cut through. The metals are corrosion resistant so that they will not corrode or become fragile from extreme weather conditions in outdoor applications. The bolts used to install each of these systems are galvanized steel. In addition, the bolts for each cover are installed on the inside of the unit so they cannot be removed from the outside.

Locks

A lock is a type of physical security device that can be used to delay or prevent a door, a gate, a window, a manhole, a filing cabinet drawer, or some other

physical feature from being opened, moved, or operated. Locks typically operate by connecting two pieces together—such as by connecting a door to a door jamb or a manhole to its casement. Every lock has two modes—engaged (or "locked"), and disengaged (or "opened"). When a lock is disengaged, the asset on which the lock is installed can be accessed by anyone, but when the lock is engaged, only access to the locked asset.

Before discussing locks and their applicability it is important to discuss *key control*. Based on our experience, many financial services sector facilities (and others) have no idea how many keys for various site/equipment locks have been issued to employees over the years. Many facilities simply issue keys to employees at hiring with no accountability for the keys upon the employee's departure. Needless to say this is not good security policy. You can have the best made locks available installed throughout your facilities but if you do not have proper key control, you do not have proper security.

Locks are excellent security features because they have been designed to function in many ways and to work on many different types of assets. Locks can also provide different levels of security depending on how they are designed and implemented. The security provided by a lock is dependent on several factors, including its ability to withstand physical damage (i.e., can it be cut off, broken, or otherwise physically disabled) as well as its requirements for supervision or operation (i.e., combinations may need to be changed frequently so that they are not compromised and the locks remain secure). While there is no single definition of the "security" of a lock, locks are often described as minimum, medium, or maximum security. Minimum security locks are those that can be easily disengaged (or "picked") without the correct key or code, or those that can be disabled easily (such as small padlocks that can be cut with bolt cutters). Higher security locks are more complex and thus are more difficult to pick, or are sturdier and more resistant to physical damage.

Many locks such as many door locks only need to be unlocked from one side. For example, most door locks need a key to be unlocked only from the outside. A person opens such devices, called single-cylinder locks, from the inside by pushing a button or by turning a knob or handle. Double-cylinder locks require a key to be locked or unlocked from both sides.

Manholes

Manholes are found at some financial services sector sites. Manholes are designed to provide access to the underground utilities, meter vaults, pumping rooms, and so on, and therefore are potential entry points to a system. Because many utilities run under other infrastructure (roads, buildings), manholes also provide potential access points to critical infrastructure. In

addition, because the portion of the system to which manholes provide entry is primarily located underground, access to a system through a manhole increases the chance that an intruder will not be seen. Therefore, protecting manholes can be a critical component of guarding an entire sector site and a surrounding community.

There are multiple methods for protecting manholes, including preventing unauthorized personnel from physically accessing the manhole, and detecting attempts at unauthorized access to the manhole.

A *manhole intrusion sensor* is a physical security device designed to detect unauthorized access to the facility through a manhole. Monitoring a manhole that provides access to a facility or processing system can mitigate two distinct types of threats. First, monitoring a manhole may detect access of unauthorized personnel to chemical systems or assets through the manhole. Second, monitoring manholes may also allow the detection of intruders attempting to place explosive or other destructive (WMD) devices into the system.

Several different technologies have been used to develop manhole intrusion sensors, including mechanical systems, magnetic systems, and fiber-optic and infrared sensors. Some of these intrusion sensors have been specifically designed for manholes, while others consist of standard, off-the-shelf intrusion sensors that have been implemented in a system specifically designed for application in a manhole.

A *manhole lock* is a physical security device designed to delay unauthorized access to the financial services sector facility or system through a manhole.

Security for Doorways—Side-Hinged Doors

Doorways are the main access points to a facility or to rooms within a building. They are used on the exterior or in the interior of buildings to provide privacy and security for the areas behind them. Different types of doorway security systems may be installed in different doorways depending on the needs or requirements of the buildings or rooms. For example, exterior doorways tend to have heavier doors to withstand the elements and to provide some security to the entrance of the building. Interior doorways in office areas may have lighter doors that may be primarily designed to provide privacy rather than security. Therefore, these doors may be made of glass or lightweight wood. Doorways in industrial areas may have sturdier doors than do other interior doorways and may be designed to provide protection or security for areas behind the doorway. For example, fireproof doors may be

installed in chemical storage areas or in other areas where there is a danger of fire.

Because they are the main entries into a facility or a room, doorways are often prime targets for unauthorized entry into a facility or an asset. Therefore, securing doorways may be a major step in providing security at a facility.

A doorway includes four main components:

- The door, which blocks the entrance. The primary threat to the actual door is breaking or piercing through the door. Therefore, the primary security features of doors are their strength and resistance to various physical threats, such as fire or explosions.
- The door frame, which connects the door to the wall. The primary threat to a door frame is that the door can be pried away from the frame. Therefore, the primary security feature of a door frame is its resistance to prying.
- The hinges, which connect the door to the door frame. The primary threat to door hinges is that they can be removed or broken, which will allow intruders to remove the entire door. Therefore, security hinges are designed to be resistant to breaking. They may also be designed to minimize the threat of removal from the door.
- The lock, which connects the door to the door frame. Use of the lock is controlled through various security features, such as keys, combinations, etc., such that only authorized personnel can open the lock and go through the door. Locks may also incorporate other security features, such as software or other systems to track overall use of the door or to track individuals using the door, etc.

Each of these components is integral in providing security for a doorway, and upgrading the security of only one of these components while leaving the other components unprotected may not increase the overall security of the doorway. For example, many facilities upgrade door locks as a basic step in increasing the security of a facility. However, if the facilities do not also focus on increasing security for the door hinges or the door frame, the door may remain vulnerable to being removed from its frame, thereby defeating the increased security of the door lock.

The primary attribute for the security of a door is its strength. Many security doors are 4–20 gauge hollow metal doors consisting of steel plates over a hollow cavity reinforced with steel stiffeners to give the door extra stiffness and rigidity. This increases resistance to blunt force used to try to

penetrate through the door. The space between the stiffeners may be filled with specialized materials to provide fire-, blast-, or bullet resistance to the door.

The Windows and Doors Manufacturers Association have developed a series of performance attributes for doors. These include the following:

- Structural resistance
- Forced entry resistance
- Hinge-style screw resistance
- Split resistance
- Hinge resistance
- Security rating
- Fire resistance
- Bullet resistance
- Blast resistance

The first five bullets provide information on a door's resistance to standard physical breaking and prying attacks. These tests are used to evaluate the strength of the door and the resistance of the hinges and the frame in a standardized way. For example, the Rack Load Test simulates a prying attack on a corner of the door. A test panel is restrained at one end, and a third corner is supported. Loads are applied and measured at the fourth corner. The Door Impact Test simulates a battering attack on a door and frame using impacts of 200-foot pounds by a steel pendulum. The door must remain fully operable after the test. It should be noted that door glazing is also rated for resistance to shattering, and so on. Manufacturers will be able to provide security ratings for these features of a door as well.

Door frames are an integral part of doorway security because they anchor the door to the wall. Door frames are typically constructed from wood or steel, and they are installed such that they extend for several inches over the doorway that has been cut into the wall. For added security, frames can be designed to have varying degrees of overlap with, or wrapping over, the underlying wall. This can make prying the frame from the wall more difficult. A frame formed from a continuous piece of metal (as opposed to a frame constructed from individual metal pieces) will prevent prying between pieces of the frame.

Many security doors can be retrofit into existing frames; however, many security door installations including replacing the door frame as well as the door itself. For example, bullet resistance per UL 752 requires resistance of the door and frame assembly, and thus replacing the door only would not meet UL 752 requirements.

Security for Vents

Vents are installed in some aboveground financial services sector storage areas to allow safe venting of off-gases. Every vent consists of an open air connection between the storage container and the outside environment. Improving vent security by making the vents tamper-resistant or by adding other security features, such as security screens or security covers, can enhance the security of the entire system.

Many municipalities already have specifications for vent security at their local industrial assets. These specifications typically include the following requirements:

- Vent openings are to be angled down or shielded to minimize the entrance of surface and/or rainwater into the vent through the opening
- Vent designs are to include features to exclude insects, birds, animals, and dust
- Corrosion-resistant materials are to be used to construct the vents.

Visual Surveillance Monitoring

Visual surveillance is used to detect threats through continuous observation of important or vulnerable areas of an asset. The observations can also be recorded for later review or use (for example, in court proceedings). Visual surveillance system can be used to monitor both the public (if applicable) and internal parts of a financial services facility/bank/site or entry or access points into specific buildings. These systems are also useful in recording individuals who enter or leave a facility, thereby helping to identify unauthorized access. Images can be transmitted live to a monitoring station, where they can be viewed in real time, or they can be recorded and reviewed later. Many financial services sector facilities have found that a combination of electronic surveillance and security guards provides an effective means of facility security.

Visual surveillance is provided through a CCTV system, in which the capture, transmission, and reception of an image is localized within a closed "circuit." This is different than other broadcast images, such as television.

At a minimum, a CCTV system consists of:

- One or more cameras
- A monitor for viewing the images
- A system for transmitting the images from the camera to the monitor.

Specific attributes and features of camera systems, lenses, and lighting systems are presented in table 9.11.

Table 9.11 Attributes of Camera, Lenses, and Lighting Systems

Attribute	*Discussion*
Camera Systems	
Camera Type	Major factors in choosing the correct camera are the resolution of the image required and lighting of the area to be viewed. • *Solid State* (including charge coupled devices, charge priming device, charge injection device, and metal oxide substrate)—these cameras are becoming predominant in the marketplace because of their high resolution and their elimination of problems inherent in tub cameras. • *Thermal*—These cameras are designed for night vision. They require no light and use differences in temperature between objects in the field of view to produce a video image. Resolution is low compared to other cameras, and the technology is currently expensive relative to other technologies. • *Tube*—These cameras can provide high resolution burn out and must be replaced after 1–2 years. In addition, tube performance can degrade over time. Finally, tube cameras are prone to burn images in the tube replacement.
Resolution (the ability to see fine details)	User must determine the amount of resolution required depending on the level of detail required for threat determination. A high definition focus with a wide field of vision will give an optimal viewing area.
Field of vision width	Cameras are designed to cover a defined field of vision, which is usually defined in degrees. The wider the field of vision, the more area a camera will be able to monitor.
Type of image produced (color, black and white, thermal)	Color images may allow the identification of distinctive markings, while black and white images may provide sharper contrast. Thermal imaging allows the identification of heat sources (such as human beings or other living creatures) from low light environments; however, thermal images are not effective in identifying specific individuals (i.e., for subsequent legal processes).
Pan/Tilt/Zoom (PTZ)	Panning (moving the camera in a horizontal plane), tilting (moving the camera in a vertical plane), and zooming (moving the lens to focus on objects that are at different distances from the camera) allow the camera to follow a moving object. Different systems allow these functions to be controlled manually or automatically. Factors to be considered in PTZ cameras are the degree of coverage for pan and tilt function sand the power of the zoom lens.
Lenses	
Format	Lens format determines the maximum image size to be transmitted.

