Course Book

INTRODUCTION TO DATA PROTECTION AND CYBER SECURITY

DLBCSIDPITS01

iu

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

LEARNING OBJECTIVES

The course **Introduction to Data Protection and Cyber Security** gives you an overview of the most important basics of this field. This course book introduces key aspects of privacy and cyber security, with a focus on practical mechanisms and concrete solutions. In addition, it provides an introduction to relevant legal aspects in a national and international context. This approach is rounded off with recommended procedures for prevention, detection, and correction of privacy and cyber security gaps.

After successful participation, you will understand and master the legal framework of data protection and cyber security, as well as the theoretical models, operational goals, and basic principles of data protection and cyber security. You will also learn about important standards and management approaches to cyber security. Finally, proven protection and security concepts for information technology (IT) devices and IT infrastructures will be presented.

UNIT 1

FUNDAMENTALS OF CYBER SECURITY AND DATA PROTECTION

STUDY GOALS

On completion of this unit, you will have learned …

- the meaning of confidentiality, integrity, and availability in the field of cyber security.
- the importance of strategy in planning security defenses.
- the importance of risk management in cyber security.
- which legal and compliance key concepts relate to cyber security.

1. FUNDAMENTALS OF CYBER SECURITY AND DATA PROTECTION

Introduction

Information technology (IT) is everywhere in our lives: in the office, in the home, in restaurants, and even in our cars. We can hardly imagine our personal lives without smartphones or email, and our relationships with friends near and far depend upon social media, such as Facebook or Instagram. People universally depend upon information and communication systems for their increasingly digital lives. Information about their personal lives, family, and health are stored online. People bank online, and their financial data and identifications numbers, such as national identification, bank, and credit card numbers, are stored in information technology. This technology is often outside of their direct control, in locations and organizations they do not know.

This holds true for organizations as well as individuals. Businesses use their web sites, Yelp reviews, and Google Maps to guide customers through their doors. They make global sales through online shopping carts and distributors. More broadly, businesses and organizations that wish to survive long into the twenty-first century must find new digital models of service and production. This increasingly technological model requires skills that business owners and producers are rarely trained in. The growing use of technology leaves the business and its owners reliant upon service providers to protect their reputation and their customers' security.

Many of these consumers and business owners are therefore concerned about the security of their data and devices—and rightfully so. The media continues to cover stories about how little control people truly have of their own private information. Social networks pass on member data to advertisers without permission. Criminal hackers succeed in gaining access to millions of customer datasets. Hospitals dispose of printed patient data in old paper containers, without shredding it or checking for sensitive health information. Businesses that run their own IT have problems finding skilled security resources to protect them, while those that outsource technology suffer from intrusions into their vendor's networks. They may even be subject to attacks from the employees and contractors who work with their vendors. Organizations are not required to publish details about their security, and only some companies are required to have proof of their implementations.

Adding to this pressure, businesses and individuals must assume that they are subject to foreign and domestic government interests. Since the revelations of Edward Snowden, an American whistle-blower and former U.S. Central Intelligence Agency employee, we must assume that there are foreign or domestic government agencies with unhindered access to our smartphones, computers, and emails (Davies, 2019). Some governments demand their own back doors for encrypted devices from the manufacturers, limit the security devices that can be used inside their borders, or even ban all encrypted communication.

Unfortunately, these are not hypothetical scenarios. Time and again, information about unwanted or unauthorized access to personal or business data reaches the public. Experts warn us that these cases are only the tip of the iceberg. The privacy of the individual, and the security of information and communication systems, is subject to continuous attack. But what is privacy within information technology? How do we measure it? What is a realistic expectation of security for information and communication systems? Which threats and dangers are most likely for private users of technology and for organizations?

1.1 Conceptual Bases, Protection Goals

This section addresses concepts in security and protection goals relevant to the field of data protection and cyber security.

Concepts in Security

Relevant security concepts are as follows: valuable assets, data protection, privacy protection, vulnerabilities, attacks, threats, and risk, including risk management and treatment.

Valuable assets

In business, the term “asset” is used to describe anything with utility to the organization. Assets may be tangible or intangible. A chair is an asset, but so are employees, computers, and the data that are stored on the computer. All assets have a value, some more quantifiable than others, and people are, without exception, the most valuable assets of a business. The lives of the workers are valuable, but so are their skills, their privacy, and their goodwill toward the organization. Data are also valuable; many organizations now make money solely because of their ability to process or generate data. Physical assets are the easiest to quantify in value, as they may be leased, sold, or purchased.

One intangible asset with considerable value is the reputation of the organization. People and businesses support an organization based, in part, upon their trust in its reputation. This applies to most organizations, whether they are commercial, charitable, or community-based; however, the impact of reputation varies widely. For professional consulting organizations, who sell services and trust, a reputation may be critical to maintaining business. For a soda manufacturer, purchasing decisions depend upon consumer appeal and name recognition, and even minor damage to the reputation of the organization may have a significant impact on sales. Reputational value and the part that it plays in gaining support is therefore difficult to quantify.

Data protection

Data are a type of asset, but, like other intangibles, their value can be hard to quantify. The value of a set of data can depend in part upon its secrecy. For instance, the secret formula for a soft drink may be of great value to its manufacturer or their competitors. Value might also depend upon utility; while a decade's worth of weather conditions in Cote d'Azur is publicly available, the combined information is valuable to a weather-predicting application only if it is correct.

Security decisions around data should account for an understanding of their content, use, and location. An organization in possession of data may have ethical or legal responsibilities for how that data is treated. If data originated elsewhere, the data handling standards may be set higher than the receiving organization would normally require.

Privacy protection

Privacy is the right for any entity to control the distribution and confidentiality of their information (NIST, n.d.). Violations of personal privacy cause significant distress and potential harm; this should be counted among the highest of organizational concerns. Personal privacy data includes, but is not limited to, national identifiers (Social Security numbers), birthdates, individual physical and email addresses, gender and sexual preference, spousal information, medical conditions, political affiliations, and financial information. Privacy protection is addressed by many of the same precautions as general data protection. Additional measures needed for privacy protections are determined based upon the type of private information involved.

Vulnerabilities

Vulnerabilities are identifiable weaknesses in technology, physical constructs, people, or procedures that create an opportunity to attack. For instance, a computer that is connected to the internet prior to proper security procedures is vulnerable to many attacks. If that same computer has been through security procedures, it will have fewer vulnerabilities and fewer attacks will succeed. Likewise, an employee who holds open doors for people they do not know presents a vulnerability. If that employee is informed that unauthorized persons are entering the building due to this behavior, they may choose not to repeat the action, thereby lowering the vulnerability to a physical intrusion.

For software and hardware, most organizations rely upon the supplier to provide "cures" for vulnerabilities. These "cures" are called patches, updates, or upgrades. Procedural and awareness vulnerabilities are usually the responsibility of the organization itself. These can be repaired by training organizational users and revising procedures, although, as is always the case with humans, the success of the repair is highly dependent upon the will to change.

Attacks

Exploits are methods of attacking vulnerabilities. Exploits may be a direct result of the vulnerability, such as guessing a short and uncomplicated or default computer password. They may be deliberately constructed, such as a complex automated software installation triggered when a user visits a risky website. For most purposes, the word exploit can be understood to mean attack for IT, whether talking about the object ("an exploit exists for this flaw") or the activity ("an attacker can exploit this flaw").

Threats

Threats in cyber security and data protection include threats to operations, as well as threats to data security. Threats include hazards, such as natural disasters and accidents, as well as malicious individuals or groups who have an interest in stealing data or otherwise damaging assets. In the scope of this course book, most of the threats identified are the aforementioned persons and groups with malicious intent. This is because disasters and hazards that are not directed by humans are well understood as risks to the business and are covered in other types of education, such as business risk management.

Entities that invest in criminal activities may be referred to by a wide variety of terms. Some are labeled specifically out of necessity, such as governments, intelligence agencies, activists, and organized crime rings. The terms used most commonly throughout this text are as follows: criminals, criminal hackers, malicious actors or bad actors, malicious organizations, criminal organizations, and attackers. All of these terms should be understood to mean the same entity or type of entity. Unless otherwise specified, these terms are generalized to all the different types of attackers. If one such type of attacker is meant to be differentiated, they will be specifically named. One should also understand that the different types of attackers have different motivations. It is possible, although less likely, that an attacker is motivated by idealism or a desire for bragging rights (or other types of fame). Some attackers are moved by organizational gain, as with patriotism. Most often, the attacker is motivated by financial gain. This is substantiated by the fact that one rarely sees data theft that is not accompanied by the attempted sale of this data in unindexed "dark web" forums.

Risk

Risk is the likelihood of an undesirable event and the result if that event occurs. The potential for harm, damage, or loss is unavoidable. Each day, humans must face risk to take any action; this also applies to making any IT decision. The goal of IT security is to reduce the amount of risk to a tolerable level. To do this, one must understand the nature of risk, what influences risk, and how risk is estimated. Risk exists when there is an asset, a vulnerability, and a threat. But how does a risk come about?

An example risk scenario

A common scenario in IT is a missing computer patch. Suppose that twenty heavily used servers in an organization are missing a patch that protects from a particular attack. Those servers host personal sensitive data and there is a known attack that works on servers without the patch. Most successful attacks force the servers to stop functioning. Very rarely, the attack allows quick creation of a new administrator account. This attack is actively being used on the internet.

The assets are the servers, both the data they store and their ability to function. The vulnerability in this case is that some servers do not have current security patches installed. The threat is the attack that creates new accounts or stops servers from functioning. The risk of failing to patch consists of the value of the information, the function of the vulnerable servers ,and how likely it is that the attack will infect computers without being noticed. Risk is quantified using a rough calculation of asset value, vulnerability severity, and likelihood of threat being realized.

The asset value is high; if twenty servers with personal data were compromised, this could harm humans whose data is stored there. Additionally, the organization and the data owners might face penalties for inadequate data protection. The vulnerability severity is also high, as there is an exploit actively spreading. There are two different possible bad outcomes: The servers may be compromised when the exploit is attempted, or they may unexpectedly shut down and take time to recover.

Data compromise
When information is inappropriately changed, or when someone accesses it without proper authorization, the data has been compromised. Data compromise is commonly understood as a result of attacks on cyber security.

We see in this scenario two different risks, with two different severities. The first of these is **data compromise**, in which the asset value and the vulnerability severity are high. The likelihood of the threat being realized is low or moderate. Overall, this calculation would be a medium risk. If data collection were the only concern, the data owner might not see this as a reason to act with urgency. They may reasonably choose to schedule installation of the missing patches later.

The other risk is that of data unavailability. In this case, the asset value and vulnerability severity remain high, the likelihood of the servers becoming unavailable is high, and the risk of data unavailability is high. If the data owner is concerned about controlled server downtime, they will be concerned about the potential for unexpected server downtime. This is a reason to act with urgency and schedule the installation of missing patches as soon as possible, even if it inconveniences server users. The high risk demands immediate action. As in this example, not all risks can or should be remediated immediately. However, high risk is a reason to act with urgency.

Risk management and treatment

Risk management
If an organization has a program to identify, remediate, and track risk, they are practicing risk management.

When determining how to handle risk, it is important to first understand how widespread risk is in the organization. The activities around discovering, quantifying, treating, and reporting on risks is called **risk management**. In large organizations, or in organizations where data is highly regulated, a formal risk management program may be required. A formal risk management program will often involve operational and financial executives, legal counsel, public relations, IT managers, and IT security personnel. In a smaller organization, risk management may be informal—a general understanding of who needs to be informed or when a decision must be made that involves a potential loss of money, functionality, or goodwill.

Risk treatment
The choice of how to address each risk is called risk treatment. Risk treatment options include accepting risk, mitigating risk, and risk transference.

Risk treatment is the set of decision and actions that follow risk discovery. Any reaction to a risk can be categorized as risk treatment. Ignoring the risk, correcting the risk, accepting the risk, insuring against the risk loss (risk transference), or finding an indirect method to lower the risk (risk mitigation), are all ways to treat risk. Although it may seem counterintuitive that accepting risk is considered treatment, not all risks are severe enough to merit change. If a risk is within the threshold of an organization's tolerance, it is said to be within the risk appetite. Risk appetite is specific to the organization, and often it is different for different departments within the organization. It should be noted that ignoring risk is an inadequate strategy for almost any scenario; its potential legal, security, and financial ramifications far outweigh the immediate gains.

Protection Goals

Relevant protection goals include the concepts of confidentiality, integrity, and availability, as well as protection targets.

Confidentiality, integrity, and availability

Implementation of security in information technology is usually based around the concepts of **confidentiality, integrity, and availability (CIA)**. These three concepts express the need for planning an IT system that is reliably functional, where the accuracy of data is preserved, and when the information is available to those with both need and permission to access it. A well-secured system incurs a low amount of business risk. The organization can perform necessary functions using this IT without anticipation of technical, reputational, or legal issues. Needs for confidentiality, integrity, and availability vary with different information systems and data collections, even inside the same businesses. Some security practices, such as reviewing data access regularly, can reasonably be applied to all information systems. Others, such as requiring a physical token to access a computer, are only needed when misuse of the information system would cause harm to the organization. IT owners and users should be able to define and explain broad considerations for each aspect of CIA.

Confidentiality, integrity, and availability (CIA)
Also called the CIA triad, these are the three protection goals of cyber security.

Confidentiality

Data are only known to authorized persons; functions are only used by authorized persons. To determine the strictness of confidentiality needed, an IT owner can consider the following questions: What is the harm if these data are published on a roadside billboard or in a newspaper? Would the organization have legal trouble as a result, or would they lose contracts and trust from their customers? Would the personally identifiable information (PII) principal be embarrassed or be subject to higher likelihood of identity fraud? Would their rights to privacy be violated?

Integrity

Data are correct, complete, and up to date; functions that process data are reliable and trustworthy. If this is not the case, the changes to the data must be obvious. To determine the strictness of integrity needed, an IT owner can consider the following questions: What is the harm if this data is inaccurate, or if conclusions based on this data are inaccurate? Would someone make a medical misdiagnosis or perform the wrong treatment? Would an organizational merger based on faulty data be disadvantageous? Would a person applying for a home loan be turned down or get a worse mortgage rate than their credit history would warrant? Integrity of data determines their utility to guide decisions. Data that are not confidential may still need strong integrity controls.

Availability

Data and functions are accessible where and when they are needed by authorized persons. The IT owner should considerthe following questions: Can a business process not be carried out without this information system or its data? Would there be penalties for missing data, and are there laws prescribing its availability? Will the lack of data be harmful to a person, such as lacking a record of their birth or educational achievements?

Confidentiality, integrity, and availability are grouped, in part, because they are interconnected, supporting and balancing each other. For instance, if few people can access data (confidentiality) and few can change them (integrity), this is, in most cases, preferable to allowing the widespread ability to view and change data. In this instance, enforcement of both confidentiality and integrity support each other. However, integrity is best maintained by careful application of access controls. Access to read data should not be unnecessarily coupled with the ability to change data. Also, the ability to enter data should not always include the ability to change it later in processing—for instance, after initial data have been reviewed or approved by others. These access controls require more people with the ability to view data, so that the organization can maintain the separation of reading, entering, and changing it. In that case, confidentiality and integrity requirements oppose each other. However, protection is maintained, the persons who own data and process them must make decisions about the balance of security requirements that best supports the organization.

Protection goals

The need for protection can be based upon expected damage if confidentiality, integrity, or availability of an asset is compromised. Damage can be to any asset, including the intangibles, such as data or reputation. Financial stability is often the most easily understood protection goal for a commercial organization, but the most important are those with direct human impact, i.e., physical safety and personal privacy. These protection goals do not stand alone. For example, failure of legal compliance often carries a significant financial impact. Likewise, failures of personal physical safety will result in damage to the organization's reputation. Common protection goals include

- legal compliance. The organization should perform at least the minimum protective activities that ensure it operates in a legal manner.
- contractual obligations. Many commercial organizations rely upon contracts to manage their business relationships. These contracts will include requirements for performance in order for the organizations to continue their relationship and the exchange of money. Cyber security, data protection, and operational targets are often the subject of the performance requirements.
- personal privacy. Even in the absence of legal requirements, organizations should strive to keep private, personal data safe from needless disclosure.
- personal physical safety. Any human, in any relationship with the organization, should be protected from physical harm caused by the action or inaction of the organization.

