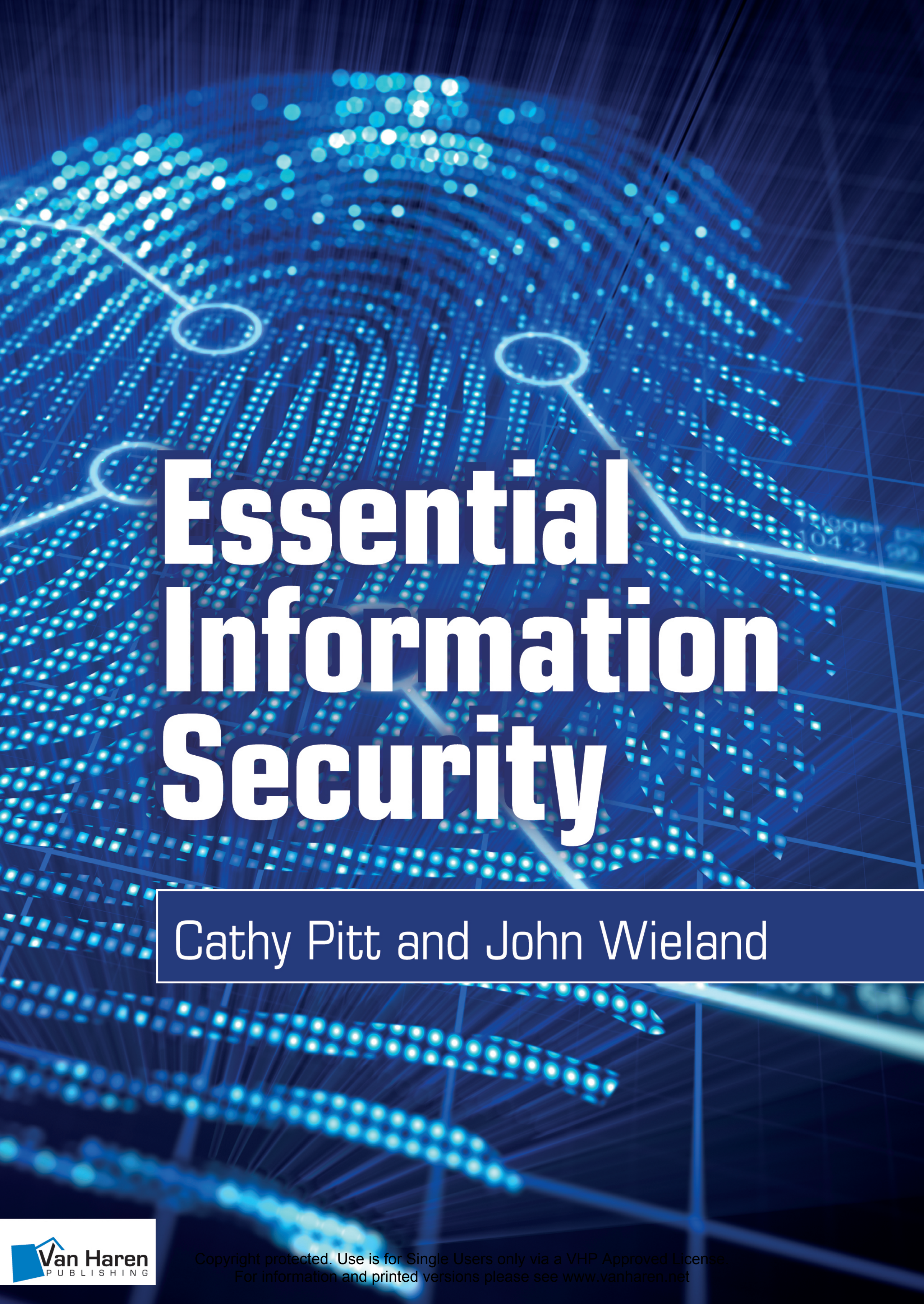


Essential Information Security

Cathy Pitt and John Wieland

Van Haren
PUBLISHING

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Essential Information Security

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business management and
- Project management

Van Haren Publishing offers a wide collection of whitepapers, templates, free e-books, trainer materials etc. in the **Van Haren Publishing Knowledge Base**: www.vanharen.net for more details.

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CATS CM®
CMMI®
CoBIT
e-CF
Frameworx
ISO 17799
ISO 27001/27002
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL®
MOF
MSF
SABSA

Architecture (Enterprise and IT)

ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Business Management

BiSL®
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SAP
SixSigma
SOX
SqEME®

Project, Program and Risk Management

A4-Projectmanagement
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP™
P3O®
PMBOK® Guide
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Essential Information Security

Van Haren
PUBLISHING

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Colophon

Title:	Essential Information Security
Authors:	Cathy Pitt and John Wieland
Texteditor:	Jane Chittenden
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Hard copy:	978 90 8753 736 4
ISBN eBook:	978 90 8753 771 5
Edition:	First edition, first impression, August 2013
Layout and DTP:	CO2 Premedia, Amersfoort
Copyright:	© Van Haren Publishing 2013

For further information about Van Haren Publishing, please send an e-mail to: info@vanharen.net

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by the publisher.

Although this edition has been composed with the utmost care, neither the author(s) nor the publisher can accept any responsibility whatsoever for damages caused by possible errors and/or imperfections in this edition.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Acknowledgement

Information is fundamental to all that we do in the modern world, in our place of work and at home.

- But who is responsible for keeping this information secure?
- What type of information needs securing and why?
- How can we make sure that critical information is kept secure?

You may be surprised to hear that the organisation you work for also shares the same concerns as you, in keeping certain information confidential and secure.

"Information Security Essentials" (ISE) has been written and structured in such a way, it is easily understood by IT professionals and non IT professionals alike. It is one of the most well rounded books I have come across and is delivered in a light-hearted way; but is critical reading for even the most seasoned security professional. With easy to follow real-life anecdotes, it provides "the why" that will help to drive home the importance of having to follow or enforce a solid security policy. Whilst the focus may be on the IT professional, the book will also appeal to anybody who uses IT in the office or indeed at home – to protect your family.

This book has been used as initial source material by Hewlett Packard for a 3 day training course (HL945s[1]) that has been certified by EXIN and APMG as a "foundation" to the ISO/IEC 27001 standard for information security. An additional two day course "ISE plus" will also qualify participants to take the CISMP[2] exam from the BCS.

