why?
c. What tools would you use to maintain engagement in the project?

2. In a small group or on your own, reflect on a business problem in your current organization (work or school).
a. Identify an opportunity for improvement in your organization's function or operation.
b. Who would you enlist to assist with requirements gathering?
c. What tools will you use to assist your efforts?
d. What are some other factors you should consider?

3. Discuss the inputs and outputs that could be present in Dr. Singh's system. Include how the data move through the data cycle in the system.

4. Reflect on a website or a mobile application that you frequently use or visit.
a. Discuss what you like and dislike about the website or mobile application. How would you describe its usability?
b. If you have any dislikes, why do you continue to visit this website? Are there competitor websites, and how do they differ?
c. Does the website or mobile application allow you to submit user feedback? If so, have you ever submitted feedback on the website's usability? Why or why not?

5

Information Systems Security Risk Management

Figure 5.1 Protection from cybersecurity attacks works in a similar way to how we protect ourselves from bad weather—by using different layers to shield us from the elements. (credit: modification of work "Clear Umbrella Rain Liverpool" by Freddie Marriage/ Wikimedia Commons, CC0 1.0)

Chapter Outline

Introduction

Imagine carrying important documents, such as a paycheck or a diploma, when it starts to rain. Without an umbrella, your documents can be damaged, although it may be possible to reprint them. However, if the rain turned into a violent storm, you'd need much more protection to keep your documents safe. Similarly, in information technology, our digital lives are constantly threatened by malicious actors, rogue governments, and natural disasters.

Just as an umbrella alone isn't enough to protect someone from a storm, people rely on multiple layers of protection to shield their digital lives. As a person navigates the digital landscape, layers of security help keep them safe, preventing severe damage that's much harder to remediate.

5.1 The Importance of Network Security

Learning Objectives

By the end of this section, you will be able to:

- Determine the difference between information security and information privacy on a public or private network
- Define the key principles and concepts of network security and their importance
- Describe potential network vulnerabilities and threats

Network security is dynamic, requiring ongoing adjustments to counter rising vulnerabilities and threats. What

may be considered safe today may not be in the future. The ever-changing nature of this field necessitates a comprehensive understanding of various technologies and advancements that influence security. The implications of a network security breach can be diverse, ranging from minor disruptions in operations, to severe data loss or compromise. Therefore, understanding the significance of network security can contribute to a larger societal benefit. It is important for IS professionals to have a conceptual understanding of network security, its mechanics, and why this protection is a key aspect of modern life, as well as the practical skills needed in securing a network.

Information Security and Information Privacy on a Public or Private Network

In the field of **cybersecurity**—which is the practice of protecting systems, networks, devices, and data from online threats—information security and information privacy are not identical terms, although they are related. On one hand, **information security** is the practice of protecting information by mitigating information risks and vulnerabilities, which encompasses data privacy, data confidentiality, data integrity, and data availability and employs methods such as encryption, firewalls, and secure network design. Its aim is to shield both organizational and individual data from unauthorized access or tampering. In contrast, **information privacy** involves the right and measure of control individuals have over the collection, storage, management, and dissemination of personal information. Information privacy involves policies regarding what data are collected, how they are stored, and who has access to share information.

The two domains of information privacy and information security are not static; they are influenced by technological advancements and emerging threats. This makes continuous learning and adaptation important for anyone interested in the field. Both students and seasoned professionals need to maintain their skills and understanding to keep up with advancements in the field. This may include learning about the latest encryption methods or understanding new data privacy laws that impact the organization.

Although both information security and information privacy are equally important, they tackle different aspects of data protection. Think of information security as a bouncer at a club. Its job is to keep unwanted guests out, so it uses tools such as encryption to hide the important data, firewalls to block unauthorized entry, and secure networks to chase away any intruders. Information privacy, then, is more like getting access to the VIP room inside that club. It manages who gets in, who sees what, and what goes on inside. Imagine you have a list of the criteria for who can access the VIP room. When you're not updating it, you keep it locked in a special drawer that only you have the key to, thus keeping the contents private. But privacy also includes making sure unauthorized people do not know who is on that list, or even that it exists.

In short, information security is about guarding the perimeter and protecting your assets, while information privacy is about managing access and keeping sensitive data private. Both are essential, but they play different roles in keeping your digital world safe. At the core of both information security and information privacy is a foundational model in cybersecurity that ensures information is protected and readily available to authorized users, called the **confidentiality, integrity, and availability (CIA) triad** (Figure 5.2).

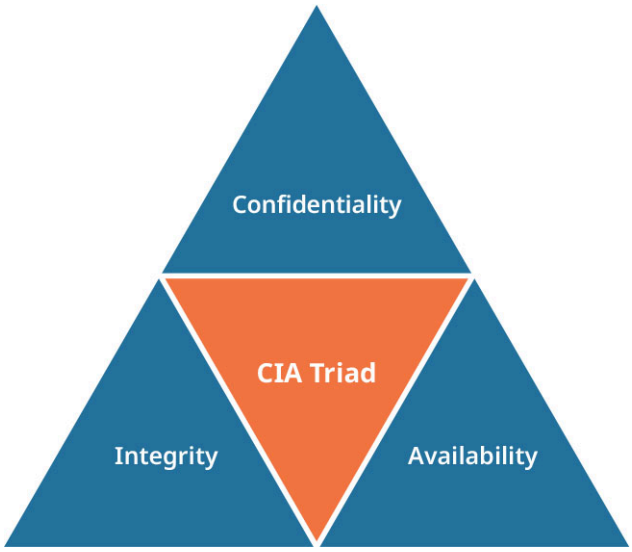

Figure 5.2 The confidentiality, integrity, and availability (CIA) triad is the cornerstone framework for information security that aids in promoting the security and reliability of information systems. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The CIA triad is the backbone for creating cybersecurity systems, aiming to strike a balance between keeping things secure and ensuring that the people who are authorized to access the data and systems have access to it. As the name implies, the CIA triad is divided into three domains:

1. The measures that are meant to prevent sensitive information from being accessed by bad actors or by those users who have not been granted access is called confidentiality. The intent is to keep data in the correct hands and away from those who want to cause harm or exploit information for nefarious purposes. Additionally, confidentiality addresses policies involving human error, such as users not keeping strong passwords, failing to secure sensitive information when not in use, and falling prey to scammers. Scams often involve **phishing**, which is a type of social engineering attack that appears as a trustworthy entity in digital communication but steals user data, such as login credentials and financial information. Two means of applying confidentiality to an IT system are encryption and access controls.
2. Preserving the fidelity of data over its life cycle is called integrity. Any alteration to database tables, user records, or other data can be very damaging, often causing legal ramifications or loss of operations. Two means of maintaining the integrity of data are hashing and digital signatures.
    - The process of converting data into a fixed-size string of characters, typically used for security purposes to ensure data integrity, is called **hashing**. Hashing can verify the authenticity of a file by assigning a hash algorithm, such as Secure Hashing Algorithm 256 (SHA-256) that has a 64-character hexadecimal hash value assigned to the file by the algorithm. This results in a hash of characters that represent every point of data in the file, bit by bit. Even the smallest change in the file results in a drastically different chain of characters.
    - An electronic signature that uses cryptographic techniques to provide authentication and ensure the integrity of the signed digital document or message is a **digital signature**. They are used in online documents such as emails, bank documents, and online forms, and employ the public key infrastructure (PKI) to protect the confidentiality and integrity of data during transit. This method works by supplying a public and private key to each user transmitting information. Aside from protecting the confidentiality and integrity of data during transit, this framework helps to verify the authenticity of a file and its sender.
3. Ensuring that authorized users can access resources such as networks, databases, and other systems is called availability. This part of the triad often encompasses disaster recovery and response plans. There are several ways to maintain availability, such as keeping up with upgrades on equipment and software, maintaining backups in case of an attack or system failure, and ensuring that redundant systems are in

place to protect the IT system.

Think about the CIA triad like this: Imagine you have a personal diary, and you want to make sure nobody else can read it. When you're writing in it, you want to be able to access it easily, but when you put it away, you want to feel confident that no one else can access it.

Storing your diary in a safe when you're not using it is a way of keeping it confidential. You could also put a seal on it, so if someone does try to tamper with it, you'll know; that's maintaining its integrity. Keeping the safe somewhere close, so you can get to your diary whenever you need it ensures that it is always available to you. This way, you've covered all the bases of the CIA triad.

Information Security

When we think of data, most of us envision pictures, documents, and videos. However, data come in all sorts of formats, types, and sizes. While our media is an important piece of the data puzzle, other types are equally important. Consider the security of passwords, bank account information, employee records, and text messages. These types of data also require both information security and information privacy. For example, in a workplace setting, protecting employee information involves encrypting sensitive data (information security) and implementing privacy policies to regulate who can view or modify this data (information privacy).

Moreover, the landscape of data protection is becoming increasingly complex with the rise of generative AI. Most organizations use generative AI, but only a third of them implement protection from generative AI threats because most companies do not fully understand the dangers. Currently, generative AI benefits attackers more than organizations, but that may change in the near future.[1] This intersection of advanced technology with traditional data types underscores the critical need for robust security measures. Acknowledging opportunities and threats posed by generative AI, blockchain, and other emerging technologies can help in developing more effective strategies to safeguard all forms of data.

Intellectual Property

Creations of the mind that are protected by law from unauthorized use or replication are called **intellectual property (IP)**. It can include inventions, literary and artistic works, designs, symbols, names, and images used in commerce. IP is often a target for cybercriminals and nation-state threat actors looking to steal technology for their own benefit. Imagine dedicating years of research and millions of dollars to an expensive project only to lose the information to a hacker in minutes. Unfortunately, hackers may still be able to bypass security controls to access an organization's IP.

Financial Data

Financial data are considered sensitive information, which is data that require high levels of confidentiality and security. Sensitive data can include financial data related to transactions and personal finance details, and employee data involving personal and professional details. Protecting this information is crucial to helping organizations prevent fraud, maintain stakeholder trust, and comply with governmental regulations. Security measures used to protect financial data often use a layered approach beyond firewalls and encryption that combines multiple security barriers and includes rigorous auditing and multi factor authentication.

Employee Data

Personally identifiable information, such as Social Security numbers and addresses, constitutes an entity such as employee, customer, or student data. Although they may not seem very sensitive, these data are valuable to hackers for identity theft, corporate espionage, harassment, and extortion. Organizations must use measures such as encryption and the principle of least privilege to protect this information.

1 Jim Tyson, "Only One-Third of Firms Deploy Safeguards Against Generative AI Threats, Report Finds," Cybersecurity Dive, May 13, 2024, https://www.cybersecuritydive.com/news/generative-ai-safeguards-splunk/715897/

Network Configurations

Network configurations are the physical and logical elements that form a network, such as servers, routers, switches, and software. A **server** is a powerful computer or computer program that provides data to other computers (clients) over a network. A **router** is a device that forwards data packets to the appropriate parts of a computer network. A **switch** is a device that connects and segments various components within a local network. Access to these systems by bad actors or rogue employees can have dire consequences for an organization. Unauthorized access to network configuration data could allow an attacker to map out a network, identify weaknesses, and access private customer information.

Internet protocol addresses, along with media access control addresses, are essential elements of a network that require protection. An **internet protocol (IP) address** is a unique identifier that allows a computer to be addressed in order to communicate on the internet. A **media access control (MAC) address** is a unique identifier that allows a computer to be addressed in order to communicate within a local area network. To gain unauthorized access to a network, attackers often use a technique called port scanning for penetration or determining an entry point. These scans allow an attacker to gather information about a network such as the unique addresses of each of the components connected. With this information, hackers can spoof addresses, which allows them to blend into the network undetected. To protect IP addresses and equipment identifiers, organizations use VPNs or proxy servers to mask IP addresses and create a secure tunnel for employees accessing information from remote locations. Passwords account for the largest vulnerability to a network due to the human factor involved. According to *Security Magazine*, close to 75 percent of users are at risk for compromise due to weak password practices.[2] Additionally, it is also estimated that nearly 80 percent of data breaches are caused by poor password management. To prevent attacks due to poor password practices, organizational leaders should implement the policies shown in Table 5.1.

Password Policy	Description
Password standards	Implement password length standards (at least eight characters) and encourage the use of complex passphrases.
Password expiration	Impose periodic password expiration dates, requiring employees to change their passwords semiyearly or annually.
Multi factor authentication	Use multi factor authentication to add another layer of protection by requiring an additional form of authentication, such as an access code.
Password policies	Ban common passwords that can be easily used by attackers.

Table 5.1 Good Password Practices Best practices in securing data keep information safe from attackers.[3]

Information Privacy

Information privacy is a critical aspect of cybersecurity and encompasses the practices, policies, and regulations that are designed to protect people and systems from unauthorized access and harm. This includes protection from access to personally identifiable information (PII), health-care records, financial statements, and data from devices such as smartphones, smartwatches, and other wearable tech.

2 Security Staff, "3 in 4 People at Risk of Being Hacked Due to Poor Password Practices," *Security*, June 21, 2023, https://www.securitymagazine.com/articles/99529-3-in-4-people-at-risk-of-being-hacked-due-to-poor-password-practices
3 "Password policy recommendations for Microsoft 365 passwords," Microsoft, last modified May 28, 2024, https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

Understanding the principles behind establishing and preserving information privacy is key to ensuring that data remains safeguarded while in transit and at rest.

Additionally, the concept of information privacy is based on a variety of policies and regulations that guide leaders and managers on how to safeguard sensitive information. As the scope of data needing protection continually expands, improvements are constantly being made to address the complexities of new, emerging technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence.

In addition, different sectors have their own specific frameworks and laws. In the United States, institutions such as hospitals or those who deal with sensitive medical information must adhere to the guidelines outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In the education sector, educational institutions must adhere to the principles outlined in the Family Educational Rights and Privacy Act (FERPA).

HIPAA

Established in 1996, HIPAA was introduced by the Health and Human Services Department (HHS) to devise legislation that would protect the privacy of those seeking medical care. One part of HIPAA, the Privacy Rule, sets standards and guidelines for organizations that manage patient information and medical records of any kind. This includes health plans, health-care providers, health-care clearinghouses, and business associates.

HIPAA provides rigorous standards for companies that possess and interact with a vast range of protected health information (PHI), such as medical history, billing information, and patient identifiers. Moreover, HIPAA's controls do not apply solely to medical providers, but rather to any entity that may possess or have access to patient data. This includes third parties who provide data hosting services, accounting firms, consultants, or any entity contracted to maintain hosting services such as patient portals and websites.

In addition to the Privacy Rule, HIPAA has a Security Rule, which works with the Privacy Rule to lay out the technical, administrative, and physical measures needed to protect electronic health information, thus tying into the larger world of information security protocols. Failure to comply with HIPAA can result in significant penalties, ranging from fines to criminal charges. These enforcement actions remind organizations to thoroughly adhere to the established guidelines and to continually update their practices.

FERPA

FERPA is a U.S. federal law that was enacted in 1974. Its main goal is to give parents and students who are 18 years and older some control over their educational records. Specifically, FERPA sets rules on who can access these records and under what circumstances. Educational institutions that receive federal funding are required to comply with FERPA's mandates, and noncompliance could result in the loss of that funding.

FERPA gives students and their parents the right to access their educational records, correct any mistakes, and have a say in how that information is shared. While this sounds simple, the implementation can be complex. For example, schools must have written consent to release information, but there are exceptions such as cases involving subpoenas or emergencies. It is important to note that not all information is protected under FERPA. Some types of directory information, such as a student's name, address, and telephone number, can be released without explicit consent, unless the student or parent opts out.[4]

To understand how FERPA protects academic information, consider a student attending a college away from home whose parents demand to know their student's test scores, homework assignments, and regular activity in classes. Under FERPA guidelines, if the student is 18 years old or older, the only one who can release that information to the parents is the student. Their parents would have no access to this type of information from the school without the student's explicit permission, except in health or safety emergencies.

4 U.S. Department of Education, "FERPA: 34 CFR PART 99 --Family Educational Rights and Privacy," accessed January 31, 2025, https://studentprivacy.ed.gov/ferpa

Key Principles and Concepts of Network Security

In the complex world of cybersecurity, it is important for everyone to understand the foundational principles of the threats to digital security and the ways to safeguard digital assets. Whether you are a student, a new employee, or a boardroom executive, having a firm grasp on the key principles can help protect you from digital harm.

Imagine you're setting up a home network. You notice that your devices receive different IP addresses from time to time. This is because many IP addresses are dynamic, changing with each connection. Now, visualize managing a large corporate network where stability and reliability are critical. Here, a company can use a **static IP address**, which is a permanent address assigned by an administrator that remains the same over time and is essential for services such as hosting servers, email servers, and network devices, or when remote access is required.

The consistency of a static IP address allows for reliable and straightforward network management, as well as easier implementation of security measures because the address can be precisely identified and controlled. Static IP addresses are used primarily for servers and network equipment. A **dynamic IP address** is one that is assigned each time a device connects to the internet and changes periodically, although not necessarily every time the device connects. This type of IP addressing is commonly used in residential and small business settings, where internet service providers (ISPs) assign these addresses to customers, and in larger companies for their client machines. Dynamic IP addressing is highly efficient for ISPs as it allows for the reuse and reallocation of a limited pool of IP addresses, optimizing the use of the IP address space, especially given the vast number of devices connecting and disconnecting from the internet.

The Internet Protocol version 4 (IPv4) is the fourth version of the fundamental protocol used for identifying devices on a network and routing data between them over the internet. It consists of four 8-bit groups that make up 32 bits total. In any given IP address under the IPv4 system, the range cannot exceed 256 in any 8-bit group; however, due to system limitations, addresses normally range from 0 to 255. The Internet Protocol version 6 (IPv6) has eight hexadecimal groups that allow up to 128 bits. There are many differences between these standards. For example, IPv6 can supply more security and a nearly limitless number of IP addresses (7.9×10^{28}). IPv6 is more secure than IPv4 because it was designed with built-in support for **Internet Protocol Security (IPsec)**, which is a suite of protocols that provides end-to-end encryption and secure data exchange. Additionally, its massive address space allows for more efficient address allocation, reducing the risks of IP conflicts and improving overall network reliability.

Both IPv4 and IPv6 addresses often come accompanied by a **subnet mask**, which is an address used in routing and network organization that divides the IP address into network and host addresses. One method for allocating IP addresses is **classless inter-domain routing (CIDR)**, which routes IP packets more efficiently than traditional classful IP addressing. CIDR is a key element of the IPv4 addressing method, as it increases efficiency and security by permitting the "borrowing" of bits of information to create a new range of IP addresses to form a **subnet**, which is a logically visible subdivision of an IP network. The subnet mask and CIDR help in segregating the network portion of an IP address from the host portion. This segregation is important for routing and for defining network boundaries, as it permits for the proper distribution of information and traffic to the intended recipient.

Another vital aspect of IP addressing is the way these addresses are allocated and managed. IPv4 addresses were developed in 1981 and were initially distributed in an erratic manner, leading to inefficient use of the address space. In contrast, IPv6 addresses are allocated based on a more hierarchical and organized structure, allowing for easier management and better security protocols. This process is managed by several organizations globally, such as the Internet Assigned Numbers Authority (IANA) and the five Regional Internet Registries (RIRs), ensuring a standardized approach to address allocation.

