Realtime publishers

The Shortcut Guide™ To

Prioritizing Security Spending

sponsored by

IBM®

Dan Sullivan

Copyright Statement

Chapter 2: Maintaining Effective Security Practices in an Increasingly Complex Environment

Infrastructure is a term we have adopted in information technology (IT) to describe the information assets of an organization, including hardware, software, data, and procedures. It is an apt term. After all, roads, bridges, and tunnels of a country's transportation infrastructure enable the flow of people and goods while IT infrastructure enables the flow of information. Both are essential for modern commerce. Even so, we do not have to push the analogy too far though to see it break down.

Roads and bridges are built to last for decades with occasional maintenance work. A 10-year-old map may not be perfectly accurate but it is probably pretty close. Although transportation infrastructure is relatively static, information infrastructure is anything but. Desktop devices are updated every few years, and servers even more frequently. Software seems to be in a constant state of change as it is modified and redeployed to meet changing business requirements. Even the technologies that underlie infrastructure change. The advent of virtualization, inexpensive storage, and ubiquitous high-speed networking has provided the foundation for cloud computing. Smartphones and wireless communications are changing the way businesses communicate and collaborate with employees, business partners, and customers. Changes in IT infrastructure are not limited to smaller computers or less expensive network equipment: new infrastructure is changing the ways we design systems and deliver services.

The dynamics of IT bring benefits and challenges. Take, for example, the need to provide customer support. In the past, customers would expect to pick up a phone, call a toll-free number, and talk with a customer representative about a problem with a new product or a question about the customer's account. Today, expensive customer support call centers have been replaced with voice response telephony, online self service support, and even collaborative forums in which customers help each other. These kinds of unquestionable efficiencies introduce problems that did not exist prior to the advent of e-business. Thieves can steal customer information and intellectual property without ever setting foot in a company's offices or stores. Disgruntled employees can sabotage an application and corrupt databases from their desks. Unsuspecting customers can fall victim to a phishing scam that uses your business as bait. The increasingly complex IT environment requires sufficiently adaptive security management practices to realize the benefits of change without falling victim to it.

This chapter considers the fundamental requirements for protecting business operations with an emphasis on three over-arching goals:

- Protecting the confidentiality of information by preventing data loss
- Preserving the integrity of information by preventing malicious operations on data
- Ensuring the availability of services by maintaining infrastructure efficiency

These three goals are subject to the same demands for efficiency as any other business operation. For that reason, this chapter will also address the need for maintaining both overall business operation productivity and security administration efficiencies.

A combination of technologies and practices can serve to protect assets and maintain operational efficiencies. Let's start our examination of that topic with a look at basic requirements for protecting business operations.

Protecting Business Operations in Complex Environments

Information security is traditionally seen as the practice of protecting and preserving the confidentiality, integrity, and availability of systems and data. Confidentiality reflects the need to limit access to certain types of data, such as customers' personal and financial information, critical financial operations information, and a business' trade secrets and other intellectual property. Confidentiality ensures we can keep information private. Integrity is a matter of preserving the accuracy of data and not allowing unauthorized changes to data. Integrity ensures we can trust the data we have. Availability ensures that data and services are accessible and functioning when needed. In addition, availability makes sure that business operations are not disrupted by malicious or unintended activity. In today's businesses, preserving these three qualities of IT operations is a challenge.

Confidentiality: Preventing Data Losses

Preventing data loss is a major concern—and with good reason. It is difficult to go more than a few weeks without hearing about another data breach. Just consider the following recent statistics. The Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm) has gathered reports on data breaches in the United States since 2005. It lists 21 breaches in November 2008, 17 in December 2008, and 17 in the first 3 weeks of January 2009. The organizations on the list include a credit card processing firm, government agencies, schools and universities, financial services firms, and hospitals. The means by which these breaches occurred varied and include stolen or lost laptops, stolen backup tapes, insider abuse, data-stealing malware, unencrypted transaction communications, and hacking attacks on applications and servers.

Even from this small sample, we can discern three key points to remember about data breaches:

- These are not infrequent incidents widely publicized to simply to promote the interest of those who depend on the "fear, uncertainty, and doubt (FUD)" approach to marketing their business.
- Data breaches are not limited to any one type of organization. Large and small businesses; federal, state, and local governments; profit and non-profit organizations; and financial and non-financial businesses across all industries have all been victims of data breaches.
- Data breaches occur in many ways, from leaving a car unlocked with a laptop inside to poorly validated application input that allows SQL injection attacks to technical vulnerabilities in boundary security exploited by skilled attackers.

