The CISO Handbook

A Practical Guide To Securing Your Company

Mike Gentile Ron Collette Tom August

Auerbach Publications
Taylor & Francis Group

The CISO Handbook

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Asset Protection and Security Management Handbook
POA Publishing
ISBN: 0-8493-1603-0

Building a Global Information Assurance Program
Raymond J. Curts and Douglas E. Campbell
ISBN: 0-8493-1368-6

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Critical Incident Management
Alan B. Sterneckert
ISBN: 0-8493-0010-X

Cyber Crime Investigator's Field Guide, Second Edition
Bruce Middleton
ISBN: 0-8493-2768-7

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella, Jr. and Robert S. Greenfield
ISBN: 0-8493-0955-7

The Ethical Hack: A Framework for Business Value Penetration Testing
James S. Tiller
ISBN: 0-8493-1609-X

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks
Susan Young and Dave Aitel
ISBN: 0-8493-0888-7

Information Security Architecture: An Integrated Approach to Security in the Organization
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Fundamentals
Thomas R. Peltier
ISBN: 0-8493-1957-9

Information Security Management Handbook, 5th Edition
Harold F. Tipton and Micki Krause
ISBN: 0-8493-1997-8

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Thomas R. Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas R. Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit, Second Edition
Fredrick Gallegos, Daniel Manson, Sandra Allen-Senft, and Carol Gonzales
ISBN: 0-8493-2032-1

Investigator's Guide to Steganography
Gregory Kipper
0-8493-2433-5

Managing a Network Vulnerability Assessment
Thomas Peltier, Justin Peltier, and John A. Blackley
ISBN: 0-8493-1270-1

Network Perimeter Security: Building Defense In-Depth
Cliff Riggs
ISBN: 0-8493-1628-6

The Practical Guide to HIPAA Privacy and Security Compliance
Kevin Beaver and Rebecca Herold
ISBN: 0-8493-1953-6

A Practical Guide to Security Engineering and Information Assurance
Debra S. Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions
Rebecca Herold
ISBN: 0-8493-1248-5

Public Key Infrastructure: Building Trusted Applications and Web Services
John R. Vacca
ISBN: 0-8493-0822-4

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

Strategic Information Security
John Wylder
ISBN: 0-8493-2041-0

Surviving Security: How to Integrate People, Process, and Technology, Second Edition
Amanda Andress
ISBN: 0-8493-2042-9

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Using the Common Criteria for IT Security Evaluation
Debra S. Herrmann
ISBN: 0-8493-1404-6

AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

The CISO Handbook

A Practical Guide to Securing Your Company

Michael Gentile, CISSP
Ronald D. Collette, CISSP
Thomas D. August, CISSP

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20131031

International Standard Book Number-13: 978-1-4200-3137-9 (eBook - PDF)

Table of Contents

Appendices

Foreword

Information security is hard. There … I've said it!

It's harder than selling life or automobile insurance because almost everyone knows they need that type of insurance. In fact, in many instances, the law mandates insurance. But the need for information security and controls, even today, is a tough sell. Notwithstanding the Health Insurance Portability and Accountability Act (HIPAA), Gramm–Leach–Bliley (GLBa), Sarbanes Oxley 404, and the myriad of recently enacted state and federal regulations intended to protect consumer privacy, implementing an effective, robust information security program is an uphill battle.

Therefore, it takes a special individual to assume the mantle and push the security agenda. I am proud to know three such individuals — persons with passion, devotion, dedication, and the sort of stick-to-it-ness that we don't often see in the corporate world.

They are the authors of this book. I've been privileged to work alongside them and consider myself fortunate to watch as they demonstrate the levels of professionalism and dedication that are critical to the work we do. Through their efforts, they've acquired and nurtured business prowess and technical proficiency that translates into personal and professional credibility. Their co-workers trust them. This crucial ingredient has encouraged others consistently to ask them to be a part of the solution. Security practitioners know this is the only way to succeed.

Moreover, they have assumed a task that few undertake — documenting the practical, real world application of a security program so others can benefit from their experience. In a logical, well thought out way, they walk the reader through a series of thought processes that tutors the burgeoning security professional toward a successful endeavor.

I encourage you to consider seriously the lessons herein, and sincerely wish you the best with your own program.

Micki Krause

Acknowledgments

Team Acknowledgment

We would all like to thank Micki Krause for her mentorship, support, and guidance during this process. We never would have attempted this project without her encouragement.

