Realtime
publishers
"Leading the Conversation"

The Definitive Guide™ To

Service-Oriented Systems Management

sponsored by

altiris®

Dan Sullivan

Chapter 10: Managing Risk in Information Systems....202
The Practice of Risk Analysis....202
Identify Information Assets and Threats....202
Servers and Client Devices....203
Network Devices....204
Databases....205
Application Code....206
Systems Documentation....207
Intellectual Property....208
Determine Impact of Risks....209
Types of Costs....209
Determine Costs....210
Determine the Likelihood of Threats....211
Calculating Risk Measures....211
Exposure Factors....212
Annualized Rate of Occurrence....212
Annualized Loss Expectancy....213
Qualitative Risk Assessment....214
Risk Analysis Steps....215
Understanding Business Impact of Risks....216
Operational Impacts....217
Compliance Impact....219
Business Relationship Impact....220
Customer Relationship Impact....221
Summary....221

Copyright Statement

Chapter 10: Managing Risk in Information Systems

The focus of this guide has been on the practice of systems management with an emphasis on best practices for creating and maintaining IT infrastructure. As useful and effective as these practices are, they cannot guarantee that operations will always go as planned, that projects will stay on schedule, or that adverse events will not occur. Part of effective systems management is managing the risks inherent in IT operations. This chapter will examine the following topics within the broader area of IT risk management:

- The practice of risk analysis
- The impact of risks and their implications for risk management

The goal of risk management is to understand the breadth of risks facing an organization and to formulate strategies for mitigating those risks to the greatest extent possible.

The Practice of Risk Analysis

Risk analysis is a methodical process for identifying risks and assigning a cost to those risks. The four basic parts of risk analysis are:

- Identify information assets and threats to those assets
- Determine the impact of threats to an organization
- Determine the likelihood for each threat
- Assess the risk versus the cost of countermeasures

Together, these steps provide the basic information that is needed to align risk management strategies with overall business strategies.

Identify Information Assets and Threats

The ancient Greek maxim “Know thyself” aptly summarizes the purpose of the first stage of risk analysis. It may sound almost trivial, but knowing what information assets are in place can be a challenge. Just consider examples of what falls under the category “information asset,” at least from a risk analysis perspective:

- Servers and client devices
- Network devices
- Databases
- Application code
- Systems documentation
- Intellectual property

The spectrum of information assets ranges from tangible hardware to intangible intellectual property. Each is subject to particular types of risks.

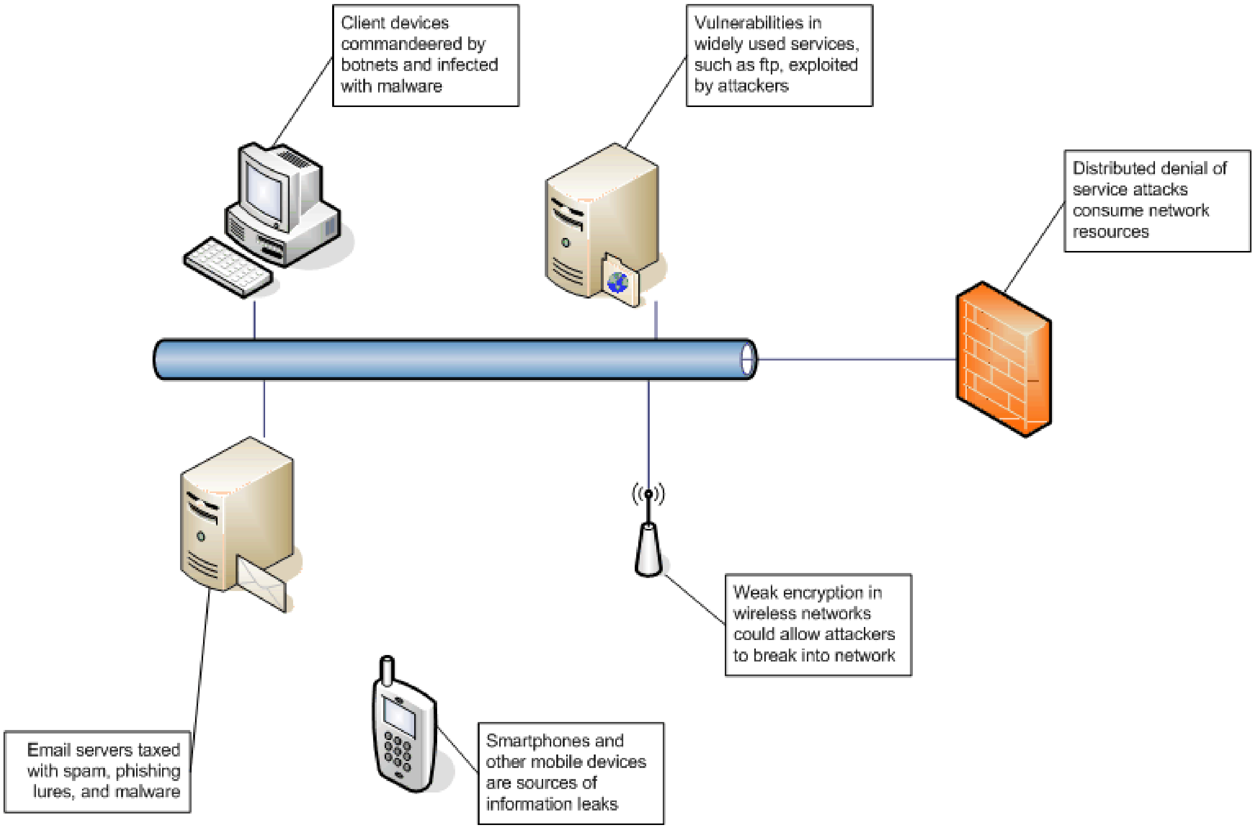
Client devices commandeered by botnets and infected with malware
Vulnerabilities in widely used services, such as ftp, exploited by attackers
Distributed denial of service attacks consume network resources
Weak encryption in wireless networks could allow attackers to break into network
Email servers taxed with spam, phishing lures, and malware
Smartphones and other mobile devices are sources of information leaks

Figure 10.1: Threats are associated with virtually every part of an IT infrastructure.

Servers and Client Devices

In many ways, the risks to hardware are the easiest to identify if for no other reason than the fact that these devices are tangible. Servers and client devices are subject to physical and logical risks. Physical risks are those that threaten the actual device, as opposed to software that runs on the device; physical risks include:

- Fire, water damage, and natural disaster
- Theft
- Electrical surges
- Component failure
- Unapproved and approved hardware changes

Logical risks can be just as disruptive; these include:

- Software bugs
- Viruses, worms, and other forms of malware
- Misconfigured applications
- Loss of backups or failure of backup media
- Unapproved and approved system changes

Network devices are subject to these threats as well as others.