The book is also being considered by an industry consortium[3] whose aim is to create a common understanding of information security and to develop a single source entry level certification that will be acknowledged worldwide.

In closing, Cathy and John have done a fantastic job in putting together a book that is easily understood, with examples that can be applied in the data centre or office and that are equally relevant in the home. In my opinion it is essential reading for the IT professional in whatever field he or she may work.

John F McDermott F.S.M.
EMEA Education Portfolio Manager
ITSM/ITIL and Information Security, Hewlett Packard

[1] HP Information Security Essentials Training Course

[2] Certificate in Information Security Management Principles

[3] Consortium members currently include: HP, CA, QT&C, EXIN, APMG, BCS, itSMF UK, The Open Group and Van Haren Publishing. Other major technology vendors are expected to be announced soon

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Dedication

We are standing on the shoulders of those who sacrificed to shape us into who we are today; family, friends, those who have pushed us to be better and to achieve more. Moms and Dads, here or gone on ahead, we love you and miss you and appreciate more than words can say, all that you gave us. Thank you. *And I love you too, Dad.*

Cathy Pitt

About this book

You become an expert in data security not by accepting the status quo, but by probing the vulnerabilities and asking awkward questions. This book gives people the knowledge to ask the right questions (and probably the courage, as well). It also helps them to question the answers they're given. If you're new to Internet security, start with this book. If you're an old hand, you probably already have a copy.

Dermot Tynan, former Technical Director for Security Products at AltaVista,
and former CEO of Copperfasten/SpamTitan

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Contents

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Introduction

According to IBM, we create 2.5 quintillion bytes of data every single day.[1] Processed data becomes information and the information that we acquire, create, use, and sell is vital to our business. Imagine suddenly not having that customer list, or years of research and development that the company has invested in. Imagine losing that database of credit card numbers, or private patient records. Arguably, information is one of your company's most valuable assets, and it is critical to the success of the business that it is properly secured.

That is where you come in.

For years, John and I have been talking about the need for a book written specifically for the person who comes into work one day as a system administrator or a project leader and goes home in the evening as "the security expert."

We know you. We have worked with you many times over the years. We recognize the pressure you are feeling, because we hear it in your voice when you ask for help. You are afraid to slip and show your lack of experience, or maybe you fear giving away a little too much of the self-doubt you are feeling because of the weight of your new responsibility in an area that is new and vast and exciting and terrifying. We know you may be feeling a bit overwhelmed trying to figure out where to begin. So we wrote this book for you.

And in case you are wondering, we did not write this book for *dummies*. We wrote it for smart people (like you) who have found themselves in a tough position without the appropriate training or resources. We will not talk down to you, but we will not use six syllables when three will do, and we will not go into such tremendous detail that the fundamental message is lost.

We wrote this book as your starting point, not to impress our friends or neighbors or those who have lost sight of what it takes to do the job.

So why *did* we write the book?

My experience in information security, which includes almost two decades as senior security consultant and strategist, chief security officer, distinguished technologist, team leader for risk assessments, and security training developer and instructor to more than 1,000 security experts, has taught me that people just want to learn so that they can be better at what they do. Teaching college courses to working adults showed

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

me that the grades and the degrees are important, but going into work the next day with something productive and useful to share is *priceless*.

As a widely recognized expert in network security, and on a relatively short list of dual Cisco Certified Internetwork Experts (John has CCIEs in both VoIP and Security), John can speak authoritatively about the days when the first commercially available firewall started to sell and about the phone calls that would come in from panicked system administrators who were not only new to the concept of a firewall but also to the concept of the *Internet*. It was a learning experience for all of us.

Today, what used to take up the same floor space as a washing machine fits on the head of a pin and lives in a cloud. More than 6 billion people carry mainframes[2] in their pockets,[3] in the form of mobile phones, and use them not only to calculate complex mathematical equations but also to tell their 853 friends what their plans are after work.

As security practitioners, we work in the real world with real people like you and have for more than 70 years between the two of us. We have helped our customers—from small businesses to large enterprises— to discover and understand their security risks and to develop cost-effective, risk-based security strategies to minimize their vulnerability.

Over the years, we've made a simple observation that drives what we do: security is not about how much money you spend on "stuff." Security is about how well you have anticipated the worst case scenario and have arranged to avoid it.

Security is about training and empowering the people around you to help you to put up a strong defense. It is about getting senior management support and working together as a team, from the top down and from the bottom up. And these are the things that we discuss in this book.

We have looked at information security from many angles but, despite that, we are not embarrassed to admit that there is still so much to learn and only so many hours in a day. So we feel your pain.

We wrote this book for you so that you can begin to add value to your company's information security posture when you go into work tomorrow or the next day.

Take a minute and breathe. We have all been there. From here on out, this is just you and us, and we are going to help you to succeed.

Cathy and John

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

> "I speak to everyone in the same way, whether he is the garbage man or the president of the university."[4]
>
> **Albert Einstein**

So what is the book about?

Information security. It is about preserving your data, keeping private data private, making sure only the people who are authorized to access the data can, making sure your data is always there, always the way you left it, keeping your secrets secret, making sure you trust your sources, and complying with government and industry regulations and standards.

It is about managing your risks and keeping the business going when it all goes south.

But the very scary reality of the business world today is that there are just not enough IT security experts to go around, with the most extreme shortages being in cloud security, mobile device security, and network security—all areas that we cover in this book!

This talent shortage puts a tremendous burden on the people who are put into a security administrator or manager role in their companies simply because they were really good at what they were already doing and senior management decided it was time to think about "getting secure."

Unfortunately, without the requisite knowledge of information security and the understanding of what makes a good security strategy good and a bad one bad, these new security managers are taking on a responsibility they may not fully understand and are putting themselves and their companies at risk.

At the same time, the bad guys keep getting smarter and bolder, more organized and better funded, and their random attacks are getting more focused and deliberate.