Mike Gentile would like to thank the following people and organizations:

- My wife, Tiffany, for supporting and believing in me on this project in a way that no one else could duplicate. And on a lighter note, for only charging a pair of shoes to review each chapter.
- My parents, Mike and Lorraine, for never missing a game — you provided me with the foundation needed to take on any challenge.
- Marcus Ziemer, for teaching me how to work effectively on a team — it is amazing how the skills you taught me through sports have paid massive dividends in the world of business.
- Mike and Laine Nelson, for being some of the most giving people I have ever met

Ron Collette would like to thank the following people and organizations:

- My wife, Alice, for her support, council, and friendship during this project; she is the best partner anyone could ever ask for
- My family for giving me the confidence to believe that I could accomplish anything
- Mitchell Kay (high school English teacher) for insisting that I learn how to form a grammatically correct sentence

Tom August would like to thank the following people and organizations:

- My family and friends for their continued trust, support, and encouragement
- Bill Barrett and Cheryl Moerson from Ernst & Young for showing me the importance of seeing the big picture early on in my career
- Stan Watkins and Rich Milo from Deloitte & Touche for their unwavering support and encouragement
- John Dubiel and Victor Wheatman from Gartner, Inc., for their sound advice and encouragement

Book Reviewers We Would Like to Thank

- Alice Collette, PMP, LC
- Tiffany Gentile, CPA
- George McBride, CISSP, CISM
- Bruce Lobree, CISSP
- Franjo Majstor, CISSP, CCIE
- Bonnie Goins, CISSP, NSA IAM
- Ben Rothke, CISSP, CISM

Cover Art Designers We Would Like to Thank

- Alice Collete of Design Alley
- Owrey Photography

Organizations We Would Like to Thank

- Richard O'Hanley and everyone at Auerbach for giving us the opportunity to make this book happen.
- The manufacturers of Red Bull, Emergen-C, the coffee growers of Columbia, and Pepsi-Cola. You all made a very tight deadline possible.
- Indie 103.1 FM for being the first commercial radio station in Southern California to take a risk and play some real music for a change.

Introduction

If you read only one section of this book, please read this. Many years of experience went into the development of this material, and it's our sincerest goal to help you to succeed with the implementation of your security program — whether your company is an established Fortune 500 enterprise or a small start-up company. This section provides the big picture of a proven methodology, and our book is designed so you can use this to identify and focus on the areas that are most critical to you.

Overview

In ancient times, mapmakers were rumored to have marked unexplored areas or regions with pictures of sea monsters and the words, "Here Be Dragons," as a warning to sailors and explorers. It's not that these areas were particularly dangerous; they just hadn't been explored or mapped before. The educational material available to information security professionals today is in many ways similar to these early maps of the world.

Perusing the shelves of your local bookstore, you'll see two main types of reading materials for the security professional — technical hacker guides or ultra high-level theory and exam preparation books.

The first and most prevalent type of book is the hacker guide. These highly technical manuals show you, in excruciating detail, how to bypass the defenses of a given set of controls and security defenses. However, they don't give any real guidance for building and defining an effective and measurable information security program that will provide the outstanding return on investment a company requires. In addition, many of these books are often written from a single point of view, thus limiting their ability to properly address areas that the author may have little expertise in. Another problem with these books is they often have to

make a number of assumptions that may have nothing in common with your environment. For example, many known vulnerabilities can only be exploited under a finite set of circumstances. While the authors of these books generally do a good job of explaining their assumptions, the fact that they have to make these assumptions cause them to be of little practical value for the practicing security professional. These books are fun, to be sure, but again they do not properly lay the groundwork necessary to build an information security program.

The second type of book falls into the category of theoretical reference textbooks and exam preparation guides. These books are essential for people wishing to learn the history of the information security industry, its key terms and concepts, and the various theoretical concepts that information security is built from. They are also very useful for preparing the various information security examinations available today. However, the material presented in them is often too generic or nebulous to be of any value to someone responsible for actually building or maintaining a security program. In addition, these books often make a number of assumptions that cause them to be of little or no practical value for the practicing security professional. For example, a common fault among these books is to assume you already have fully functioning processes in your company, such as an integrated Systems Development Life Cycle (SDLC). While that assumption may be fine for a theoretical discussion of how things should be, the reality of the situation is many companies simply don't have the robust control structure that would effectively support a full-fledged SDLC. Another real world example is when executive management insists that an application system be implemented within a truly non-optimal timeframe (i.e., yesterday, or sooner if possible). In the meantime, you are faced with a huge challenge — how can we still keep our company safe?