The **Domain Name System (DNS)** translates human-readable domain names to IP addresses, allowing users

to access websites using familiar names. Essentially, it acts like a directory of the internet. This process is fundamental to web navigation, as it makes it possible for people to access information online without needing to remember complex numeric addresses. Just like a contact list keeps numbers, a DNS keeps IP addresses. Also, just like a contact list, these numbers must be updated frequently as people and equipment change. Figure 5.3 depicts how a DNS matches the client's computer (i.e., IP address) to an organization's website. While DNS is integral to web navigation, it can be exploited for malicious purposes, such as DNS spoofing, an attack where hackers corrupt DNS servers to redirect traffic to another server or website.

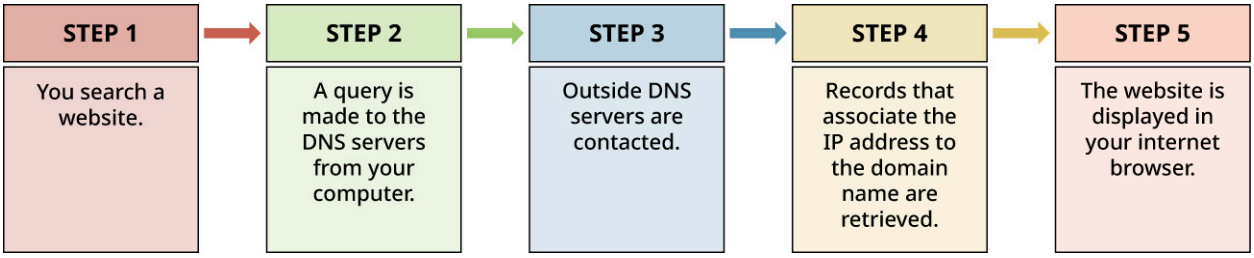

Figure 5.3 A DNS helps to identify and align the correct IP address to the URL. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

It is crucial to implement DNS security measures to mitigate vulnerabilities. One way is to use Domain Name System Security Extensions (DNSSEC), a suite of extensions that add security by enabling DNS responses to be digitally signed and verified. This verification process helps in safeguarding against DNS spoofing and other types of DNS-based attacks. Furthermore, securing DNS resolvers with threat intelligence that prevents users from accidentally visiting sites that could compromise their security can also help block known malicious domains. Implementing these advanced DNS security measures is increasingly considered best practice in both professional and consumer settings. One type of threat DNSSECs can prevent is those involving DNS spoofing, such as a man-in-the-middle (MitM) attack, which is one that manipulates the DNS to redirect a website's traffic to a different IP address, often controlled by the attacker. This allows the attacker to intercept and potentially modify the communication between the user and the intended website.

Another fundamental concept in network and information security is **encryption**, which transforms legible data into a coded format, making it unreadable to unauthorized entities. The encrypted data can only be converted back into its original format, a process called decryption, with the proper **cryptographic key**, which is a string of data used by encryption algorithms to encrypt and decrypt data. Encryption is particularly effective for safeguarding sensitive information during transmission or storage, making it an important tool for protecting data privacy and integrity.

The two most common types of encryption are symmetric and asymmetric. With **symmetric encryption**, the same key encrypts and decrypts the data. This approach can quickly and easily handle a lot of data all at once. The tricky part, though, is that both parties need to have the key, and sharing it securely can be challenging. In **asymmetric encryption**, also known as public-key cryptography, a public and a private key secure the connection. This eliminates the need to securely share a key, but it is slower than symmetric encryption. Each type of encryption serves specific use cases: symmetric is often used for data at rest, and asymmetric for data in transit. Asymmetric encryption is used in **Secure Sockets Layer (SSL)**, a communication protocol that establishes a secure connection between devices or applications on a network by encrypting data sent between a browser and a website or between two servers, and **Transport Layer Security (TLS)**, an updated version of SSL that uses an encrypted tunnel to protect data sent between a browser, a website, and the website's server. TLS prevents unauthorized access to messages and protects against hackers hijacking connections. The standard symmetric encryption algorithm used globally to secure data, known for its speed and security, is **advanced encryption standard (AES)**, while **RSA encryption** is a commonly used asymmetric cryptographic algorithm used for secure data transmission that is particularly useful in public-key cryptography.

The mechanism of **authentication** is the process of verifying the identity of a user, application, or device trying

to access a network or system, often through credentials such as passwords or digital certificates. This can range from simple methods such as username and password combinations to more sophisticated techniques involving **multi factor authentication (MFA)**, which is a security measure that requires users to verify their identity using multiple forms of credentials, such as a password, a security token, or biometric data, to access a system. MFA might require something you know (password), something you have (a mobile device for a token), and something you are (biometrics such as a fingerprint). Proper authentication methods are vital to ensuring that only authorized personnel have access to sensitive data and systems. However, if mismanaged, they could also become a massive security risk, such as if someone gained access to your biometric data to imitate your likeness.

Other key components in network security include firewalls, intrusion detection systems (IDSs), and virtual private networks. A **virtual private network (VPN)** is a service that creates a secure, encrypted connection over a less secure network, typically the internet, ensuring private data remains protected. A **firewall** is a network security system that uses security rules to monitor and control incoming and outgoing traffic, typically between a trusted network and an untrusted entity (such as local area networks or the internet). Intrusion detection systems (IDSs) are more advanced in their capability, as they use pattern detection. Firewalls are mostly a preventive measure, whereas IDSs are a detective measure. IDSs can watch network traffic to detect anomalies that could be a security breach. VPNs, on the other hand, are network configurations that can supply a secure virtual tunnel for data transmission, often used for establishing secure remote access to a network. Think of a VPN as a private, secure, virtual tunnel through the internet. This tube ensures that no one can intercept or access the data during its journey. Similarly, a VPN encrypts your internet connection, creating a secure tunnel that protects your data from hackers, spies, and other potential threats, ensuring that your online activities remain private and secure. Together, these technologies form the foundational layers of a comprehensive network security architecture, each serving a specific role but collectively contributing to the robustness of the entire system.

Network Vulnerabilities and Threats

Network vulnerabilities and threats are critical issues that impact the security posture of any organization. Weak configurations, outdated software, and lax security policies often make networks susceptible to a range of malicious activities. Understanding these vulnerabilities is a fundamental step in fortifying a network's defenses.

Types of Network Vulnerabilities

When it comes to network security, software vulnerabilities often serve as an open door for attackers. A software vulnerability is a weakness or flaw within a software system, particularly in outdated or unpatched systems, that can be exploited by cybercriminals to gain unauthorized access or to disrupt the software's normal functioning. Outdated software and unpatched systems are particularly risky because they may have known flaws that have not been addressed, making them a target for cybercriminals. Imagine your software as a building: If everyone knows there is a broken lock on one of the doors, it is only a matter of time before an unauthorized individual enters. Therefore, keeping software up to date is essential.

Several new vulnerabilities have been introduced into the digital world with the advent of **artificial intelligence (AI)**, the branch of computer science focused on creating intelligent machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. One beneficial use of AI is to generate complex passwords. However, the technology can also be used in damaging ways. For example, computer-generated voices have increased robocalls, causing excess cell network traffic, and have been used by attackers to exploit and steal money from victims in social engineering attacks. Attackers have also used this same technology to crack passwords through brute-force attacks.

LINK TO LEARNING

In early 2024, the Federal Communications Commission (FCC) made it illegal for companies to use AI-generated voices in robocalls. Read their press release related to voice cloning technology (https://openstax.org/r/109VoiceTech) to learn more about how companies use the technology and why the FCC has made it illegal.

Software updates not only provide new features and improve system performance, they also often deliver critical patches that resolve these vulnerabilities. Cybersecurity demands continuous monitoring and control from a proactive and reactive perspective. Unpatched systems may function normally, which can lead to a false sense of security. Breaches of such systems can compromise the entire network's integrity. The risks include unauthorized data access, identity theft, or even denial of service attacks that can bring business operations to a halt. By understanding the risks posed by software vulnerabilities, organizations can make educated decisions about how to protect their network assets effectively.

Hardware Vulnerabilities

Hardware vulnerabilities can be just as dangerous as software vulnerabilities, but they are often overlooked. A hardware vulnerability is a weakness or flaw within the physical components of a network, such as routers or IoT devices. For example, unsecured routers and other networking devices can be weak points in an organization's cybersecurity defenses. Imagine a router that's still using the default password or is not properly configured; it becomes an easy target for cyberattacks. While it may seem trivial, the hardware that connects your network to the outside world should be as secure as the information it is supporting.

Issues can also arise with IoT devices. These gadgets, such as smart thermostats and smart coffee makers, are increasingly popular but are not always designed with security in mind. Even in an environment where computer systems are well protected, these seemingly harmless devices can be weak points for cyber threats. Without robust security measures, such as strong passwords and regular firmware updates, IoT devices can be manipulated to spy on an organization or serve as a launch pad for broader network attacks. Recognizing these hardware vulnerabilities is the first step toward developing a more comprehensive approach to network security.

Configuration Issues

Poor configuration can be a significant threat to security. Default settings on hardware and software are especially dangerous because they often turn into easy entry points for cybercriminals. For instance, leaving administrative credentials at their factory settings can provide an all-access pass into sensitive systems, compromising the entire network's integrity. Similarly, poorly configured firewalls can be likened to having a state-of-the-art lock but leaving the key under the mat. Even advanced intrusion detection systems become largely ineffective if the firewall rules are not appropriately configured to filter malicious or unnecessary traffic. Poor configurations can lead to unauthorized access, data leaks, and theft of sensitive information.

Real-world incidents have underscored these risks. In 2017, the WannaCry ransomware attack exploited a vulnerability that could have been mitigated with proper security configurations.[5] The malicious software that encrypts users' files such as photos, documents, or other sensitive information and demands a ransom for their release is called **ransomware**. The WannaCry ransomware attack exploited a vulnerability in Microsoft Windows known as "EternalBlue," which allowed the attack to spread across networks, encrypting files along the way (Figure 5.4). Microsoft published a fix for the vulnerability; however, many organizations were slow to make the update, which ultimately resulted in organizations losing billions of dollars. Additionally, numerous data breaches have occurred due to misconfigured cloud storage solutions, exposing sensitive customer data to the public.[6] These incidents serve as cautionary tales, highlighting the need for mindfulness in system and network configurations.

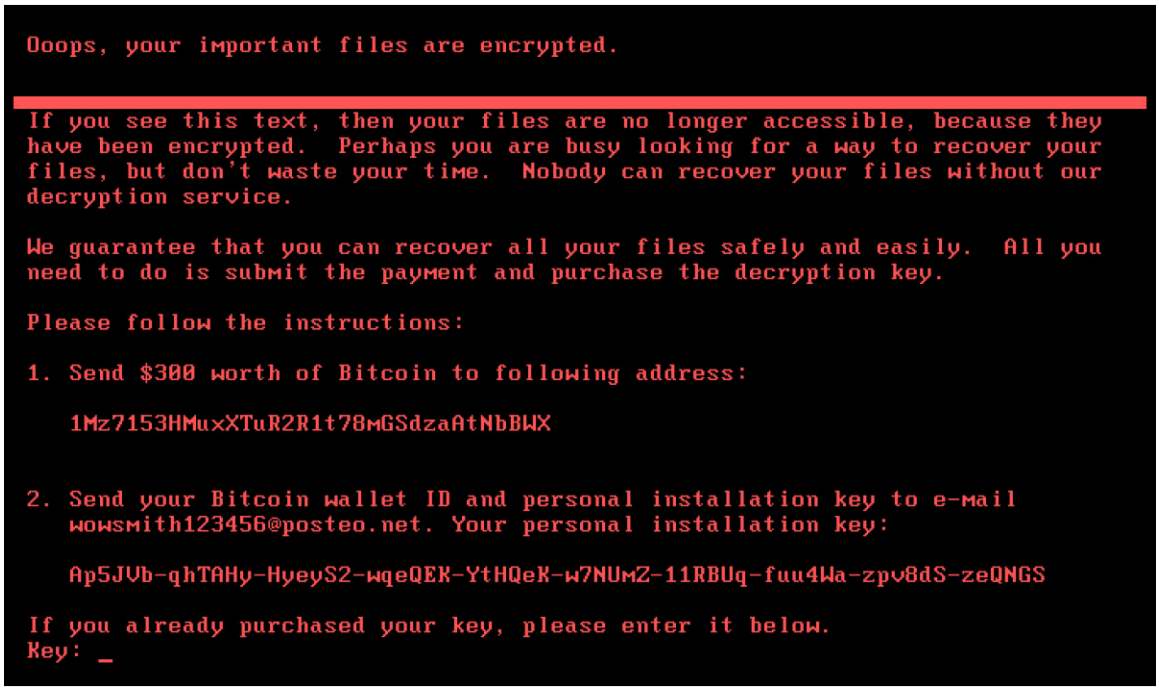

Figure 5.4 Ransomware such as Eternal Blue is malware that encrypts a user's files and demands payment in return for the decryption key. (credit: "Petya (malware)" by Petya/Wikimedia Commons, Public Domain)

Ensuring proper configuration is not just a task for the IT department but requires an organization-wide commitment to adhering to the best practices in cybersecurity. Properly configured settings are the first line of defense in a multilayered security approach, and lapses in this area can have catastrophic implications for any organization.

Types of Network Threats

As we navigate our day-to-day online activities at work, school, or home, there are multiple threats that we must mitigate for our safety. Threats from natural disasters and storms can disable a network, and threats from an external attacker can result in loss of operations or theft. Moreover, an internal threat that originates from within an organization can result in sabotage, data loss, or network compromise. There are three types of network threats: environmental, external, and internal, as Figure 5.5 illustrates.

5 Josh Fruhlinger, "WannaCry Explained: A Perfect Ransomware Storm," CSO, August 24, 2022, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html
6 Edward Kost, "Top 5 Security Misconfigurations Causing Data Breaches," UpGuard, updated November 18, 2024, https://www.upguard.com/blog/security-misconfigurations-causing-data-breaches

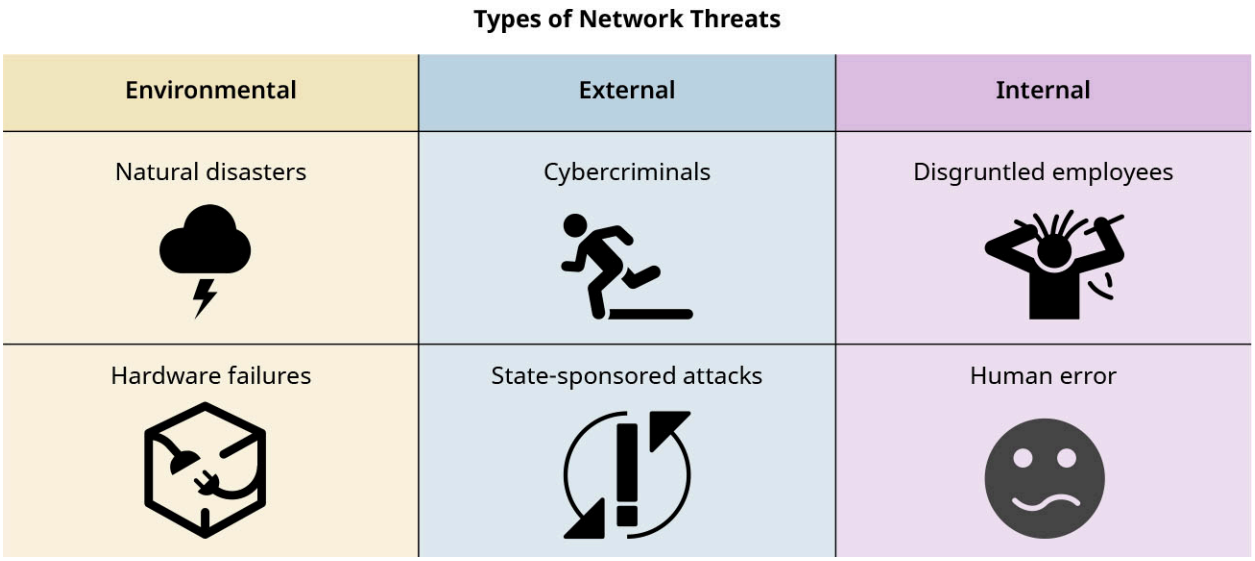

Figure 5.5 Network threats typically fall into three categories: environmental, external, and internal. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit top left: modification of work "Noun storm 2616921" by Uswatun Hasanah/ Wikimedia Commons, CC BY 4.0; credit top middle: modification of work "Noun Project 469419 Run Icon" by Gregor Cresnar/ Wikimedia Commons, CC BY 3.0; credit top right: modification of work "Noun frustration Luis 163554" by Luis Prado/Wikimedia Commons, CC BY 4.0; credit bottom left: modification of work "API - The Noun Project" by "Five by Five"/Wikimedia Commons, CC0 1.0; credit bottom middle: modification of work "Noun Project problems icon 2417098" by "Template, TH"/Wikimedia Commons, CC BY 3.0; credit bottom right: modification of work "Noun confused 274449" by Ben Davis/Wikimedia Commons, CC BY 4.0)

Environmental and External Threats

An **environmental threat** in cybersecurity is an uncontrollable external factor such as a natural disaster or hardware failure that can damage data centers and disrupt business operations. These threats often get overshadowed by the dramatic nature of hacker attacks and internal espionage, yet their impact can be equally catastrophic. For instance, natural disasters such as earthquakes, floods, or hurricanes can severely damage data centers that host critical information and applications. The inability to access or recover this data not only interrupts business operations, but can also have legal and reputational ramifications. Moreover, as these calamities are beyond human control, they are particularly difficult to mitigate. In recent years, the increasing frequency of extreme weather events attributed to climate change has escalated this environmental risk, necessitating an urgent review and adaptation of existing disaster recovery and business continuity plans.[7]

Another common environmental threat is hardware failure. Servers, storage systems, and networking equipment can wear out over time. Without proper monitoring and maintenance, these failures can cause data loss or service interruptions. Unlike natural disasters, hardware failures are often preventable through regular inspections, timely upgrades, and redundancy systems. Many organizations employ real-time monitoring tools that alert them to potential hardware issues before they escalate into full-blown failures. Nonetheless, the commonplace nature of these threats should not lead to complacency; both natural disasters and hardware failures require strategic planning, investment in robust infrastructure, and ongoing vigilance to ensure organizational resilience.

7 Renaud Guidee, "The Next Decade Will Be Defined by Climate Change and Cyber Risk," World Economic Forum, October 7, 2021, https://www.weforum.org/agenda/2021/10/the-next-decade-will-be-defined-by-climate-change-and-cyber-risks/

An **external threat** in this context refers to a threat that originates from outside an organization, typically posed by cybercriminals or state-sponsored attackers who aim to exploit vulnerabilities for financial or strategic gain. Cybercriminals often appear as resourceful yet malicious actors who continually refine their tactics to evade detection and maximize their gains. Various methods, such as phishing schemes, malware deployment, and ransomware attacks, are among their preferred tools. These individuals or groups are not the only external threats, however; state-sponsored attacks present an even more daunting challenge. Orchestrated by nations aiming to steal critical information or disrupt infrastructures, these attacks benefit from considerable resources and advanced capabilities, turning cybersecurity into a complex game of geopolitics.[8]

Understanding the techniques of these external threats is necessary for developing effective defensive measures. For example, a common method used by cybercriminals is **social engineering**, which involves manipulating employees into revealing sensitive information, often leading to unauthorized system access. At the other end of the spectrum, state-sponsored attacks might employ highly sophisticated methods such as advanced persistent threats (APTs) to gain and maintain long-term access to target networks. These types of threats can include software such as a rootkit or malware. A **rootkit** enables attackers to have access to a system by masquerading as operating system processes, and **malware** is malicious software designed to damage, exploit, or infect systems, or otherwise compromise data, devices, users, or networks, using viruses, worms, and spyware that is installed into the basic input-output system (BIOS) of a computer. While cybercriminals are motivated primarily by financial gains, state-sponsored actors often have a more complex agenda, which could include espionage, destabilization, or strategic advantage. This complexity demands a full understanding, not just of the technological aspects of these threats, but also of the political dimensions that underlie them.

