Realtime
publishers

The Shortcut Guide™ To

Prioritizing Security Spending

sponsored by

IBM®

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: Optimizing Business-Driven Security

Today we are witnessing a confluence of technical, social, economic, and business trends that shape the challenges we face in information security. Fortunately, these same trends contain the means for addressing the challenges. Monolithic applications have given way to component-based systems based on Service-Oriented Architectures (SOAs) and mashups. Virtualization and cloud computing are changing the nature of the data center with a shift from dedicated hardware for applications to a shared hardware model. Social drivers include an increased awareness of risks to personal information and an associated undermining of trust in organizations' ability to protect that information. The current economic slowdown is a dominant business concern for obvious reasons but it has less obvious implications for information security as well. How are businesses to manage security spending in such a dynamic and multifaceted environment?

This eBook, *The Shortcut Guide to Prioritizing Security Spending*, provides a context for understanding today's information security environment and selecting an optimal set of technologies, policies, and practices to meet the needs of your particular business. This guide consists of four chapters, each of which addresses a key part of the overall framework:

- Chapter 1 examines how the slowing economy creates opportunities as well as challenges for businesses. The chapter examines security as it relates to topics such as the dynamic workforce, evolving technologies, and compliance issues. It also considers opportunities provided by cost optimizations, business consolidation, and competitive advantages enabled by improved security.
- Chapter 2 focuses on protecting business operations and optimizing staff efficiency. Business operations are considered with respect to preserving the confidentiality, integrity, and availability of information and services. Staff efficiency includes both overall productivity in an organization as well as security administration efficiencies.

- Chapter 3 considers several key technological trends that must be accommodated within a security management framework, including virtualization, cloud computing, distributed information flows, application security, and Web 2.0 technologies.
- Chapter 4 describes a multi-phased approach for prioritizing security spending. Starting with an assessment of the business environment, the process moves on to design and deployment issues followed by a discussion of implementation and management topics. The final phase considers education, a critical but sometimes overlooked practice in prioritizing security spending. The goal is to deliver optimized security that can adapt with agility.

The emerging business environment will no doubt pose unusual challenges for information security accompanied by constrained resources. This reality makes prioritization of security spending all the more important. The first step in prioritizing security spending is to understand the risks and threats, and that is where we will turn now.

Today's Economy: Challenges and Opportunities

There is no doubt that the current economic outlook is decidedly less promising than it has been for years, perhaps decades. Current headlines reflect a widespread sense that difficult times will be with us for some time, as the following sample from popular news, business and social publications highlights:

- "No End to The Nightmare" *The Economist* December 30, 2008
- "Why 2009 Will be Worse than 2008: We Are Not Out of the Woods Yet" *Reason* January 2, 2009
- "Manufacturing Reports Show Depth of Global Downturn" *New York Times* January 2, 2009
- "The Year of Investing Dangerously" *Vanity Fair* February 2009
- "The Market Isn't So Wise After All: This Year Saw the End of an Illusion" *Wall Street Journal* December 31, 2008

What headlines such as these do not reflect is that new economic realities also create opportunities. At times such as these, businesses, governments, and other organizations have an opportunity to turn inward and consider how to better align their operations with demands and opportunities in the market. Yes, there will be painful transition periods for many, but these can also be periods of realignment that leave departments, divisions, and even entire organizations better able to respond to changes in the market.

It would be unfortunate to think of information security only in terms of "fear, uncertainty, and doubt" (FUD). The FUD perspective is one way to get attention and justify expenditures. Although we should not underestimate the risks at hand, we should not focus on them to the exclusion of opportunities to improve business operations with changes in the ways we implement and manage security. This section will first examine technical and business factors that argue for increased attention to security and then turn to opportunities for improving one overall competitive position.