We all know that you don't have an unlimited security budget and that every dollar counts. So, before you head out to your local "Security Stuff Store" with your entire annual security budget in your pocket, we want to make you aware of all of the free stuff that you should be doing first. We will talk about your processes, your training strategy, your policies, and your contingency plans. We will help you to look at your risks in ways that you may not have considered, and we will help you to maximize the effectiveness of the "stuff" that you do need to buy.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

> "While the global economic slowdown has been putting pressure on IT budgets, security is expected to remain a priority through 2016, according to Gartner, Inc. Worldwide spending on security is expected to rise to $60 billion in 2012, up 8.4 percent from $55 billion in 2011. Gartner expects this trajectory to continue, reaching $86 billion in 2016."[5]
>
> **Gartner Newsroom**

By any other name

Throughout the book, we use the terms *security manager* and *IT security manager* pretty freely and pretty interchangeably, though one could make the case that these are two different terms and describe two different roles. The truth is, in our experience working with companies that want us to help them preserve the confidentiality, availability, and integrity (referred to as *CIA*) of the sensitive information in their care, there is usually (hopefully) a security person who can have any one of the following titles: IT security manager, information security manager, security manager, chief security officer, director of security, director of information security, or director of IT security. Sometimes the title of the person responsible for preserving CIA of sensitive data is the *risk manager.*

But the title that the company has chosen to hire their information security expert under is not hard and fast from one company to the next; there are no rules.

Small and medium-sized companies tend to be even more fluid in their use of job definitions and job titles, because they want the one person who can fulfill all of their information security needs. And, no matter what the official title is, that person is forever after known to all as "the security expert" anyway.

But words are important, and we recognize that because we just wrote a book and had to use a lot of them.

In this case, our choice and use of these particular job titles may lead someone to believe that this book is not appropriate for them. Let us clarify it right here and now so that we can get on to the important stuff:

You know this book is for you if:

- You have been tasked with ensuring that your company's information is always as private as it should be, always trustworthy, and always there when you need it.
- Someone in senior management called you into their office last week, shook your hand, and told you that you are now in charge of security.
- Your company has recently been hacked (or is being hacked as we speak), and everyone is looking at you to do something about it.
- You think that IT/information security is "where it's at" and want to start with a good foundation without getting buried up to your neck in the concrete, hoping that, someday soon, you too may rightly be called "the security expert."

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

- You just want to know more about information security because it is important, no matter who you are or what it says on your business card.

So, as you read through the book, when we use the word “you” or refer to “the security manager,” we really mean “you” the person reading the book, regardless of your official job title. And when we say “we,” it means Cathy and John, or it may mean the collective “we” who are all in this together, just trying to get better at this security stuff everyday to protect the company castle and the company treasure from the bad guys.

Chapter Overview

Here’s a preview of what lies ahead.

Chapter 1: Setting a Foundation—We begin with an introduction to information security key concepts, such as access control and identity management, including authentication and authorization. We discuss confidentiality, integrity, and availability, and we define that triad as the basis for your security management efforts.

Chapter 2: A Peek into the Underbelly of Client/Server Communications—Here, we stray into the technical realm, at a high level—just enough to get your feet wet—and introduce you to the client/server relationship, TCP/IP, and Internet addressing. We discuss how server listener ports—those open doors that the client and server use to communicate—are a key point of attack or threat vector into your environment. And we talk about a few of the client/server applications that make the Internet function, such as the domain name service (DNS) and the address resolution protocol (ARP).

Chapter 3: A Most Important Ten Percent: Security Technologies—Firewalls, intrusion prevention devices (IPSs), virtual private networks (VPNs), and several other security technologies, including data loss prevention (DLP), network access control (NAC), and cryptography, are the focus of this chapter.

Chapter 4: Stronger Security through Better Administration—This is where you learn that security really is not just all about the things we talked about in Chapter 3! We discuss processes, programs, plans, policies, and procedures, and putting all of these into the proper perspective.

Chapter 5: Physical Security: CIA Beyond the Traditional—Information security is also about keeping people away from the places where your information lives. In this chapter, we introduce the other things that you can touch to help safeguard the CIA of your valuable information assets. Physical security controls include fencing, lights, guards, dogs, guards with dogs and, beyond the obvious, we introduce man traps, piggy backing, ID badges, fire suppression, and several other deterrents that you can deploy in your environment. This is a place where information security management and security management may diverge, depending on your company.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Chapter 6: Moving to the Cloud Without Giving Away the Farm—In this chapter, we introduce cloud computing, along with the security advantages and disadvantages of moving your sensitive information to a cloud provider—"gracefully losing control while maintaining accountability."[6] This chapter will show you when and why you might choose to move some or all of your information to a cloud provider. But we also reinforce the security risks and the idea that the data owner is still ultimately responsible for ensuring that the data is safe.

Chapter 7: Securing the "Bring Your Own Whatever" Environment—Chapter 7 presents IT consumerization in the workplace, how society's social networking obsession is driving the way business looks at technology, and why you cannot simply close the door on mobile devices and social networking in the office. As we read through several eye-opening statistics, it becomes clear that bring your own device (BYOD) and social media, combined with cloud services, will continue to dominate the security discussion (and your time) into the future.

Chapter 8: Putting It All Together—This chapter provides an opportunity to stop and refresh what we have learned and to begin to think of all the pieces and parts holistically. Keeping your information safe is going to take a unified approach, not a rag-tag array of unrelated security "things" tossed into hat. Think of this chapter as your seventh-inning stretch.[7]

Chapter 9: Taking Stock of Your Risks—In this chapter, we introduce risk management as an ongoing program and not just as a concept. We present the business impact analysis (BIA) as the process that helps you to determine your most critical information assets and that is, therefore, an important driver of everything you do as the information security manager.

Chapter 10: Keeping the Business Going When It All Goes South—We discuss another very important program that focuses on business resilience and recovery. Bad things happen, and your business will survive or fail depending on how quickly and cost effectively it recovers. You will begin to look at information security in a whole new light—as a business differentiator.

Chapter 11: Put It in Writing: Security Policies — Your Strategy in Black and White—Throughout the book, we talk about security strategy and security policies and, in this chapter, we identify the roles and relationships between strategy and policy. We provide details of what makes a good security policy good, and we discuss a few of the must-have policies.

Chapter 12: Hacked, Cracked, and Attacked—Statistically, your company has either already been hacked, is currently being hacked, or will likely be hacked by sometime around noon tomorrow. This is the reality-check chapter where we talk about many of the ways that bad people really are out to get you. We provide some anecdotal evidence of why and where your company is vulnerable, and we share some "low-hanging-fruit" things that you can do to minimize your risks.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Chapter 13: Summary and Next Steps—Where do you go from here? In Chapter 13, we bring it all down to something that you can wrap your arms around and apply to your own unique company needs. And we outline some next steps to get you started.

Appendix A—We summarize the key terms that we have introduced throughout the book.