If these examples are not enough to convince you of the breadth of data breach risks, browse the content of the Privacy Rights Clearinghouse Chronicle of Data Breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm), The Data Breach Blog (http://breach.scmagazineblogs.com/), or the Open Security Foundation's Data Loss Database (http://datalossdb.org/primary_sources); for examples of data breaches involving intellectual property theft, see the US Department of Justice's Computer Crime and Intellectual Property Section Web site (http://www.usdoj.gov/criminal/cybercrime/index.html).

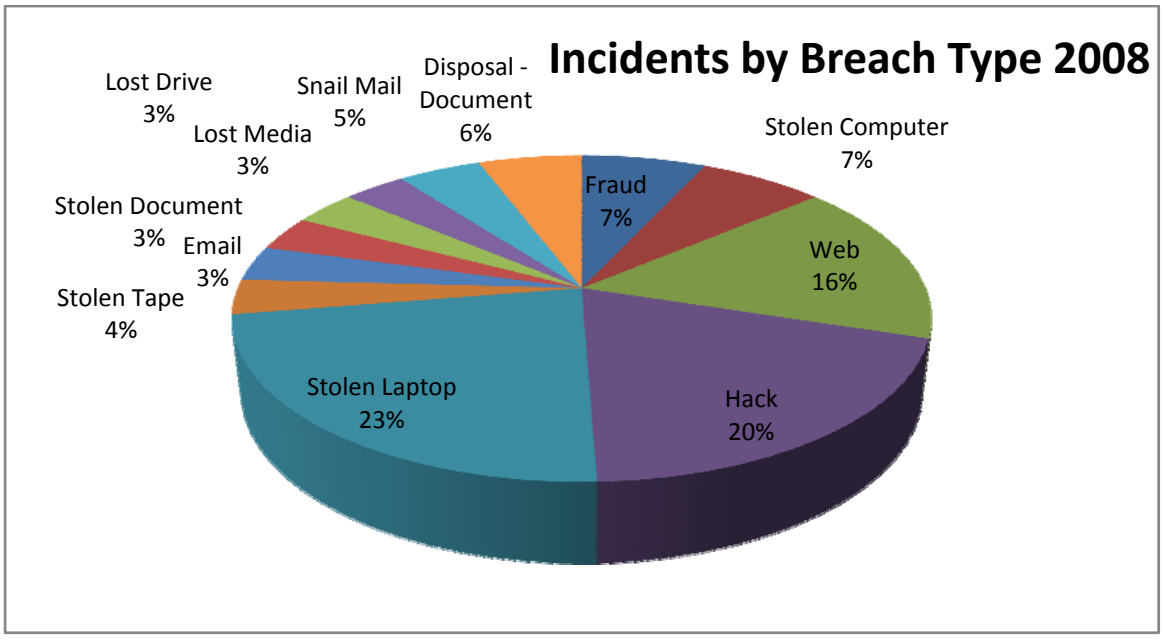

Figure 2.1: In 2008, stolen laptops, attacks on systems ("hack"), and Web-based attacks constituted the majority of data breach methods, but attackers have other methods as well (Source: Open Security Foundation and DataLossDB.org at http://datalossdb.org/statistics?timeframe=last_year).

The risk of a data breach is like a flu epidemic: you know it is out there, it seems to be spreading, and while you appreciate the aggregate statistics about how bad it is, a major concern is what happens if it hits you. Let's take a look at an example to see just how far the ripple effects can spread.

Retail Industry Data Loss Example

A well-known retailer suffered a data breach in 2006 resulting in the loss of information about 45 million payment cards. With so many data breach cases to choose from, one might expect a description of a less well-known incident. This case is illustrative for several reasons related to the type of data stolen, the amount of data stolen, and the ultimate impact on the business.

Summary of Attack

In late 2006, the company discovered that its payment processing system had been attacked and an intruder had gained access to customer payment information. The breach affected customers in Canada, the United States, Puerto Rico, the United Kingdom, and Ireland. The retailer notified the US Secret Service and comparable agencies in other countries and conducted an investigation into the breach. In addition to credit card data, the retailer collected names, addresses, and driver's license numbers in relation to un-receipted merchandise returns.

The intruders might have gained access from outside of two stores in Florida using a decryption tool to compromise the Wireless Encryption Protocol (WEP) that was in use at the time. Also, other data transmissions, such as the to-payment card processor, were not encrypted. Detecting the breach and the subsequent investigation were made more difficult by the fact that intruders used anti-forensic measures to remove indications of their presence.

