Network Security Concepts and Policies

In this chapter, you learn how to develop a comprehensive network security policy to counter threats against information security. You also learn about possible threats and how to describe and implement the process of developing a security policy.

In this chapter, you learn about the following topics:

- Fundamental concepts in network security, including identification of common vulnerabilities and threats, and mitigation strategies
- Implementation of a security architecture using a lifecycle approach, including the phases of the process, their dependencies, and the importance of a sound security policy

The open nature of the Internet makes it vital for businesses to pay attention to the security of their networks. As companies move more of their business functions to the public network, they need to take precautions to ensure that the data cannot be compromised and that the data is not accessible to anyone who is not authorized to see it.

Unauthorized network access by an outside hacker or a disgruntled employee can cause damage or destruction to proprietary data, negatively affect company productivity, and impede the capability to compete. The Computer Security Institute reported in its *2010/2011 CSI Computer Crime and Security Survey* (available at http://gocsi.com/survey) that on an average day, 41.1 percent of respondents dealt with at least one security incident (see page 11 of the survey). Unauthorized network access can also harm relationships with customers and business partners, who might question the capability of a company to protect its confidential information. The definition of "data location" is being blurred by cloud computing services and other service trends. Individuals and corporations benefit from the elastic deployment of services in the cloud, available at all times from any device, but these dramatic changes in the business services industry exacerbate the risks in protecting data and the entities using it (individuals, businesses, governments, and so on). Security policies and architectures require sound principles and a lifecycle approach, including whether the data is in the server farm, mobile on the employee's laptop, or stored in the cloud.

To start on our network security quest, this chapter examines the need for security, looks at what you are trying to protect, and examines the different trends for attacks and protection and the principles of secure network design. These concepts are important not only for succeeding with the IINS 640-554 exam, but they are fundamentals at all security endeavors on which you will be embarking.

Building Blocks of Information Security

Establishing and maintaining a secure computing environment is increasingly more difficult as networks become increasingly interconnected and data flows ever more freely. In the commercial world, connectivity is no longer optional, and the possible risks of connectivity do not outweigh the benefits. Therefore, it is very important to enable networks to support security services that provide adequate protection to companies that conduct business in a relatively open environment. This section explains the breadth of assumptions and challenges to establish and maintain a secure network environment.

Basic Security Assumptions

Several new assumptions have to be made about computer networks because of their evolution over the years:

- Modern networks are very large, very interconnected, and run both ubiquitous protocols (such as IP) and proprietary protocols. Therefore, they are often open to access, and a potential attacker can with relative ease attach to, or remotely access, such networks. Widespread IP internetworking increases the probability that more attacks will be carried out over large, heavily interconnected networks, such as the Internet.
- Computer systems and applications that are attached to these networks are becoming increasingly complex. In terms of security, it becomes more difficult to analyze, secure, and properly test the security of the computer systems and applications; it is even more so when virtualization is involved. When these systems and their applications are attached to large networks, the risk to computing dramatically increases.

Basic Security Requirements

To provide adequate protection of network resources, the procedures and technologies that you deploy need to guarantee three things, sometimes referred to as the CIA triad:

- **Confidentiality:** Providing confidentiality of data guarantees that only authorized users can view sensitive information.
- **Integrity:** Providing integrity of data guarantees that only authorized users can change sensitive information and provides a way to detect whether data has been tampered with during transmission; this might also guarantee the authenticity of data.
- **Availability of systems and data:** System and data availability provides uninterrupted access by authorized users to important computing resources and data.

When designing network security, a designer must be aware of the following:

- The threats (possible attacks) that could compromise security
- The associated risks of the threats (that is, how relevant those threats are for a particular system)
- The cost to implement the proper security countermeasures for a threat
- A cost versus benefit analysis to determine whether it is worthwhile to implement the security countermeasures

Data, Vulnerabilities, and Countermeasures

Although viruses, worms, and hackers monopolize the headlines about information security, risk management is the most important aspect of security architecture for administrators. A less exciting and glamorous area, risk management is based on specific principles and concepts that are related to asset protection and security management.

An *asset* is anything of value to an organization. By knowing which assets you are trying to protect, as well as their value, location, and exposure, you can more effectively determine the time, effort, and money to spend in securing those assets.

A *vulnerability* is a weakness in a system or its design that could be exploited by a threat. Vulnerabilities are sometimes found in the protocols themselves, as in the case of some security weaknesses in TCP/IP. Often, the vulnerabilities are in the operating systems and applications.

Written security policies might also be a source of vulnerabilities. This is the case when written policies are too lax or are not thorough enough in providing a specific approach or line of conduct to network administrators and users.

A *threat* is any potential danger to assets. A threat is realized when someone or something identifies a specific vulnerability and exploits it, creating exposure. If the vulnerability exists theoretically but has not yet been exploited, the threat is considered latent. The entity that takes advantage of the vulnerability is known as the threat agent or threat vector.

A *risk* is the likelihood that a particular threat using a specific attack will exploit a particular vulnerability of a system that results in an undesirable consequence. Although the roof of the data center might be vulnerable to being penetrated by a falling meteor, for example, the risk is minimal because the likelihood of that threat being realized is negligible.

NOTE

If you have a vulnerability but there is no threat toward that vulnerability, technically you have no risk.

An *exploit* happens when computer code is developed to take advantage of a vulnerability. For example, suppose that a vulnerability exists in a piece of software, but nobody knows about this vulnerability. Although the vulnerability exists theoretically, there is no exploit yet developed for it. Because there is no exploit, there really is no problem yet.

A *countermeasure* is a safeguard that mitigates a potential risk. A countermeasure mitigates risk either by eliminating or reducing the vulnerability or by reducing the likelihood that a threat agent will be able to exploit the risk.

Key Concepts

An **asset** is anything of value to an organization.

A **vulnerability** is a weakness in a system or its design that could be exploited by a threat.

A **threat** is a potential danger to information or systems.

A **risk** is the likelihood that a particular vulnerability will be exploited.

An **exploit** is an attack performed against a vulnerability.

A **countermeasure** (safeguard) is the protection that mitigates the potential risk.

Data Classification

To optimally allocate resources and secure assets, it is essential that some form of data classification exists. By identifying which data has the most worth, administrators can put their greatest effort toward securing that data. Without classification, data custodians find it almost impossible to adequately secure the data, and IT management finds it equally difficult to optimally allocate resources.

Sometimes information classification is a regulatory requirement (required by law), in which case there might be liability issues that relate to the proper care of data. By classifying data correctly, data custodians can apply the appropriate confidentiality, integrity, and availability controls to adequately secure the data, based on regulatory, liability, and ethical requirements. When an organization takes classification seriously, it illustrates to everyone that the company is taking information security seriously.

The methods and labels applied to data differ all around the world, but some patterns do emerge. The following is a common way to classify data that many government organizations, including the military, use:

- **Unclassified:** Data that has little or no confidentiality, integrity, or availability requirements and therefore little effort is made to secure it.
- **Restricted:** Data that if leaked could have undesirable effects on the organization. This classification is common among NATO (North Atlantic Treaty Organization) countries but is not used by all nations.
- **Confidential:** Data that must comply with confidentiality requirements. This is the lowest level of classified data in this scheme.
- **Secret:** Data for which you take significant effort to keep secure because its disclosure could lead to serious damage. The number of individuals who have access to this data is usually considerably fewer than the number of people who are authorized to access confidential data.
- **Top secret:** Data for which you make great effort and sometimes incur considerable cost to guarantee its secrecy since its disclosure could lead to exceptionally grave damage. Usually a small number of individuals have access to top-secret data, on condition that there is a need to know.
- **Sensitive But Unclassified (SBU):** A popular classification by government that designates data that could prove embarrassing if revealed, but no great security breach would occur. SBU is a broad category that also includes the For Official Use Only designation.

It is important to point out that there is no actual standard for private-sector classification. Furthermore, different countries tend to have different approaches and labels. Nevertheless, it can be instructive to examine a common, private sector classification scheme:

- **Public:** Companies often display public data in marketing literature or on publicly accessible websites.
- **Sensitive:** Data in this classification is similar to the SBU classification in the government model. Some embarrassment might occur if this data is revealed, but no serious security breach is involved.
- **Private:** Private data is important to an organization. You make an effort to maintain the secrecy and accuracy of this data.
- **Confidential:** Companies make the greatest effort to secure confidential data. Trade secrets and employee personnel files are examples of what a company would commonly classify as confidential.

Regardless of the classification labeling used, what is certain is that as the security classification of a document increases, the number of staff that should have access to that document should decrease, as illustrated in Figure 1-1.

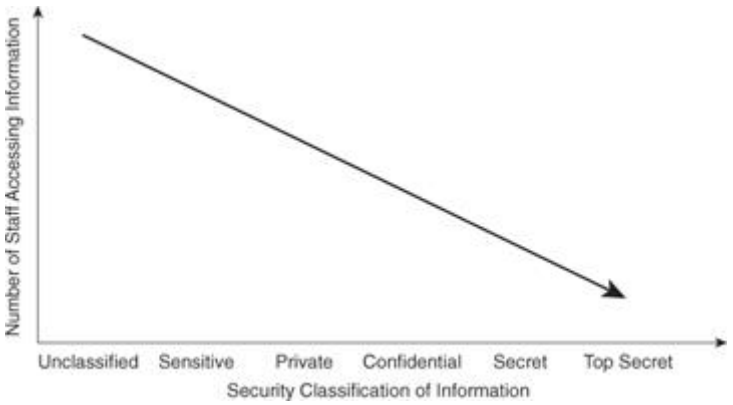

Figure 1-1. Ratio: Staff Access to Information Security Classification

Many factors go into the decision of how to classify certain data. These factors include the following:

- **Value:** Value is the number one criterion. Not all data has the same value. The home address and medical information of an employee is considerably more sensitive (valuable) than the name of the chief executive officer (CEO) and the main telephone number of the company.
- **Age:** For many types of data, its importance changes with time. For example, an army general will go to great lengths to restrict access to military secrets. But after the war is over, the information is gradually less and less useful and eventually is declassified.
- **Useful life:** Often data is valuable for only a set window of time, and after that window has expired, there is no need to keep it classified. An example of this type of data is confidential information about the products of a company. The useful life of the trade secrets of products typically expires when the company no longer sells the product.
- **Personal association:** Data of this type usually involves something of a personal nature. Much of the government data regarding employees is of this nature. Steps are usually taken to protect this data until the person is deceased.

NOTE

To further understand the value of information, think about the Federal Reserve Bank (commonly called the Fed) and the discount rate it sets. The discount rate is, in essence, the interest rate charged to commercial banks by the Fed.

Periodically, the Fed announces a new discount rate. Typically, if the rate is higher than the previous rate, the stock market reacts with sell-offs. If the discount rate is lower, the stock market rises.

Therefore, moments before the Fed announces the new discount rate, that information is worth gazillions of dollars. However, the value of this information drops to nothing when it hits the wire, because everyone then has free access to the information.

For a classification system to work, there must be different roles that are fulfilled. The most common of these roles are as follows:

- **Owner:** The owner is the person who is ultimately responsible for the information, usually a senior-level manager who is in charge of a business unit. The owner classifies the data and usually selects custodians of the data and directs their actions. It is important that the owner periodically review the classified data because the owner is ultimately responsible for the data.
- **Custodian:** The custodian is usually a member of the IT staff who has the day-to-day responsibility for data maintenance. Because the owner of the data is not required to have technical knowledge, the owner decides the security controls but the custodian marks the data to enforce these security controls. To maintain the availability of the data, the custodian regularly backs up the data and ensures that the backup media is secure. Custodians also periodically review the security settings of the data as part of their maintenance responsibilities.
- **User:** Users bear no responsibility for the classification of data or even the maintenance of the classified data. However, users do bear responsibility for using the data in accordance with established operational procedures so that they maintain the security of the data while it is in their possession.

Vulnerabilities Classifications

It is also important to understand the weaknesses in security countermeasures and operational procedures. This understanding results in more effective security architectures. When analyzing system vulnerabilities, it helps to categorize them in classes to better understand the reasons for their emergence. You can classify the main vulnerabilities of systems and assets using broad categories:

- Policy flaws
- Design errors
- Protocol weaknesses
- Software vulnerabilities
- Misconfiguration
- Hostile code
- Human factor

This list mentions just a few of the vulnerability categories. For each of these categories, multiple vulnerabilities could be listed.

There are several industry efforts that are aimed at categorizing threats for the public domain. These are some well-known, publicly available catalogs that may be used as templates for vulnerability analysis:

- **Common Vulnerabilities and Exposures (CVE):** A dictionary of publicly known information security vulnerabilities and exposures. It can be found at http://cve.mitre.org/. The database provides common identifiers that enable data exchange between security products, providing a baseline index point for evaluating coverage of tools and services.
- **National Vulnerability Database (NVD):** The U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. The database can be found at http://nvd.nist.gov.
- **Common Vulnerability Scoring System (CVSS):** A standard within the computer and networking fields for assessing and classifying security vulnerabilities. This standard is focused on rating a vulnerability compared to others, thus helping the administrator to set priorities. This standard was adopted by significant players in the industry such as McAfee, Qualys, Tenable, and Cisco. More information can be found, including the database and calculator, at http://www.first.org/cvss.

Countermeasures Classification

After assets (data) and vulnerabilities, threats are the most important component to understand. Threat classification and analysis, as part of the risk management architecture, will be described later in this chapter.

Once threat vectors are considered, organizations rely on various controls to accomplish in-depth defense as part of their security architecture. There are several ways to classify these security controls; one of them is based on the nature of the control itself. These controls fall into one of three categories:

- **Administrative:** Controls that are largely policies and procedures
- **Technical:** Controls that involve electronics, hardware, software, and so on
- **Physical:** Controls that are mostly mechanical

Later in this chapter, we will discuss models and frameworks from different organizations that can be used to implement network security best practices.

Administrative Controls

Administrative controls are largely policy and procedure driven. You will find many of the administrative controls that help with an enterprise's information security in the human resources department. Some of these controls are as follows:

- Security-awareness training
- Security policies and standards
- Change controls and configuration controls
- Security audits and tests
- Good hiring practices
- Background checks of contractors and employees

For example, if an organization has strict hiring practices that require drug testing and background checks for all employees, the organization will likely hire fewer individuals of questionable character. With fewer people of questionable character working for the company, it is likely that there will be fewer problems with internal security issues. These controls do not single-handedly secure an enterprise, but they are an important part of an information security program.

Technical Controls

Technical controls are extremely important to a good information security program, and proper configuration and maintenance of these controls will significantly improve information security. The following are examples of technical controls:

- Firewalls
- Intrusion prevention systems (IPS)
- Virtual private network (VPN) concentrators and clients
- TACACS+ and RADIUS servers
- One-time password (OTP) solutions
- Smart cards
- Biometric authentication devices
- Network Admission Control (NAC) systems
- Routers with ACLs

NOTE

This book focuses on technical controls because implementing the Cisco family of security products is the primary topic. However, it is important to remember that a comprehensive security program requires much more than technology.

Physical Controls

While trying to secure an environment with good technical and administrative controls, it is also necessary that you lock the doors in the data center. This is an example of a physical control. Other examples of physical controls include the following:

- Intruder detection systems
- Security guards
- Locks
- Safes
- Racks
- Uninterruptible power supplies (UPS)
- Fire-suppression systems
- Positive air-flow systems

When security professionals examine physical security requirements, life safety (protecting human life) should be their number one concern. Good planning is needed to balance life safety concerns against security concerns. For example, permanently barring a door to prevent unauthorized physical access might prevent individuals from escaping in the event of a fire. By the way, physical security is a field that Cisco entered a few years ago. More information on those products can be found at http://www.cisco.com/go/physicalsecurity.

Convergence of Physical and Technical Security

One of the best examples of the convergence of physical and technical security I have witnessed was during a technical visit with a bank in Doha, Qatar, a few weeks before the grand opening of their new head office. They had extensive physical security, using a mix of contactless smart cards and biometrics.

They had cleverly linked the login system for traders to the physical security system. For instance, a trader coming to work in the morning had to use his smart card to enter the building, to activate the turnstile, to call the exact floor where the elevator was to stop, and to be granted access through the glass doors of the trading floors. The movements of the traders were recorded by the physical security systems. Minutes later, upon logging in to perform the first trade of the day, the trading authentication, authorization, and accounting (AAA) system queried the physical security system about the location of the trader. The trader was granted access to the trading system only when the physical security system confirmed to the trading AAA system that the trader was physically on the trading floor.

Controls are also categorized by the type of control they are:

- **Preventive:** The control prevents access.
- **Deterrent:** The control deters access.
- **Detective:** The control detects access.

All three categories of controls can be any one of the three types of controls; for example, a preventive control can be administrative, physical, or technical.

NOTE

A security control is any mechanism that you put in place to reduce the risk of compromise of any of the three CIA objectives: confidentiality, integrity, and availability.

Preventive controls exist to prevent compromise. This statement is true whether the control is administrative, technical, or physical. The ultimate purpose for these controls is to stop security breaches before they happen.

However, a good security design also prepares for failure, recognizing that prevention will not always work. Therefore, detective controls are also part of a comprehensive security program because they enable you to detect a security breach and to determine how the network was breached. With this knowledge, you should be able to better secure the data the next time.

With effective detective controls in place, the incident response can use the detective controls to figure out what went wrong, allowing you to immediately make changes to policies to eliminate a repeat of that same breach. Without detective controls, it is extremely difficult to determine what you need to change.

Deterrent controls are designed to scare away a certain percentage of adversaries to reduce the number of incidents. Cameras in bank lobbies are a good example of a deterrent control. The cameras most likely deter at least some potential bank robbers. The cameras also act as a detective control.

NOTE

To be more concrete, examples of types of physical controls include the following:

- **Preventive:** Locks on doors
- **Deterrent:** Video surveillance
- **Detective:** Motion sensor

NOTE

It is not always possible to classify a control into only one category or type. Sometimes there is overlap in the definitions, as in the case of the previously mentioned bank lobby cameras. They serve as both deterrent and detective controls.