Appendix B—You may be surprised when you read about some of the things that you have never even considered when contemplating your information security risks.

Appendix C—Knowing what a firewall is and what it does is not necessarily the same as knowing where it will provide the most bang for the buck in your network design. We have provided a few simple example topologies designed with security in mind.

A Few Final Things You Should Know Before We Get Started

We did not write this book to teach you how to pass a security certification test. It is not a study guide; it is a learning guide. We are focused on you, at work, facing real challenges—not you, in a room, sweating over "A," "B," "C," or "D."

We talk about the current state of information security, the challenges and the threats, and who is winning this cyber-brawl so that you know why your role is so critical and fully appreciate what you should be worried about.

We explain some common security technologies in real-people terms and at a foundational level. We want to help you to take a closer look at the technology investments your company has already made and to consider whether there may be ways to put your technology "stuff" to better use. But this is not intended to be a technical manual, which is good, considering that information security is only 10 percent about technology.

In this book, we introduce you to information security best practices and strategies, programs and products, so you can begin the processes of assessing your risks and building a better defense. And when you find yourself at the front and center of the threats and assaults that confront your company on a daily basis, you need real-world solutions, fast. It would be good to know where to begin.

And one last thing before we get started: if security was the Empire State Building, this book would be a walk around the lobby. Information security is vast, and deep, and broad, and wide and there is no one book or resource or blog or class that will give you everything you will ever need to know in one helping.

This is the beginning.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

References

1 “What is Big Data?” Big Data at the Speed of Business. http://www-01.ibm.com/software/data/bigdata/

2 “Super Computers Vs Mobile Phones.” Walking Randomly. June 2, 2010. http://www.walkingrandomly.com/?p=2684

3 “Global mobile statistics 2012 Part A: Mobile subscribers; handset market share; mobile operators.” mobiThinking. June 2012. http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

4 Goodreads, “Albert Einstein > Quotes,” http://www.goodreads.com/author/quotes/9810/Albert_Einstein. “I speak to everyone in the same way, whether he is the garbage man or the president of the university”

5 “Gartner Says Worldwide Security Infrastructure Market Will Grow 8.4 Percent.” Gartner Newsroom. September 13, 2012. http://www.gartner.com/it/page.jsp?id=2156915

6 Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. December 2009. https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

7 Seventh-inning stretch. http://en.wikipedia.org/wiki/Seventh-inning_stretch

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

1 Setting a Foundation

> "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us"[1].
>
> **Anonymous**

Repeat after me, "There are mean people out there who are very smart at computer stuff and they really are out to get me." It's true. They are generally smart and motivated and possibly well-funded and never tire of the game. They may be the run-of-the-mill bullies with cyber-smarts, or government-sponsored paid cyber-assassins. They may simply be thieves looking to steal something of value, or self-proclaimed heroes looking to right something that *they* deem wrong. They may work as individuals or as large global collectives. They may or may not actually hate you or your company or organization—they may not even know you or be targeting you specifically—but they enjoy watching you struggle as you attempt to fight off their malicious, aggressive violations of your cyberspace. "The harbingers of judgment, we laugh in the face of tragedy; we mock those in pain. We ruin the lives of other people simply because we can."[2] The taunts are nonstop. The threat is real. Hackers and *hactivists* have garnered a lot of attention in the media over the past few years with their very public masked-face protests, cyber-blackmail and attacks on those with whom they disagree. They can pose a serious threat to your business, and maybe they really *are* out to get you. And they may not even be the biggest problem you have.

Threats to your business environment come from people, but they also come from nature and technology. They are not always an intentional act, and they are not always easy to defend against. Your role as the security manager is to defend your business against threats, regardless of their form.

Key Terms

- **Asset** is something of value (We will talk more about what *value* really means later.)
- **Vulnerability** is a weakness that creates an opportunity for something bad to happen
- **Threat** is something that can harm the asset. A bad thing.
- **Threat agent (source)** is where the threat comes from
- **Likelihood (probability)** is what the chances are that a bad thing will actually happen
- **Control (safeguard, countermeasure)** is something to stop the threat and protect the asset

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

To get started, let us define a few key information security words that we will use. We will do this throughout the book when we introduce key terms or concepts so you do not spend a lot of time going to the glossary to figure out what we are talking about!

Asset

An asset is something of value to your business. When we talk about Information Security, we can generally narrow the asset discussion to mean *information assets*, *data* and those things that support the data through all phases of the data lifecycle including creation, processing, storing, sharing and destruction. These data-supporting things can include computers, buildings, people (People are assets? Really? Yup!), etc. And while you may be wondering how you would go about determining the actual dollar value of your data, it can be done and in fact, it's a critical step in developing your security strategy. We will talk about how to apply a real cost to data in Chapter 9: Taking Stock of Your Risks. In the meantime, if you could sum up your primary responsibility as information security manager, it would be to safeguard your company's *information assets.*

Vulnerability

This one is fairly self-explanatory on the surface: a weakness, a hole, a gap that allows the bad thing in. When we talk about information, *vulnerabilities* most often exist in our handling of the data. An easy example of vulnerability is a hole that we create when we use weak passwords, which makes it easier for a potential hacker to gain unauthorized access to our systems. A *vulnerability* provides the *opportunity* for a *threat* to harm our *asset.*

Threat and Threat Agents

Threats can be man-made, or come from nature or from technology. The threat-agent is the person or thing that can, or attempts to, carry out the threat. The Open Web Application Security Project (OWASP) defines a threat agent this way: "Threat Agent = Capabilities + Intentions + Past Activities,"[3] but I would not discount someone as a threat agent just because this is their first attempt! To keep it simple, a worm is a threat, and the person who created the worm and sent it to you in email is the threat agent. *Threat agents* exploit a *vulnerability* to carry out the *threat* against the *asset.*

Likelihood (probability)

This defines the chances (the odds, the probability) that the threat agent will be successful. Now if you are a math person, you would point out that the word, "probability," is actually a statistical term that describes "the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes,"[4] And when we get into Chapter 9: Taking Stock of Your Risks and talk about risk analysis, the level of exactness becomes very important. For now, we are using the less precise definition: how likely is it, given all of the controls we have, that this *threat agent* will be successful and harm our assets? What is the *likelihood* that the *threat agent* will successfully exploit a *vulnerability* to carry out the *threat* against the *asset*?