Consequences of the Attack

The attack on the retailer was widely reported. One might assume this would cause damage to the retailer's brand but such consequences are difficult to quantify. Other responses were clear and included:

- Banks issued thousands of replacement credit cards for customer's whose data was compromised during the breach
- Banks almost immediately started to report increases in fraudulent activity thought to be related to the breach
- Within weeks of announcing the breach, the banks filed a class action lawsuits seeking tens of millions of dollars in damages for costs incurred by the banks in response to the breach

- A number of shareholders filed suits against the company
- Just in the first quarter of 2007, the company spent $12 million to investigate the incident, upgrade security, cover legal fees, and communicate with customers
- The company was investigated by a number of government agencies including multiple states' Attorney General offices, the US Federal Trade Commission (FTC), and the Privacy Commissioner of Canada.

As this list demonstrates, the consequences of a data breach can have material repercussions beyond the cost of investigating the breach and preventing future breaches.

Especially Notable Points About the Attack

In the spirit of learning from the past, it is worth noting several other points about the breach. Although this example comes from the retail industry, the lessons learned are applicable to IT security practices in general.

An organization is damaged by a breach and so are its clients, customers, stakeholders, and business and organizational partners. Ours is a highly interconnected world and businesses, government agencies, and other organizations have a wide array of relationships. In the case of the retailer, the company maintained confidential financial and personal information and when it was stolen, others suffered as well. A similar situation could arise in the case of a company sharing intellectual property with a business partner and that partner losing it in a data breach. Data is a valuable commodity, sometimes more valuable than tangible brick-and-mortar assets.

A business case can be made for storing more information than necessary for a transaction, but that practice could introduce unanticipated risks. In the case of the retail stores collected driver's license numbers and addresses when merchandise was returned without a receipt. One can easily imagine how this data could help reduce the likelihood of fraud related to returns and so it appears at first to be a legitimate reason to collect information. There are two potential problems.

First, collecting extra information may violate industry or government regulations. Care must be taken to review relevant privacy regulations. This task is especially challenging for large enterprises that operate in many jurisdictions. For example, 44 states have data breach notification laws in addition to federal regulations that apply to specific industries. Companies serving global markets have to attend to other national regulations, such as Canada's Personal Information Protection and Electronic Documents Act and Australia's National Privacy Principals as well as trans-national regulations such as the European Union's Directive on Data Protection.

The second problem is that once the organization collects that data, the organization is responsible for protecting it. This task is an added burden with regards to determining data classification, protecting the data in transit and during storage, ensuring backups and copies made for disaster recovery purposes are properly managed, and so on. Data is moved and duplicated for a variety of legitimate reasons but they multiply the amount of effort and resources required to protect it. Organizations should be prepared for managing the full life cycle of data. They should not be lulled into optimistic assessments of the costs of collecting data by focusing only on the initial collection and storage requirements.

Cost of Data Breaches

Data breach costs can be difficult to estimate because there can be so many ripple effects from a breach that make it difficult to identify all costs associated with the loss. Nonetheless, there are sufficient data sources based on surveys to at least develop a rough estimate of the cost of data breaches.

The Ponemon Institute (www.ponemon.org), a research group specializing in information and privacy management, conducted annual surveys on the cost of data breaches from 2005 to 2008 The cost per record lost increased roughly 30% each year up to 2007; 2008 saw a small increase of about 2.5%.