The goal of our book is simple: provide practical insight and guidance to those tasked with one or more aspects of implementing an effective and measurable information security program — one that provides true value to the stakeholders of a company. We feel this area remains a mystery to many security professionals — especially those ultimately responsible for its design and implementation. Our goal is to present several essential high-level concepts and then build a robust framework that you can use to map these concepts to your environment.

What this book is:

- A comprehensive roadmap for designing and implementing an effective information security program based on real-world scenarios
- A bridge between high-level theory and practical execution
- A set of actionable practices that security professionals can use in the course of their everyday jobs

- A look at information security from experienced professionals with different functional backgrounds providing the reader with a blended perspective
- An assessment tool to assist people in understanding all of the practical issues related to information security, including items often overlooked by theoretical books
- An integrated and modular resource that can either be read from cover to cover or straight to the applicable chapter
- A framework that can be expanded or contracted to accommodate your unique situation

What this book is not:

- A high-level theory or history book
- An exam prep guide
- A technical how-to hacker manual
- A product-specific technical guide

Chapter Structure

The following shows how each chapter is organized.

Overview

This section should be self-explanatory. If you have only a couple of minutes to read something, this is a good place to start.

Foundation Concepts

This section defines those essential concepts that we found to be critical success factors to understanding the material presented in each chapter. Failure to review and understand these items could impede your ability to fully understand or implement the ideas presented in the chapter. This book simply isn't large enough to provide in-depth training on each these concepts, but merely points them out and bring them to your attention. To be honest, most of these concepts have already been written about by people far more knowledgeable than we are in these areas. Our goal here is to point you to sources you might want to familiarize yourself with.

Methodology

This is the section where we identify and explain the steps necessary to achieve the goals of each chapter. This is explained in more detail in the following pages.

Chapter Checklist

Here we illustrate the key items that you should be able to document as you complete the material in each chapter. Each set of deliverables feeds into the successive chapter. For example, the deliverables from the chapter on Assess are inputs into the following chapter on Plan.

Examples and Scenarios

Many times, dry discussions about how to do something can best be explained with a simple example or case study. Here is where we'll show you some real-world examples of things we've seen over the years — from the outstanding to the supremely non-optimal. Where applicable, we will present how the situations may look from different points of view.

Methodology

The book is presented in chapters that follow a consistent methodology — assess, plan, design, execute, and report. Each chapter is related to the prior chapter in a dependent hierarchy, where the information gathered in one chapter provides the inputs for the next. Below, in Figure 1, we have illustrated the entire flow of the book and the corresponding relationships of each chapter.

Assess

In this chapter, we guide the reader through a process of identifying the various elements that drive the need for an information security program, such as regulatory requirements, competition, industry best practices, technology standards, geographic and political considerations, as well as physical and environmental constraints.

Some of the key deliverables that you should be able to complete after finishing this chapter include:

- An inventory of your stakeholders
- An analysis of your business or regulatory requirements
- An assessment of a number of other known drivers for an Information security program

Plan

In this chapter, we discuss how to build the foundation for your information security program. These elements include how to:

- Obtain an executive mandate for the program
- Develop a charter or mission for your program