- operational performance. Most operations have an expected uptime and output. The success of the organization will often depend on meeting or exceeding operational performance goals. Protecting all resources needed to meet these performance goals should be a priority of the organization.
- reputation. The impairment of an organization’s reputation can have a long-lived impact on their ability to attract clients and consumers. Further, reputation is a significant factor in attracting high-performing workers.
- financial impact. Although it is not the most critical protection factor, financial impact is often widely visible. IT incidents in any form can deeply affect the health of an organization, especially in combination with the contractual and legal impacts.

Organizations often attempt to reduce protection goals to financial impact. This is a reasonable method of normalizing risk quantity. However, there are further aspects to consider when deciding which protection goals to prioritize. Protecting humans should always be given priority, even above legal compliance.

1.2 Attacks and Threats

This section introduces the most common physical attacks and their threat actors relevant to the field of data protection and cyber security.

Physical Attacks

Well known physical attacks that pose a threat to the protection of data and cyber security include technology theft, shoulder surfing, and document theft.

Technology theft

Stationary IT devices (e.g., desktops and external hard disk arrays) and mobile IT devices (e.g., laptops, notebooks, tablets, smartphones, and USB sticks) store organization information. For this reason alone, they should not fall into the hands of unauthorized persons. Also, in spite of the constant drop in the price of IT equipment, the material damage caused by equipment theft can be significant. In the home or workplace, theft protection can be supported by observing the clean-desk principle, which implements the tasks of tidying up and locking. Order makes it easier to track items in your workspace and see that none are missing; keeping order by securely storing materials not in use also reduces the risk of IT equipment falling into the hands of unauthorized persons. Digital equipment and sensitive documents not actively in use should not be visible to casual visitors of a workspace. In addition, mobile IT devices, including mobile phones, should be locked away (e.g., in a cupboard, drawer, or roller container) if they are not required for the current work task. During longer absences, for example, at the end of a working day, the rooms and containers that house IT devices should be locked. Keys should be removed from the locks and kept separately.

Shoulder surfing

Shoulder surfing is the surprisingly effective attack of looking over the shoulder of a target to view sensitive information. A common scenario for shoulder surfing is when the attacker watches the victim enter a personal identification number into an ATM or unlock their phone with a numeric code. This attack is not limited to access codes and passwords; intruders may find great value in simply viewing confidential information in presentations or documents of those whom they pass behind in a public space such as an airport, café, or train. Shoulder surfing requires physical access to the target, but it does not require physical interaction. Unless the victim is particularly observant, shoulder surfing often goes unnoticed. The difficulty of using the stolen information dependends on the target of the activity. For instance, if a person is typing sensitive information, the information itself may be sufficient for the theft to be complete. If the input information is one of several components needed for the attack (like the aforementioned personal identification number for an automatic teller or a mobile phone), additional actions may be required. The criminal may need to obtain the credit card or a clone of the card, or they may require access to the person's phone. Access need not be permanent, but it must be long enough for the criminal to perform their intended action.

Although the above combination of shoulder surfing and theft is more difficult to perform in rapid succession, planning ahead for the physical theft is not as necessary as one might believe. It is not unusual to exit a public space or an office with a bag containing a laptop. People are not often stopped and asked to prove that a cellphone or laptop is legitimately their own.

Document theft

Document theft is another effective and old-fashioned data attack. Whenever an intruder can enter an office or a shared public space with a printer, they may find documents to which they should not have access. It is normal for users to print many documents but retrieve them only when there is another reason to leave their desks, or even to forget about the print-out altogether. Yet there might be no other mechanism in place to protect their document, leaving it available for anyone who passes by to peruse. One does not normally find it suspicious to see someone standing at a printer looking at the documents that might belong to them. Nor does it seem unusual to see a person remove documents from a printer.

Logical Attacks

Well known logical attacks that pose a threat to the protection of data and cyber security include phishing, malware, denial of service (DoS), and distributed denial of service (DDoS).

Phishing

Phishing is a type of social engineering attack that uses email, social media, or text messages. In the message, the scammer describes a fictional situation and hopes the recipient will provide data in a suggested response. The response might require that the recipient provide private data or directs the recipient to take a form of action, such as electronically sending money. Phishing scams often have a type of emotional impact to prey upon greed, fear, or sympathy. Examples of phishing are

- pretending to be royalty of a far-away country, hoping for someone to assist with moving assets out of the country;
- sending emails stating that a person's social security number has been compromised, and it will be "shut down" unless they verify by giving personal information; and
- posing as a friend who was robbed while traveling and now needs funds to return home.

Phishing scams will impart a sense of urgency, inciting the victim to act immediately. These scams remain popular because they require a low investment relative to the potential reward. Judged individually, a phishing attempt is unlikely to succeed. However, phishing attempts are rarely individually distributed. Automation, such as mass emails or text messages, make it possible for the criminal to send thousands of phishing attacks at a once for little effort and expense. Phishing therefore offers a potential return for little work, providing a high return on investment for each success.

Malware is a portmanteau made of the term "malicious software," and both can be used interchangeably. Malware is the name for several different types of software with undesirable effects. Most malware is installed and run without the user's knowledge. In the case of a computer worm, it may be run without any activity. Currently known types of malware are viruses, worms, Trojan horses, spyware, and ransomware. Ransomware is the youngest and most sophisticated malware categorization, but all have the potential to cause significant damage to an organization.

Malware
This can be self-contained or disguised as part of another item, causes harm to the recipient, and often seeks to propagate within an organizational boundary.

In IT, viruses are self-propagating software fragments. Viruses spread from computer to computer executing pre-programmed malicious functions. Viruses are attached to a legitimate file, such as an email or an office-software document. The virus then infects the machine and attempts to propagate itself with the resources of the new computer. Virus programs are often designed to hide their own existence and, at the same time, infect as many other hosts as possible. Viruses may rely upon user actions or the execution of another file to begin their infection and spread.

In contrast to viruses, computer worms are complete software programs that use the IT infrastructure to spread themselves, independent of user activity. Worms can also affect platforms (e.g., smartphones) that have otherwise long been spared from viruses. A famous worm from 2003, SQL Slammer (also called SQL Sapphire), spread from its original release around the world in minutes. Commercial datacenters and internet providers were overwhelmed in a matter of hours, with the unexpected result that much of the internet, from websites to automatic teller machines (ATMs), could not send or receive any other network traffic. This behavior illustrated the danger of automated attacks to common resources for internet-dependent devices (Grimes, 2019).

Ransomware is a special type of virus that weaponizes encryption technologies. Modern encryption allows data to be security scrambled so that a certain device, certificate, or passphrase (key) is required to make the data readable. Ransomware is an attack in which the data are encrypted but the attacker has the key. The operating principle is simple: The malware is sent as an attachment to an e-mail or downloaded as a file. If a user clicks the file, the ransomware installs itself and begins to encrypt data. Some ransomware encrypts everything it can access, including cloud storage. The user is then asked to pay a fee (to ransom the data) if they want to receive the key for decryption. Ransomware is a newly popular type of attack, but it is dependent upon the target organization being unable or unwilling to restore the encrypted information from backup data.

Trojan horses (also known as Trojans) are programs disguised as useful applications, but which contain additional functions that are executed without the user's knowledge or intent. Trojans, like viruses, secretly execute actions on the system so that the user does not notice them. Unlike viruses, the user knows that they are installing an application—they just do not understand everything that is being installed. Trojans are full applications that could perform a wide range of illicit, hostile functions. Common Trojan horses will capture banking and personal information, perform attacks on other IT systems and networks, or even provide full access to the user's computer on which the Trojan is installed.

Spyware is a specialized categorization of undesirable software. It may be incorporated into overt malware, or it may be packaged into a legitimate software. Whether software is considered spyware is determined by its functionality, not its source; it provides data about the user or organization back to the software provider. Spyware may target a variety of data, including, but not limited to, the user's internet browsing habits, the information that they type on the keyboard, or their confidential information stored in the computer. This type of malware is unusual, in that spyware almost always spreads when the user deliberately is installing software (though the user, of course, does not realize what exactly they are installing).

Spyware as software installation has become less popular as organizations have learned to interact with their users' internet browsers. Often a computer user will allow cookies (small tracking code) to be stored on their browser to make returning to sites more convenient. This allows organizations to monitor other sites and products the browser visits, thereby allowing for more targeted advertising. Some businesses sell or share visitor information with others, though this practice is also becoming less popular as consumers realize that organizations may build advertising profiles or profit from monitoring their browsing habits.

Denial of service and distributed denial of service (DOS/DDOS)

Denial of service (DOS)
This is an attack that prevents information technology resources from providing intended services by overwhelming or blocking expected activities, usually as part of a network-based attack.

Denial of service (DOS) attacks aim to paralyze networks and, by extension, the services offered in networks. This is typically achieved by bombarding a service offered in the network with so many requests that it can no longer comply with regular requests. In connection with DoS attacks, data rates of over 300 Gigabits per second are often observed. In distributed DoS attacks (DDoS), a DoS attack is carried out by several participants simultaneously. DDoS attacks can also be executed by a botnet, which is a group of network devices that can be remotely controlled. In most cases, the owners do not even know that their devices are part of a botnet.

Unfortunately, it is difficult to protect against DoS attacks. Services can rarely distinguish regular requests from attacks when the target is a publicly offered service. Therefore, it is especially important to completely disable unnecessary network services. If a service is overloaded by only one or a few attackers, protection against a denial of service attack can be prevented with the help of simple traffic-deny lists, which are enforced by a firewall. Another possible countermeasure against overloads is load balancing, where the affected service is executed on several IT devices. The latter measure would also be effective to prevent some DDoS attacks.

Threat Actors

A threat is any source that might cause the loss of use of an asset. For cyber security, it is important to understand the threat actors, which are people and groups who attack information systems and network. Threat actors are differentiated by their motivations, attack goals, and behaviors. Most attackers are, in some way, driven by financial gain. Those who are not have similarly strong motivations, such as patriotism or loyalty to a cause. Threat actors whose work is primarily computer-based are often simply called “hackers” in the media and casual parlance, but this is a misnomer. The term “hacker” can be used for anyone who enjoys finding workarounds or disassembling technologies. This misleading use of language should be avoided, as many law-abiding hardware and software enthusiasts consider themselves to be hackers.

Opportunists

Opportunists are criminals who do not specifically plan a long-term strategy to attack a single organization, sector, or type of person. Instead, an opportunist sees an opening for exploitation of vulnerability and acts on it with agility. Opportunists rely upon organizations and people to be careless in the execution of their security responsibilities; therefore, the opportunist must have a ready ability to exploit a situation.

Opportunists do not specifically aim to make a steady career from the opportunities they exploit. Instead, their less-planned attacks are agile, spontaneous, and difficult to predict. An opportunist cannot cause a great deal of damage, but their methodology is not dependent upon long-term outcome.

Professional criminal hackers

While opportunists act in an agile and less-planned fashion, professional criminal hackers or groups of criminal hackers will often coordinate a strategy to ensure that the results of their criminal activities are as profitable as possible. Professional criminal hackers make their entire living from performing computer and network crime; they may work independently or perform activities at the request of others for an exchange of funds (criminal hackers for hire).

The professional computer criminal is also not to be confused with loose-knit idealist groups, such as Anonymous, which is comprised of volunteer members who do not know each other well but instead act due to a common goal. These groups of professional hackers perform activities that ultimately lead to the exchange of money for their skill in unlawfully penetrating networks. While these professional criminals share characteristics with nation-state actors and hackers for organized crime, they lack the patriotic or organizational affinity that defines the other two groups.

Organized crime

The traditional picture of organized crime is of those who deal in physical crimes. Human trafficking, illegal drugs, and extortion have long been known to be in-person activities. However, with the advent of the internet and the poor protection of data assets, the ability to perform these same crimes with a digital component should not be underestimated. Human traffickers routinely use the internet to perform sales or arrange time with their victims. Likewise, those who trade in illegal drugs can do everything from advertise their substances to accurately plan caravan routes for the movement of illegal substances across country borders. Finally, the collection of information for extortion becomes a great deal simpler when private data are available on unprotected networks and computers. Organized crime has found new methods of business by buying and selling personal and financial data on unindexed sites on the internet. Transactions that bring in only small amounts each are not worthwhile on their own. However, when data are sold in bulk, the small price of each transaction adds up to a substantial amount.

Business competitors

Even the most honest business finds it worthwhile to understand their competitors' goals, financial situation, level of skill, and future plans. Some organizations move past honest competition and into illegal methods of gathering data. It is not unusual for business competitors to perform information-gathering by collecting publicly available data, luring away top talent, or consulting research professionals to estimate the strategies and financial moves of their industry leaders for the next several years. However, some organizations find that they can efficiently gather data using network intrusions and physical intrusions into a competitor's space. Once inside, the rewards of a successful intrusion may include all the above. As a bonus, theft of intellectual property from the compromised network may grant the dishonest organization the benefit of months or years of research without the investment that is normally required.

Nation-state actors

Nation-state actors
These are people who represent the interests of governments or military organizations in the compromise of networks and information systems.

Nation-state actors are groups of governmental employees, and often military personnel, who are hired and empowered by their governments to perform cross-border network crimes. These personnel are trained professionals whose daily work is to perform sophisticated attacks on other governments' networks. Occasionally, it is also in the interest of these government hackers to attack their victim's contractors. It is rare for nation-state actors to perform attacks against small businesses. Instead, they concentrate on large organizations that either directly influence the workings of a government, the foreign government itself, or the economic health of that government in some fashion. Recently, there have also been attacks on organizations that manage governmental health data, whether it be public or private. It should be assumed that the goal of these attacks is not the sale of this information on the criminal networks, but instead, the use by the home government.

Advanced persistent threat

The advanced persistent threat (APT) is any type of network criminal who has a reason to use stealth and planning to achieve their goals. Characteristics of the APT attacker are: stealth, usage of new or unannounced vulnerabilities, technical skills, and long-term goals. APT intruders do not attempt to gain access, perform their tasks, and stop using the computers quickly, as with many other patters of criminal hacker behavior. Instead, they attempt to enter the network undetected, remain in the network for as long as possible without discovery, and execute only subtle activities. This usually manifests in attacks that are deliberately below detection thresholds for any sort of network detection that the organization uses. The advanced persistent threat, once it has infiltrated the network, will find computers open to compromise. It then uses these computers as a base for its operations. This broad footprint inside an organization aids in the effort to create a long-lasting and uninterrupted presence.

The goals vary depending on the type of criminal acting as the advanced persistent threat. In the case of the competitor, they may choose to move data outside of the victims' network and into their own, targeting financial or legal information. The organized criminal may choose to exfiltrate personal health or financial information and sell it on unmonitored internet sites that were established for such criminal purposes. The nation-state actor, which is the most common type of advanced persistent threat, may choose any number of activities, including sabotaging the networks; retrieval of data, such as classified documents or documents that would cause reputational harm to the organization; theft of intellectual property; or simply watching network and computer traffic, providing a virtual base to spy on the organization that they have infiltrated.

Advanced persistent threat actors commonly use "zero-day exploits." Zero-day exploits are attacks that have not yet been recognized by the general security or hacker communities or by the impacted software manufacturers. They are rarely detected by network or virus intrusion detection methods. Though indicators of compromise might be available, the indicators are not recognized and the victim, therefore, does not understand what has occurred on the network.

1.3 Security Strategy

For most organizations, security strategy is merely choosing the approaches to information security that best suit their budget, legal or contractual requirements, and types of data to be protected. Security strategies are not meant to stand alone; an organization will choose several security strategies in order to implement a full program with adequate protection. Some of the most popular security strategies, which demonstrate how strategies complement each other and overlap, are defense in depth, encryption everywhere, and assume breach.

Defense in Depth

Defense in depth
This organization strategy for security depends on layers of controls rather than single points of protection, such as organizational firewalls.