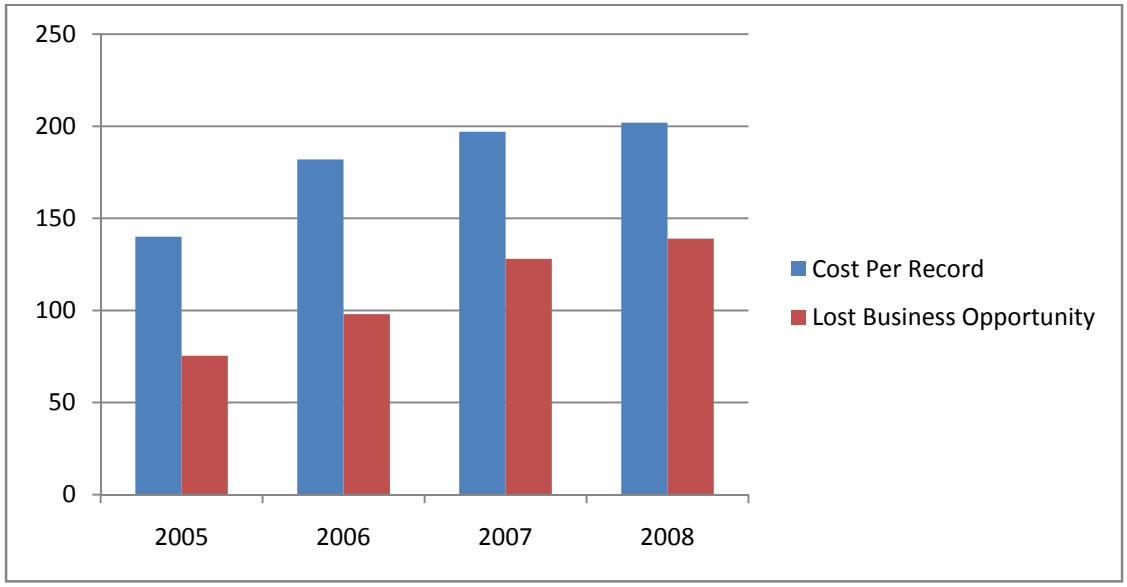

Figure 2.2: Ponemon annual cost of data breach survey findings show roughly a 30% increase per year in cost per record lost and cost due to lost business opportunity.

The total cost of breaches is, of course, also a function of the size of those breaches. The Open Security Foundation has tracked data breaches back to 2000 and a summary of their statistics are shown in Figures 2.3 and 2.4.

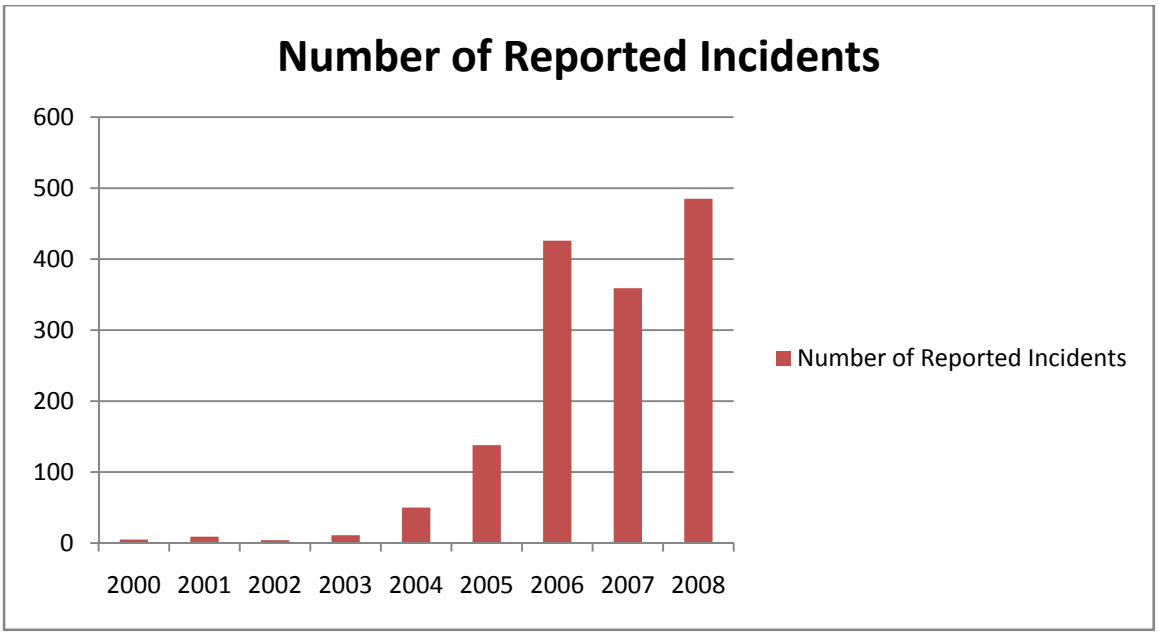

Figure 2.3: The number of incidents reported by DataLossDB.org has generally increased since 2000. The large increase after 2005 may be due to better reporting of breaches, an actual increase in breaches, or a combination of both.