Network Devices

Network devices such as routers, firewalls, intrusion prevention systems (IPSs), content filters, and other security appliances are subject to the risks of network attacks. The Denial of Service (DoS) attack is relatively simple but highly effective, especially when launched from multiple, distributed devices.

> 🕮 For an example of just how disruptive a distributed DoS (DDoS) attack can be, see Scott Berinato's "Attack of the Bots" in *Wired Magazine* at http://www.wired.com/wired/archive/14.11/botnet.html.

Other types of network attacks include:

- DNS poisoning
- IP spoofing
- Man-in-the-middle attacks
- Eavesdropping

DNS poisoning corrupts DNS servers so that URLs are redirected away from legitimate sites to a third-party site. For example, if www.myrealbanksite.com should map to 192.160.100.10 but the DNS server is modified to change the mapping to some other address (such as 180.101.10.12), a person trying to browse to the bank site may be drawn into a phishing scam without even knowing it.

IP spoofing is the practice of changing the source IP address of a packet to make it appear as if it came from another source. IP spoofing is possible because of the design of the IP protocols, but IPv6 addresses these threats.

In a man-in-the-middle attack, a third party intercepts a communication session between two other parties and can monitor, change, and interject communications between the two. Secure communications protocols are designed to prevent this type of attack, or at least raise the cost so high that it is not an efficient strategy for the attacker.

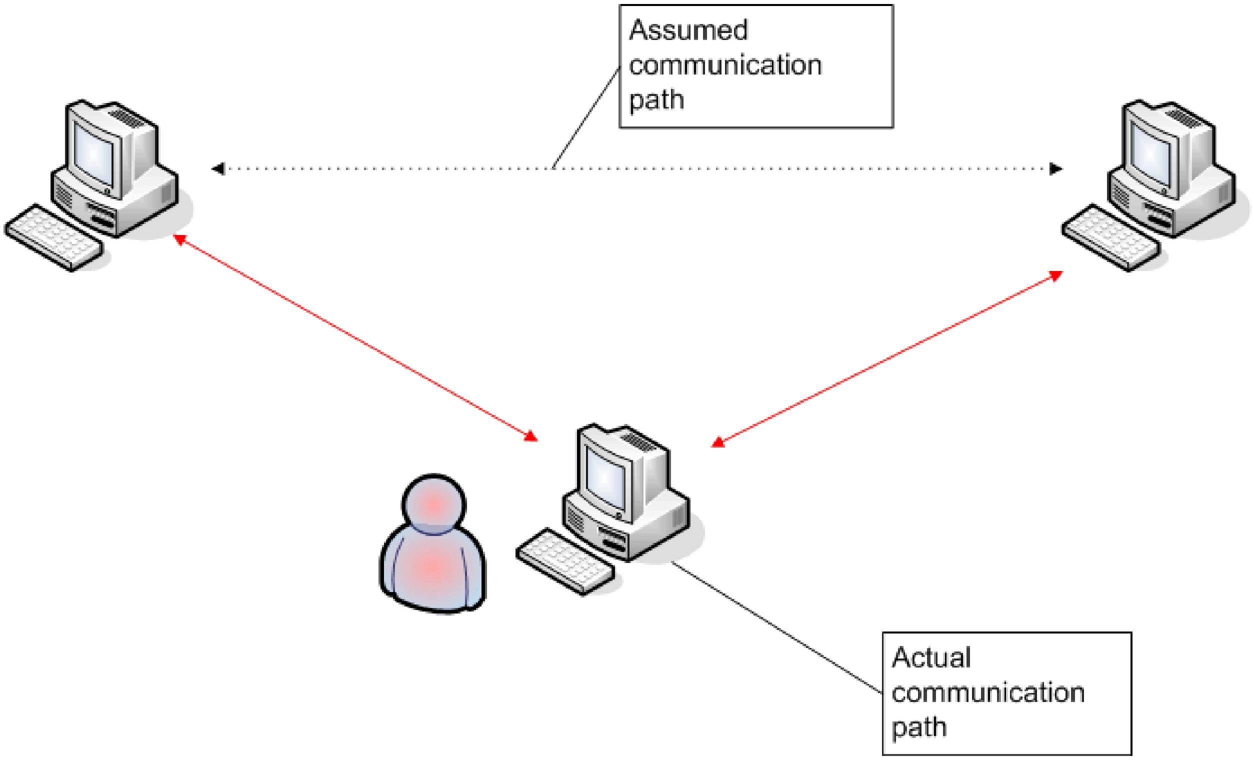

Figure 10.2: A man-in-the-middle attack entails intercepting and tampering with communications between two parties that is presumed to be secure.

Eavesdropping, of course, is monitoring the communications of other parties. Strong encryption can minimize the risk of eavesdropping.

Databases

Databases are an obvious target of attack. These are the repositories of a wide range of information, including:

- Personal information about customers
- Employee information
- Financial records
- Operational information

All databases with a user interface are subject to SQL injection attacks, which can result in data theft. In this type of attack, an attacker creates a query that exploits vulnerabilities in the interface's query processing code. There are multiple techniques for preventing SQL injection attacks, most of which are based on sound coding practices.

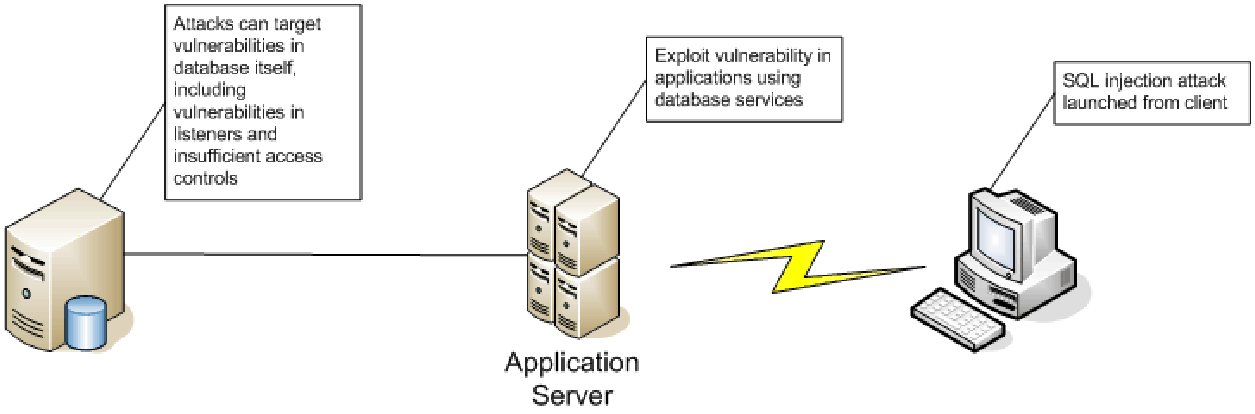
Attacks can target vulnerabilities in database itself, including vulnerabilities in listeners and insufficient access controls
Exploit vulnerability in applications using database services
SQL injection attack launched from client
Application Server

Figure 10.3: Databases are vulnerable to attacks at multiple points.