(*Continued*)

Table 9.11 (Continued)

Attribute	*Discussion*
Focal Length	This is the distance from the lens to the center of the focus. The greater the focal length, the higher the magnification, but the narrower the field of vision.
F Number	F number is the ability to gather light. Smaller F numbers may be required for outdoor applications where light cannot be controlled as easily.
Distance and width approximation	The distance and width approximations are used to determine the geometry of the space that can be monitored at the best resolution.
Lighting Systems	
Intensity	Light intensity must be great enough for the camera type to produce sharp images. Light can be generated from natural or artificial sources. Artificial sources can be controlled to produce the amount and distribution of light required for a given camera and lens.
Evenness	Light must be distributed evenly over the field of view so that there are no darker or shadowy areas. If there are lighter vs. darker areas, brighter areas may appear washed out (i.e., details cannot be distinguished) while no specific objects can be viewed from darker areas.
Location	Light sources must be located above the camera so that light does not shine directly into the camera.

Source: USEPA (2005).

COMMUNICATION INTEGRATION

In this section, those devices necessary for communication and integration of financial services sector processing operations, such as electronic controllers, two-way radios, and wireless data communications are discussed. In regard to security applications, electronic controllers are used to automatically activate equipment (such as lights, surveillance cameras, audible alarms, or locks) when they are triggered. Triggering could be in response to variety of scenarios, including tripping of an alarm or a motion sensor; breaking of a window or a glass door; variation in vibration sensor readings; or simply through input from a timer.

Two-way wireless radios allow two or more users that have their radios tuned to the same frequency to communicate instantaneously with each other without the radios being physically lined together with wires or cables.

Wireless data communications devices are used to enable transmission of data between computer systems, without individual components being physically linked together via wires or cables. In financial processing systems,

these devices are often used to link remote monitoring stations or portable computers (i.e., laptops) to computer networks without using physical wiring connections.

Electronic Controllers

An electronic controller is a piece of electronic equipment that receives incoming electric signals an uses preprogrammed logic to generate electronic output signals based on the incoming signals. While electronic controllers can be implemented for any application that involves inputs and outputs (e.g., control of a piece of machinery in a factor), in a security application, these controllers essentially act as the system's "brain," and can respond to specific security-related inputs with preprogrammed output response. These systems combine the control of electronic circuitry with a logic function such that circuits are opened and closed (and thus equipment is turned on and off) through some preprogrammed logic. The basic principle behind the operation of an electrical controller is that it receives electronic inputs from sensors or any device generating an electrical signal (e.g., electrical signals from motion sensors), and then uses it preprogrammed logic to produce electrical outputs (e.g., these outputs could turn on power to a surveillance camera or to an audible alarm). Thus, these systems automatically generate a preprogrammed, logical response to a preprogrammed input scenario.

The three major types of electronic controllers are timers, electromechanical relays, and programmable logic controllers (PLCs), which are often called "digital relays." Each of these types of controller is discussed in more detail below.

Timers use internal signal/inputs (in contrast to externally generated inputs) and generate electronic output signals at certain times. More specifically, timers control electric current flow to any application to which they are connected, and can turn the current on or off on a schedule prespecificed by the user. Typical timer range (amount of time that can be programmed to elapse before the timer activates linked equipment) is from 0.2 seconds to 10 hours, although some of the more advanced timers have ranges of up to 60 hours. Timers are useful in fixed applications that don't require frequent schedule changes. For example, a timer can be used to turn on the lights in a room or building at a certain time every day. Timers are usually connected to their own power supply (usually 120–240 V).

In contrast to timers, which have internal triggers based on a regular schedule, *electromechanical relays* and *PLCs* have both external inputs and external outputs. However, PLCs are more flexible and more powerful than are electromechanical relays, and thus this section focuses primarily on

PLCs as the predominant technology for security-related electronic control applications.

Electromechanical relays are simple devices that use a magnetic field to control a switch. Voltage applied to the relay's input coil creates a magnetic field, which attracts an internal metal switch. This causes the relay's contacts to touch, closing the switch and completing the electrical circuit. This activates any linked equipment. These types of systems are often used for high voltage applications, such as in some automotive and other manufacturing processes.

Two-Way Radios

Two-way radios, as discussed here, are limited to a direct unit-to-unit radio communication, either via single unit-to-unit transmission and reception, or via multiple handheld units to a base station radio contact and distribution system. Radio frequency spectrum limitations apply to all handheld units, and directed by the FCC. This also distinguishes a handheld unit from a base station or base station unit (such as those used by an amateur (ham) radio operator), which operate under different wave length parameters.

Two-way radios allow a user to contact another user or group of users instantly on the same frequency, and to transmit voice or data without the need for wires. They use "half-duplex" communications; or communication that can be only transmitted or received; it cannot transmit and receive simultaneously. In other words, only one person may talk, while other personnel with radio(s) can only listen. To talk, the user depresses the talk button and speaks into the radio. The audio then transmits the voice wirelessly to the receiving radios. When the speaker has finished speaking and the channel has cleared, users on any of the receiving radios can transmit; either to answer the first transmission, or to begin a new conversation. In addition to carrying voice data, many types of wireless radios also allow the transmission of digital data, and these radios may be interfaced with computer networks that can use or track these data. For example, some two-way radios can send information such as global positioning system (GPS) data, or the ID of the radio. Some two-way radios can also send data through a SCADA system.

Wireless radios broadcast these voice or data communications over the airwaves from the transmitter to the receiver. While this can be an advantage in that the signal emanates in all directions and does not need a direct physical connection to be received at the receiver, it can also make the communications vulnerable to being blocked, intercepted, or otherwise altered. However, security features are available to ensure that the communications are not tampered with.

Wireless Data Communications

A wireless data communication system consists of two components: a "Wireless Access Point" (WAP), and a "Wireless Network Interface Card" (sometimes also referred to as a "Client"), which work together to complete the communications link. These wireless systems can link electronic devices, computers, and computer systems together using radio waves, thus eliminating the need for these individual components to be directly connected together through physical wires. While wireless data communications have widespread application in water and wastewater systems, they also have limitations. First, wireless data connections are limited by the distance between components (radio waves scatter over a long distance and cannot be received efficiently, unless special directional antenna are used). Second, these devices only function if the individual components are in a direct line of sight with each other, since radio waves are affected by interference from physical obstructions. However, in some cases, repeater units can be used to amplify and retransmit wireless signals to circumvent these problems.

(1) *WAP*: The WAP provides the wireless data communication service. It usually consists of a housing (which is constructed from plastic or metal depending on the environment it will be used in) containing a circuit board; flash memory that holds software; one of two external ports to connect to existing wired networks; a wireless radio transmitter/receiver; and one or more antenna connections. Typically, the WAP requires a one-time user configuration to allow the device to interact with the Local Area Network (LAN). This configuration is usually done via a web-driven software application which is accessed via a computer.

(2) *Wireless Network Interface Card/Client*: A wireless card is a piece of hardware that is plugged in to a computer and enables that computer to make a wireless network connection. The card consists of a transmitter, functional circuitry, and a receiver for the wireless signal, all of which work together to enable communication between the computer, its wireless transmitter/receiver, and its antenna connection. Wireless cards are installed in a computer through a variety of connections, including USB Adapters, or Laptop CardBus (PCMCIA) or Desktop Peripheral (PCI) cards. As with the WAP, software is loaded onto the user's computer, allowing configuration of the card so that it may operate over the wireless network

Two of the primary applications for wireless data communications systems are to enable mobile or remote connections to a LAN, and to establish wireless communications links between SCADA remote telemetry units (RTUs) and sensors in the field. Wireless car connections are usually used for LAN access from mobile computers. Wireless cards can also be incorporated into RTUs to allow them to communicate with sensing devices that are located remotely.

CYBER PROTECTION DEVICES

Various cyber protection devices are currently available for use in protecting financial services sector computer systems. These protection devices include antivirus and pest eradication software, firewalls, and network intrusion hardware/software.

Antivirus and Pest Eradication Software

Antivirus programs are designed to detect, delay, and respond to programs or pieces of code that are specifically designed to harm computers. These programs are known as "malware." Malware can include computer viruses, worms, and Trojan Horse programs (programs that appear to be benign but which have hidden harmful effects).

Pest eradication tools are designed to detect, delay, and respond to "spyware" (strategies that websites use to track user behavior, such as by sending "cookies" to the user's computer), and hacker tools that track keystrokes (keystroke loggers) or passwords (password crackers).

Viruses and pests can enter a computer system through the Internet or through infected CDs. They can also be placed onto a system by insiders. Some of these programs such as viruses and worms then move within a computer's drives and files, or between computers if the computers are networked to each other. This malware can deliberately damage files, utilize memory and network capacity, crash application programs, and initiate transmissions of sensitive information from a PC. While the specific mechanisms of these programs differ, they can infect files, and even the basic operating program of the computer firmware/hardware.

The most important features of an antivirus program are its abilities to identify potential malware and to alert a user before infection occurs, as well as its ability to respond to a virus already resident on a system. Most of these programs provide a log so that the user can see what viruses have been detected and where they were detected. After detecting a virus, the antivirus software may delete the virus automatically, or it may prompt the user to delete the virus. Some programs will also fix files or programs damaged by the virus.