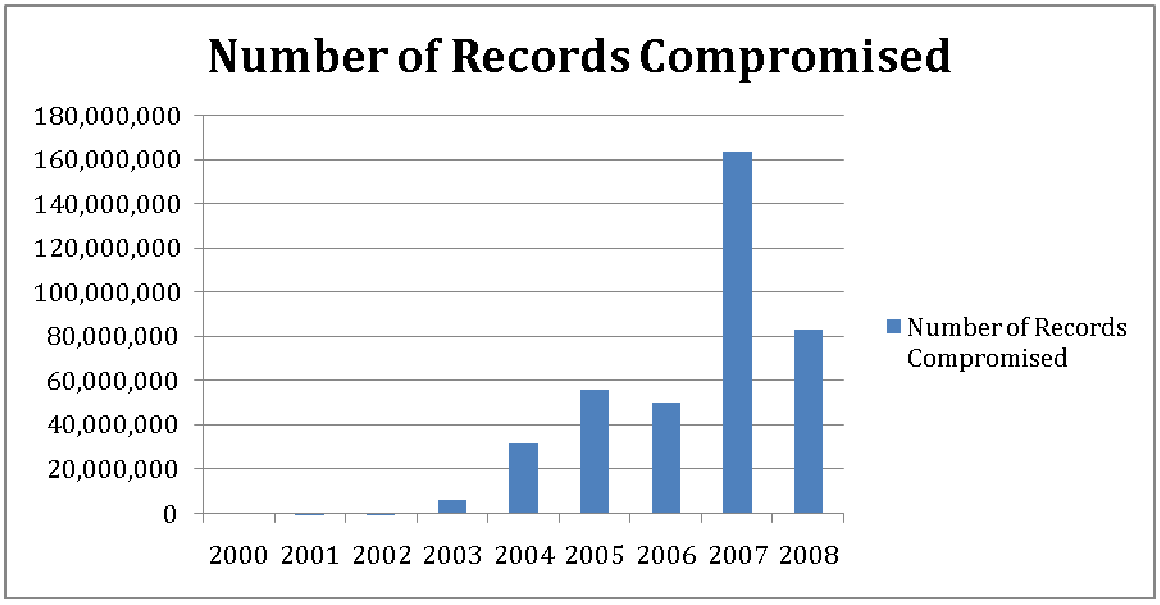

Figure 2.4: The size of data breaches is on an upward trend, with 2007 significantly higher in part due to the large breach at one company.

Security technologies and practices can reduce the risk of data breach and the earlier they are deployed, the sooner the benefits begin. Technologies to consider with respect to protecting confidentiality include encrypting data, both during storage and transmission, identity and access control systems, endpoint security controls, intrusion prevention systems (IPSs), and security management reporting systems.

Integrity: Protecting the Accuracy of Data

Keeping data safe from tampering is another critical requirement. Consider the impact on an organization if

- Details about a sales transaction were changed so that a customer received more than the customer actually paid for
- A disgruntled employee tampered with database records and linked customers with invoices belonging to other customers
- An attacker tampered with monitoring logs to erase evidence of a new privileged account created on a financial management application
- A employee in the finance department embezzled funds and changed ledger entries to hide the theft
- Patient healthcare records were tampered with so that invalid procedures were performed and incorrect medications were prescribed, resulting in literally life or death situations

Clearly many of our day-to-day activities in business and government assume that we can trust what our data tells us.

Access controls and identity management play a central role in maintaining data integrity. These two practices and technologies can effectively manage the range of operations a person or program can perform on data. They depend on appropriate classification of data and proper assignment of roles to individuals, at least in the form of their digital identities. Of course, an employee with legitimate access to data might change it without a business justification, so monitoring and auditing are also essential to preserving data integrity.

External threats to data integrity are addressed, to some degree, by access controls and identity management, but more is required. For example, an operating system (OS) vulnerability that allows an attacker to gain elevated privileges will not be hindered by conventional access controls. A combination of vulnerability assessments, patch management, and monitoring can mitigate such risks from external threats. This reality shows the importance of a defense-in-depth strategy: no one control should be counted on to protect an asset; multiple overlapping controls should be used to reduce the risk of any one of the controls failing. Another aspect of protecting business operations is ensuring the availability of systems and data.

Availability: Keeping the Proverbial Lights On

Keeping systems functioning effectively and efficiently is difficult because of the inherent complexity of the systems themselves and the business processes they support. Malicious activity compounds the problem.