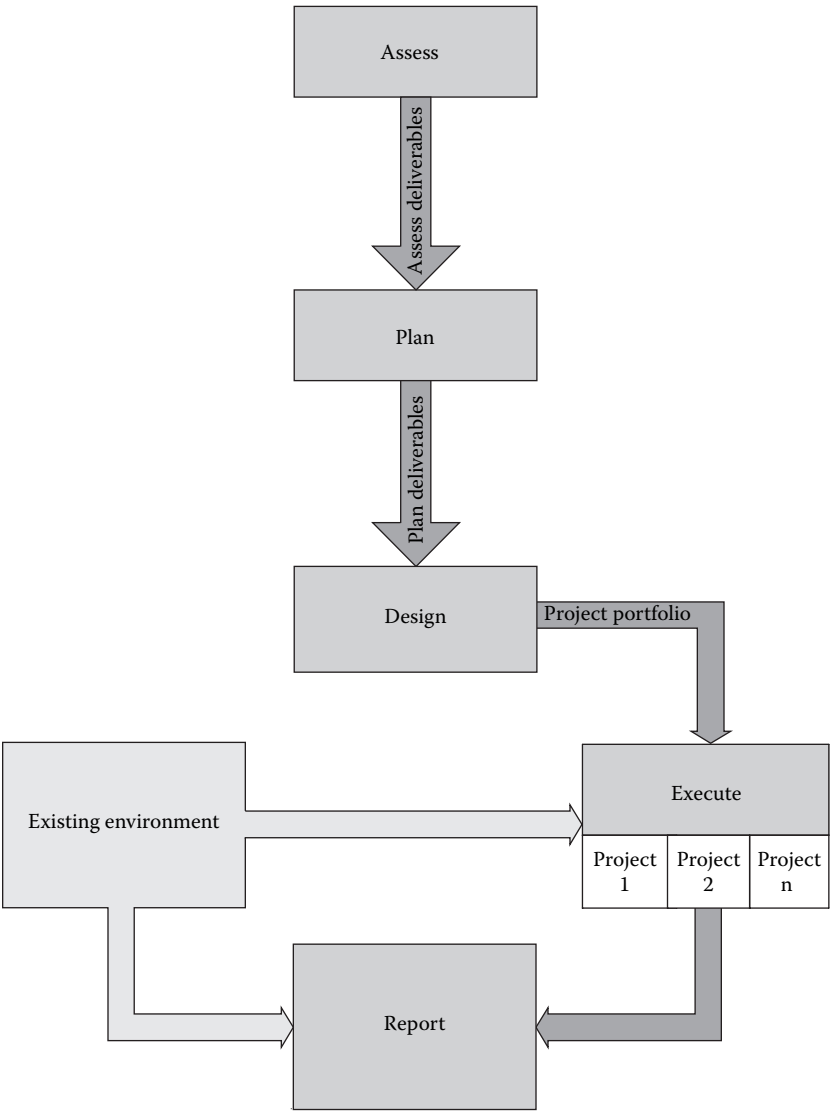

Figure 1 Methodology Overview

- Develop your overall program strategy
- Define the organization structure of your team
- Create job descriptions for your team members
- Identify key personality traits we've found to be critical for the different roles a program may have

Some of the key deliverables would include:

- Your program's charter or mission statement
- Executive support in the form of a formal policy statement or executive mandate
- A list of the business requirements the program should meet
- High-level reporting metrics to show the program's effectiveness
- An organization structure with defined roles and responsibilities that truly fits your business

Design

This is the chapter where we show you how to take the business requirements you've identified so far and construct the policies and procedures that can be implemented to meet them. This chapter will show you how to perform a gap analysis to identify areas where your business may not meet the business requirements you identified in the earlier chapter. We then show you a methodology for identifying the technologies, processes, and education/awareness projects you will need to undertake to meet the spirit of your policies. Other critical areas addressed in this chapter include capital budgeting, resource planning, and project scheduling.

Some of the key deliverables you should be able to complete after reviewing this chapter include:

- A completed gap analysis against your business requirements
- A set of clearly defined and actionable project requirements
- A prioritized list or portfolio of all of the major projects to be completed in order to successfully implement your program
- A rough capital budget for use in soliciting the financial support necessary for implementing your program

Execute

This chapter addresses the need for a successful execution model for implementing the security projects identified in the previous chapters. It has been our experience that having a consistent methodology for executing security projects is one of the most critical success factors in running a successful program. The overall goal of this chapter is to present some guidance on how to successfully execute your security projects given all of the various constraints you face everyday in your business.

This chapter focuses on the project management skills and execution tactics you will need to ensure that the projects you have won management's support for actually get accomplished to everyone's satisfaction.

This is absolutely critical in that your security program's credibility and ongoing success will depend on how well you identify and execute your projects and leverage your successes.

After discussing the elements of project management techniques, we will leverage that knowledge to aid you in the incorporation of security into every initiative within your organization; even if it isn't an initiative driven by the security office.

We also try to address some the known "gotchas" and realities that face many of us each day in our jobs. We discuss the most common types of project failures and how to prevent them, how to establish successful project teams, how to effectively define team roles and responsibilities, how to capture clear, and actionable project requirements, and how to develop clear, actionable, and measurable project goals that can be leveraged as you build your program.

The only deliverables to come from this chapter should be your ongoing portfolio of successfully implemented projects.

Report

This chapter focuses on the reporting process for both external and internal stakeholders of your program. We discuss the various types of audiences, their needs, successful strategies for reporting to them, the types of information they will be most interested in, and the best methods and formats for communicating this information to them.