Internal Threats

An **internal threat** is one that originates from within an organization, such as disgruntled employees or poor security training for employees resulting in social engineering attacks. In cybersecurity, internal threats are particularly tricky because they relate to the risk of someone inside a company using their access to systems to cause damage or steal data. While organizations spend a lot on protecting their assets from external hackers, the risks from within can be just as damaging. Disgruntled employees, for instance, already have access to the organization's network and thus can bypass one of the organization's first lines of defense. As the motivations of such people can range from revenge to financial gain, they function as unpredictable actors within the cybersecurity landscape. To further complicate matters, insider threats may not even be intentionally malicious; they could simply be employees who unknowingly compromise security through poor practices, such as using weak passwords or falling victim to phishing scams.

Understanding the risks from internal threats means thinking beyond just technical fixes. The human factor is an important factor. Organizations must create a workplace where employees feel comfortable talking about their concerns. This can help reduce the chances of anyone becoming disgruntled. Simultaneously, companies must implement robust monitoring systems to identify unusual activity that could signal an internal threat. By recognizing the multifaceted nature of internal threats, organizations can develop a holistic strategy that integrates technological, psychological, and administrative measures to safeguard their assets.

FUTURE TECHNOLOGY

The Future of Cyberattacks

Emerging technologies such as quantum computing and AI pose novel threats that organizations must

8 Adam Hunt, "State-Sponsored Cyberattacks Aren't Going Away—Here's How to Defend Your Organization," *Forbes*, May 10, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/10/state-sponsored-cyberattacks-arent-going-away---heres-how-to-defend-your-organization/?sh=7acb1aad230b

prepare for. Quantum computing, a method of computing that uses qubits (a measurement of four states as opposed to two), with its unparalleled computational speed, has the potential to break existing encryption algorithms, rendering most current data protection measures obsolete. Initiatives such as post-quantum cryptography are in the works to counter this impending threat, but widespread adoption and implementation remain a challenge.

Alternatively, AI-driven cyberattacks are becoming increasingly sophisticated. Advanced machine learning algorithms can quickly analyze network vulnerabilities and execute complex attacks with little to no human intervention. Moreover, these algorithms can adapt and learn from each cyberattack, making them more effective with each iteration. This intensifies the need for cybersecurity measures to evolve in tandem, incorporating AI-driven threat detection and response systems that can match the capabilities of next-generation threats. Therefore, staying abreast of these future trends is not just advisable; it is imperative for long-term security resilience.

5.2 Security Technologies and Solutions

Learning Objectives

By the end of this section, you will be able to:

- Identify technologies and solutions to protect information and networks
- Identify potential security threats and vulnerabilities, and choose appropriate countermeasures
- Describe best practices for secure computing and risk management
- Determine legal and ethical issues in securing information and networks

As technology continues to advance, protecting digital information and networks has become a top priority for individuals, organizations, and governments alike. With the rise of increasingly sophisticated cyber threats, it is essential to understand the tools and strategies available to safeguard sensitive data and critical infrastructure. Effective security requires not only the right technologies to defend against potential attacks, but also a solid understanding of how to identify vulnerabilities and implement measures that mitigate risk. In addition to technical solutions, secure computing practices and thoughtful risk management play a crucial role in maintaining system integrity. Furthermore, navigating the complex landscape of legal and ethical issues surrounding information security is vital, as the balance between privacy, compliance, and protection continues to evolve.

Technologies and Solutions to Protect Information and Networks

In cybersecurity, numerous technologies and solutions stand as defenses against an array of threats that aim to compromise information and network security. The field of **information security risk management (ISRM)** involves identifying, assessing, and mitigating risks to the confidentiality, integrity, and availability of information and information systems. From foundational measures such as firewalls and encryption protocols to specialized tools for intrusion detection and risk assessment, the complexities of maintaining a secure digital environment are wide-ranging. These technologies play critical roles in safeguarding both individual and organizational digital assets. Furthermore, these technologies can enable ISRM professionals to promote digital trust, a valuable tool for growth and success of businesses.

Firewalls

Firewalls serve an important role in network security, functioning as the gatekeepers that police the flow of data coming in and out of a network. Acting as the first line of defense, they are necessary in preventing potential cyber threats from external sources. The versatility of modern firewalls allows for a comprehensive approach to managing data flow. Advanced versions meticulously examine the content within a **data packet**, which is a small unit of data transmitted over a network, and differentiate various forms of web traffic such as

file transfers, browser activity, and applications accessing the internet, thus facilitating the implementation of nuanced security policies.

For instance, firewalls can authorize access to applications that have undergone rigorous vetting processes and are deemed safe while promptly blocking others that pose a potential security risk. These applications vary, ranging from video games seeking updates to activity in the background while browsing the internet.

Types of Firewalls

There are several types of firewalls, each with a distinct set of features and functionalities, but they are broadly categorized into hardware and software firewalls. The most basic type of firewall is a packet filtering firewall, which checks the header of packets as they pass through, looking for specific characteristics such as source and destination address, port number, and protocol used. They are usually software based, and they operate by examining packets of data to determine whether to allow them through based on preset rules.

A more advanced type of firewall is a stateful inspection firewall, which monitors active connections and uses that context to block or allow connections. These types of firewalls may be software or hardware based. A next-generation firewall (NGFW) is an advanced type of firewall that provides more comprehensive security features than traditional packet filtering and stateful inspection and uses a proactive approach to network security. These firewalls come equipped with integrated intrusion detection and prevention systems (IDPSs), offering an additional layer of security. These IDPS functionalities are engineered to actively scan for, identify, and neutralize known threats as they occur.

A proxy firewall is a network security device that filters incoming and outgoing traffic by acting as an intermediary between users and the web. It is software based and provides an additional layer of isolation and security.

Firewall Implementation Challenges

Firewalls are essential for **network security**, which is the process of guarding network infrastructure and IT systems from unauthorized access, misuse, malfunction, or improper disclosure to unintended parties. It involves using a variety of tools, technologies, and policies to ensure the safety and security of data traveling over the network. Configuring detailed security policies can get complicated, and there is a risk of false positives in intrusion detection. Plus, firewalls need regular updates to handle new threats, so they require ongoing maintenance. Despite these challenges, firewalls are an important part of any solid network security plan. To boost cybersecurity, it is smart to have backup plans in place. This also goes for hardware. Using two different firewalls from two different providers can add extra layers of protection and reliability.

Protocols

A **protocol** is a fundamental rule or procedure that governs communication between devices in a network. Protocols ensure that data are transmitted accurately, reliably, and securely by defining how data are packaged, transmitted, and received. Protocols operate at various layers of the network stack, addressing different aspects of communication. By standardizing communication processes, protocols enable interoperability between different systems and devices, making seamless and efficient digital communication possible. Think of them as rules that computers must obey, like how drivers must obey traffic laws. Common protocols include HTTP, HTTPS, VPN, and S/MIME.

Hypertext Transfer Protocol (HTTP) and its secure alternative HTTP secure (HTTPS) form the foundation of web communications (Table 5.2). **Hypertext Transfer Protocol (HTTP)** is proficient at transmitting hypertext over the internet, and **Hypertext Transfer Protocol Secure (HTTPS)** adds a secure, encrypted layer to HTTP via SSL/TLS protocols. To understand how HTTP works, imagine that you make a request for a web page through a browser. This happens when you click on a link or enter an address in the search bar of your browser, initiating an HTTP request. This request is sent to a web server, which then responds by supplying the requested information in the form of hypertext. This hypertext is what your browser interprets and displays as a web

page. The process is remarkably fast, enabling standardized and consistent viewing of websites across different browsers. Encrypting a connection ensures that the data in transit is secure. For ISRM professionals, understanding the importance of HTTPS over HTTP is essential, especially when dealing with sensitive information.

	HTTP	HTTPS
Security	Data are sent in plain text, making them vulnerable to interception	Data are encrypted, ensuring privacy and security; uses SSL/TLS protocols
Port	80	443
URL prefix	URLs begin with http://	URLs begin with https://
Trust	Does not provide a certificate to verify the website's identity	Provides a digital certificate issued by a certificate authority (CA)

Table 5.2 Comparing HTTP and HTTPS HTTPS provides much more security, whereas HTTP provides little to no protection.

Virtual private networks (VPNs) serve as a proxy for internet communication by establishing a private encrypted connection or tunnel that makes it difficult for attackers to breach. Various protocols such as Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and OpenVPN are used for different security and speed requirements. PPTP is fast but less secure, whereas OpenVPN offers a balance of speed and security. L2TP usually operates with IPsec for added security.

A Secure/Multipurpose Internet Mail Extension (S/MIME) is a standard for public key encryption and signing of MIME data. It is frequently used for securing email messages. S/MIME allows for cryptographic security services such as authentication and message integrity checks, ensuring that both the sender and the information remain uncompromised.

Intrusion Detection and Prevention Systems

In network security, an **intrusion detection and prevention system (IDPS)** monitors networks for malicious activity or policy violations. This is vital for keeping information secure. Think of protocols as a set of rules that allow machines to communicate smoothly. IDPSs, on the other hand, are specialized hardware and software tools that monitor network traffic to detect and prevent security breaches. These systems come in various forms and can be deployed in different ways to best protect against potential threats. By actively monitoring communications, IDPSs help prevent security incidents before they can cause harm. Signature-based IDPSs are designed to detect known threats by searching for specific patterns, such as malware signatures. Anomaly-based systems, on the other hand, focus on identifying abnormal patterns in data flow or behavior that might signify a security threat. Both have their own advantages and limitations; signature-based systems are highly effective against known threats but can miss new, previously unseen threats, while anomaly-based systems can detect novel threats but are prone to false positives.

Network-based IDPSs are used to monitor and analyze network traffic to protect an entire network from threats, whereas host-based systems are installed on individual devices and protect against unauthorized data manipulation or software vulnerabilities specific to those devices. These systems often rely on signature-based detection methods along with anomaly-based methods that look for unusual patterns in network traffic that could be harmful.

Monitoring Tools

The foundation of an effective information security strategy begins with simple and effective monitoring tools, such as log files, alarms, and keyloggers. Although these measures might appear basic, their importance cannot be overstated, especially when it comes to instilling a sense of digital trust.

A **log file** is a file generated by security applications that contains event information that aids in determining the status and health of a network. These are invaluable for diagnostics, troubleshooting, and security audits. An alarm is a protection device often installed on equipment to notify staff in the event of tampering or breach. It serves as a real-time alert system that notifies administrators of potential security threats. These are usually triggered by predefined conditions set within the IDPS or other security software. A **keylogger** is a tool or technology often used maliciously to capture keystrokes on a computer to obtain sensitive information such as passwords. Although they are often associated with malicious activities, legitimate versions exist for monitoring and auditing purposes. However, these tools must be managed carefully to ensure they do not compromise the very security they are meant to uphold.

In addition, the following tools are also used for monitoring network security:

- A **packet sniffer**, also known as a network analyzer or protocol analyzer, is a tool that captures and analyzes network traffic. It intercepts data packets flowing across a network, allowing for examination of the data within these packets, including their source, destination, and content. Packet sniffers can capture data packets in "promiscuous mode," meaning they can see all traffic on the network, not just traffic intended for the sniffing device. For example, Wireshark is a popular open-source packet analyzer that allows capture and analysis of network traffic.
- A **protocol analyzer** is a tool that examines network communication protocols to understand how data are exchanged between devices and applications on a network. Protocol analyzers capture and analyze data packets, decode them based on the protocol used, and provide insights into the communication process. They can identify errors, performance bottlenecks, and security vulnerabilities related to specific protocols. Protocol analyzers and packet sniffers are often used interchangeably, as they both involve capturing and analyzing network traffic. However, protocol analyzers focus more on understanding the communication protocols and analyzing the data within the context of those protocols.
- A **security information and event management (SIEM)** system is a security solution that collects, analyzes, and correlates security data from different sources to detect and respond to security threats in real time. SIEM systems gather logs, events, and alerts from various security tools and network devices, and then use advanced analytics to identify suspicious activity, potential vulnerabilities, and security incidents. SIEM helps organizations improve threat detection, incident response, security compliance, and overall security posture.

Best Practices for Network Threat Mitigation

In the complex domain of information security, best practices serve as guiding principles that are universally applicable across various sectors and organizational structures. They are the reliable methods that provide consistent security outcomes and contribute to the establishment of digital trust. Best practices in the information security field include the following:

- multi factor authentication (MFA), which adds an additional layer, or layers, of security, ensuring that even if one factor is compromised, unauthorized access is still restricted
- regular updates and patch management, the routine process of updating software to address security vulnerabilities, are ongoing, proactive measures that attempt to close the gap through which cyberattackers can infiltrate systems
- zero trust, or "never trust, always verify," a cybersecurity model where access to resources is granted based on strict verification and continuous authentication, rather than assuming trust based on network location or device ownership

- defense in depth, a cybersecurity strategy that employs multiple layers of security controls to protect against attacks, so that if one layer fails, others will still be in place to prevent a breach
- vendor diversity, the practice of using multiple vendors for different security products and services instead of relying on a single vendor to mitigate risks associated with vendor lock-in, reduce security vulnerabilities, and improve overall security posture
- security training and awareness programs, which educate employees about the importance of information security, the role they play in safeguarding organizational assets, and how to recognize phishing attempts, maintain password integrity, and ensure secure data transmission

The human element is often regarded as the weakest link in the security chain. By adopting these best practices, information security and risk management professionals not only enhance an organization's resilience against internal and external cyber threats, they also contribute positively to building digital trust, thereby enabling business to grow and thrive in an increasingly interconnected world.

Security Threats, Vulnerabilities, and Appropriate Countermeasures

Security threats and vulnerabilities are constantly changing, posing an ongoing challenge for organizations and individuals alike. As the IoT, machine learning algorithms, and other technologies integrate deeper into our lives, they offer an attack surface for malicious actors. The stakes are not just financial or operational; they traverse digital trust, which is a confidence in the ability of processes, technology, and organizations to create a secure digital world. Digital trust is a valuable notion that protects organizational branding and confidence. When digital trust is compromised, it significantly impacts the organization and its stakeholders, including customers, partners, and regulators.

For example, in 2024, New Hampshire voters filed a lawsuit against the creators of a deepfake robocall that used AI to generate a fake audio message of former president Joe Biden asking voters to stay home and not go to the voting booths or poll stations.[9] Conceptually, such deepfake scams typically involve creating realistic audio or video imitations of trusted figures to deceive individuals into taking unauthorized actions. When these scams are uncovered, consumers lose their digital trust in the organization that created them. People are naturally protective of their assets, valuables, and identity, all of which they perceive as threatened when they see an organization misusing digital assets. Through a detailed understanding and implementation of security mechanisms, individuals and organizations can defend against threats and build resilient systems that adapt to new challenges as they arise.

Types of Threats

As the internet has gathered more users over the last few decades, cyberattacks have significantly increased. These attacks vary greatly, consisting of password attacks, phishing attempts, Trojan viruses, malware, and ransomware that holds users' sensitive files hostage for ransom payment. Understanding these attacks and how to prevent them is key to information security.

As the most fundamental of access controls, passwords are a frequent target of malicious actors. Two primary types of password attacks exploit weaknesses in password security: brute-force attacks and dictionary attacks. In a **brute-force attack**, an attacker systematically checks all password or encryption key possibilities until the correct one is found. In contrast, a **dictionary attack** uses a precompiled list of likely passwords. Imagine trying to crack a padlock with four digits, each ranging from 0 to 9. If you don't have any hints, you'd have to try every possible combination, which adds up to 10,000 different permutations (10^4), which is a lot of guessing.

Now, consider a dictionary attack. Instead of trying every single combination, a dictionary attack gives you a list of likely combinations based on common patterns or known sequences. This way, you might find the

9 Ali Swenson and Will Weissert, "New Hampshire Investigating Fake Biden Robocall Meant to Discourage Voters Ahead of Primary," *Associated Press*, updated January 22, 2024, https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5

correct code faster. To guard against both types of attacks, organizations implement stringent password policies that encourage complex combinations, and they use MFA.

Phishing attacks aim to trick individuals into revealing sensitive information. The attacker often masquerades as a trustworthy entity, employing emails or messages (Figure 5.6) that prompt users to enter passwords or other confidential data. Implementing robust email filtering technology and educating users about the elements of phishing schemes are critical components of a well-rounded defense strategy.

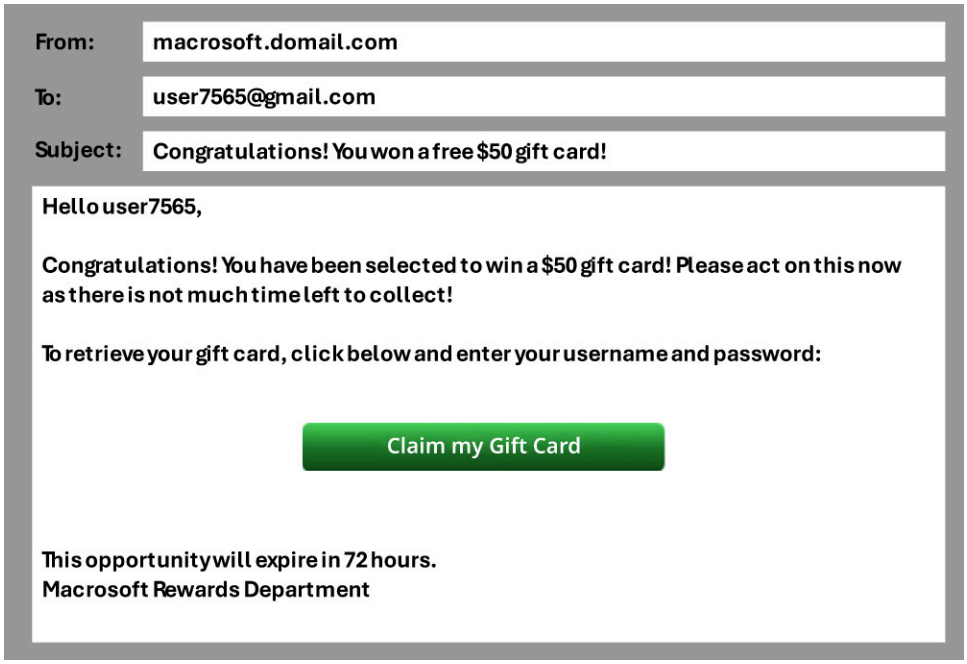

Figure 5.6 Many phishing attempts will appear to originate from a trusted source. However, on careful inspection, one can notice several discrepancies that discredit the attempt. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

By weaving these basic security measures into an integrated strategy, ISRM professionals can better arm organizations against a range of threats. Simple security measures serve both as a first line of defense and as foundational elements that support more complex security protocols. This layered approach to security helps maintain digital trust, fostering an environment where businesses can operate with greater confidence in the digital realm.

Among the most frequently encountered security threats are malware variants such as viruses, worms, and Trojans (Figure 5.7). A **virus** attaches itself to clean files and propagates to other files and programs. A **worm** is a stand-alone software program that spreads without requiring a host program. A **Trojan** is a program that conceals itself as a safe program but often carries many other different types of malicious payloads.