Challenges: The Increased Need for Security

The increased need for security is driven by several factors, including the economic downturn. Other factors shaping these needs include:

- Dynamics of today's workforce
- Increasing sophistication of cybercrime
- Decreasing consumer confidence in information security
- Dynamic market conditions and their implications for information security

Let's consider each in turn.

Dynamics of Today's Workforce

The size and composition of a businesses' workforce is often in flux. Employees retire, move on to positions in other companies, and switch careers. Contractors and consultants are brought on and let go as immediate demand for their skills require. Mergers and acquisitions yield wholesale changes in composition of the workforce. These trends will continue but at possibly different paces.

The constriction of the credit markets that began in the fall of 2008 quickly rippled through the global economy. Demand for products plummeted in some industries, such as the auto industry. Both consumer and business spending has been curtailed. Unemployment and layoffs are up. These aggregate trends indicate that the normal dynamics of the workforce are complemented by macroeconomic factors and will ultimately have an impact on information security.

The most obvious change is staff reductions. Any time an employee leaves a business, their access privileges have to be rescinded. In an ideal situation this task can be accomplished by updating a centralized identity management and access control system. Less ideal but more common scenarios require changes to multiple authentication and authorization systems. The task of ensuring management approvals are in place and all access controls are properly updated can involve a complex, multi-step workflow. Imagine undertaking this process for hundreds or thousands of employees at one time. The difficulties are compounded if some of the affected staff is responsible for managing access controls, especially given the increasing threats from privileged insiders.

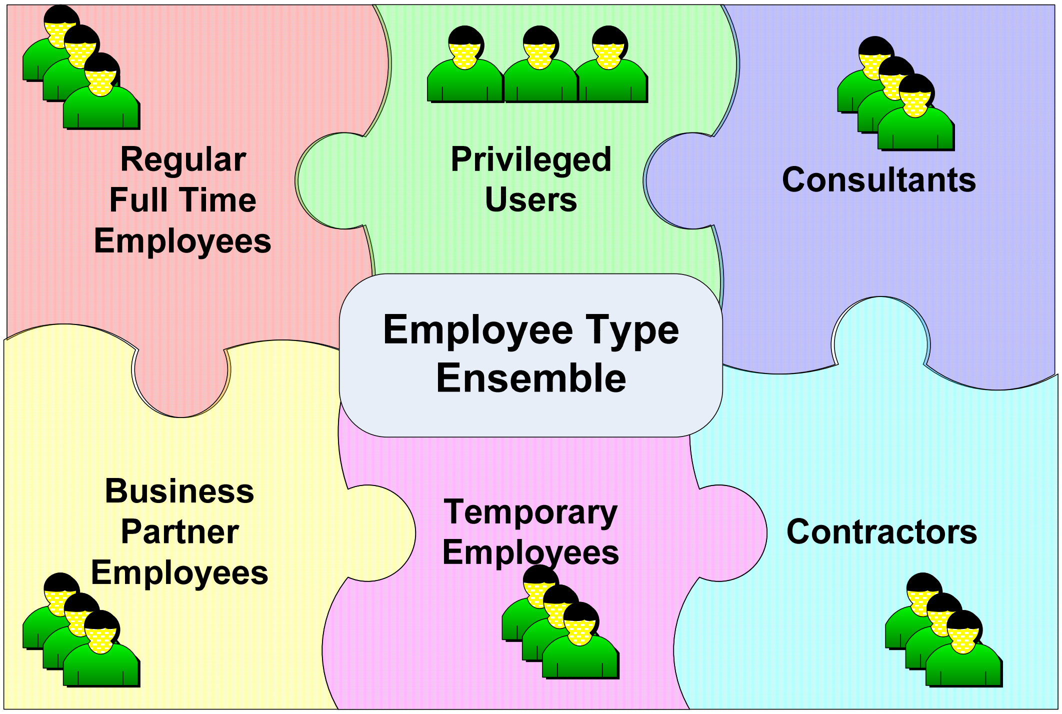

Figure 1.1: Businesses use an ensemble of staff types, from regular full-time employees to freelancers and contractors, all of which may require distinct security policies.