Key deliverables from this chapter include an analysis of your various reporting audiences, a strategy for reporting to each audience type, and an assessment of the types of information you'll need to report and where to find it in your organization.

The Final Phase

This small book is packed with information, as well as repeatable proven processes and techniques to aid in developing your own information security program. Along each step of the way, we have attempted to distill each critical concept into a digestible and mechanical process that can be adapted to your unique circumstance. So, find a comfortable chair, pour yourself a drink, and hold on for the ride.

Chapter 1

Assess

Overview

The assess phase of the methodology is the process of determining information about the enterprise to support the planning of your information security program. This process involves the identification of the external and internal business drivers for your program, so your program can be built on a solid structure that meets the essential factors influencing your business.

In some organizations, this process is not undertaken in a formal, structured manner. This typically results in a band aid approach to building an information security program. If we view it in terms of purchasing a new car, it would be similar to purchasing a two-seat convertible to move a large family across the country. In this example, action was taken prior to understanding the specific requirements that needed to be met.

In the assess phase, we identify major categories and components that are common to every business, as well as their impact on the development of an information security program. Though we acknowledge that there are additional factors that can play a role in the assessment, we have attempted to distill the common high impact items.

Why do we start with assessing your environment? The initial evaluation of any environment is analogous to dating someone for the first time — you need to gather a lot of critical information as quickly and efficiently as possible. You're attempting to get the big picture, which will provide insight into the very reasons you need a program in the first place.

The goal of this chapter is to provide you with a consistent methodology for quickly and effectively gathering this critical information. Before

moving on to the methodology, we will start with the foundation concepts needed to be successful.

Foundation Concepts

The objective of the foundation concepts for this chapter is to help identify critical skills and information you should possess to provide the necessary leverage to successfully implement your information security program. Critical skills are those soft skills that will help you get the most from your efforts, while critical knowledge applies to the essential information you will need to give you the appropriate perspective, or leverage, as you assess your environment.

Critical Skills

Consultative Sales Skills

Most people see security as a cost center, not a profit center. This perception almost automatically places you in the unenviable position of constantly having to sell the virtues and benefits of your program. Selling and marketing the initiatives and ideas associated with your information security program is easily one of the most important skills you can develop. This skill has helped us to no end in the implementation of the security projects and programs we build or maintain.

Your customers may be external companies who have hired your firm, or it might be someone from another department of your enterprise. By treating them all as valuable customers, you are effectively saying to them your success matters to me, and are setting yourself up for increased cooperation and improved participation in the development of your program.

Information security controls are sometimes seen as having a negative or adverse impact on enterprise culture, a high administrative price tag, and they are sometimes seen as hindering the enterprise's ability to profit. Because these controls do not directly add to market share or revenue, they often take a backseat to more visible revenue-generating activities. As a result, you will need to be able to market your program to show either (a) enabling new business opportunities, or (b) reducing business risk.

Enabling New Business Opportunities

This can best be explained through a quick example. With the advent of the Internet, many companies are attempting to deliver business solutions via the Web. As a result, they are implementing systems that are processing

sensitive data over the Internet. This presents a new twist on an old business issue — getting potential customers to trust your business. Because of the many risks and threats associated with doing business over the Internet, one significant way to help market your information security program is to show how increased security controls can directly increase your potential customer's trust. By implementing controls such as firewalls, encryption, logging, strong authentication, and independent testing, you will most likely have a strong set of controls that will help your customers trust your business. By working with your public relations and marketing personnel, you might be able to leverage the existence of these controls into your enterprise's marketing plans. Consultative sales skills allow you to work with other people and teams, understand their needs, co-develop potential solutions, sell them to the powers that be, and ensure their successful implementation. Companies such as eBay, e*Trade, and Amazon.com are great examples of companies whose information security professionals have successfully enabled new Internet business through their strong consultative skills.

Reducing Business Risk

Another way to show the value of your information security program is to show a reduction in overall business risk. In a sense, this method is similar to selling insurance — you're trying to sell the benefits of a plan to minimize the impact of an unforeseen event to the enterprise. This is the most prevalent method we are seeing security professionals use today, and entire books have been written on how to best do this. Because a great deal of information on this subject already exists, we will not try to reinvent the wheel. However, we would like to share a few key ideas that have proven helpful in our careers:

- Take the time to learn about the needs and issues your customers are facing.
- Actively listen to your customers. Keep an open mind and try not to project your ideas into their statements.
- Identify the root cause of the problem the customer is trying to communicate to you — not just the symptoms.
- Co-develop solutions with your customers that you both can support.
- Co-present your solutions to management in a manner that is appropriate for the management level, educational background, temperament, and political motivations of your audience.
- Leverage your wins — as you help one customer, use them as a reference for other projects where feasible. Establish and maintain forward momentum in all your initiatives.