Availability is best thought of in terms of a continuum rather than a simple "on/off" distinction. Consider several examples:

- An email system may be available so that users can send and receive messages, but if the user has to manually filter out spam, phishing messages, and malware-laden messages, the effective availability of the system is reduced
- A relational database server compromised with botnet software may have slower response time to user queries because the malicious software is consuming I/O resources needed by the database
- A workstation riddled with spyware functions will perform basic operations more slowly because legitimate applications must compete with the spyware for resources
- Routine maintenance operations are less efficient because spam and other unwanted content imposes a burden on storage and backup operations as well as, in some cases, compliance efforts

Another example of malicious activity adversely affecting malware is the existence of botnets. These are networks of computers controlled by an attacker, commonly known as a bot herder, who utilizes the storage and compute resources of compromised computers for generating spam, launching Denial of Service (DoS) attacks or other activities that require significant computing or network resources. In some ways, botnets are cybercrime's version of cloud computing: on demand resources without the overhead of capital investments and ongoing maintenance. Owners of compromised devices typically continue to use their computers but at lower performance levels. In extreme cases, such as the DoS attack on the two main Internet Service Providers (ISPs) in the central Asian republic of Kyrgyzstan that essentially shut down the Internet in the country, the damage can be widespread. (Source: Christopher Rhoads, "Kyrgyzstan Knocked Offline" *Wall Street Journal,* January 28, 2009.)

Performance is also reduced when devices are infected with spyware and malware. Spyware may require compute cycles and thus compete with legitimate applications. If a device is infected with enough spyware, the impact on performance is noticeable.

Protecting business operations is, in part, a process of assessing risks to the confidentiality, integrity, and availability of information, applications, and infrastructure. Another important component is the implementation of controls to mitigate those risks as efficiently as possible.

Optimizing Staff Efficiency

The challenges of optimizing staff efficiency with regards to security practices can be broadly divided into those having to do with maintaining overall productivity and those focused specifically on security administration efficiencies.

Maintaining Overall Productivity

Security management practices have implications for many day-to-day operations within an organization. Some of these are obviously security related while the security aspects of others are less apparent:

- Identity management and user provisioning
- Application deployment and security testing
- Security operations
- Industry and government regulations

How well we implement each of these can have a direct impact on the efficiency of business processes well beyond IT and security management.

Identity Management and User Provisioning

Dynamic workforces require dynamic user provisioning. When a new employee begins work, she will need access to a multitude of systems, such as email, document management systems, collaboration portals, HR self-service applications, file servers, and applications relevant to her job. This complexity of the application environment in which many of us work is a good reason to automate the user provisioning process; however, controls must be in place.

In the most basic of circumstances, an employee's access can be determined by job role. Everyone is granted email access and provided with a home directory on a shared network. Other applications require more nuanced provisioning. Managers need to sign off before access may be granted to sensitive material. New users must be assigned to groups or roles appropriate to job function but these assignments may not follow any strict organization hierarchy. For example, a financial analyst may be temporarily assigned to work on a marketing project that requires access to the marketing department's document management system. When an employee leaves the organization or changes responsibilities, identity management system must be updated.

One way to improve efficiencies is to establish workflows that manage the basic provisioning operations using identity and role data stored in multi-use directories such as Lightweight Directory Access Protocol (LDAP) directories and Active Directory (AD) directories. In the case of large enterprises or a multi-organizational initiative, further efficiencies can be gained with federated identity management built on industry standards for exchanging authentication and authorization information, such as the Security Assertion Markup Language (SAML).

When federated identity management systems are used, it is important to understand the policies and practices of partners. By trusting another organization, we implicitly agree to their methods for verifying identity, granting authorizations, and properly terminating access rights as needed. This raises issues of how to perform due diligence on federated identity management partners, including:

- How frequently should federated identity partners' policies and procedures be reviewed?
- Should partners have access to audit reports on authentication and authorization practices and reports of any implementation problems?
- If a breach occurs in one partner's systems, what is that partner obliged to share with others?

Federated identity management enables more efficient flows of information across organizational boundaries, but it introduces management responsibilities that do not exist when identity management is centralized in a single organization.

Application Deployment and Security Testing

Ensuring security is built-in to the software development life cycle and that applications are well tested before deployment and continuing to patch and scan for vulnerabilities is another way to improve operational efficiencies. The old adage "an ounce of prevention is worth a pound of cure" applies to IT and security. Vulnerabilities that are found during development and before deployment avoid several factors that can hamper productivity:

- Exposing production data to potential theft or tampering
- Delaying scheduled processes due to errors in application code or configuration
- Requiring the deployment of secondary, possibly manual, procedures to compensate for application problems
- Effectively turning users into testers and service support personnel into debuggers
- The later a defect is found, the costlier it is to fix

It is important to note that even if applications appear to function according to requirements, there might still be vulnerabilities. A common problem in Web applications is the potential for SQL injection attacks. These can occur when an application accepts input from a user and without proper validation, passes it along with query code to a relational database for execution. Such attacks can be used to collect more information than legitimately required. SQL injection vulnerabilities can be detected during development; other problems, such as zero-day vulnerabilities, may not be made known until applications have been deployed. Regular automated vulnerability scanning and testing with an application security scanner can help detect such vulnerabilities even after they are made public.