Another dynamic is the changing composition of the workforce itself. Regular, full-time employees work side by side with contractors, temporary workers, freelancers, business partners' employees working onsite, university researchers and temporary student interns, and even former employees brought back for special projects. Different policies are needed to accommodate the varying access privileges each of these groups will have. Introducing new types of workers can also require changes to the way policies are defined. For example, regular full-time employees might have privileges assigned based on their home departments but a contractor might not have such a designation, so access policies will have to be based on other attributes and include valid durations of time..

Increasing Sophistication of Cybercrime

Judging by organization and function, cybercrime has become an industry in its own right. There is a specialization of services, markets for exchanging goods and services, competition among providers, and prices set by supply and demand.

Cybercrime can be thought of as a vertical industry. At the bottom are malware developers and system attackers that provide the raw material of the business: malicious software and the skills needed to compromise systems. These services are leveraged by those that seek to perform the next level of cybercrime, such as stealing authentication information or creating a botnet.

> A *botnet* is a collection of compromised computers controlled by a single agent known as the *bot herder.*

The next layer in the vertical industry are phishers, extortionists, and cyber thieves who use botnets to generate spam or launch Denial of Service (DoS) attacks or commit fraud with stolen credentials. Facilitating interactions among these cybercriminals are forums for exchanging these goods and services.

As with other industries, the cybercrime market has competition to secure resources. This competition is apparent in malware that is designed to detect and disable other malware. This is especially important for bot herders who, ironically, want to protect their bots against falling victim to another botnet.

The law of supply and demand is one of the few laws followed within the cybercrime economy. Take, for example, the pricing of credit card information. Recent studies have found that a full set of credit card information, such as account number, expiration data, and so on will cost between $2 and $3 in online forums. Identity information, such as name, mother's maiden name, and Social Security Number costs about $10. Such information has become a virtual commodity where pricing is heavily dictated by short-term supply and demand.

The inner workings of cybercrime might not be apparent to the general public but its impact is clearly seen in increasing concerns about information security and demand for security legislation and controls to protect private consumer information.

Decreasing Consumer Confidence in Information Security

An average consumer does not need to go any further than their morning newspaper or favorite news aggregator to find stories about ineffective information security. Consider these recent and well-publicized examples:

- A major retailer suffered a data breach from May through December 2006 resulting in a loss of information about 40 million credit cards. Consumer data was stored in violation of credit card industry regulations.
- In 2007 and 2008, a supermarket chain *that was in compliance* with industry standards lost more than 4 million credit card records when thieves went after data in transit during the authorization process.
- A major New York bank lost tapes containing unencrypted information about 4.5 million people and 700 companies in 2008.
- In late 2008, a pharmaceutical benefits management company received extortion threats to expose millions of customer records unless the thieves' demands were met.
- More than 1 million customers of a number of financial services companies were exposed when a server from a data archiving company was sold on eBay in 2008.
- In 2007, a stolen portable hard drive used by an employee of the U.S. Department of Veterans' Affairs contained personal information about veterans and billing information for 1.3 million doctors and cost $20 million dollars just within the first 5 months after the breach.

These examples illustrate that data breaches span industries. Government agencies have also been targets. This problem is not isolated to the United States; data breaches have been reported in Europe and South America and there have been calls to strengthen data breach laws in Asia.

The cumulative effect of such stories is difficult to measure but a Ponemon Institute survey of consumer response to data breach notices found that 63% of respondents said their notices contained no specific instruction on how to protect their information, 57% lost trust and confidence in the organization, and 31% terminated their relationship (Source: Press Release "Ponemon Institute Examines Consumer Response to Data Breach Notices" April 14, 2008 available at http://www.ponemon.org/press/Ponemon_2008%20ID%20Experts%20Study%20FINAL.pdf).