Various sources of information are available to inform the general public and computer system operators about new viruses being detected. Since antivirus programs use signatures (or snippets of code or data) to detect the presence of a virus, periodic updates are required to identify new threats. Many antivirus software providers offer free upgrades that are able to detect and respond to the latest viruses.

Firewalls

A *firewall* is an electronic barrier designed to keep computer hackers, intruders, or insiders from accessing specific data files and information on a financial services sector's computer network or other electronic/computer systems. Firewalls operated by evaluating and then filtering information coming through a public network (such as the Internet) into the utility's computer or other electronic system. This evaluation can include identifying the source or destination addresses and ports, and allowing or denying access based on this identification.

There are two methods used by firewalls to limit access to the utility's computers or other electronic systems from the public network:

- The firewall may deny all traffic unless it meets certain criteria
- The firewall may allow all traffic through unless it meets certain criteria.

A simple example of the first method is to screen requests to ensure that they come from an acceptable (i.e., previously identified) domain name and Internet protocol address. Firewalls may also use more complex rules that analyze the application data to determine if the traffic should be allowed through. For example, the firewall may require user authentication (i.e., use of a password) to access the system. How a firewall determines what traffic to let through depends on which network layer it operates at and how it is configured. Some of the pros and cons of various methods to control traffic flowing in and out of the network are provided in table 9.12.

Firewalls may be a piece of hardware, a software program, or an appliance card that contains both.

Advanced features that can be incorporated into firewalls allow for the tracking of attempts to log-on to the LAN system. For example, a report of successful and unsuccessful log-in attempts may be generated for the computer specialist to analyze. For systems with mobile users, firewalls allow remote access in to the private network by the use of secure log-on procedures and authentication certificates. Most firewalls have a graphical user interface for managing the firewall.

In addition, new Ethernet firewall cards that fit in the slot of an individual computer bundle additional layers of defense (like encryption and permit/deny) for individual computer transmissions to the network interface function. These new cards have only a slightly higher cost than traditional network interface cards.

Network Intrusion Hardware/Software

Network intrusion detection and prevention system are software- and hardware-based programs designed to detect unauthorized attacks on a computer network system.

Table 9.12 Pros and Con of Various Firewall Methods for Controlling Network Access

Method	*Description*	*Pros*	*Cons*
Packet Filtering	Incoming and outgoing packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded. There are two type of packet filtering: static (the most common) and dynamic.	Static filtering is relatively inexpensive, and little maintenance required. It is well-suited for closed environments where access to or from multiple addresses is not allowed.	Leaves permanent open holes in the network; allows direct connection to internal hosts by external sources; offers no user authentication, method can be un-manageable in large networks.
Proxy Service	Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa. In this way, the firewall can limit the information made known to the requesting system, making vulnerabilities less apparent.	Only allows temporary open holes in the network perimeter. Can be used for all types of internal protocol services.	Allows direct connections to internal hosts by external clients; offers no user authentication
Stateful Pattern Recognition	This method examines and compares the contents of certain key parts of an information packet against a database of acceptable information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. If not, the information is discarded.	Provides a limited time window to allow pockets of information to be sent; does not allow any direct connections between internal and external hosts; supports user-level authentication.	Slower than packet filtering; does not support all types of connections.

Source: USEPA (2005).

While other applications, such as firewalls and antivirus software, share similar objectives with network intrusion systems, network intrusion systems provide a deeper layer of protection beyond the capabilities of these other systems because they evaluate patterns of computer activity rather than specific files.

It is worth noting that attacks may come from either outside or within the system (i.e., from an insider), and that network IDSs may be more applicable for detecting patterns of suspicious activity from inside a facility (i.e., accessing sensitive data, etc.) than are other information technology solutions.

Network IDSs employ a variety of mechanisms to evaluate potential threats. The types of search and detection mechanisms are dependent upon the level of sophistication of the system. Some of the available detection methods include the following:

- *Protocol analysis*—Protocol analysis is the process of capturing, decoding, and interpreting electronic traffic. The protocol analysis method of network intrusion detection involves the analysis of data captured during transactions between two or more systems or devices, and the evaluation of these data to identify unusual activity and potential problems. Once a problem is isolated and recorded, problems or potential threats can be linked to pieces of hardware or software. Sophisticated protocol analysis will also provide statistics and trend information on the captured traffic.
- *Traffic anomaly detection*—Traffic anomaly detection identifies potential threatening activity by comparing incoming traffic to "normal" traffic patterns, and identifying deviations. It does this by comparing user characteristics against thresholds and triggers defined by the network administrator. This method is designed to detect attacks that span a number of connections, rather than a single session.
- *Network honeypot*—This method establishes non-existent services in order to identify potential hackers. A network honeypot impersonates services that don't exist by sending fake information to people scanning the network. It identifies the attacker when they attempt to connect to the service. There is no reason for legitimate traffic to access these resources because they don't exist; therefore any attempt to access them constitutes an attack.
- *Anti-intrusion detection system evasion techniques*—These methods are designed for attackers who may be trying to evade intrusion detection system scanning. They include methods called IP defragmentation, TCP streams reassembly, and deobfuscation.

While these detection systems are automated, they can only indicate patterns of activity that a computer administer or other experienced individual must interpret to determine whether or not they are potentially harmful.

Monitoring the logs generated by these systems can be time consuming, and there may be a learning curve to determine a baseline of "normal" traffic patterns from which to distinguish potential suspicious activity.

REFERENCES AND RECOMMENDED READING

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.* Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

Garcia, M. L. 2001. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann.

IBWA. 2004. *Bottled Water Safety and Security*. Alexandria, VA: International Bottled Water Association.

NAERC. 2002. *Security Guidelines for the Electricity Sector*. Washington, DC: North American Electric Reliability Council.

Schneier, B. 2000. *Secrets & Lies*. New York: Wiley.

USEPA. 2005. *Water and Wastewater Security Product Guide*. Accessed April14, 2016 @ http://cfpub.epa.gov.safewater/watersecurity/guide.

Chapter 10

Fourteen Features of Active and Effective Security

> It takes disasters to trigger change because dangers that remain hypothetical fail to trigger appropriate sensory response.
>
> —D.D. P. Johnson and E.M.P Madin

> If men would learn from history, what lessens it might teach us!
>
> —Samuel Coleridge

The events of 9/11 dramatically changed this nation and focused us on combating terrorism. As a result, in 2003 and subsequent years, the Department of Homeland Security (DHS) in conjunction with members from the general public, state and local agencies, and private groups concerned with the safety of critical infrastructures, established a Water Security Working Group (WSWG) to consider and make recommendations on infrastructure security issues. Although it was initially created to make recommendations for water/wastewater security, WSWG is an excellent template for use with other critical infrastructures, including communication assets. For example, the WSWG identified active and effective security practices for critical infrastructure, and provided an approach for adopting these practices. It also recommended mechanisms to provide incentives that facilitate broad and receptive response among critical infrastructure sectors to implement active and effective security practices. Finally, WSWG recommended mechanisms to measure progress and achievements in implementing active and effective security practices, and identify barriers to implementation.

The WSWG recommendations on security are structured to maximize benefits to critical industries by emphasizing actions that have the potential both to improve the quality or reliability of service, and to enhance security.

These recommendations, based on original recommendations from the 2003 National Drinking Water Advisor Council (NDWAC), were designed primarily, as the name suggests, for use by water systems of all types and sizes, including systems that serve less than 3,300 people. However, it is the author's opinion, that NDWAC's recommendations, when properly adapted to applicable circumstances and locations, can be applied to any and all critical infrastructure sectors, including the financial services sector.

The NDWAC identified 14 features of active and effective security programs that are important to increasing security and that are relevant across the broad range of utility circumstances and operating conditions. USEPA (2003) points out that the 14 features are, in many cases, consistent with the steps needed to maintain technical, management, and operational performance capacity related to overall water quality; as pointed out earlier, these steps can be applied to other critical infrastructures as well. Many facilities may be able to adopt some of the features with minimal, if any, capital investment.

14 FEATURES OF ACTIVE AND EFFECTIVE SECURITY

It is important to point out that the 14 features of active and effective programs emphasize that "one size does not fit all" and is not a cookie cutter approach to effective implementation of security measures. There will be variability in security approaches and tactics among financial securities sector facilities, based on industry-specific circumstances and operating conditions. The 14 features are as follows:

- Sufficiently flexible to apply to all communication assets, regardless of size.
- Incorporate the idea that active and effective security programs should have measurable goals and timelines.
- Allow flexibility for financial services sector facilities to develop specific security approaches and tactics that are appropriate to industry-specific circumstances.

Financial services sector facilities can differ in many ways including the following:

- Number of supply sources
- Energy capacity
- Operation risk
- Location risk
- Security budget
- Spending priorities
- Political and public support

- Legal barriers
- Public versus private ownership

Financial services sector facilities should address security in an informed and systematic way, regardless of these differences. Financial services sector facilities need to fully understand the specific, local circumstances and conditions under which they operate and develop a security program tailored to those conditions. The goal in identifying common features of active and effective security programs is to achieve consistency in security program outcomes among financial services sector facilities, while allowing for and encouraging facilities to develop utility-specific security approaches and tactics. The features are based on a comprehensive "security management layering system" approach that incorporates a combination of public involvement and awareness, partnerships, and physical, chemical, operational, and design controls to increase overall program performance. They address security in four functional categories: *organization*, *operation*, *infrastructure*, and *external*. These functional categories are discussed in greater detail below.

- *Organizational*—There is always something that can be done to improve security. Even when resources are limited, the simple act of increasing organizational attentiveness to security may reduce vulnerability and increase responsiveness. Preparedness itself can help deter attacks. The first step to achieving preparedness is to make security a part of the organizational culture, so that it is in the day-to-day thinking of frontline employees, emergency responders, and management of every communication sector facility in this country. To successfully incorporate security into "business as usual," there must be a strong commitment to security by organization leadership and by the supervising body, such as the board of stockholders. The following features address how a security culture can be incorporated into an organization.
- *Operational*—In addition to having a strong culture and awareness of security within an organization, an active and effective security program makes security part of operational activities, from daily operations, such as monitoring of physical access controls, to scheduled annual reassessments. Financial services sector entities will often find that by implementing security into operations they can also reap cost benefits, and improve the quality or reliability of the energy service.
- *Infrastructure*—These recommendations advise utilities to address security in all elements of financial services sector infrastructure—from source to distribution and through processing and product delivery.
- *External*—Strong relationships with response partners and the public strengthen security and public confidence. Two of the recommended features of active end effective security programs address this need.