- Be flexible.
- Project confidence. Would you let a surgeon perform an operation on you if she seemed uncertain of the procedure?
- Don't second guess yourself. Collect enough information to make an informed decision and resist alterations.

Hopefully, we've whetted your interest on this topic, and have shown how these skills can help you in the implementation of your information security program. A number of excellent reference books that have helped us on this topic can be found in the Appendix.

Critical Knowledge

In this section, we will identify areas of information you will need to effectively perform an assessment of your environment. However, it is well beyond the scope of this book to provide comprehensive instructions on each topic. Where applicable, we will point you to a few reference materials we found to be of value in understanding these critical knowledge areas.

The several areas of critical knowledge we present are:

- Understanding your business
- Understanding risk
- Understanding your enterprise differentiators
- Understanding your legal and regulatory environment
- Understanding your organization
- Understanding your organizational dynamics
- Understanding your enterprise culture
- Understanding your enterprise's view of technology

In our opinion, these areas are critical in your ability to perform an assessment of your environment. If you feel you possess a deficiency in any of the material presented in the foundation concepts, we suggest you refer to the recommended reading Appendix for additional guidance. The concepts identified above will continue to be used and built on throughout the book.

Understanding Your Business

How does your enterprise make money? Exactly what products or services does your enterprise provide? Who are your largest clients or customers? Is your enterprise profitable? If you don't know the answers to these

questions, then we strongly recommend that you start learning about your business immediately. If you are in a publicly held enterprise the answers to many of these questions can be found in your company's annual report. If you are in a charitable organization, smaller enterprise, or a government entity, you may need to ask around to get the answers to these questions. People you may want to talk to include your public relations staff, chief financial officer, and sales directors.

Here are just a few of the things all of the members of your information security program should know:

- How does your enterprise make money?
- Does your enterprise have any subsidiaries or minority interests in other companies? The other side is also a great question to ask — is your enterprise a subsidiary or minority interest of another company?
- Where does your enterprise usually spend most of its money?
- Is your enterprise profitable?
- Does your enterprise have a positive cash flow from operations?
- Is your enterprise publicly or privately funded?
- How does management decide what products or services your enterprise should provide?
- Exactly what products or services does your enterprise provide?
- Who are your largest clients or customers?

To understand how to best implement an information security program that adds the most value to your enterprise, you need to understand the role your information security program will play in the overall scheme of your business. There is usually a significant cost to implementing an information security program, and being able to balance the operational needs of your enterprise with the business risks your enterprise faces is a critical success factor. This concept is the whole point of the chapter. Throughout this chapter, we will guide you through the process of assessing the business drivers behind your need for an information security program, and how to determine the basic level of information security controls that should be implemented.

Knowing the various drivers of your information security program and their relationship with the business operations of your enterprise is a critical success factor in effectively implementing your program. For example, implementing too few information security controls, when your business drivers require otherwise, can lead to a number of problems for your enterprise. These may include such issues as regulatory non-compliance, numerous audit findings, theft/loss of data, lost revenues, inaccurate data, excessive costs, wasted time, inability to prosecute wrongdoers, and

excessive system downtime. On the other hand, implementing too restrictive of a control environment without the requisite business drivers can actually hurt your enterprise. Lost revenues, excessive costs, wasted time, redundant processes, and crushed employee morale are just a few of the negative results that can come from an overzealous information security program.

Figure 1.1 helps to illustrate the costs associated with implementing too few or too many controls.

In addition to understanding general information about your enterprise's business operations, you should also have a strong understanding of its internal financial processes. Knowledge of your enterprise's financial budget cycle and approval process is a success factor that will directly impact your ability to get funding for the initiatives that you will want to put into operation as you build your enterprise's information security program.

Listed below are a few critical items you should know about your enterprise as you implement your information security program:

- How does management decide what internal projects your enterprise should invest in?
- What is our enterprise's budget cycle?
- Who is involved in the budgeting process and exactly what are they responsible for?
- What types of projects or which sponsors typically have the most success in being funded?
- How far in advance should you begin to start marketing your ideas to your key financial decision makers?
- What sort of research, analysis, or supporting documentation would be of most help in persuading these key financial decision makers to support your initiatives?