Dynamic Market Conditions and Their Implications for Information Security

The ripple effects of changing market conditions can ultimately reach beyond the financial realm of business into information technology (IT) functions. Examining the full scope of these implications is beyond this guide, but we can consider several ways in which information security management is affected by dynamic market conditions—in particular:

- Identity management and staffing
- Application security and integration
- Compliance reporting
- Evolving technology adoption
- Evolving threat landscape

These topics are often interrelated and changes in one area can have an impact on others.

Identity Management and Staffing

Changes in the size and composition of a workforce create further demands for efficient and effective identity management as described earlier. In addition to those primarily internal changes, there are externally oriented issues with identity management.

The drive to find and exploit efficiencies in business processes has led to closer links between businesses. Suppliers may monitor customer inventory to ensure adequate levels while realizing the benefits of just-in-time delivery. Customers may monitor account statuses and use analytic reports provided by business partners to better understand trends in their purchasing. In scenarios such as these, federated identity management can reduce the overall burden of managing authentication and authorization.

Partners in federated identity relationships agree to authenticate users in their companies and vouch for their identities. When a user accesses a service from a partner, identity information is shared with the service provider who then uses that information to determine the types of services and data that will be provided to the user. During periods of unusually high rates of change, it is imperative that all partners in such relationships keep their authentication information up to date; otherwise, there is the potential, for example, of a recently terminated employee gaining access to business partners' applications.

Market dynamics and the drive for more efficient operations can lead to complex identity relationships. These in turn require adequate policies to accommodate more finely tuned authorizations among partners. Regardless of the level of policy complexity, business partners need to attend to enrollment and credential management issues to ensure identity management services remain effective.

Application Integration and Security

The trend away from monolithic applications to distributed systems has enabled more flexible, adaptive, and cost-effective information systems. Distributed systems are found from back-office applications to user interfaces (UIs) built from mashups. Distinctive characteristics of distributed systems, especially those built on SOAs, entail security concerns that must be addressed:

- The need to manage multiple data streams, possibly with different risk profiles
- Increased use of encryption, which brings additional key management responsibilities
- Composite applications are more difficult to understand in their entirety and therefore more difficult to analyze for vulnerabilities
- Changes to components can occur without centralized planning and management, making the software development life cycle more challenging

The fundamental security issues—such as data classifications, key management, and secure software development—are not unique to distributed systems but are more complex than their counterparts in monolithic applications.

Compliance Reporting

Dynamic market conditions can force businesses to change how they meet compliance requirements. And challenging market conditions can create incentives to improve IT controls to better align with industry and regulatory compliance reporting requirements including PCI, SOX, HIPAA, BASEL II, and so on. These improvements can occur through better data stewardship, comprehensive data classification, and effective monitoring controls.

Data stewardship is the practice of maintaining metadata about data elements to support data reuse and interchange. Such stewardship is especially important for SOAs, which need precise definitions of data elements to enable data exchange; it is also useful for compliance operations. Regulations require businesses to protect and manage some types of data in particular ways. Data stewardship practices can improve how organizations track and report on those data elements.

Data classification likewise supports compliance reporting. Some types of data are more valuable than others, and data classification schemes reflect those differences. A basic data classification scheme, for example, includes four categories: public, sensitive, private, and confidential. Public data can be disclosed without any adverse affect on the business; press releases are one example. Sensitive data includes data that should not be shared outside the company or business partners, but if it were disclosed, would not cause severe consequences. Project timetables, status reports, and invoices, for example, fall into this category. Private data, such as human resources records, and confidential data, such as trade secrets, must be protected to prevent harm to individuals and the business. An appropriately applied data classification scheme can help ensure that only data that needs to be subject to rigorous, and sometimes costly, controls is in fact subject to those measures.