Defense in depth assumes that one layer of security (such as malware protection or rigorous patching) is not sufficient. Instead, the organization creates a set of interrelated controls to stop an attacker at many different levels of activity, even an attacker who has already penetrated the network. Defense in depth begins with the recognition that a firewall is not sufficient to keep out an intruder and goes on to assume that any one area of protection may fail, thus, another layer of protection must be available to protect assets. For example, information on the end user's workstation should be protected in several different ways. It is necessary to have virus protection, rigorous software patching, authorization and identification control, and encryption of any sensitive data. If a user's workstation is mobile, then there must be the ability to protect the workstation from physical theft. By having these several types of controls, the defense in depth strategy protects both access to functionality and physical access to the user's computer. The user can then protect their machine from malicious network attacks through rigorous patching and virus protection. Finally, if there is access to machines either physically or through the network, the data themselves are encrypted and only those who need them have access to the encryption keys. This is merely one example of defense in depth, but the basic philosophy can be used to design protections for all of the organization.

Encryption Everywhere

A part of protecting information in any information security strategy is encryption. Encryption everywhere is the concept that data are vulnerable in storage and in transit. This strategy protects data that are transmitted over the internet and the local intranet, data that are stored in databases or on the servers, and files on workstations. When encryption first became available for data storage and transmission, businesses had a legitimate concern that encryption and decryption of data would impose too heavy a burden on the computers' processors. As computer processors have become much faster, and computers have become able to hold more data in memory, this concern is no longer valid.

Several of the original types of available encryption are now obsolete or considered weak or easily broken. An organization should choose encryption that is considered to still be effective for as long as the information needs protection and it must provide decryption access only to those who need it. Encryption decisions should consider the type of encryption and the location of the data, as well as the question of who should possess encryption keys. More technical units of this course book go into detail about the types of encryption and how to manage an encryption program for your organization. It suffices to say here that encryption is no longer a burden on the processing power of the computer and all data should be encrypted unless there is a specific reason to choose otherwise.

Assume Breach

Assume breach
This strategy plans security controls with the underlying assumption that past attacks have already been successful.

Assume breach is a modern security mentality that presupposes intrusion into the network or compromise of computers on the network has already happened. While this may seem like a pessimistic outlook, assume breach requires the IT professional to ask the question, "Are we protected from this attack?" even when it can only be launched from inside the network. This is a useful position from which to design new implementations for computer networks and for information systems. The assume breach mentality allows the business to more easily react and recover from true breaches that occur. It is unrealistic to think that an organization will never experience a security incident that makes it past firewalls and intrusion detection mechanisms. This modern strategy allows the organization to play out what-if scenarios and determine whether internal security protections and procedures depend on only a few critical first-layer defenses.

Compliance and Security

Responsibility for security

When an organization defines an IT security program, one of the most important decisions will be who ultimately bears responsibility for security. It is tempting for the organization to assign responsibility for IT protections to those in the information security department, but this would be a mistake. Most information security departments do not own the data or operational functions that make the business run. They are in charge of creating and implementing programs for protection, but they rarely have the ability to determine the amount of money allotted for tools and personnel. The data owners are ultimately responsible for its protection: they determine the value of the data and related IT assets, the risk appetite, and the amount of funds available to protect it. Information security departments cannot be effective without strong support from the business owners to prioritize security programs and fund them in line with their goals. If a data owner does not take responsibility for the data protection, then the organization will suffer an inability to appropriately prioritize information security.

The data owner makes decisions based upon the risk as they perceive it. Therefore, it is extremely important for the information security department to express risk to information systems, people, data, and networks in an understandable way. The data owner can then appropriately react, taking responsibility for decisions on behalf of data subjects. In some circumstances, responsibility for data security belongs at the highest level of the organization. Decisions for protection must, therefore, be based upon organizational policies endorsed and defended from the very top of the organization.

Standards and regulations

Almost every industry has specific standards that apply to cyber security. Standards and regulations for personally identifiable health data and financial data tend to be the strongest, with the highest penalties for breaches. Outside of health and finance, regulation is often lacking. For this reason, standards, which can be optional, are often enforced by contract. Common security standards relate to the protection of personal private data, protection of networks, protection of data received by the client or vendor with whom the contract is shared, or to the individual who provides their personal information. These contractual agrements often focus on common **national and international standards** for cyber security and information protection systems. These standards are often used by private industry, providing a commonly understood and publicly available benchmark. Including international or national standards in contracts is good practice, as providing a private detailed information security requirement risks a missing requirement that the common standard would cover.

1.4 Legal Regulations

National and international standards
In the context of cyber security, these standards are mostly released by organizations such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE). Although in general such standards are not legally binding, adhering to them is usually considered best practice.

Critical infrastructure
Infrastructure, organizations and facilities that are considered essential for society and whose failure would cause sustained shortages or significant disruptions to safety and security. Examples are the provision of food, electricity or public transport.

While conforming to national and international standards on cyber security and on privacy is recommended rather than legally required, nations around the globe are also passing and enforcing laws on IT privacy and security, and conforming to them is usually required. Since the purpose of such laws usually is the protection of the general public, legislation on privacy generally is considered more important, while a lack of security mainly affects the organizations themselves, and so the law makers tend to leave it up to the organizations to decide on the level of security they want. However, there is an increasing risk for society caused by inadequate cyber security, in particular regarding

Critical infrastructuresand governments are more and more passing laws requiring organizations to set up adequate cyber security as well.

There is no single international law that can be used to solidify an approach to privacy and cyber security across the globe. Privacy regulations range from those that protect the rights of the citizen, such as the EU’s General Data Protection Regulation, to laws that favor providing information on citizens' activities to the nation’s government, such as the former United States Patriot Act (European Data Protection Board, 2018; The USA Patriot Act, 2001).

Data laws generally apply to the geographic location in which the data originate, are processed, or are stored. This allows the government(s) of each location to apply their laws and enforce them in their own courts. A small number of laws also apply outside of the country that created them, even though this is difficult to enforce. Regarding privacy, the main reason to do so is that governments want to ensure that even if personal data of their citizens are transferred to another country, these data are still adequately protected. Otherwise, a company might transfer the personal data abroad to some country with very weak privacy legislation, and thus till, a government may decide that a law has reciprocity, that is, another government’s law will be enforced. In the United States, for example, the federal Department of Commerce (USDOC) regulates and enforces privacy agreements with the EU and Switzerland based on a set of principles which will be discussed in more detail below in the context of cross-border data flow.

More often, a national IT-related law will carry restrictions for the companies within the government’s jurisdiction. The EU’s General Data Protection Regulation (GDPR) supports the privacy of EU citizens’ sensitive data, regardless of where the data are stored or processed. Since the EU does not have legal jurisdiction over all global organizations, this is difficult to directly enforce. However, in Article 27 GDPR, it is stipulated that, in such cases, organizations have a representative within the EU that can be held accountable for any breach of the GDPR requirements (European Data Protection Board, 2018).

SUMMARY

IT security requires that an organization understands the value of its assets, the attacks to which it is vulnerable, and who has an interest in harming the organization. Risk management, i.e., the ability to measure and treat risk, is not one-size-fits-all. Instead, a risk management program must be tailored to the organization's ability to accept loss and its legal responsibilities.

Potential attacks on an organization may be physical or virtual. Both have the potential to allow theft of private information and intellectual property as well as intrusion to servers and networks. Threats to IT include natural disasters and physical hazards, but the most damage is performed by humans with specific (usually financial) interests in mind. Cyber security and privacy law is usually geographically dependent. For a law to apply to more than one country, the implementing government must have a method of enforcing penalties for non-compliance.

UNIT 2

DATA PROTECTION

STUDY GOALS

On completion of this unit, you will have learned …

- the meaning of data protection and privacy.
- the theory of data economies and importance of consent.
- the importance of law to protect data privacy.
- which data protection key concepts relate to everyday life.

2. DATA PROTECTION

Introduction

A user of social media notices that the advertisements on their feed are for products and companies that they clicked on within the past couple of months. When the social media company releases a new privacy policy, they see that the advertiser has changed their treatment of advertisements. Now, advertisers are allowed to rent access to historical user tracking data. This policy was changed without consent of the social media account holders. Is it legal for the social media company to sell its advertisers access to data on its users, including the other advertisers the user has visited, posts they read, and purchases they have made from within the social media mobile app?

A company receives applications for a job it has advertised. What should the company do with the application data of other applicants once one of the candidates has been selected and employed? Is it allowed to keep those data in case other suitable jobs may come up? Would it be acceptable to keep the addresses for sending out information about new products? Such questions pose a very real problem in our highly digital and increasingly globalized world, and impact our professional as well as our private lives.

2.1 Data Protection as a Personal Right

In order to establish protection and security, humans create communities. While communities are used foremost to satisfy innate social needs, they also create standards and laws that protect the individual. The security of the individual can be divided into the following three main spheres for which they expect both freedom and privacy:

1. The intimate sphere. This area of life includes personal opinions, health, sexuality, finances, and educational records such as grades.
2. The personal sphere. This area of life includes relationship information and personally identifiable information, such as physical and email addresses.
3. The social sphere. This area of life includes public personal and professional activities such as employer, degrees and colleges attended, and professional certifications.

In this context, the two terms “privacy” and “data protection” are often used almost synonymously, though not in all cases. In Europe, the term data protection is more common (e.g., the UK has a “Data Protection Bill”), while in the U.S., the term privacy is more commonly used. Additionally, privacy mainly focuses on keeping personal data confidential, while data protection additionally addresses user rights. Both terms are mainly used in the narrow sense of referring to personal data only, but in the wider sense, can also refer to data in general. Generally speaking, privacy and data protection apply to natural persons, i.e., humans, as opposed to legal persons defined under law, such as corporations. However, there are exceptions and data protection law in some countries, e.g., Switzerland, to some extent also addresses data about persons defined under law.

Privacy Law in the United States

As an initial example, we will have a look at privacy law in the United States. Later in this unit, we will also discuss the General Data Protection Regulation which applies in the European Union (i.e. large parts of Western and Central Europe). In the United States, personal privacy law is anchored in the Bill of Rights (the first ten amendments to the United States Constitution), several of which restrict the United States government from interfering in the private lives of its citizens (U.S. Const. amend. I-X). These freedoms were brought into wider scrutiny by the 1890 Harvard Law Review article “The Right to Privacy” by Samuel Warren and Louis Brandeis (1890), wherein the authors argue the innate right to privacy of humankind. In this article, Warren and Brandeis focused on the interrelationship of public interest, personal interests, and private information. They argued for legal protections from candid photographs or the spread of sensitive personal information for entertainment value (as opposed to the interests of the public) (Warren & Brandeis, 1890).

Until the mid-twentieth century, decisions about privacy for communications and of personal data were generally resolved based on either the Bill of Rights or court precedent influenced by Warren and Brandeis. With the advent of new electronic surveillance methods, computerized surveillance, and an interest in the personal privacy of women, laws about rights to individual and household privacy began to strongly emerge. Personal information privacy, i.e., freedom from the collection of information and from use without consent of the subject, grew parallel to the use of the computers. Each governmental entity of the United States can publish laws that regulate the use of sensitive personal information; many states, territories, and indigenous tribes have chosen to do so.

As the U.S. is a republic of many different jurisdictions, it is important to understand how different data protection and privacy laws can co-exist. Laws from different governments may contradict each other, even if they share a common geography (for instance, in the case of U.S. federal law and U.S. state laws). In these cases, where it is impossible to obey both the federal and more localized laws, the federal law usually preempts the state or local law. That preemption is determined by the law’s relationship to the U.S. Constitution and based on the express or implied intent of the lawmakers (U.S. Const. art. VI, §2).

More often, laws do not directly contradict one another, but rather misalign. For example, the state of California grants more privacy-related rights to its workers than federal law requires. An organization that satisfies federal employment law may still find itself in legal difficulty unless they accommodate the additional privacy protections in California. When two sets of laws do not agree, it is best to enforce the more restrictive applicable law until or unless the conflict is resolved.

Bill of Rights: U.S. Constitutional Protections for Privacy

The foundation of U.S. privacy law is in the U.S. Constitution’s Bill of Rights. The third through the fifth amendments in the U.S. Bill of Rights address the concepts of stationing soldiers in a home without consent; search and seizure of assets, properties, and persons; and the protection from self-incrimination (U.S. Const. amend. I-X). These rights have necessarily been expanded to include technologies as they arise. From the implementation of the American postal service to the rise of texting and email, the right to privacy in communications has been tested in the law with each new method of transporting words, pictures, and sentiments.

Within the United States court system, it is generally accepted that the fourth amendment to the U.S. Constitution includes communications privacy (Desai, 2007). This interpretation of privacy originates from the notion that U.S. citizens should be “secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” conducted by their government (U.S. Const. art. VI, §2). Note that the fourth amendment, like the entire Bill of Rights, describes citizens' rights rather than human rights. This implies that, according to U.S. law, these rights apply only to U.S. citizens. The prohibition of governmental interception and examination of communications was first applied to the postal system, wherein U.S. governments do not have the right to view someone’s mail prior to its delivery or without a warrant or subpoena.

In 1967 to 1968, the U.S. Supreme Court expanded the fourth amendment protections against governmental mail and telegraph interception to include wiretapping, which is covertly listening to telephone calls (Katz v. United States, 1967). Protections were expanded further in 1986, when U.S. Congress revised the wiretapping laws to include general “electronic communications,” such as email. This new right of privacy included freedom from government observations without cause, but also included freedom from observation by service providers and advertisers. Limitations of these rights allow for warrant-enabled observation by law enforcement agencies, as well as for providers of communications services to review communications if it is necessary in order to perform their service (18 U.S. Code § 2511, 1986).

In comparison, laws on data protection outside of the United States tend more heavily toward the protection of the person or organization rather than the convenience of business. Within the US, personal privacy is rarely treated in isolation from general data privacy. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA) apply only to a subset of personal data, and only to its handling by specified entities. In Europe, the protections for individual privacy are more stringent than in the US, and they have a wider scope.

2.2 Basic Principles of Data Protection

Data protection is required as well as enforced in different countries in very different ways. Strong privacy protections are required for compliance with EU standards; other countries often have defined much weaker privacy requirements. In locations with weak privacy requirements, or in areas where they are not enforced, the individual’s information may be exchanged for financial or economic gain. This exchange is outside of the control of the individual, or consent may have been automatically given through the fine print of a user agreement. In order to promote a common understanding of the principles of data protection to be used in relevant legislation, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have jointly defined a set of such principles in ISO/IEC 29100.

International Standard ISO/IEC 29100

The international organizations ISO and IEC have jointly published a publicly available standard called “Information Technology—Security techniques—Privacy framework”, known as ISO/IEC 29100 (ISO, 2024). The year given at the end denotes the year of publication of this version of the standard. When referring to the standard in general rather than this specific version, we will leave out the year. This standard provides a high-level framework for the management of personally identifiable information in automated processing systems. It is important to understand that this standard is just that - a standard, but not a law, and therefore not legally binding. As with many other ISO documents, its purpose it to provide a single central understanding of concepts, terminologies, and structure for a single subject (ISO, 2024).

Data Protection Roles and Terminology

In the following table, a short summary of the main terminology used in ISO/IEC 29100 and in GDPR is given. The data covered by privacy are called “personally identifying information” (PII) in ISO/IEC 29100, while GDPR refers to them as “personal data.” In privacy or data protection, three groups of participants are distinguished. Each of these participants plays a role in the justification of data collection and processing, as well as the responsibility for data protection:

1. Affected persons. These are the natural persons whose data are processed.
2. Controller. This is the person or other entity that decides on the methods and technology for processing data and is therefore responsible for it. This data controller may carry out the processing themself or have it carried out by others, for example a data processor.
3. Processor. This is the person or other unit that carries out the processing on behalf of the responsible person. They must carry out this processing in accordance with the instructions of the controller and based on a written contract. Outside of the contractual obligations, the data processor does not normally bear responsibility for the lawfulness of the processing. However, the processor is responsible for ensuring security within his work environment, and for implementing all protective measures as agreed with the controller. Furthermore, he is not allowed to process the data for any purposes of his own but only for the purposes set by the controller. It is important to note that a processor does not always exist since the controller may process the data themself rather than contracting a separate processor to do so.