Need for Network Security

Business goals and risk analysis drive the need for network security. For a while, information security was influenced to some extent by fear, uncertainty, and doubt. Examples of these influences included the fear of a new worm outbreak, the uncertainty of providing web services, or doubts that a particular leading-edge security technology would fail. But we realized that regardless of the security implications, business needs had to come first.

If your business cannot function because of security concerns, you have a problem. The security system design must accommodate the goals of the business, not hinder them. Therefore, risk management involves answering two key questions:

- What does the cost-benefit analysis of your security system tell you?
- How will the latest attack techniques play out in your network environment?

  Dealing with Risk

  There are actually four ways to deal with risk:

  Reduce: This is where we IT managers evolve and it is the main focus of this book. We are responsible for mitigating the risks. Four activities contribute to reducing risks:

  - **Limitation/avoidance:** Creating a secure environment by not allowing actions that would cause risks to occur, such as installing a firewall, using encryption systems and strong authentication, and so on
  - **Assurance:** Ensuring policies, standards, and practices are followed
  - **Detection:** Detecting intrusion attempts and taking appropriate action to terminate the intrusion
  - **Recovery:** Restoring the system to operational state

  Ignore: This is not an option for an IT manager. The moment you become aware of a risk, you must acknowledge that risk and decide how to deal with it: accept this risk, transfer this risk, or reduce this risk.

Accept: This means that you document that there is a risk, but take no action to mitigate that risk because the risk is too far-fetched or the mitigation costs are too prohibitive.

Transfer: This is buying insurance against a risk that cannot be eliminated or reduced further.

Figure 1-2 illustrates the key factors you should consider when designing a secure network:

- **Business needs:** What does your organization want to do with the network?
- **Risk analysis:** What is the risk and cost balance?
- **Security policy:** What are the policies, standards, and guidelines that you need to address business needs and risks?
- **Industry best practices:** What are the reliable, well-understood, and recommended security best practices?
- **Security operations:** These operations include incident response, monitoring, maintenance, and auditing the system for compliance.

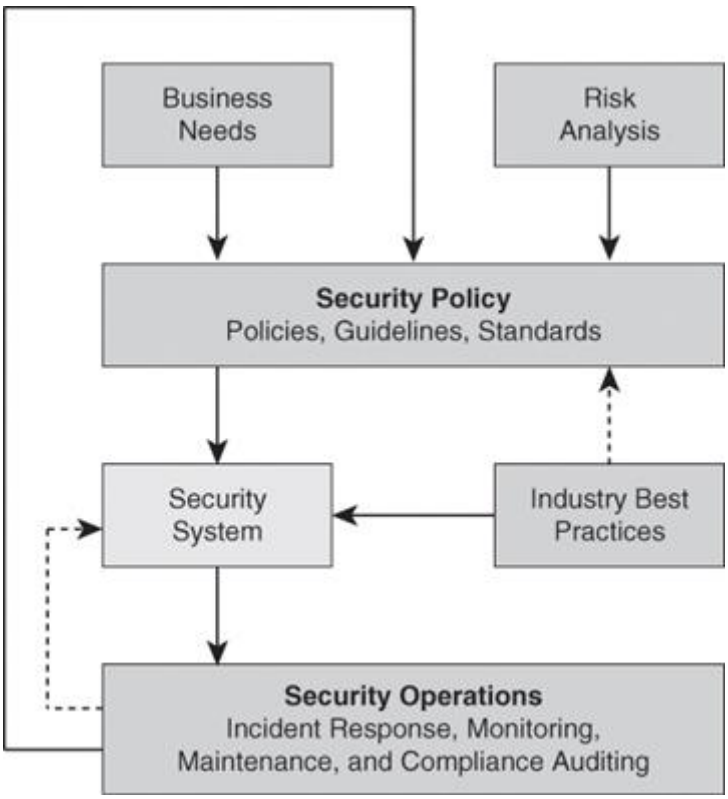

Figure 1-2. Factors Affecting the Design of a Secure Network

Risk management and security policies will be detailed later in this chapter.

Intent Evolution

When viewed from the perspective of motivation intersecting with opportunity, risk management can be driven not only by the techniques or sophistication of the attackers and threat vectors, but also by their motives. Research reveals that hackers are increasingly motivated by profit, where in the past they were motivated by notoriety and fame. In instances of attacks carried out for financial gains, hackers are not looking for attention, which makes their exploits harder to detect. Few signatures exist or will ever be written to capture these "custom" threats. In order to be successful in defending your environments, you must employ a new model to catch threats across the infrastructure.

Attackers are also motivated by government or industrial espionage. The Stuxnet worm, whose earliest versions appear to date to 2009, is an example. This worm differs from its malware "cousins" in that it has a specific, damaging goal: to traverse industrial control systems, such as supervisory control and data acquisition (SCADA) systems, so that it can reprogram the programmable logic controllers, possibly disrupting industrial operations.

This worm was not created to gather credit card numbers to sell off to the highest bidder, or to sell fake pharmaceuticals. This worm appears to have been created solely to invade public or private infrastructure. The cleverness of Stuxnet lies in its ability to traverse non-networked systems, which means that even systems unconnected to networks or the Internet are at risk.

Security experts have called Stuxnet "the smartest malware ever." This worm breaks the malware mold because it is designed to disrupt industrial control systems in critical infrastructure. This ability should be a concern for every government.

Motivation can also so be political or in the form of vigilantism. Anonymous is currently the best known hacktivist group. As a recent example of its activities, in May 2012, Anonymous attacked the website of the Quebec government after its promulgation of a law imposing new requirements for the right to protest by college and university students.

Threat Evolution

The nature and sophistication of threats, as well as their pervasiveness and global nature, are trends to watch.Figure 1-3 shows how the threats that organizations face have evolved over the past few decades, and how the growth rate of vulnerabilities that are reported in operating systems and applications is rising. The number and variety of viruses and worms that have appeared over the past three years is daunting, and their rate of propagation is frightening. There have been unacceptable levels of business outages and expensive remediation projects that consume staff, time, and funds that were not originally budgeted for such tasks.

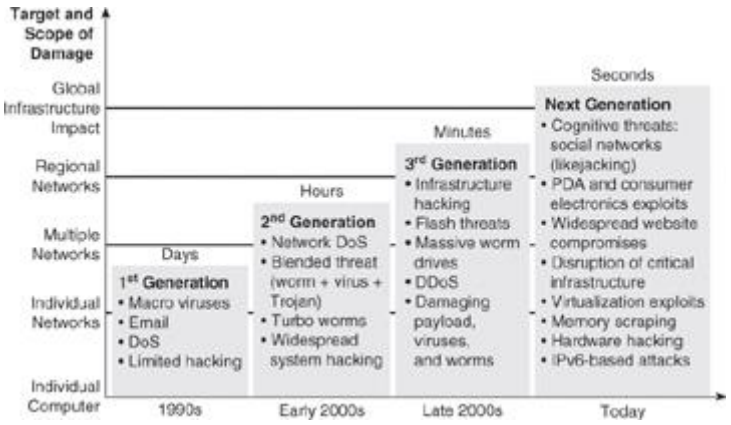

Figure 1-3. Shrinking Time Frame from Knowledge of Vulnerability to Release of Exploits

New exploits are designed to have global impact in minutes. Blended threats, which use multiple means of propagation, are more sophisticated than ever. The trends are becoming regional and global in nature. Early attacks affected single systems or one organization network, while attacks that are more recent are affecting entire regions. For example, attacks have expanded from individual denial of service (DoS) attacks from a single attacker against a single target, to large-scale distributed DoS (DDoS) attacks emanating from networks of compromised systems that are known as botnets.

Threats are also becoming persistent. After an attack starts, attacks may appear in waves as infected systems join the network. Because infections are so complex and have so many end users (employees, vendors, and contractors), multiple types of endpoints (company desktop, home, and server), and multiple types of access (wired, wireless, VPN, and dial-up), infections are difficult to eradicate.

More recent threat vectors are increasingly sophisticated, and the motivation of the attackers is reflected in their impact. Recent threat vectors include the following:

- **Cognitive threats via social networks (likejacking):** Social engineering takes a new meaning in the era of social networking. From phishing attacks that target social network accounts of high-profile individuals, to information exposure due to lack of policy, social networks have become a target of choice for malicious attackers.
- **PDA and consumer electronics exploits:** The operating systems on consumer devices (smartphones, PDAs, and so on) are an option of choice for high-volume attacks. The proliferation of applications for these operating systems, and the nature of the development and certification processes for those applications, augments the problem.
- **Widespread website compromises:** Malicious attackers compromise popular websites, making the sites download malware to connecting users. Attackers typically are not interested in the data on the website, but use it as a springboard to infect the users of the site.
- **Disruption of critical infrastructure:** The Stuxnet malware, which exploits holes in Windows systems and targets a specific Siemens supervisory control and data acquisition (SCADA) program with sabotage, confirmed concerns about an increase in targeted attacks aimed at the power grid, nuclear plants, and other critical infrastructure.
- **Virtualization exploits:** Device and service virtualization add more complexity to the network. Attackers know this and are increasingly targeting virtual servers, virtual switches, and trust relationships at the hypervisor level.
- **Memory scraping:** Increasingly popular, this technique is aimed at fetching information directly from volatile memory. The attack tries to exploit operating systems and applications that leave traces of data in memory. Attacks are particularly aimed at encrypted information that may be processed as unencrypted in volatile memory.
- **Hardware hacking:** These attacks are aimed at exploiting the hardware architecture of specific devices, with consumer devices being increasingly popular. Attack methods include bus sniffing, altering firmware, and memory dumping to find crypto keys.
- **IPv6-based attacks:** These attacks could become more pervasive as the migration to IPv6 becomes widespread. Attackers are focusing initially on covert channels through various tunneling techniques, and man-in-the middle attacks leverage IPv6 to exploit IPv4 in dual-stack deployments.

Trends Affecting Network Security

Other trends in business, technology, and innovation influence the need for new paradigms in information security. Mobility is one trend. Expect to see billions of new network mobile devices moving into the enterprise worldwide over the next few years. Taking into consideration constant reductions and streamlining in IT budgets, organizations face serious challenges in supporting a growing number of mobile devices at a time when their resources are being reduced.

The second market transition is cloud computing and cloud services. Organizations of all kinds are taking advantage of offerings such as Software as a Service (SaaS) and Infrastructure as a Service (IaaS) to reduce costs and simplify the deployment of new services and applications.

These cloud services add challenges in visibility (how do you identify and mitigate threats that come to and from a trusted network?), control (who controls the physical assets, encryption keys, and so on?), and trust (do you trust cloud partners to ensure that critical application data is still protected when it is off the enterprise network?).

The third market transition is about changes to the workplace experience. Borders are blurring in the organization between consumers and workers and between the various functions within the organization. The borders between the company and its partners, customers, and suppliers, are also fading. As a result, the network is experiencing increasing demand to connect anyone, any device, anywhere, at any time.

These changes represent a challenge to security teams within the organization. These teams now need to manage noncontrolled consumer devices, such as a personal tablet, coming into the network, and provide seamless and context-aware services to users all over the world. The location of the data and services accessed by the users is almost irrelevant. The data could be internal to the organization or it could be in the cloud. This situation makes protecting data and services a challenging proposition.

NOTE

Readers interested in staying current with Network Security trends and technologies could subscribe to some of the numerous podcasts available on iTunes, such as:

- Cisco Interactive Network TechWiseTV
- Security Now!
- Security Wire Weekly
- Silver Bullet Security
- Crypto-Gram Security

Attacks are increasingly politically and financially motivated, driven by botnets, and aimed at critical infrastructure; for example:

- Botnets are used for spam, data theft, mail relays, or simply for denial-of-service attacks (ref: http://en.wikipedia.org/wiki/Botnet).
- Zeus botnets reached an estimated 3.6 million *bots*, infected workstations, or “zombies” (ref: http://www.networkworld.com/news/2009/072209-botnets.html).
- Stuxnet was aimed at industrial systems.
- Malware is downloaded inadvertently from online marketplaces.

One of the trends in threats is the exploitation of trust. Whether they are creating malware that can subvert industrial processes or tricking social network users into handing over login and password information, cybercriminals have a powerful weapon at their disposal: the exploitation of trust. Cybercriminals have become skilled at convincing users that their infected links and URLs are safe to click, and that they are someone the user knows and trusts. Hackers exploit the trust we have in TinyURLs and in security warning banners. With stolen security credentials, cybercriminals can freely interact with legitimate software and systems.

Nowhere is this tactic more widespread than within social networking, where cybercriminals continue to attract victims who are willing to share information with people they believe are known to them, with malware such as Koobface. One noticeable shift in social engineering is that criminals are spending more time figuring out how to assume someone's identity, perhaps by generating emails from an individual's computer or social networking account. A malware-laden email or scam sent by a "trusted person" is more likely to elicit a click-through response than the same message sent by a stranger.

Threats originating from countries outside of the United States are rapidly increasing. Global annual spam volumes actually dropped in 2010, the first time this has happened in the history of the Internet. However, spammers are originating in increasingly varied locations and countries.

Money muling is the practice of hiring individuals as "mules," recruited by handlers or "wranglers" to set up bank accounts, or even use their own bank accounts, to assist in the transfer of money from the account of a fraud victim to another location, usually overseas, via a wire transfer or automated clearing house (ACH) transaction. Money mule operations often involve individuals in multiple countries.

Web malware is definitely on the rise. The number of distinct domains that are compromised to download malware to connecting users is increasing dramatically. The most dangerous aspect of this type of attack is the fact that users do not need to do much to get infected. Many times, the combination of malware on the website and vulnerabilities on web browsers is enough to provoke infection just by connecting to the website. The more popular the site, the higher the volume of potential infection.

Recently there have been major shifts in the compliance landscape. Although enforcement of existing regulations has been weak in many jurisdictions worldwide, regulators and standards bodies are now tightening enforcement through expanded powers, higher penalties, and harsh enforcement actions. In the future it will be more difficult to hide failures in information security wherever organizations do business. Legislators are forcing transparency through the introduction of breach notification laws in Europe, Asia, and North America as data breach disclosure becomes a global principle.

As more regulations are introduced, there is a trend toward increasingly prescriptive rules. For example, recent amendments introduced in the United Kingdom in 2011 bring arguably more prescriptive information protection regulations to the Privacy and Electronic Communications Directive. Such laws are discussed in more detailed later in this chapter. Any global enterprise that does business in the United Kingdom today will likely be covered by these regulations. Lately, regulators are also making it clear that enterprises are responsible for ensuring the protection of their data when it is being processed by a business partner, including cloud service providers. The new era of compliance creates formidable challenges for organizations worldwide.

For many organizations, stricter compliance could help focus management attention on security, but if managers take a "check-list approach" to compliance, it will detract from actually managing risk and may not improve security. The new compliance landscape will increase costs and risks. For example, it takes time and resources to substantiate compliance. Increased requirements for service providers give rise to more third-party risks.

With more transparency, there are now greater consequences for data breaches. For example, expect to see more litigation as customers and business partners seek compensation for compromised data. But the harshest judgments will likely come from the court of public opinion, with the potential to permanently damage an enterprise's reputation.

The following are some of the U.S. and international regulations that many companies are subject to:

- Sarbanes-Oxley (SOX)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Digital Millennium Copyright Act (DMCA)
- Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- European Union Data Protection Directive (EU 95/46/EC)
- Safe Harbor Act - European Union and United States
- International Convergence of Capital Measurement and Capital Standards (Basel II)

The challenge becomes to comply with these regulations and, at the same time, make that compliance translate into an effective security posture.

Adversaries, Methodologies, and Classes of Attack

Who are hackers? What motivates them? How do they conduct their attacks? How do they manage to breach the measures we have in place to ensure confidentiality, integrity, and availability? Which best practices can we adopt to defeat hackers? These are some of the questions we try to answer in this section.

People are social beings, and it is quite common for systems to be compromised through social engineering. Harm can be caused by people just trying to be "helpful." For example, in an attempt to be helpful, people have been known to give their passwords over the phone to attackers who have a convincing manner and say they are troubleshooting a problem and need to test access using a real user password. End users must be trained, and reminded, that the ultimate security of a system depends on their behavior.

Of course, people often cause harm within organizations intentionally: most security incidents are caused by insiders. Thus, strong internal controls on security are required, and special organizational practices might need to be implemented.

An example of a special organizational practice that helps to provide security is the separation of duty, where critical tasks require two or more persons to complete them, thereby reducing the risk of insider threat. People are less likely to attack or misbehave if they are required to cooperate with others.

Unfortunately, users frequently consider security too difficult to understand. Software often does not make security options or decisions easy for end users. Also, users typically prefer "whatever" functionality to no functionality. Implementation of security measures should not create an internally generated DoS, meaning, if security is too stringent or too cumbersome for users, either they will not have access to all the resources needed to perform their work or their performance will be hindered by the security operations.

Adversaries

To defend against attacks on information and information systems, organizations must begin to define the threat by identifying potential adversaries. These adversaries can include the following:

- Nations or states
- Terrorists
- Criminals
- Hackers
- Corporate competitors
- Disgruntled employees
- Government agencies, such as the National Security Agency (NSA) and the Federal Bureau of Investigations (FBI)

Hackers comprise the most well-known outside threat to information systems. They are not necessarily geniuses, but they are persistent people who have taken a lot of time to learn their craft.

Many titles are assigned to hackers:

- **Hackers:** Hackers are computer enthusiasts who break into networks and systems to learn more about them. Some hackers generally mean no harm and do not expect financial gain. Unfortunately, hackers may unintentionally pass valuable information on to people who do intend to harm the system. Hackers are subdivided into the following categories:
    - White hat (ethical hacker)
    - Blue hat (bug tester)
    - Gray hat (ethically questionable hacker)
    - Black hat (unethical hacker)
- **Crackers (criminal hackers):** Crackers are hackers with a criminal intent to harm information systems. Crackers are generally working for financial gain and are sometimes called black hat hackers.
- **Phreakers (phone breakers):** Phreakers pride themselves on compromising telephone systems. Phreakers reroute and disconnect telephone lines, sell wiretaps, and steal long-distance services.

  NOTE

  When describing individuals whose intent is to exploit a network maliciously, these individuals are often incorrectly referred to as hackers. In this section, the term hacker is used, but might refer to someone more correctly referred to as a cracker, or black hat hacker.