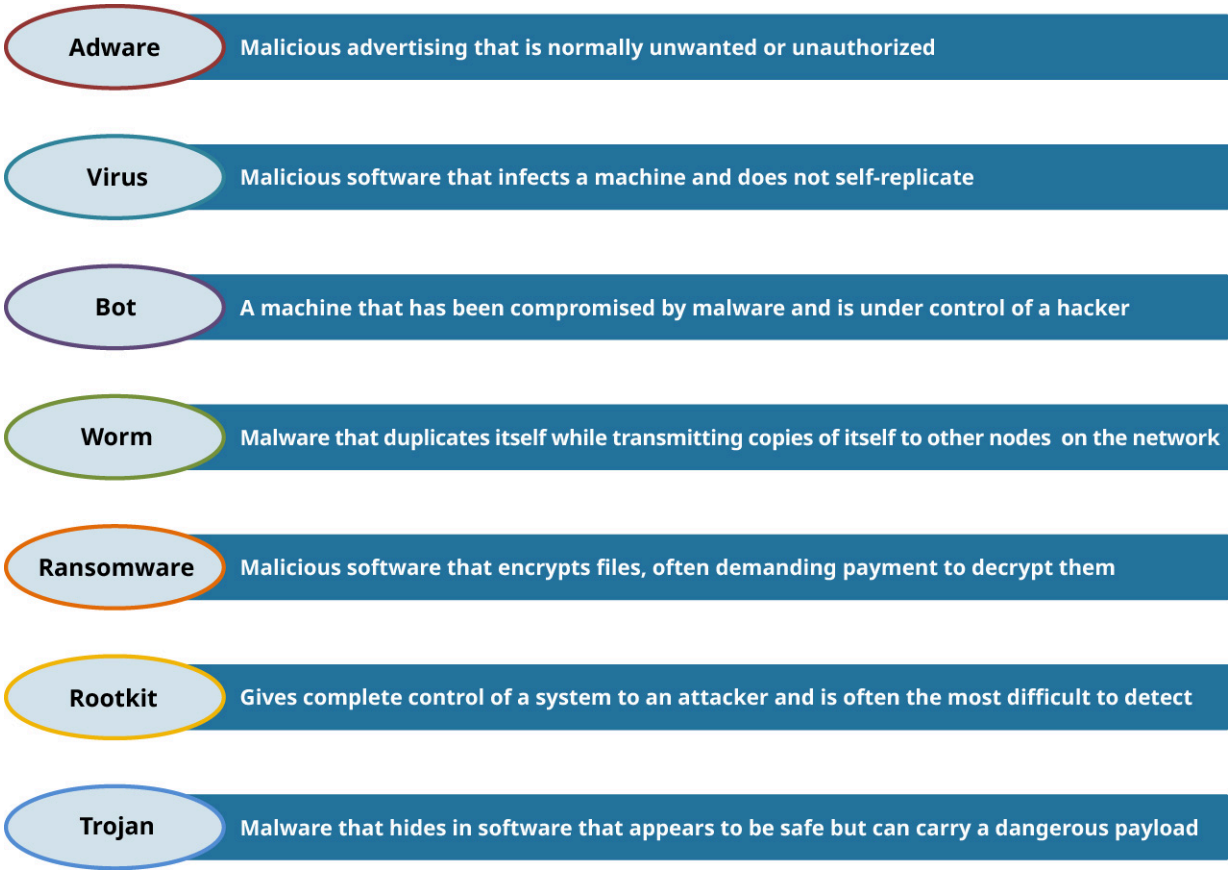

Figure 5.7 While not an exhaustive list of malware, these are the most common types. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Malware such as Trojan horses and ransomware represent more sophisticated external threats. Trojans trick users into willingly downloading malicious software that is often disguised as a legitimate program. The software provides attackers unauthorized access to systems. Advanced endpoint security solutions coupled with regular updates and patches can offer significant protection against these types of malware.

In recent years, more insidious forms of malware such as fileless malware have emerged. Unlike traditional malware, which relies on files stored on the hard disk, **fileless malware** exploits in-memory processes to conduct its nefarious activities. By leveraging legitimate system tools such as PowerShell or Windows Management Instrumentation, fileless malware conducts operations entirely within the device's random access memory (RAM), leaving little to no footprint on the hard disk. This makes it significantly more challenging for traditional antivirus solutions to detect and eliminate. For a better understanding of how fileless malware works, look at how Figure 5.8 follows a user’s click in a spam email.

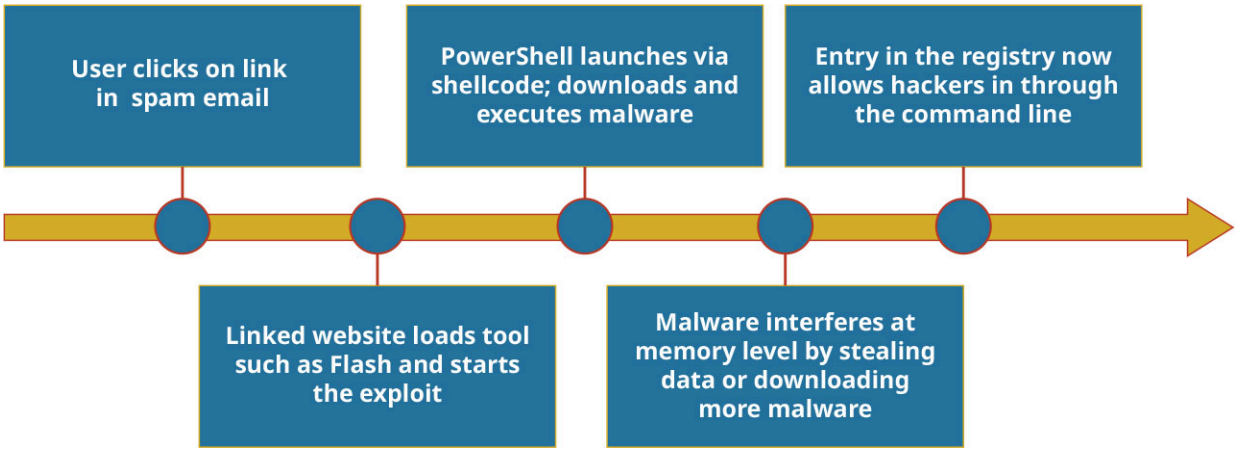

Figure 5.8 This example demonstrates how fileless malware operates. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

In contrast to software-based threats, which target vulnerabilities in computer systems, social engineering attacks such as phishing and pretexting leverage human vulnerabilities. A social engineering attack includes deceptive tactics used to manipulate individuals into divulging confidential information, exemplified by phishing and pretexting. Phishing usually involves sending deceptive emails to trick employees into revealing sensitive information. On the other hand, **pretexting** involves creating a fabricated scenario to obtain private data. Despite the sophistication of technical countermeasures, the human factor remains a vulnerability, making these types of attacks especially harmful to the establishment of digital trust.

An insider threat is a risk posed by individuals within an organization who have access to sensitive information and systems; they warrant special attention because employees or contractors with insider information can perpetrate or facilitate attacks that may bypass conventional security measures. This "inside advantage" makes the threat more complex, as mitigating such threats requires a blend of technical controls and organizational policies.[10] Some of these policies include actions such as mandatory vacations to prevent fraud, role-based access controls that limit employee access to sensitive information, security awareness training, and regular audits.

A **distributed denial-of-service (DDoS)** is an attack that uses multiple computers or servers to overwhelm a network, resulting in loss of usability. These pose a unique threat: unlike other attacks that seek to gain unauthorized access or retrieve sensitive information, DDoS attacks aim to incapacitate the target's operations. The immediate impact is not just operational disruption, but also a severe degradation of digital trust among stakeholders.

Vulnerabilities

One of the most well-known software vulnerabilities is the **buffer overflow**, a condition where an application writes more data to a buffer than it can hold. This results in data corruption and could allow an attacker to execute arbitrary code. Another common vulnerability is Structured Query Language (SQL) injection, which occurs when attackers insert or manipulate SQL queries in an input field, allowing them to gain unauthorized access to a database. This kind of attack can lead to data leaks, loss of data integrity, and other security issues.

Attacks on firmware (hardware) are increasingly prevalent. These are more difficult to detect as they target the device at the BIOS or firmware level. This also makes it harder to remove the malware once in the system. Physical tampering, while straightforward, is another hardware vulnerability. Unauthorized physical access to hardware can result in the installation of keyloggers or data extraction.

10 Cybersecurity and Infrastructure Security Agency, "Defining Insider Threats," accessed October 12, 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Although cyber threats often originate from the application of sophisticated hacking techniques, it is not uncommon that the root cause of a breach can be traced back to a simple configuration error. The T-Mobile data breach of 2023, where a third of its customer base had private information exposed, shows what can occur when application programming interface (API) configurations are not sufficiently secured.[11] An API is a set of protocols, tools, and definitions that enable different software applications to communicate and interact with each other, allowing for the exchange of data and functionality. In this breach, insecure APIs allowed threat actors to access sensitive customer data, impacting not just the affected individuals, but also T-Mobile's reputation. As more companies transition their services to the cloud, the risk posed by insecure API configurations is escalating.

Countermeasures for Threats

Countermeasures to mitigate cybersecurity threats involve a diverse set of tools and approaches. They often need to be tailored to the specific types of threats and vulnerabilities that an organization faces, but some universally applicable solutions have proven effective across multiple sectors.

- Antivirus and anti-malware software: The most basic but critical line of defense is antivirus and anti-malware software. These programs provide real-time protection against known threats and offer heuristic analysis to detect previously unknown forms of malware.
- Employee training and awareness: Human error remains one of the most significant vulnerabilities in any organization. Phishing simulations and awareness training can drastically reduce the likelihood of an employee inadvertently compromising security. A 2024 study has shown that a combination of phishing awareness programs and phishing testing programs can significantly reduce the click-through rate on phishing emails.[12]
- Intrusion detection systems: An intrusion detection and prevention system is vital to monitoring network behavior for unusual or suspicious activity.
- Access control policies: One method of access control, **role-based access control (RBAC)**, bases data access on a person's role in the organization, giving each employee the minimum level of access they need to perform their job functions. This requires an organization to maintain a complete list of data elements combined with a list of viewable roles and attributes. For example, a health-care organization can successfully thwart an internal threat by limiting access to patient records to only those employees who require it for their job duties. Given the complexity and ever-evolving nature of cyber threats, these countermeasures serve as foundational elements in the continuous effort to uphold digital trust.
- Regular software patching: One of the most effective ways to mitigate vulnerabilities is through timely software patching. In 2017, the WannaCry ransomware attack exploited a vulnerability in older Windows systems. Microsoft had issued a patch months before, but because many organizations had not updated their systems, this led to widespread damage.[13]
- Physical security measures: Physical intrusion can bypass the most sophisticated digital security measures. One type of social engineering known as tailgating is a good example of this. Tailgating is the act of following someone very closely as they enter a secured building. This enables the attacker to enter the facility without having to use credentials such as an ID badge. Once inside, the attacker has access to critical infrastructure and can cause a data breach or other damage. Strict controls such as mantraps, which prevent more than one person from entering a facility simultaneously, help to mitigate this threat.

Additional Practices for Secure Computing and Risk Management

Cybersecurity threats are always changing, and vulnerabilities can pop up when least expected. That is why

11 "T-Mobile Informing Impacted Customers about Unauthorized Activity," T-Mobile, January 19, 2023, https://www.t-mobile.com/news/business/customer-information
12 Gry Myrtveit Gundersen, "Does Phishing Training Work? Yes! Here's Proof," *CyberPilot*, January 5, 2024, https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof
13 Josh Fruhlinger, "WannaCry Explained: A Perfect Ransomware Storm," CSO, August 24, 2022, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html

prevention should be the cornerstone of any threat mitigation strategy. Organizations need to tackle cyber threats with proactive strategies, using secure computing and risk management practices that are both thorough and flexible.

Ethical Hacking

The process of attempting to break into an organization's computer systems, network, or applications with permission to identify vulnerabilities is called **ethical hacking**. It has gained considerable attention as a much-needed practice within the cybersecurity field. While the goals of ethical hackers align with those of cybersecurity experts in identifying vulnerabilities, the methods employed can resemble those of malicious hackers. This raises questions regarding the ethical and legal boundaries that distinguish ethical hacking from unauthorized, illegal activities.

The concept of consent is fundamental in ethical hacking. Unlike malicious actors, ethical hackers operate with explicit permission from the organization that owns the system. This consent is often given under a legal contract that outlines the extent of the testing, the systems that can be assessed, and the methods that can be used. Consent provides the ethical and legal basis for the hacking activities, turning what could otherwise be considered an illegal breach into an accepted practice.

One example that illustrates the gray area in ethical hacking is a 2019 case involving a cybersecurity firm. Two of its ethical hackers were arrested in Iowa while conducting a physical security assessment of a courthouse. Despite their having a contract that permitted them to perform physical intrusion testing, the authorities arrested them, and the hackers faced criminal charges. This was particularly surprising because the cybersecurity company had been hired by Iowa's judicial branch to conduct the assessment.[14]

This incident highlighted the potential ambiguity and legal risks involved in ethical hacking, even when it's conducted under a contract. It sparked an extensive debate in the cybersecurity community about the legal safeguards needed for ethical hackers. The charges against the two ethical hackers were eventually dropped, but not without the individuals and the firm suffering reputational damage. The case became a watershed moment for ethical hacking, urging the community, lawmakers, and organizations to be more explicit in contracts and to establish clearer legal guidelines.

This case serves as reminder that ethical hacking is a field still very much in the process of defining its legal and ethical contours. There is a clear need for explicit and transparent guidelines for ethical hackers and legislators, and they need to maintain an ongoing dialogue to build a more robust legal framework.

CAREERS IN IS

The Role of Ethical Hackers

Ethical hackers are security professionals with specialized training in simulating cyberattacks under controlled conditions. Their role is to systematically assess the security posture of an organization by conducting targeted tests first to identify and then to exploit vulnerabilities in software, hardware, and operational procedures. They conduct penetration testing that simulates real attacks by scanning systems, then attempting to breach them, and then determining how deep they can get into the system. Ethical hackers can also perform security audits and assessments and report the results of their penetration testing and audits to the organization with recommendations for improving the security. An organization may also hire an ethical hacker for continuous monitoring. Their work must fall within all laws and standards, following guidelines from the Open Web Application Security Project (OWASP) or standards from the National Institute of Standards and Technology (NIST). All ethical hackers must have authorization from the organization, maintain integrity of the system and data, and maintain confidentiality when handling

14 Faegre Baker Daniels, "Coalfire Investigation Report," October 9, 2019, https://www.iowacourts.gov/collections/445/files/919/embedDocument

data.

Risk Management Approaches

Risk assessments are important for identifying vulnerabilities and determining how they impact organizational objectives. These assessments can be either quantitative or qualitative in nature (Table 5.3).

Qualitative Risk Assessment	Quantitative Risk Assessment
Uses subjective criteria such as expert opinions and likelihood scales	Uses numerical data and statistical methods
Uses data from interviews and observations	Uses measurable data such as historical records and figures
Usually returns more descriptive insights	Information returned is generally descriptive in nature
Requires less in terms of tools for analysis	Normally requires more resources and analysis tools
Suited best for situations where exact data are not available	Preferred for risks that can be accurately measured

Table 5.3 Comparison of Qualitative and Quantitative Risk Assessments Qualitative assessments are subjective, whereas quantitative assessments are objective.

Before organizations can assess risks, they should try to determine two factors: their appetite for it and their level of tolerance. A **risk appetite** refers to the level of risk an organization is willing to accept in pursuit of its ambitions or goals and is more qualitative in nature. It is a strategic outlook set by top management and influences how resources for security measures are allocated. Unlike risk appetite, **risk tolerance** is the number of unfavorable outcomes an organization is willing to accept while pursuing goals and other objectives. It is more operational and quantitative than risk appetite, using statistical probability to identify potential risk outcomes. It defines the boundaries of risk variations that are acceptable during the execution of specific projects or processes. In a cybersecurity setting, addressing risk tolerance could include prioritization strategies on how resources are allocated on a network, the network credentials of employees, and budget allocation for IT management. One example of this is a company that allows their ethical hackers to monitor malicious and dangerous sites to identify potential threats. While this is a proactive approach to identifying new threats, monitoring outside threats does not come with the same explicit permission an ethical hacker would have to penetrate the organization's systems. The hacker would need to be especially careful not to violate the site's terms of service or acceptable use policies.

Frameworks for Risk Management

In the world of information security, frameworks play a very important role in managing and controlling risks. A framework is a structured set of guidelines and best practices that help an organization to implement, manage, and maintain security protocols. There are many frameworks to guide risk management practices. One recognized model is NIST's Cybersecurity Framework. The NIST framework is widely adopted due to its user-friendly nature and applicability across many sectors. Moreover, it aligns well with other standards and is scalable to the size of the industry. The NIST framework is divided into five core functions (Figure 5.9).

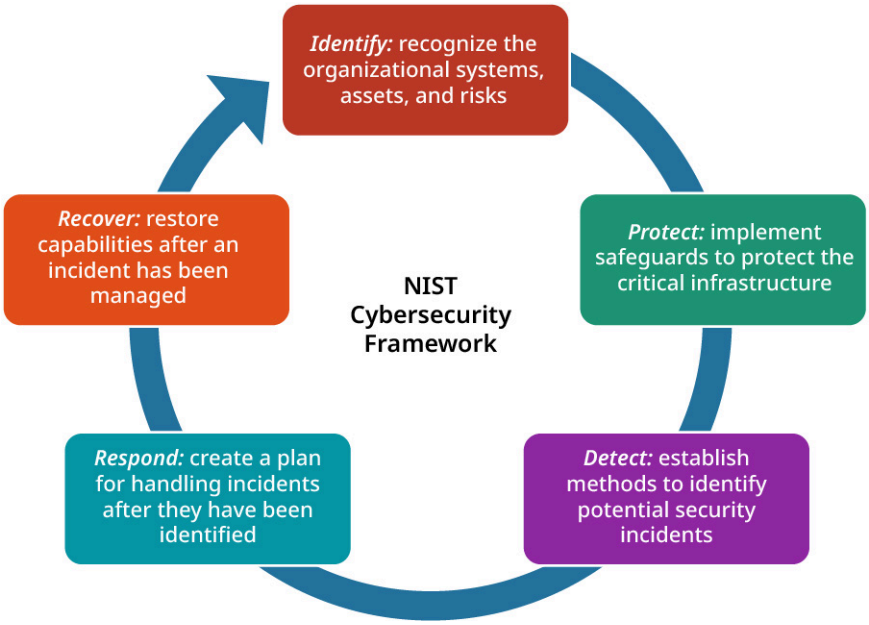

Figure 5.9 The five steps of the NIST process for risk management are to identify, protect, detect, respond, and recover. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The NIST framework provides a flexible and cost-effective approach to improving cybersecurity across industries. It is designed to be adaptable to organizations of all sizes and is widely used to strengthen cyber defenses.

Building a Culture of Security

As you've learned, human error or negligence often poses a significant information security risk. Implementing technical solutions is only part of the equation; the other part lies in fostering a strong security culture within an organization. Training programs and regular awareness sessions can provide employees with the necessary skills and knowledge they need to serve as the organization's first line of defense. Training can help them recognize phishing attempts, use strong passwords, and follow security best practices. Educating staff on proper behavior is key to reducing the risk of human error and preventing security breaches.