Consolidation of monitoring controls is another way to improve compliance reporting. Many regulations overlap in their areas of focus. Consider, for example, the many state laws protecting consumer privacy and industry regulations, such as the Payment Card Industry (PCI) data security standards. There is significant overlap in the data protected by these regulations and consolidated monitoring controls can address multiple regulations at one time.

Despite the invariant need for compliance during recessionary periods of the business cycle, such times also present ample opportunities to adopt new technologies.

Evolving Technology Adoption

IT is constantly improving, sometimes in incremental changes and in other cases in more radical ways. Faster processors, higher-capacity hard drives, and faster network switches are examples of incremental improvements in technology. They allow us to do what we do faster and cheaper. Other changes are more fundamental and can dictate the transformation of entire business processes or management procedures. Three such technologies include

- Virtualization
- Cloud computing
- Mobile devices

Each of these is noteworthy from a management perspective because they each introduce new sets of security concerns.

Virtualization

Server virtualization and storage virtualization enable more efficient use of computer and storage resources. The ease with which virtual servers can be set up and taken down while meeting the needs of many different applications at a fraction of the cost of physical servers has led to their widespread adoption. The disadvantage of such ease has come to be known as *virtual server sprawl*.

Virtual servers need to be managed and controlled because they have specific security requirements that do not always have counterparts in physical servers. These include:

- Virtual machine instances continuing to run even when they are no longer needed
- Unnecessary consumption of licenses
- Stale machine images that are not patched
- Potential for a malware-infected image to be deployed to production because the image has not been scanned with the latest antivirus signature databases

Cloud Computing

Another promising technology for improving the efficiency of computing services is cloud computing. The economics behind cloud computing make for a compelling argument to adopt the technology: there is little or no requirement for capital expenditure, no need to maintain peak capacity resources, and the burden to constantly maintain physical disaster recovery centers is eliminated. A move to a cloud environment brings with it the need to modify management operations.

Service level agreements (SLAs) will have to be in place to ensure resources are available when needed. For example, an SLA may dictate the maximum time required to bring a cloud server online, minimum percentage of uptime, and recovery point policies in case of a server or storage failure. Data protection measures should also be considered. If data is transmitted and stored in encrypted form, key management will be a concern. For large enterprises or multiple cloud applications, there will likely be multiple storage domains, each requiring distinct sets of encryption keys. Needless to say, losing the encryption key to a set of strongly encrypted data is equivalent to losing the data itself. Cloud service providers and their customers need to address broad security issues, such as securing cloud infrastructure, securing data in the cloud, and providing additional cloud-based security services as needed by customers.

Mobile Devices

Mobile devices have unfettered many of us from the confines of the office without sacrificing the ability to communicate with colleagues or work with data and applications. Initially, the security concerns around mobile devices were similar to those of remote offices. Virtual private networks (VPNs) provided secure communication while asset management, patch management, and other administrative applications kept the overhead costs in check. As long as remote employees and “road warriors” were using company-issued laptops, the security regimen and management protocols were clear and relatively effective. Today, mobile devices comprise much more than company-issued laptops.

Blackberry smartphones and iPhones are ubiquitous in the business world. Corporate emails, spreadsheets, and sales lists are accessed and sometimes stored on these and similar devices that are fundamentally different from corporate-issued laptops—and not in terms of computing power or storage capacity. To begin with, these devices may not be running operating systems (OSs) supported in the business and there may be limited support provided to users. As these devices may be owned by the employee, and not the business, there are limits to how much control IT departments have over patching, use of encryption, use of passwords, and other security measures. There may be fewer technical controls on these devices, so user training about sound security practices is even more important than in other cases. One of the last things a manager wants to hear is that an employee’s iPhone containing confidential documents and customer data was just stolen.

Technologies such as virtualization, cloud computing, and the widespread adoption of mobile devices can be a boon for innovation, especially when coupled with other enabling tools, such as mashups. With new technologies, however, come new risks.