In addition to SQL injection attacks, vulnerabilities in database components, such as the listener (the application that listens on a specified port for requests to the database), can be used to compromise a database. Once an attacker has gained access to a database, the attacker can also tamper with the data as well as steal it. Relatively small changes to data can be difficult to detect unless auditing and monitoring policies are well established. Database servers are also subject to disruption from DoS attacks.

Application Code

The importance of application code can range from the mundane, such as scripts for cleaning up temporary directories, to mission-critical systems, such as enterprise resource planning (ERP) systems. These assets are subject to several risks, including:

- Flaws in logic
- Insufficient error-handling code
- Dependency on flawed library or other shared code
- Insufficient CPU, storage, or network resources

Flaws in application logic will be found in any sufficiently complex system. Vendors and developers routinely patch applications to correct known problems.

Insufficient error-handling code is a problem because applications will encounter conditions that will disrupt normal operations. When a storage device is full, the application will not be able to save data. How does the application respond? Graceful degradation of services requires that the application provide alternative means for systems administrators or users to respond to the problem.

Complex applications are modular and layered. Lower levels provide services for upper levels. For example, a customer management system uses databases for persistent storage; database systems depend on files systems or, in some cases, low-level I/O routines provided by the operating system (OS). Client applications, such as office productivity programs, depend on graphical interface components provided by the OS. Vulnerabilities in any of these lower-level systems can create risks for any application that uses them.

In addition to the long-term risks associated with flawed code, there are transient risks such as insufficient resources. An error in an application or a mistake by an operator can consume large portions of available bandwidth on the network, for example, by unnecessarily transferring a set of large files. Similarly, a poorly formed database query can easily consume available CPU cycles and I/O operations.

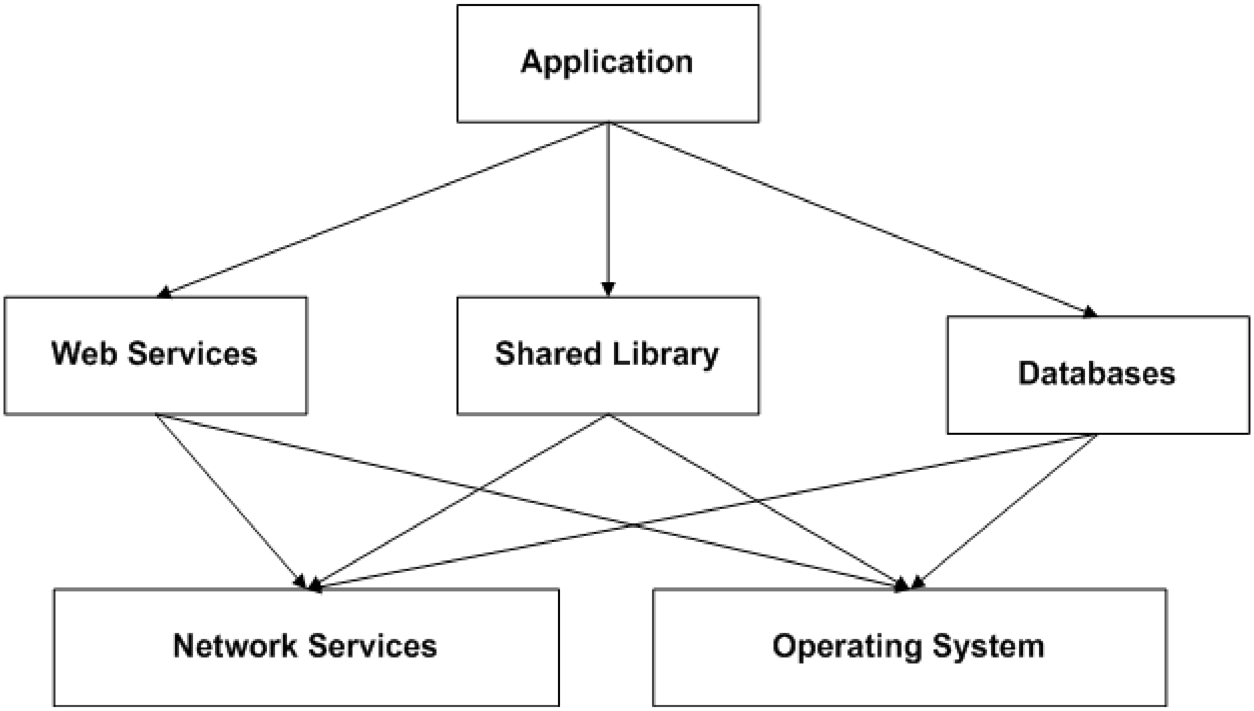

Figure 10.4: Layered applications introduce dependencies that pose potential risks.

Systems Documentation

Documentation rarely makes it on any top-ten list of information assets, but it should. Organizations that depend on the knowledge of their staff, contractors, consultants, and business partners without formally documenting processes and procedures are at risk. Employees leave, contractors move on to the next assignment, and partners go out of business. The need to formalize and capture information about IT systems is obvious.

Capability maturity models, such as Carnegie Mellon Software Engineering Institutes' model, define levels of capability that range from ad hoc management to optimized management. Moving from ad hoc through more capable stages requires, among other things, formalized and documented processes. Without this, organizations are subject to a number of risks, including:

- Disruption of services
- Additional expenses associated with reverse engineering
- Delayed deployment of applications and services
- Increased need for training
- Poor quality control

Systems documentation is just one type of institutional knowledge that constitutes an organizational asset.

📖 For more information about capability maturing models, see the Software Engineering Institute's (SEI) Web site at http://www.sei.cmu.edu/cmm/.