Security Operations

Network operations and security operations are closely linked and depend on much of the same data and similar types of procedures. Network managers monitor network traffic to ensure key metrics, such as latency and bandwidth utilization, are in acceptable ranges. When problems arise, such as a spike in traffic, network managers will want to investigate as will security operations staff. Such a spike could be an indication of a data breach—for example, copying a database dump file to an attacker-controlled server—or the existence of unauthorized processes on machines, such as bots in a botnet generating spam or DoS attacks.

Network operations staff and information security staff can often use the same preliminary data to identify potential problems. They may both drill down into more specific data sources to identify root causes of the problem and at that point, their paths may diverge with network operations staff responding to legitimate peak demands by reallocating resources and security professionals responding to a data breach by isolating compromised devices and shutting down the attack. Combining network operations and security operations can help avoid duplicated operations, improve communications between network managers and security staff, and reduce the response time to significant security incidents.

Industry and Government Regulations

Sound security practices designed primarily to protect the confidentiality, integrity, and availability of information assets also support compliance with government and industry regulations. Measures taken to mitigate potential data breaches are clearly relevant to privacy regulations; controls that reduce the chances of unauthorized changes to information support the overall objectives of governance regulations, such as the Sarbanes-Oxley (SOX) Act. Monitoring and reporting processes can also serve multiple functions.

Security considerations permeate business operations. The fact that many of the operations performed in the name of security and compliance also support operational efficiency in general is a testament to the fundamental importance of proper security controls. As one might expect, there are even more efficiencies to consider when it comes to security administration.

Security Administration Efficiencies

Implementing effective security controls can be time consuming and, if not done properly, unnecessarily costly. Security management is in some ways like a multi-front war of attrition: there is little room to focus on one problem at a time and there are no quick victories. This is a long-term, multifaceted effort. Several of the areas that need to be addressed include:

- Consolidating compliance reporting
- Centralizing patch management
- Implementing network access controls and policy administration
- Efficiently protecting client devices
- Employing managed services to increase overall efficiency
- Centralizing security management and reporting

This is by no means an exhaustive list of security concerns; for example, there is no mention of supporting governance or disaster recovery. These are certainly important subjects but the purpose here is to focus on the efficiency of operations that are executed on a day-to-day basis.

Consolidating Compliance Reporting

Businesses and even some government agencies can face a variety of compliance requirements. Some regulations, such as privacy protections dictated by states, national governments, and trans-national governments (such as the European Union—EU), apply to many businesses. Others, such as financial services-focused and healthcare-specific regulations, are more targeted. Government-specified regulations span a range of industries:

- SOX applies to publicly traded companies and requires demonstrated protections of the privacy and integrity of company data
- The Health Insurance Portability and Accountability Act (HIPAA) regulations define privacy protections for patient's protected healthcare information and apply to medical service providers and other healthcare industry businesses, such as health insurance companies
- The Gramm-Leach-Bliley Act requires banks and financial service providers to protect the confidentiality and integrity of customers' personal information, such as names, addresses, and Social Security numbers
- The Safe Harbor framework developed by the US Department of Commerce and the EU provides a mechanism for US companies doing business in Europe to comply with the EU's Directive on Data Protection

Governments are not the only ones in the regulation business. Industries have created their own regulations in an effort to police themselves. The Payment Card Industry (PCI) data protection standards is one well-known example; the BASEL II standards of the banking industry have generated less press but are another example of industry-generated regulation.

Given the wide range of regulations, it is fortunate that many focus on protecting the fundamental principles of information security: protecting confidentiality and integrity of data and ensuring the availability of systems and data. You can take advantage of this fact to consolidate reporting and develop a reporting process that encompasses the breadth of requirements. In some cases, this can help ensure that as regulations evolve, minimal changes are required in the process. For example, a state might change the details of privacy protection reporting rules for its citizens but a comprehensive compliance reporting process may have already provided for such changes for other states.