Table 1: Comparison of Terminology between GDPR and ISO/IEC 29100

GDPR	ISO/IEC 29100
Data protection	Privacy
Personal data	Personally identifying information (PII)
Special categories of personal data	Sensitive PII
Data subject	PII principal

GDPR	ISO/IEC 29100
Controller	PII controller
Processor	PII processor

Source: Kneuper (2021).

Data Protection Principles in ISO/IEC 29100

ISO/IEC 29100 includes a breakdown of the principles necessary for an organized and comprehensive privacy program. As a supplement to general data protection laws, or in countries where few data protection laws exist, the ISO/IEC 29100 principles are a solid foundation for organizations to build upon. The eleven principles enumerated within the document are (ISO, 2024):

1. Consent and choice. A person should be able to choose whether to allow processing of their personal information except where law allows doing so without consent. This consent must be made without duress and with a clear understanding of the conditions for the processing.
2. Purpose legitimacy and specification. Data processing should, at a minimum, be legally permissible. The anticipated use of the data must be understood by the PII principal prior to its collection.
3. Collection limitation. Only truly necessary personally identifiable information should be collected. This necessity is based on the documented purpose of the data, established prior to the collection.
4. Data minimization. Data should be made accessible only to those with an established need to know them. Personally identifiable information (PII) should not be processed if the required outcomes can be reached without its use.
5. Use, retention, and disclosure of information. After data are collected, their use and retention must be consistent with the purposes disclosed to the PII principal. If data must be retained past their intended use, as is sometimes the case for legal obligations, they must be protected properly until they can be destroyed.
6. Accuracy and quality. Personally identifiable information must be accurate and updated unless there is a justification for doing otherwise. The PII principal has the right to verify and update the data, especially in cases where the inaccuracy or irrelevance of data is harmful to their interests.
7. Openness, transparency, and notice. The PII principal has the right to clear and accessible information about processing of their data, how to request correction of the data or limit their use, and who will have access to the data.
8. Individual participation and access. PII principals can access and review their personal information, and can have it amended, corrected, or removed where both possible and appropriate.
9. Accountability. The processor of personally identifiable information must adopt privacy-related policies and practices. A privacy officer, or other specified individual, will take responsibility for the handling of personal data. This accountability is expanded to ensure that any third party to whom the data flow is also bound to the same level of diligence. Breaches of privacy are to be disclosed and redress may be required.

10. Information security. Appropriate technical, physical, and organizational controls must be implemented to properly protect the private data. Those controls are required whether data are processed and stored within the original collecting organization or another entity altogether. Data usage and access are always limited to those with both need-to-know and appropriately granted permissions.
11. Privacy compliance. Privacy must be ensured by adherence to a privacy program that meets security standards and privacy laws. The program must be periodically audited to ensure its effectiveness, and risk assessments are used to evaluate compliance with the program.

The above summary intends only to familiarize the reader with an overall structure. It does not replace a thorough understanding of the defined materials for building a privacy program foundation. Many more specific items are found in the standard, allowing for a comprehensive and tailored implementation of protections.

GDPR is based on very similar principles, although there are some differences in detail. Where these protection principles are in place, there is a high likelihood that personal information is handled ethically and with conscientious security. These principles do not unnecessarily limit the collection or use of personal data. However, they do limit the transactions that can be performed without the consent of the persons to whom data applies. Companies with large stores of personal data may provide it to their business partners, but only on terms that have been allowed by that data subject. In the following, we look at some concepts of data protection and privacy in more detail.

Protection

Any action or item that explicitly serves to increase security is called protection. Protective measures may be preventative, detective, or corrective, and the difference can be thought of as separated on a timeline. Preventative protections are future-oriented and stop activities that would reduce security. Detective protections are both past and present-oriented, meaning they determine whether an action is taking place that would reduce security if the state is already insecure. An important aspect of detection is the quick identification of attacks when they take place, in order to react and ward them off. Corrective actions are after-the-fact; they are actions that change an insecure state to a secure state. Corrective actions are taken when needed, not only when the state has recently become insecure. Corrective actions can also be inspired by the discovery of new risks in an otherwise unchanged circumstance.

Data Economy

Large amounts of data are necessary for some organizational activities, not all of them commercial. Activities that need large datasets vary, from public health initiatives, to training artificial intelligence, to determining advertising algorithms to identify and target the most likely consumers for a service or product. These datasets exist in organizations that gather the data deliberately (such as research focus groups and hospitals), but they are also gathered for other purposes—most famously, social media.

Data economy
This term describes the sale, rental, and leasing of person-related data from the original collector to a third party.

A **data economy** is a network of providers and clients who exchange large data collections in exchange for a fee. Transactions within data economies range from helpful to morally neutral, depending upon the outcomes of the data. For instance, Google retains a great deal of individual and household data based upon internet searches using their tool (Haselton, 2017). Some of these households do not have individual Google logins through which a single user can be identified, though most do. If Google takes part in a data economy by selling this collected data or by using it themselves, is that a moral action? It depends upon the outcome. Most would look favorably upon Google using a geographical aggregate of influenza-related searches to detect spreading illness and publish health warnings. Many would view Google selling this aggregate, anonymized information to a pharmacy as neither helpful nor harmful to the consumer. By contrast, what if Google sells identified consumer data to an advertiser who will bombard the household with advertisements for cold and flu medications? This is not desirable behavior and is helpful only to Google and to the advertiser.

In the above scenario, the advertiser's attempt to influence the customer is not itself illegal. Depending on the geography, however, the sale of identified customer data might be. Article 6 of the General Data Protection Regulation (GDPR) states that the processing of personal data must be performed with the full and knowing consent of the data subject, since none of the other legal bases listed in the article are applicable in this scenario. Furthermore, article 5 (1) item b) states that the use of data must agree with the published purposes of its collection (European Parliament and Council of the European Union, 2016). The first and second use cases, where Google uses or sells aggregate data, do not specifically go against this legislation. The third case, where Google collects data for purposes of an internet search and sells it with identification of the user, conflicts with the consent requirement.

One of the mechanisms for gathering user consent electronically is the now-common cookie banner. Organizations publish their intention to collect data via small IT markers called "cookies" and ask users to agree or disagree with their usage on the site. These banners also usually have links to the websites' privacy and data usage policies. Users of the sites have the option to consent, disagree, or sometimes customize the cookies. The website owners then have explicit consent to their policies, which may then include selling or otherwise profiting from the users' behaviors while on the website.

Consent

The concept of consent is straightforward on the surface—the subject provides permission for an action or inaction. For instance, a consumer may grant consent for a commercial website to track their purchasing habits to make suggestions for other purchases from the same business. They may also opt-in to the businesses' newsletter, which uses their email address and allows the business to use it to send them updates on their offerings and sales throughout the year.

Where consent becomes unclear is in the specificity of the request and the response. If the user fills in their address, cell phone, and email and checks a box that says "I would like to hear from Business X," what have they consented to receive? Could they receive targeted advertisements? Political fundraisers and statements? Attempts to be recruited for employment? How will the business attempt to contact them? Will they consent to receive texts and phone calls? Worse, what if they simply check the box that says, “I consent to Business X using my personal information to provide exciting services”? This consent could allow the business to sell their information to another organization, under the pretext that they may be excited by their services, when really the point of the sale is to make money for the original business.

Because of these differences in gaining consent and informing the user, newer laws about consent and commercial advertising have been published. One of the most notable is GDPR, which defines, among other requirements, that consent must be specific for a certain purpose. Non-specific consent as described in the examples above would therefore not be considered valid according to article 4. It is worth noting that children (under 13 in the US, under 16 in the EU) are incapable of giving consent for their data to be used (European Parliament and Council of the European Union, 2016).

Explicit consent

With **explicit consent**, a personally identifiable information (PII) principal allows the collection or use of some of their personal data for a specific purpose. However, PII principals can only give their meaningful consent to the collection or use of PII if they are able to assess their consequences with sufficient clarity. For explicit consent to be given, GDPR explicitly requires that it must be a “freely given, specific, informed and unambiguous indication of the data subject’s wishes” (European Parliament and Council of the European Union, 2016, art. 4, point 11). When requesting consent, it is important to inform the data subject about the purpose of the collection or use of the data as well as the right and the consequences of providing or refusing consent. Since the consent must be freely given, the PII principal must be able to refuse consent without any serious negative consequences. The external appearance of the consent is to be emphasized. The following is an example of a declaration of consent:

Explicit consent
This is written or electronic permission to collect or use personal data for a clearly expressed purpose.

> I agree to receive information about your new products and services. I can revoke this consent at any time in writing by letter or by e-mail to <email-address-which-will-be-processed> with effect for the future. Please use the following contact data for sending the information: [e-mail address or postal address]

Consent under the GDPR does not have to be given in writing, although this is often recommended for posterity. It is also possible, for example, to give your consent electronically via web form, e-mail, or fax. However, it must be ensured that the electronic consent is given clearly and consciously. Typically, web forms must have a box with a check mark, which the customer must tick, and only then is their consent granted (known as an “opt-in procedure”). Electronic declarations of consent must also be logged by the system. This means that it must be possible at any time to view the consent text and to revoke the declaration of consent.

There are two different forms to provide consent in an electronic format. The first is “opt-in consent,” which describes the concept that, by default, consent is refused and the user has to perform some explicit activity to provide consent, typically check a check box. Alternatively, with “opt-out,” the default is that consent is provided, but the user may perform some activity to withdraw consent, such as removing a tick from a check box. As stated above, GDPR requires an “unambiguous indication” of consent, which implies that only opt-in is acceptable as valid consent.

2.3 The General Data Protection Regulation

In 2016, the European Union adopted the General Data Protection Regulation (GDPR). GDPR is meant to ensure that all European Union citizens are afforded a minimum privacy standard in the handling and movement of their private personal data. This regulation took effect in May of 2018 (European Parliament and Council of the European Union, 2016).

Scope of Application

The General Data Protection Regulation differs from other privacy laws in that it applies based on the location of the data subjects, not upon the location or origin of the data. This law applies to the data on humans rather than non-human legal entities with corporate citizenship. An exception is made in the case that the private data of the business are also the private data of human persons, such as with a partnership.

Personally identifiable information (PII)
Referred to as private data, this can be traced back to a single person, and provide enough knowledge to distinguish that person.

Personal data that are covered by GDPR include both sensitive and non-sensitive **personally identifiable information (PII)**. In the United States, bank data and personal sensitive data about medical conditions would be considered private data. In the European Union, further information that could serve to identify an individual, such as full name, address, and telephone number, are also covered by this privacy-related regulation. Similarly to the U.S., data fall out of scope when they are fully anonymized and can no longer be related to an individual person. Name alone is not relevant in this context, although it gains relevance in combination with additional information about the named person. The concept of personal data includes data that have been stored or processed under a pseudonym. Unless data are aggregated or fully anonymized, they count as personal data and the relevant data protection requirements apply.

In general, data processing security requirements covered under GDPR focus on the use of information technology. Unlike people who may process individual pieces of information, technology has the capacity to correlate and evaluate aggregate stored data from a non-identified to an identified state. There are two important exceptions where the GDPR also applies to information processed manually. Firstly, purposeful data collections with similar structure, and with standard characteristics, are subject to data protection law even when they are not automated (e.g., patient file cards in a doctor's practice). Secondly, employees’ personal information may only be collected and used if necessary for the establishment, implementation, or termination of an employment relationship. This applies irrespective of the use of information technology, so that, if necessary, paper files on employees must also be kept in conformity with data protection regulations.

Some personal information is considered particularly sensitive and may therefore only be collected or used under specific conditions. According to the GDPR, this applies to data that reveal information regarding “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,” as well as “the processing of genetic data, biometric data ... data concerning health or data concerning a natural person’s sex life or sexual orientation” (European Parliament and Council of the European Union, 2016, Art. 9 No. 1).

Prohibition Subject to Permission

In GDPR, as well as many other cases, data protection law is based on the prohibition principle with reservation of permission. This principle states that the collection or use of personal data is prohibited in principle. Exceptions to this principle require a relevant legal basis which may be an explicit legal provision or the (effective) consent of the person concerned.

Legal Basis for Processing Personal Data According to GDPR

To permit processing of personal data, GDPR defines the following conditions in article 6. Processing is only allowed if at least one of the following conditions is satisfied:

a) The PII principal has given their consent to the processing of personal data concerning them for one or more specified purposes;
b) the processing is necessary for the performance of a contract to which the PII principal is party or to implement pre-contractual measures taken at the request of the PII principal;
c) the processing is necessary for compliance with a legal obligation to which the controller is subject;
d) the processing is necessary to protect the vital interests of the PII principal or of another natural person
e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary to protect the legitimate interests of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the PII principal which require the protection of personal data, in particular where the PII principal is a child.

In practice, the most important legal bases are consent (condition a), fulfillment of the contract (condition b), and legitimate interest (condition f). A typical example for condition b is delivery addresses, because without them the delivery and thus the fulfilment of a sales contract could not take place. However, this applies expressly only to the processing that is necessary for the execution of the contract. If the same data are to be used later for the sending of advertising, then condition b is no longer sufficient as a legal basis and separate consent is required for this. Please note that condition f requires a balancing of interests between the legitimate interests of the person responsible and the interests of the PII principal.

Consequently, the legality of our example related to the tracking of social media users will depend upon the adoption of GDPR principles by the government of the relevant jurisdiction. In places where GDPR is applied, it is not allowed to single-handedly change the use of personally identifiable information for the profit of the business. In places that do not have GDPR or similar regulations, the social media company is not prevented from selling access to its commercial partners without the explicit consent of the user.

In the case of the example of storing job applications that were not successful, condition b allows the employer to store and process the data as long as the application process is underway. After that, for a limited time of a few months the company may still keep the data in case of any complaints about the application process, e.g., alleged discrimination against a candidate, based on legitimate interest (condition f). If the company wants to keep the application data beyond that time frame, for example because new jobs may come up that might be relevant for the applicant, the company will have to ask the applicant for their consent (condition a). If the company additionally wants to use the data for marketing purposes, this will also only be allowed with consent (Kneuper, 2021).

Rights of the PII Principals

GDPR defines a number of rights of the PII principals, for example the right to access the data an organization maintains about them. Any data subject can request to have all their information provided. They have the right to request that inaccurate information be updated or corrected. Additionally, individuals have the right to ask for their records to be permanently removed. Any actions taken automatically based on personal data, such as credit decisions or rental agreements, must protect the person's rights and freedoms. This generally means that there should be a simple method for human review or intervention in automated data processes.

2.4 Further International Regulations on Data Protection

This section serves to introduce the main discrepencies between the application and relevancy of the EU General Data Protection Regulation (GDPR) inside and outside of the EU.

National Data Protection Laws within the EU

Even before the GDPR was released, all EU countries did have national laws on data protection. Although most of the contents of these laws were moved to or replaced by the GDPR, the laws were not replaced and withdrawn completely. Instead, there are a couple of issues that are still regulated on a national level, such as the structure of the national regulatory body for data protection.

The Federal Data Protection Act of Germany

One example of national data protection legislation in the EU is the Federal Data Protection Act of Germany. This Act, called *Bundesdatenschutzgesetz* (BDSG), outlines responsibilities of the German government and private entities with access to personal private data (Federal Ministry of the Interior, 2017). BDSG predates General Data Protection Regulation of the European Union. A new version of BDSG was implemented in parallel with GDPR, no longer an independent law in terms of content, but containing concretizations and additions to the GDPR (Federal Ministry of the Interior, 2017). Additional supplemental laws are in place in Germany to fully cover handling of personal sensitive data, for instance, the Telecommunications Act (TKG), Telemedia Act (TMG) or the Social Security Code (SGB). As privacy concerns grow more complex and technology continues to evolve, we can expect that legislation, both local and international, will continue to evolve.