Evolving Threat Landscape

The last set of challenges we will examine is the evolving threat landscape. This topic deserves a full-book length treatment but, for our purposes, the focus is on four representative examples that illustrate the breadth and depth of threats faced by businesses today:

- Increasingly complex blended threats
- Sophisticated evasive techniques
- Resilient malware
- Application-specific attacks

Let’s begin with a look at how early and relatively simple computer viruses have led to an array of multifaceted types of malware.

Increasingly Complex Blended Threats

Early malicious software was transmitted through shared floppy disks and did little more than display taunting messages to their victims. Today’s malware is transmitted in ways that were not even possible during the advent of the computer virus and are far more malevolent than its predecessors.

Email proved an effective method for transmission of malware although antivirus and content-filtering software is effective against these threats. Infecting Web sites with malicious content to produce “drive-by downloads” is an emerging method that exploits weaknesses in server security and browser technologies to distribute malicious software. The payload carried in contemporary malware often includes multiple pieces of code and is known as a *blended threat*. Such malware can include worms to replicate the threat, Trojans to mask the malicious content of an apparent utility, keyloggers and video frame grabbers to capture login credentials and other valuable pieces of information, and command and control modules for communicating with servers that provide updates and issue commands to carry out specific tasks on compromised devices.

Of course, malware is of little use to those who took the time to develop and distribute it if the code is detected and eliminated before it infects target machines. Malware developers have cultivated admittedly impressive techniques for hiding the presence of their code.

Sophisticated Evasive Techniques

Evasive techniques, such as rootkits and anti-forensic techniques, are used by attackers to reduce the risk of detection. Rootkits are sets of programs designed to hide the presence of programs and related files on disks as well as to conceal running processes. Rootkits may alter low-level operating system (OS) code, such as libraries used to list running processes. This alteration is especially problematic because it calls into question the validity of any information provided by a compromised OS. Formatting a drive and re-installing the OS is often considered the only reliable way to remove a rootkit.

Anti-forensic techniques are used by attackers to cover their tracks. Tricks such as altering time modification metadata in file headers, hiding data in null directory entries, and using RAM rather than disk storage are just some of the ways to disrupt forensic investigations. Considering how long some attacks have persisted, such as the retailer that lost more than 40 million credit cards, it is reasonable to assume that a collection of anti-forensic techniques were used in such cases.

Resilient Malware

One of the hallmarks of a well-designed system is that it gracefully degrades under adverse conditions. A network component in the Internet may fail but traffic will be rerouted around the failure. A single drive in a disk array may fail but read-and-write operation can continue. The same software engineering principles that work well for legitimate applications work for malicious software as well. A command and control server for a botnet may be shut down but another server will assume the role of the offline server and allow the botnet to continue to function. The same software engineering principles that work well for legitimate applications work for malicious software as well.

The *Washington Post* reported in November 2008 that spam levels across the Internet dropped significantly after Internet service providers (ISPs) cut off access to a major U.S. service hosting botnet-related activities (Source: Brian Krebs "Host of Internet Spam Groups Is Cut Off," *Washington Post*, November 12, 2008; available at http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html). Within 2 weeks, the botnet was back. The designers had encoded an algorithm to generate new domain names should the old domains become inaccessible. The bot herders needed only to register the newly generated domain names and assign their servers to them.

Application-Specific Attacks

The final example from the evolving threat landscape is application-specific attacks. Unlike broadly targeted malware and phishing scams, application-specific attacks are designed to exploit the particular vulnerabilities of a business or government application. Attackers may use vulnerabilities in unpatched software running in the application stack, weak network security to gain access to servers, or SQL injection attacks to steal or tamper with data in relational databases.

When summarizing the nature of security challenges, it is safe to say the combined impact of the dynamic workforce, the increasing sophistication of cybercriminals, the threat of decreasing consumer confidence in information security, and the various aspects of dynamic market conditions and their implications for information security pose a considerable set of risks unlike those seen in earlier eras of business computing. However, it is important to also remember that adverse conditions create opportunities if businesses are able to see beyond the obvious negative impacts of the situation.