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Controls (safeguards, countermeasures)
Controls are the things (processes, technology, physical objects, etc.) that you put in place to minimize the likelihood that the threat agent can harm your assets. Firewalls, a change management process, applying patches, a guard dog with big foamy teeth—all of these are examples of controls that you might use to protect your assets. As you can see, some will cost more than others, some may be more complicated to deploy, some will probably do a better job than others and some may even have fleas! Because this is such a key aspect of your job as the security manager, we are going to spend a lot of time discussing how you decide which controls to deploy. *Controls* should minimize the likelihood that the *threat agent* will successfully exploit a *vulnerability* to carry out the *threat* against the *asset*.

In addition to becoming very familiar with the common security terms and concepts, it is also important that you understand some of the key drivers of your security program. Sure, it is obvious that it is all about keeping everything important to your business (assets) safe from everything dangerous to your assets (threats), but there are a lot of influencers and components that we must understand before we get to the juicy stuff. These are the critical foundations that will help you to build a strong security program developed for your unique needs.

Getting into the Security Frame of Mind

There are more than a few companies in business today that do not have an information security strategy. We know them because we often have the opportunity to work with them after they have experienced a security breach, or failed a compliance audit. For some companies, it is just too much of an effort for them to build a security strategy and it never seems to be a business priority until it is too late. For others, they do not know where to begin. Still others just do not see the need to invest the time, money or people in the effort because, after all, who would want to attack them?

As the security manager for your company, you are going to do things differently. You understand that a strong, well-developed security strategy is critical to your company's success. That is why you are here now, with us, building the foundation that will help you to be successful.

Why should be worry about security?

Seriously, why worry about this stuff? Besides being a nuisance to you and your staff, security breaches can put you out of business. The loss or compromise of sensitive information can hurt productivity, impact customer loyalty, result in costly litigation, damage your reputation, reduce your ability to compete, and cause a loss in revenue or even the loss of the entire business.

If that is not enough, there is a good chance that you have some government or industry-imposed compliance requirements intended to safeguard specific types of sensitive data (HIPAA for private patient information, PCI for private payment

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

card information, FERPA for private student information, etc.) You'll notice that a common theme here is: *information privacy*. While noncompliance can result in severe penalties or loss of privileges, being breached is much worse. In 2012, the Blue Cross Blue Shield of Tennessee "agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules" after allegedly losing more than 1 million private patient records due to the theft of 57 unencrypted hard drives[5]. Not being compliant is one thing, but being breached is a whole other story.

Most countries have developed privacy laws intended to protect personal information, and the penalties for violating those laws vary greatly. Of course, given that many businesses have a global presence these days, understanding the laws in each country where business is conducted becomes a challenging, but necessary, continuous effort. This would be a good time to start a to-do list.

But do not let your pursuit of compliance lead you into complacency. Despite all of these government and industry efforts to ensure privacy by enforcing strong security, being compliant does *not* mean you are secure. This one is worth repeating: ***Being compliant does not mean you are secure.*** There are many examples of companies that had recently passed compliance reviews only to be breached a short time later.

> "We certainly didn't understand the limitations of PCI and the entire assessment process. PCI compliance doesn't mean secure. We and others were declared PCI compliant shortly before the intrusions."[6]
>
> **Heartland CEO, Robert Carr**

If you feel strongly that you are secure because you are compliant, do a Google search on "Heartland breach" and heed the words of Heartland CEO Robert Carr who said, "Anyone that thinks they're not going to be breached is being naive."[7] Enough said.

Who is responsible?

Who really owns the security strategy at your company? The board of directors and the executives -upper management- owns the company security strategy. They own final approval, hiring the right people (like you!), getting the word out corporate-wide, and generating (and mandating) support. After all, they own the budget and are ultimately responsible for failures. *Security governance*, as it is referred to, is about building and implementing a strong, top-down security program that has complete support from upper management and is applied equally across the entire company. If the big guys do not support your program, it is time to do something different with your life.

This is a good time to share a real life story about someone we worked with recently. To protect the innocent (and the guilty) we will call it, "The Story of Marcello." Marcello was a strong security advocate as the company's Chief Security Officer (CSO). He was well equipped to do an excellent job, motivated, and passionate about

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

the business and keeping it secure. His efforts to assess the company's vulnerabilities uncovered several areas of concern that he addressed with management, only to be rebuked. One of his biggest concerns was that the engineering group that maintained the company's home-grown business application had complete access to its customer database and used that live data for test purposes. Marcello's challenge was that he reported to the same director as the manager of the engineering group. As a peer, Marcello had no influence over the engineering manager, and the director had no desire to step into the middle of a rift between two of his direct reports. Marcello had no management support despite the egregious breach of security best practices. Despite his CSO title, he had no power, no influence, no support, and no chance of success. Our advice to Marcello: run away.

If your management does not actively, aggressively and passionately support you and your security expertise, you should consider a possible alternative approach or another company. You cannot succeed if you attempt to implement your strategy bottom up. And you will not succeed if you are fighting an uphill battle. Run away.