The Role of GDPR Outside the EU

As mentioned before, GDPR is special in that it aims for an international scope. It applies to the personal data of all EU residents, regardless of where that data is held. GDPR applies to all organizations who offer goods or services to EU persons (European Parliament and Council of the European Union, 2016). GDPR requires that impacted organizations protect the privacy of EU citizens. Organizations must have a reason to collect and process personal data and they must publish information about these activities in their privacy policies; there is no exemption for ignorance.

As a foundation for ensuring privacy, the data must be catalogued, and the location and security must be known to the organization’s officers. The regulation requires that these organization establish security and privacy policies for handling personal data. This allows for the anonymization and aggregation of data to lower the risk of misuse, and requires confidentiality measures such as encryption. Furthermore, in certain cases, GDPR requires the establishment of a data protection officer, an internal role responsible for GDPR compliance across the organization.

2.5 Cross-Border Data Flow

As laws for data protection vary between governments, laws restricting when and how data can move between countries are important. Cross-border data flow or transfer, i.e., the movement of data from one country to another, may be necessary for companies with a global scope or with international partners. In itself, cross-border data flow is neither illegal nor inherently insecure. For example, the GDPR defines such restrictions regarding the movement of personal data out of the EU as previously described.

Data Protection for Centralized Services and Cloud Services

In a global organization, data centers routinely use shared backend computer services and have interoperable networks. Enterprise services may only be offered from a single location, such as centralized data backups or the use of expensive ERP software. This implies that data (personal or other) will have to be transferred across borders to the data center where they are to be processed.

Technology providers are continuously finding ways to offer services in a more efficient, centralized manner. An outgrowth of this trend is the move toward cloud computing. Cloud computing is the abstraction of computer resources so that they can be sold in a metered, public fashion. Cloud services are usually consumed over the internet rather than through a private network. Providers of cloud services usually have high levels of redundancy in their infrastructure, which increases the reliability of customer services. However, this redundancy may entail data storage and processing in multiple geographic areas.

Cloud technology has several advantages, such as service reliability, rapid delivery of new offerings, scalability, and broad access. Organizations in highly regulated industries may still choose to use cloud services, but the responsible data owners and IT personnel must fully examine the cloud provider's policies on cross-border data flow. It may be possible for the organization to restrict geographies for their data storage and processing, though this sometimes means that not all cloud services will be available to them. Fortunately for many customers, cloud service providers have realized that data movement may need restriction in response to law or policy. Global providers are making it easier for their customers to enforce the geographic boundaries of their data by building in simple implementations of data flow control within their customer-managed configurations. In regions with strict data movement regulations, smaller cloud providers have developed a successful business in offering in-country-only cloud environments. These environments are suitable for their customers who wish for the advantages of cloud-based computing but cannot risk the possibility that the data would be accidentally or maliciously moved into another country.

Data Transfer from the EU to other countries

In order to ensure that data transferred from the EU to other ("third") countries will still be protected adequately and data protection regulation is not circumvented by moving the data outside the EU, the GDPR defines a set of rules when such a transfer is allowed. First of all, any such data transfer is a form of processing the data, and the general regulations about processing the data apply, independent of whether they are transferred within the same country or outside the EU. This is sufficient if the data are transmitted to institutions in other member states within the European Union, and to institutions in signatory states to the Agreement on the European Economic Area (Norway, Liechtenstein, Iceland). In all other cases, however, PII may not be transferred to foreign institutions without additional caveats that are required to ensure an adequate level of data protection can be assumed at a receiving institution abroad. This applies to both separate organizations and to member companies within an international conglomerate group.

From the point of view of the data controller, the easiest case is an adequacy decision: for certain countries, the EU commission has decided that the level of data protection is comparable to that required within the EU and therefore adequate. Such adequacy decisions exist, for example, for Argentina, Japan, New Zealand and Switzerland, and personal data can be transferred to these countries under the same conditions as they can be transferred within any EU member state.

If no adequacy decision exists for the target country, several safeguards are defined by GDPR which can be used to ensure that the data are treated adequately. For example, there may be a contract between both parties including “standard data protection clauses“ as defined by the EU commission, which essentially list the relevant GDPR data protection requirements as a set of contractual rules. Similarly, “binding corporate rules“ can be used to ensure that these requirements are met when data are transferred within an international corporation. In both cases, additional measures may be necessary to address specific situations in the target country that are not covered by the standard clauses and rules.

The GDPR also defines several other possible legal basis for data transfer abroad which however have little practical relevance.

Data Transfer from the EU to the United States

Since many IT service providers, such as cloud service providers or social networks, are based in the U.S., it is particularly important for their EU customers to allow easily transfer personal data to the U.S. On the other hand, the U.S. have a different philosophy regarding data protection compared to the EU, for example putting a much higher value on freedom of speech and on national security. From an EU point of view, it is therefore doubtful whether personal data are adequately protected in the U.S., and under what conditions a transfer of personal data from the EU to the U.S. is acceptable. This has led to a lengthy back and forth of relevant regulations for such data transfer.

The easiest way to allow the transfer of personal data out of the EU is based on an adequacy decision by the EU commission. To make such an adequacy decision possible for transferring data to the U.S., the EU and the U.S. originally set up the Safe Harbor agreement. Under this agreement, U.S. organizations were able to register, confirming that they would conform to a set of minimum data protection requirements going beyond the U.S. legal requirements. The EU and the U.S. agreed that transferred data would be adequately protected when these additional requirements are met, and the EU commission set up an adequacy decision for U.S. organizations that were registered under the Safe Harbor scheme. However, in 2015 the European Court of Justice (ECJ) decided that these defined additional requirements are not sufficient and revoked the adequacy decision. (This is usually called the “Schrems I“ decision after Max Schrems, an Austrian lawyer who initiated these legal proceedings.) Several years later, a new agreement called EU-U.S. Privacy Shield was set up, defining stricter requirements, but in 2020 the resulting adequacy decision was again revoked by the ECJ (“Schrems II“). The main reasons for these decisions were that U.S. intelligence services were considered to have inadequate rights of access to the personal data of non-U.S. citizens based on the CLOUD act and similar legislation. Furthermore - as previously mentioned - the privacy rights defined in the Bill of Rights only apply to U.S. citizens, and there are no similiar rights for EU citizens in the U.S.

A third agreement, committing to a “Trans-Atlantic Data Privacy Framework“, was set up in 2022, leading to an executive order by President Biden that restricts the powers of U.S. intelligence services and eventually a new adequacy decision by the EU commission in July 2023. This is currently valid but again expected to be challenged in court.

Although the discussion so far only referred to the EU and its member states, the same holds true for the members of the European Economic Area EEA (Liechtenstein, Norway and Iceland), and to Switzerland and the UK which have similar agreements with the U.S.

2.6 Data Protection in Everyday Life

Laws about data handling are in place to ensure conscientious collection, handling, and destruction specifically by organizations, as it would make no sense to regulate what an individual can do with their own data. However, it should not be taken to mean that privacy protection is always in the hands of a third party. People regularly make decisions about the handling of their private data, and these decisions are key to its protection.

The protection of physical data is familiar enough to influence our general habits. Workers routinely lock offices and desk drawers. Small paper and plastic shredders are used at home to ensure expired bank cards, financial statements, and personal medical records are destroyed. The protection of logical data, of which the user has less visibility, is less intuitive, and therefore less likely to be implemented regularly. The following actions significantly lower the risk of data unintentionally falling into the hands of criminal third parties:

- Provide only the necessary personal data, especially online.
- Shred documents and papers with personal data and financial information.
- Never disclose governmental identification numbers (e.g., Social Security number, driver’s license numbers, and passport number) unless it is legally required.
- Never use governmental identification numbers as a password.
- Keep all personal documents (e.g., passport and birth certificate) in a locked area, preferably in a safe. Similarly, keep electronic copies of such documents safe, for example, by storing them in an encrypted folder.
- Provide little personal information on social media. Review privacy settings and security mechanisms for changes.
- Never disclose account names and passwords when contacted by email or telephone. If you receive a request, contact the service provider yourself through published customer service channels or links to ensure that the request for disclosure is legitimate.
- Always use complex passwords, and do not use names or numbers associated with family, sports, or addresses. Never write down or share passwords. Software for password management may help.

- Make sure that your mobile phone and computer software is always up to date. Enable automatic software updates if available.
- Encrypt your confidential data in storage and in transmission.
- Do not use public Wi-Fi spots without encrypted communication mechanisms, such as a virtual private network (VPN) or using hypertext transfer protocol secure (HTTPS).
- When downloading or using apps, grant required access to personal data only for functions you need.
- Pay close attention to balances on credit and debit cards. Check them regularly, preferably daily.
- Contact issuers immediately if you cannot locate a credit or debit card. They can either temporarily disable or replace the card.
- Obtain your credit score from each of the major credit bureaus annually. This is free of charge in most countries.

SUMMARY

Data protection as a personal right is highly dependent upon the definition of person and of privacy. These are both defined by governments that make and enforce the applicable regulations, and they vary between countries. Security, safety, and the protection from risk are driven by human needs. Laws are established to protect people from intrusions from each other and from their governments.

The EU General Data Protection Regulation (GDPR) is a comprehensive prohibition against the misuse of private data. It applies to all EU citizens, regardless of the location in which their data are stored or processed. Privacy Shield was an EU and Swiss agreement with other countries on a minimum standard for handling of sensitive data, which was revoked by the European Court of Justice in 2020 (Court of Justice of the European Union, 2020).

Cloud computing and global networks have made it simple for data to cross borders through negligence or malicious activity. The owners of data must ensure that they understand how data can be moved between geography, and that all legal and moral requirements for data protection are met.

UNIT 3

BASIC FUNCTIONS OF CYBER SECURITY AND THEIR IMPLEMENTATION

STUDY GOALS

On completion of this unit, you will have learned …

- the meanings of identity, authentication, and authorization.
- the theory of rights management in data protection.
- the importance of evidence preservation and why it matters.
- which rights management key concepts relate to data protection.

3. BASIC FUNCTIONS OF CYBER SECURITY AND THEIR IMPLEMENTATION

Introduction

Those who plan and implement levels of confidentiality, integrity, and availability for an information technology (IT) network are confronted with complex questions: What is considered secure? How can security be implemented and enforced in a repeatable manner? Fortunately for them, solutions for security implementation have been established.

This unit begins with concepts of identification, authorization, and rights management. We then move on to concepts of data protection which depend upon user permissions and object permissions to apply their protection, and will discuss models of access protections and the benefits and difficulties inherent in their usage. After establishing the basis of data access, you should understand the concepts of evidence and data reprocessing. These useful topics explore how data are collected and used in a manner that builds confidence in their authenticity, as well as how their usage may continue to provide utility when they are securely collected and stored. Finally, we look at the security aspects of functionality for the organization's IT services. Most availability concerns fall into the realm of IT operations; nonetheless, we discuss the important considerations for service availability that are impacted in a failure of security.

3.1 Identification and Authentication

Access control
These are mechanisms to ensure that data and functionality are available only to intended recipients.

To ensure the confidentiality of data and functions on an IT device, **access control** is required. Access control mechanisms allow only authorized persons to gain access to the data and functions of the IT device. Access control has three aspects: identification, authentication, and authorization. Identification is the ability of the user to assert that they have a representation on the information system, such as a username or an email address. Authentication is proof that supports the user identity asserted belongs to the person attempting to access the device. Authorization is the set of permissions that the identity is assigned on the information system, so that there is a record of activities they are allowed to perform, and objects that the activities can impact.

Identification

Identification is the very first step of gaining access to a resource. In information technology, it is the process of asserting an identity, which will likely be represented by an assigned username, a number, or an email address. Identification itself does not convey any privileges to the user. Instead, it begins the process of access so that other activities, such as proving the assignment of the identity and applying the rights assigned to the identity, can begin.

Identification is an easily explained concept, but the practice of assigning and managing identities in an organization can be difficult. For this reason, a common practice is to assign a role to a group of users with similar business functions, such as “Administrator” for those who run the IT systems or “Helpdesk” for those who answer user requests for assistance. While the management of these identities is less time-consuming than providing each user with an individual username and password, use of a single identity for multiple persons must be avoided. Note that assigning a group of users to one identity is different from assigning a group of user identities to a single group. This is illustrated by the following two different ways of assigning administrator permissions to a team of IT workers:

- single identity. An administrative user identity was created, called Admin. Every person on the IT helpdesk has the password for this login. This action causes many issues for information security functionality, such as lack of user accountability.
- group permissions. Each person on the IT helpdesk has a uniquely assigned user identity for access and creates a password that is not shared. All of these users are assigned to a group called Admin. The admin group has all necessary administrator permissions to perform the role, as if the person were assigned the original administrative user account.

Organizations with common identities are unable to easily determine which user with the admin account performed an action. In the case of negligent or malicious activity, the organization is unable to react adequately if the common identity was used. Moreover, group identities have shared authenticators (such as passwords). If a password is assigned to the identity, and someone who knows the password leaves the organization or transfers departments, it is possible that they will retain an active password for the group identity and could use it for their own gain.

By contrast, creating role-based groups and populating them with uniquely assigned user identities generates logging and activity histories that can be traced back to the single user account that performed the action. Because these identities are not shared, the authenticators remain private. Movement of a user in the group within the organization or to another company requires removing the user identity from their role-based groups, but doing so does not impact the identities or authenticators of the remaining team members.

Authentication

Authentication, the act of proving to the information system that the asserted identity is being used by the correct person, usually involves presenting some sort of secret knowledge to the information system. That secret can be something that the user knows, such as a password or personal identification number (PIN); something about the user, such as a fingerprint or a retina pattern; or something that the user has, such as a single-use number from a hardware token or a mobile phone known to belong to the identified user.

Access to sensitive data and functions, such as bank accounts or changing a password, may require more than one form of authentication, for example, logging in with an email then providing a PIN sent when requesting the sensitive function. This request for more than one form of verification is called multi-factor authentication. Multifactor authentication (MFA) is a good defense for any information system login that is easily exploited to take advantage of user resources. Multifactor is commonly used for internet-facing sensitive resources, such as allowing an organization's user to join their workstation to the corporate network when on a public internet connection.

Passwords

Most people can remember strings of alphanumeric characters as secrets for the purposes of authentication, provided they are not too complicated. Such strings are called passwords. Passwords are the most common way to authenticate identity, though they are also quite easily compromised. Unfortunately, most humans must either choose passwords with low complexity or write down the more complicated options. Several well-known methods of compromise rely upon password-only authentication.

Password-only authentication should be used for low-value information systems, accounts, and data. It should never be used for administrative logins that have significant rights on the system, nor should it be used for information systems that have sensitive data. In addition, strict rules must be enforced (if possible) when using only passwords. According to the current state of the art, these rules include the following (Grassi et al., 2017):

- Never use information related to yourself or a family member as a password or part of the password (e.g., first name, date of birth).
- Avoid terms that (could) come from a book.
- Combine different types of characters, i.e. upper/lower case letters, numbers and special characters (e.g., !@#%$*~;).
- Give the password a length of at least 8 (better 10 or 12) characters.
- Never use the same password for different applications. Otherwise, if an attack on the password used in one system is successful, the passwords used for other systems will become known as well. This is true even if the user selects a very strong password and stores it securely but the passwords are not securely stored on at the system used and stolen from there.

The number of possible passwords of length $n$is z^n, where $z$describes the number of different symbols allowed. This shows that an increase of the password length has far more impact on the number of possible passwords (and therefore the difficulty of a brute force search) than an increase of the number of different symbols used. An example: given a set of 62 symbols (small and capital letters, digits) and a password length of 8 symbols results in $62^8 \approx 2.18 * 10^{14}$ different possible passwords. Allowing an additional 10 special symbols increases the number to $72^8 \approx 7.22 * 10^{14}$ passwords, a little more than three times as many. If instead one increases the password length by only one symbol, the number of possible passwords increases to $62^9 \approx 1.35 * 10^{16}$ which shows that the effect is much larger. A precondition for a similar increase of security (in both cases) is of course that one uses a genuinely random sequence of symbols rather than a longer word from a dictionary.

In the past, it was also recommended to change passwords periodically. However, it is now widely accepted that this actually reduces security because humans cannot remember new passwords so often. The U.S. American standardization organization NIST therefore now recommends that users should not be required to change their passwords periodically, but only if there is evidence that the password has been compromised (Grassi et al., 2017).