14 Features

Feature 1. Make an explicit and visible commitment of the senior leadership to security.

Financial services sector facilities should create an explicit, easily communicated, enterprise-wide commitment to security, which can be done through

- incorporating security into a utility-wide mission or vision statement, addressing the full scope of an active and effective security program—that is, protection of worker/public health, worker/public safety, and public confidence, and that is part of core day-to-day operations;
- developing an enterprise-wide security policy, or set of policies.

Financial services sector entities should use the process of making a commitment to security as an opportunity to raise awareness of security throughout the organization, making the commitment visible to all employees and customers, and to help every facet of the enterprise to recognize the contribution they can make to enhancing security.

Feature 2. Promote security awareness throughout the organization.

The objective of a security culture should be to make security awareness a normal, accepted, and routine part of day-to-day operations. Examples of tangible efforts include the following:

- Conducting employee training
- Incorporating security into job descriptions
- Establishing performance standards and evaluations for security
- Creating and maintaining a security tip line and suggestion box for employees
- Making security a routine part of staff meetings and organization planning
- Create a security policy

Feature 3. Assess vulnerabilities and periodically review and update vulnerability assessments (VAs) to reflect changes in potential threats and vulnerabilities.

Because circumstances change, financial services sector facilities should maintain their understanding and assessment of vulnerabilities as a "living document," and continually adjust their security enhancement and maintenance priorities. Financial services sector facilities should consider their

individual circumstances and establish and implement a schedule for review of their vulnerabilities.

Assessments should take place once every three to five years at a minimum. Financial services sector facilities may be well served by doing assessments annually.

Feature 4. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.

Dedicated resources are important to ensure a sustained focus on security. Investment in security should be reasonable considering utilities' specific circumstances. In some circumstances, investment may be as simple as increasing the amount of time and attention that executives and managers give to security. Where threat potential or potential consequences are greater, greater investment likely is warranted.

This feature establishes the expectation that chemical industrial facilities should, through their annual capital, operations, and maintenance, and staff resources plans, identify and set aside resources consistent with their specific identified security needs. Security priorities should be clearly documented and should be reviewed with utility executives at least once per year as part of the traditional budgeting process.

Feature 5. Identify managers and employees who are responsible for security and establish security expectations for all staff.

- Explicit identification of security responsibilities is important for development of a security culture with accountability.
- At minimum, communication sector facilities should identify a single, designated individual responsible for overall security, even if other security roles and responsibilities will likely be dispersed throughout the organization.
- The number and depth of security-related roles will depend on a utility's specific circumstances.

Feature 6. Establish physical and procedural controls to restrict access to chemical industrial infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.

Examples of physical access controls include fencing critical areas, locking gates and doors, and installing barriers at site access points. Monitoring for physical intrusion can include maintaining well-lighted facility perimeters, installing motion detectors, and utilizing intrusion alarms. The use of

neighborhood watches, regular employee rounds, and arrangements with local police and fire departments can support identifying unusual activity in the vicinity of facilities.

Examples of procedural access controls include inventorying keys, changing access codes regularly, and requiring security passes to pass gates an access sensitive area. In addition, utilities should establish the means to readily identify all employees including contractors and temporary workers with unescorted access to facilities.

Feature 7. Employee protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.

Until progress can be made in development of practical and affordable online contaminant monitoring and surveillance systems, most financial services sector facilities must use other approaches to contaminant monitoring and surveillance.

Many utilities already measure the above parameters (and many others) on a regular basis to control plant operations and confirm chemical mixture quality; monitoring these parameters more closely may create operational benefits for facilities that extend far beyond security, such as reducing operating costs and chemical usage. Financial services sector facilities also should thoughtfully monitor customer complaints and improve connections with local public health networks to detect public health anomalies.

Feature 8. Define security-sensitive information; establish physical, electronic, and procedural controls to restrict access to security-sensitive information; detect unauthorized access; and ensure information and communications systems will function during emergency response and recover.

Protecting information technology (IT) systems largely involves using physical hardening and procedural steps to limit the number of individuals with authorized access and to prevent access by unauthorized individuals. Examples of physical steps to harden SCADA and IT networks include installing and maintaining fire walls, and screening the network for viruses. Examples of procedural steps include restricting remote access to data networks, and safeguarding critical data through backups and storage in safe places. Utilities should strive for continuous operation of IT and telecommunications systems, even in the event of an attack, by providing uninterruptible power supply and backup systems, such as satellite phones.

In addition to protecting IT systems, security-sensitive information should be identified and restricted to the appropriate personnel. Security-sensitive information could be contained within the following:

- Facility maps and blueprints
- Operations details
- Tactical level security program details
- Any other information on utility operations or technical details that could aid in planning or execution of an attack.

Identification of security-sensitive information should consider all ways that utilities might use and make public information (e.g., many chemical industrial facilities may at times engage in competitive bidding processes for construction of new facilities or infrastructure). Finally, information critical to the continuity of day-to-day operations should be identified and backup.

Feature 9. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; include consideration of opportunities to reduce risk through physical hardening and adoption of inherently lower-risk design and technology options.

Prevention is a key aspect of enhancing security. Consequently, consideration of security issues should begin as early as possible in facility construction (i.e., it should be a factor in building plans and designs). However, to incorporate security considerations into design choices, chemical facilities need information about the types of security design approaches and equipment that are available and the performance of these designs and equipment in multiple dimensions. For example, financial services sector facilities would want to evaluate not just the way that a particular design might contribute to security, but would also look at how that design would affect the efficiency of day-to-day operations and employee safety.

Feature 10. Monitor available threat-level information and escalate security procedures in response to relevant threats.

Monitoring threat information should be a regular part of a security program manager's job, and utility**-,** facility-, and region-specific threat levels and information should be shared with those responsible for security. As part of security planning, financial services sector facilities should develop systems to access threat information, procedures that will be followed in the event of

increased industry or facility threat levels, and should be prepared to put these procedures in place immediately, so that adjustments are seamless. Involving local law enforcement and FBI is critical.

Financial services sector facilities should investigate what networks and information sources might be available to them locally, and at the state and regional level. If a utility cannot gain access to some information networks, attempts should be made to align with those who can and will provide effective information to the financial services sector facility.

Feature 11. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans to reflect changes in potential threats, physical infrastructure, chemical processing operations, critical interdependencies, and response protocols in partner organizations.

Financial services sector facilities should maintain response and recovery plans as "living documents." In incorporating security considerations into their emergency response and recovery plans, chemical facilities also should be aware of the National Incident Management System (NIMS) guidelines, established by DHS, and of regional and local incident management commands and systems, which tend to flow from the national guidelines.

Financial services sector facilities should consider their individual circumstances and establish, develop, and implement a schedule for review of emergency response and recovery plans. Financial services sector facility plans should be thoroughly coordinated with emergency response and recovery planning in the larger community. As part of this coordination, a mutual aid program should be established to arrange in advance for exchanging resources (personnel or physical assets) among agencies within a region, in the event of an emergency or disaster that disrupts operation. Typically, the exchange of resource is based on a written formal mutual and agreement. For example, Florida's Water-Wastewater Agency Response Network (FlaWARN) deployed after Hurricane Katrina and allowed the new "utilities helping utilities" network to respond to urgent requests from Mississippi for help to bring facilities back online after the hurricane.

The emergency response and recovery plans should be reviewed and updated as needed annually. This feature also establishes the expectation that chemical facilities should test or exercise their emergency response and recovery plans regularly.

Feature 12. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, rate setting organizations, and customers.

An active and effective security program should address protection of public health, public safety (including infrastructure), and public confidence. Financial services sector facilities should create an awareness of security and an understanding of the rationale for their overall security management approach in the communities they reside in and/or serve.

Effective communication strategies consider key messages; who is best equipped/trusted to deliver the key messages; the need for message consistency, particularly during an emergency; and the best mechanisms for delivering messages and for receiving information and feedback from key partners. The key audiences for communication strategies are utility employees, response organizations, and customers.

Feature 13. Forge reliable and collaborative partnerships with the communities served, managers of critical interdependent infrastructure, response organizations, and other local utilities.

Effective partnerships build collaborative working relationships and clearly define roles and responsibilities, so that people can work together seamlessly if an emergency should occur. It is important for financial services sector facilities within a region and neighboring regions to collaborate and establish a mutual aid program with neighboring utilities, response organizations, and sectors, such as the power sector, on which utilities rely or impact. Mutual aid agreements provide for help from other organizations that is prearranged and can be accessed quickly and efficiently in the event of a terrorist attack or natural disaster. Developing reliable and collaborative partnerships involves reaching out to managers and key staff and other organizations to build reciprocal understanding and to share information about the facility's security concerns and planning. Such efforts will maximize the efficiency and effectiveness of a mutual aid program during an emergency response effort, as the organizations will be familiar with each others' circumstances, and thus will be better able to serve each other.

It is also important for financial services sector facilities to develop partnerships with the communities and customers they serve. Partnerships help to build credibility within communities and establish public confidence in utility operations. People who live near financial services sector facility structures can be the eyes and ears of the facility, and can be encouraged to notice and report changes in operating procedures or other suspicious behaviors.