Intellectual Property

Intellectual properties are intangible assets based on the creativity of an organization or individual and provide some type of competitive advantage or constitute an asset that can be sold. Intellectual property includes:

- Patents
- Trade secrets
- Designs and art work
- Processes
- Copyright material

The more knowledge-based a business, the more important the intellectual property. This type of asset is subject to a number of risks but the most important, and threatening, is theft. Headlines from the U.S. Department of Justice (DoJ) press releases depict the range of crimes related to intellectual property theft:

- "Former Vancouver Area Man Sentenced to Five Years in Prison for Conspiracy Involving Counterfeit Software and Money Laundering: Web of Companies Sold up to $20 million of Microsoft Software with Altered Licenses"
- "Pharmaceutical Distributor Pleads Guilty to Selling Counterfeit Drugs"
- "Local Business Owner Sentenced to Year In Jail for Copyright Infringement Conspiracy Related to the Sales of Counterfeit Goods"
- "California Man Sentenced for Electronically Stealing Trade Secrets from his Former Employer, a Construction Contractor"

📖 For more examples, see the Computer Crime & Intellectual Property Section of the U.S. Department of Justice Web site at http://www.usdoj.gov/criminal/cybercrime/ip.html.

Intellectual property theft can occur in many ways, including:

- Attackers can breach electronic security measures and steal information from servers.
- Thieves can steal notebook computers, PDAs, and smartphones with documents, diagrams, and other confidential and private information.
- Employees and other insiders can steal or leak information for their own use or for sale to others.
- Contractors and consultants can breach non-disclosure agreements and use knowledge acquired at one client while working for one of that client's competitors.

Mitigating the risks to intellectual property is challenging. Unlike tangible assets that can be locked down and monitored, intellectual property pervades an organization, is embedded in software that is distributed to customers, and may be remembered by employees and other insiders long after they leave an organization.

The types of information assets and risks to those assets are wide ranging. From the most mundane PC to the valuable intellectual property, the relative impact of risks must be assessed in order to properly manage risk.

Determine Impact of Risks

Once information assets and the risks associated with them have been identified, the next step of risk analysis is to determine the impact each of those risks can have on an organization.

Types of Costs

The impact of threats is a function of the value of the asset damaged by a threat, the cost of restoring the asset, and the cost of not having the functional asset. For example, if an application server is destroyed in a fire, the cost to the organization includes:

- Replacing the server
- Restoring data to the replacement server
- Configuring the replacement server
- Testing the replacement server
- Lost revenue or productivity during downtime
- Cost of switching to and from failover servers, if used

These costs apply to other types of assets as well. In addition to these, consider the following when determining the impact:

- The value of intellectual property to competitors
- The potential for penalties for violating regulations, such as failure to comply with privacy regulations if a customer database is compromised
- The costs to brand value due to the public disclosure of a security breach
- Contractual penalties for not meeting service level agreements (SLAs)

Identifying the types of costs is followed by steps to quantify those costs.

Determine Costs

Quantifying costs related to risks is far from straightforward. To begin, let's examine the simplest of cases and then move on to the more challenging areas.

Quantitative Measures of Costs

It is relatively easy to calculate the costs of tangible assets with known replacement costs, depreciation schedules, and such. A comprehensive inventory of assets along with information tracked in financial management systems can provide most if not all information needed to quantify the cost of replacing those assets.

Valuing intellectual property is more difficult, but there are formal methods for doing so, including:

- Basing the value of intellectual property on the amount of royalties an organization would have to pay if it licensed the intellectual property from another party
- The premium price charged for a product when compared with similar products that lack the benefit of the intellectual property
- The cost to develop the intellectual property, perhaps adjusted for inflation
- The cost of redeveloping the intellectual property
- Valuing all intellectual property as the value of the business less the value of all tangible assets

The value of other assets, particularly brand value and reputation, do not lend themselves to quantitative measures.

Qualitative Evaluations

Qualitative techniques are used when quantitative measures cannot be used. These techniques typically depend on the reasoned opinions of experts or others knowledgeable about a particular area. For example, if a bank is trying to assess the cost of a security breach in which 10,000 customer records are compromised, it might consult with:

- Attorneys regarding disclosure regulations
- Marketing executives for an assessment of the negative publicity
- Industry consultants who have worked with competitors in similar situations
- Customer focus groups

The outcome of the evaluations may be ordered sets of risks with relative measures—such as high, moderate, and low—assigned to each. Although these assignments are not as precise as quantitative measures, they can provide enough guidance to allocate resources to protect these assets. The value of assets is one component of risk analysis calculations; another is the likelihood of threats.

Determine the Likelihood of Threats

Although there are many threats to information assets, many occur rarely enough that only occasional review is required; however, other threats are constant and require continual monitoring. Understanding the likelihood of each threat is essential to properly allocating resources.

The likelihood of fires, floods, storms, and other natural disasters can be determined using historical data. Insurance companies may be able to provide relevant statistics.

Disruptions due to equipment failures can be calculated using metrics such as the mean time between failures (MTBF). Manufacturers should be able to provide MTBF measures.

Statistics about security threats are more difficult to come by. The Computer Security Institute (CSI) and U.S. Federal Bureau of Investigation (FBI) conduct an annual computer security survey that is often cited for security trends. Although useful, the CSI/FBI study is limited to surveying cooperative organizations. Not all companies or government agencies are inclined to discuss security practices and events. Furthermore, even when organizations are willing to share information, they can describe only what they are aware of. There may be botnets, rootkits, and Trojan horses installed on the corporate network without the knowledge of systems administrators.

> 📖 The CSI/FBI report is available from the CSI Web site at http://gocsi.com/. For more information about the limited usefulness of self assessments, see Jeffrey Gangemi's article "Cybercriminals Target Small Biz" in BusinessWeek online. According to the article "approximately 70% of small businesses consider information security a high priority, and more than 80% have confidence in their existing protective measures" yet almost 20% do not use antivirus scanning and 60% do not use encryption on their wireless networks.

With asset values and the likelihood of experiencing particular threats calculated, you can move on to the next stage of risk assessment, calculating risk measures.

Calculating Risk Measures

Ultimately, you need to put monetary value on risks so that you can determine the appropriate level of resources dedicated to protecting assets. The building blocks of this process are:

- Asset value
- Exposure factor (EF)
- Single loss expectancy (SLE)
- Annualized rate of occurrence (ARO)
- Annualized loss expectancy (ALE)

Asset value is the calculated as described earlier.

Exposure Factors

EF is the percentage of the value of an asset lost in one occurrence of a threat. For example, if a server is completely destroyed by a flood, the EF is 100 percent; if one-fifth of the data in a database is stolen or otherwise compromised, the EF is 20 percent. Note that each threat will have a distinct EF.