Centralizing Patch Management

Patching operating systems (OSs), applications, and middleware should be a routine IT process. It can be put off and handled in an ad hoc manner, but doing so is less efficient, harder to track, and more likely to lead to security problems related to unaddressed vulnerabilities. In contrast, centralized patch management offers a number of efficiencies:

- An application infrastructure for tracking which devices have been patched
- Ability to respond faster to newly discovered vulnerabilities
- By combining with asset management procedures, a patch management system can provide detailed inventory information, which is useful for additional business functions, such as license management
- Support for compliance reporting

It is worth emphasizing that you can put off patching but it cannot be avoided forever, and the need for patching shows no signs of waning. Thus, centralized patch management should be considered as part of security operation efficiencies.

The reality is, however, that many systems are left unpatched due to the fact that vendor patches are just not available. According to the 2008 X-Force trend report released in January 2009, of all the vulnerabilities disclosed in 2008, only 47 percent can be corrected through vendor patches. Clearly, other mitigation strategies are required to compensate for the lack of patches.

Network Access Controls and Policy Administration

Who is on your network and what are they allowed to do? These are two fundamental questions that IT professionals must be able to answer and provide controls for. Many organizations will have to manage a large number of users with a wide range of authorization; policy-based authorizations can provide for more efficient access management than more individualized, ad hoc management practices.

Efficiently Protecting Client Devices

Client devices are proliferating well beyond the desktop; laptops and smartphones are commonly used to access corporate data and applications. A minimal set of controls on client devices include:

- Use of antivirus, anti-spyware, and personal firewalls
- Disk encryption for confidential information
- Routine vulnerability scanning and patching
- Limited use of privileged accounts

Centralized, policy-based verification of these configurations can provide more efficient and effective quality assurance than manual procedures can offer. We should note, though, that many of these controls are provided by different vendors, making policy consistency difficult to achieve.

Employee smartphones and other mobile devices are not as easily controlled. For example, in most cases, employees will not standardize on a small number of device models running similar configurations, and you cannot expect to force that standardization on employees. Similarly, a business can recommend security best practices but has little room to enforce those practices. Policies should be established about minimal acceptable configurations before sensitive or confidential corporate information or applications are accessed through such devices.

Employing Managed Services

The 17th century English economist William Petty noticed that a specialization of labor among workers in Dutch shipyards lead to more efficient ship building compared with a setup in which laborers had to perform many different tasks. What was true in Dutch shipyards is true today of IT operations centers. By having teams specialize and master a specific subset of tasks, you can more efficiently complete complex operations. Today, you have the opportunity to use managed services provided by specialists for a number of security tasks such as identity and access management, application vulnerability scanning, intrusion prevention management and monitoring, cloud-delivered event log management, firewall configuration and email encryption, to name a few. By employing managed security services for security functions, in house IT staff can focus on business-oriented tasks that cannot be easily outsourced.

Centralized Security Management Reporting

In an ideal world, we would have centralized management consoles from which we could monitor events from security applications and devices throughout the network. Today, we are still a long way from that ideal state, but improvements are being made. For example, the ability to gather consolidated logging information in a central repository is improving, allowing seemingly unrelated events to be correlated and analyzed as part of a broader security event trend. As time goes on, we expect to see continued enhancements that allow for more efficient collection, filtering, automated analysis, and reporting of log data.

Security professionals are asked to implement policies, monitor and test applications, implement controls on devices, support service desk staff, and the list goes on. Identifying and implementing more efficient ways to meet these kinds of demands is imperative to ensuring that increasingly complex security requirements are met without corresponding increases in cost.

Summary

Business, governments, and other organizations are charged with protecting the confidentiality and integrity of data and the availability of systems in an increasingly hostile security environment. The many well-publicized data breaches over the past several years are indicative of the difficulties of maintaining confidentiality. Threats to confidentiality range from carelessness with mobile devices and stolen backup tapes to vulnerable applications and well-orchestrated attacks on targeted victims. Successfully protecting the integrity of data requires careful attention to identity management and access controls. Federated identities compound the complexity of identity management operations, but the efficiencies realized with that technology can make it a compelling solution for collaborative business requirements. The availability of IT resources can be undermined by something as simple as spyware or as devastating as natural disasters. We must attend to the latter but at the same time we cannot ignore the incremental impact of "small" threats to availability.

It is essential to implement effective and appropriate security measures but doing so must be accomplished in a cost-effective manner. Some of the areas to attend to include identity management and user provisioning, application deployment and security testing, combining network operations and security operations, and consolidated management of government and industry compliance efforts. The practices outlined in this chapter provide a starting point for understanding how to efficiently deliver security controls to an organization.