- **Script kiddies:** Script kiddies think of themselves as hackers, but have very low skill levels. They do not write their own code; instead, they run scripts written by other, more skilled attackers.
- **Hacktivists:** Hacktivists are individuals who have a political agenda in doing their work. When government websites are defaced, this is usually the work of a hacktivist.

Methodologies

The goal of any hacker is to compromise the intended target or application. Hackers begin with little or no information about the intended target, but by the end of their analysis, they have accessed the network and have begun to compromise their target. Their approach is usually careful and methodical, not rushed and reckless. The seven-step process that follows is a good representation of the methods that hackers use:

- **Step 1.** Perform footprint analysis (reconnaissance).
- **Step 2.** Enumerate applications and operating systems.
- **Step 3.** Manipulate users to gain access.
- **Step 4.** Escalate privileges.
- **Step 5.** Gather additional passwords and secrets.
- **Step 6.** Install back doors.
- **Step 7.** Leverage the compromised system.

CAUTION

Hackers have become successful by thinking "outside the box." This methodology is meant to illustrate the steps that a structured attack might take. Not all hackers will follow these steps in this order.

To successfully hack into a system, hackers generally first want to know as much as they can about the system. Hackers can build a complete profile, or "footprint," of the company security posture. Using a range of tools and techniques, an attacker can discover the company domain names, network blocks, IP addresses of systems, ports and services that are used, and many other details that pertain to the company security posture as it relates to the Internet, an intranet, remote access, and an extranet. By following some simple advice, network administrators can make footprinting more difficult.

After hackers have completed a profile, or footprint, of your organization, they use tools such as those in the list that follows to enumerate additional information about your systems and networks. All these tools are readily available to download, and the security staff should know how these tools work. Additional tools (introduced later in the "Security Testing Techniques" section) can also be used to gather information and therefore hack.

- **Netcat:** Netcat is a featured networking utility that reads and writes data across network connections.
- **Microsoft EPDump and Microsoft Remote Procedure Call (RPC) Dump:** These tools provide information about Microsoft RPC services on a server.
- **GetMAC:** This application provides a quick way to find the MAC (Ethernet) layer address and binding order for a computer running Microsoft Windows locally or across a network.
- **Software development kits (SDK):** SDKs provide hackers with the basic tools that they need to learn more about systems.

Another common technique that hackers use is to manipulate users of an organization to gain access to that organization. There are countless cases of unsuspecting employees providing information to unauthorized people simply because the requesters appear innocent or to be in a position of authority. Hackers find names and telephone numbers on websites or domain registration records by footprinting. Hackers then directly contact these people by phone and convince them to reveal passwords. Hackers gather information without raising any concern or suspicion. This form of attack is called *social engineering*. One form of a social engineering attack is for the hacker to pose as a visitor to the company, a delivery person, a service technician, or some other person who might have a legitimate reason to be on the premises and, after gaining entrance, walk by cubicles and look under keyboards to see whether anyone has put a note there containing the current password.

The next thing the hacker typically does is review all the information that they have collected about the host, searching for usernames, passwords, and Registry keys that contain application or user passwords. This information can help hackers escalate their privileges on the host or network. If reviewing the information from the host does not reveal useful information, hackers may launch a Trojan horse attack in an attempt to escalate their privileges on the host. This type of attack usually means copying malicious code to the user system and giving it the same name as a frequently used piece of software.

After the hacker has obtained higher privileges, the next task is to gather additional passwords and other sensitive data. The targets now include such things as the local security accounts manager database or the Active Directory of a domain controller. Hackers use legitimate tools such as pwdump and lsadump applications to gather passwords from machines running Windows, which then can be cracked with the very popular Cain & Abel software tool. By cross-referencing username and password combinations, the hacker is able to obtain administrative access to all the computers in the network.

If hackers are detected trying to enter through the "front door," or if they want to enter the system without being detected, they try to use "back doors" into the system. A back door is a method of bypassing normal authentication to secure remote access to a computer while attempting to remain undetected. The most common backdoor point is a listening port that provides remote access to the system for users (hackers) who do not have, or do not want to use, access or administrative privileges.

After hackers gain administrative access, they enjoy hacking other systems on the network. As each new system is hacked, the attacker performs the steps that were outlined previously to gather additional system and password information. Hackers try to scan and exploit a single system or a whole set of networks and usually automate the whole process.

In addition, hackers will cover their tracks either by deleting log entries or falsifying them.

Thinking Outside the Box

In 2005, David Sternberg hacked the Postal Bank in Israel by physically breaking into one of the bank's branches in Haifa and connecting a wireless access point in the branch's IT infrastructure. Sternberg rented office space about 100 feet from the bank and proceeded to transfer funds to bank accounts in his name or in friends' names.

So instead of trying for months to break into the IT security of the bank, Sternberg thought outside of the box and broke through physical security to gain access to the IT system.

Sternberg was discovered when bank auditors noticed regular transfers from the main bank account to the same individual accounts.

I guess that Sternberg had not heard about the security axiom that says “predictability is the enemy of security.”

A common thread in infosec forums is that information security specialists must patch all security holes in a network—a hacker only has to find the one that wasn’t patched. Security is like a chain. It is only as strong as its weakest link.

Threats Classification

In classifying security threats, it is common to find general categories that resemble the perspective of the attacker and the approaches that are used to exploit software. Attack patterns are a powerful mechanism to capture and communicate the perspective of the attacker. These patterns are descriptions of common methods for exploiting vulnerabilities. The patterns derive from the concept of design patterns that are applied in a destructive rather than constructive context and are generated from in-depth analysis of specific, real-world exploit examples. The following list illustrates examples of threat categories that are based on this criterion. Notice that some threats are not malicious attacks. Examples of nonmalicious threats include forces of nature such as hurricanes and earthquakes.

Later in this chapter, you learn about some of the general categories under which threats can be regrouped, such as:

- Enumeration and fingerprinting
- Spoofing and impersonation
- Man-in-the-middle
- Overt and covert channels
- Blended threats and malware
- Exploitation of privilege and trust
- Confidentiality
- Password attacks
- Availability attacks
    - Denial of service (DoS)
    - Botnet
- Physical security attacks
- Forces of nature

To assist in enhancing security throughout the security lifecycle, there are many publicly available classification databases that provide a catalog of attack patterns and classification taxonomies. They are aimed at providing a consistent view and method for identifying, collecting, refining, and sharing attack patterns for specific communities of interest. The following are four of the most prominent databases:

- **Common Attack Pattern Enumeration and Classification (CAPEC):** Sponsored by the U.S. Department of Homeland Security as part of the software assurance strategic initiative of the National Cyber Security Division, the objective of this effort is to provide a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy. More information can be found at http://capec.mitre.org.
- **Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS):** OWASP is a not-for-profit worldwide charitable organization focused on improving the security of application software. The primary objective of ASVS is to normalize the range in the coverage and level of rigor available in the market when it comes to performing web application security verification using a commercially workable open standard. More information can be found at https://www.owasp.org.
- **Web Application Security Consortium Threat Classification (WASC TC):** Sponsored by the WASC, this is a cooperative effort to clarify and organize the threats to the security of a website. The project is aimed at developing and promoting industry-standard terminology for describing these issues. Application developers, security professionals, software vendors, and compliance auditors have the ability to access a consistent language and definitions for web security-related issues. More information can be found at http://www.webappsec.org.
- **Malware Attribute Enumeration and Characterization (MAEC):** Created by MITRE, this effort is international in scope and free for public use. MAEC is a standardized language for encoding and communicating high-fidelity information about malware based on attributes such as behaviors, artifacts, and attack patterns. More information can be found at http://maec.mitre.org.

Enumeration and Fingerprinting with Ping Sweeps and Port Scans

Enumeration and fingerprinting are types of attacks that use legitimate tools for illegitimate purposes. Some of the tools, such as port-scan and ping-sweep applications, run a series of tests against hosts and devices to identify vulnerable services that need attention. IP addresses and port or banner data from both TCP and UDP ports are examined to gather information.

In an illegitimate situation, a port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services (each service is associated with a well-known port number) the computer provides. Port scanning can be automated to scan a range of TCP or UDP port numbers on a host to detect listening services. Port scanning, a favorite computer hacker approach, provides information to the hacker about where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is being used and needs further probing.

A ping sweep, also known as an Internet Control Message Protocol (ICMP) sweep, is a basic network-scanning technique that is used to determine which IP addresses map to live hosts (computers). A ping sweep consists of ICMP echo-requests (pings) sent to multiple hosts, whereas a single ping consists of ICMP echo-requests that are sent to one specific host computer. If a given address is live, that host returns an ICMP echo-reply. The goal of the ping sweep is to find hosts available on the network to probe for vulnerabilities. Ping sweeps are among the oldest and slowest methods that are used to scan a network.

IP Spoofing Attacks

The prime goal of an IP spoofing attack is to establish a connection that allows the attacker to gain root access to the host and to create a backdoor entry path into the target system.

IP spoofing is a technique used to gain unauthorized access to computers whereby the intruder sends messages to a computer with an IP address that indicates the message is coming from a trusted host. The attacker learns the IP address of a trusted host and modifies the packet headers so that it appears that the packets are coming from that trusted host.

At a high level, the concept of IP spoofing is easy to comprehend. Routers determine the best route between distant computers by examining the destination address, and ignore the source address. In a spoofing attack, an attacker outside your network pretends to be a trusted computer by using a trusted internal or external IP address.

If an attacker manages to change the routing tables to divert network packets to the spoofed IP address, the attacker can receive all the network packets addressed to the spoofed address and reply just as any trusted user can.

IP spoofing can also provide access to user accounts and passwords. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization. The attacker could send email messages to business partners that appear to have originated from someone within your organization. Such attacks are easier to perpetrate when an attacker has a user account and password, but they are also possible when attackers combine simple spoofing attacks with their knowledge of messaging protocols.

A rudimentary use of IP spoofing also involves bombarding a site with IP packets or ping requests, spoofing a source, a third-party registered public address. When the destination host receives the requests, it responds to what appears to be a legitimate request. If multiple hosts are attacked with spoofed requests, their collective replies to the third-party spoofed IP address create an unsupportable flood of packets, thus creating a DoS attack.

Technical Discussion of IP Spoofing

TCP/IP works at Layer 3 and Layer 4 of the Open Systems Interconnection (OSI) model, IP at Layer 3 and TCP at Layer 4. IP is a connectionless model, which means that packet headers do not contain information about the transaction state that is used to route packets on a network. There is no method in place to ensure proper delivery of a packet to the destination, since at Layer 3, there is no acknowledgement sent back to the source by the destination once it has received the packet.

The IP header contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify the source address field. Note that in IP each datagram is independent of all others because of the stateless nature of IP. To engage in IP spoofing, hackers find the IP address of a trusted host and modify their own packet headers to appear as though packets are coming from that trusted host (source address).

TCP uses a connection-oriented design. This design means that the participants in a TCP session must first build a connection using the three-way handshake, as shown in Figure 1-4.

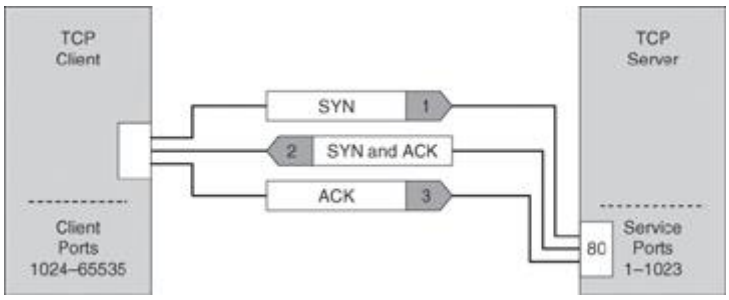

Figure 1-4. TCP Three-Way Handshake

After the connection is established, TCP ensures data reliability by applying the same process to every packet as the two machines update one another on progress. The sequence and acknowledgments take place as follows:

1. The client selects and transmits an initial sequence number.
2. The server acknowledges the initial sequence number and sends its own sequence number.
3. The client acknowledges the server sequence number, and the connection is open to data transmission.

Sequence Prediction

The basis of IP spoofing during a TCP communication lies in an inherent security weakness known as sequence prediction. Hackers can guess or predict the TCP sequence numbers that are used to construct a TCP packet without receiving any responses from the server. Their prediction allows them to spoof a trusted host on a local network. To mount an IP spoofing attack, the hacker listens to communications between two systems. The hacker sends packets to the target system with the source IP address of the trusted system, as shown in Figure 1-5.

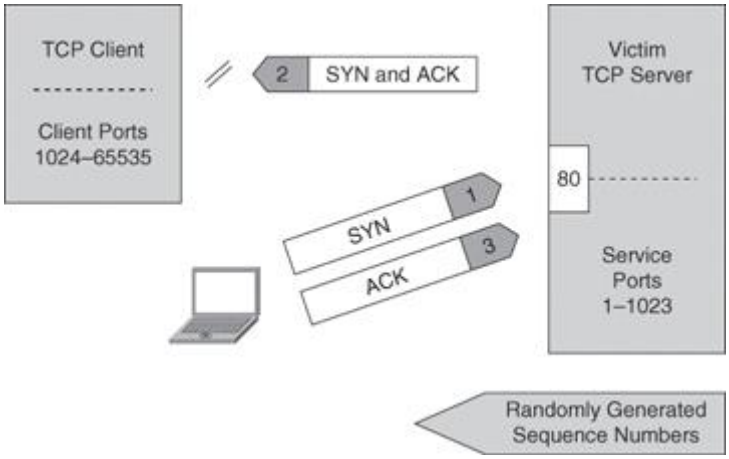

Figure 1-5. Sequence Number Prediction

If the packets from the hacker have the sequence numbers that the target system is expecting, and if these packets arrive before the packets from the real, trusted system, the hacker becomes the trusted host.

To engage in IP spoofing, hackers must first use a variety of techniques to find an IP address of a trusted host and then modify their packet headers to appear as though packets are coming from

that trusted host. Further, the attacker can engage other unsuspecting hosts to generate traffic that appears as though it too is coming from the trusted host, thus flooding the network.

Trust Exploitation

Trust exploitation refers to an individual taking advantage of a trust relationship within a network.

As an example of trust exploitation, consider the network shown in Figure 1-6, where system A is in the demilitarized zone (DMZ) of a firewall. System B, located in the inside of the firewall, trusts System A. When a hacker on the outside network compromises System A in the DMZ, the attacker can leverage the trust relationship it has to gain access to System A.

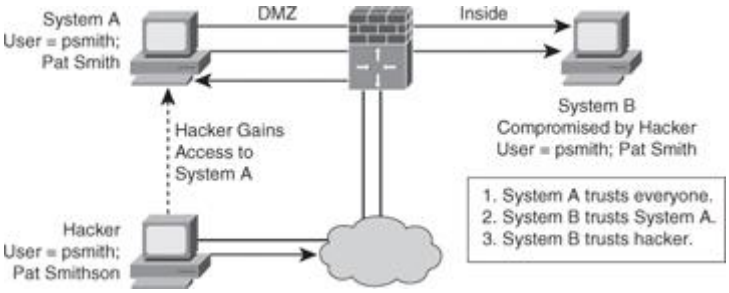

Figure 1-6. Trust Exploitation

A DMZ can be seen as a semi-secure segment of your network. A DMZ is typically used to provide to outside users access to corporate resources, because these users are not allowed to reach inside servers directly. However, a DMZ server might be allowed to reach inside resources directly. In a trust exploitation attack, a hacker could hack a DMZ server and use it as a springboard to reach the inside network.

Several trust models may exist in a network:

- Windows
  - Domains
  - Active Directory
- Linux and UNIX
  - Network File System (NFS)
  - Network Information Services Plus (NIS+)

Password Attacks

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, keyloggers, packet sniffers, and dictionary attacks. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called *brute-force attacks*.

To execute a brute-force attack, an attacker can use a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker gains access to a resource, the attacker has the same access rights as the rightful user. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account.

Just as with packet sniffers and IP spoofing attacks, a brute-force password attack can provide access to accounts that attackers then use to modify critical network files and services. For example, an attacker compromises your network integrity by modifying your network routing tables. This trick reroutes all network packets to the attacker before transmitting them to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

Passwords present a security risk if they are stored as plain text. Thus, passwords must be encrypted in order to avoid risks. On most systems, passwords are processed through an encryption algorithm that generates a one-way hash on passwords. You cannot reverse a one-way hash back to its original text. Most systems do not decrypt the stored password during authentication; they store the one-way hash. During the login process, you supply an account and password, and the password encryption algorithm generates a one-way hash. The algorithm compares this hash to the hash stored on the system. If the hashes are the same, the algorithm assumes that the user supplied the proper password.

Remember that passing the password through an algorithm results in a password hash. The hash is not the encrypted password, but rather a result of the algorithm. The strength of the hash is such that the hash value can be re-created only by using the original user and password information, and that it is impossible to retrieve the original information from the hash. This strength makes hashes perfect for encoding passwords for storage. In granting authorization, the hashes, rather than the plain-text password, are calculated and compared.

Hackers use many tools and techniques to crack passwords:

- **Word lists:** These programs use lists of words, phrases, or other combinations of letters, numbers, and symbols that computer users often use as passwords. Hackers enter word after word at high speed (called a *dictionary attack*) until they find a match.
- **Brute force:** This approach relies on power and repetition. It compares every possible combination and permutation of characters until it finds a match. Brute force eventually cracks any password, but it might take a long, long time. Brute force is an extremely slow process because it uses every conceivable character combination.
- **Hybrid crackers:** Some password crackers mix the two techniques. This combines the best of both methods and is highly effective against poorly constructed passwords.

Password cracking attacks any application or service that accepts user authentication, including the following:

- NetBIOS over TCP (TCP 139)
- Direct host (TCP 445)
- FTP (TCP 21)
- Telnet (TCP 23)
- Simple Network Management Protocol (SNMP) (UDP 161)
- Point-to-Point Tunneling Protocol (PPTP) (TCP 1723)
- Terminal services (TCP 3389)

NOTE

RainbowCrack is a compilation of hashes that provides crackers with a list that they can use to attempt to match hashes that they capture with sniffers.