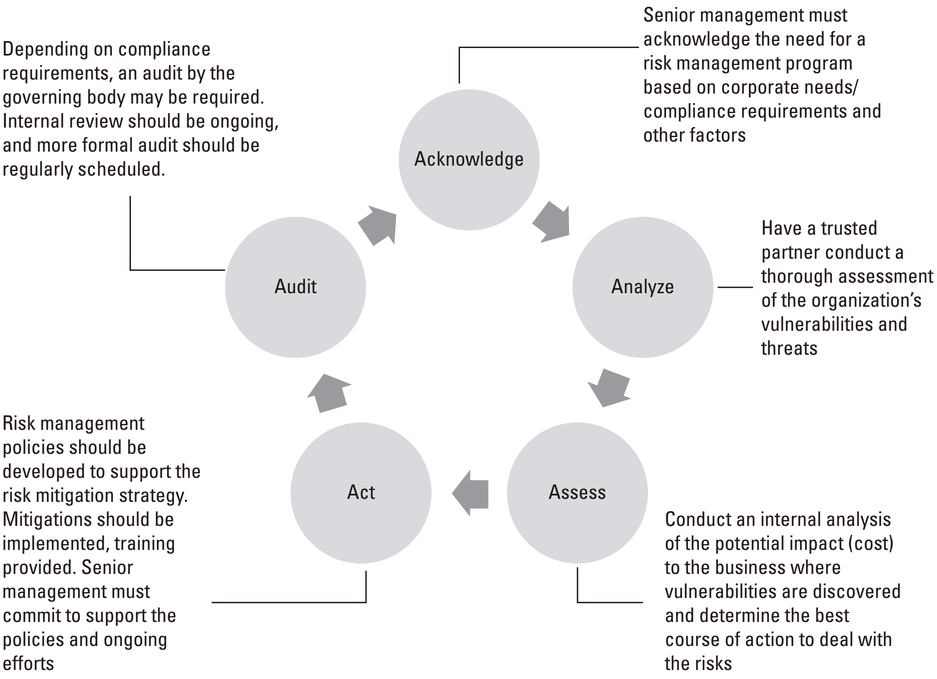
Developing a Security Strategy

You may be asking "What exactly *is* a security strategy and how do I get one?" Your *security strategy* is the foundation for safeguarding your company's assets. Your *security policy* is the document that reflects the security strategy in simple, uncomplicated directives that everyone can understand and support. The security strategy should be developed with leadership from upper management and based on your company's unique business needs. It defines how you plan to deal with risks to preserve the confidentiality, integrity and availability (CIA) of your valuable information assets. (We will talk about CIA in just a few minutes.) Once you have determined what things are the most important to the continued success of your business (based on executive input), you must then determine the risks to the continued availability/reliability of those things. Next, you determine how bad those risks are and how bad things might be if data or access to the data were to become compromised in some way, and then decide how you will minimize the chances of bad things happening and the impact to the business if those bad things happen. Finally, you put that strategy into a security policy that you share company-wide with full support from upper management. Figure 1-1 provides a general overview of the risk management lifecycle. We will expand on the lifecycle and discuss risk management in great detail in Chapter 9: Taking Stock of Your Risks.

Really, this is not a quick project that you jump into without a lot of effort from many stakeholders. A well-conceived, well-developed security strategy is critical to your success as the Security Manager.

If you do not know which assets the business considers to be critical, you do not know where to allocate your scare resources: people, time, and money. If you spend unwisely, you may be leaving yourself open to a breach. Without going through the efforts to analyze and understand the potential impact from a failure in your company's security, you could just as easily overspend as underspend. There is also

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net



Senior management must acknowledge the need for a risk management program based on corporate needs/ compliance requirements and other factors

Have a trusted partner conduct a thorough assessment of the organization's vulnerabilities and threats

Conduct an internal analysis of the potential impact (cost) to the business where vulnerabilities are discovered and determine the best course of action to deal with the risks

Risk management policies should be developed to support the risk mitigation strategy. Mitigations should be implemented, training provided. Senior management must commit to support the policies and ongoing efforts

Depending on compliance requirements, an audit by the governing body may be required. Internal review should be ongoing, and more formal audit should be regularly scheduled.

Figure 1-1. General Risk Management Framework

no guarantee that you have sufficiently addressed the real risks or safeguarded your most critical assets.

And here is another point to consider: regardless of your particular environment, compliance requirements, business segment, company size, financial holdings, or number of employees, a security strategy is a requirement for success. ***A well-developed security strategy is a business differentiator***. Whether you run your own data center or rely on a public cloud, you need to understand the risks and develop a strategy to deal with those risks. What is the message here? Do not avoid this effort. It must be done and done right.

> "Those who do not manage their risks to prevent business process downtime will have difficulty competing against those who do."[8]
>
> **Gartner Real Time Enterprise Business Continuity & Availability**

Staying the course

"And what if I'm just too busy? Can I just skip to the chase?" It is time for another real-life story. On one of our very first security assessments, we visited a company that recently experienced a security breach and subsequently invested thousands of dollars in technology. We guessed that their new strategy was "increased security through increased spending," because they spared no expense in buying all of the bells and

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

whistles that money could buy. The CSO was confident in his strategy and anxious for our assessment team to heap praise on his efforts. Sadly, in less than a half day of our assessment, we obtained some of the company's most sensitive client documents from one of the most secure areas in the building. And this was without re-enacting a scene from *Mission: Impossible*, dressing in black tights or rappelling from the rooftop! He was shocked (and embarrassed!) How could this have happened with all of his newly-installed advanced security? Well, first, he failed to fully recognize what constituted sensitive information and had not placed an adequate level of focus on that particular asset. *Know your assets*. Second, while he had invested significantly in hardware and software, he had not invested at all in training his employees. *Know your weaknesses*. The sad reality is that we breached his security by *social engineering* our way past a security guard into a secured area accessible only by card keys, past several employees (including managers) into the unlocked storage room labeled "CREDIT STORAGE."

We walked out of that area—unchallenged—with an armful of sensitive documents. They had a poor security strategy resulting from poor up-front analysis. Not knowing what these assets represented and their impact on the business led to what could have been a catastrophic breach of security. Luckily, all the CSO lost that day was a little bit of ego. *Know your risks*.

Remember, a sound, well-developed security strategy is critical to preserving your most critical assets and keeping the business safe. The security policy should reflect the intent of the security strategy and provide direction on how to implement the strategy across the company. But without the up-front efforts to determine what constitutes a critical or sensitive asset and the risk exposure to those assets, it is impossible to make wise decisions on where to apply your scare resources, and your security strategy will be weak. ***Insufficient due diligence equals a possible breach***.

Understanding the Key Components

"Security is the process of protecting data (in any form the data may take: electronic, print, or other forms) in motion or at rest, from unauthorized access, use, disclosure, destruction, modification, or disruption so as not to compromise the confidentiality, integrity, and availability of the information for use by the organization throughout the Security Lifecycle." This general description of security has been edited and translated and repeated so many times that it is impossible to give credit to a single source, so instead, I will attribute it to the security community at large. However many times it has been modified to reflect the reality of the current times, it does pretty much sum up all of the elements that are referred to as the "Tenets of Security"—that is, all of those things that we agree are fundamental to information security.

Let us take a closer look at these key elements.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

CIA

CIA stands for confidentiality, integrity and availability, three fundamental characteristics that we are attempting to preserve when it comes to sensitive or otherwise critical information.

- **Confidentiality** pertains to privacy and ensuring that only those people who should have access do.
- **Integrity** addresses the level of confidence you have that the content of a document remains exactly as it was when you left it.
- **Availability** is making sure that people who should have access do whenever they want it.