Legal and Ethical Issues in Securing Information and Networks

Compliance with laws and regulations is a required aspect of cybersecurity. These regulations not only protect the digital privacy of citizens, but also provide a mechanism of action for those whose rights are violated. Some examples of regulations are the General Data Protection Regulation (GDPR), which impacts data storage and sharing practices within the EU, and the Payment Card Industry Data Security Standard (PCI DSS), which lays out regulations for organizations that handle credit card transactions. As new threats emerge, regulations like these can change frequently, especially as attackers gain access to new technologies and attack methods. Being caught not complying with regulations can lead to heavy penalties or even legal action. Thus, regular updates and audits are vital in ensuring continuous compliance with current regulations.

Understanding the relationship between legal frameworks and ethical considerations is critical for legal compliance and maintaining stakeholder trust and safeguarding organizational reputation. With the expansion of digital technologies into every aspect of daily life, compliance with legal and ethical norms and guidelines becomes not just advisable but essential. Not adhering properly to such norms or guidelines can result in severe ramifications, ranging from legal penalties to a loss of customer trust. Moreover, noncompliance can irreparably harm an organization's standing in the global market.

Legal Protections Afforded to Employees and Users

There are legal guidelines in place that affect every stakeholder in an organization to protect them from harm.

Understanding these protections is essential for organizations to protect their users, human capital, and assets. Increasingly, employees who report cybersecurity lapses are protected by whistleblower laws. This protection introduces an additional layer of legal complexity for organizations. Disciplinary actions against employees who report cybersecurity issues can lead to legal repercussions, such as lawsuits and regulatory action. One way to avoid such situations is to emphasize the need for a robust internal reporting and response mechanism.

User Agreements and Legal Recourse

End-user license agreements (EULAs) and terms of service (ToS) often contain clauses related to data security and privacy. However, these agreements are coming under increasing scrutiny for being "contracts of adhesion," giving consumers little negotiating power. In the context of cybersecurity, these agreements frequently encompass clauses specifically related to data security and privacy, outlining the responsibilities of service providers in protecting user data and detailing the measures taken to prevent data breaches and cyberattacks.

As cybersecurity incidents become more prevalent, courts are beginning to scrutinize these agreements more closely, particularly assessing whether they provide adequate protection to users against cybersecurity threats. This shift in legal perspective is significant as it could lead to more stringent requirements for cybersecurity measures in user agreements, offering enhanced legal recourse to consumers in cases of lax cybersecurity practices. The evolving legal landscape around EULAs and ToS underscores the need for robust cybersecurity measures and fair user agreements to maintain digital trust and legal compliance.

Regional Laws, Intellectual Property Rights, and Consequences

Regional laws and their implications can serve as critical indicators of how various jurisdictions respond to the challenges posed by cybersecurity and data protection. In the United States, for instance, the California Consumer Privacy Act (CCPA) serves as a legislative example that is often considered to be the most stringent data protection law in the country. Not only does it allow Californians to understand what personal data are being collected about them, it also gives them the ability to deny the sale of their data.[15]

One of the most challenging aspects of cybersecurity law is the notion of jurisdiction in cyberspace. An organization based in one country may store data or have data centers in another. This poses questions about which laws apply and how they can be enforced. For instance, a European company with U.S.-based clients will need to consider both GDPR and any relevant U.S. laws.

Navigating jurisdictional conflicts can be quite complex for organizations. To handle these challenges effectively, it is essential to have a solid grasp of international law as it applies to cyberspace. This knowledge is becoming increasingly important as businesses expand globally, each country bringing its own set of regulations and requirements. Staying current with these diverse legal landscapes is not just good practice, it is necessary for maintaining compliance and ethical standards in today's digital world. GPDR and laws like it have had a major impact on how companies respond to takedown requests for data and how they protect data in storage and transit. Failure to comply with these regulations has resulted in substantial fines.

LINK TO LEARNING

TechTarget provides news and trending topics (https://openstax.org/r/109TechTarget) in security.

Intellectual property rights, particularly copyright laws, are a crucial element in the digital domain. These laws grant the creators of original works exclusive rights to their intellectual property, allowing them to control the distribution, modification, and public performance of their creations. In cybersecurity, this can include

15 "AB-375 Privacy: Personal Information: Businesses," California Legislative Information, June 29, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

software code, databases, and even certain types of algorithms, beyond the more traditional forms of media such as text, images, and music.

Copyright infringement in the digital age has developed into an important topic due to the ease of data replication and dissemination. Whether it is pirated software, illegal downloading of copyrighted music or movies, or unauthorized distribution of proprietary information, infringement can have a significant financial impact for an organization that relies heavily on copyrighted material for their business operations. They can lose substantial revenue, which could, in turn, affect their ability to innovate and compete. The legal consequences for infringement can range from fines to imprisonment.

Moreover, copyright infringement can result in a cascade of legal disputes that may involve multiple jurisdictions, especially if the data are stored or transmitted across borders. This complexity can strain resources as companies are forced to engage in lengthy and costly legal battles. For cybersecurity professionals, understanding the subtleties of copyright laws and their enforcement mechanisms is essential not just for risk mitigation, but also for ensuring ethical conduct in an organization's digital operations. This underscores the need for a robust copyright protection strategy as a part of an organization's overall cybersecurity posture.

In addition to copyright infringement, organizations face substantial legal consequences for failing to protect intellectual property (IP). Laws protecting intellectual property, such as patents, copyrights, and trade secrets, can be leveraged to file lawsuits against organizations that fail to protect these assets adequately. The legal ramifications can include both civil and criminal penalties, such as fines and, in extreme cases, imprisonment for key decision-makers within the organization.

Gaining unlawful access to computer systems can lead to criminal charges, often categorized under statutes like the Computer Fraud and Abuse Act (CFAA) in the United States. Such charges can result in imprisonment and hefty fines for individuals. The key element in such cases is the concept of "unauthorized access," which covers activities ranging from hacking into networks to merely exceeding the limits of authorized access.

ETHICS IN IS

Digital Privacy and Law Enforcement

A notable case that underscores the ethical dilemma faced by law enforcement regarding information security involves the FBI's handling of the iPhone belonging to one of the terrorists involved a December 2015 shooting in San Bernardino, CA. The FBI secured a court order requiring Apple to create a software bypass to the phone's encryption. Apple resisted,[16] sparking a national debate over the ethics of privacy and security. After Apple's refusal to create a bypass for the shooter's six-digit pin, the FBI found a small Australian company that had created an effective iPhone hacking tool that allowed them to break into the phone.[17] Although this meant that Apple was able to avoid creating a potentially dangerous tool that could compromise the safety and privacy of all Apple customers, there was one that already existed. The FBI was able to use this tool to work around the legal fight, but it did not resolve the ethical battle. The core of that ethical dilemma rested in balancing the need for national security and the investigation of a terrorist act against the protection of privacy rights and the potential implications of creating a vulnerability that could be exploited by others.

16 Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, https://www.apple.com/customer-letter/
17 Adam Entous, "The FBI Wanted to Hack into the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/

5.3 Information Security and Risk Management Strategies

Learning Objectives

By the end of this section, you will be able to:

- Identify the key components and principles of an effective ISRM strategy
- Describe various compliance frameworks and regulations related to information security and risk management and how they are used
- Develop a comprehensive risk management plan
- Determine the importance of continuous monitoring and improvement of the ISRM strategy

It is essential for today's organizations to have a well-crafted information security and risk management (ISRM) strategy, which is a structured approach to managing an organization's security processes, tools, and policies to mitigate risk. Organizations may be attracted to the capabilities of emerging technologies, but they must also recognize that it is imperative for them to safeguard their physical and digital assets. Not only does a well-structured ISRM strategy protect against data breaches and cyberattacks, it also serves as a mechanism for managing the organization's overall risk exposure.

Key Objectives, Principles, and Components of ISRM Strategy

ISRM does not merely involve deploying the latest security technologies or adhering to compliance regulations, although these are important. Its primary purpose is to develop a composed set of practices to protect an organization's informational assets and data infrastructure. A robust ISRM strategy aims to achieve three fundamental objectives: to safeguard organizational assets, to prevent data breaches and cyberattacks, and to reduce overall risk exposure. These objectives are embedded into the core components and principles that define the ideal ISRM strategy.

With cybercriminals employing increasingly sophisticated techniques, from social engineering to advanced malware, the need for proactive cyber defense mechanisms has also been increasing. These mechanisms should ideally include, but not be limited to, network monitoring, penetration testing, and employee training on cybersecurity best practices. A proactive approach can significantly reduce the probability of a successful attack, thereby preserving stakeholder trust and ensuring data integrity.

Another objective of ISRM is to reduce an organization's overall risk exposure. This involves not only implementing technological solutions, but also facilitating a cultural shift within the organization toward prioritizing cybersecurity. By conducting regular risk assessments, adopting a layered security approach, and encouraging a culture of cybersecurity awareness, organizations can significantly mitigate the risks they face. In doing so, organizations can protect their assets while simultaneously positioning themselves favorably in a competitive market where consumers and clients are becoming increasingly savvy about data security. To establish and maintain an effective ISRM strategy, several core components must be diligently addressed and continually refined. These include risk assessment, policy development, control implementation, training and awareness, monitoring and auditing, and response and recovery.

Risk Assessment

Risk assessment involves identifying potential threats and vulnerabilities, and the impact they could have on an organization's assets. It requires a thorough understanding of the organization's infrastructure, data, and business processes. By employing methodologies such as threat modeling and vulnerability assessments, organizations can prioritize risks based on their likelihood and potential impact, enabling them to allocate resources more effectively.

Policy Development

Policy development follows risk assessment as a critical step in articulating the organization's stance on various security issues. Policies provide a formal set of guidelines that dictate how assets should be protected

and how security incidents should be managed. These policies should be clear, concise, and easily understandable, ensuring that all stakeholders, from the CEO to the newest employee, are on the same page regarding security expectations and responsibilities. Additionally, IT managers should ensure that the organization maintains adequate documentation such as acknowledgment forms and training records to track employee training.

Control Implementation

Control implementation involves putting into place the necessary safeguards to mitigate identified risks. These controls can be administrative (policies and procedures), technical (such as firewalls and encryption), or physical (like security cameras and access controls). The key is to establish a balanced mix of these controls to create a multilayered security environment. Control effectiveness should also be regularly reviewed to ensure they are performing as intended.

Training and Awareness

Training and awareness programs are essential for cultivating a culture of security within an organization. Employees are often the first line of defense against cyber threats, so it is vital that they are equipped with the knowledge and tools they need to recognize and respond to potential security incidents. Regular training sessions, coupled with awareness campaigns, can significantly reduce the risk of human error, which is a leading cause of data breaches.

Monitoring and Auditing

Monitoring and auditing are crucial for maintaining visibility over the organization's security posture. Continuous monitoring of network traffic, user activities, and system configurations ensures that any anomalous behavior can be detected and addressed promptly. Auditing provides a retrospective analysis, helping to uncover security lapses and ensure compliance with relevant laws and policies.

Response and Recovery

Finally, response and recovery involve being prepared to act when a security incident occurs. An organization should have in place a plan for **incident response**, which is a predetermined set of procedures and steps taken to identify, investigate, and respond to a potential security incident. After identifying the breach, an organization should have procedures for containing the threat, eradicating the malicious elements, and recovering any lost data. Post-incident analysis is also important, as it provides insights that can be used to strengthen the organization's defenses against future attacks.

By effectively addressing these core components, organizations can build a resilient ISRM strategy that can protect their assets, maintain stakeholder trust, and ensure the continuity of their operations. Each component is important, and only when they are seamlessly integrated can an organization truly safeguard itself in the digital age.

Compliance Frameworks and Regulations Related to ISRM

In the context of ISRM, a compliance framework is a set of guidelines and best practices designed to help an organization comply with legal, regulatory, and technical standards. It serves as the foundation of secure and resilient organizational practices. These frameworks provide a structured set of guidelines and best practices that are designed to aid organizations in safeguarding their digital assets and ensuring their adherence to the CIA triad. Additionally, these frameworks help to establish a foundation for security practices, aligning organizational processes with industry standards and thus ensuring legal and regulatory compliance.

For organizations aiming to support their security posture and maintain the trust of their stakeholders, adhering to regulations not only mitigates the risk of legal repercussions, but also fosters a culture of continuous improvement and due diligence in security practices.

Table 5.4 shows some of the frameworks that are often used to provide guidance for stakeholders as they seek

to stay within the boundaries and laws of their organization's host government.

Framework	Description
ISO/IEC 27001 Information Security Management Systems Requirements	• International standard for ISRM • Provides a framework for constant improvement of an ISMS • Takes more of a risk-based approach to managing and securing sensitive information • Provides a structured methodology for compliance with best practices in information security
National Institute of Standards and Technology (NIST)	• Provides a framework for improving cybersecurity in multiple sectors • Flexible and adaptable to many fields • Consists of five core functions: identify, protect, detect, respond, and recover
NIST-800-137 NIST Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"	• More specialized framework that provides comprehensive guidelines and best practices in cybersecurity • Provides detailed guidance on specific areas such as risk management, security controls, incident response, and information system security

Table 5.4 Common Frameworks Used in ISRM An organization may use multiple frameworks in developing a robust ISRM strategy.

ISO/IEC 27001

ISO/IEC 27001 is a globally recognized standard for the establishment and certification of an **information security management system (ISMS)**, a framework that helps organizations manage their information security by defining policies, procedures, and controls. Developed by the International Organization for Standardization (ISO), ISO/IEC 27001 sets out the criteria for assessing and treating information security risks tailored to the needs of the organization. The standard encompasses both the technical and organizational aspects of information security, ensuring an integrated approach.

The significance of ISO/IEC 27001 lies in its universal applicability across industries and organizations of any size. It provides a robust framework that helps organizations secure their information assets, enhance their resilience against cyber threats, and establish trust with stakeholders. By achieving certification, organizations demonstrate their commitment to information security, which can lead to competitive advantages, improved client relationships, and compliance with legal and regulatory requirements.

The ISO/IEC 27001 standard is structured into ten main clauses, with the last six dedicated to the ISMS requirements:[18]

1. Scope: Defines the boundaries and applicability of the ISMS
2. Normative references: Lists the standards referenced in ISO 27001

18 International Organization for Standardization, *ISO/IEC 27001:2022* (ISO, 2022).

3. Terms and definitions: Clarifies the terminology used in the standard
4. Context of the organization: Explains the internal and external factors that can impact the ISMS
5. Leadership: Emphasizes the importance of top management's involvement and the establishment of an information security policy
6. Planning: Covers risk assessment and the process of establishing information security objectives
7. Support: Encompasses resources, competence, awareness, communication, and documented information
8. Operation: Deals with the execution of the processes and controls necessary to manage information security risks
9. Performance evaluation: Involves monitoring, measurement, analysis, evaluation, internal audit, and management review
10. Improvement: Focuses on continual improvement of the ISMS

Although not one of the clauses, guidance on implementing specific controls is discussed in Annex A.

The principles of ISO/IEC 27001 are organized around a risk-based approach, and this ensures that the ISMS is tailored to the specific risks faced by the organization. The approach promotes a culture of continuous improvement, transparency, and accountability.

National Institute of Standards and Technology

Imagine taking the role as the new chief information security officer of a bank and the CEO asks you, "How secure are we?" How would you approach answering this question? Or where could you go to get the information? One place to start would be with the National Institute of Standards and Technology (NIST). NIST is a nonregulatory federal agency within the U.S. Department of Commerce that helps to set standards and guidelines to ensure the security and privacy of information systems. NIST's contribution to U.S. cybersecurity is significant, as the agency provides resources, best practices, and frameworks to assist organizations in safeguarding their information.

The NIST Special Publications 800 series is a collection of documents that cover various aspects of information security. These publications provide guidelines, recommendations, and best practices to help organizations manage and protect their information systems. Comparing the practices of your hypothetical bank against the guidelines set forth by NIST could help you answer your boss's question about security. One of the most notable contributions from NIST is the framework for improving critical infrastructure cybersecurity, commonly known as the NIST Cybersecurity Framework. This framework comprises five domains: identify, protect, detect, respond, and recover (refer to Figure 5.7). Each domain involves specific security activities that, when implemented, provide organizations with a strategic view of their cybersecurity posture.

Numerous organizations across different sectors have adopted NIST standards to enhance their cybersecurity practices. For example, a financial institution might align its security policies and procedures with NIST's best practices to improve its resilience against cyber threats. In the health-care sector, a hospital might use NIST guidelines to secure patient data and ensure HIPAA compliance. These real-world applications demonstrate the versatility and effectiveness of NIST standards in bolstering cybersecurity defenses and fostering a culture of security awareness and compliance.

Other Compliance Frameworks and Regulations

There are several frameworks and regulations in addition to NIST, NIST-800, and ISO/IEC 27001 that guide information security policy within an organization. Many of these depend on the nature of the business, the type of data that is collected, or even the geographic location of the business's headquarters.

- The Federal Information Security Management Act (FISMA) is a U.S. law that is part of the E-Government Act of 2002. It is designed to bolster information security across federal agencies, and it establishes a comprehensive framework that mandates agencies to develop, document, and implement security programs to protect information and assets. FISMA emphasizes a risk-based policy for cost-effective

security, requiring agencies to conduct regular risk assessments, implement security measures, and undergo continuous monitoring. Compliance with FISMA demonstrates an organization's commitment to protecting governmental information and assets.

- The Health Information Technology for Economical and Clinical Health (HITECH) Act, enacted in 2009, represents significant legislation in health information technology and privacy. It aims to promote the adoption and meaningful use of health information technology, while also strengthening the privacy and security provisions of HIPAA. HITECH introduced stricter enforcement of HIPAA rules and increased penalties for noncompliance, emphasizing the need for health-care providers and related entities to safeguard electronic protected health information (ePHI). It also incentivized the implementation of electronic health records (EHRs), marking a transformative step in the modernization of health-care data management and security.

Developing a Comprehensive Risk Management Plan

A **risk management plan (RMP)** is a strategic document that outlines how risk is assessed, monitored, and mitigated within an organization. An RMP is a critical component in an organization's information security and risk management strategy. It provides a structured four-stage approach to identifying, assessing, mitigating, and monitoring potential risks that could compromise sensitive data, intellectual property, and other vital assets. This strategic document is crucial for shaping an organization's cybersecurity posture, guiding the allocation of resources, and prioritizing actions to enhance resilience against cyber threats.

Phase 1: Risk Identification

The initial phase of developing an RMP, identifying potential risks, is the priority. This process involves using various techniques and tools to uncover vulnerabilities, threats, and potential impact on organizational assets. A **strengths, weaknesses, opportunities, and threats (SWOT) analysis** is a commonly used method that helps in understanding both internal and external factors that could pose risks. When applied to risk identification in ISRM, SWOT becomes a powerful instrument in the hands of cybersecurity professionals. The SWOT analysis in Figure 5.10 shows how it has been used and adapted to meet the needs of a team assessing their own information security. By evaluating the strengths of an organization, such as robust security policies or advanced technological infrastructure, professionals can form policies that enhance brand value, increase employee awareness to reduce attacks, and make data-informed decisions regarding system upgrades.