Confidentiality and Integrity Attacks

Confidentiality breaches can occur when an attacker attempts to obtain access to read-sensitive data. These attacks can be extremely difficult to detect because the attacker can copy sensitive data without the knowledge of the owner and without leaving a trace.

A confidentiality breach can occur simply because of incorrect file protections. For instance, a sensitive file could mistakenly be given global read access. Unauthorized copying or examination of the file would probably be difficult to track without having some type of audit mechanism running that logs every file operation. If a user had no reason to suspect unwanted access, however, the audit file would probably never be examined.

In Figure 1-7, the attacker is able to compromise an exposed web server. Using this server as a beachhead, the attacker then gains full access to the database server from which customer data is downloaded. The attacker then uses information from the database, such as a username, password, and email address, to intercept and read sensitive email messages destined for a user in the branch office. This attack is difficult to detect because the attacker did not modify or delete any data. The data was only read and downloaded. Without some kind of auditing mechanism on the server, it is unlikely that this attack will be discovered.

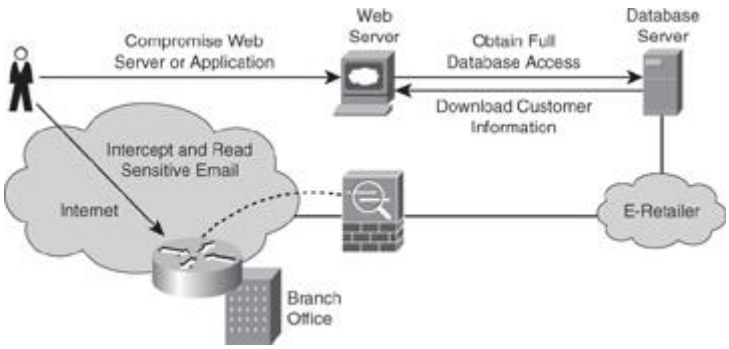

Figure 1-7. Breach of Confidentiality

Attackers can use many methods to compromise confidentiality, the most common of which are as follows:

- **Ping sweeps and port scanning:** Searching a network host for open ports.
- **Packet sniffing:** Intercepting and logging traffic that passes over a digital network or part of a network.
- **Emanations capturing:** Capturing electrical transmissions from the equipment of an organization to deduce information regarding the organization.
- **Overt channels:** Listening on obvious and visible communications. Overt channels can be used for covert communication.
- **Covert channels:** Hiding information within a transmission channel that is based on encoding data using another set of events.
- **Wiretapping:** Monitoring the telephone or Internet conversations of a third party, often covertly.
- **Social engineering:** Using social skills or relationships to manipulate people inside the network to provide the information needed to access the network.
- **Dumpster diving:** Searching through company dumpsters or trash cans looking for information, such as phone books, organization charts, manuals, memos, charts, and other documentation that can provide a valuable source of information for hackers.

- **Phishing:** Attempting to criminally acquire sensitive information, such as usernames and passwords, by masquerading as trustworthy entities.
- **Pharming:** Redirecting the traffic of a website to another, rogue website.

Many of these methods are used to compromise more than confidentiality. They are often elements of attacks on integrity and availability.

Man-in-the-Middle Attacks

A complex form of IP spoofing is called man-in-the-middle attack, where the hacker monitors the traffic that comes across the network and introduces himself as a stealth intermediary between the sender and the receiver, as shown in Figure 1-8.

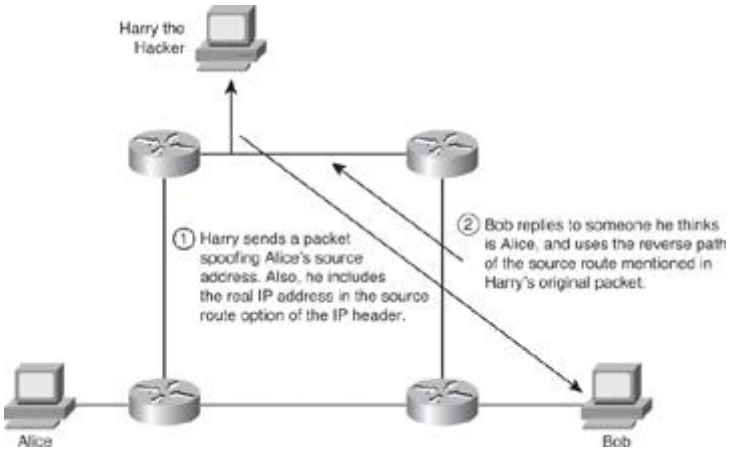

Figure 1-8. IP Source Routing Attack

Hackers use man-in-the-middle attacks to perform many security violations:

- Theft of information
- Hijacking of an ongoing session to gain access to your internal network resources
- Analysis of traffic to derive information about your network and its users
- DoS
- Corruption of transmitted data
- Introduction of new information into network sessions

Attacks are blind or nonblind. A blind attack interferes with a connection that takes place from outside, where sequence and acknowledgment numbers are unreachable. A nonblind attack interferes with connections that cross wiring used by the hacker. A good example of a blind attack can be found at http://wiki.cas.mcmaster.ca/index.php/The_Mitnick_attack.

TCP session hijacking is a common variant of the man-in-the-middle attack. The attacker sniffs to identify the client and server IP addresses and relative port numbers. The attacker modifies his or her packet headers to spoof TCP/IP packets from the client, and then waits to receive an ACK packet from the client communicating with the server. The ACK packet contains the sequence number of the next packet that the client is expecting. The attacker replies to the client using a modified packet with the source address of the server and the destination address of the client. This packet results in a reset that disconnects the legitimate client. The attacker takes over communications with the server by spoofing the expected sequence number from the ACK that was previously sent from the legitimate client to the server. (This could also be an attack against confidentiality.)

Another cleaver man-in-the-middle attack is for the hacker to successfully introduce himself as the DHCP server on the network, providing its own IP address as the default gateway during the DHCP offer.

NOTE

At this point, having read about many different attacks, you might be concerned that the security of your network is insufficient. Do not despair: many of the attacks described here are mitigated by techniques explained in this book or in other Cisco Press security books, such as *CCNP Security SECURE 642-637 Official Cert Guide*.

Overt and Covert Channels

Overt and covert channels refer to the capability to hide information within or using other information:

- **Overt channel:** A transmission channel that is based on tunneling one protocol inside of another. It could be a clear-text transmission inserted inside another clear-text protocol header.
- **Covert channel:** A transmission channel that is based on encoding data using another set of events. The data is concealed.

There are numerous ways that Internet protocols and the data that is transferred over them can provide overt and covert channels. The bad news is that firewalls generally cannot detect these channels; therefore, attackers can use them to receive confidential information in an unauthorized manner.

With an overt channel, one protocol is tunneled within another to bypass the security policy; for example, Telnet over FTP, instant messaging over HTTP, and IP over Post Office Protocol version 3 (POP3). Another example of an overt channel is using watermarks in JPEG images to leak confidential information.

One common use of overt channel is for instant messaging (IM). Most organization firewalls allow outbound HTTP but block IM. A user on the inside of the network can leak confidential information using IM over an HTTP session.

In Figure 1-9, the firewall allows outbound HTTP while a user on the inside of the network is leaking confidential information using instant messaging over HTTP.

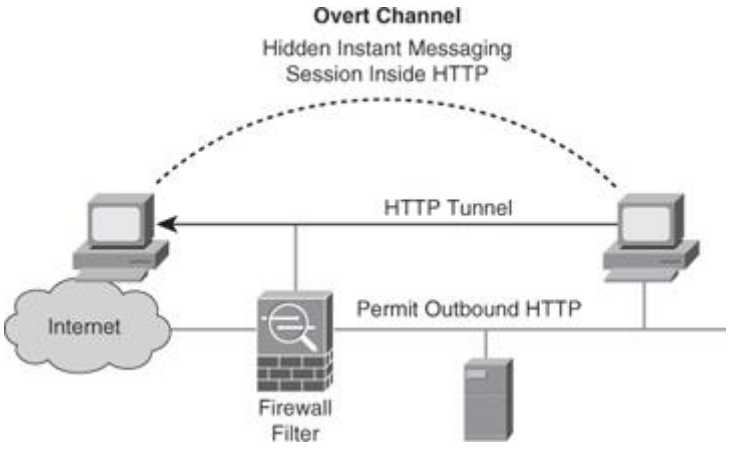

Figure 1-9. Overt Channel

NOTE

You can use the advanced protocol inspection in the Cisco IPS products and Cisco ASA 5500 series appliances to counter attacks such as a hidden IM session being sent inside HTTP.

Steganography is another example of an overt channel. Steganography (from the Greek word *steganos*, meaning "covered" or "secret") literally means covered or secret writing. The combination of CPU power and interest in privacy has led to the development of techniques for hiding messages in digital pictures and digitized audio.

For example, certain bits of a digital graphic can be used to hide messages. The key to knowing which bits are special is shared between two parties that want to communicate privately. The private message typically has so few bits relative to the total number of bits in the image that changing them is not visually noticeable. Without a direct comparison of the original and the processed image, it is practically impossible to tell that anything has been changed. Still, it might be detected by statistical analysis that detects non-randomness. This non-randomness in a file indicates that information is being passed inside of the file.

NOTE

Steganography is very difficult to detect or prevent.

With a covert channel, information is encoded as another set of events. For example, an attacker could install a Trojan horse on a target host. The Trojan horse could be written to send binary information back to the server of the attacker. The client, infected with the Trojan horse, could return to the hacker's server a ping status report in a binary format, where a 0 would represent a successful ping over a one-minute period, and a 1 would represent two successful pings over a one-minute period. The hacker could keep connectivity statistics for all the compromised clients he has around the world.

If ICMP is not permitted through a firewall, another tactic is to have the client visit the web page of the attacker. The Trojan horse software, now installed on the client, has a "call home" feature that automatically opens a connection to TCP port 80 at a specific IP address, the address of the hacker's web server. All of this work is done so that the hacker can keep precise statistics of how many compromised workstations he possesses around the world. One visit per day would be represented by a 1, and no visits would be represented by a 0. As you might imagine, this technique is usually quite limited in bandwidth.

NOTE

Covert channels are very difficult to detect or prevent.

Phishing, Pharming, and Identity Theft

Identity theft continues to be a problem. In computing, phishing is an attempt to criminally acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity. Phishing is typically carried out by email or instant message (IM), although sometimes phone contact is attempted; the phisher often directs users to enter details at a website, as shown on the left in Figure 1-10. Phishing is an example of social engineering.

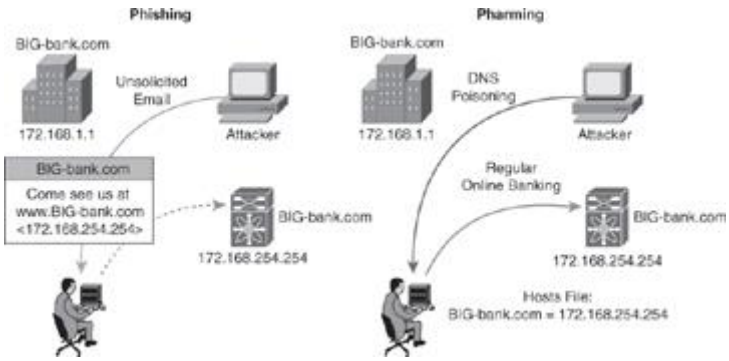

Figure 1-10. Phishing and Pharming Attacks

NOTE

A variation on phishing is spear phishing. In this case, a hacker sends an email that appears genuine to all the employees of an organization and hopes that a few get hooked. As an example, the email could say: "This is Christina, your HR director. The Automatic Payment organization which processes your pay is unable to do so this week. Please email me directly your banking information, and I will ensure that your pay is directly deposited in your bank account for Thursday morning."

Pharming, also illustrated in Figure 1-10, is an attack aimed at redirecting the traffic of a website to another website. Pharming is conducted either by changing the hosts file on a victim computer or by exploiting a vulnerable Domain Name System (DNS) server. Pharming has become a major concern to businesses hosting e-commerce and online banking websites.

NOTE

Antivirus software and spyware-removal software cannot protect against pharming. Additional methods are needed such as server-side software, DNS protection, and web browser protection.

To protect against pharming, organizations implement "personalization" technologies, such as user-chosen images on the login page. Consider also supporting identified email initiatives such as DomainKeys Identified Mail (DKIM); these initiatives are beyond the scope of this book.

Availability Attacks

DoS attacks attempt to compromise the availability of a network, host, or application. They are considered a major risk because they can easily interrupt a business process and cause significant loss. These attacks are relatively simple to conduct, even by an unskilled attacker.

DoS attacks are usually the consequence of one of the following:

- The failure of a host or application to handle an unexpected condition, such as maliciously formatted input data or an unexpected interaction of system components.
- The inability of a network, host, or application to handle an enormous quantity of data, which crashes the system or brings it to a halt. Even if the firewall protects the corporate web server sitting on the DMZ from receiving a large amount of data and thus from crashing, the link connecting the corporation with its service provider will be totally clogged, and this bandwidth starvation will itself be a DoS.

Hackers can use many types of attacks to compromise availability:

- Botnets
- DoS
- DDoS
- SYN floods
- ICMP floods
- Electrical power
- Computer environment

NOTE

Many availability attacks can be used against confidentiality and integrity.

Botnets

Botnet is a term for a collection of software robots, or bots, that run autonomously and automatically. They run on groups of "zombie" computers controlled by crackers.

Although the term *botnet* can be used to refer to any group of bots, it is generally used to refer to a collection of compromised systems running worms, Trojan horses, or back doors, under a common command and control infrastructure. The originator of a botnet controls the group of computers remotely, usually through a means such as Internet Relay Chat (IRC).

Often, the command and control takes place via an IRC server or a specific channel on a public IRC network. A bot typically runs hidden. Generally, the attacker has compromised a large number of systems using various methods, such as exploits, buffer overflows, and so on. Newer bots automatically scan their environment and propagate using detected vulnerabilities and weak passwords. Sometimes a controller will hide an IRC server installation on an educational or corporate site, where high-speed connections can support a large number of other bots.

Several botnets have been found and removed from the Internet. The Dutch police found a 1.5-million node botnet (http://www.wisegeek.com/what-is-a-botnet.htm), and the Norwegian ISP Telenor disbanded a 10,000-node botnet. Large, coordinated international efforts to shut down botnets have also been initiated. Some estimates indicate that up to 25 percent of all personal computers are part of a botnet (http://everything.explained.at/Botnet/).

DoS and DDoS Attacks

DoS attacks are the most publicized form of attack. They are also among the most difficult to eliminate. A DoS attack on a server sends an extremely large volume of requests over a network or the Internet. These large volumes of requests cause the attacked server to slow down dramatically. Consequently, the attacked server becomes unavailable for legitimate access and use.

DoS attacks differ from most other attacks because DoS attacks do not try to gain access to your network or the information on your network. These attacks focus on making a service unavailable for normal use. Attackers typically accomplish this by exhausting some resource limitation on the network or within an operating system or application. These attacks typically require little effort to execute because they either take advantage of protocol weaknesses or use traffic normally allowed into a network. DoS attacks are among the most difficult to completely eliminate because of the way they use protocol weaknesses and accepted traffic to attack a network. Some hackers regard DoS attacks as trivial and in bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

System administrators can install software fixes to limit the damage caused by all known DoS attacks. However, as with viruses, hackers constantly develop new DoS attacks.

A DDoS attack generates much higher levels of flooding traffic by using the combined bandwidth of multiple machines to target a single machine or network. The DDoS attack enlists a network of compromised machines that contain a remotely controlled agent, or zombie, attack program. A master control mechanism provides direction and control. When the zombies receive instructions from the master agent, they each begin generating malicious traffic aimed at the victim.

DDoS attacks are the "next generation" of DoS attacks on the Internet. This type of attack is not new. UDP and TCP SYN flooding, ICMP echo-request floods, and ICMP directed broadcasts (also known as Smurf attacks) are similar to DDoS attacks; however, the scope of the attack is new. Victims of DDoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses, which brings their network connectivity to a grinding halt. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With DDoS tools, an attacker can conduct the same attack using thousands of systems.

Figure 1-11 shows the process of a DDoS attack:

1. The hacker uses a host to scan for systems to hack.
2. After the hacker accesses handler systems, the hacker installs zombie software on them to scan, compromise, and infect agent systems.
3. Remote control attack software is loaded on agent systems.
4. When the hacker issues instructions to handlers on how to carry out the DDoS attack.

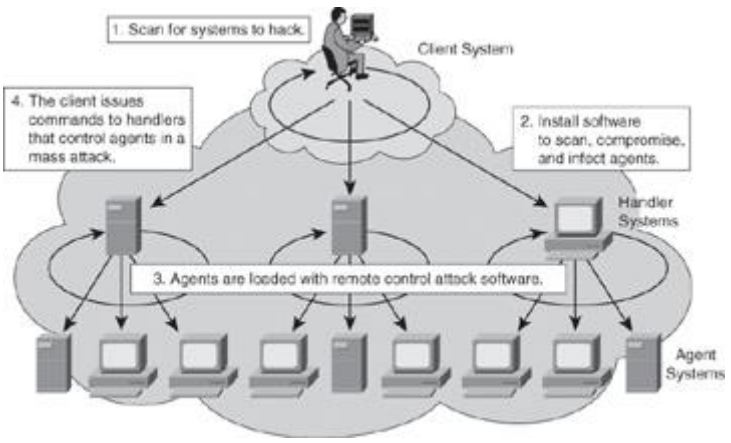

Figure 1-11. DDoS Attack

NOTE

Stacheldracht, which means “barbed-wire” in German, is a well-known tool used to conduct DDoS.

Blended Threats

The actual breach and vulnerability exploit is often accomplished using a combination of malware that infects, propagates, and delivers its payload following different techniques associated with traditional malware. Known as blended threats, these attack mechanisms combine the characteristics of viruses, worms, Trojan horses, spyware, and other malware.

A blended threat will exploit a vulnerability such as a buffer overflow or lack of HTTP input validation. Such attacks can spread without human intervention by scanning for other hosts to infect, embedding code in HTML, or by spamming, to name a few methods.