Opportunities: Leveraging Increased Security for Broad Business Advantages

Keeping in mind that we should view security as a business-driven operation, we will realize that formulating strategies and implementing controls to address the challenges previously outlined also serves a broader purpose. Business-driven security creates a framework of security controls and solutions that can help sustain a business. To some, these may appear to be unintended consequences—additional benefits that were unplanned for. That is one way to look at it, but it is a limiting view.

Business-driven security strategies focus on risks from a business perspective so that an organization can align security to achieve the most important business goals. In an ideal world, such security measures would allow businesses to purse business strategies without any concern for the litany of challenges and risks that were just discussed. We are not nor will be at that point in the foreseeable future. Nonetheless, opportunities are open to businesses' with sound security measures in place; such are opportunities are not available to others with less control over their environments.

Once again, rather than try to describe all possible ways security controls create opportunities, let's explore several representative examples, such as:

- Enabling secure collaboration
- Optimizing return on investment (ROI)
- Consolidating business processes
- Establishing competitive advantages

One of the most basic requirements for a functioning business is the ability for colleagues to communicate.

Enabling Secure Collaboration

Project teams and established business operations groups often draw members from different departments located in different offices, different geographies, and sometimes in different companies. To operate effectively, they need to be able to communicate and share documents, tools, and databases—in short, they need to collaborate on their work products.

Given the litany of threats to information security, from malware to application-specific attacks, it is understandable for business executives to hesitate to roll out new applications or services to support collaboration. Is reducing the time it takes to complete a complex workflow worth risking a compliance violation and the accompanying impact on reputation and brand value? Of course, the sales staff would be able to respond to customer inquiries faster with access to databases and documents through their mobile devices, but what assurances are there that the risk of a data breach is mitigated? With a business-driven security strategy, these types of concerns are accounted for and addressed *before* the specific requirements of such initiatives are defined.

Optimization of Return on Investment

“Do more with less” is an often-repeated mantra in the halls of IT departments. The drive for cost optimization is as old as competitive markets, but new kinds of security concerns can impede it. Assuming decision makers act rationally, they will not make changes unless the expected outcome is better than if one continued with the status quo. Uncertainty about security can introduce unknown risk factors that cannot be quantified or qualitatively reasoned about. Answers to questions such as “What are the best ways to ensure our confidential data is protected?” and “How do we leverage existing security systems and practices to protect internal data while we increase business partners’ access to back office systems?” may determine whether a cost optimization measure is taken. Of course, the cost of implementing and managing security measures also factors into such decisions; for example, a managed service may provide higher-quality controls at lower costs than a comparable in-house implementation.

A comprehensive security strategy driven by business requirements can provide a foundation for reasoning about risks, benefits, and levels of uncertainty that is required for a rational approach to cost-optimization decisions.

Business Consolidations

Business consolidations are difficult operations—duplicate functionality needs to be eliminated, data must be migrated, and new systems incorporated into existing asset management procedures. The process can be made easier when a security framework is already in place. For example, data classification policies can be used to categorize new data, asset and patch management procedures could be applied to newly acquired devices, and identity management systems would be in place to accommodate new employees. Having these and other security controls in place reduces the chance that compliance or security concerns will derail an otherwise sound business consolidation.