SLE is calculated with the formula:

SLE = asset value × exposure factor

For example, if the value of a database is $500,000 and the EF is 20 percent, the SLE is $100,000 (500,000 x 0.2).

An asset may be subject to multiple threats, so there can be multiple SLEs for a single asset. A notebook, for example, is exposed to theft, malware attack, hardware failure, and, in some cases, fire due to battery overheating. SLE would need to be calculated for each of these possible events.

Annualized Rate of Occurrence

ARO is the expected frequency of a threat occurring within one year. As with the SLE, there is a separate ARO for each threat. If threats are expected to materialize less than once per year, the ARO will be less than one and greater than zero. If the rate of occurrence is greater than once per year, the ARO will be greater than one.

ARO may or may not take into account existing countermeasures. The threat of a virus, worm, or other malware attack is relatively high; however, the likelihood of a successful malware attack on devices running antivirus scanners and being fully patched is much less. If a risk analysis is being done from scratch and countermeasures are not taken into account, use an estimated rate of occurrence based on the frequency with which malware is found in the wild. However, if countermeasures are already in place, and the goal of risk analysis is to analyze the need for additional countermeasures, an ARO based on the likelihood of malware avoiding detection by existing defenses is more appropriate.

Annualized Loss Expectancy

ALE is calculated according to the following formula:

ALE = single loss expectancy × annualized rate of occurrence

ALE is calculated for each threat to each asset to determine the overall loss expectancy. Table 10.1 shows an example of calculating the total loss expectancy for a single asset.

Laptop Value	Threat	EF	SLE	ARO	ALE
$5,000	Theft	100%	$5,000	0.1	$500
	Fire	100%	$5,000	0.01	$50
	Malware	20%	$1,000	0.2	$200
	Hardware Failure	10%	$500	0.05	$25
				Total Loss Expectancy	**$775**

Table 10.1: Total loss expectancy for a notebook in a one year period.

From the calculations in Table 10.1, you can see that it would be reasonable to spend as much as $500 per year in anti-theft devices but no more than $50 for anti-fire measures. Ideally, the outcome of risk analysis is a plan to minimize the cost of countermeasures while maximizing the reduction in the overall level of exposure to assets.

> For an in-depth look at risk assessment, see the Risk Management Guide for Information Technology published by the U.S. National Institute for Standards and Technology, available at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Of course, if you do not have the detailed cost information for this type of calculation, such a formal method is not useful. An alternative method, which is especially useful when qualitative risk assessments are used, is the risk-level matrix.

Qualitative Risk Assessment

It is not always possible to assign accurate quantitative measures to threats and their potential impacts. Consider examples such as:

- The impact on brand from a security breach and the disclosure of a large number of customer records
- The likelihood of an employee planting a logic bomb in a script set to execute after the employee terminates
- The likelihood of a high-priority vulnerability in a new network appliance
- The chance that a business partner's Web services will be unavailable due to a DoS attack, hardware failure, or other cause

In these examples, you could probably develop a consensus around imprecise likelihoods and impact measures. Often a simple breakdown into high, medium, and low likelihoods and impacts is sufficient to order risks so that a rational remediation plan can be formulated. Table 10.2 shows the basic form of a risk matrix, which can be used to combine the measures of likelihood and impact to determine the overall importance of a threat.

	Impact			
		High	Medium	Low
Likelihood	High	High	Medium	Low
	Medium	Medium	Medium	Low
	Low	Medium	Low	Low

Table 10.2: A risk matrix that combines likelihood and impact to assess the overall importance of risks.

Some of the combinations of likelihood and impact yield obvious overall risk levels. For example, a high likelihood risk—such as malware infected emails—combined with high impact—such as infecting a large number of clients or consuming network resources, a la SQL Slammer—yields a high risk threat. Low likelihood threats with low impacts present little risk to an organization and should not be the focus of attention during risk analysis.

Asymmetric combinations of likelihood and impact are more difficult to judge. For example, how much effort should be made to mitigate a low likelihood but high impact threat? For an organization with a conservative perspective, such a risk should be categorized as medium; however, a more risk-tolerant company may categorize it as a low risk.

The risk levels in Table 10.2 are suggestive but by no means definitive. The risk tolerance of an organization should dictate the risk levels when different combinations of impact and likelihood are in question.

Risk Analysis Steps

Risk analysis is a methodical process for understanding both the types of threats and their likelihood. The goal of risk analysis is to identify the highest impact threats, order the priority of risks based on their impact on the organization, and understand the optimal level of investment in mitigating those risks. To summarize, the practice of risk management entails:

- Identifying information assets and threats to those assets
- Determining the impact of threats to an organization
- Determining the likelihood for each threat
- Assessing the risk versus the cost of countermeasures

In addition to these steps is the need for monitoring and analysis that provide fundamental information about likelihoods and impacts for future iterations of the risk analysis life cycle, as depicted in Figure 10.5.

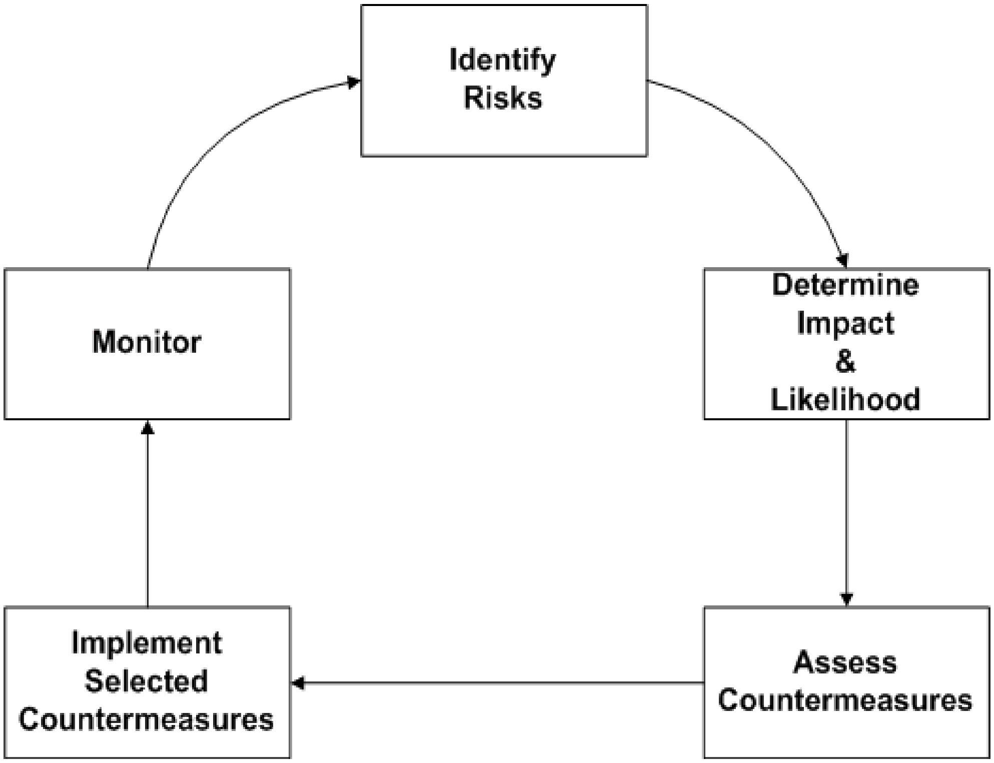
Identify Risks
Determine Impact & Likelihood
Assess Countermeasures
Implement Selected Countermeasures
Monitor