From an organizational point of view, it is necessary that access data are not kept in writing. Professional attackers can easily find such hidden passwords. This applies whether the passwords are hidden in such classic locations as a sticky note under the keyboard or in a desk drawer, or if they are in the slightly more sophisticated location of an address books or telephone. This is a compelling reason why passwords alone are rarely sufficient for information protection. A useful alternative is to use a password safe, a small program that stores passwords in an encrypted form, so that the user only needs to remember one password to access the password safe, rather than a separate password for each service used.

Security tokens

Security tokens may take the form of hardware or software. A security token is considered a thing that a person has. Security tokens are often separate hardware devices that have an ever changing, multi-digit number generated by a pseudo-random algorithm. As a result, the number generated is known only to the server that tracks the hardware token and the token itself. A software token may also be an application on a mobile phone that, like a hardware token, generates a number with an algorithm that is secret between that application and the server that runs its software.

The security token often provides the second part of a secret, so the user will enter both something that they know or something that they are (a password or a biometric), and also enter the software token to complete the secret needed to gain access. Software tokens feature complex algorithms and require painstaking management, but they are very simple devices to use. They are often in a form factor that would fit on a keychain, so that they are easy to carry and to access. Some security tokens require another type of activity prior to generating a token, for example, they may have a keypad that requires the user to enter information prior to having a visible security code. In these cases, the code generated by the token is not visible until the user has performed authentication on the token itself. More commonly, security tokens have a visible number demonstrated on their faces, so the number itself can be observed by anyone looking from the right angle. This makes the security hardware token somewhat less secure unless the user is always very certain of its location. A lost security token is reason for alarm in that, as previously discussed, passwords are not reliable methods of having secret data. Therefore, if the user's password has been compromised, it is more problematic if the user has lost their security token. At the point that the user has lost their security token, it should be assumed that their network account is fully compromised. If their security token is misplaced but the user does not currently believe that the token itself is lost (for instance, the user has misplaced the token since its last use, but they live alone), it may be appropriate for the token to be temporarily suspended and either a different token assigned or an additional static token issued so that they can continue work. The additional static token, while convenient for the user, should have a limited lifespan. Otherwise, the user simply has a longer password.

Biometrics

For natural persons, biometric features (e.g. facial geometry, iris structure, fingerprint, or voice) or skills (e.g., typing characteristics on a specific keyboard) are often used as characteristics. A biometric authenticator is considered something that a person is. Biometrics have been used for the authentication of persons for decades; however, their ratio of false positives to true positives was not favorable early in their implementation. Therefore, biometric identifiers have only recently become useful enough for widespread adoption. New personal computers and mobile phones have begun using biometric authenticators regularly within the past five years. Depending on configuration, biometric authenticators are not prone to false positives; that is, it is unlikely that a biometric identifier is going to provide the wrong user with access to a resource, but rather experiences false negatives, refusing access even to legitimate users. However, biometric identifiers should be implemented with caution; the biometric cannot be changed if compromised. Therefore, although these complex and highly accurate methods of authentication may seem like an ideal solution to the failures of passwords, biometric authentication is still somewhat problematic.

Authorization

Authorization refers to the information system's ability to determine whether a resource should be made available to the account attempting to access it. If the user has been identified and authenticated to the system, and the user has the correct rights, then they will be authorized for access to the resource. Otherwise, the user's attempt to access the resource will fail, and a record of the attempt should be placed in the information system's logs.

The user's authorization should depend on a recorded business need for access to any information system, process, or data. Authorization always stems from decisions made by the data owner, although the authorization may be indirect. For instance, the data owner approves a project for the use of their data, but they do not mandate who should be a member of the project team. The data owner should understand and explicitly consent to the use of their data for any project, or for the data to be sold, traded, or given to an internal or external entity.

3.2 Rights Management

Within the field of information security, rights management is the concept that all data should be restricted to the least access needed to perform the organization's functions. Rights management is performed through one of several models of access control, i.e., restrictions based upon a user and upon the objects with which they interact.

Access Control List (ACL)

The access control list (ACL) is a one of the first measures of cyber security controls from the beginnings of commercial computing, when mainframe computers were still predominant in IT. Mainframes were large computers that managed and processed the data and access controls for many users. The ACL individually relates each user account and each object in a system, creating a matrix of user rights granted to the respective user at the specific object. The user account can belong to a person, system process, or machine. The rights could be read, write, or execute, and the object could be a file, directory, database, database entry, program, or any other data or processing construct. The ACL compares the user account, their permissions, and the object to any command given by the user. If the command is supported by the explicit relationship of the account, permissions, and object, it is allowed. Otherwise, the command is rejected and does not take effect.

Table 2: Access Control List in Rights Management for Files, Databases, and Printing at Dr. Maxwell's Office

Username	Medical files	Prescriptions database	Billing software	Receipts printer
Alice	Read/write	Read/write	Read/write	Read/write/execute
Bahar	None	None	Read/write	Read/write/execute
Osa	Read	Read/execute	None	None
Raj	None	None	Read	Read/write/execute

Source: Gunnels (2021).

In the figure above, each row lists a user and their permissions for a fictional example in a doctor's office, and the columns list the objects. The rights of use are then noted at the points of intersection. In this example, Bahar cannot access the medical files or the prescription database at all. They can, however, check and update billing information, as well as print receipts for the practice's clients. Alice, on the other hand, can update medical files and the prescription database, as well as perform all available activities in the billing and receipts functions. Osa can only see prescription information and execute commands (perhaps send information electronically to the pharmacy). Raj can see the patient's billing information but cannot change it; however, they can update and print receipts for the practice's services to the patients.

Access control lists must be maintained when there are changes to staff or the objects they access. Access control methods can be categorized as discretionary, mandatory, or role based.

Discretionary Access Control (DAC)

Discretionary access control (DAC) allows the data owner to determine the rights of use. UNIX and other Unix-like operating systems (Linux, Minix, etc) use DAC. The name "discretionary" indicates that the data owner can define usage rights for themselves, for the members of their group, and for all other users. A less technical example is in social networks; DAC is demonstrated by a user's ability to determine who can access their posts and personal information.

In practice, DAC can be problematic in that permissions are managed based entirely on the choice of the owner for each person or group. There is no check to see if the recipient has a responsibility that requires those permissions. It also adds complication to the management of rights when a user changes roles. Even if an employee starts off as a database administrator, they may not stay in that role. If their permissions were added individually by the database owner, they may retain administration privileges after changing roles, or even after leaving the organization.

Mandatory Access Control (MAC)

In contrast, rigorous control of users and permissions is enforced by mandatory access control (MAC). In MAC, the ACL is centrally maintained and automatically enforced. Data owners do not have the ability to override any central access policies that are put into place by the administrator. For instance, in DAC, a data owner could grant access to their files for everyone. That means, if there were a guest account created that required no password, the guest would still have access to the owner's files. In contrast, if there were a central MAC security policy stating that no one has access to certain data without providing a name and password when logging on, the guest user would not be able to read the data. The data owner may not even be able to set the guest permissions to read, or the permissions might simply not work.

Whether DAC or MAC, the maintenance of an access control list quickly becomes problematic as the number of users and computers grow and the amount of data expands. For this reason, it is now common for users and objects to be assigned to specific groups, where rights can then be defined for these groups. In a medical praxis, for example, the nurses, medical assistants, and physicians may be assigned to a group called "practice_staff." The "practice_staff" group is granted access to read and write (view and modify) files that are defined as "medical_files."

Groups used for MAC can also be assigned as part of other groups. Group rights are then inheritable, meaning a sub-group inherits all rights of use that were granted to an adjacent group. While this is generally an efficient practice, it can be difficult to troubleshoot an error if there are conflicting permissions. The inheritance chain is searched from bottom to top until an explicit permission to grant or deny access is found. For instance, suppose that permissions for the group "doctors" allows members to read confidential data, but permission for the group "medical_assistants" explicitly denies member access to confidential data. The doctors can never be added to the "medical_assistants" group, because it will limit their ability to perform their jobs. However, if the group "nurses" does not explicitly address permissions for confidential data, then adding the “doctors” group to “nurses” would grant a doctor all of the privileges of the “nurses” group without removing their group’s access.

Role-Based Access Control (RBAC)

In role-based access control (RBAC), users are assigned to groups, and groups are assigned permissions or roles. Users can have multiple group memberships, and groups can have multiple permissions or roles. Users inherit all rights from all groups of which they are a member. Rights serve to permit, not deny, therefore, there is no conflict in adding a user to multiple groups with different permissions. The user simply inherits all permissions that are available to their groups. For instance, if the user is assigned to the group “nurse” and the group “doctor,” the user inherits all combined permissions from both groups.

Some groups have high levels of access that, when combined, can compromise security. For instance, let’s assume the group “medical_assistants” has permission to enter prescriptions in the patient system, but only the group “doctors” can authorize the prescription. This would be a good way to ensure that medical assistants cannot prescribe drugs and authorize them to the pharmacy without oversight. If anyone in the “medical_assistants” group is also assigned to the “doctors” group in the system, they would be able to create and authorize prescriptions to any patient, including themselves. This could allow access to highly restricted substances without any oversight. Even with good intentions, it removes the safety check that a second medical professional provides, thus endangering patients if the medical assistant makes a mistake.

Separating roles that can balance each other’s access is called separation of duties, and it is used to prevent deliberate or accidental cases where a user can perform critical actions without oversight. Separation of duties is a form of least privilege, which is the principle that access should be limited to only those permissions necessary to perform in a role. This does not mean that some roles do not need significant permissions. For instance, system administrators must have access to most possible activities on a database server. However, system administrators do not usually have significant permissions for the databases themselves. If a user had administrator permissions for both the database information and the server, they could give themselves access to read or change any data, then remove the logs of doing so. Security personnel must therefore review the roles on an information system and group membership, so that separation of duties and least privilege are not compromised.

3.3 Rights Check

There are many possible methods of authorization, and two of the most popular are explained below. The first, Bell-LaPadula, is an authorization model for the viewing of data which protects confidentiality. The second model is Biba, which provides less protection for confidentiality but a great deal of protection for data integrity (Mattord & Whitman, 2017). These are not the only two models of authorization control, but they are straightforward and conceptually applicable for both IT and non-IT scenarios.

Models of IT Security for User Authorization

The approaches presented so far do not support fine-grained control of usage rights. Consider a requirement, such as “laboratory data of the last three calendar years may only be deleted by the practice owner.” There is no way to directly map this requirement to the permission controls listed above without implementing a cyber security model. A cyber security model relates the protection goals of the information system to the security rules that are implemented. Along with managing the user rights, the administration must also assign rules to the objects. When the IT system enforces desired object access rules and user rights, it is possible to manage the confidentiality and integrity of IT system data.

Numerous models of cyber security are available, such as Chinese Wall, BMA, and Clark-Wilson. These models each suit different types of data and security requirements. For user rights, the Bell-LaPadula model and the Biba model are often applied. These two simple models are low-effort and high return-methods to enforce certain rules of a cyber security strategy. Bell-LaPadula allows enforcement of confidentiality requirements on shared objects. The Biba model allows enforcement of object integrity (Mattord & Whitman, 2017).

Bell-LaPadula

Bell-LaPadula extends definitions of the usage rights in an ACL with a general access rule, enforced each time a user accesses an object. Users and objects are divided into levels. Object classifications define the needed confidentiality, while user clearance levels reflect their ability to read data. As classification levels for object confidentiality go up, so do required clearance levels for access permissions. This is a familiar concept in military security, where object confidentiality levels might be public, confidential, secret, or top secret. In patient data, the object labels might be public, private, or confidential. Bell-LaPadula establishes the rule that a subject may only read objects of lower or the same security rating (no-read-up) and only write objects of higher or the same rating (no-write-down) (Mattord & Whitman, 2017).

In our medical practice example, Dr. Maxwell may define different clearance levels to determine the patient data access that each of their staff members has. They decide to separate the object and user levels into “public,” “individual,” “private,” and “confidential.” They further decide to use RBAC, where staff clearance levels are determined by their roles in the practice. Since Dr. Maxwell is concerned about their patient’s confidence and trust, they decide to reserve read access to confidential data to themselves. They decide that any additional practice physician can have clearance to read documents up to the security level of private. The additional physicians can also read public, individual, and private data. The rest of the staff can read only public and individual data.

The doctor also knows that write access for their staff cannot be restricted to the same levels. Everyone in the practice is able to write up to confidential data, whether they can read it or not. Therefore, the patient intake can be performed by any available staff member. Once the intake record is written, only those with the appropriate access can read it, meaning that the non-medical staff cannot always view the same records they have entered. It also means they would be unable to correct mistakes in records that they have entered, if said information is categorized higher than their access level.

Staff having permission to write information they cannot read or correct is a minor inconvenience, and it is a worthwhile trade-off for the confidentiality that it enforces. This keeps staff in similar roles from being able to read records entered by each other. A user in the Bell-LaPadula model can only write at their assigned access level or higher. This is a strong protection against data being inaccurately assigned for read access, but it also ensures that data steadily migrate upward in categorization. The remedy for this issue is manual re-categorization of data, which can be a long and difficult process.

The table below provides insight into the problem of migrating permissions. Notice that Dr. Maxwell can read anything in their practice, but everything they write or modify is classified as confidential. This applies to new information that they generate, and to information that they modify. Therefore, no one else can access and use the information entered by Dr. Maxwell, even if the information is harmless and general, such as adding a note that the patient is allergic to their new cat. Dr. Maxwell will need to manually recategorize their notes and system entries in order to let the rest of the staff work with the new patient's file. Further, any printer Dr. Maxwell uses to print documents cannot be used by anyone else in the office if they don't have additional security measures (for example, a passcode is needed to print their documents).

The write-up requirement seems very restrictive, but it serves a necessary purpose. By ensuring data access is automatically limited to the same or higher clearance level as the data producer, Bell-LaPadula prevents Dr. Maxwell from accidentally including confidential data in a document that can be read by any other staff member until they manually change the classification. If Dr. Maxwell carefully reviews documents before changing their classification, they will spot any data that must be removed before assigning a lower access requirement.

Table 3: Rights Management in Bell-LaPadula Model

Role	Can read	Can write	Minimum write level
Receptionist	Public	All	Public
Nurses and medical assistants	Public, individual	Individual, private, confidential	Individual
Employed doctors	Public, individual, private	Private, confidential	Private
Dr. Maxwell	All	Confidential	Confidential

Source: Gunnels (2021).

Biba

The Biba model also uses security ratings similar to the Bell-LaPadula model, but it assumes permissions related to integrity of objects is the most important quality. Biba inverts the Bell-LaPadula model. Here, objects are not protected against knowledge, they are instead protected against manipulation by unauthorized persons. The user and the object still have assigned clearance and classifications. However, to protect integrity, the user is assigned an access level for writing and modification of information. The user is not entrusted with the ability to add or modify data that require higher integrity than their rank. Any information they input is assigned (or downgraded) within the users' access levels (Mattord & Whitman, 2017). If the medical assistants need to update information entered by Dr. Maxwell, they can. However, the information is no longer assumed to be as accurate as it as before, since they changed an object at a higher level. So if the case file was written by Dr. Maxwell and saved at the confidential level, the level of integrity will be lowered any time another person in the office writes to the file. If it is assumed that a higher security rating also means higher integrity, the Biba model establishes the rule that a subject may only write objects of lower or the same security rating (no-write-up) and only read objects of higher or the same rating (no-read-down).

For example, if a nurse has the classification "individual," when using Biba, they can read a private report from the employed physician. If they change the current copy or save it under a different name, then the changed copy or new file can have an integrity level of public or individual, because those are the highest levels of integrity confidence available to the nurses and medical practitioners. If the doctors in the practice require that file to have a higher level of integrity, they should review the changes and save the file with their own permissions, in effect validating that they believe the changed object maintains integrity after the changes. As with Bell-LaPadula, the documents have a tendency to migrate away from their first confidentiality or clearance designation. Here, they migrate toward less confidence in integrity as they files are changed. Manual review and approval from employees with higher levels of integrity assigned are required in order to restore the original classification.