In determining the balance between business operations and security controls, the next portion of the equation is the concept of risk.

Understanding Risk

> Risk comes from not knowing what you're doing.
>
> **—Warr en Buf fett**

The concept of risk is often defined using many different examples, types, and forms. Some of the more well-known terms used to describe risks

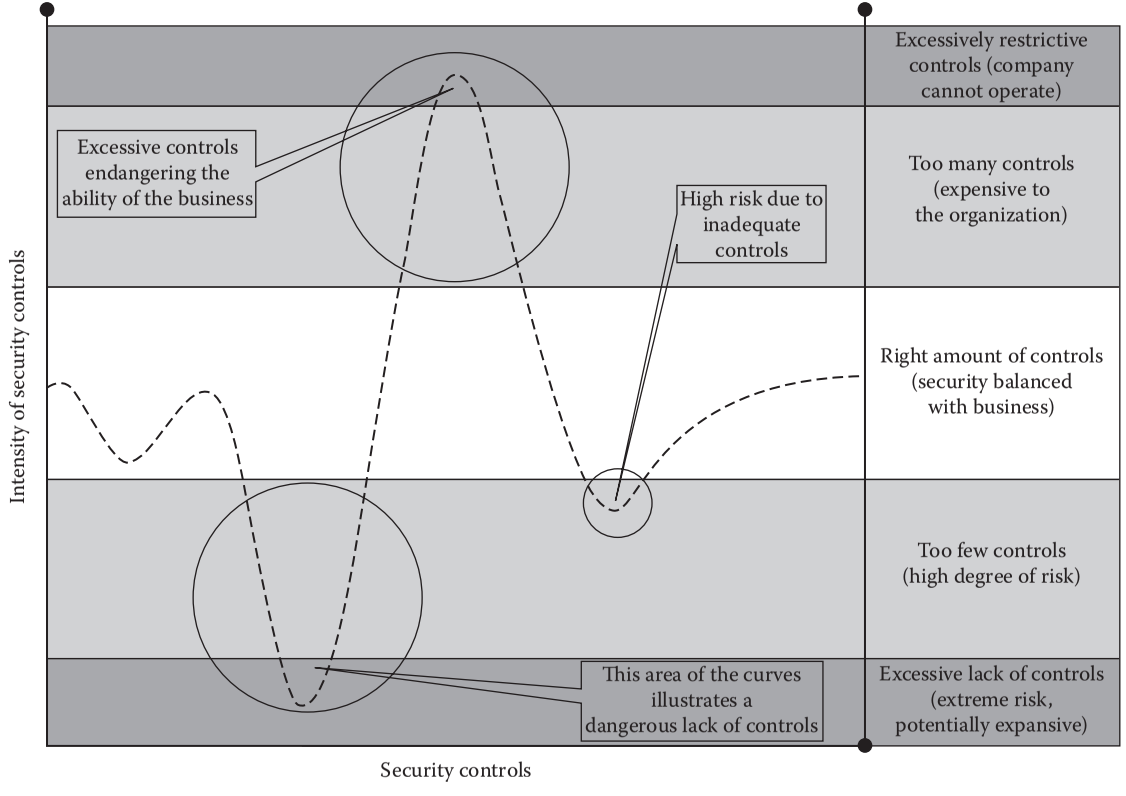

Figure 1.1 Control Result Chart

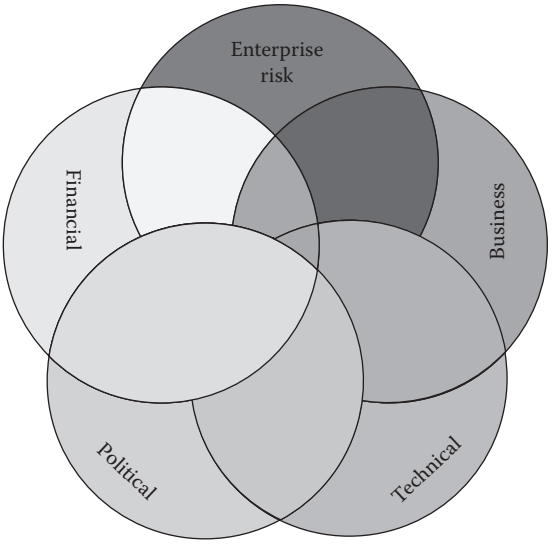

Figure 1.2 Enterprise Risk Factors

facing today's enterprises include business risk, financial risk, geo-political risk, and technology risk (see Figure 1.2). Understanding the various elements of risk that affect your enterprise can be a powerful tool for building support for your program. Understanding the nature of these risks and being able to communicate their potential impact to your business operations can be a valuable tool in getting some stakeholders to support your program.