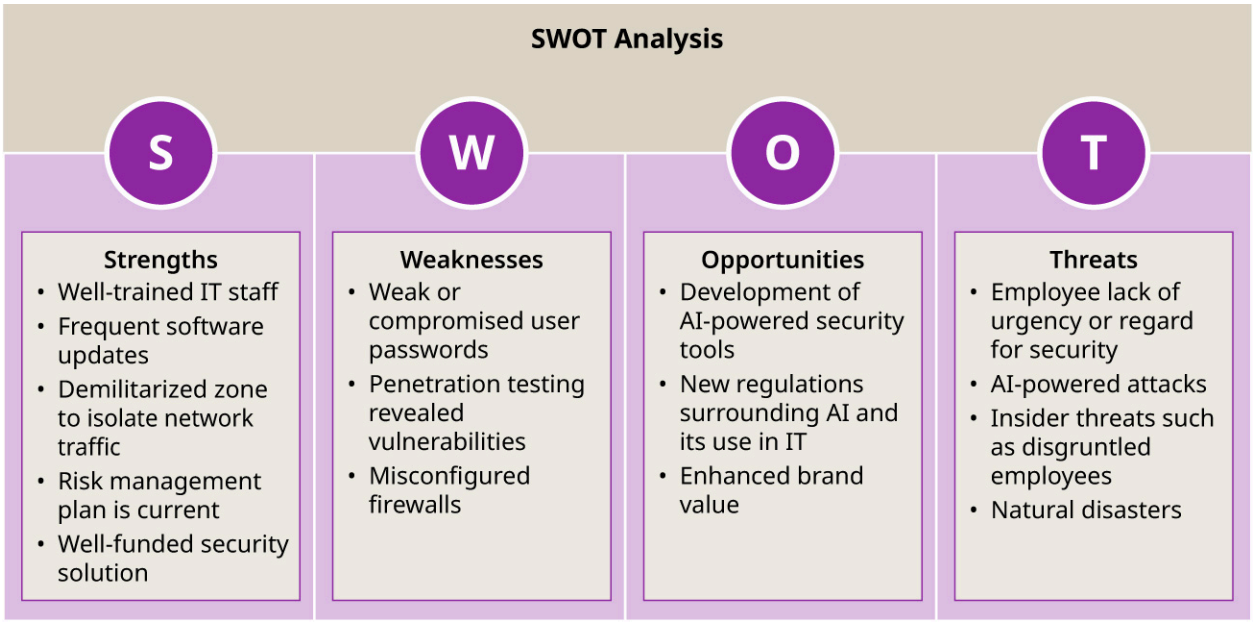

Figure 5.10 This hypothetical SWOT analysis completed by an information security team strategizes against threats to an IT system in a social media company. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The assets at risk in an organization can be vast and varied, including tangible assets such as hardware and intangible assets such as data and intellectual property. Protecting these assets requires a clear understanding of their value and the potential repercussions of any compromise. To aid in this process, a range of tools and technologies is available. Scanners, for instance, can automatically detect vulnerabilities in a network, while AI-based solutions offer advanced capabilities to predict and identify emerging threats. By employing these tools and methodologies, organizations can develop a clear and actionable understanding of their risk landscape, laying the foundation for effective risk management.

Phase 2: Risk Assessment

The risk assessment phase is a critical stage in the RMP, where the organization dives into the potential likelihood and impact of various identified risks. This process is like a detective's investigation, where each clue helps in prioritizing risks based on their severity. Imagine a team of cybersecurity experts evaluating a network system, much like detectives combing through a crime scene. They identify potential threats and vulnerabilities, such as what types of data are at risk, what protections are currently in place, and what additional measures are necessary to close any security gaps.

This phase is not just about finding problems, but also about devising strategies to mitigate them. Through risk assessments, ISRM professionals can make data-driven decisions to align security measures with organizational objectives. The comprehensive nature of risk assessment technologies and approaches highlights the need for ISRM professionals to have a similar breadth and depth of knowledge. With the appropriate certifications and continuous learning, these professionals can contribute to a safer and more secure digital landscape.

The two predominant assessment methods are quantitative and qualitative.

- Quantitative assessment: Quantitative assessments are often viewed as more time intensive than qualitative but can be more accurate when evaluating risk. The impact of the risk is often evaluated in the context of the expected cost of the risk. One method used in quantitative risk assessment is expected monetary value (EMV) analysis, which is a mathematical calculation for determining the expected monetary impact of risks: it multiplies the dollar cost of a risk by the probability of that risk occurring and then adds the values together for all risks. A decision tree analysis is another quantitative method that is more visual than EMV (Figure 5.11). The decision tree includes each risk, along with its financial impact and the probability associated with each risk. The project manager then can see the path that offers the least impact (cost) on the project. Regardless of the method chosen, quantitative risk assessment involves calculations that give a monetary value to the impact of the risks to the project.
- Qualitative assessment: Qualitative impacts can be categorized as high, medium, and low with the probability of occurrence ranked on a scale from very likely to highly unlikely. Even though the assessments are more subjective than the quantitative approaches, there are methods that can facilitate the processes. For example, a brainstorming session with key stakeholders or with the project team could generate a list of potential risks. Additionally, in-depth interviews with experts or stakeholders can identify risks and begin to assess the impact and probability. A SWOT analysis can be used as well. In particular, the internal weaknesses and the external threats can be considered risks to evaluate in the project.

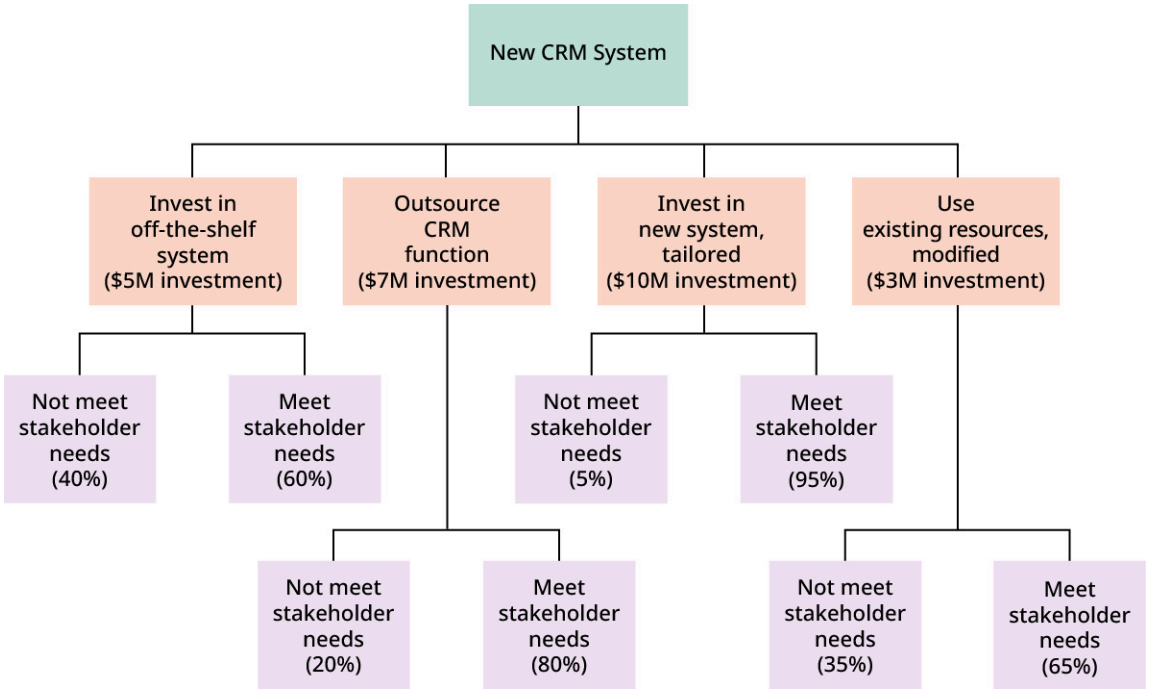

Figure 5.11 This hypothetical decision tree analysis shows how it can help a project manager visualize the various risks associated with a project. Through calculations such as EMV, the project manager can quantify the path that offers the least impact. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Another method used when conducting the qualitative assessment of risks is the Delphi method, which involves rounds of questionnaires sent to individuals with expertise who provide anonymous responses in which they identify risks and assess their impact and probabilities. The project manager will analyze the responses after each round to look for commonalities. Then, the compiled results are presented to the experts again and they have the opportunity reevaluate the responses and amend the list. The end result of the Delphi method is a list of risks that the experts have arrived at through this consensus-building process. Whatever method is used for conducting the qualitative assessment of the RMP, the important factor is to get input from various stakeholders and experts in the field to identify the risks and then organize the risks based on their impact and probability of occurrence. Figure 5.12 illustrates the contrast between quantitative and qualitative assessments when applied to an organization that specializes in IP generation.

Qualitative Assessment and Quantitative Assessment of Asset 1: Intellectual Property (IP)		**Qualitative Assessment and Quantitative Assessment of Asset 2: Human Resources (HR) Data**	
Qualitative Assessment	**Quantitative Assessment**	**Qualitative Assessment**	**Quantitative Assessment**
The loss or compromise of IP is categorized as high risk due to the potential severe impact on the company's competitive edge and market reputation. The likelihood of such an event could be rated as medium, considering the advanced security measures in place, yet acknowledging the high interest of competitors in this data.	If IP is compromised, the estimated financial loss is calculated at $5 million, considering factors like potential revenue loss, legal costs, and damages. The probability of this event, based on industry data and past incidents, is assessed at a 20% chance within the next year.	The breach of HR data, containing sensitive employee information, is categorized as medium risk. While it has significant implications for privacy and compliance (e.g., GDPR), it may not directly impact core business operations. The likelihood is assessed as high due to the larger volume of HR data and its accessibility.	A breach of HR data could lead to a financial impact of around $2 million, primarily due to legal repercussions and potential fines. The likelihood of such a breach is estimated at 30% in the next year, based on current trends in data breaches involving personal information.

Figure 5.12 This hypothetical scenario shows the two lenses of conducting a risk assessment: qualitative and quantitative. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

A risk matrix is a visual representation of the identified risks categorized by both impact and probability. A risk

matrix can be used with both qualitative and quantitative assessments. In qualitative assessments, the matrix will be populated with categories that are subjective, such as high probability or low impact, whereas a quantitative risk matrix would include the numerical measures of these values. Often the matrix is color coded with a predetermined color scheme to help quickly identify those risks that have the highest impact or probability.

In Figure 5.13, the highest-risk items are highlighted in red with the lower-risk items in green. Each risk matrix can be evaluated by the project manager to determine which risks should be monitored more closely and to prioritize the highest impact items. Then, the RMP can address the appropriate risk mitigation strategies for those higher priority items while putting less focus on risks with minimal overall impact on the project.

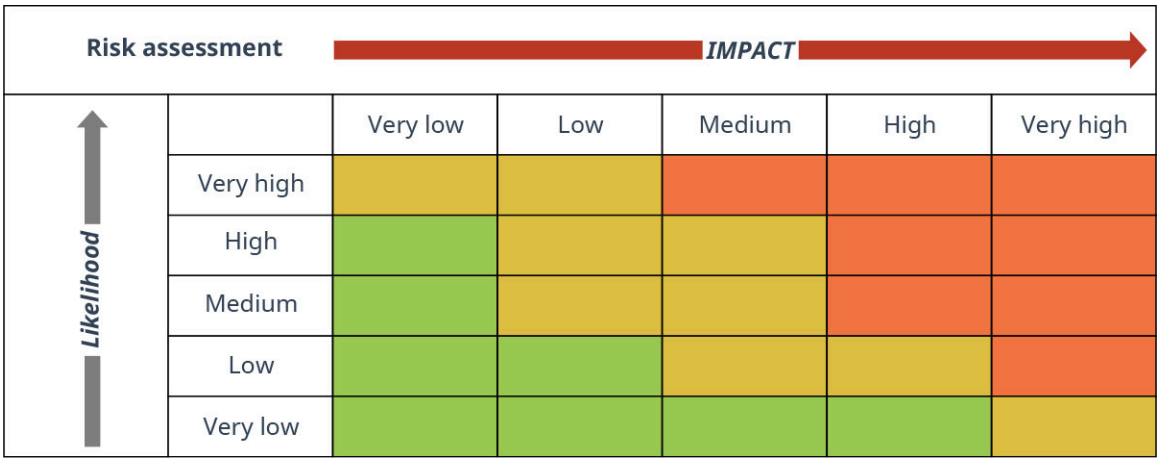

Figure 5.13 A risk matrix assists leaders in quantifying risks that may affect the organization. (credit: modification of work "Risk matrix (FAA Safety Risk Management Policy, 8040.4B)" by U.S. Department of Transportation Federal Aviation Administration/ Wikimedia Commons, Public Domain)

Phase 3: Risk Mitigation Strategies

Uncertainty in projects cannot be eliminated, but it can be mitigated. Some broad mitigation strategies include being proactive and developing a plan to deal with risks if they materialize. Each identified risk should have a strategy attached so that there is a plan in place to minimize the impact of the risk on the project. These broad strategies offer some general decisions that can be made with each risk; however, the actual activities used to alleviate the impact will need to be tailored to the specific risk. Figure 5.14 lists broad strategies for dealing with risk.

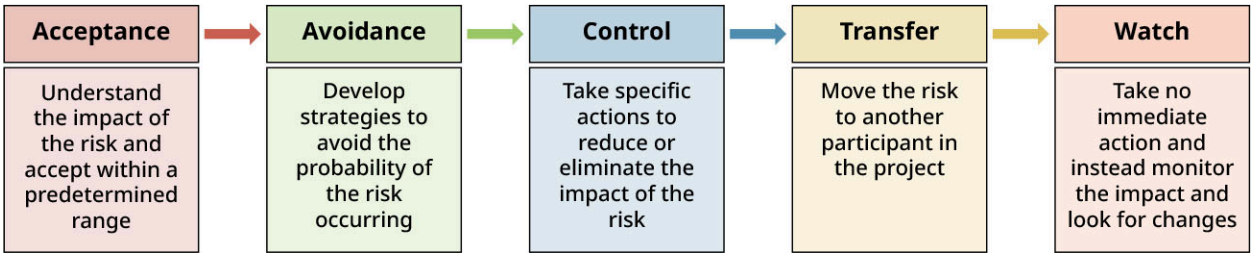

Figure 5.14 Developing action plans on how to deal with each risk in RMP can save time and money in the long run. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The first strategy, acceptance, describes a situation where the risk, impact, and probability are known, and the project team makes the decision to accept the impact. The risk might be at a level where it would not have a meaningful impact on the overall project. In some cases, the benefit of accepting the risk outweighs any negative impacts from the risk. Generally, the acceptance strategy is used when there are minimal impacts to the cost, the schedule, or team performance. It is important to continue to monitor the risk to ensure the impact remains at an acceptable level. Overall, the project continues to move forward without substantive consequences to the project plan and deliverables.

In the avoidance approach, the project team develops strategies to prevent the risk from occurring. For example, to avoid the risk of a new CRM system not functioning properly, the system could be tested with key stakeholders to make sure it meets performance measures. With risk avoidance, the project manager might consider moving resources from one part of the project (such as personnel or funding) to another part to help reduce the risk. Risk avoidance is used when there are risks to performance and could involve having backup vendors in case one vendor cannot fulfill what they are contracted to do. Avoiding risks to the schedule may involve setting realistic deadlines that are not too aggressive.

The control approach to mitigating risks involves trying to minimize the impact of risks. This involves consistent monitoring and having a plan in place to proactively respond to the risks. For example, tracking expenses against the expected budget at regular intervals can help the project team identify when line items are at risk of going over budget. When the project manager notices this, they can then implement strategies to manage the expense in that line to control the risk of going over budget. To control the risk of going over schedule, the project manager can keep close tabs on the time needed for tasks and redelegate as needed to make sure the project stays on time.

The transfer strategy can be used to shift the risk—and thus the impact—to another entity associated with the project. However, this approach may not be the best strategy because unintended consequences can arise. For example, if the project is running behind schedule, the project manager could transfer the cause of that delay to an individual team member rather than to the project team as a whole. Although the project team's reputation might be preserved somewhat, this kind of action could greatly impact the team dynamics. Likewise, if the impact of a product's failure is transferred to a particular vendor used to produce the product, the business relationship could be altered, even if the costs of the failure are no longer the responsibility of the project team. Caution should be used when choosing this strategy because of the additional consequences that could result.

Finally, the watch strategy involves essentially taking no action but having activities in place in the project plan to consistently monitor the risk for changes that could either increase the probability of occurrence or increase the impact. Strategies such as tracking the actual expenses versus budgeted expenses on a regular basis, or having project team updates on the status of action items, can be used to watch for changes. Monitoring is a key strategy that should be used for all risks identified and should be a key component of the RMP. The bottom line with any of the approaches to risk mitigation is to invest time on the front end of the planning process to be proactive in how the project team responds to risk.

Phase 4: Monitoring and Review

The implementation of risk mitigation strategies is not the end of the risk management process. In fact, mitigation requires ongoing attention and diligence to ensure its effectiveness and adaptability to new threats and changes in the organization's environment. This phase emphasizes the necessity of continuous monitoring and regular reviews to maintain the integrity of the RMP.

Frameworks for Continuous Monitoring and Improvement of the ISRM Strategy

The ongoing process of assessing the security posture and compliance of an IT infrastructure by automatically collecting, analyzing, and reporting data on various security controls is called **continuous monitoring**. It is critical for detecting and responding to threats and vulnerabilities in real time. It helps to ensure that the implemented risk mitigation strategies are working as intended and that no new risks have emerged. Continuous monitoring aids in maintaining a strong security posture, as it provides ongoing insights into the effectiveness of security controls and the organization's overall risk exposure.

Continuous monitoring plays an important role in ensuring the ongoing integrity, availability, and security of critical assets and information. Continuous monitoring is a necessary component of an effective ISRM strategy, ensuring that security controls are operating as intended and that any malicious activities are detected and

addressed in a timely manner.

The **Information Systems Audit and Control Association (ISACA)** is an international association that provides IT professionals with knowledge, credentials, education, and community in IT governance, control, risk, security, audit, and assurance. IT governance is the process of managing and controlling an organization's IT capabilities to improve IT management, ensure compliance, and increase the value of IT investments. ISACA offers several certifications and comprehensive cyber education and plays an important role in setting global standards for cybersecurity. Through its publications, certifications, and guidance, ISACA provides industry best practices and frameworks that organizations can adopt to enhance their monitoring capabilities and align with relevant regulatory requirements.

One of ISACA's most notable contributions to the field is the development of the **Control Objectives for Information and Related Technologies (COBIT)** framework (Figure 5.15), a comprehensive framework developed by ISACA for IT governance and management that helps organizations meet business challenges in the areas of regulatory compliance, risk management, and aligning IT strategy with organizational goals.[19] In addition to COBIT5, NIST also provides a continuous monitoring strategy.[20] It is recognized globally and is widely adopted by organizations seeking to align their IT processes with their strategic objectives, while ensuring that risks are managed effectively and resources are used responsibly.