Figure 10.5: The risk analysis life cycle.

Understanding Business Impact of Risks

Throughout, the discussion of risk analysis has described a number of threats and discussed how the likelihood of those threats is used to assess the level of risk associated with those threats. Of course, the likelihood alone is not enough to understand the risk posed by a threat; you need to take into account the impact.

Impact is the effect a threat has on an organization when a threat is realized; examples include:

- The loss of revenue that occurs because an online sales application fails, perhaps due to a software failure, a network services disruption, or a malware attack
- The fines and penalties incurred due to violations of regulations
- Penalties specified in contractual agreements that require a specified level of quality of service
- Loss of brand value to negative publicity associated with a high-profile failure or security breach

These are representative examples of the broad categories of business objectives that should be considered when assessing the impact of threats to operations and security. The categories addressed in this chapter include:

- Operational impact
- Compliance impact
- Business relationship impact
- Customer relations impact

As detailed in this section, these topic areas cover a wide range of business objectives. Like threats, it is sometimes possible to quantify with a fair level of accuracy and confidence the level of impact; in other cases, more qualitative assessments are required.

> ✎ It should be noted that these categories are not mutually exclusive. In fact, impacts of threats can be measured in more than one of these categories at a time. A high-profile security breach can have an impact on customer relations as well as lead to fines and penalties for violations of privacy regulations. A failed server at a retailer can impact both operations and customer relations, especially if the failure occurs during the high-volume holiday season.

As Figure 10.6 shows, impacts can be thought of as affecting multiple categories at the same time.

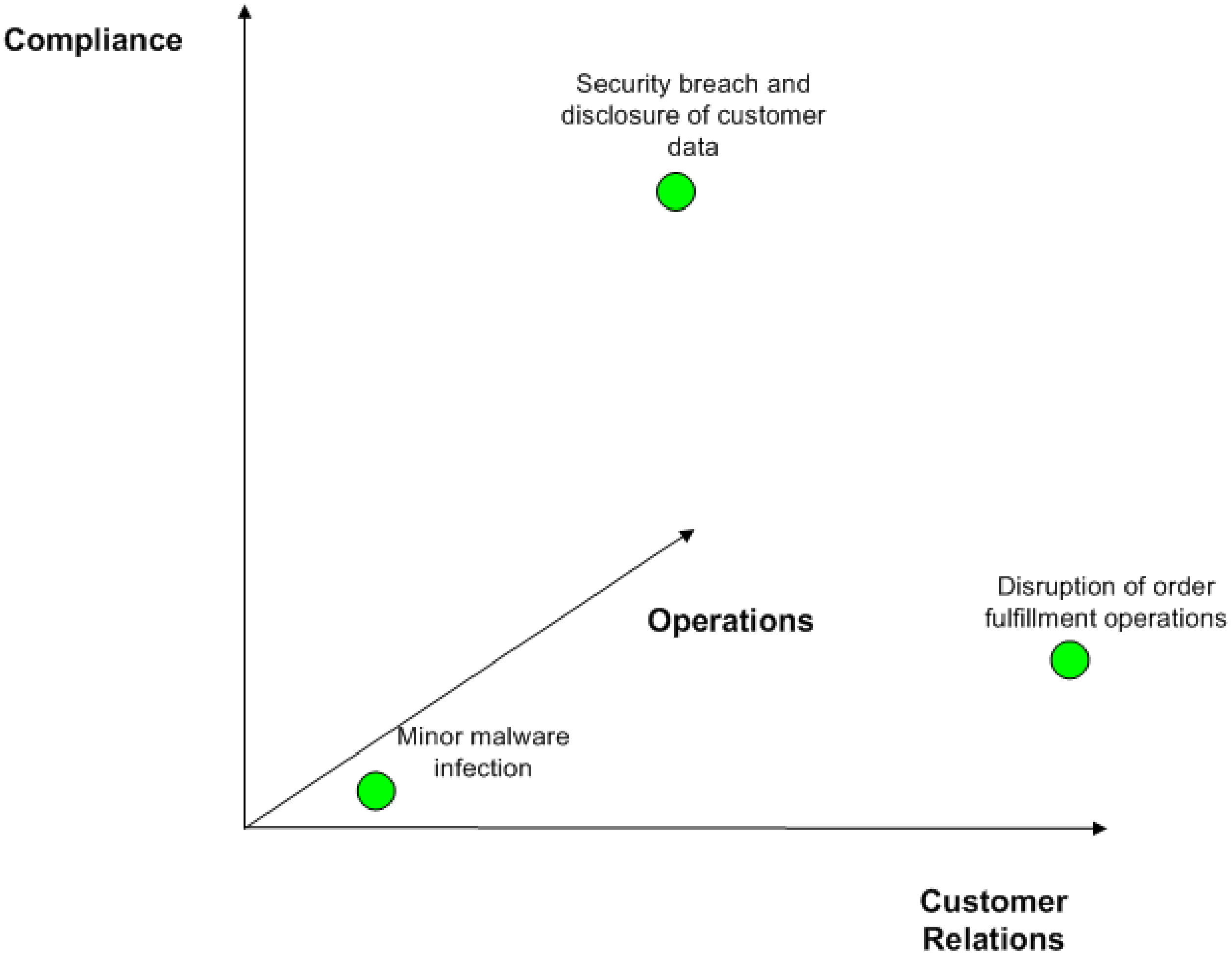
Compliance
Security breach and disclosure of customer data
Operations
Disruption of order fulfillment operations
Minor malware infection
Customer Relations

Figure 10.6: Threats can have impacts along multiple business dimensions simultaneously.