NOTE

If you are planning to take a security certification exam, study all aspects of implementing and preserving CIA thoroughly. CIA is a prominent subject on these exams and the cornerstone of information security.

Most importantly, we cannot overemphasize how important it is that you completely understand and appreciate the importance of each of these fundamental concepts, and recognize the risks to each along with the potential impact to the business if any are compromised. And yes, we do intend to keep harping on the importance of data confidentiality, integrity and availability throughout this book!

Access Control and Identity Management

Of course to preserve the CIA of important information, you must control each person's level of access to specific information, and when they can access it. Generally, a few people need complete access, some people need some access, and most people need no access. Access should be granted based on *least privilege*, meaning as little as is absolutely necessary. Though making a "who, how much, what, when" determination may seem trivial, the reality is that often, many people receive more access than they should have. And when the right access decisions are made, you must then select the most appropriate control protocol for the situation. Luckily, there are several good implementation strategies for access control to get you started:

- **Role-based** controls grant access based on a particular job. For example, all doctors may have access to all patient records at the hospital. All school principals may have access to all student records at the school. (By the way, both of these examples provide more access than is generally needed!) Nurses at the hospital may have limited access based on the ward they are working in, and teachers at the school may have limited access based on the class they are teaching. Job roles dictate what each is allowed to access.
- **Need-to-know** controls restrict access to those who must know based on job title or job description. If they can function without it, they should not have it.
- **Rule-based** controls regulate access by forcing a match in a table to an applicable rule. For example, a rule might specify that System A is allowed access to a particular resource, in which case, access would be granted. Another rule may deny access from System B, in which case, that request from System B would be

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

rejected. This type of access control is commonly used on firewalls where the firewall administrator would add and remove rules as access demands change.

There is so much more to choosing the right access control strategies to implement for your business; you may need to implement more than one single strategy depending on the complexity of your business. Overall, the determining factors will be the nature of the data, the sensitivity level, and outside influencers, such as government or industry requirements, how much time and money you can spend to implement access levels, and the risks in having the data overly accessible or overly inaccessible. Applying sensitivity levels to data will help you determine access requirements. You have likely heard terms such as “Top Secret,” “Secret” and “Confidential.” These labels constitute different levels of sensitivity the information holds based on (usually) the content. Your company may choose to develop and implement a sensitivity rating for data and grant access based on the ratings applied. In some environments, data labeling is mandatory.

- **Mandatory Access Control (MAC)** — requires that all data be labeled and access be granted based on that label. There are strict guidelines for determining the appropriate sensitivity levels for paper documents or electronic data (as examples). Access is limited based on the data label—among other things.
- **Discretionary Access Control (DAC)** — allows the data owner to determine access rights based on personal knowledge of circumstances. The data owner can provide as much or as little access to anyone he or she desires as long as it doesn’t conflict with tighter restrictions in the company.

How do all of these access control implementations work together? As an example, your particular environment may demand the implementation of MAC and *need to know*, in which case the highest ranking member of the organization may have the highest clearance level available but still not have *authorization* to access a particular document, because he or she does not have the need to do so. We will talk more about authorization in a minute.

Controlling access also means verifying that someone or something (the entity) is exactly what they or it claim to be. This is referred to as *authentication* and generally falls under the category of *identity management*. Once the identity of the person/entity has been verified (authenticated), the next step is to verify that they/it are allowed to access the resource that they are/it is asking to access. This is the *authorization* part and falls under the *access control* category. By the way, identity management and access control are generally combined and referred to as Identity and Access Management (IAM).

- **Authentication**—Confirming the identity of a person or assuring that a computer program is trusted
- **Authorization**—Granting the right to do something based on an established identity

It is easy to confuse the two terms (and we are not even done yet!), but remember that it is less important to memorize the words than it is to understand the concepts. Keep

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

this in mind: I may identify you as my friend (authentication), but that does not mean you have permission to drive my car (authorization). And while we are talking about my car, you may have access to my keys, but you are *still* not authorized to drive my car!

Because you have already decided that not all people should have access to all things, you need to determine who is authorized to access what, how you will go about verifying that they are who they say they are, and then matching up who they are with what they can get each and every time without exception. No problem! (And yes, you should go back and re-read this last paragraph until it makes perfect sense to you!)

Authentication

The more stringent your test for authentication is, the more confidence you can have that the person really is who they say they are. Obviously, the more critical accurate authentication is to your business, the more effort you will demand in order for authentication to be considered reliable enough.

The concept of *factors* provides for additive exercises for identification. These factors are referred to as something you know, something you have, and something you are. Any one of these factors is known as *single-factor authentication* and is the weakest requirement for authentication. Any combination of two is referred to as *two-factor authentication* and is generally accepted as good enough. More stringent data control may require *three-factor authentication* and would likely cost more to implement, be more time-consuming to conduct, but be more difficult to subvert.

- **Something you know** refers to a piece of information that (hopefully) only the correct person would know, such as a password, passphrase, date, PIN, or mother's maiden name. This type of authentication is generally done in an otherwise controlled environment, such as within an intranet or trusted environment, and is usually implemented as a username and password combination. Note that although a username (something you know) and a password (something else you know), together provide greater proof of identity, these still only constitute single-factor authentication. This should really be considered the bare minimum authentication requirement in most circumstances.
- **Something you have** could be a token, a smartcard, or perhaps a key to a lock. The most typical combination of factors would include something you know, such as a pin, and something you have, such as a smartcard. The next time you step up to an Automated Teller Machine (ATM), consider how many factors of authentication the bank is asking you to provide before they dispense money to you! And again, just because you have two keys; or a key and a smart card; or nine keys, three smart cards, a token, and a secret decoder ring, you are still only meeting the requirements for single-factor authentication, because all are something you have. Just throw in a password and you have upped it to two-factor authentication.
- **Something you are** becomes a little more complicated and a lot more personal as it tests a person against an existing sample from themselves. This is where biometrics comes into play in the form of fingerprints, voice patterns, retinal and iris scans, ear geometry and even facial recognition and palm geometry—among other methods.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Obviously, biometrics are generally more expensive to implement and are generally considered more intrusive, therefore less desirable, to those being tested.