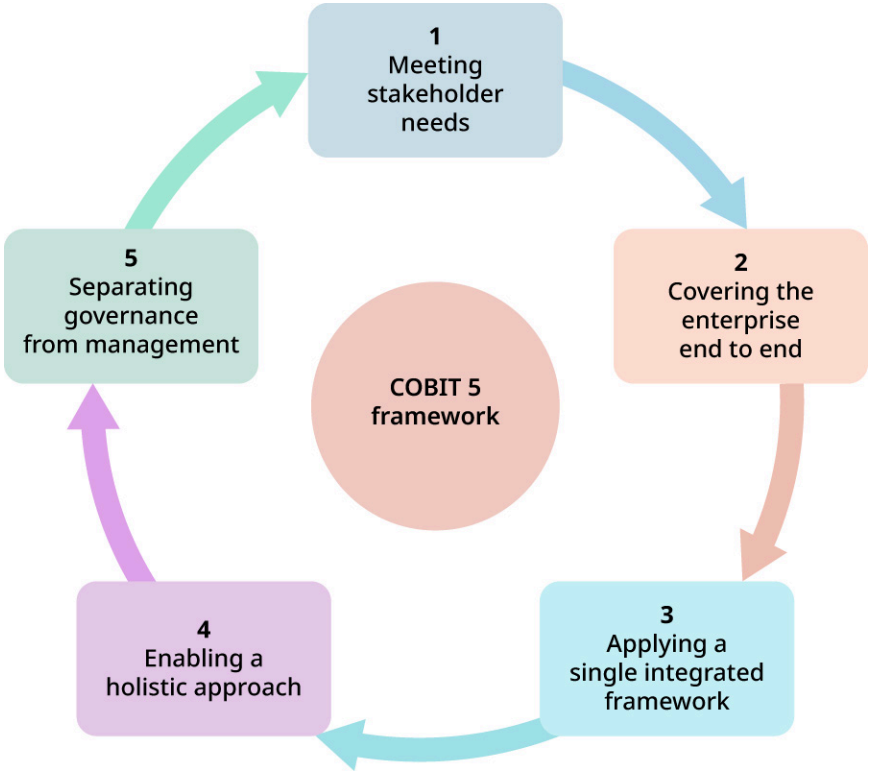

Figure 5.15 The COBIT5 framework consists of five principles that scaffold an IT governance structure. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Various tools and technologies play a pivotal role in facilitating continuous monitoring, each serving specific purposes and providing different insights into the organization's security posture.

One of the key tools available for continuous monitoring is a security information and event management (SIEM) system, a centralized security tool that combines security information management with security event

19 COBIT5 was published in 2012, and a new version (COBIT 2019) was released in 2018. COBIT 2019 was updated for newer technology and has six principles that use some revised terminology. Although COBIT 2019 is the most current version, many organizations still use COBIT5. 6.3 Data Security and Privacy from a Global Perspective discusses COBIT 2019.

20 Kelley Dempsey, Nirali S. Chawla, Arnold Johnson, et al. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," *NIST Special Publication 800-137*, National Institute of Standards and Technology, September 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

management. The tool collects, consolidates, and organizes data within the system, including user data, application data, and network data, to analyze and detect suspicious activity within the system. The aggregated data are analyzed to detect unusual activities, patterns, or events. The tools not only detect attacks but can also prevent and block threats to the system. Additionally, the tool can compile the necessary information for compliance reporting purposes. Finally, the SIEM system can monitor user actions to identify potential issues before those actions pose a threat to the organization. For example, if confidential employee information is being shared via email to an entity outside of the company that is not known to have a business need for the information, the SIEM system can flag those emails as threats. In a similar way, the system can identify incoming phishing emails and automatically block the sender. Through analytics, the SIEM system can quickly recognize unusual activity and take appropriate action to minimize the impact.

An intrusion detection system (IDS) is integrated into the SIEM system. The IDS looks specifically at traffic on the network to determine if there is suspicious activity coming into or out of the network. That data are then fed into the SIEM system to be aggregated with the other data gathered. The IDS can also detect security violations within the network. The tool does not stop the threat; it simply identifies the threat, sends the data on, and alerts network administrators of the threat. The IDS looks for known sources of threats. For example, the detection system could pick up on a specific chain of characters or source code that is part of a known malware threat. Because the IDS checks traffic against known threats, it is important to regularly update the system to make sure the newest cyber threats are being monitored.

The IDS works in conjunction with an intrusion prevention system (IPS) to prevent ongoing attacks to the network. The IPS is a more proactive approach to maintaining the security of the network. One example of an IPS is a firewall web application that prevents downloading of material from unsecured websites. To prevent threats from entering the network, all traffic goes through the IPS before entering the network. As with the IDS, the IPS works off of known threats, so new cyberattacks might get through. When suspicious activity is noticed, the IPS will block the activity from getting into the network, send an alert to administrators (facilitated by the SIEM system), and often terminate the connection where the threat originated in the system. This could mean a user is disconnected from the system to prevent further intrusion until the threat can be mitigated. Today's IPS tools have detection capabilities built in and are now referred to as intrusion detection and prevention systems (IDPSs). Many organizations use one integrated tool rather than having two separate tools to manage security.

5.4 Career Focus: Key Certifications

Learning Objectives

By the end of this section, you will be able to:

- Describe various career roles and responsibilities in information security
- Determine the certifications and degree programs needed to prepare for a career in information security
- Recognize organizations where information security careers are most viable

At this point, you may be wondering how to find and obtain a job in one of the roles described in the information systems security field. The answer lies not just in building academic credentials, but also in gaining a variety of certifications. Obtaining a certification diversifies and deepens your expertise. These certifications demonstrate specialized knowledge and help individuals pursue career advancement.

The globally recognized Certified Information Systems Security Professional (CISSP) certification is one example. The CISSP and similar certifications enhance your skills and provide a mark of quality on your professional profile, making you a more desirable candidate in a competitive job market.

Information security is a sizable field that presents multiple pathways for career trajectories, each with its own challenges and rewards. From roles like a security analyst and network security engineer to high-level

positions such as chief information security officer (CISO), the sector offers a spectrum of career avenues. The primary functions associated with these roles range from securing network perimeters to establishing organizational security strategies. It is essential to understand that certifications provide technical proficiency, but it is the alignment of this knowledge with specific job responsibilities that completes a person's professional portfolio.

Career Roles and Responsibilities in Information Security

With the rising complexities of information systems, there has been an increase in the number of roles that fall under the umbrella of information security. No longer is it a one-size-fits-all discipline that is solely the responsibility of an IT department. The field has morphed into a diverse landscape, offering an array of opportunities that encompass areas such as IT, business, law, and even psychology. From entry-level roles like security analysts to leadership positions such as CISOs, the profession now offers a variety of pathways for individuals with a range of interests and skills.

Overview of Information Security as a Profession

As you've learned, information security is the practice of safeguarding digital assets from unauthorized access, disclosure, alteration, or destruction. The scope of this profession has become both broad and deep, often encompassing multiple domains, including, but not limited to, network security, application security, endpoint security, identity management, cloud security, and even social engineering. In all these domains, the goal is still to protect an organization's data and systems from internal and external threats, thereby supporting its broader mission and objectives. In the public sector, it may involve safeguarding critical national infrastructure or sensitive governmental data.

LINK TO LEARNING

As a cybersecurity professional, it is vitally important to stay up to date with the latest developments in cybersecurity. This field changes often as new technologies are developed and hackers develop new methods of attack. SANS provides a variety of free and paid information security resources (https://openstax.org/r/109SecResources) such as courses, conferences, and newsletters.

The field of information security straddles several disciplines, and professionals may be able to integrate knowledge and techniques from a variety of sectors. While not an exhaustive list, Table 5.5 identifies some of these disciplines that intersect within the information security field.

Discipline	Relation to Information Security
Information technology	IT forms the backbone of information security. Professionals need to be familiar with various hardware and software systems, network protocols, and security architectures.
Business	Understanding the strategic goals and operational nuances of an organization is key to effective security planning. It includes concepts such as business continuity and disaster recovery planning.
Law	Legal considerations, such as compliance with regulations like HIPAA in U.S. health care or GDPR in the European Union, are fundamental. Ignorance of legal requirements is not an excuse, and the ramifications of noncompliance can be severe.

Table 5.5 Disciplines within the Information Security Field Information systems is an eclectic discipline with several connected disciplines.

Discipline	Relation to Information Security
Psychology	An often-overlooked aspect of information security is understanding human behavior, especially as it relates to social engineering tactics. Security awareness training, for instance, is an important element for creating a secure organization.
Ethics	The ethical dimensions of data management and privacy are increasingly gaining prominence, especially as society becomes more conscious of individual rights related to personal data.

Table 5.5 Disciplines within the Information Security Field Information systems is an eclectic discipline with several connected disciplines.

Roles and Careers in Information Security

A career in information security not only requires a good understanding of technology, but it also requires a holistic understanding of a variety of subjects that impact the security of an organization. By acknowledging this interdisciplinary nature, professionals can better position themselves for successful and impactful careers. Roles in cybersecurity fields range from those working in a security operations center to specialized positions such as cryptographers and forensic specialists, as noted in Table 5.6.

Field	Role
Security operations center	The security analyst typically serves as an organization's first line of defense, monitoring security alerts, analyzing anomalies, and initiating incident response protocols. Their role may also include vulnerability assessment and working with different departments to improve overall security posture.
Security governance and risk	Security governance and risk roles represent a merger between the duties of a security auditor and a security engineer.
Strategic security management	Typically, an information security manager is responsible for the day-to-day operations related to cybersecurity. This could include overseeing a team of security experts, managing security initiatives, and ensuring compliance with internal and external regulations.
Forensics and ethics	Forensic experts specialize in investigating and analyzing past security incidents to understand how they occurred and to recommend ways to prevent future occurrences. They are the detectives of the cyber world, piecing together clues to resolve complex security puzzles.

Table 5.6 Roles in Cybersecurity Fields There are various career opportunities in the information systems security and risk management domains.

Together, these roles create a robust framework for both proactive and reactive security measures, encompassing the creation of secure environments, detailed investigation of breaches, and preemptive identification of potential vulnerabilities. This consolidated specialization serves as an advanced line of defense, often working behind the scenes, that is critically important in bolstering an organization's overall cybersecurity posture.

LINK TO LEARNING

The Information Security Forum is a professional organization that provides links to security research (https://openstax.org/r/109SecResearch) as well as forums, tools, products, services, events, and news regarding information security and risk management.

Certifications and Degree Programs for Careers in Information Security

Continuous professional development is fundamental in information security. As threats become more sophisticated and bad actors continue to refine their craft, ongoing education is necessary. Within this context, certifications and formal education programs serve dual purposes. First, they provide the foundational and advanced knowledge required to confront emerging security challenges effectively. Second, they serve as universally recognized markers of expertise, enhancing career prospects and lending credibility to skills.

The role of certifications in information security is important. A certification such as **Certified Ethical Hacker (CEH)** signifies proficiency in ethical hacking techniques and tools, and the ability to assess the security of computer systems by looking for vulnerabilities in a lawful and legitimate manner. CompTIA is a professional organization that specializes in certifications in IT. **Security+** is an entry-level certification from CompTIA that covers foundational skills and knowledge in network security, compliance, operational security, threats and vulnerabilities, data and host security, access control, and identity management. Other certifications offer structured learning paths and are often prerequisites for specialized roles in the industry (Table 5.7). For example, **Certified Information Security Manager (CISM)** focuses on management and governance of information security, and **Certified Information Systems Security Professional (CISSP)** is an advanced certification that focuses on the knowledge and skills required to design, implement, and manage a comprehensive information security program. Certifications act as both a road map for skill acquisition and a validation of those skills, especially valuable for professionals looking to transition into higher-level positions.

Certification	Related Jobs
CompTIA A+	Systems administrator, help desk technician, computer repair specialist, desktop support technician, IT asset manager, field service technician
CompTIA Security+	Security administrator, security analyst, incident response analyst, cybersecurity analyst
Cisco Certified Network Professional	Network engineer, network administrator, cloud network engineer, solutions architect, IT manager
EC-Council Certified Ethical Hacker	Cybercrime investigator, ethical hacker, forensic investigator, penetration tester, information security auditor, vulnerability analyst
Certified Information Systems Security Professional (CISSP)	Chief information security officer (CISO), incident response manager, cybersecurity engineer, risk manager, security analyst

Table 5.7 Common Certifications and Related Jobs There are several certifications available for those looking to work in a cyber-related field.

Formal education, such as bachelor's and master's degrees in cybersecurity or information security, provides a comprehensive overview of the field. These programs often cover a broader curriculum, touching on related disciplines such as business, law, and ethics, preparing students for the interdisciplinary nature of modern

information security roles.

Both certifications and formal degree programs are vital in shaping a path to a successful career in information security. They equip professionals with the skills needed to adapt and thrive in a dynamic environment while simultaneously serving as benchmarks of competence for employers.

Empowering Cybersecurity Careers: Value and Impact of Professional Certifications and Related Degrees

Certifications and degrees in information security play an important role in validating a professional's skills and competencies. While traditional degree programs offer a broad scope of knowledge, certifications are focused on skill sets and methodologies directly applicable to the job. Unlike generic evaluations or internal assessments within an organization, certifications are designed and recognized by industry experts. Obtaining a certification often requires passing rigorous exams and, in some instances, demonstrating hands-on expertise in a controlled environment. As such, certifications act as a third-party endorsement of a professional's capabilities, lending weight to résumés and professional profiles.

Certifications

CEH certification concentrates on penetration testing and vulnerability assessments, skills immediately deployable in the workplace. Cisco's Certified Network Professional (CCNP), which focuses on advanced networking practices, is highly sought after by employers looking to increase their talent pool. Selecting the right certifications is a foundational step for a strong and definitive career path in information security. Certifications signal to employers that a candidate possesses a level of technical insight that has been rigorously evaluated and approved by a recognized accrediting body. In an increasingly competitive job market, such validation can distinguish one individual from other professionals in the field, and in many cases, it may be a formal requirement for securing a particular role.

Each certification level, whether entry-level or advanced, typically builds on the last, creating a pathway for continuous skill acquisition and career progression. This is particularly significant in information security. By regularly updating and expanding your certification portfolio, you are not just meeting the requirements of your current role, but also preparing yourself for the more complex challenges that lie ahead in higher-level positions.

For example, suppose you are an IT professional with experience in data analysis, and you are interested in transitioning into a threat intelligence analyst role. In this case, CompTIA Cybersecurity Analyst (CySA+) would be a strategic certification to pursue. The CySA+ specializes in behavioral analytics to identify cybersecurity threats, a skill often required for threat intelligence analysis. For more senior roles, such as information security manager or CISO, the CISSP is considered a gold standard. The CISSP provides a comprehensive overview of information security and may be a requirement for high-level security roles within large organizations.

Aligning certifications with career goals can deliver tangible benefits, enabling individuals to tailor their professional development to meet the expectations of future roles. It is worth investing the time to research and select the certifications that offer the most direct path toward a desired career trajectory in the field of information security.

Degree Programs

Earning certifications in cybersecurity-related fields can help with obtaining employment with many employers. However, degree programs complement the certification stack and demonstrate to potential employers that you can perform tasks both in an academic and in a technical manner. Additionally, many employers seek individuals who possess a degree in higher education for higher level roles in an organization such as chief information officer or CISO. For example, in their analysis of employer hiring behaviors, one study found that several employers favored those who possessed a degree accompanied by certifications over those with certifications alone (Figure 5.16).[21]

Figure 5.16 Obtaining a degree in a cyber-related field greatly improves your chances of employment. (credit: modification of work "Spring 2023 commencement ceremony" by Germanna Community College/Flickr, CC BY 2.0)

Degrees in cyber-related fields include the following:

- Undergraduate programs: Bachelor in cybersecurity. Many institutions offer a bachelor's degree in a cybersecurity-related discipline. Several of these programs incorporate general networking, ethical hacking, penetration testing, programming in various languages (such as Python, C#, and C++), and network defense. Additionally, these programs often have specializations or "tracks" that allow students to specialize in a particular area of cybersecurity. According to the U.S. Bureau of Statistics, the number of jobs related to cybersecurity to be added by the year 2033 could be more than 59,000.[22] Many of these positions require a minimum of a bachelor's degree coupled with certifications to be considered for employment.
- Graduate programs: Master in cybersecurity. Those holding this credential are often sought after by enterprise organizations looking to hire senior-level managers to oversee teams in a cybersecurity environment. Those enrolled in these programs acquire industry-recognized skills along with skills in leadership and management. The curriculum in these programs is normally designed to expose learners to practical skills that can be immediately applied upon graduation.

Combining Certifications and Degrees

Combining both certifications and formal education provides the benefits of a formal degree coupled with industry-recognized skill sets. Formal education helps to provide a broad theoretical understanding of the field along with the soft skills sought after by the industry. Moreover, the depth of knowledge gained during the formal education process helps to reinforce the concepts of practical application by supplying a broad understanding of the field.

21 Jim Marquardson and Ahmed Elnoshokaty, "Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs," *Information Systems Education Journal* 18, no. 1 (2020): 22–28.
22 Bureau of Labor Statistics, "Information Security Analysts," *Occupational Outlook Handbook*, U.S. Department of Labor, last modified August 29, 2024, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

The act of acquiring both industry-recognized certifications and formal educational qualifications in cybersecurity demonstrates more than mere skill acquisition; it reflects a commitment to mastering the complexities of the field. Each of these educational pathways offers benefits. Certifications such as Security+, CISSP, or CISM are tailored to validate a specific set of skills and are often updated more frequently than traditional academic curricula. They provide practical, firsthand experience and are excellent at helping to build immediate competency in specialized areas. Certifications also offer quicker routes to career advancement by serving as easily recognizable benchmarks for employers.

Organizations for Information Security Careers

A fulfilling career in the cybersecurity domain depends not only on skill and qualifications, but also on the organization one joins. Organizations provide context in which professionals apply their expertise to real-world challenges, influencing both job satisfaction and career path. Therefore, selecting the right workplace becomes an important decision, affecting not just individual career growth, but also the broader mission of enhancing digital trust in society.

Corporate Sector

The corporate sector is the most expansive area for information security professionals, encompassing technology companies, financial institutions, health-care providers, and e-commerce businesses. Each of these subsectors demands specialized knowledge and skill sets, from safeguarding intellectual property to ensuring customer data privacy.

FUTURE TECHNOLOGY

Meta's AI

After the release of ChatGPT from Open AI, several tech companies rushed to develop their own models to compete. For example, Google developed Bard (now known as Gemini), Tesla is working on their own models under xAI to try to generate a platform that outperforms GPT, and Microsoft implemented Copilot, which is another large language model (LLM) that was deployed in November 2023. Another contender in this field is Meta, who released the second iteration of their open-source LLM called Llama 2 in 2023. Their model is optimized for lower resource usage and can be deployed in a number of environments, ranging from academia to the commercial sector. One other important feature of the Llama 2 model is its ability to be trained and adapted to complete different tasks. Meta has partnered with Microsoft for Llama 2 to provide global access to their AI technology to encourage users to innovate by building on their model, which can in turn benefit businesses around the world.

Government, Public Sector, and Nonprofit Think Tanks

In the government and public sector, certified information security professionals contribute significantly to the safeguarding of national interests and public welfare. Holding certifications not only validates a professional's skills, but also reinforces the level of trust and credibility in governmental operations. For example, certified professionals can be instrumental in developing secure electoral systems, safeguarding public health records, and ensuring the confidentiality of sensitive diplomatic communications. By doing so, they facilitate an environment of digital trust that is important to maintain the public's confidence in governmental systems and operations. Professionals in this area are often employed by government agencies such as the Department of Defense or the Department of Justice.

The nonprofit sector and think tanks also help to shape the landscape of information security. These organizations primarily focus on research, advocacy, and public awareness, often working to address the cybersecurity needs of vulnerable populations or to shape public policy. They apply their specialized knowledge to developing solutions or frameworks that advance the cause of digital trust. Certified

professionals may be seen as holders of digital trust, advocating for responsible and secure use of technology. Some of these types of entities include:

- Cybersecurity research organizations: Nonprofits such as the Electronic Frontier Foundation (EFF) or the Center for Internet Security (CIS) often conduct groundbreaking research on cyber threats, security technologies, and ethical computing practices. Their work may result in white papers, open-source tools, or policy recommendations.
- Educational institutions: Think tanks and educational nonprofits aim to raise cybersecurity awareness and literacy. They may offer training programs, certifications, or collaborate with academic institutions to promote cybersecurity as an essential part of the curriculum.