Financial services sector facilities and public health organizations should establish formal agreements on coordination to ensure regular exchange of information between facilities and public health organizations, and outline roles and responsibilities during response to and recovery from an emergency. Coordination is important at all levels of the public health

Table 10.1 14 Features of Active and Effective Security Matrix

Features	*Checklist: Potential Measures of Progress*
Organizational Features	
Feature 1—Explicit commitment to security	Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?
Feature 2—Promote security awareness	Are incidents reported in a timely way, and are lessons learned from incident responses reviewed and, as appropriate, incorporated into future utility security efforts?
Feature 5—Defined security roles and employee expectations	Are managers and employees who are responsible for security identified?
Operational Features	
Feature 3—Vulnerability Assessment (VA) up to date	Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?
Feature 4—Security resources and implementation priorities	Are security priorities clearly identified, and to what extent do security priorities have resources assigned to them?
Feature 7—Contamination detection	Is there a protocol/procedure in place to identify and respond to suspected contamination events?
Feature 10—Threat-level-based protocols	Is there a protocol/procedure of responses that will be made if threat levels change?
Feature 11—Emergency Response Plan tested and up to date	Do exercise address the full range of threats—physical, cyber, and contamination—and is there a protocol/procedure to incorporate lessons learned from exercises and actual response into updates to emergency response and recovery plans?
Feature 14—Industry-specific measures and self-assessment	Does the utility perform self-assessment at least annually?
Infrastructure Features	
Feature 6—Intrusion detection and access control	To what extent are methods to control access to sensitive assets in place?
Feature 8—Information Protection and continuity	Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how to control measures perform under testing?
Feature 9—Design and construction standards	Are security considerations incorporated into internal utility design and construction standards for new facilities/infrastructure and major maintenance projects?

(*Continued*)

Table 10.1 (Continued)

Features	*Checklist: Potential Measures of Progress*
External Features	
Feature 12—Communications	Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns?
Feature 13—Partnerships	Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, and response organizations been established?

Source: USEPA (2003).

community—national public health, county health agencies, and healthcare providers, such as hospitals.

Feature 14. Develop chemical facility–specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

Although security approaches and tactics will be different depending on chemical utility–specific circumstances and operating conditions, we recommend that all financial services sector facilities monitor and measure a number of common types of activities and achievements, including existence of program policies and procedures, training, testing, and implementing schedules and plans.

The 14 Feature Matrix

In table 10.1, a matrix of recommended measures to assess effectiveness of a financial services sector facility's security program is presented. Each feature is grouped according to its functional category: organization, operation, infrastructure, and external.

Ultimately, the goal of implementing the 14 security features (and all other security provisions) is to create a significant improvement in financial services sector facilities on a national scale, by reducing vulnerabilities, and therefore risk to public health from terrorist attacks and natural disasters. To create a sustainable effect, the financial services sector as a whole must not only adopt and actively practice the features, but also incorporate the features into "business as usual."

REFERENCES AND RECOMMENDED READING

DHS. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed @ https://www.dhs.gov/xlibrary/assets/physical_Strat.

DHS. 2007. *Banking and Finance*. Washington, DC: U.S. Department of Homeland Security.

DHS. 2009. *National Infrastructure Protection Plan*. Accessed May 11, 2017 @ http://www.dhs.gov/ xlibrary/assets/NIPP.Plan.pdf.

DHS. 2013. *Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Accessed @ https://www.dihs.gov/xabout/laws/gc_1214597989952.shtm.

USEPA. 2003. *Active and Effective Water Security Programs*. Accessed June 6 @ http://cfpub.epa.gov/safewater/watersecurity/14 features.cfm.

Appendix

Definition of Terms

A

Access control point—A station at entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.

Acid bomb—A crude bomb made by combining muriatic acid with aluminum strips in a 2-liter soda bottle.

Active vehicle barrier—An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.

Aerosol—A fine mist or spray, which contains minute particles suspended in a gas (e.g., fog, smoke).

Agency—A division of government with a specific function, or a non-governmental organization (e.g., private contractor or business) that offers a particular kind of assistance. In the incident command system, agencies are defined as jurisdictional (having statutory responsibility for incident mitigation) or assisting and/or cooperating (providing resources and/or assistance).

Aggressor—Any person seeking to compromise a function or structure.

Airborne contamination—Chemical or biological agents introduced into and fouling the source of supply of breathing or conditioning air.

Al Qaeda—Meaning "the Base"; an international terrorist group founded in approximately 1989 and dedicated to opposing non-Islamic governments with force and violence. One of the principal goals of al Qaeda was to drive the U.S.-armed forces out of the Saudi Arabian peninsula and Somalia by violence. Currently wanted for several terrorist attacks, including those on

the U.S. embassy in Kenya and Tanzania as well as the first and second World Trade Center bombings, and the attack on the Pentagon.

Al Tahwid—A Palestinian group based in London which professes a desire to destroy both Israel and the Jewish people throughout Europe. Eleven al Tahwid were arrested in Germany allegedly as they were about to begin attacking that country.

Alarm assessment—Verification and evaluation of an alarm alert through the use of closed-circuit television (CCTV) or human observation. Systems used for alarm assessment are designed to respond rapidly, automatically, and predictably to the receipt of alarms at the security center.

Alarm priority—A hierarchy of alarms by order of importance. This is often used in larger systems to give priority to alarms with greater importance.

All-Hazards—A grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property, or alternatively causing functional degradation to social, economic, or environmental aspects.

Alpha radiation—The least penetrating type of nuclear radiation. Not considered dangerous unless particles enter the body.

Ammonium nitrate-fuel oil (ANFO)—A powerful explosive made by mixing fertilizer and fuel oil. The type of bomb used in the first World Trade Center attack as well as the 1995 Oklahoma City bombing.

Annunciation—A visual, audible, or other indication by a security system of a condition.

Anthrax—An often fatal infectious disease contracted from animals. Anthrax spores have such a long survival period; the incubation period is short; disability is severe, making anthrax a bioweapon of choice by several nations.

Antidote—A remedy to counteract the effects of poison.

Antigen—A substance which stimulates an immune response by the body immune system recognizes such substances as foreign and produces antibodies to fight them.

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts.

Antitoxin—An antibody which neutralizes a biological toxin.

Area lighting—Lighting that illuminates a large exterior area.

Assessment—The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Asset—A person, structure, facility, information, material or process that has value. In the context of the National Infrastructure Protection Plan (NIPP), people are not considered assets.

Asymmetric threat—The use of crude or low-tech methods to attack a superior or more high-tech enemy.

Axis of Evil—Iran, Iraq, and North Korea as defined by President George W. Bush during his State of the Union speech in 2002 as nations that were a threat to U.S. security due to harboring terrorism.

Audible alarm device—An alarm device that produces an audible announcement (e.g., bell, horn, siren) of an alarm condition.

B

Ballistics attack—An attack in which small arms (e.g., pistols, submachine guns, shotguns, rifles) are fired from a distance and rely on the flight of the projectile to damage the target.

Bioaccumulative—Substances that concentrate in living organisms as the breather contaminated air drink or live in contaminated water or eat contaminated food rather than being eliminated through natural processes.

Biochemical warfare—Collective term for use of both chemical warfare and biological warfare weapons.

Biochemterroism—Terrorism using as weapons biological or chemical agents.

Biological agents—Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

Biological ammunition—Ammunition designed specifically to release a biological agent used as the warhead for biological weapons. Biological ammunition may take many forms, such as a missile warhead or bomb.

Biological attacks—The deliberate release of germs or other biological substances that cause illness.

Biometric reader—A device that gathers and analyzes biometric features.

Biometrics—The use of physical characteristics of the human body as a unique identification method.

Biosafety Level 1—Suitable for work involving well-characterized biological agents not known to consistently cause disease in healthy adult humans, and of minimal potential hazard to lab personnel and the environment. Work is generally conducted on open bench tops using standard microbiological practices.

Biosafety Level 2—Suitable for work involving biological agents of moderate potential hazard to personnel and the environment. Lab personnel should have specific training in handling pathogenic agents and be directed by competent scientists. Access to the lab should be limited when work is being conducted, extreme precautions should be taken with contaminated sharp items, and certain procedures should be conducted in biological

safety cabinets or other physical containment equipment if there is a risk of creating infectious aerosols or splashes.

Biosafety Level 3—Suitable for work done with indigenous or exotic biological agents that may cause serious or potentially lethal disease as a result of exposure by inhalation. Lab personnel must have specific training in handling pathogenic and potentially lethal agents and be supervised by competent scientists who are experienced in working with these agents. All procedures involving the manipulation of infectious material are conducted within biological safety cabinets or other physical containment devices, or by personnel wearing appropriate personal protective clothing and equipment. The lab must have special engineering and design features.

Biosafety Level 4—Suitable for work with the most infectious biological agents. Access to the two Biosafety Level 4 labs in the United States is highly restricted.

Bioterrorism—The use of biological agents in a terrorist operation. Biological toxin would include anthrax, Ricin, botulism, the plague, smallpox, and tularemia.

Bioterrorism Act—The Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

Blast-resistant glazing—Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.

Blister agents—Agents which cause pain and incapacitation instead of death and might be used to injure many people at once, thereby overloading medical facilities and causing fear in the population. Mustard gas is the best known blister agent.

Blood agents—Agents based on cyanide compounds. More likely to be used for assassination than for terrorism.

Bollard—A vehicle barrier consisting of a cylinder, usually made of steel and sometimes filled with concrete, placed on end in the ground and spaced about 3 feet apart to prevent vehicles from passing, but allowing entrance of pedestrians and bicycles.

Botulism—An illness caused by the botulinum toxin, which is exceedingly lethal and quite simple to produce. It takes just a small amount of the toxin to destroy the central nervous system. Botulism may be contracted by the ingestion of contaminated food or through breaks or cuts in the skin. Food supply contamination or aerosol dissemination of the botulinum toxin are the two ways most likely to be used by terrorists.

Boundary penetration sensor—An interior intrusion detection sensor that detects attempts by individuals to penetrate or enter a building.

Building hardening—Enhanced construction that reduces vulnerability to external blast and ballistic attacks.

Bush Doctrine—The policy that holds responsible nations which harbor or support terrorist organizations and says that such countries are considered hostile to the U.S. From President George W. Bush's speech: "A country that harbors terrorists will either deliver the terrorist or share in their fate. …People have to choose sides. They are either with the terrorists, or they're with us."

Business continuity—The ability of an organization to continue to function before, during, and after a disaster.

BWC—Officially known as the "Convention on the Prohibition of Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and Destruction." The BWC works toward general and complete disarmament, including the prohibition and elimination of all types of weapons of mass destruction.

C

Capacitance sensor—A device that detects an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.

Card reader—A device that gathers or reads information when a card is presented as an identification method.

Carrier—A person or animal that is potentially a source of infection by carrying on infectious agent without visible symptoms of the disease.