Establishing Competitive Advantages

Of course, not all businesses commit to the same levels of risk management and information security. For those that take these issues seriously, there are opportunities to establish competitive advantages through risk management. Consider the potential areas in which risk management can improve business operations and customer perception:

- A company with sound privacy controls is less likely to suffer a customer relations nightmare of having to deal with a massive security breach. As the previously mentioned Ponemon study found, 57% of customers involved in a data breach lost trust and confidence in the organization and 31% of them terminated their relationship with the company. What better place for that 31% to turn than a competitor without a well-publicized security breach?
- Companies spend years and valuable resources building brands that should be protected. Staying in compliance, actively monitoring data and assets for security incidents, and keeping security strategies linked to business strategies can help reduce the possibility of a brand-damaging incident.
- Information systems can make large-scale intellectual property theft seem almost trivial. For example, a former employee of a major chip manufacturer accepted a position with a competitor and before leaving his former position, downloaded $1 billion dollars worth of trade secrets, including more than a dozen documents categorized as “top secret” in the company’s data classification scheme. Well-managed identity and access management and careful security event and information management controls contribute to protecting valuable intellectual property.
- Well-formulated business strategies are often more cost effective than *ad hoc* responses to market conditions. The same is true with IT and security operations. When risk management procedures are in place, they can be tuned, improved, and replicated across different parts of the business.

Information security is certainly about mitigating risks, containing threats, and complying with regulations, but that is not the whole story. The security environment is a subset of the broader environment that businesses operate in. Changes in those environments create challenges and opportunities; the two go hand in hand. How a business responds to those changes dictates how well the business benefits from or is harmed by those changes.

Aligning Security with Business Operations

A key to benefiting from today's dynamic business and technical environment is properly assessing the security priorities and risk posture of our businesses.

Assessing Security Priorities

Security priorities will vary from one industry to another and one organization to another. Critical issues in finance and banking may be dwarfed by other considerations in healthcare. Retailers with a strong online presence may have greater concerns about securing transactions across multiple channels than a comparable retailer concentrated on brick-and-mortar outlets.

Even if a CEO in a business decided today that the company would adopt a business-driven security strategy, it would be starting with assets, information, and security controls already in place. How well protected are these? What are the strengths and weaknesses of existing security measures? The answers to these questions constitute the risk posture of the business and describe the starting point for optimizing security spending.

Optimizing Security Spending

To optimize security spending, a business must understand the risk posed to the assets they value. Earlier, this chapter described a range of risks that businesses will face to varying degrees. It is important to identify those risks that are most relevant to your business. Many well-written guides are available on the basics of risk assessment; that content will not be duplicated here. Instead, this discussion will assume that you will use such techniques as necessary to assess threats, their probabilities, and the overall potential costs to the business.

Throughout the remaining chapters, this guide will describe ways to maintain effective security practices in dynamic environments, address particular concerns about new technologies and IT service delivery models, and document best practices for prioritizing security spending. How those topics are addressed is influenced by a few principles.

First, business strategy dictates security strategy. There is no ideal state of security independent of business objectives and means of execution. It does not make sense to try to meet some checklist of security best practices that does not take into account what the business is trying to accomplish and how it is constrained by market conditions, government regulations, and other external factors.

Second, security technologies and practices are constantly improving and threats are changing. As a general design principle, we should employ countermeasures that protect against multiple threats. For example, content-filtering appliances can scan incoming traffic for malware as well as spam and phishing lures. This principle is complemented by the final principle.

Third, countermeasures should be combined to maximize the total amount of risk that is mitigated. Just as one countermeasure can address multiple threats, multiple countermeasures should be deployed to address a single threat. This practice, known as *defense in depth*, acknowledges that security controls are not perfect. Antivirus software misses some malware. Vulnerability scanners do not detect all flaws. Background checks on employees cannot detect future motives. As you deploy security controls, it should be done in a way that realizes the goals of defense in depth in the most cost effective manner.

Aligning security with business operations is crucial to ensuring that security measures are relevant and that business needs are met.

Summary

The recent economic downturn in combination with significant advances in the success of cybercrime activities is creating an especially challenging environment. Factors such as the dynamic workforce, evolving technologies, and compliance issues create both challenges and opportunities for businesses; how they respond dictates whether they will benefit or suffer from these changes. Security strategies can be as important to creating competitive advantages as they are to preserving existing business assets and operations. The next chapter focuses on the details of how to realize those benefits by maintaining effective security practices.