Freelance and Consultancy

The freelance and consultancy sector is suitable for those who prefer project-based or contractual work, often serving clients across the same sectors. It offers flexibility but demands a versatile skill set and an entrepreneurial mindset. In any of these sectors, certifications serve as a testament to an individual's skills and as a basis for advancing digital trust. A certified professional lends credibility to an organization's cybersecurity posture, thereby facilitating trust.

LINK TO LEARNING

There are many opportunities available to those interested in freelancing or performing consulting work in cybersecurity. Some of these resources include online courses, industry forums, and professional networks. Read this article about becoming a cybersecurity consultant (https://openstax.org/r/109CyberConsult) from Springboard for some suggestions on getting started.

Importance of Continuous Learning and Adaptability

Cybersecurity is a rapidly changing field with evolving threats and vulnerabilities that demand constant vigilance. Herein lies the importance of continuous learning and adaptability. The ongoing process of acquiring new knowledge and skills, particularly to keep pace with evolving cybersecurity threats and technologies, is called continuous learning. The ability to change or be changed to fit new circumstances is called adaptability, which is a critical trait for cybersecurity professionals facing a dynamic threat landscape. Cyber threats mutate and adapt, and so must professionals in the field.

Technologies such as cloud computing and generative AI bring novel challenges, such as data breaches and AI-powered attacks. These evolving risks highlight the importance of adaptability and continuous learning in cybersecurity. Staying informed and flexible enables professionals to effectively safeguard digital trust across all sectors. Additionally, the ability to pivot and evolve your skill set in response to new types of cybersecurity risks is invaluable. It is this combination of continuous learning and adaptability that enables an information security professional to remain effective.

LINK TO LEARNING

As more nations adopt AI, there encounter both benefits and risks. On one hand, AI can be leveraged to read x-rays, and chat with a person in real time, or complete mundane tasks. On the other hand, AI can also be used to ramp up social engineering attacks (https://openstax.org/r/109AIAttacks) such as phishing, spam, and other malicious applications that threaten security.

Key Terms

advanced encryption standard (AES) symmetric encryption algorithm used globally to secure data, known for its speed and security

artificial intelligence (AI) branch of computer science focused on creating intelligent machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation

asymmetric encryption (also, public-key cryptography) type of encryption that uses a public and private key

authentication process of verifying the identity of a user or device, often through credentials such as passwords or digital certificates

brute-force attack attack method where an attacker systematically checks all password or encryption key possibilities until the correct one is found

buffer overflow condition where an application writes more data to a buffer than it can hold

Certified Ethical Hacker (CEH) certification that signifies proficiency in ethical hacking techniques and tools, and the ability to assess the security of computer systems by looking for vulnerabilities in a lawful and legitimate manner

Certified Information Security Manager (CISM) certification that focuses on management and governance of information security

Certified Information Systems Security Professional (CISSP) advanced certification that focuses on the knowledge and skills required to design, implement, and manage a comprehensive information security program

classless inter-domain routing (CIDR) method for allocating IP addresses and routing IP packets more efficiently than traditional classful IP addressing

confidentiality, integrity, availability (CIA) triad foundational model in cybersecurity that ensures information is protected, accurate and trustworthy, and readily available to authorized users

continuous monitoring ongoing process of assessing the security posture and compliance of an IT infrastructure by automatically collecting, analyzing, and reporting data on various security controls

Control Objectives for Information and Related Technologies (COBIT5) framework comprehensive framework developed by ISACA for IT governance and management that helps organizations meet business challenges in the areas of regulatory compliance, risk management, and aligning IT strategy with organizational goals

cryptographic key string of data used by encryption algorithms to transform data into a secure format and its subsequent decryption

cybersecurity practice of protecting systems, networks, devices, and data from online threats

data packet small unit of data transmitted over a network

dictionary attack attack method where an attacker uses a precompiled list of likely passwords

digital signature electronic signature that uses cryptographic techniques to provide authentication and ensure the integrity of the signed digital document or message

distributed denial-of-service (DDoS) attack that uses multiple computers or servers to overwhelm a network resulting in loss of usability

Domain Name System (DNS) system that translates human-readable domain names to IP addresses, allowing users to access websites using familiar names

dynamic IP address address that is assigned each time a device connects to the internet; changes periodically, although not necessarily every time the device connects

encryption process of transforming legible data into a coded format, making it unreadable to unauthorized entities

environmental threat uncontrollable external factor such as a natural disaster or hardware failure that can damage data centers and disrupt business operations

ethical hacking process of attempting to break into an organization's computer systems, network, or applications with permission to identify vulnerabilities

external threat threat that originates from outside an organization, typically posed by cybercriminals or state-sponsored attackers who aim to exploit vulnerabilities for financial or strategic gain

fileless malware type of malware that exploits in-memory processes to conduct its nefarious activities

firewall network security system that uses security rules to monitor and control incoming and outgoing traffic

hashing process of converting data into a fixed-size string of characters, typically used for security purposes to ensure data integrity

HTTP Secure (HTTPS) protocol that adds a secure, encrypted layer to HTTP via SSL/TLS protocols

Hypertext Transfer Protocol (HTTP) protocol that is proficient at transmitting hypertext over the internet

incident response predetermined set of procedures and steps taken to identify, investigate, and respond to potential security incidents

information privacy right and measure of control individuals have over the collection, storage, management, and dissemination of their personal information

information security practice of protecting information by mitigating information risks and vulnerabilities, which encompasses data privacy, data confidentiality, data integrity, and data availability; employs methods such as encryption, firewalls, and secure network design

information security management system (ISMS) framework that helps organizations manage their information security by defining policies, procedures, and controls

information security risk management (ISRM) field that involves identifying, assessing, and mitigating risks to the confidentiality, integrity, and availability of information and information systems

Information Systems Audit and Control Association (ISACA) international association that provides IT professionals with knowledge, credentials, education, and community in IT governance, control, risk, security, audit, and assurance

intellectual property (IP) creations of the mind that are protected by law from unauthorized use or replication

internal threat one that originates from within an organization, such as disgruntled employees or poor security training for employees resulting in social engineering attacks

internet protocol (IP) address unique identifier that allows a computer to be addressed in order to communicate on the internet

Internet Protocol Security (IPsec) suite of protocols that provides end-to-end encryption and secure data exchange

intrusion detection and prevention system (IDPS) tool that monitors networks for malicious activity or policy violations

IT governance process of managing and controlling an organization's IT capabilities to improve IT management, ensure compliance, and increase the value of IT investments

keylogger tool or technology often used maliciously to capture keystrokes on a computer to obtain sensitive information such as passwords

log file file generated by security applications that contains event information that aids in determining the status and health of a network

malware malicious software designed to damage, exploit, infect systems, or otherwise compromise data, devices, users, or networks, using viruses, worms, and spyware that is installed into the basic input-output system (BIOS) of a computer

media access control (MAC) address unique identifier that allows a computer to be addressed in order to communicate within a local area network

multi factor authentication (MFA) security measure that requires users to verify their identity using multiple forms of credentials, such as a password, a security token, or biometric data, to access a system

network security process of guarding network infrastructure and IT systems from unauthorized access, misuse, malfunction, or improper disclosure to unintended parties

packet sniffer (also, network analyzer or protocol analyzer) tool that captures and analyzes network traffic

phishing type of social engineering attack that appears as a trustworthy entity in digital communication but

steals user data, such as login credentials and financial information

pretexting social engineering attack that involves creating a fabricated scenario to obtain private data

protocol fundamental rule or procedure that governs communication between devices in a network

protocol analyzer tool that examines network communication protocols to understand how data are exchanged between devices and applications on a network

ransomware type of malicious software that encrypts users' files such as photos, documents, or other sensitive information and demands a ransom for their release

risk appetite level of risk an organization is willing to accept in pursuit of its ambitions or goals

risk management plan (RMP) strategic document that outlines how risk is assessed, monitored, and mitigated within an organization

risk tolerance number of unfavorable outcomes an organization is willing to accept while pursuing goals and other objectives

role-based access control (RBAC) method of access control that bases data access on a person's role in the organization, giving each employee the minimum level of access they need to perform their job functions

rootkit software that enables attackers to have access to a system masquerading as operating system processes

router device that forwards data packets to the appropriate parts of a computer network

RSA encryption asymmetric cryptographic algorithm used for secure data transmission; particularly useful in public-key cryptography

Secure Sockets Layer (SSL) communication protocol that establishes a secure connection between devices or applications on a network by encrypting data sent between a browser and a website or between two servers

security information and event management (SIEM) security solution that collects, analyzes, and correlates security data from different sources to detect and respond to security threats in real time

Security+ entry-level certification that covers foundational skills and knowledge in network security, compliance, operational security, threats and vulnerabilities, data and host security, access control, and identity management

server powerful computer or computer program that provides data to other computers (clients) over a network

social engineering manipulation of employees into revealing sensitive information, often leading to unauthorized system access

static IP address permanent address assigned by an administrator that remains the same over time and is essential for services such as hosting servers, email servers, and network devices, or when remote access is required

strengths, weaknesses, opportunities, and threats (SWOT) analysis commonly used method that helps in understanding both internal and external factors that could pose risks

subnet logically visible subdivision of an IP network, increasing its efficiency and security

subnet mask address used in routing and network organization that divides the IP address into network and host addresses

switch device that connects and segments various components within a local network

symmetric encryption type of encryption in which one key both encrypts and decrypts the data

Transport Layer Security (TLS) updated version of SSL that uses an encrypted tunnel to protect data sent between a browser, a website, and the website's server

Trojan program that conceals itself as a safe program but often carries many other different types of malicious payloads

virtual private network (VPN) service that creates a secure, encrypted connection over a less secure network, typically the internet, ensuring private data remains protected

virus malware that attaches itself to clean files and propagate to other files and programs

worm stand-alone software program that spreads without requiring a host program

Summary

5.1 The Importance of Network Security

- Routers act as gateways to both internal and external networks, with the capability of blocking unauthorized access and filtering traffic when the router has a firewall installed in it.
- Switches allow for network segmentation, and they can provide another layer of security by isolating traffic within VLANs.
- Networks go far beyond basic components and include protocols and services that control how information is transmitted and received. These items may include advanced firewalls, intrusion detection systems, and intrusion prevention systems.
- Key principles of network security include confidentiality, integrity, and availability (CIA) along with ensuring authentication, and authorization to track and monitor access.
- Information security focuses on shielding information from unauthorized access and breaches, promoting confidentiality, integrity, and availability of data. Alternatively, information privacy involves the proper handling, use, and storage of information and focuses more on the rights of individuals.
- There are several types of data that range broadly from simple files such as text messages, videos, and pictures to more sensitive types of data such as passwords, intellectual property, and personal data that require special handling and storage to promote safety.
- Vulnerabilities range widely from poorly configured networks to poorly trained staff weak in areas such as social engineering.

5.2 Security Technologies and Solutions

- Robust antivirus, anti-malware solutions, and intrusion detection systems are foundational technologies and solutions critical for protecting information and networks against a multitude of cyber threats.
- Understanding the nature of malware, social engineering, insider threats, DDoS attacks, and software and hardware vulnerabilities enables the identification of potential security threats and the selection of targeted countermeasures such as employee training and regular software patching.
- Regular penetration testing and vulnerability assessments are vital in recognizing security flaws, allowing for the proactive remediation of threats and the reinforcement of an organization's cyber defenses.
- Secure computing and risk management best practices involve conducting regular security assessments and enforcing access control policies to safeguard organizational assets effectively.
- While the cyber domain may be vast, there are several regulatory frameworks, such as GDPR and CCPA that provide protection for consumers from data mishandling, theft, and exploitation.
- Ethical considerations in cybersecurity, such as those involving ethical hacking, demonstrate the importance of employing security skills for defensive purposes, supported by a strict code of ethics to prevent misuse of expertise.

5.3 Information Security and Risk Management Strategies

- An effective ISRM strategy integrates risk identification, protection mechanisms, incident response, and recovery strategies, and it is underpinned by continuous monitoring and improvement.
- A comprehensive risk management plan encompasses the identification of potential threats, assessment of vulnerabilities, implementation of protective controls, and continuous evaluation to mitigate risks to the organization's information assets.
- Compliance frameworks such as COBIT5 by ISACA and regulations such as NIST's standards provide structured guidelines and best practices that organizations can use to align their ISRM strategies with industry requirements and improve their security posture.
- Continuous monitoring and improvement are vital to an organization's ISRM strategy, ensuring that the organization can adapt to new threats, leverage emerging technologies, and refine defenses in line with the changing security landscape.

5.4 Career Focus: Key Certifications

- The chief information security officer (CISO) oversees an organization's overall security strategy, developing policies and managing the protection of IT infrastructure, including incident response planning.
- Information security is an interdisciplinary field involving several sectors, such as IT, business, law, and psychology. This combination of disciplines is driven by the evolving nature of cyber threats and requires IT security professionals to be highly adaptable or have knowledge that spans several domains of IT.
- Earning certifications validates a professional's expertise and dedication to the field of cybersecurity. These certifications can be pivotal for career progression, moving professionals into specialized roles or leadership positions within information security.
- While entry-level certifications provide foundational knowledge, advanced certifications and degrees demonstrate a candidate's broad and deep knowledge of information security as well as their suitability for taking on high-level managerial roles that involve overseeing an organization's security strategy and IT teams. Financial institutions, government agencies, and health-care organizations are highly viable sectors for information security careers due to their need to protect sensitive data, comply with stringent regulations, and maintain public trust.
- Cybersecurity careers are not limited to the IT industry; they are critical in diverse sectors such as manufacturing, retail, and education. This is due to the increasing reliance on digital systems and the imperative to protect against growing cybersecurity threats in all areas of commerce and society.

Review Questions

1. What principle primarily concerns protecting information from unauthorized access, modification, or deletion?
   a. data encryption
   b. information security
   c. information privacy
   d. user authentication

2. What type of attack manipulates the Domain Name System (DNS) to redirect a website's traffic to a different IP address?
   a. phishing
   b. spoofing
   c. man-in-the-middle
   d. brute-force attack

3. What type of social engineering attack appears as a trustworthy entity in digital communication but steals user data, such as login credentials and financial information?
   a. spoofing
   b. hacking
   c. identity theft
   d. phishing

4. What authentication mechanism is the most secure?
   a. username and password
   b. two-factor authentication
   c. multi factor authentication
   d. biometric verification

5. What is the purpose of role-based access control (RBAC) in network security?
   a. to monitor and filter outgoing internet traffic
   b. to prevent data loss through email and web applications

c. to ensure users have access only to the resources necessary for their roles
d. to encrypt data transmissions over the network

6. Why are regular penetration tests important for maintaining organizational security?
a. They help in training IT staff on how to respond to media inquiries.
b. They allow for constant updating of the company website's content.
c. They enable the identification and remediation of early vulnerabilities.
d. They are a regulatory requirement for all businesses.

7. What is the cyber safety significance of applying regular software updates and patches?
a. They maintain the software's compatibility with new hardware.
b. They often add new features to the software.
c. They address identified security vulnerabilities to prevent exploits.
d. They are mainly for aesthetic improvements to the user interface.

8. How does ethical hacking differ from malicious hacking?
a. Ethical hacking is performed without the permission of the target entity.
b. Ethical hacking is intended to strengthen systems, not to harm them.
c. Ethical hacking does not require a deep understanding of IT systems.
d. There is no real difference; all hacking is considered unethical.

9. What is the purpose of antivirus software?
a. to increase the speed of the computer's processor
b. to protect against known threats and analyze system behavior to detect new threats
c. to manage the organization's email server
d. to offer technical support for software developers

10. What is the primary aim of a distributed denial-of-service (DDoS) attack?
a. modifying unauthorized data
b. disrupting the availability of a target's network resources
c. gaining unauthorized access to secure data
d. causing physical damage to the network infrastructure

11. What is a key process of an effective information security risk management (ISRM) strategy?
a. periodic security training
b. continuous monitoring
c. single-layer security
d. annual risk assessments

12. COBIT5 is an example of what type of ISRM resource?
a. a compliance framework
b. a risk management plan
c. a network security protocol
d. an incident response system

13. What organization is well known for developing standards and frameworks like COBIT to support compliance with ISRM practices?
a. IEEE
b. ISO
c. ISACA
d. NIST

14. What is the first step in developing a comprehensive risk management plan?
a. identifying risks

b. implementing controls
c. assessing risks
d. establishing the context

15. Why is continuous monitoring in an ISRM strategy important?
a. It allows for one-time setup of complete security controls.
b. It helps eliminate all cyber risks.
c. It ensures security measures are effective over time against evolving threats.
d. It provides a static security environment.

16. Why is it important to integrate continuous monitoring with other security processes?
a. to ensure compliance with COBIT5 only
b. to guarantee zero risk posture
c. to reduce the need for security training
d. to maintain a comprehensive approach to organizational security

17. Who is responsible for implementing security measures to protect an organization's data and ensuring that these measures are aligned with regulatory requirements?
a. security consultant
b. compliance analyst
c. security software developer
d. threat intelligence analyst

18. What role does continuous learning play in the field of cybersecurity?
a. to stay updated with the latest cybersecurity trends and technologies
b. to maintain a static skill set over time
c. to focus solely on traditional cybersecurity methods
d. to decrease the need for professional certifications

19. In the context of cybersecurity, what does the term "digital trust" primarily refer to?
a. the encryption standards used in digital communications
b. the confidence stakeholders place in an organization's ability to secure data and systems
c. the digital certificates used for website authentication
d. the trustworthiness of digital signatures

20. What is a significant cybersecurity challenge posed by the rise of cloud computing?
a. simplified IT infrastructure
b. decreased data storage needs
c. unique risks such as data breaches, unauthorized access, and compromised integrity of shared resources
d. reduced need for network security

21. In which type of organization would a Certified Information Security Manager (CISM) certification be especially beneficial for career advancement?
a. tech start-ups
b. government agencies
c. financial institutions
d. nonprofit organizations

22. Which role is essential for creating strategies to protect against large-scale cyber threats and managing an organization's overall cybersecurity posture?
a. network security administrator
b. chief information security officer (CISO)
c. IT support technician

d. cybersecurity legal advisor

Check Your Understanding Questions

1. Explain the role of encryption in network security and why it is considered a key principle.
2. What are some common network vulnerabilities, and how can they pose a threat to the integrity and availability of a network?
3. What is a common security vulnerability found in many web applications, and what countermeasure can be implemented to mitigate this risk?
4. Why is it important to consider ethical issues when performing penetration tests?
5. Explain why it is important for an ISRM strategy to have clearly defined roles and responsibilities within an organization.
6. What are the essential elements to include in a comprehensive risk management plan?
7. What are the primary responsibilities of a CISO, and how do they differ from those of an information security analyst?
8. Identify and describe the types of organizations where information security careers are most viable and explain why these organizations are optimal for such roles.

Application Questions

1. Reflect on the ethical implications of the distinction between information security and information privacy. How do these two concepts impact personal freedom and responsibilities in a digital age?
2. Consider a scenario where ethical considerations might conflict with legal requirements in the context of securing information and networks. How would you navigate such a situation?
3. Watch this video on developing an ISRM strategy (https://openstax.org/r/109ISRMstrategy) from ISACA Live. Search for an ISRM case study and look for some of the elements discussed. What elements discussed in the video are missing from the ISRM case study you found?
4. Should managers depend solely on IT people to solve all security challenges? (*Hint*: Consider the types of decisions made by general managers versus IT managers.)
5. Consider the sectors that are currently most at risk for cyberattacks. How do you think the demand for information security roles within these sectors will evolve in the next five years?
6. How would you describe the job of a cybersecurity engineer/manager to someone who does not work in the tech field?