Cascading event—The occurrence of one event that causes another event.

Causative agent—The pathogen, chemical, or other substance that is the cause of disease or death in an individual.

Cell—The smallest unit within a guerrilla or terrorist group. A cell generally consists of two to five people dedicated to a terrorist cause. The formation of cells is born of the concept that an apparent "leaderless resistance" makes it hard for counterterrorists to penetrate.

Chain of custody—The tracking and documentation of physical control of evidence.

Chemical agent—A toxic substance intended to be used for operations to debilitate, immobilize, or kill military or civilian personnel.

Chemical ammunition—A munition, commonly a missile, bomb, rocket, or artillery shell, designed to deliver chemical agents.

Chemical attack—The intentional release of toxic liquid, gas or solid in order to poison the environment or people.

Chemical warfare—The use of toxic chemicals as weapons, not including herbicide used to defoliate battlegrounds or riot control agents such as gas or mace.

Chemical weapons—Weapons that produce effects on living targets via toxic chemical properties. Examples would be sarin, VX nerve gas, or mustard gas.

Chemterrorism—The use of chemical agents in a terrorist operation. Well-known chemical agents include sarin and VX nerve gas.

Choking agent—Compounds that injure primarily in the respiratory tract (i.e., nose, throat, and lungs). In extreme cases membranes swell up, lungs become filled with liquid, and death results from lack of oxygen.

Cipro—A Bayer antibiotic that combats inhalation anthrax.

Clear zone—An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.

Close-circuit television (CCTV) —An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.

Collateral damage—Injury or damage to assets that are not the primary target of an attack.

Community—A political entity that has the authority to adopt and enforce laws and ordinances for the area under its jurisdiction. In most cases, the community is an incorporated town, city, township, village, or unincorporated area of a country; however, each state defines its own political subdivisions and forms of government.

Consequence analysis—The estimate of the potential public health and economic impacts that a successful attack could cause.

Consequence management—Measures to protect public health and safety, restore essential governmental services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise the primary authority to respond to the consequences of terrorism.

Contamination—The undesirable deposition of a chemical, biological, or radiological (CBR) material on the surface of structures, areas, objects, or people.

Continuity of services and operations—Controls to ensure that, when unexpected events occur, departmental/agency minimum essential infrastructure services and operations, including computer operations, continue without interruption or are promptly resumed, and that critical and sensitive data are protected through adequate contingency and business recovery plans and exercise.

Control center—A sophisticated monitoring and control system responsible for balancing power generation and demand; monitoring flows over

transmission lines to avoid overloading; planning and configuring the system to operate reliably; maintaining system stability; preparing for emergencies; and placing equipment in and out of service for maintenance and emergencies.

Control systems—Computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operation data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA system, Process Control Systems, and Distributed Control Systems.

Controlled area—An area into which access is controlled or limited. The portion of a restricted area usually near or surrounding a limited or exclusion area. Correlates with exclusion zone.

Controlled perimeter—A physical boundary at which vehicle and personnel access is controlled at the perimeter of a site. Access control at a controlled perimeter should demonstrate the capacity to search individuals and vehicles.

Conventional construction—Building construction that is not specifically designed to resist weapons, explosives, or CBR effects. Conventional construction is designed only to resist common loadings and environmental effects such as wind, seismic, and snow loads.

Counterintelligence—Information gathered and activities conducted to protect against: espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

Counterterrorism—Measures used to prevent preempt, or retaliate against terrorist attacks.

Covert entry—Attempts to enter a facility by using false credentials or stealth.

Crash bar—A mechanical egress device located on the interior side of a door that unlocks the door when pressure is applied in the direction of egress.

Crisis management—The measures taken to identify, acquire, and plant the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

Critical assets—Those assets essential to the minimum operations of the organization, and to ensure the health and safety of the general public.

Critical infrastructure—Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal. State, regional, territorial, or local jurisdiction.

Criticality—A description of the importance of a particular sector asset, system, network, or function in relation to national or regional security issues. Includes a consideration of public health and economic impacts.

Cutaneous—Related to or entering through the skin.

Cutaneous anthrax—Anthrax that is contracted via broken skin. The infection spreads through the bloodstream causing cyanosis, shock, sweating, and finally death.

Cyanide agent—Used by Iraq in the Iran war against the Kurds in the 1980s, and also by the Nazis in the gas chambers of concentration camps, cyanide agents are colorless liquid which is inhaled in its gaseous form while liquid cyanide and cyanide salts are absorbed by the skin. Symptoms are headache, palpitations, dizziness, and respiratory problems followed later by vomiting, convulsions, respiratory failure and unconsciousness, and eventually by death.

Cybersecurity—The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentially, integrity, and availability. Includes protection and restoration, when needed, or information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Cyber system—Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services. Examples include business systems, control systems, and access control systems.

Cyberterrorism—Attacks on computer networks or systems, generally by hackers working with or for terrorist groups. Some forms of cyberterrorism include denial of service attacks, inserting viruses or stealing data.

D

Data transmission equipment—A path for transmitting data between two or more components (e.g., a sensor and alarm reporting system, a card read and controller, a CCTV camera and monitor, a transmitter and receiver).

Decontamination—The reduction or removal of a CBR material from the surface of a structure, area, object, or person.

Defensive layer—Building design or exterior perimeter barriers intended to delay attempted forced entry.

Defensive measures—Protective measures that delay or prevent attack on an asset or that shield the asset from weapons, explosives, and CBR effects. Defensive measures include site work and building design.

Dependency—The one-directional reliance of an asset, system network, or collection thereof, within or across sectors, in input, interaction, or other requirement from other sources in order to function properly.

Detection layer—A ring of intrusion detection sensors located on or adjacent to a defensive layer or between two defensive layers.

Detection measures—Protective measures that detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the responsive force. Detection measures include detection systems, assessment systems, and access control system elements.

Dirty bomb—A makeshift nuclear device which is created from radioactive nuclear waste material. While not a nuclear blast, an explosion of a dirty bomb causes localized radioactive contamination as the nuclear waste material is carried into the atmosphere where it is dispersed by the wind.

Domestic terrorism—The unlawful use, or threatened use, or force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

Dose rate (radiation)—A general term indicating the quantity (total or accumulated) or ionizing radiation or energy absorbed by a person or animal, per unit of time.

Duress alarm devices—Also known as panic buttons, these devices are designated specifically to initiate a panic alarm.

E

eBomb (or e-bomb)—Electromagnetic bomb which produces a brief pulse of energy which affects electronic circuitry. At low levels, the pulse temporarily disables electronics systems, including computers, radios, and transportation systems. High levels completely destroy circuitry, causing mass disruption of infrastructure while sparing life and property.

Ecotage—Is the portmanteau of the "eco-" prefix and "sabotage." It is used to describe illegal acts of vandalism and violence, committed in the name of environmental protection.

Ecoterrorism—A neologism for terrorism that includes sabotage intended to hinder activities that are considered damaging to the environment.

Effective standoff distance—A standoff distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating constitution or retrofit.

Electromagnetic Pulse (EMP)—A burst of electromagnetic radiation by deliberate means, such as nuclear attack, or through natural means, such as a large-scale geomagnetic storm. Magnetic and electric fields resulting from EMP have the potential to disrupt electrical and electronic systems by causing destructive current and voltage surges.

Electronic security system—An integrated system that encompasses interior and exterior sensors, CCTV systems for assessment of alarm conditions, electronic entry control systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.

Emergency alert system—A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communications Commission (FCC). The system provides the president and other federal, state and local officials the means to broadcast emergency information to the public before, during, and after disasters.

Entry control point—A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.

Entry control stations—Entry control stations should be provided at main perimeter entrances where security personnel are present. Entry control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.

Evacuation—organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

Exclusion area—A restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

F

Facial recognition—A biometric technology that is based on features of the human face.

Fallout—The descent to the earth's surface of particles contaminated with radioactive material from a radioactive cloud. The term can also be applied to the contaminated particulate matter itself.

Fatah—Meaning "conquest by means of jihad"; a political organization created in the 1960s and led by Yasser Arafat. With both a military and intelligence wing, it has carried out terrorist attacks on Israel since 1965. It joined the PLO in 1968. Since 9/11, the Fatah was blamed for attempting to smuggle 50 tons of weapons into Israel.

Fence sensor—An exterior intrusion detection sensor that detects aggressors as they attempt to climb over, cut through or otherwise disturbs a fence.

Fenestration—A building opening.

Fiber optics—A method of data transfer by passing bursts of light through a strand of glass or clear plastic.

Field of view—The visible area in a video picture.

Forced entry—Entry to a denied area achieved through force to create an opening in fence, walls, doors, etc., or to overpower guards.

Fragment-retention film (FRF)—A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.

Frame rate—In digital video, a measurement of the rate of change in a series of pictures, often measured in frames per second.

Frangible construction—Building components that are designed to fail to vent blast pressures from an enclosure in a controlled manner and direction.

Frustration-aggression hypothesis—A hypothesis that every frustration leads to some form of aggression and every aggressive act results from some prior frustration.

Function—A service, process, capability, or operation performed by an asset, system, network, or organization.

Fundamentalism—Conservative religious authoritarianism. Fundamentalism is not specific to Islam; it exists in all faiths. Characteristics include literal interpretation of scriptures and a strict adherence to traditional doctrines and practices.

G

Geneva Protocol 1925—The first treaty to prohibit the use of biological weapons. The 1925 Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases and Bacteriological Methods of Warfare.

Germ warfare—The use of biological agents to cause harm to targeted people either directly, by bringing the people into contact with the agents or indirectly, by infecting other animals and plants, which would in turn cause harm to the people.

Glanders—An infectious bacterial disease known to cause inflammation in horses, donkeys, mules, goats, dogs and cats. Human infection has not been seen since 1945, but because so few organisms are required to cause disease, it is considered a potential agent for biological warfare.

Glare security lighting—Illumination projected from a security perimeter into the surrounding area, making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.

Glass-break detector—An intrusion detection sensor that is designed to detect breaking glass either through vibration or acoustics.

Government Coordinating Council (GCC)—The government counterpart to the SCC for each sector established to enable interagency coordination. The GCC comprises representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the security and operations landscape of each individual sector.