Blended threats plant Trojans and back doors. They are often part of botnet attacks, which try to raise privilege levels, create network shares, and steal data.

Most blended attacks are considered “zero day,” meaning that they have not been previously identified. Blended attacks are ever-evolving and pretested by cybercriminals on common antivirus products before they are released. These threats easily breach firewalls and open channels, and they represent a challenge to detect and mitigate.

Offline Versus Online Password Cracking

Password cracking techniques can be classified as offline or online. Offline password cracking involves having the hashed result of the original password. At its own pace, the hacker could try hashing different combinations of characters until one of the hash results matches the hash of the original password. Online password cracking involves, as an example, different combinations of password on a live system. It is more difficult to achieve success with this method because most login pages lock after a certain number of unsuccessful login attempts.

Principles of Secure Network Design

In planning an overall strategy for security architecture design, sound principles are needed to accomplish an effective security posture. The selective combination of these principles provides the fundamentals for threat mitigation within the context of a security policy and risk management.

- **Defense in depth:** This is an umbrella term that encompasses many of the other guidelines in this list. It is defined by architectures based on end-to-end security, using a layered approach. The objective is to create security domains and separate them by different types of security controls. The concept also defines redundancy of controls, where the failure of one layer is mitigated by the existence of other layers of controls.
- **Compartmentalization:** Creating security domains is crucial. Different assets with different values should reside in different security domains, be it physically or logically. Granular trust relationships between compartments would mitigate attacks that try to gain a foothold in lower-security domains to exploit high-value assets in higher-security domains.

- **Least privilege:** This principle applies a need-to-know approach to trust relationships between security domains. The idea, which originated in military and intelligence operations, is that if fewer people know about certain information, the risk of unauthorized access is diminished. In network security, this results in restrictive policies, where access to and from a security domain is allowed only for the required users, application, or network traffic. Everything else is denied by default.
- **Weakest link:** This is a fundamental concept—a security system is as effective as its weakest link. A layered approach to security, with weaker or less protected assets residing in separated security domains, mitigates the necessary existence of these weakest links. Humans are often considered to be the weakest link in information security architectures.
- **Separation and rotation of duties:** This is the concept of developing systems where more than one individual is required to complete a certain task. The principle is that this requirement can mitigate fraud and error. This applies to information security controls, and it applies to both technical controls and human procedures to manage those controls.
- **Hierarchically trusted components and protection:** This principle applies a hierarchical approach to the compartmentalization and least privilege ideas, aiming at providing a more structured approach to data classification and security controls. The concept assumes that the hierarchy will be easier to implement and manage, resulting in similarly manageable and compartmentalized security controls.
- **Mediated access:** This principle is based on centralizing security controls to protect groups of assets or security domains. In that sense, firewalls, proxies, and other security controls act on behalf of the assets they are designed to protect, and mediate the trust relationships between security domains. Special considerations should be in place to prevent the mediation component from becoming a single point of failure.
- **Accountability and traceability:** This concept implies the existence of risk and the ability to manage and mitigate it, and not necessarily avoid or remove it. Information security architectures should provide mechanisms to track activity of users, attackers, and even security administrators. They should include provisions for accountability and nonrepudiation. This principle translates into specific functions, such as security audits, event management and monitoring, forensics, and others.

Cisco has always been a proponent of defense in depth. This was made clear in 2000 when it released its Cisco SAFE Blueprint for enterprise (SAFE is not an acronym), where it laid out its vision for defense in depth.

Defense in Depth

Addressing the fact that a security system is only as strong as its weakest link is often difficult when designing a system’s security. The complexity of modern systems makes it hard to identify each individual weak link, let alone the weakest one. Thus, it is often most desirable to eliminate possible weaknesses by instituting several concurrent security methods.

Securing information and systems against all threats requires multiple, overlapping protection approaches that address the human, technological, and operational aspects of information technology. Using multiple, overlapping protection approaches ensures that the system is never unprotected from the failure or circumvention of any individual protection approach.

When a system is designed and implemented, its quality should always be questioned through design reviews and testing. Identification of various failure modes might help a designer evaluate

the probability of element failure, and identify the links that are the most critical for the security of the whole system. Many systems have a security-based single point of failure, an element of functionality or protection that, if compromised, would cause the compromise of the whole system. It is desirable to eliminate or at least harden such single points of failure in a high-assurance system.

Defense in depth is a philosophy that provides layered security to a system by using multiple security mechanisms:

- Security mechanisms should back each other up and provide diversity and redundancy of protection.
- Security mechanisms should not depend on each other, so that their security does not depend on other factors outside their control.
- Using defense in depth, you can eliminate single points of failure and augment weak links in the system to provide stronger protection with multiple layers.

The defense-in-depth strategy recommends several principles:

- **Defend in multiple places**: Given that insiders or outsiders can attack a target from multiple points, an organization must deploy protection mechanisms at multiple locations to resist all classes of attacks. At a minimum, you should include three defensive focus areas:
    - **Defend the networks and infrastructure:** Protect the local- and wide-area communications networks from attacks, such as DoS attacks. Provide confidentiality and integrity protection for data that is transmitted over the networks; for example, use encryption and traffic flow security measures to resist passive monitoring.
    - **Defend the enclave boundaries:** Deploy firewalls and intrusion detection systems (IDS) or intrusion prevention systems (IPS) or both to resist active network attacks.
    - **Defend the computing environment:** Provide access controls and host intrusion prevention systems (HIPS) on hosts and servers to resist insider, close-in, and distribution attacks.
- **Build layered defenses:** Even the best available information assurance products have inherent weaknesses. Therefore, it is only a matter of time before an adversary finds an exploitable vulnerability. An effective countermeasure is to deploy multiple defense mechanisms between the adversary and the target. Each of these mechanisms must present unique obstacles to the adversary. Further, each mechanism should include both protection and detection measures. These measures increase the risk of detection for adversaries while reducing their chances of success, or make successful penetrations unaffordable. One example of a layered defense is to have nested firewalls (each coupled with IDS or IPS) that are deployed at outer and inner network boundaries. The inner firewalls may support more granular access control and data filtering.
- **Use robust components:** Specify the security robustness (that is, strength and assurance) of each information assurance component as a function of the value of what it is protecting and the threat at the point of application. For example, it is often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop.
- **Employ robust key management:** Deploy robust encryption key management and public key infrastructures that support all the incorporated information assurance technologies and that are highly resistant to attack.

- **Deploy an IDS or IPS:** Deploy infrastructures to detect and prevent intrusions and to analyze and correlate the results and react accordingly. These infrastructures should help the operations staff answer the following questions:
    - Am I under attack?
    - Who is the source?
    - What is the target?
    - Who else is under attack?
    - What are my options?

Evaluating and Managing the Risk

The security policy developed in your organization drives all the steps taken to secure network resources. The development of a comprehensive security policy prepares you for the rest of your security implementation. To create an effective security policy, it is necessary to do a risk analysis, which will be used to maximize the effectiveness of the policy and procedures that will be put in place. Also, it is essential that everyone be aware of the policy; otherwise, it is doomed to fail.

All design guidelines and principles, and the resulting security architecture, should be aimed at managing risk. Risk is, or should be, the building block of information security.

Levels of Risks

By its very nature, risk management is a tradeoff between the effort (cost) to protect organizational assets and the resulting level of exposure of those assets. This simple rule is a good starting point: the cost to protect an asset will likely not be greater than the value of the asset itself. There are obviously exceptions to the rule; for instance, cases that involve national security, or instances where the value of the asset is incalculable, such as cases where human life is involved.

The tradeoffs in risk management are based on its building blocks: assets and vulnerabilities, threats and countermeasures. Different values and scenarios for these components move the risk indicators up and down. Understanding these values and scenarios is critical in defining a risk management strategy.

For instance, would you use old, worn tires at high speed on a highway? The answer is obviously no. The asset that you are trying to protect (your life) is too valuable, and the countermeasure to mitigate the risk of navigating the highway, driving at a slow speed, is not good enough. It is inexpensive but not effective.

However, using a worn-down tire as a swing does not result in life-threatening risk in the majority of situations. The asset (your life) remains the same, but the threats that are able to exploit the vulnerabilities of the tire are mitigated or nonexistent. The premise changes again if you think that this worn-down tire will be used to swing your child. You may or may not risk using the old tire, but the value of the asset may prevent you from facing risk even if it is minimal.

The previous example is a simplistic view of information security risk. Imagine an organizational risk management effort, considering thousands of assets with different (and often subjective) valuation criteria, different (and often unknown) levels of vulnerability, and potentially exposed to an avalanche of threats that change by the minute. Risk management

becomes a delicate balance and involves constant tuning of countermeasures in the face of sophisticated threat vectors, exploiting assets that are often located outside of corporate control.

Information security risk management is a comprehensive process that requires organizations to frame risk (in other words, establish the context for risk-based decisions), assess risk, respond to risk, and monitor risk on an ongoing basis. The result is a dynamic process in nature, evolving along with internal factors (assets, vulnerabilities, security policies, and architectures) and external factors (threats, and business, legal, and compliance forces).

Other sections in this chapter will expand on these concepts and present commonly used risk management strategies, within the context of a security policy and a security lifecycle process.

Risk Analysis and Management

Every process of security should first address the following questions:

- Which are the threats the system is facing?
- Which are the probable threats and what would be their consequence, if exploited?

The threat-identification process provides an organization with a list of threats to which a system is subject in a particular environment.

NOTE

An interesting method of modeling security threats is the attack trees method developed by Bruce Schneier. You can find more information about this method at http://en.wikipedia.org/wiki/Attack_tree.

Risk Analysis

Risk analysis is the systematic study of uncertainties and risks. Risk analysts seek to identify the risks that a company faces, understand how and when they arise, and estimate the impact (financial or otherwise) of adverse outcomes. Risk managers start with risk analysis, and then seek to take actions that will mitigate these risks. Risk analysis tries to estimate the probability and severity of threats faced by an organization's system that needs protection, and then provides to the organization a prioritized list of risks that the organization must mitigate. This allows the organization to focus on the most important threats first.

Two types of risk analysis are of interest in information security:

- **Quantitative:** Quantitative risk analysis uses a mathematical model that assigns monetary values to assets, the cost of threats being realized, and so on. Quantitative risk analysis provides an actual monetary figure of expected losses, which is typically based on an annual cost. You can then use this number to justify proposed countermeasures. For example, if you can establish that you will lose $1,000,000 by doing nothing, you can justify spending $300,000 to reduce that risk by 50 percent to 75 percent.
- **Qualitative:** Qualitative risk analysis uses a scenario model. This approach is best for large cities, states, and countries to use because it is impractical for such entities to try to list all their assets, which is the starting point for any quantitative risk analysis. By the time a typical national government could list all of its assets, the list would have hundreds or thousands of changes and would no longer be accurate.

Qualitative risk analysis is straightforward provided you have the resources to document all the assets. However, quantitative risk analysis is more tricky, so we will take a closer look at it.

Quantitative Risk Analysis Formula

Quantitative risk analysis relies on specific formulas to determine the value of the risk decision variables. These include formulas that calculate the asset value (AV), exposure factor (EF), single loss expectancy (SLE), annualized rate of occurrence (ARO), and annualized loss expectancy (ALE). The ALE formula is as follows: ALE = (AV * EF) *ARO.

The AV is the value of an asset. This would include the purchase price, the cost of deployment, and the cost of maintenance. In the case of a database or a web server, the AV should also include the cost of development. AV is not an easy number to calculate.

The EF is an estimate of the degree of destruction that will occur. For example, suppose that you consider flood a threat. Could it destroy your data center? Would the destruction be 60 percent, 80 percent, or 100 percent? The risk-assessment team would have to make a determination that evaluates everything possible, and then make a judgment call. For this example, assume that a flood will have a 60 percent destruction factor, because you store a backup copy of all media and data offsite. Your only losses would be the hardware and productivity.

As another example of EF, consider data entry errors, which are much less damaging than a flood. A single data entry error would hardly be more than a fraction of a percent in exposure. The exposure factor of a data entry error might be as small as .001 percent.

CAUTION

One of the ironies of risk analysis is how much estimating (guessing) is involved.

The SLE calculation is a number that represents the expected loss from a single occurrence of the threat. The SLE is defined as AV * EF.

To use our previous examples, you would come up with the following results for the SLE calculations:

- Flood threat
    - Exposure factor: 60 percent
    - AV of the enterprise: US$10,000,000
    - $10,000,000 * .60 = $6,000,000
- Data entry error
    - Exposure factor: .001 percent
    - AV of data and databases: $1,000,000
    - $1,000,000 * .000001 = $10 SLE

The ARO is a value that estimates the frequency of an event and is used to calculate the ALE.

Continuing the preceding example, the type of flood that you expect could reach your data center would be a “flood of the century” type of event. Therefore, you give it a 1/100 chance of occurring this year, making the ARO for the flood 1/100.

Furthermore, you expect the data entry error to occur 500 times a day. Because the organization is open for business 250 days per year, you estimate the ARO for the data entry error to be 500 * 250, or 125,000 times.

Risk analysts calculate the ALE in annualized terms to address the cost to the organization if the organization does nothing to counter existing threats. The ALE is derived from multiplying the SLE by the ARO. The following ALE calculations continue with the two previous examples:

- Flood threat
    - SLE: $6,000,000
    - ARO: .01
    - $6,000,000 * .01 = $60,000 ALE
- Data input error
    - SLE: $10
    - ARO: 125,000
    - $10 * 125,000 = $1,250,000 ALE

A decision to spend $50,000 to enhance the security of our database applications to reduce data entry errors by 90 percent is now an easy decision. It is equally easy to reject a proposal to enhance our defenses against floods that costs $3,000,000.

When you perform a quantitative risk analysis, you identify clear costs as long as the existing conditions remain the same. You compile a list of expected issues, the relative cost of those events, and the total cost if all expected threats are realized. These numbers are put into annual terms to coincide with the annual budgets of most organizations.

You then use these numbers in decision making. If an organization has a list of 10 expected threats, it can then prioritize the threats and address the most serious threats first. This prioritization enables management to focus their resources where it will do the most good.

For example, suppose an organization has the following list of threats and costs as the product of performing a quantitative risk analysis:

- **Insider network abuse:** $1,000,000 in lost productivity
- **Data input error:** $500,000
- **Worm outbreak:** $100,000
- **Viruses:** $10,000
- **Laptop theft:** $10,000

Decision makers could easily decide that it is of greatest benefit to address insider network abuse and leave the antivirus solution alone. They could also find it easy to support a $200,000 URL filtering solution to address insider network abuse and reject a $40,000 solution designed to enhance laptop safety. Without these numbers from a risk analysis, the decisions made would likely differ.

Building Blocks of Risk Analysis

Conducting a risk analysis starts with the gathering of pertinent information. The building blocks of the process follow the definition of risk used in this book: the organizational impact of threat vectors exploiting vulnerabilities of the assets you are trying to protect.

In that sense, the initial information gathering, in preparation for the risk calculations described in the previous example, should collect and define the following:

- **Assets and their value:** This information, shown in Table 1-1, is typically obtained from data classification, inventories of assets, and other sources. A general principle is to use discrete numerical values for the exposure factor (EF) based on discrete values that reflect the impact of losing the asset. These values are generally based on data classification techniques (confidential, secret, top secret, and so on), and the impact is based on organizationally relevant criteria (replacement cost, liability, and so on).

  Table 1-1. List of Assets and Their Value

	Confidentiality	Integrity	Availability
Low Value	Limited effect	Limited effect	Limited effect
Moderate Value	Serious effect	Serious effect	Serious effect
High Value	Severe effect	Severed effect	Severe effect

- **Vulnerabilities:** This information is typically gathered from vulnerability assessments, which will be discussed further later in this chapter. Several tools are available, like Nessus and other commercial vulnerability assessment products. The use of public- or platform-specific vulnerability classification databases is commonplace. They include the Common Vulnerabilities and Exposures (CVE) effort by MITRE, http://cve.mitre.org, and the National Vulnerability Database (NVD) sponsored by the National Institute of Standards and Technology (NIST), http://nvd.nist.gov. An example of vulnerability categorization is shown in Table 1-2.

  Table 1-2. Example of Vulnerability Categorization Headings

  Categorization Procedures Processes Systems Network

- **Threats, their impact, and rate or probability of occurrence:** This information is commonly obtained from publicly available databases, such as the MITRE Common Attack Pattern Enumeration and Classification (CAPEC), http://capec.mitre.org. Calculating the rate of occurrence is a probabilistic exercise and is often considered subjective and specific for individual organizations or industries. Table 1-3 shows an example of this information gathering.

  Table 1-3. Example of Threats, Impact, and Probability of Occurrence

Impact Category	Critical	Serious	Moderate	Minor	Negligible
Definition	Inability to achieve minimum requirements	Major cost and schedule increases	Moderate cost and schedule increases	Small cost and schedule increases	No effect

Risk Scores

With asset, vulnerability, and threat components defined, risk scores are obtained by applying formulas of quantitative risk analysis. Figure 1-12 illustrates the process.

Figure 1-12. Obtaining a Risk Score

A risk matrix is then calculated, including risk scores for assets and groups of assets and, ideally, an organization risk score that can be used in security monitoring, incident response, and policy reviews. These risk scores provide an idea of the landscape of assets, threats, vulnerabilities, and countermeasures, the components of risk, at a given point in time.