Authorization

Authorization is about controlling who is allowed to have, do, read, modify, write, execute, see, use, control, access, enter, move (pick a verb). It should be managed in degrees based on concepts such as the need to know. Developing a strategy for who is authorized to do what is no trivial task and pretty much sums up security. How do you determine who needs authorization to do what? As we have already discussed, there are many ways to control access, but determining how to grant access based on who *needs* to have access is a whole different story. Access versus authorization, you ask? Access is getting there. Authorization is having permission to get there. Confusing to be sure, but it starts to make more sense if you apply it to normal conversation:

- "I authorize you to access my bank account information."
- "This was an unauthorized access."
- "I had complete access to the museum, but was not authorized to actually touch the paintings."
- "Unauthorized access to this system is prohibited."
- "When we use weak passwords, we make it easier for a potential hacker to gain unauthorized access to our systems."

So in real life (as opposed to book life!), why is access management so important? Here is another story to answer that question.

On a Payment Card Industry (PCI) assessment at a nonprofit organization, we were trying to determine exactly who of the 5,000 or so employees had access to credit card information. Management had no idea, and there was not an easy way to tell because, quite frankly, they had done a pretty poor job of controlling who had access to how much and when and why. The security manager we were working with thought that maybe 30 or 40 employees who worked in billing had access to PCI data. In the interest of time, we developed a quick online survey and asked every employee a few simple questions:

- Do you have access to credit card information?
- If yes, do you have access to identifiable credit card information, which would include the card holder's name, the card number, the expiration date, and the code on the back of the card?
- If yes, do you feel that you need this information to perform your daily tasks?

After just a few days and several hundreds of "yes" responses across the board, it became clear that in fact, *most* of their employees had access to credit card information, while less than 1% actually worked in any sort of billing capacity. This company was clearly in for a few long nights if it had any hope of passing an official PCI audit. But more importantly, they had put themselves and their clients at great risk by allowing this to get out of control. Unfettered access to full credit card information to thousands of employees was a disaster waiting to happen. Their problem was that they had no plan to determine who should be authorized to access the data, and they had

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

no access control strategy in place to limit access to those who were authorized. For this customer, a role-based solution would have likely done the trick, ensuring that only those in a job function that required access to the payment card information to do their jobs were authorized to access the information.

Keeping People Out

So far, we have discussed several access control methods such as mandatory and discretionary access, and the need to know. Certainly there is an almost endless list of other possibilities. Let us take a minute to define a few other common controls for keeping people out. Common physical access controls would include things such as doors, windows, fences, barriers, lighting, video surveillance, dogs, and moats stocked with alligators (you get the idea), while technical controls include firewalls, intrusion detection or prevention devices, and routers with access control lists. All of these controls can play an important role in your security strategy and will be discussed in detail throughout the rest of the book.

Arguably, one of the best security strategies is *defense in depth*, where a variety of controls are put into place to work together much like the old castles with their watch towers, their moats and big heavy draw bridges, gigantic wooden doors, and dark entryways into the interior walls guarded by armored guards with big swords. But if you recall, even that well-considered strategy was defeated by a simple wooden horse.

Putting it all together

"Where do I start?" Remember that exercise we talked about where you need to build your security strategy early—where you work with senior management to determine how critical certain assets are and the impact they would have on your business if they became unavailable or degraded? That exercise is known as a *Business Impact Analysis (BIA)* and will pay off as you begin to decide how much you need to spend on your access control strategy. If you do not know what your critical assets are, then you do not know where to invest your scare resources: time, people, and money. That is where you should start.

We will go into greater detail on the BIA in "Chapter 10: Keeping the Business Going When it All Goes South," but for now, take some time to consider which assets are most critical to your business. Do you know? Are you focusing enough on those assets in your security strategy? Are your scarce resources (time, people, money) being used as effectively as possible to keep your company safe from a data breach? We will help you answer that question and more in this book.

Summary

Despite the almost romanticized notion of the "everyman" rising up (wearing a Guy Fawkes mask, of course) to fight tyranny, injustice and corrupt governments, getting

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

your data stolen, damaged, or destroyed can be catastrophic, and that is the more likely result from *hacktivism* as it is today.

Tight access control is vital to preserving the confidentiality, integrity, and availability (CIA) of your most critical assets, but to know where to focus your scarce resources (time, people and money) you must conduct a business impact analysis to determine which assets are the most critical, which represent the greatest risk to the company if breached, and to determine an appropriate identity and access management strategy.

A well-considered security strategy requires upper-management support to be effective, while a well-written security policy provides the detailed representation of the security strategy and must be shared corporate-wide.

Consider this:

You have a locked box with a confidential letter inside.

You have the combination to the lock on the box.

Inside is another box with another lock, to which you have the key.

Inside that box is another box with another lock to which you also have the key.

Finally, inside of that box, is a letter with a wax stamped seal on it with the initials ***BR***.

How many factors of authentication were used to protect this letter?
Consider our discussion on CIA and apply those concepts to the letter.
How could you improve the security of this box and the letter?

Also Consider:

You are the security administrator for a large hospital.

You have stored your backup tapes in a large storage locker at a public rental facility.

The tapes contain electronic, protected health information (ePHI).

The Health Insurance Portability and Accountability Act (HIPAA) requires that every covered entity (anyone who must possess ePHI) establish procedures for obtaining critical ePHI in a timely manner.

Based on our discussion regarding CIA, is this security strategy sufficient for this type of data?

See “Chapter 13: Summary and Next Steps,” for discussion on these questions.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

References

1 Yale Law & Technology, “We Are Anonymous, We Are Legion,” http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/

2 AnonQuotes, Pastebin, http://pastebin.com/mms4nFMh

3 Open Web Application Security Project (OWASP), “Threat Agent,” https://www.owasp.org/index.php/Category:Threat_Agent

4 Merriam-Webster, definition of probability, http://www.merriam-webster.com/dictionary/probability

5 U.S. Department of Health & Human Services, “HHS settles HIPAA case with BCBST for $1.5 million, http://www.hhs.gov/news/press/2012pres/03/20120313a.html

6 **Bill Brenner**, “Heartland CEO on Data Breach: QSAs Let Us Down” *CSO Data Protection,* http://www.csoonline.com/article/499527/heartland-ceo-on-data-breach-qsas-let-us-down?page=1

7 **Kitten, Tracy**, “Heartland CEO on Breach Response”, *Data Breach Today*, http://www.databreachtoday.eu/interviews/heartland-ceo-on-breach-response-i-1564

8 **Hewlett Packard**, Business Continuity and Availability with Resilient Storage http://h71028.www7.hp.com/enterprise/downloads/bca.pdf

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net