Grid wire sensor—An intrusion detection sensor that uses a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.

Ground zero—From 1946 until 9/11, ground zero was the point directly above, below, or at which a nuclear explosion occurs or the center or origin of rapid, intense, or violent activity or change. After 9/11, the term, when used with initial capital letters, refers to the ground at the epicenter of the World Trade Center attacks.

Guerrilla warfare—The term was invented to describe the tactics Spain used to resist Napoleon, though the tactic itself has been around much longer. Literally, it means "little war." Guerilla warfare features cells and utilizes no front line. The oldest form of asymmetric warfare, guerilla warfare is based on sabotage and ambush with the objective of destabilizing the government through lengthy and low-intensity confrontation.

H

Hacktivist—One who hacks into computer networks to achieve a certain political ai—msometimes only to create disruption to direct attention to a specific cause.

Hamas—A radical Islamic organization which operates primarily in the West Bank and Gaza Strip whose goal is to establish an Islamic Palestinian state in place of Israel. On the one hand, Hamas operates overtly in their capacity as social services deliverers, but its activists have also conducted many attacks, including suicide bombings, against Israeli civilians and military targets.

Hand geometry—A biometric technology that is based on characteristics of the human hand.

Hazard—An inherent physical or chemical characteristic that has the potential for causing harm to people, the environment, or property.

Hazard assessment—The process of evaluating available information about the site to identify potential hazards that might pose a risk to the site characterization team. The hazard assessment results in assigning one of four levels to risk: lower hazard, radiological hazard, high chemical hazard, or high biological hazard.

Hemorrhagic fevers—In general, the term viral hemorrhagic fever is used to describe severe multisystem syndrome wherein the overall vascular system is damaged, and the body becomes unable to regulate itself. These symptoms are often accompanied by hemorrhage; however, the bleeding itself is not usually life-threatening. While some types of hemorrhagic fever viruses can cause relatively mild illnesses.

High-Impact, Low-Frequency (HILF)—HILF evens are occurrences that are relatively unusual, but have the potential to cause catastrophic disruption. Examples include pandemic disease, terrorist attack, and electromagnet pulse.

High-risk target—Any material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

Hizbollah (Hezbollah)—Meaning "The Party of God." One of many terrorist organizations which seek the destruction of Israel and of the United States. They have taken credit for numerous bombings against civilians and have declared that civilian targets are warranted. Hezbollah claims it sees no legitimacy for the existence of Israel, and that their conflict becomes one of legitimacy that is based on religious ideals.

Homeland Security—An agency organized after 9/11. The Office of Homeland Security is at the top of approximately 40 federal agencies charged with protecting the United States against terrorism.

Homicide bombings—A term the White House coined to replace "suicide bombings."

Human-caused hazard—Human-caused hazards are technological hazards and terrorism. They are distinct from natural hazards primarily in that they originated from human activity. Within the military services, the term threat is typically used for human-caused hazard.

I

Improvised explosive device (IED)—A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate conventional military construction (e.g., artillery round), but is normally devised form nonmilitary components.

Incident—A confirmed occurrence that requires response actions to prevent or minimize loss of life or damage to property and/or natural resources. A drinking water contamination incident occurs when the presence of a harmful contaminant has been confirmed.

Infrastructure—The framework of interdependent networks and systems comprising identifiable industries, (including people and procedures),

and distribution capabilities that provide a reliable flow of products and services essential to the defense of economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

Inhalation anthrax—A form of anthrax that is contracted by inhaling anthrax spores. This results in pneumonia, sometimes meningitis, and finally death.

Insider compromise—A person authorized access to a facility (an insider) compromises assets by taking advantage of that accessibility.

Insider threat—An aggressor who is an employee of a business, institution, or agency seeking to compromise a function or the building of the employer.

Intercom system—An electronic system that allows simplex, half-duplex, or full-duplex audio communications.

Interdependency—Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.

Intifada (intifadah)—(alternatively Intifadah, from Arabic "shaking off") The two intifadas are similar in that both were originally characterized by civil disobedience by the Palestinians which escalated into the use of terror. In 1987, following the killing of several Arabs in the Gaza Strip, the first intifada began and went on until 1993. The second intifada began in September 2000, following Ariel Sharon's visit to the Temple Mount.

Intrusion detection sensor—A device that initiates alarm signals by sensing the stimulus, change, or condition for which it was designed.

Intrusion detection system—The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.

ISIS (ISIL) Islamic State of Iraq and the Levant—Islamic extremist terrorist group that formerly controlled territory in Syria, Iraq, Libya, and Nigeria, and others. Known for brutal murders and war crimes.

J

Jersey barrier—A protective concrete barrier initially and still used as a highway divider that now also functions as an expedient method for traffic speed control at entrance gates and to keep vehicles away from buildings.

Jihad—Meaning "struggle." The definition is a subject of vast debate. There are two definitions generally accepted. The first is a struggle against oppression, whether political or religious. The second is the struggle within oneself, or a spiritual struggle.

K

Key resources—As defined in the Homeland Security Act, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

L

LD50—The dose of a substance which kills 50% of those infected.

Laboratory Response Network (LRN)—A network of labs developed by the CDC, APHL, and FBI for the express purpose of dealing with bioterrorism threats, including pathogens and some biotoxins.

Laminated glass—A flat-lite ™ of uniform thickness of two monolithic glass plies boned together with an interlayer material as defined in ASTM Specification C1172. Many different interlayer materials are used in laminated glass.

Laser card—A card technology that uses a laser reflected off of a card for uniquely identifying the card.

Lassa fever—An acute, often fatal, viral disease characterized by high fever, ulcers of the mucous membranes, headaches, and disturbances of the gastrointestinal system.

Layers of Protection—A traditional approach in security engineering using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

Line of sight—Direct observation between two points with the naked dye or hand-held optics.

Line-of-sight sensor—A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.

Links—The means (road, rail, barge, or pipeline) by which a chemical is transported from one node to another.

M

Magnetic lock—An electromagnetic lock that unlocks a door when power is removed.

Magnetic stripe—A card technology that uses a magnetic stripe on the care to encored data used for unique identification of the card.

Microwave motion sensor—An intrusion detection sensor that uses microwave energy to sense movement within the sensor's field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.

Mindset—According to *American Heritage Dictionary*: "1. A fixed mental attitude or disposition that predetermines a person's response to an interpretation of situations; 2. and inclination or a habit." *Merriam Webster's Collegiate Dictionary* (10th ed.) defines it as "1. A mental attitude or inclination; 2. a fixed state of mind." The term dates from 1926.

Mitigation—Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident.

Molotov cocktail—A crude incendiary bomb made of a bottle filled with flammable liquid and fitted with a rag wick.

Monkeypox—The Russian bioweapon program worked with this virus, which is in the same family as smallpox. In June 2003, a spate of human monkeypox cases was reported in the U.S. Midwest. This was the first time that monkeypox was seen in North America, and it was the first time that monkeypox was transferred from animal to human. There was some speculation that it was a bioattack.

Motion detector—An intrusion detection sensor that changes state based on movement in the senor's field of view.

Mustard gas—Blistering agents which cause severe damage to the eyes, internal organs, and respiratory system. Produced for the first time in 1822, mustard gas was not used until World War I. Victims suffered the effects of mustard gas 30 to 40 years after exposure.

N

Narcoterrorism—The view of many counterterrorist experts that there exists an alliance between drug traffickers and political terrorists.

National Pharmaceutical Stockpile—A stock of vaccines and antidotes which are stored at Centers for Disease control in Atlanta, to be used against biological warfare.

Nerve agent—The Nazis used the first nerve agents: insecticides developed into chemical weapons. Some of the better known nerve agents include VX, sarin, soman, and tabun. These agents are used because only a small quantity is necessary to inflict a substantial damage. Nerve agents can be inhaled or can absorb through intact skin.

Network—A group of components that share information or interact with each other in order to perform a function.

Nodes—A facility at which a chemical is produced, store, or consumed.

Non-persistent agent—An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent

Nuclear, biological, or chemical weapons—Also called weapons of mass destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

Nuclear blast—An explosion of any nuclear material which is accompanied by a pressure wave, intense light and heat, and widespread radioactive fallout which can contaminate the air, water, and ground surface for miles around.

O

Opportunity Contaminant—A contaminant that might be readily available in a particular area, even though they may not be highly toxic or infectious or easily dispersed and stable in treated drinking water.

Osama bin Laden (also spelled "Usama")—A native of Saudi Arabia, was born in 1957 the 17th of 24 sons of Saudi Arabian builder Mohammed bin Oud bin Laden, a Yemeni immigrant. Early in his career, he helped the mujahedeen fight the Soviet Union by recruiting Arabs and building facilities. He hated the United States because he viewed the United States as having desecrated holy ground in Saudi Arabia with their presence during the first Gulf War. Expelled from Saudi Arabia in 1991 and from Sudan in 1996, he operated terrorist training camps in Afghanistan. His global network al Qaeda was credited with the attacks on the United States on September 11, 2001, the attack on the USS *Cole* in 2000, and a number of other terrorist attacks. Was killed by U.S. special forces on May 2, 2011.

Owners/operators—Those entities responsible for day-to-day operation and investment in a particular asset or system.

P

Pandemic influenza—Defined by the World Health Organization (WHO) as a global outbreak of influenza, characterized by an emergent strain of the virus, little to no immunity among the general population, rapid and sustained person-to-person transmission, and lack of a vaccine. On June 11, 2009, WHO determined that 2009 H1N1 influenza (also known as "swine flu") had reached pandemic status.

Pan-tilt-zoom (PTZ) camera.—A camera that can move side to side, up and down, and zoom in or out.

Passive infrared motion sensor—A device that detects a change in the thermal energy pattern caused by a moving intruder and initiates an alarm when the change in energy satisfies the detector's alarm criteria.

Passive vehicle barrier—A vehicle barrier that is permanently deployed and does not require response to be effective.

Patch panel—A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.

Pathogen—Any agent which can cause disease.

Pathways—The sequence of nodes and links by which a chemical is produced, transported, and transformed from its initial source to its ultimate consumer.