Table 4: Rights Management in Biba Model

Role	Can read	Can write	Maximum write level
Receptionist	Public, individual, private, confidential	Public	Public
Nurses and medical assistants	Individual, private, confidential	Public, individual	Individual
Employed doctors	Private, confidential	Public, individual, private	Private
Dr. Maxwell	Confidential	Public, individual, private, confidential	Confidential

Source: Gunnels (2021).

In their pure form as described above, both the Bell-LaPadula and the Biba model are rather restrictive and therefore difficult to use, in particular because of the restrictions regarding access to objects with a lower security level (no-write-down/no-read-down). Therefore, in practice these models are usually weakened in some form, e.g. allowing access to objects with a lower security level after explicit confirmation. For example, in the Biba model, Dr. Maxwell might be able to read public, individual or private contents after confirming that they realize that these contents have a lower level of integrity.

3.4 Preservation of Evidence

Evidence in an information technology system ranges from the logs for user and system activities to the data that were stored on the computer during a particular timeframe. Evidence preservation has two functions in information technology: the ability to diagnose and recreate an information system activity, and the ability to provide proof of an illegal activity to law enforcement.

Administrators of an information system must have adequate training to perform evidence preservation. Simply copying the information from one system to another, such as an online or tape backup, does not preserve the metadata around the evidence in a way that proves its authenticity and applicability. A “forensic copy” of evidence provides a perfect replication of the evidence, including the correct access records. Specialist tools and procedures are available to make forensic copies of data or entire computers, but they require that the user have access to and expertise with certain tools. Therefore, the ability to preserve evidence is not a natural outgrowth of an organization’s IT system and must be deliberately planned in the purchasing and training budget.

Along with capturing both the content and the context of computer evidence, the organization must prove that the information has not been altered before it is put to use. The common method of doing so is to label the evidence and lock it in a room (or preferably a safe) where only a few named and trusted individuals have the ability to retrieve it. Evidence is expected to stay in the locked location until there is a specific reason for its retrieval. At that time, an entry is made on a designated paper to record its handling. This paper record is called the chain of custody, and it includes the name and signature of those people who had possession of the evidence at any time. Chain of custody tracking complements the secure storage of evidence, and it is surrendered with data to law enforcement, if that is the purpose for which the data were collected.

Reprocessing

Data reprocessing, i.e., the ability to review data for new analysis, is critical to functionality in information security. Data reprocessing is commonly known as analytics or forensic analysis. It allows security professionals to perform structured reviews of large amounts of evidence, and to determine what activities may have occurred. The reprocessing of data is a method of determining whether there are indicators of compromise that may have been missed when the compromise occurred. Indicators of compromise in a network are signs that an attack has been successful. They may be evidence that any of the following has occurred: an intruder logged in to an account not their own; malware has been installed; a device is performing a function that is not intended; a file has been changed unexpectedly; or someone who is legitimately allowed to access the system has performed an inappropriate function. As one might expect, meaningful reprocessing depends on applying the information system and the network to collect records (logs). Logs must include the name of the account that performed an activity, when the activity was performed, what the activity was, whether the action was successful, and the object impacted. Without this information to replay and examine, it is virtually impossible for the examiner to determine what happened. Reprocessing of data may occur at several different points, and the data may be reprocessed immediately. The data can (and should) be saved for later review against newly found indicators of compromise. For example, if the compromise is caused by a zero-day exploit, indicators of compromise may not be entirely understood.

SUMMARY

Identification is the action of asserting a username; authentication is providing evidence such as a password, PIN, or biometric to demonstrate the identity belongs to the one asserting it. Authorization matches the identified user to a resource and determining if permission is granted for its access.

Rights management models all include some combination of the user's proven identity and a methodical way for assigning access. Discretionary access is controlled by the data owner, while mandatory access is centrally controlled at the account level, and role-based access is controlled with the assignment of a user to a role. Evidence is preserved both to recreate the events that occurred in a system or network and to ensure that it can be reprocessed in order to determine if an unrecognized compromise occurred. Functionality of business assets is a concern of information security, but the responsibility is shared with information technology operations teams.

UNIT 4

CYBER SECURITY MANAGEMENT

STUDY GOALS

On completion of this unit, you will have learned …

- the definition of a protection requirements analysis.
- what protection standards should apply to an organization.
- which international standards apply to information security.
- what benefit is provided by choosing a protection standard.

4. CYBER SECURITY MANAGEMENT

Introduction

This lesson provides an overview of an information technology (IT) protection program. You will learn to choose which objects to protect, determine which standard to apply, and close the gaps between the necessary protections and the protections already in place. This lesson also introduces selected cyber security standards. These standards are from international and U.S.-based organizations; some are freely available, some are available to any person or organization for a fee, and some are restricted to limited audiences, with or without fees.

Technical progress moves quickly, and standards change to accommodate it. This introduction and analysis are accurate as of early 2021, but ongoing development means that it will become outdated. The application of standards always requires a detailed investigation of current needs and applicable guidance. This lesson will remain valuable for a reasonable period to justify learning it, but any deeper detail needs independent confirmation for a real-world application.

4.1 Basic Concepts and Standards in Cyber Security Management

Cyber security is achieved through cooperative action against an organized plan. Many smaller organizations begin with a piecemeal implementation of cyber security, reacting to incidents or regulation as they come to the attention of the executives. Value is improved by a coordinated, comprehensive approach that includes every department. Regardless of their size, organizations benefit from choosing a standardized methodology. These published overviews are created by experts to ensure all aspects of the organization can be protected.

Within the U.S., there is no centralized requirement to follow an information security basic protection plan, let alone a requirement for a specific one. Many different organizations—governmental, international, or for-profit—have developed standards for the creation of a baseline protection plan. Whoever is tasked with security planning should review several different methodologies to choose the one best suited to the needs of their environment.

Methodologies for information security programs follow the same overall pattern. They require an understanding of the assets to be covered, an assessment of the hazards and risks which could manifest, the implementation of a plan to minimize risk impact, and a review process to ensure the plan remains effective. The following section is a generalized overview of the pattern. It is not aligned to a specific standard, but sufficient to familiarize the reader with information security program goals.

Protection Requirements Analysis

Protection requirements analysis in cyber security is data centric. Evaluation of the estate to be protected, and the potential for harm, are expressed through damage to the organization when data lose confidentiality, integrity, or availability.

Loss scenarios

To tailor protection requirements, organizations should consider the types of assets they possess and the factors that demand their protection. This is not a one-to-one relationship. If the organization suffers a security incident, such as failure to protect personal health data, they see consequences of violating laws, but they may also suffer **reputational damage** and financial damages from the same event. The loss scenarios for any organization will vary from a pre-determined list. However, the most common types of loss scenarios are

Reputational damage
This term refers to intangible loss from the public removing its trust from a company or brand. It is reflected in lower sales, loss of stock value, or lower overall public opinion.

- violation of law, regulation, or contract;
- failure to protect personal sensitive data;
- failure to protect client or organizational sensitive data:
- danger of physical harm to humans;
- inability to perform the business function;
- reputational or other consequences of public disclosure; and
- financial impact to the organization.

Quantifying damages

Damages caused by cyber security loss scenarios are rarely quantifiable to a specific monetary amount. Instead, losses are classified into categories of damage, such as low, moderate, or high. These categories can then be defined in amount ranges that make sense for the enterprise. For instance, an international organization with multiple billion dollars in annual revenue may see two hundred thousand dollars as a low loss threshold. A start-up company with only a few hundred thousand dollars of annual revenue would classify that range as high damages.

The initial scope of the analysis should be solely about possible effects on the organization in case of damage occurs. Estimation of likelihood is reserved until later in the process. This determination of the need for protection should be applied to

- applications, operating systems, and software;
- IT and network hardware;
- communications equipment;
- offices or other workspaces; and
- humans, regardless of their relationship to the organization.

Risk appetite

Risk appetite
This is the willingness of the business to accept potential losses related to physical or virtual events. Risk appetite is often based on financial impact to the organization.

Risk appetite is the amount of risk that an organization is prepared to tolerate to perform business-related activities ("Risk appetite," 2019). In terms of cyber security, risk appetite is applied to choices that impair vulnerability remediations. If loss scenarios are unknown, and damages unquantified, the organization will tend to make risk decisions based upon the circumstances they do know, such as sales impact and potential business losses. This inflates the risk appetite for cyber security.

For instance, there may be a known vulnerability on an internet-facing application server. If the business depends on the application to make sales, they may be reluctant to fix the vulnerability until they are certain such changes will not ruin the application and decide to delay fixing the vulnerability until the changes have been thoroughly tested. In this example, the business faces two potential risks: cyber security risk around the vulnerability, and business risk around the loss of sales. Without quantifying the damages, their appetite for cyber security risk is greater than the appetite for loss of sales. No one can be certain whether the potential loss in either scenario is higher, so the decision is made based upon a desire to avoid sales loss.

A protection requirements analysis with realistic loss scenarios and quantified damages will assist the cyber security professional in communicating risk to the organization. When security risk is better understood, the decision-makers can more evenly balance business and security risk appetites.

Protection Standards

Protection standards
This is security guidance that covers a stated range of security protections with the aim of providing sensible choices for multiple types and sizes of organizations.

For entities based within the U.S., there are a number of popular **protection standards**. The most common approaches are Control Objectives for Information and Related Technology (COBIT) from ISACA, the U.S. federal government's National Institute of Standards and Technology (NIST) series, and the 2700x series created by International Organization for Standardization (ISACA, 2021; NIST, 2015; ISO, n.d.-b). These security selections are appropriate for almost any organization, as they can be tailored to fit organizational goals, data sensitivity, enterprise structure, and many other characteristics. Certifications against these catalogues are available, but many enterprises follow them without the intention of becoming certified. Instead, their goal is to find a proven process that covers most, or all of, their IT and business assets.

Governance
The responsible and systematic leadership and control of an organization. In the case of IT, the fundamental design and objectives play a key role in an organization's governance framework, which is then implemented by the organization's management.

COBIT is a methodology created by ISACA. Its purpose is to describe a uniform, integrated **governance** framework for all IT processes, including information security. COBIT contains requirements for data protection and cyber security in its goals APO13 ("Managed Security") and DSS05 ("Managed Security Services"). Version 5 of COBIT also provides structured implementation "best practice" approaches. COBIT is a top-down approach, which begins with the corporate goals and strategies and flows down through architecture, processes, and operations (ISACA, 2021).

The International Organization for Standardization is an international, non-governmental voluntary body. Expert representatives from member countries provide input to the creation of each new standard (ISO, n.d.-a). The International Electrotechnical Commission is an additional expert body that collaborates with ISO through their Joint Technical Committees (JTCs). There are two JTCs; JTC 1 participates in the creation of information technology standards. The ISO/IEC JTC1 2700x series standardizes approaches for Information Security Management Systems (ISMS), audits these implementations, and dives deeper into specific portions of information security. It is most applicable for large organizations with either an international scope or a need to prove security compliance to its clients (ISO, 2022a).

The U.S. National Institute of Standards and Technology publishes their Special Publications (SP) series free of charge on the internet. The Special Publications 800 series covers information security measures, including cyber security. This set of documents comprises over 150 standards, reports, and guides on topics of security (NIST, 2018a). Organizations that store, transmit, or process non-classified sensitive data belonging to the U.S. federal government must abide by the SP 800 series requirements, including the creation of a security program (SP 800-37) and specified types of security controls based on data sensitivity level (SP 800-171). Organizations that do not possess U.S. federal government data may use the standards directly or use a subset of them to supplement their other controls. NIST SP 800 series allows a data-centric, customizable approach to creation of and information security program. The control guidance is detailed without specifying any required technology, and this flexibility, combined with its free distribution, makes it a popular choice for enterprises not required to follow another model (NIST, 2018a).

Protection Implementation

The implementation of protections within an organization follow a basic procedure of control selection, inspection, and the remediation of missing controls.

Control selection

After the selection of the assets to be protected and the choice of control catalog, an organization should engage in control selection—that is, determining which elements within the control catalog should be applied. In this step of protection, the organization determines how loss is likely to happen to each asset. From the resulting loss scenarios, the organization selects controls that would prevent the loss. The selection of controls does not require choosing a particular product or vendor for the implementation, Instead, the organization should concentrate on finding the correct control requirements list to protect assets within the organization’s risk tolerance.

Control implementation, in which the organization chooses technologies and processes to protect assets, should be completed once the control requirements are set. If the organization chooses technologies prior to determining the control set needed, there is a danger that the technologies will not fully meet the final control set. New purchases, configuration changes, and protection gaps are likely to result from choosing technologies before understanding the protection requirements.

Control inspection

Control inspection
In this type of audit, security control implementation and effectiveness are reviewed, either all controls within one audit, or by choosing the most critical controls.

Control inspection is a method of audit in which the effectiveness of security measures is validated. Control inspection should be performed regularly on a schedule that is tailored to the organization. Annual control reviews are sufficient for many organizations. For those where a thorough review of every control for every protected asset is overwhelming, a more sensible plan may be to perform limited reviews of critical security controls on most areas. The regular complete review is then limited to those assets of highest value to the organization. This method aligns with the general security principle of rigorous protection for the most valuable assets and information systems.

Remediation of missing controls

Changes in information systems, addition of new assets, and changes to processes are just a few of the conditions under which security controls may be missed. The inspection of control implementation provides an opportunity to locate and remediate these errors. When a control is absent, the reaction should not be to immediately demand its placement, even if the resulting vulnerability is outside of the organization's willingness to accept risk. Instead, the control implementation should be scheduled and planned. This way, the organization does not harm itself further with a hasty action that leads to downtime or other mistakes. The organization can and should act with urgency when a critical control is found missing, but changes must be thoroughly tested and scheduled with the necessary expertise available in case of problems.

The organization should maintain and update a list of the controls that are missing, when the issue was discovered, how it is to be corrected, and when the correction is scheduled. The NIST SP 800-37 model includes a template for a "Plan of Action and Milestones." This template is a simple and detailed way of tracking the risk and planning for fixing it. The contents of the plan are flexible, allowing information like the budget commitment for the fix, the assigned resources and business owner for the commitment, or conditions that lower the risk until it can be fully removed (NIST, 2018b).

After missing controls are put in place, the organization should validate their effectiveness. This validation can be performed internally, but it should be outside of the implementation team and not within the reporting structure of the business owner. This allows the necessary freedom to inspect the control implementation and report any inadequacies in is repair without danger of reprisal.

4.2 The ISO/IEC 270xx Series of Standards

ISO/IEC 270xx describes a series of international standards on information security and information security management systems.

What Are ISO and IEC?

ISO is the short name used for the International Organization for Standardization in which the various national organizations for standardization work together to publish international standards. In the context of technology standards, ISO often works together with the International Electrotechnical Commission (IEC) to publish joint international standards such as those on information security labeled the 270xx series. The name of the series indicates the range of numbers included in the series.

Naming conventions for ISO/IEC standards

ISO and ISO/IEC standards are named with a number containing up to five digits, followed by a dash and another number if published in more than one part, and a colon followed by the year in which it was published. For example, the proper name of the IT service management standard is ISO/IEC 20000-1:2018, which means it is the first part of a standard with multiple parts and was published or revised in 2018. Likewise, the standard to protect personally identifying information in cloud infrastructures (27018:2019) can be understood to have only one part and waspublished in year 2019. In most situations, the standards names will be shortened for ease of use. The common method of reference is to use "ISO" and the standard number, even when the standard is cooperative with another organization. ISO/IEC 27017:2015, for example, would often be called "ISO 27017". If the year is left out, the name references the version that is currently in force.

Important ISO Standards for Information Security

ISO publishes international standards for multiple aspects of information technology, including information security and cyber security. Information security is supported by the proliferation of IT standards in general. Predictably configured information technology is simpler to monitor for abnormalities than a collection of unique configurations. However, there are specific information security standards within the ISO/IEC 270xx series.