A Lifecycle Approach to Risk Management

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization, including the following:

- Senior leaders and executives who provide the strategic vision and top-level goals and objectives for the organization
- Midlevel leaders who plan, execute, and manage projects
- Individuals who operate the information systems supporting the organization's mission and business functions

Figure 1-13 shows that risk management is a comprehensive process that requires organizations to do the following:

- Frame risk (that is, establish the context for risk-based decisions)
- Assess risk
- Respond to risk once determined
- Monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations

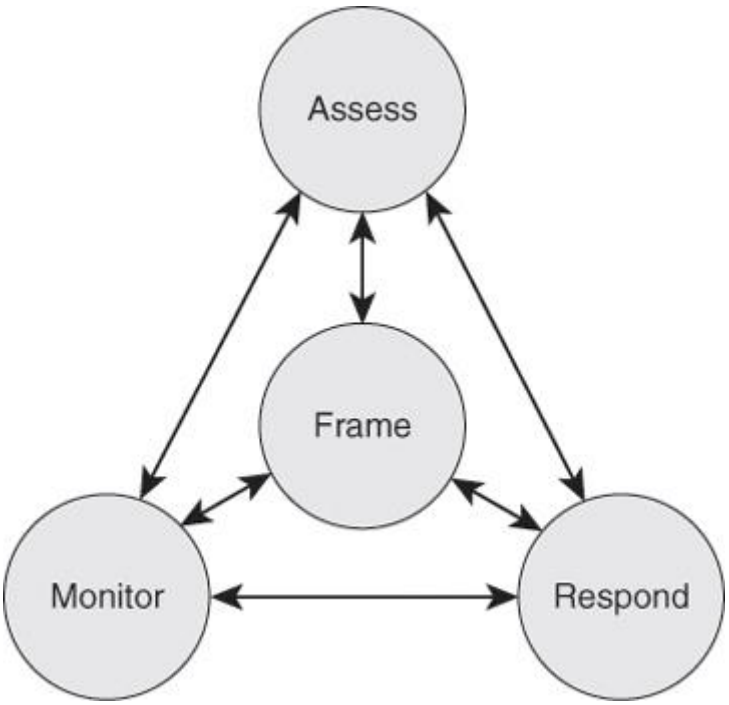

Figure 1-13. Lifecycle Approach to Risk Management According to NIST 800-39

Source: NIST 800-39, 2011

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level. Approaching risk management in this way ensures that risk-based decision making is integrated into every aspect of the organization.

Regulatory Compliance

Compliance regulations have been a major driver for security in organizations of all kinds, and the following trends have emerged over the past decade:

- Strengthened enforcement
- Global spread of data breach notification laws
- More prescriptive regulations
- Growing requirements regarding third parties (business partners)
- Risk-based compliance on the rise
- Compliance process streamlined and automated

The compliance regulation defines not only the scope and parameters for the risk and security architectures of an organization, but also the liability for those who do not comply. Recently there have been major shifts in the compliance landscape:

- Although enforcement of existing regulations has been weak in many jurisdictions worldwide, regulators and standards bodies are now tightening enforcement through expanded powers, higher penalties, and harsh enforcement actions.
- In the future, it will be more difficult to hide information security failings wherever organizations do business. Legislators are forcing transparency through the introduction of breach notification laws in Europe, Asia, and North America as data breach disclosure becomes a global principle.

- As more regulations are introduced, there is a trend toward increasingly prescriptive rules. For example, laws in the states of Massachusetts and Nevada, which went into effect in 2010, apply not only to companies based in these states but also to all external organizations that manage the personal information of these states' residents.
- Regulators are also making it clear that enterprises are responsible for ensuring the protection of their data when it is being processed by a business partner, including cloud service providers.
- For many organizations, stricter compliance could help focus management attention on security; but if they take a "check-list approach" to compliance, it will detract from actually managing risk and may not improve security.
- The new compliance landscape will increase costs and risks. For example, it takes time and resources to substantiate compliance. Increased requirements for service providers give rise to more third-party risks.
- With more transparency, there are now greater consequences for data breaches. For example, expect to see more litigation as customers and business partners seek compensation for compromised data. But the harshest judgments will likely come from the court of public opinion—with the potential to permanently damage the reputation of an enterprise.

Table 1-4 illustrates some examples of relevant compliance regulations (most of which were introduced earlier in the chapter) that affect organizations all over the world. Geographic boundaries are blurring as globalization makes organizations subject to regulations in several countries. Industry scope boundaries are also blurring. For instance, many service organizations providing services to the U.S. government have to comply with U.S. federal regulations related to information security.

Table 1-4. Examples of Compliance Regulations

Regulation	Geographic Scope	Applies To
EU Data Protection Directive (EU 95/46/EC)	European Union	All organizations operating in the 27 EU member countries
Sarbanes-Oxley	United States	All publicly traded companies in the U.S. (exemption for smaller reporting companies)
PIPEDA	Canada	All organizations in Canada
PCI DSS	Global	All organizations processing credit card data
HIPAA	United States	All healthcare organizations in the U.S.
FISMA	United States	Federal agencies and service organizations
Basel II	Global	All internationally active banks with assets of $250 billion or more
DMCA	United States	Individuals and organizations in the U.S.
NERC	North America	North America users, owners, and operators of the bulk electric power system
GLBA	United States	All financial institutions in the U.S.
Safe Harbor Act	European Union	U.S. companies doing business in the EU

The following are descriptions of some of the regulations listed in Table 1-4:

- The Gramm-Leach-Bliley Act (GLBA) of 1999 erased long-standing antitrust laws that prohibited banks, insurance companies, and securities firms from merging and sharing information with one another. The idea was that smaller firms would then be able to pursue acquisitions or alliances, or both, that would help encourage competition against many of the larger financial institutions. Included in the GLBA were several consumer privacy protections. Namely, companies must tell their customers what kinds of data they plan to share and with whom, and they must give their customers a chance to opt out of that data sharing.
- On the healthcare side, the Health Insurance Portability and Accountability Act (HIPAA) of 2000 requires the U.S. Department of Health and Human Services to develop a set of national standards for healthcare transactions. These standards provide assurance that the electronic transfer of confidential patient information will be as safe as, or safer than, paper-based patient records.
- The Sarbanes-Oxley (SOX) Act of 2002 is a U.S. law that was created in response to a number of major corporate and accounting scandals, including those affecting Enron, Tyco International, Peregrine Systems, and WorldCom. These scandals resulted in a decline of public trust in accounting and reporting practices.
- The Federal Information Security Management Act (FISMA) of 2002 was intended to bolster computer and network security within the U.S. government and affiliated parties by requiring yearly audits. FISMA also brought attention within the U.S. government to cyber security, which the U.S. government had largely neglected previously.

Globalization, as with any other context, is changing the face of regulatory compliance. Regulators are not just looking at ways to strengthen existing laws. Regulators are also introducing new laws that are aimed at forcing more transparency, in a way that affects organizations on a global basis.

Data breach disclosure is becoming a global principle as jurisdictions worldwide adopt privacy and data protection laws that include a general obligation to notify government agencies, individuals, and other authorities such as law enforcement of unauthorized access or use of personal data. Requirements vary, including who must be notified, the type of data that triggers notification, and if there is a risk-of-harm threshold.

California's landmark legislation SB-1386 set off a wave of state breach notification laws that now cover almost the entire United States. Recently, this trend has spread to the European Union. The Privacy and Electronic Communications Directive (e-Privacy Directive) was amended in late 2009 to include data breach notification. It is now mandatory for telephone companies and ISPs in the EU to inform national regulatory authorities of any data security breach. Depending on the effects of the breach, they may also be required to inform subscribers. The upcoming overhaul of the EU Data Protection Directive is expected to include data breach notification requirements, which would broaden breach disclosure to cover all industries in all 27 member countries in the EU.

Table 1-5 shows how regulations are becoming the norm around the world.

Table 1-5. Acceleration of Compliance Regulation Around the World

Year	Country	Data Breach Notification Law
2003	U.S.	California's landmark SB-1386 starts wave of state laws.
2003–2010	U.S	46 states enact notification laws.
2008	U.K.	Information Commissioner's Office issues best practice guidance requiring notification.
2009	EU	e-Privacy Directive amended to include notification requirements for electronic communications sector.
	Germany	National privacy law amended to include notification.
2010	Austria	National privacy law amended to include notification.
	France	Draft legislation passed in senate would make notification mandatory.
	Canada	National privacy law amended to include notification.
	Mexico	New privacy law enacted that includes notification.
	Ireland	Code of Practice issued regarding notification.
	Hong Kong	Privacy Commissioner issues guidance note on breach notification.
	EU	Data Protection Directive under review for revision; proposed law expected by 2011 to include notification requirements for all industries; to be implemented in all 27 EU member countries.

Security Policies

Every organization has something that someone else wants. Someone might want that something for himself, or he might want the satisfaction of denying something to its rightful owner. Your assets are what need the protection of a security policy.

Determine what your assets are by asking (and answering) the following questions:

- What do you have that others want?
- What processes, data, or information systems are critical to you, your company, or your organization?
- What would stop your company or organization from doing business or fulfilling its mission?

The answers identify assets in a wide range, including critical databases, vital applications, vital company customer and employee information, classified commercial information, shared drives, email servers, and web servers.

A security policy comprises a set of objectives for the company, rules of behavior for users and administrators, and requirements for system and management that collectively ensure the security of network and computer systems in an organization. A security policy is a "living

document," meaning that the document is never finished and is continuously updated as technology and employee requirements change.

The security policy translates, clarifies, and communicates the management position on security as defined in high-level security principles. The security policy acts as a bridge between these management objectives and specific security requirements. It informs users, staff, and managers of their obligatory requirements for protecting technology and information assets. It should specify the mechanisms that you need to meet these requirements. It also provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the security policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.

The three reasons for having a security policy are as follows:

- To inform users, staff, and managers
- To specify mechanisms for security
- To provide a baseline

One of the most common security policy components is an acceptable use policy (AUP). This component defines what users are allowed and not allowed to do on the various components of the system, including the type of traffic that is allowed on the networks. The AUP should be as explicit as possible to avoid ambiguity or misunderstanding. For example, an AUP might list the prohibited website categories.

NOTE

Some sites refer to an acceptable use policy as an *appropriate use policy*.

A properly defined security policy does the following:

- Protects people and information
- Sets the rules for expected behavior
- Authorizes staff to monitor, probe, and investigate
- Defines the consequences of violations

The audience for the security policy is anyone who might have access to your network, including employees, contractors, suppliers, and customers. However, the security policy should treat each of these groups differently.

The audience determines the content of the policy. For example, you probably do not need to include a description of *why* something is necessary in a policy that is intended for the technical staff. You can assume that the technical staff already knows why a particular requirement is included. Managers are also not likely to be interested in the technical aspects of why a particular

requirement is needed. However, they might want the high-level overview or the principles supporting the requirement. When end users know why a particular security control has been included, they are more likely to comply with the policy.

In the policy, users can be organized into two audiences:

- Internal audience
  - Managers and executives
  - Departments and business units
  - Technical staff
  - End users
- External audience
  - Partners
  - Customers
  - Suppliers
  - Consultants and contractors

One document will not likely meet the needs of the entire audience of a large organization. The goal is to ensure that the information security policy documents are coherent with its audience needs.

Security Policy Components

Figure 1-14 shows the hierarchy of a corporate policy structure that is aimed at effectively meeting the needs of all audiences.

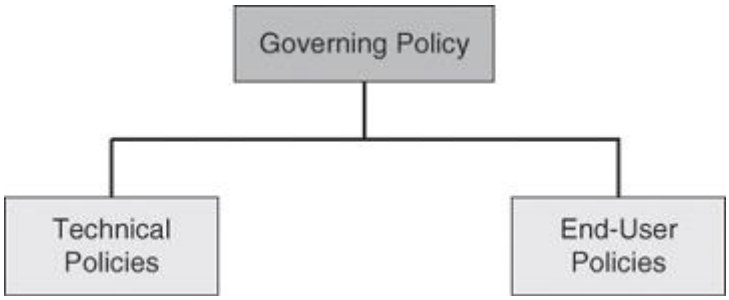

Figure 1-14. Components of a Comprehensive Security Policy

Most corporations should use a suite of policy documents to meet their wide and varied needs:

- **Governing policy:** This policy is a high-level treatment of security concepts that are important to the company. Managers and technical custodians are the intended audience. The governing policy controls all security-related interaction among business units and supporting departments in the company. In terms of detail, the governing policy answers the "what" security policy questions.
- **End-user policies:** This document covers all security topics important to end users. In terms of detail level, end-user policies answer the "what," "who," "when," and "where" security policy questions at an appropriate level of detail for an end user.
- **Technical policies:** Security staff members use technical policies as they carry out their security responsibilities for the system. These policies are more detailed than the governing policy and are system or issue specific (for example, access control or physical security issues). In terms of detail, technical policies answer the "what," "who," "when," and "where" security policy questions. The "why" is left to the owner of the information.

NOTE

To assist you at drafting your security policies, consider the SANS security policies repository at http://www.sans.org/resources/policies.

For readers interested in security policies for academic institutions, visit the University of Toronto's Computer Security Administration website for a comprehensive example of a network security policy for a higher education institution: http://www.cns.utoronto.ca/newsite/documentation/policies/policy_5.htm

Governing Policy

The governing policy outlines the security concepts that are important to the company for managers and technical custodians:

- It controls all security-related interactions among business units and supporting departments in the company.
- It aligns closely with not only existing company policies, especially human resource policies, but also any other policy that mentions security-related issues, such as issues concerning email, computer use, or related IT subjects.
- It is placed at the same level as all companywide policies.
- It supports the technical and end-user policies.
- It includes the following key components:
    - A statement of the issue that the policy addresses
    - A statement about your position as IT manager on the policy
    - How the policy applies in the environment
    - The roles and responsibilities of those affected by the policy
    - What level of compliance to the policy is necessary
    - Which actions, activities, and processes are allowed and which are not
    - What the consequences of noncompliance are

End-User Policies

End-user policies are compiled into a single policy document that covers all the topics pertaining to information security that end users should know about, comply with, and implement. This policy may overlap with the technical policies and is at the same level as a technical policy. Grouping all the end-user policies together means that users have to go to only one place and read one document to learn everything that they need to do to ensure compliance with the company security policy.

Technical Policies

Security staff members use the technical policies in the conduct of their daily security responsibilities. These policies are more detailed than the governing policy and are system or issue specific (for example, router security issues or physical security issues). These policies are essentially security handbooks that describe what the security staff does, but not how the security staff performs its functions.

The following are typical policy categories for technical policies:

- General policies
  - **Acceptable use policy (AUP):** Defines the acceptable use of equipment and computing services, and the appropriate security measures that employees should take to protect the corporate resources and proprietary information.
  - **Account access request policy:** Formalizes the account and access request process within the organization. Users and system administrators who bypass the standard processes for account and access requests may cause legal action against the organization.
  - **Acquisition assessment policy:** Defines the responsibilities regarding corporate acquisitions and defines the minimum requirements that the information security group must complete for an acquisition assessment.
  - **Audit policy:** Use to conduct audits and risk assessments to ensure integrity of information and resources, investigate incidents, ensure conformance to security policies, or monitor user and system activity where appropriate.
  - **Information sensitivity policy:** Defines the requirements for classifying and securing information in a manner appropriate to its sensitivity level.
  - **Password policy:** Defines the standards for creating, protecting, and changing strong passwords.
  - **Risk-assessment policy:** Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the information infrastructure that is associated with conducting business.
  - **Global web server policy:** Defines the standards that are required by all web hosts.
- Email policies
  - **Automatically forwarded email policy:** Documents the policy restricting automatic email forwarding to an external destination without prior approval from the appropriate manager or director.
  - **Email policy:** Defines the standards to prevent tarnishing the public image of the organization.
  - **Spam policy:** The AUP covers spam.
- Remote-access policies
  - **Dial-in access policy:** Defines the appropriate dial-in access and its use by authorized personnel.
  - **Remote-access policy:** Defines the standards for connecting to the organization network from any host or network external to the organization.
  - **VPN security policy:** Defines the requirements for remote-access IP Security (IPsec) or Layer 2 Tunneling Protocol (L2TP) VPN connections to the organization network.
- Personal device and phone policies
  - **Analog and ISDN line policy:** Defines the standards to use analog and ISDN lines for sending and receiving faxes and for connection to computers.
  - **Personal communication device policy:** Defines the information security's requirements for personal communication devices, such as voicemail, smartphones, tablets, and so on.
- Application policies
  - **Acceptable encryption policy:** Defines the requirements for encryption algorithms that are used within the organization.
  - **Application service provider (ASP) policy:** Defines the minimum security criteria that an ASP must execute before the organization uses the ASP's services on a project.

    - **Database credentials coding policy:** Defines the requirements for securely storing and retrieving database usernames and passwords.
    - **Interprocess communications policy:** Defines the security requirements that any two or more processes must meet when they communicate with each other using a network socket or operating system socket.
    - **Project security policy:** Defines requirements for project managers to review all projects for possible security requirements.
    - **Source code protection policy:** Establishes minimum information security requirements for managing product source code.
- Network policies
    - **Extranet policy:** Defines the requirement that third-party organizations that need access to the organization networks must sign a third-party connection agreement.
    - **Minimum requirements for network access policy:** Defines the standards and requirements for any device that requires connectivity to the internal network.
    - **Network access standards:** Defines the standards for secure physical port access for all wired and wireless network data ports.
    - **Router and switch security policy:** Defines the minimal security configuration standards for routers and switches inside a company production network or used in a production capacity.
    - **Server security policy:** Defines the minimal security configuration standards for servers inside a company production network or used in a production capacity.
- **Wireless communication policy:** Defines standards for wireless systems that are used to connect to the organization networks.
- **Document retention policy:** Defines the minimal systematic review, retention, and destruction of documents received or created during the course of business. The categories of retention policy are, among others:
    - **Electronic communication retention policy:** Defines standards for the retention of email and instant messaging.
    - **Financial retention policy:** Defines standards for the retention of bank statements, annual reports, pay records, accounts payable and receivable, and so on.
    - **Employee records retention policy:** Defines standards for the retention of employee personal records.
    - **Operation records retention policy:** Defines standards for the retention of past inventories information, training manuals, suppliers lists, and so forth.

Standards, Guidelines, and Procedures

Security policies establish a framework within which to work, but they are too general to be of much use to individuals responsible for implementing these policies. Because of this, other, more-detailed documents exist. Among the more important of these detailed documents are the standards, guidelines, and procedures documents.

Whereas policy documents are very much high-level overview documents, the standards, guidelines, and procedures documents are documents that the security staff will use regularly to implement the security policies.