Operational Impacts

Operational impacts are those that challenge the ability of an organization to carry out its workflows. Some common operational workflows are:

- Receiving and processing customer orders
- Fulfilling orders
- Conducting marketing and advertising
- Managing customer relations
- Providing service desk support to internal IT users
- Performing maintenance
- Executing projects
- Managing operations

Within the set of operational impacts, the timeframes along with when the impact of a threat is realized can vary significantly. For example, consider the difference in impact if a point of sales system fails and if a data warehouse database server fails.

When a point of sales system fails, revenues from sales stop. Merchandise is not sold, customers may turn to other providers for the products they need, and financial reporting and reconciliation operations are blocked. In short, critical, time-sensitive operations are disrupted and losses may be permanent. This is not the case when a decision support system is offline.

Consider how a data warehouse or other business intelligence application is used. Managers receive reports about sales, revenues, expenses, and other measures of the financial state of their department and lines of business. Often, one of the main purposes of a business intelligence application is to provide a comprehensive view of the state of operations that is not available from traditional transaction reporting systems, such as account receivables and account payable systems. These transaction-oriented systems have been designed to keep financial records and ensure accurate and comprehensive accounting. Business intelligence systems supplement those with reports designed for analyzing longer-term trends and patterns of activity that required consolidating data from multiple systems.

Now imagine a data warehouse database server is down for a day. What is the impact on business? In the short term, the impact of such a disruption is minimal. Managers and executives can presumably continue to manage day-to-day operations and can perform planning and strategic analysis later when the data warehouse is back online. There is not a threat of lost revenues, the disruption is not obvious to customers or business partners, and presumably this type of management system is not directly subject to compliance regulations, at least in terms of availability.

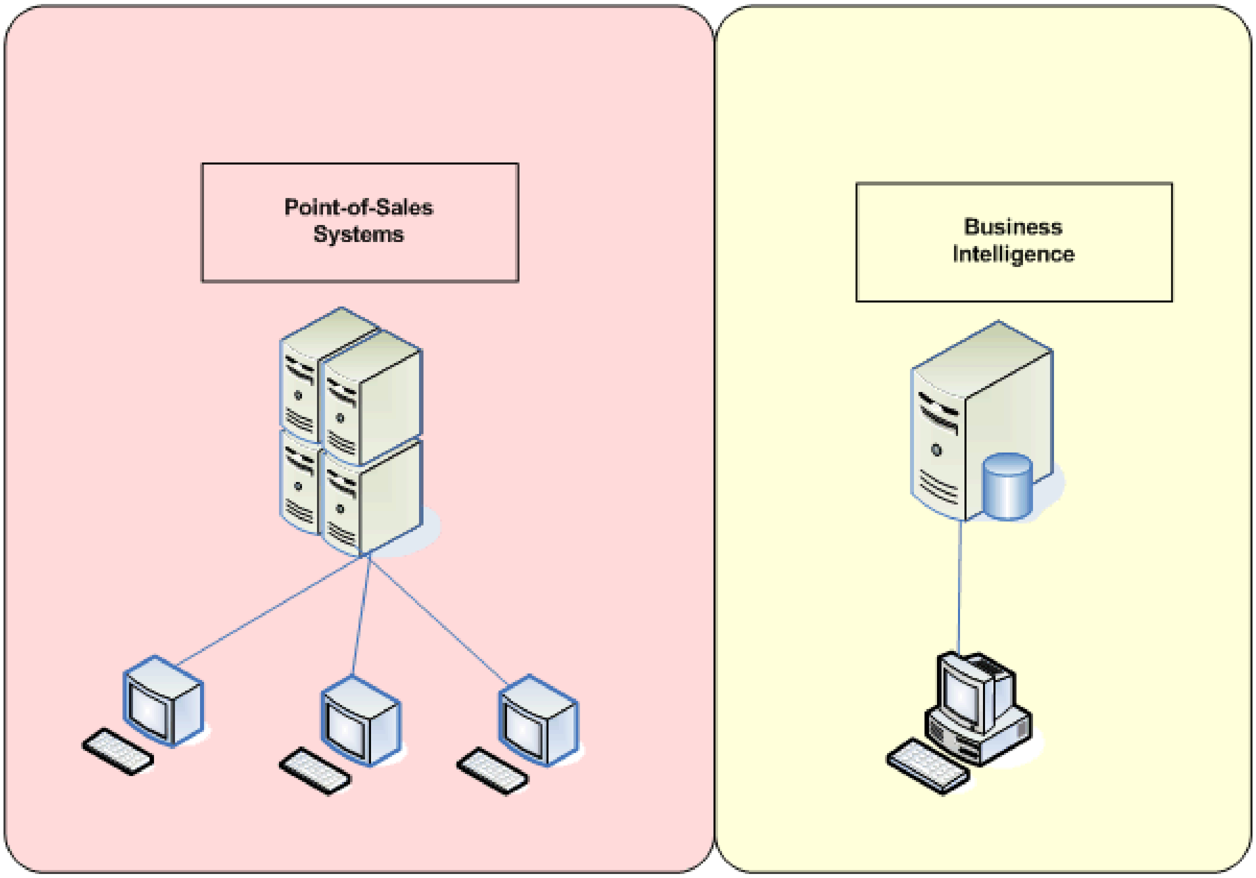

Figure 10.7: Threats to time-critical operations, such as sales, have more significant impacts than threats to less time-sensitive operations, such as business intelligence reporting.

Compliance Impact

Operational and security risks can have an impact on regulatory compliance. The past several years have witnessed heightened awareness about regulations as well as the advent of new, high-profile regulations. The list of regulations that affect business and government agencies and departments is long and spans multiple jurisdictions. Some of the most well-known and broadly applicable are:

- The Sarbanes-Oxley Act (SOX), which governs financial reporting and other aspects of management in publicly traded companies in the United States
- The Gramm-Leach-Bliley Act, another U.S. regulation, provides for the protection of personal financial information
- The Health Insurance Portability and Accountability Act (HIPAA), which regulates the use and disclosure of protected health care information in the United States
- The Australian Federal Privacy Act and the Canadian Personal Information Protection and Electronics Documents Act (PIPEDA), which establish privacy protections in their respective countries
- The European Union Data Privacy Directive and Directive on Privacy and Electronic Communications provide protections for those living in EU member countries
- California State Bill (SB) 1386 requires business and government agencies to notify victims living in California when personal private information is disclosed
- Bank of International Settlements' BASEL II requirements cover reporting and disclosures by financial institutions
- The U.S. Food and Drug Administration (FDA) 21 CFR Part 11 regulations govern operations of pharmaceutical companies
- Federal Financial Institutions Examination Council (FFIEC) guidelines on business continuity planning in financial institutions
- Federal Information Security Management Act (FISMA), established by the U.S. federal government, to establish standards for information security within departments and agencies of the U.S. federal government.