Perimeter barrier—A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

Persistent agent—An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 mines to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazardous are still a concern, extreme caution should be taken to avoid skin contact as well.

Physical security—The use of barriers and surveillance to protect resources, personnel, and facilities against crime, damage, or unauthorized access.

Plague—The pneumonic plague, which is more likely to be used in connection with terrorism, is naturally carried by rodents and fleas but can be aerosolized and sprayed from crop dusters. A 1970 World Health Organization assessment asserted that, in a worst case scenario, a dissemination of 50 kg in an aerosol over a city of 5 million could result in 150,000 cases of pneumonic plague, 80,000-100,000 of which would require hospitalization, and 36,000 of which would be expected to die.

Planter barrier—A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping cap ability of the individual planter.

Plume—Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.

Political terrorism—Terrorist acts directed at governments and their agents and motivated by political goals (i.e., national liberation).

Polycarbonate glazing—A plastic glazing material with enhanced resistance to ballistics or blast effects.

Potassium iodide—An FDA-approved nonprescription drug for use as a blocking agent to prevent the thyroid gland from absorbing radioactive iodine.

Predetonation screen—A fence that causes an anti-tank round to detonate or prevents it from arming before it reaches its target.

Preparedness—The activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents.

Pressure mat—A mat that generates an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.

Presumptive results—Results of chemical and/or biological field testing that need to be confirmed by further lab analysis. Typically used in reference to the analysis of pathogens.

Prevention—Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervention and stop an occurrence, or to mitigate effects.

Primary asset—An asset that is the ultimate target for compromise by an aggressor.

Prioritization—In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk reduction or mitigation efforts are most needed and to subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection—Actions or measures taken to cover of shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resilience and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems and redundancy, incorporating hazard resistant into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercises, and implementing cyber security measures, among various others.

Protective barriers—Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.

Proximity sensor—An intrusion detection sensor that changes stated based on the close distance or contact of a human to the sensor. These sensors often measure the change in capacitance as a human body enters the measured field.

Psychopathy—A mental disorder, especially an extreme mental disorder marked usually by egocentric and antisocial activity, according to *Webster's*.

Psychopathology—The study of psychological and behavioral dysfunction occurring in mental disorder or in social disorganization, according to *Webster's*.

Psychotic—Of, relating to, or affected with psychosis, which is a fundamental mental derangement (as schizophrenia) characterized by defective or lost contact with reality, according to *Webster's*.

R

Radiation—High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Particles can be either charged alpha or beta particles or neutral neutron or gamma rays.

Recovery—The development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as flexible; evaluate the incident to identify lessons learned and develop initiatives to mitigate the effects of future incidents.

Redundancy—An energy reliability strategy based on the notion that multiple systems provide needed backup if one system fails or cannot meet demand.

Resilience/resiliency—The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. In the context of energy security, resilience is measured into terms of robustness, resourcefulness, and rapid recovery.

Resolution—The level to which video details can be determined in a CCTV scene.

Response—Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic humans needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increasing security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes;

immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Response force—The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordinance disposal team, or a fire department.

Response time—The length of time from the instant an attack is detected to the instant a security force arrives on site.

Retinal pattern—A biometric technology that is based on features of the human eye.

Ricin—A stable toxin easily made from the mash that remains after processed castor beans. At one time, it was used as an oral laxative, castor oil; castor oil causes diarrhea, nausea, vomiting, abdominal cramps, internal bleeding, liver and kidney failure, and circulatory failure. There is no antidote.

Risk—A measure of the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

S

Salmonella—An infection caused by a gram-negative bacillus, a germ of the Salmonella genus. Infection with this bacteria may involve only intestinal tract or may be spread from the intestines to the bloodstream and then to other sites in the body. Symptoms of salmonella enteritis include diarrhea, nausea, fever, and abdominal cramps. Dehydration resulting from the diarrhea can cause death, and the disease could cause meningitis or septicemia. The incubation period is between 8 and 48 hours, while the acute period the illness can hang on for 1 to 2 weeks.

Sarin—A colorless, odorless gas. With a lethal dose of .5 mg (a pinprick-sized droplet), it is 26 times more deadly than cyanide gas. Because the vapor is heavier than air, it hovers close to the ground. Sarin degrades quickly in humid weather, but sarin's life expectancy increases as temperature gets higher, regardless of how humid it is.

Sector—A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 critical infrastructures sectors, identified by the criteria set forth in HSPD-7. This number has been condensed to 14 by Presidential Directive 21.

Security console—Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.

Semi-isolated fenced perimeters—Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence and where the general public or other personnel seldom have reason to be in the area.

Sentinel laboratory—An LRN lab that reports unusual results that might indicate a possible outbreak, and refers specimens that may contain select biological agents in reference labs within the LRN.

Shielded wire—Wire with a conductive wrap used to mitigate electromagnetic emanations.

Situational awareness—An understanding of the current environment and the ability to accurately anticipate future problems in order to respond effectively.

Sleeper cell—A small terrorist cell which keeps itself undetected until such time as they can "awaken" and cause havoc.

Smallpox—The first biological weapon, used during the 18th century, smallpox killed 300 million people in the 19th century. There is no specific treatment for smallpox disease, and the only prevention is vaccination. This currently poses a problem, since the vaccine was discontinued in 1970 and the WHO declared smallpox eradicated. Incubation is 7 to 17 days, during which the carrier is not contagious. 30% of people exposed are infected, and it has a 30% mortality rate.

Smart card—A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.

Smart grid—The electric delivery network, from electrical generation to end-use customer, integrated with the latest advances in digital and information technology to improve customer, integrate with the latest advances in digital and information technology to improve electric-system reliability, security, and efficiency.

Sociopathic—Of, relating to, or characterized by asocial or antisocial behavior or a psychopathic (q.v.) personality, according to *Webster's*.

Specific threat—Known or postulated aggressor activity focused on targeting a particular asset.

Spore—An asexual, usually single-celled reproductive body of plants such as fungi, mosses or ferns; a microorganism, as a bacterium, in a resting or dormant state.

System—Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

T

Taut wire sensor—An intrusion detection sensor using a column of uniformly spaced horizontal wires, security anchored at each end and stretched taut. Each wire is attached to a sensor to indicated movement of the wire.

Terrorism—Premeditated threat or act of violence against non-combatant persons, property, and environmental or economic targets to induce fear, intimate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives.

Terrorist group—A group which practices or has significant elements which are involved in terrorism.

Thermally tempered glass (TTG)—Glass that is heat-treated to have a higher tensile strength and resistance to blast pressures, although with a greater susceptibility to airborne debris.

Threat—An indication that a harmful incident, such as contamination of the drinking water supply, may have occurred. The threat may be direct, such as a verbal or written threat, or circumstantial, such as a security breach or unusual water quality.

Threat analysis—A continual process of compiling and examining all available information concerning potential threats and human-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.

Toxin—A poisonous substance produced by living organisms capable of causing disease when introduced into the body tissues.

Tularemia—An infectious disease caused by a hardy bacterium *Francisella tularensis*, found in animals, particularly especially rabbits, hares, and rodents. Symptoms depend upon how the person was exposed to tularemia but can include difficulty breathing, chest pain, bloody sputum, swollen and painful lymph glands, ulcers on the mouth or skin, swollen and painful eyes, and sore throat. Symptoms usually appear from 3 to 5 days after exposures but sometimes will take up to two weeks. Tularemia is not spread from person to person, so people who have it need not be isolated.

U

Unobstructed space—Space around an inhabited building without obstruction large enough to conceal explosive devices 150 mm (6 inches) or great in height.

Unshielded wire—Wire that does not have a conductive wrap.

V

Value proposition—A statement that outlines the national and homeland security interest in protecting the nation's critical infrastructure and articulates

the benefits gain by all critical infrastructure partners through the risk management framework and public-private partnership described in the NIPP.

Vector—An organism which carries germs from one host to another.

Vesicle—A blister filled with fluid.

Vibration sensor—An intrusion detection sensor that changes state when vibration is present.

Video analytics—The use of computer software in surveillance to automatically identify things of interest such as behavior, objects, or attitude, without an operator having to view the video.

Video motion detection—Motion detection technology that looks for changes in the pixels of a video image.

Voice recognition—A biometric technology that is based on nuances of the human voice.

Volumetric motion response—An interior intrusion detection sensor that is designed to sense aggressor motion within a protected space.

Vulnerability—A physical feature or operational attribute that renders an entity open to exploitations or susceptible to a given hazard.

W

Weapons of mass destruction (WMD)—According to the National Defense Authorization Act: Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of

- toxic or poisonous chemicals or their precursors
- a disease organism
- radiation or radioactivity

X

Xenophobia—Irrational fear of strangers or those who are different from oneself.

Z

Zyklon b—A form of hydrogen cyanide. Symptoms of inhalation include increased respiratory rate, restlessness, headache, and giddiness followed later by convulsions, vomiting, respiratory failure and unconsciousness. Used in the Nazi gas chambers in WWII.

Index

About the Author

Frank R. Spellman, PhD, is a retired assistant professor of environmental health at Old Dominion University, Norfolk, Virginia, and the author of more than 110 books covering topics ranging from homeland security to all areas of environmental science and occupational health. Many of his texts are readily available online, and several have been adopted for classroom use at major universities throughout the United States, Canada, Europe, and Russia; two have been translated into Spanish for South American markets. Dr. Spellman has been cited in more than 450 publications. He serves as a professional expert witness for three law groups and as an incident/accident investigator for the U.S. Department of Justice and a Northern Virginia law firm. In addition, he consults on homeland security vulnerability assessments for critical infrastructures including water/wastewater facilities nationwide and conducts pre-Occupational Safety and Health Administration (OSHA)/Environmental Protection Agency EPA audits throughout the country. Dr. Spellman receives frequent requests to coauthor with well-recognized experts in several scientific fields; for example, he is a contributing author of the prestigious text *The Engineering Handbook*, 2nd ed. (CRC Press). Dr. Spellman lectures on sewage treatment, water treatment, biosolids and homeland security, and lectures and safety topics throughout the country and teaches water/wastewater operator short courses at Virginia Tech (Blacksburg, Virginia). He holds a BA, in public administration, a BS in business management, an MBA, and an MS and PhD in environmental engineering.