Standards

Standards enable an IT staff to be consistent. They specify the use of specific technologies so that IT staff members can narrow the focus of their expertise to those technologies instead of trying to know everything about all sorts of technologies. Standards also try to provide consistency in the network, because supporting multiple versions of hardware and software is unreasonable unless it is necessary. The most successful IT organizations have standards to improve efficiency and to keep things as simple as possible.

Standardization also applies to security. One of the most important security principles is consistency. If you support 100 routers, it is important that you configure all 100 routers as similarly as possible. If you do not do this, it is difficult to maintain security. When you do not strive for the simplest of solutions, you usually fail in being secure.

Guidelines

Guidelines help provide a list of suggestions on how you can do things better. Guidelines are similar to standards, but are more flexible and are not usually mandatory. You will find some of the best guidelines available in repositories known as "best practices." The following is a list of widely available guidelines:

- National Institute of Standards and Technology (NIST) Computer Security Resource Center; http://csrc.nist.gov/
- National Security Agency (NSA) Security Configuration Guides; http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml
- The Common Criteria for Information Technology Security Evaluation; http://www.commoncriteriaportal.org/
- Defense Information Systems Agency (DISA) Field Security Operations Office – Security Technical Information Guides (STIG); http://iase.disa.mil/stigs/

NOTE

Note that the Rainbow Series from NIST was historically a reliable source for InfoSec guidelines but is now outdated.

Procedures

Procedure documents are longer and more detailed than the standards and guidelines documents. Procedure documents include the details of implementation, usually with step-by-step instructions and graphics. Procedure documents are extremely important for large organizations to enable them to have the consistency of deployment that is necessary to have a secure environment. Inconsistency is the enemy of security.

Table 1-6 provides a comparative chart for standards, guidelines, and procedures, which accompany security policies.

Table 1-6. Comparison Between Standards, Guidelines, Procedures

	Characteristics
Standards	Specify the use of specific technologies in a uniform way
	Improve efficiency
	Are usually mandatory
	Accomplish consistency and uniformity
Guidelines	Are similar to standards, but more flexible and not usually mandatory
	Can be used to define how standards should be developed or to guarantee adherence to general security policies
	Include NIST Computer Security Resource Center, NSA Security Configuration Guides, Common Criteria, and others
Procedures	Are usually required
	Are the lowest level of the policy chain
	Provide detailed steps used to perform specific tasks
	Provide the steps required to implement the policies, standards, and guidelines
	Are also known as practices

Security Policy Roles and Responsibilities

In any organization, it is senior management, such as the CEO, that is always ultimately responsible for everything. Typically, senior management only oversees the development of a security policy. The creation and maintenance of a security policy is usually delegated to the people in charge of IT or security operations.

Sometimes the senior security or IT management personnel, such as the chief security officer (CSO), the chief information officer (CIO), or the chief information security officer (CISO), will have the expertise to create the policy, sometimes they will delegate it, and sometimes it will be a bit of both strategies. But the senior security person is always intimately involved in the development and maintenance of security policy. Guidelines can provide a framework for policy decision making.

Senior security staff is often consulted for input on a proposed policy project. They might even be responsible for the development and maintenance of portions of the policy. It is more likely that senior staff will be responsible for the development of standards and procedures.

Everyone else who is involved in the security policy has the duty to abide by it. Many policy statements will include language that refers to a potential loss of employment for violation of the policy. IT staff and end users alike are responsible to know the policy and follow it.

Security Awareness

Technical, administrative, and physical controls can all be defeated without the participation of the end-user community. To get accountants, administrative assistants, and other end users to think about information security, you must regularly remind them about security. The technical staff also needs regular reminders because their jobs tend to emphasize performance, such as introducing new technologies, increasing throughput, and the like, rather than secure performance, such as how many attacks they repelled. Therefore, leadership must develop a nonintrusive program that keeps everyone aware of security and how to work together to maintain the security of their data. The three key components used to implement this type of program are awareness, training, and education.

An effective computer security-awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security-awareness and training program should encompass the following seven steps:

- **Step 1. Identify program scope, goals, and objectives.**

  The scope of the program should provide training to all types of people who interact with IT systems. Because users need training that relates directly to their use of particular systems, you need to supplement a large, organization-wide program with more system-specific programs.

- **Step 2. Identify training staff.**

  It is important that trainers have sufficient knowledge of computer security issues, principles, and techniques. It is also vital that they know how to communicate information and ideas effectively.

- **Step 3. Identify target audiences.**

  Not everyone needs the same degree or type of computer security information to do his or her job. A computer security-awareness and training program that distinguishes between groups of people, presents only the information that is needed by the particular audience, and omits irrelevant information will have the best results.

- **Step 4. Motivate management and employees.**

  To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consider using motivational techniques to show management and employees how their participation in a computer security and awareness program will benefit the organization.

- **Step 5. Administer the program.**

  Several important considerations for administering the program include visibility, selection of appropriate training methods, topics, and materials, and presentation techniques.

- **Step 6. Maintain the program.**

You should make an effort to keep abreast of changes in computer technology and security requirements. A training program that meets the needs of an organization today may become ineffective when the organization starts to use a new application or changes its environment, such as by connecting to the Internet.

- **Step 7. Evaluate the program.**

  An evaluation should attempt to ascertain how much information is retained, to what extent computer security procedures are being followed, and the general attitudes toward computer security.

A successful IT security program consists of the following:

1. Developing IT security policy that reflects business needs tempered by known risks.
2. Informing users of their IT security responsibilities, as documented in agency security policy and procedures.
3. Establishing processes for monitoring and reviewing the program.

You should focus security awareness and training on the entire user population of the organization. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that you can deploy and implement in various ways and be aimed at all levels of the organization, including senior and executive managers. The effectiveness of this effort usually determines the effectiveness of the awareness and training program and how successful the IT security program will be.

Secure Network Lifecycle Management

The lifecycle approach looks at the different phases of security, such as assessment, testing, implementation, monitoring and so forth, to provide methodology in securing our networks. The roles of risk, regulatory compliance, and security policies in designing and building effective security architectures have been described. How are these three components related?

IT Governance, Risk Management, and Compliance

Organizational efforts for IT governance, risk management, and compliance (sometimes known as IT GRC) are often separated by department or regulation type within organizations. This can create many problems, including unidentified risks, redundancies, and higher costs, requiring more resources, time, and effort to achieve a secure IT environment that meets regulatory compliance requirements. Moreover, while business processes and business process improvements are common practices in most organizations, this approach is often missing in the area of security.

Today, organizations of all kinds are making a conscious effort to simplify the process, given the multiple places in which these three areas operate concurrently. The result is a more effective process of defining risk within the context of existing organizational rules and business objectives, and within the framework of compliance regulations, as shown in Figure 1-15. The IT governance component creates stringent requirements for information security architectures, within the goal of adding business value, in addition to mitigating risk.

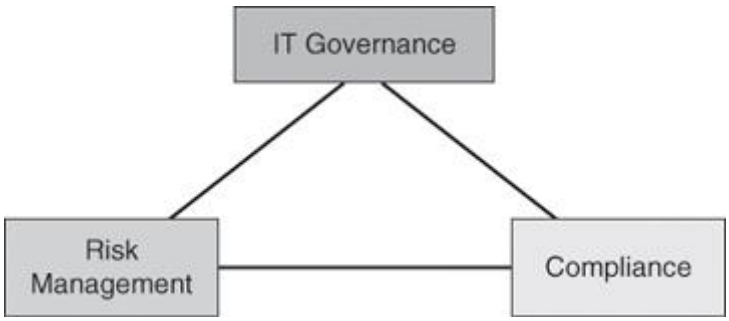

Figure 1-15. Organization-wide Integration of IT Governance, Risk Management, Compliance

This convergence results in an ideal framework and context to create a lifecycle approach to information security.

Secure Network Life Cycle

By framing security within the context of IT governance, compliance, and risk management, and by building it with a sound security architecture at its core, the result is usually a less expensive and more effective process. Including security early in the information process within the system design life cycle (SDLC) usually results in less-expensive and more-effective security when compared to adding it to an operational system.

A general SDLC includes five phases:

1. Initiation
2. Acquisition and development
3. Implementation
4. Operations and maintenance
5. Disposition

Each of these five phases includes a minimum set of security steps that you need to follow to effectively incorporate security into a system during its development. An organization either uses the general SDLC or develops a tailored SDLC that meets its specific needs. In either case, the National Institute of Standards and Technology (NIST) recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process.

Initiation Phase

The initiation phase of the SDLC includes the following:

- **Security categorization:** This step defines three levels (low, moderate, and high) of potential impact on organizations or individuals should a breach of security occur (a loss of confidentiality, integrity, or availability). Security categorization standards help organizations make the appropriate selection of security controls for their information systems.
- **Preliminary risk assessment:** This step results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

Acquisition and Development Phase

The acquisition and development phase of the SDLC includes the following:

- **Risk assessment:** This step is an analysis that identifies the protection requirements for the system through a formal risk-assessment process. This analysis builds on the initial risk assessment that was performed during the initiation phase, but is more in depth and specific.
- **Security functional requirements analysis:** This step is an analysis of requirements and can include the following components: system security environment, such as the enterprise information security policy and enterprise security architecture, and security functional requirements.
- **Security assurance requirements analysis:** This step is an analysis of the requirements that address the developmental activities required and the assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, is used as the basis for determining how much and what kinds of assurance are required.
- **Cost considerations and reporting:** This step determines how much of the development cost you can attribute to information security over the life cycle of the system. These costs include hardware, software, personnel, and training.
- **Security planning:** This step ensures that you fully document any agreed upon security controls, whether they are just planned or in place. The security plan also provides a complete characterization or description of the information system and attachments of or references to key documents that support the information security program of the agency. Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment, a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- **Security control development:** This step ensures that the security controls that the respective security plans describe are designed, developed, and implemented. The security plans for information systems that are currently in operation may call for the development of additional security controls to supplement the controls that are already in place or the modification of selected controls that are deemed less than effective.
- **Developmental security test and evaluation:** This step ensures that security controls that you develop for a new information system are working properly and are effective. Some types of security controls, primarily those controls of a nontechnical nature, cannot be tested and evaluated until the information system is deployed. These controls are typically management and operational controls.
- **Other planning components:** This step ensures that you consider all the necessary components of the development process when you incorporate security into the network life cycle. These components include the selection of the appropriate contract type, the participation by all the necessary functional groups within an organization, the participation by the certifier and accreditor, and the development and execution of the necessary contracting plans and processes.

Implementation Phase

The implementation phase of the SDLC includes the following:

- **Inspection and acceptance:** This step ensures that the organization validates and verifies that the functionality that the specification describes is included in the deliverables.
- **System integration:** This step ensures that the system is integrated at the operational site where you will deploy the information system for operation. You enable the security control settings and switches in accordance with the vendor instructions and the available security implementation guidance.

- **Security certification:** This step ensures that you effectively implement the controls through established verification techniques and procedures. This step gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the information system of the organization. Security certification also uncovers and describes the known vulnerabilities in the information system.
- **Security accreditation:** This step provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.

Operations and Maintenance Phase

The operations and maintenance phase of the SDLC includes the following:

- **Configuration management and control:** This step ensures that there is adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.
- **Continuous monitoring:** This step ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.

Disposition Phase

The disposition phase of the SDLC includes the following:

- **Information preservation:** This step ensures that you retain information, as necessary, to conform to current legal requirements and to accommodate future technology changes that can render the retrieval method of the information obsolete.
- **Media sanitization:** This step ensures that you delete, erase, and write over data as necessary.
- **Hardware and software disposal:** This step ensures that you dispose of hardware and software as directed by the information system security officer.

Models and Frameworks

The five-phase approach of the SDLC gives context to the process of designing, creating, and maintaining security architectures. It is based on NIST Publication 800-64 revision 2. Other frameworks and models exist, providing similar guidance to your security architecture:

- The ISO 27000 series is a comprehensive set of controls comprising best practices in information security. It is about information security, not IT security. It is also an internationally recognized information security standard, broad in scope and generic in applicability. It focuses on risk identification, assessment, and management. It is aligned with common business goals:
    - Ensure business continuity
    - Minimize business damage

- Maximize return on investments

ISO 27000 standards are much more commonly applied in commercial organizations than in government. Originally created as BS17799, this framework was first submitted in 1995, and revised in 1998, but was not adopted by the ISO until 1999. Significantly revised in 2005, it was formally converted to two related ISO/International Electrotechnical Commission (ISO/IEC) standards, 27001 and 27002.

- Control Objectives for Information and Related Technology (COBIT) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. The good practices provided by COBIT represent the consensus of experts. These good practices are strongly focused more on control and less on execution.

  These practices will help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong. COBIT is generally considered complementary to ISO/IEC 27001 and 27002.

- The Information Technology Infrastructure Library (ITIL) was developed under the supervision of the Central Computer and Telecommunications Agency in the UK. ITIL is a set of eight practice guidebooks covering most aspects of IT service management. The fourth service management set is Security Management. ITIL Security Management is based on the code of practice in ISO 27002.

Table 1-7 provides a summary of the different frameworks.

Table 1-7. Comparison of Frameworks

Framework	Strengths	Focus
COBIT	IT controls	IT governance
	IT metrics	Audit
ISO 27000 series	Global acceptance	Information security
	Certification	Management system
	Security control	
ITIL	Processes	IT service
	Certification	management
NIST 800 series	Detailed, granular	Information systems
	Tiered controls	FISMA (federal government)
	Available for free	

Network Security Posture

By assessing all aspects of the networked business environment, it is possible to determine the ability of the organization to detect, defend against, and respond to network attacks. The following are the key activities:

- **Security posture assessment (also known as vulnerability assessment):** The first step in planning network security requires an evaluation of the network security posture of the organization. The security posture assessment provides a snapshot of the security state of the network by conducting a thorough assessment of the network devices, servers, desktops, and databases. The effectiveness of the network security is analyzed against recognized industry best practices to identify the relative strengths and weaknesses of the environment and document specific vulnerabilities that could threaten the business. Because network security involves all aspects of the business, it is necessary to assess security from various perspectives, including the internal, external, dial-up, and wireless networks, and to provide recommendations on how to improve overall network security.

- **Internal assessment:** With so much attention devoted to threats and incidents by hackers, administrators may overlook the security of the internal, trusted network. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices. The assessment identifies the steps that are needed to thwart intentional attacks or unintentional mistakes from trusted insiders to effectively secure valuable information assets. To go beyond automated detection of vulnerabilities, you could simulate a real intruder in a controlled, safe manner to confirm vulnerabilities manually. The assessment provides a more structured approach to identifying vulnerabilities that may go undetected. This secondary exploitation may include attempting to exploit trusted relationships between hosts, exploiting password weakness, or gaining administrative access to systems.

- **External assessment:** The goal of an external assessment is to quantify the security risk that is associated with Internet-connected systems. After researching and confirming the registration of Internet devices, assessors scan the device for external visibility. Because most services have inherent and well-known vulnerabilities, it must be determined whether the services offered are potentially vulnerable.

- **Wireless assessment:** The wireless assessment provides an evaluation of the security posture of the wireless network within the organization and identifies risks and exposures that are associated with a wireless deployment. Assessors analyze the wireless technology architecture and configurations to identify authorized and unauthorized access points and to recommend solutions to strengthen the security of the wireless infrastructure. Assessors also check outside customer buildings to find wireless network traffic leaking from the buildings.

- **Security posture assessment analysis and documentation:** This assessment quantifies the security posture of the organization network by using metrics and graphs. The report should also provide technical details, including analysis of each IP address, an explanation of methods that are used to compromise network devices and systems, and a description of the likelihood that an attacker will use that same approach. The report then prioritizes the vulnerabilities, recommends actions to correct the security risks, and details remediation steps that will prevent future exploitation.

Network Security Testing

Security testing provides insight into the other SDLC activities, such as risk analysis and contingency planning. You should document security testing and make the documentation available for staff involved in other IT and security-related areas. Typically, you conduct network security testing during the implementation and operational stages, after the system has been developed, installed, and integrated.

During the implementation stage, you should conduct security testing and evaluation on specific parts of the system and on the entire system as a whole. Security test and evaluation (ST&E) is an examination or analysis of the protective measures that are placed on an information system after it is fully integrated and operational. The following are the objectives of the ST&E:

- Uncover design, implementation, and operational flaws that could allow the violation of the security policy
- Determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- Assess the degree of consistency between the system documentation and its implementation

Once a system is operational, it is important to ascertain its operational status. You can conduct many tests to assess the operational status of the system. The types of tests you use and the frequency in which you conduct them depend on the importance of the system and the resources available for testing. You should repeat these tests periodically and whenever you make a major change to the system. For systems that are exposed to constant threat, such as web servers, or systems that protect critical information, such as firewalls, you should conduct tests more frequently.

Security Testing Techniques

You can use security testing results in the following ways:

- As a reference point for corrective action
- To define mitigation activities to address identified vulnerabilities
- As a benchmark to trace the progress of an organization in meeting security requirements
- To assess the implementation status of system security requirements
- To conduct cost and benefit analysis for improvements to system security
- To enhance other lifecycle activities, such as risk assessments, certification and authorization (C&A), and performance-improvement efforts

There are several different types of security testing. Some testing techniques are predominantly manual, and other tests are highly automated. Regardless of the type of testing, the staff that sets up and conducts the security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, IPSs, operating systems, programming, and networking protocols, such as TCP/IP.

Many testing techniques are available, including the following:

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review

- Integrity checkers
- Virus detection
- War dialing
- War driving (802.11 or wireless LAN testing)
- Penetration testing

Common Testing Tools

Many testing tools are available in the modern marketplace that you can use to test the security of your systems and networks. The following list is a collection of tools that are quite popular; some of the tools are freeware, some are not:

- Nmap
- GFI LanGuard
- Tripwire
- Nessus
- Metasploit
- SuperScan by Foundstone, a division of McAfee

Many other excellent tools exist. This list is only a representative sampling.

NOTE

Visit http://www.backtrack-linux.org to download BackTrack 5, released in August 2011. BackTrack 5 is packed with hundreds of security tools to test and secure your network. Use BackTrack 5 responsibly and legally, which entails getting written permission from the organization where you would like to use BackTrack prior to using it.

Incident Response

Risk cannot be completely eliminated in some business environments.