A number of conclusions can be drawn from examining this list:

- Regulations are defined by a range of governing bodies, from state-level governments, such as California, to trans-national institutions, such as the EU
- Regulations are targeting both the integrity of business operations, as seen in SOX and BASEL II, and the protection of individuals' privacy, seen in California SB 1386 and the EU's privacy directives
- Regulations apply to a broad range of industries and governments; in some cases, regulations are directed at specific industries (the FDA's 21 CFR Part 11 regulations of pharmaceuticals); in other cases, regulations are broadly applicable (such as SOX, which applies to all public companies in the U.S. and FISMA, which is broadly applicable across the U.S. federal government)

Clearly, compliance is a significant category when assessing the impact of risks; however, it is not just the government that you must be concerned with when considering the impact of risks on operations.

Business Relationship Impact

The impacts of risks are not limited to an organization’s boundaries. The ripple effects of a disruption in services can directly and indirectly affect business partners as well. Supply chains now span multiple businesses, including manufacturers and service providers, and a loss of continuity can affect all participants.

Consider, for example, a simple supply chain:

- An electronics manufacturer produces graphics co-processors for high-end scientific and engineering applications. The market for this is limited, so production is done in relatively small quantities.
- The electronics manufacturer uses a single parcel carrier to transport the chips to a graphics card manufacturer.
- The graphics card manufacturer produces the high-end graphics cards, along with other products, for use by several PC manufacturers.
- The graphics manufacturer ships components using two different parcel carriers.
- PC manufacturers order graphics cards from the graphics card manufacture in such a way as to maintain a just-in-time inventory.
- The PC manufacturer ships complete systems to customers using multiple parcel carriers.

Now imagine that the parcel carrier used by the graphics co-processor manufacture is delayed shipping components to the graphics card manufacturer. The graphics card manufacturer cannot ship needed graphics cards, so PC manufactures are delayed in delivering completed systems, which, in turn, causes customers to cancel orders.

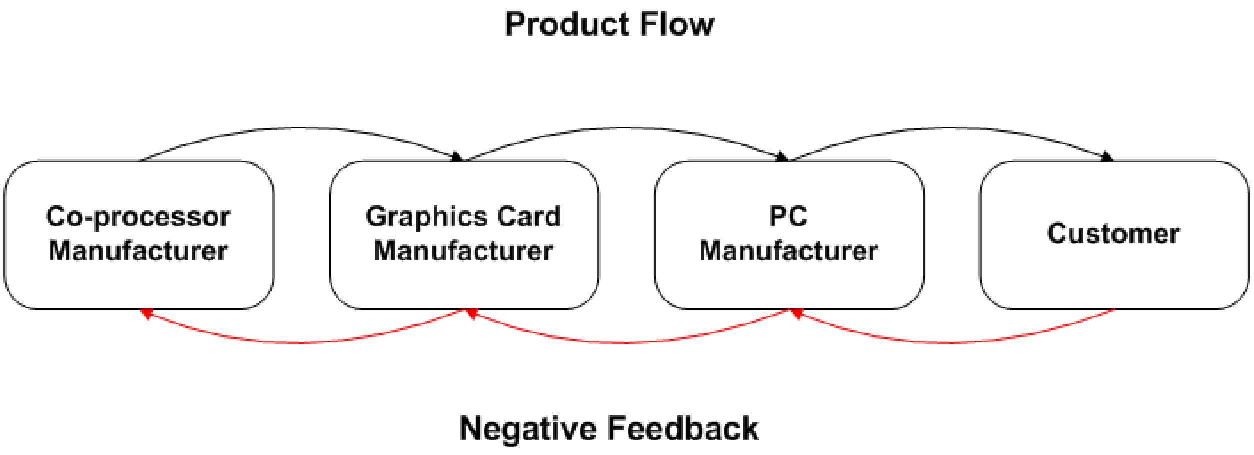

Figure 10.8: Supply chains now expose organizations to the impact of operation disruptions from other businesses.

Negative feedback can spread across the supply chain as the impact of unfilled orders, missed opportunities, and long-term customer dissatisfaction becomes known.

Customer Relationship Impact

In the past, the inner workings of a business were relatively opaque to customers. As long as products arrived as ordered, bills were accurate, payments were processed correctly, and quality service was maintained, customers would not necessarily care how vendors conducted their operations. Although this is still true to some extent, the publicity around financial mismanagement and improper reporting, such as at Enron and WorldCom, and the widespread concern over security breaches and the disclosure of personal information, has changed the customer relationship landscape.

Privacy regulations, such as California SB 1386 and the EU privacy directives, are requiring that businesses and government agencies notify customers and citizens when private information is improperly disclosed. There is also greater publicity about privacy breaches; well-known incidents include:

- The ChoicePoint breach in 2005 in which personal information about 163,000 victims was stolen
- A breach at the University of California, Los Angeles resulted in the theft of information about 800,000 individuals, including current and former students, current and former faculty members, as well as parents and applicants
- The theft of a notebook computer from the home of a U.S. Veterans Administration that contained personal information about approximately 28.5 million veterans and spouses; the notebook was later recovered and no data appears to have been compromised or exploited

> 📖 For a list of privacy breaches, see the Privacy Clearinghouse Chronology of Data Breaches at http://www.privacyrights.org/ar/chrondatabreaches.htm.

Quantitative measurements of the impact of such breaches and the negative publicity are difficult if not impossible; qualitative measures are the best that can be expected in such cases.

The impact of risks should be understood along several dimensions, including operational impact, compliance impact, business relationship impact, and customer relations impact. This is a fundamental aspect of risk analysis and without a thorough understanding of the range of effects of different threats, you cannot accurately gauge and mitigate threats to the organization.

Summary

Risks are a constant in the realm of IT infrastructure management. Security risks are well publicized and a wide range of countermeasures have been deployed to mitigate security risks. Other types of threats to business continuity and integrity, such as natural disasters and disruptions to supply chains, can also present risks to both short-term operations and long-term strategic goals. The practice of risk management has evolved, providing the tools and techniques to effectively and efficiently understand these threats. Of course, the ultimate goal is to mitigate these threats, and risk analysis enables this goal even with limited resources.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.