A number of security vendors use an extreme form of this strategy in trying to sell you their products and services — they employ the use of FUD (fear, uncertainty, and doubt) to scare customers into buying their products. Although we certainly don't recommend ever playing the FUD card, we found that the ability to clearly understand and articulate the potential impact of the various risks facing your enterprise can sometimes help to convert even the most stubborn obstructionist to a champion.

Understanding Your Enterprise Differentiators

Enterprise differentiators are aspects of the business that cause an enterprise to succeed against its competitors, e.g., better product and service offerings, lower prices, faster delivery, better customer service. These are all things that make one enterprise stand out from another. Accordingly,

these elements need to be protected because they are either directly or indirectly responsible for generating revenues.

The primary concept is that business requirements drive security programs…not vice versa. To effectively plan your information security program, identify your enterprise differentiators and watch out for information security controls that could have a negative impact on them. The following is a quick example to illustrate.

Scenario

SpamCo is in the business of direct mass e-mail marketing, and derives its revenue from the ability to design and execute direct marketing campaigns to individuals. SpamCo's most critical enterprise differentiator is how effectively it processes e-mail responses from its various direct marketing campaigns. Oblivious of this fact, SpamCo's new information security officer decides they need an e-mail filtering system to cut down on the volume of inbound spam its employees are receiving on their desktops. He researches the various options, chooses the most aggressive one available, and has the engineering staff route all incoming mail through it — including the e-mail responses from its direct marketing campaigns. By not understanding SpamCo's main enterprise differentiator, the information security officer managed to negatively impact a mission critical area of the business, and "won" a big CLM (career limiting move) award.

Analysis

This was an extreme example, but it is clear that the factors that were taken into consideration when determining the use of an inbound spam filter were incomplete. This error was compounded by the fact that it was introduced into an aspect of the enterprise's competitive advantage. Though the initiative reduced the risk, it sacrificed a major component of the business.

Understanding Your Legal and Regulatory Environment

For purposes of this book, we'll define your regulatory environment as being comprised of laws and regulations imposed on your enterprise by outside entities. It is essential that you obtain a solid understanding of the federal, state, and international laws that affect your business. In addition, industry groups, trade associations, and governmental entities often have regulatory requirements your company must follow to operate in a given industry. Laws and industry regulations are often mandatory,

and are usually critical drivers for information security programs. As such, they can also be very effective tools that can be used to solicit support for your program. The best resource for obtaining information about the laws and regulations facing your enterprise is your company's legal counsel and executive officers. These requirements will become major factors in the development of your information security program.

Understanding Your Organizational Structure

The next step in your quest to understand your role is to obtain a copy of your enterprise's organization chart — not just for your immediate area, but for the entire enterprise. A quick review of your enterprise's organization chart can yield a large amount of information without much work on your part. What can you learn from your org chart? First, does your organization even have one? If not, that speaks volumes. An organization that has failed to document the roles and responsibilities of their management and staff may not have the control infrastructure necessary to support an effective information security program yet. This would be analogous to a soccer coach placing players on the field without assigning positions or informing the players of their roles. Second, how accurate and current is the org chart? An organization that fails to maintain a relatively current set of org charts may not strongly emphasize maintaining a strong set of internal controls, and may be a difficult place to build an effective information security program. Third, the org chart is an excellent reference for identifying the key players in the organization, their roles and responsibilities, and the areas they may exert some control or influence over. You always want to be prepared to speak to the level of the target audience; not find out who they are after you have misspoken. Finally, review the organization structure itself. Identify whether the following areas exist — operations, information technology (IT), sales and marketing areas, financial operations, internal audit, regulatory compliance, and public relations and their relation to the overall organization. Is this organization centralized or decentralized? The organization structure review is the most subjective aspect of your review, and will be referenced throughout our book.

The functional design of the organization is going to vary based on the business of the enterprise. We are not attempting to provide a lecture on organization dynamics. Our objective is merely to provide some basic techniques that will aid you in performing a cursory analysis.

The best place to start is to compare and contrast the structure to companies that you have been exposed to in the past. What worked? What didn't work? Obviously, this task will be made easier if you have worked at a similar type of enterprise. If not, apply what you think is