Security Diminishing Returns and Residual Risk

Earlier I mentioned that a way to deal with risk is to reduce it by investing in security measures. The concept of diminishing returns applies to those security investments. Looking at Figure 1-16, you will notice that each additional security investment reduces risk (at least in theory). However, also notice that each additional security investment yields a lower additional risk reduction than the previous investment. In economics, this is what is called *diminishing returns*. Also, notice that regardless of how many resources you dedicate toward mitigating a risk, you can never reduce it to zero. There will always be residual risk. If that residual risk is unacceptable for your organization, you could consider buying insurance against it. Buying insurance against a risk would be considered *transferring the risk*.

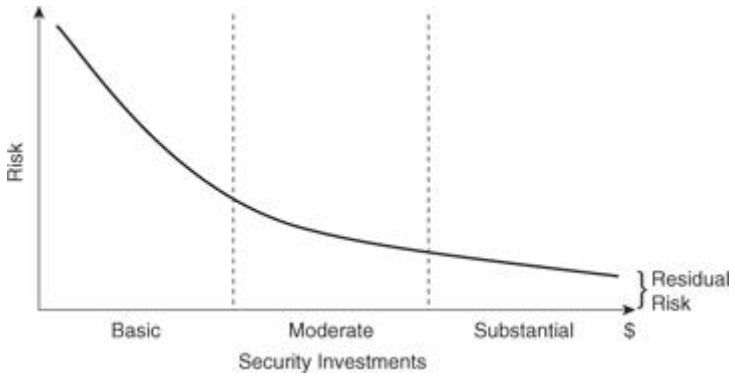

Figure 1-16. Security Investment: Diminishing Returns and Residual Risk

One way to eliminate risk is to simply withdraw from doing business at all, an unlikely scenario. For this reason, incident response has become an important component of the secure network life cycle. The breadth and sophistication of threat vectors in information security has increased exponentially. Every day new techniques emerge, and the motivation of the attackers becomes increasingly aggressive, driven by political reasons, industrial espionage, and terrorism. Preventative measures help, but not all incidents can be prevented. Risk avoidance is unlikely; risk mitigation is more realistic.

It is, then, almost required to implement an incident response capability to streamline the incident detection capabilities, contain the impact of those incidents to minimize loss and destruction, reduce the scope of weaknesses, and restore services within the parameters of the organization.

Implementing an incident response plan effectively can be challenging because of the amount and scope of the resources needed. The first critical step is to deploy an effective intrusion detection and prevention capability. Even if the incident response plan is not in place, incident detection and prevention can provide a first line of response. However, incident response is not completely effective without framing it within an incident response plan. Assessing the current and potential business impact of incidents is critical. Other crucial factors include the implementation of effective methods of collecting, analyzing, and reporting data. Also, it is important to define the framework of communication between the teams involved (for example, technical teams, human resources, legal) and between the organization and external entities (such as other incident response teams and law enforcement).

Incident Management

The incident response process has several phases:

- **Preparation:** As with any other activity, preparation is the building block of incident response methodologies. Preparation creates the foundation for a sound incident response plan and lays the groundwork for an incident prevention culture within the organization. These are some examples of the tasks typically implemented during the preparation phase:
    - Prepare the facilities (such as a central coordination room and storage facilities for collected evidence) and the communication mechanisms (cell phones, contact and on-call information, and others).
    - Define the incident analysis hardware and software tools, such as protocol analyzers and forensics software.
    - Define prevention procedures, such as patch management and user awareness and training methods.
- **Detection and analysis:** With any luck, this is where the incident response team will spend most of its time. This phase starts with the definition of a threat vector classification scheme, in order to define detection and analysis capabilities more effectively per type of threat. Clearly defining the difference between events and incidents is critical. The incident response team should analyze and implement tools for log and event correlation, in order to facilitate the navigation across eventually thousands of security-related events. Efficiently and effectively identifying the business- and risk-relevant incidents out of thousands of events is a key component of the detection strategy. The best way to start is to define a sound framework to prioritize, document, and provide notice about incidents.
- **Containment, eradication, and recovery:** When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. The containment strategy could start with a clear definition of tools to identify the attacker through IP addresses, usernames, and other means, followed by a clear definition of the context and time to perform this function (need for evidence preservation, time and resources to implement the strategy, sustainable service availability, and others). All containment strategies should also include steps to eradicate the threat and vulnerabilities, or at least mitigate them, and steps to recover operating systems, hardware components, and productive time. In light of this, ensure that the security policies are adapted to let remediation take place in a timely and effective manner if an attack is detected.
- **Post-incident activity:** This phase is crucial. The more the incident response team learns from past experience and (specially) mistakes, the more prepared it will be for future incidents. Focusing on how to collect and use data is a good first step. How to document what happened, especially the symptoms and fingerprint of the attack, should follow, leading to a full root-cause analysis. At this point, the incident response team should have a clear understanding of the options to go after the attacker (involve law enforcement, prosecution, and others).

Computer Crime Investigations

If you intend to successfully prosecute an individual who breaches your security, it is necessary to establish three things in most countries (in addition to evidence, the collection of which is covered next):

- **Motive:** Motive is concerned with why an individual performed the illegal act. As you investigate a computer crime, it is important to start with individuals who might have been motivated to commit the crime.
- **Opportunity:** Having identified a list of suspects, the next thing to consider is whether they had the opportunity to commit the crime. For example, if you can establish that three of the suspects were all participating in a wedding at the time of the security breach, they may have been motivated, but they did not have the opportunity. They were busy doing something else.
- **Means:** The means is an important thing to prove as well. Do not accuse someone who does not have the technical knowledge to accomplish the deed. Means is the ability to perform the crime. However, keep in mind that hacking tools have become easy for even a novice to use.

If you do not establish these three things, it is difficult to prove that the perpetrator is guilty of the offense should you decide to prosecute. When you can establish motive, opportunity, and means, and offer evidence, you are closer to a list of possible guilty parties.

NOTE

Different countries have different legal standards. Most countries and courts in the world accept this particular standard.

When working with computer data as part of a forensics case, you must maintain the integrity of the data if you will rely on the data in a court of law. It is difficult to maintain the integrity of the data in the virtual world of computers where it is trivial to change time stamps or any item of data. The flipping of a single bit can sometimes be all that is required to falsely establish an alibi.

Collection of Evidence and Forensics

Data collection is a volatile thing in the virtual world of computers. For this reason, a common procedure in response to security breaches is the immediate isolation of the infected system. Dumping the memory to disk is required because the system flushes the memory every time a device is powered off. Multiple copies of the hard drive are usually made after the device is powered down, to establish master copies. These master copies are usually locked up in a safe, and investigators use working copies for both the prosecution and the defense. You can answer any charges of tampering with data by comparing working copies to the master copy that has been secured and untouched since the beginning of the investigation.

It is important to note that when making copies of hard drives, a hardware write blocker must be used to ensure that the data on the source drive has not been modified by the copy. EnCase Forensic suite from Guidance Software is a product that uses hardware write blocker.

Laws and Ethics

This section describes key laws and codes of ethics that are binding on information systems security (infosec) professionals.

For many businesses today, one of the biggest considerations for setting security policies is compliance with the law. For that reason, it is important for infosec professionals to be at least conversant in the basics of law.

In most countries, there are three types of laws:

- **Criminal:** Concerned with crimes, and its penalties usually involve the risk of fines or imprisonment, or both. If fines are paid, they are usually to the court and are used to defray court costs.
- **Civil (also called tort):** Focuses on correcting wrongs that are not crimes. An example of a civil law case is if one company sues another company for infringing on a patent. The penalty in civil law is usually monetary, although there can also be performance requirements such as ceasing to infringe on the patent. If money is awarded, it is given to the party who won the lawsuit. Imprisonment is not possible in civil law.
- **Administrative:** Involves government agencies enforcing regulations. For example, a company may owe its employees vacation pay. An administrative court could force the company to pay and would probably also levy a fine that is payable to the agency. Therefore, in administrative law cases, monetary awards are often split between the government agency and the victim whose wrongs have been righted.

Ethics involves a standard that is higher than the law. It is a set of moral principles that adherents follow to be considered ethical. These ethics are often formalized in codes appropriately entitled "codes of ethics" by the professions formalizing the code.

The information security profession has a number of codes that have been formalized:

- International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ Code of Ethics
- The Computer Ethics Institute's Ten Commandments of Computer Ethics
- RFC 1087, "Ethics and the Internet," by the Internet Activities Board (IAB)
- Generally Accepted System Security Principles (GASSP)

Liability

Companies must take into account the legal liability for the country in which they reside. Take, for example, an Internet service provider (ISP) that has hundreds of e-businesses that rely on the ISP to run their websites with 100 percent uptime. If a hacker or a virus takes down this ISP, there is a chance for the ISP to be found liable, if it is discovered that the ISP did not take enough precautions or did not secure the network against internal or external threats.

In such cases, legal liability is likely to depend on what prevention technologies and practices are available and whether these technologies and practices are reasonably cost-effective to implement. While developing and implementing our security procedures, we must demonstrate due diligence and due care.

Showing due diligence includes everything from implementing technologies such as firewalls, intrusion-detection tools, content filters, traffic analyzers, and VPNs, to having best practices for continuous risk-assessment and vulnerability testing.

Due care is concerned with the operations and maintenance of the secure mechanisms put in place by practicing due diligence.

Lack of due care can lead to downstream liability. This is the case when a network is used by hackers as a springboard to conduct an attack against a third party. The victim of the attack could prosecute not only the hackers, but also the organization whose security was lax enough that its network was used as the launching pad for the attack.

Disaster Recovery and Business Continuity Planning

Business continuity planning and disaster recovery procedures address the continuing operations of an organization in the event of a disaster or prolonged service interruption that affects the mission of the organization. Such plans should address an emergency response phase, a recovery phase, and a return to normal operation phase. You should identify the responsibilities of personnel during an incident and the resources that are available to them.

In reality, contingency and disaster recovery plans do not address every possible scenario or assumption. Rather, they focus on the events most likely to occur and they identify an acceptable method of recovery. Periodically, you should exercise the plans and procedures to ensure that they are effective and well understood.

Business continuity planning provides a short- to medium-term framework to continue the organizational operations. The following are objectives of business continuity planning:

- Moving or relocating critical business components and people to a remote location while the original location is being repaired
- Using different channels of communication to deal with customers, shareholders, and partners until operations return to normal

Disaster recovery is the process of regaining access to the data, hardware, and software necessary to resume critical business operations after a natural or human-induced disaster. A disaster recovery plan should also include plans for coping with the unexpected or sudden loss of key personnel. A disaster recovery plan is part of a larger process known as business continuity planning.

After the events of September 11, 2001, when many companies lost irreplaceable data, the effort put into protecting such data has changed. It is believed that some companies spend up to 25 percent of their IT budget on disaster recovery planning to avoid larger losses. Research indicates that of companies that had a major loss of computerized records, 43 percent never reopened, 51 percent closed within two years, and only 6 percent survived long term (http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan and http://en.wikipedia.org/wiki/Disaster_recovery).

Not all disruptions to business operations are equal. Whether the disruption is natural or human, intentional or unintentional, the effect is the same. A good disaster recovery plan takes into account the magnitude of the disruption, recognizing that there are differences between catastrophes, disasters, and nondisasters. In each case, a disruption occurs, but the scale of that disruption can dramatically differ.

- **Nondisaster:** A situation where a business process is unavailable for a given period of time
- **Disaster:** A situation that makes a facility unusable for an entire day or more
- **Catastrophe:** A situation that destroys the facility

Business Continuity Concepts

Building a business continuity plan requires extensive planning, with knowledge of the business requirements, budgets, and levels of risk the organization is willing to take. Some of the building block components, however, are more easily defined. The goal, from a rather simplified point of view, is to define objectives for the recovery of host computing systems that run the applications that support the business processes. These objectives are stated as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

RTO is the number of hours or days that management has set as the objective for resuming a business process or a system. RPO describes the age of the data you want the ability to restore to in event of a disaster. For example, if the RPO is 8 hours, systems should be restored in the state they were in no longer than 8 hours ago. The technical disaster recovery strategy depends upon meeting RTO and RPO specifications. The RTO and RPO requirements determine which option of the disaster recovery plan to implement. Recovery time and how current data is are key components in determining the level of service a business process requires in the event of a major disruption. To properly implement a disaster recovery plan, one must know the RTO and RPO that the organization is willing to accept in a disaster. The technical disaster recovery strategy of different options of recovery is based upon a combination of these requirements.

Key Concepts

Maximum Tolerable Downtime (MTD)

The total amount of time the system owner or authorizing official is willing to accept for a mission or business process outage or disruption, and includes all impact considerations.

Recovery Time Objective (RTO)

The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission, or business processes.

Recovery Point Objective (RPO)

The point in time, prior to a disruption or system outage, to which mission or business process data can be recovered (given the most recent backup copy of the data) after an outage.

Summary

To have a comprehensive security solution, it is important to cover all aspects of the operation of an organization. Comprehensive security requires suitable reliance on technical, physical, and administrative controls; implementing defense in depth; and developing an all-inclusive security policy. You will also be required to demonstrate forward thinking, taking into consideration the threats of tomorrow.

In this chapter you have learned that

- The confidentiality, integrity, and availability of the data need to be protected.
- Assets, vulnerabilities, and countermeasures can be classified to assist in developing a comprehensive set of security policies.
- New trends and threats are appearing frequently in the borderless network environment where we are evolving.
- To provide a comprehensive security solution, it is essential that there be a combination of technical, physical, and administrative controls in place.
- Defense in depth is a philosophy used to provide layered security to a system by using multiple security mechanisms.
- A security policy is a set of objectives for the company, rules of behavior for users and administrators, and requirements for system and management that collectively ensures the security of network and computer systems in an organization.

References

For additional information, refer to these resources.

Publications

Harris, S. *CISSP All-in-One Exam Guide, Fifth Edition* (McGraw-Hill Professional, 2010).

McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed, Sixth Edition* (McGraw-Hill Professional, 2009).

McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed, Seventh Edition* (McGraw-Hill Professional, 2012).

NIST SP 800-27 Rev A, *Engineering Principles for Information Technology Security*.

NIST SP 800-42, *Guidelines on Network Security Testing*.

NIST SP 800-64 Rev. A, *Security Considerations in the Information System Development Life Cycle*.

Richardson, R. *2010-2011 CSI Computer Crime and Security Survey* (http://gocsi.com/survey).

Wood, C. *Information Security Policies Made Easy, Version 11* (Information Shield, 2009).

Web Resources

Insecure.org, http://www.insecure.org/nmap/

SecurityFocus, http://www.securityfocus.com/

Security-Solutions.net, http://www.security-solutions.net/download/index.html

The GNU Netcat Project (G. Giacobbi), http://netcat.sourceforge.net/

The Jargon File, http://www.catb.org/~esr/jargon/html/index.html

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in the appendix, "Answers to Chapter Review Questions."

1. Which are the three primary objectives of security?
    a. Integrity
    b. Confidentiality
    c. Antireplay functionality
    d. Authentication
    e. Availability
2. Which are the three categories of controls?
    a. Administrative
    b. Executive
    c. Managerial
    d. Technical
    e. Physical
3. Show that you understand the different types of controls by matching them with their related technology.

    Type of controls

    a. Preventative
    b. Deterrent
    c. Detective

    Technologies

    d. Motion sensor
    e. Video surveillance
    f. Lock
4. Match the different types of hackers and the like with their appropriate description.

    Hacker types

    d. White hat
    e. Black hat
    f. Gray hat
    g. Blue hat

h. Cracker
i. Phreaker
j. Script kiddy
k. Hacktivist

Hacker descriptions

i. Bug tester
j. Hacker with little skill
k. Unethical hacker
l. Hacker of telecommunication systems
m. Ethically questionable hacker
n. Hacker with a political agenda
o. Synonymous with black hat hacker
p. Breaks security for nonmalicious reasons

5. Organize the following steps in the order in which they are used to compromise targets and applications.
   i. Escalate privilege
   j. Leverage the compromised system
   k. Perform footprint analysis
   l. Install back doors
   m. Enumerate applications and operating systems
   n. Gather additional passwords and secrets
   o. Manipulate users to gain access
6. Which of the following is (are) not part of the technical policies. (Select all that apply.)
   . End-user policy
   a. Acceptable usage policy
   b. Email policy
   c. Governing policy
   d. Rainbow Series
   e. Network policy
   f. Common Criteria Standard
   g. Wireless policy
7. Reorder the classification levels of the private sector, from the least secure document to the most secure document.
   . Confidential
   a. Private
   b. Public
   c. Sensitive
8. Which of the following is not a criterion used to classify data?
   . Value
   a. Age
   b. Useful life
   c. Copyright
   d. Personal association
9. Match each of the following information classification roles with its definition.

   Roles

   . Owner
   a. Custodian
   b. User

Definitions

d. Responsible for using the data
e. Responsible on a day-to-day basis for the classified data
f. Ultimately responsible for the data

10. Which of the following is a technical control?
    d. Network Admission Control system
    e. Security policies and standards
    f. Security audits
    g. Security awareness training
    h. Change and configuration management
11. Which of the following is not a characteristic of defense in depth?
    . Security mechanisms back each other up.
    a. Security mechanisms do not depend on each other.
    b. Does not require IDS or IPS.
    c. The weakest links can be augmented so that single points of failure can be eliminated.
12. Match the definition with the appropriate attack method.

Definitions

. Searching a network host and open ports
a. Capturing electrical transmission
b. Hiding information within a transmission
c. Intercepting traffic that passes over a physical network

Attack methods

e. Packet sniffing
f. Man-in-the-middle
g. Emanation capturing
h. Covert channel
i. Impersonation
j. Port scanning

13. Reorder the phases of a system development life cycle.
    e. Operations and maintenance
    f. Initiation
    g. Disposition
    h. Acquisition and development
    i. Implementation
14. Which of the following security concepts limits a user's rights to the lowest possible level needed to perform his tasks?
    . Need to know
    a. Least privilege
    b. Universal participation
    c. Diversity of defense

---

800 East 96th Street, Indianapolis, Indiana 46240