The following are several ISO/IEC standards for important topics in **information security management and implementation (ISMS)**. ISO/IEC 27001, the standard for creation of an ISMS, can be viewed as the most important document within the series when it comes to information security. Many of the remaining documents can be used with an ISMS that was not based upon ISO standards. However, the establishment of a comprehensive and effective security practice depends upon a robust ISMS. ISO/IEC 27001 is one of the few widely accepted standards for creation of an ISMS (ISO, 2018a).

Information security management system (ISMS)
This is the high-level implementation of security planning and guidance for an organization.

ISO/IEC 20000-1—Service management

This standard outlines requirements for the running of IT services. Service management, as established in this document, includes concepts, such as planning, delivery, service improvement, and response to service failures. ISO/IEC 20000-1 includes specifications for information security management, incident management, and service continuity management. In these areas, the standard overlaps with, but does not completely cover, ISO/IEC 27001 requirements (ISO, 2018b).

ISO/IEC 27001—Information security management systems

ISO/IEC 27001 is the most important standard in the ISO/IEC 27000 series for information security. This standard defines the essential requirements for an IT security management system (ISMS) and is the only part of the ISO/IEC 27000 series of with a corresponding certification, i.e. organizations can get their ISMS certified as conformant to ISO/IEC 27001. This standard is process-oriented and does not dictate types of technology to implement or suggest vendors. Instead, it focuses on the establishment, implementation, execution, monitoring, inspection, maintenance, and improvement of an ISMS (ISO, 2022a). This process-oriented approach includes the following points:

- understanding requirements for an IT security organization
- defining a guideline and goals for IT security
- cyber security risk management and its integration with the organization’s general business risk
- monitoring and reviewing ISMS performance and effectiveness
- objectively measuring continuous improvement of the ISMS

ISO/IEC 27002—Information security controls

ISO/IEC 27002 provides guidance for organizations in the process of security mechanism implementation (ISO, 2022b). ISO/IEC 27002 is a supplementary guideline for the management of IT security. Its purpose is to provide a better understanding of the requirements in ISO/IEC 27001 and to serve as a basis for the development of institution-specific procedures and regulations. It can be used whether the organization has chosen recommendations from ISO/IEC 27001 standards, commonly accepted security controls, or a custom security management implementation (ISO, 2022b).

ISO/IEC 27003—Information security management system implementation guidance

ISO/IEC 27003 provides guidance for on the implementation of the information security management system (ISMS) as outlined in ISO/IEC 27001. It covers a very narrow range of information security, in that it does not provide guidance for any requirements outside of the process for managing information security (ISO,2017).

ISO/IEC 27004—Information security management—measurement

ISO/IEC 27004 provides a framework for the measurement of security program effectiveness. It assists the organization in determining what to measure, how it can be measured, and whether the measurement processes are appropriately implemented. This standard can be applied to any security program, not only those based upon ISO/IEC 27001 (ISO, 2016).

ISO/IEC 27005—Guidance on managing information security risks

ISO/IEC 27005 provides a structure for understanding and evaluating risk within an organization. It also describes methodologies for risk treatment and risk monitoring (ISO, 2022c).

ISO/IEC 27017—Information security controls based on ISO/IEC 27002 for cloud services

This cloud security standard expands the operational and implementation guidance found in ISO/IEC 27002. It applies to both cloud service providers and cloud service customers. The standard discusses a division of responsibility in the relationship between cloud providers and cloud customers. It also includes additional new security controls suitable for cloud and the guidance to implement them (ISO, 2015a).

ISO/IEC 27018—Protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27018 is a standard with specific scope—it deals with the processing of personally identifiable information (PII) by public cloud service providers. It differentiates the ownership of data from the processing responsibility, ensuring that those abiding by the standard keep management control of the PII within the scope of the organization that owns the data. This guidance provides the recommended set of information security controls—technical and process—that both the cloud service provider and the cloud customer should use to assess the implementation of privacy and security measures by the vendor (ISO, n2019).

ISO/IEC 27033—Security techniques—network security

This is a seven-part standard, ranging from ISO/IEC 27033-1:2015 to ISO/IEC 27033-7:2023. The ISO/IEC 27033 series provides guidance on the secure procurement, maintenance, and operation of networks. It assists in the identification of network risk and defines potential controls to aid in reducing this risk. This standard can be used to understand secure network operational requirements and plan ongoing monitoring and review. Part one of this standard also provides a guide to other six sections (ISO, 2015b).

ISO/IEC 27039:2015—Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

ISO/IEC 27039 is the standard for selection and operation of an Intrusion Detection System (IDS) or an Intrusion Protection System (IPS). Both IDS and IPS are systems that ensure the organization is alerted by behaviors that indicate an intruder into the network or hosts. An IDS is, by nature, passive. It alarms when inappropriate usage is found. The IPS assists in prevention of a compromise, taking pre-programmed actions to stop an intruder from continuing.

When planning a new IDS/IPS solution, the standard requires selection responds primarily to the identified problem areas of a network. Expenses should be considered, including acquisition and operation. Deciding factors should be alerting strategies (via e-mail, SMS, and dashboard) and any additional tools that make the solution more functional in the target environment. Deployment under ISO/IEC 27039 includes a plan for its implementation. Activities, such as determining the location and the security requirements to protect the device, are included in the plan. Operational processes are also directed, whether that is the ongoing maintenance of the IDS/IPS rules or the handling of alarms and incidents. As this is a mature standard, it contains detailed explanations and proven implementation solutions.

ISO/IEC is one of several organizations producing standards for information security, and smaller organizations may need to implement a smaller selection of standards and controls than the 2700x series describes. In that case, other standards, such as those mentioned in the first half of this unit, may be applicable. The most important element of choosing a standard is, ultimately, its relationship with the data the organization is processing and protecting.

SUMMARY

The value of a cyber security program is improved by a coordinated, comprehensive approach that includes every department. This approach should include the use of published security standards, some of which are available without cost. Certification of compliance with standards is also available, and this step is sometimes required to work with government agencies or large and security-conscious organizations.

The U.S. has no centralized or legal requirement for businesses to follow an information security standard. Regardless of this, it is important to choose or create one suitable for the enterprise’s needs. All security standards require an understanding of the assets to be covered, assessment of applicable risks, implementation of a mitigation plan, and ongoing review and improvement.

The International Organization for Standardization (ISO) has created many IT and cyber security-specific standards. ISO is a volunteer group that allows participation from a variety of international subject matter experts, and the standards they provide are approved by consensus. This makes the ISO standards a good guideline for international organizations, as the standards are generally recognized as fit for their purpose (ISO, n.d.-a). The ISO/IEC 2700x series of IT service management includes the information security and cyber security standards. The 27001 and 27002 standards are the most important standards for information security overall, and organizations may be independently certified to comply with 27001 (ISO, 2022a; 2022b). The 27017 standard for cloud service security and the 27018 standard for protecting personally identifiable information in cloud services are two of the few cloud-hosting security guides that clearly outline responsibilities of both customers and service providers (ISO, 2015a; 2019).

UNIT 5

CYBER SECURITY MANAGEMENT IN EVERYDAY LIFE

STUDY GOALS

On completion of this unit, you will have learned …

- the definition of social engineering.
- the attacks that target end users and the computers used by attackers.
- which end user behaviors pose the most danger to cyber security.
- what role physical protection plays in maintaining cyber security.

5. CYBER SECURITY MANAGEMENT IN EVERYDAY LIFE

Introduction

It is tempting to think of cyber security as being mysterious and technical, but many of the most important protections for data and computer systems are in the hands of the end user. Administrators can set password requirements, schedule backups, and turn on malware protection on the users' machines, but as long as the end user opens emails or visits websites without showing proper caution, there is a good chance that security controls will be rendered useless.

Instead of viewing the following controls as the responsibility of the security team alone, the organization should look for ways to help security and end users communicate. The willingness to follow security guidance is a product of understanding how important the user's role is in protecting their own interests. If the user has any one most important security role, it is in preventing the success of social engineering. There is no technical response to social engineering, since it depends upon the vulnerabilities of human society. Only by educating workers and reinforcing their responsibility can the security team have any defense against these simple and successful attacks.

5.1 Password Management

Most technology still uses account names and passwords for authentication. In these cases, service users should ensure their passwords are difficult to guess or resistant to brute force, but not difficult to remember for those who are supposed to know them. The goal is to eliminate the need to write a password down, but not because the password itself is simple.

Accounts with passwords are subject to the password strength requirements of the managing organization. An objectively strong password is one that neither another human nor a computer program can discover in a reasonable amount of time. The characteristics of a strong password will change as computer programs and criminal hackers grow more sophisticated. It is currently recommended that passwords contain a minimum of eight characters, preferably more, and a mixture of letters and numbers, as well as both lowercase and uppercase letters. If possible, the password should also contain a symbol.

To avoid **password guessing attacks**, a password should not be a single word or a short set of words. This is true even if a number is added to the beginning or end of the words. The passwords should not contain names or numbers related to the owner's family; names of children and pets are known to be common passwords and are often the criminal hacker's first guess. Addresses, sports teams, and player names are also common passwords that are easily discovered. Passphrases, i.e., a longer string of words such as a full line of obscure poetry, a line of a song, or a favorite phrase from a movie complete with punctuation, are preferable to short passwords, especially if there can be numbers and symbols included.

Password guessing attack
This is an attempt to break into a user or computer account protected with only a password. This attack tries common letter and number combinations in the hope that the user has not created a complex or unusual password.

Guidance for the account owner

Passwords should be handled with care and never shared. If a password-protected resource needs to be shared, the user should be provided with a method that does not require sharing the password. When passwords must be stored, the owner of the account should use a tool designed for protection. Password keepers are programs that allow the user to store multiple passwords in a small database. This database is itself protected, whether with a unique password or a biometric authenticator. This database allows the user to have multiple unrelated passwords for different functions and only use one to unlock it. This method of password storage is preferable to other types that rely upon the criminal hacker not knowing the whereabouts of the password list. Excel spreadsheets, text files on the user's desktop, sticky notes under the keyboard or in a desk drawer, and personal phone books are all well-known sources of plain-text passwords. It is tempting to find one strong password and reuse it for multiple accounts. However, this is problematic due to the limited number of account names used. If an account name is common to the password (for instance, email address as login), then any compromise of one account means all identical logins are at risk.

In the past, it was also recommended that users should update their passwords regularly, preferably every thirty to sixty days. However, experience has shown that this often leads users to define very weak passwords that they can remember easily, and thus actually reduces security. Therefore, the requirement to periodically change passwords is no longer recommended (Grassi et al., 2017). The best defense against password theft is to reduce the use of passwords, or to add another type of authentication along with the password. Biometric access, physical access tokens, or **multifactor authentication** through a mobile phone should be enabled whenever the user has the option.

Multifactor authentication
The use of more than one type of authenticator, such as what you have (a token or phone), what you know (a password), and what you are (a fingerprint or facial geometry). Two out of the three factors are usually considered sufficient.

Guidance for the information technology (IT) administrator

For a new user account, the login and password are routinely predictable. This efficiency is to the organization's advantage when adding a user, but anyone who knows the pattern will find it simple to use the account. If user accounts must be enabled prior to their first login attempt, requirements can be set to lower the risk of an unauthorized access. Systems for account management may allow the administrator to set an expiration for the initial password, prevent **password reuse**, and force a password change upon first login. Expiration of the password ensures that the administrator controls how long an unauthorized user has potential to discover and compromise the account. The combination of forced password change and no reuse provides two forms of password security. First, the user is prevented from keeping the predictable pre-set password. Second, it raises the likelihood that a compromised new account will be discovered and the initial password will no longer work when the authorized user attempts to log in.

Password reuse
Users may choose one password for accounts belonging to different organizations. This is considered a poor choice, as it allows one compromised organization to open access wherever the password is used.

5.2 Data Backup

Data backup contributes to the successful security strategy of any enterprise. When data are accidentally or maliciously deleted, backups are the efficient (and usually only) way to completely regain access to the information. If data integrity is in question, backups can be used to prove when and by whom the data were created, changed, or deleted.

Backups for data should be executed based on the criticality and amount to be stored. For most enterprise-level data, backups should be performed in a schedule of both comprehensive **full-data backups and incremental change backups**. In this method, restoring data from any checkpoint is possible, and the cost of data storage is low than full daily backups. When backups are restored with the combination of the latest full data and supplemented with the incremental changes, only a day or a few days worth of updates are missing.

Full and incremental backups
When data is first backed up, the record should consist of all system data. After that, a series of backups should be taken on a regular schedule that only include changes made from the original

An organization may find that critical enterprise-level data must always be fully up to date. In these circumstances, data are also written to immediate online storage. This is seen with critical databases, where the database is "mirrored," meaning every change in the database is immediately also written to another database that exists solely to provide a perfect copy. Mirroring databases does not prevent problems caused by erroneous data entries, but it avoids any gap between the last scheduled backup and the point when a critical database becomes unavailable. When the main database becomes unavailable, the administrators can "break the mirror" (disconnect the databases), and the full critical data set is still available and perfectly up to date. This backup becomes the new active database, and administrators set up a new mirroring system to replace it.

User workstation backups are best handled as an extension of the IT department's responsibility. Commercial products are available to automatically fetch all user files from workstations and write them to a centralized location. This allows the IT department, or even a tech-savvy end user, to restore a file that was mistakenly deleted from their workstation. Organizations that have embraced cloud computing also have the option of backups that are managed and operated by cloud service providers. These backups are, like mirrored databases, up-to-the-moment copies of information that allow minimal data loss.

If data backups are the responsibility of each user, the IT helpdesk can expect significant numbers of request for file restoration, many of which they have no power to service. If a user fails to perform regular backups, the data available to restore will be little and dated. Some users may choose small **USB drives** to store data and, while these drives are convenient and portable, they are easily lost and may not store information securely. These drives may store data without encryption and without any authentication requirement to restore data to a target workstation.

USB drives
Also called memory sticks, these small hard drives connect to the universal serial bus (USB) slot of a computer. A USB drive is often used to provide portability to files and small programs.

Wherever data storage takes place and whoever stores them, the ability to retrieve data must be limited in the same manner that the original data access is limited. This usually means that data backups should be protected with encryption in every location. Data that have been retrieved from a backup should remain associated with their original access permissions; the ability to restore data and unencrypt them should not be the only limitation to their access. Encryption that is unbroken at this point may become insufficient in the future, which would leave data unprotected from anyone with access to restore them. Further, persons assigned the responsibility for performing backup administration may not need access to read that data that they are handling. Continuing the association of ownership and access controls throughout the backup and retrieval of data prevents these inappropriate access scenarios.

When doing backups, it is important to regularly check that these backups are indeed readable and complete, and to ensure the security of the backup data.

5.3 Email Security

Email security covers a wide range of protections. Email ingress (intake) filtering lessens the barrage of unwanted commercial email and phishing attempts. Egress (exit) filtering allows a checkpoint for software that prevents data loss, assuming this capability is implemented in the organization. Backups of email prevent loss of data. Email can be signed to prove its authenticity, and it can be encrypted to ensure its confidentiality.

Email security is a cooperative effort between the administrators and users of an email system. Email and security administrators are responsible for implementation of the functionality listed above via the commercial tools that may be purchased separately or may be integrated into the email server software. If an organization chooses to use email services provided by a third party (such as Microsoft O365 or Google's Gmail), security services are included with the service costs. These services are enhanced by the scope of the provider's network and experience, and they benefit from system-wide protections developed in response to attempted intrusions on other customers. However, the local administrator still has a responsibility to enable protection options and configure them appropriately for their organization.

User behavior is the most important aspect of protection against malware delivered through email. If the user exercises a healthy skepticism toward unexpected electronic communications, they can protect the computer from attacks that avoid the malware scanner. Constructive user behaviors include deleting suspicious emails unopened, verifying that email attachments are expected and necessary, and opening internet links from trusted communications. Additional non-email methods of malware protection can be found in the next section. If an **exploit** succeeds in the email environment, the email and security staff must work to identify any malicious emails or attachments. This may involve access to end users' email accounts, which requires caution not to accidentally intrude upon the users' privacy by reading legitimate email with sensitive data.

Exploit
A generic label for a cyber security attack, this is used as both a noun and a verb. Criminal hackers attempt to exploit computers and users. Viruses and other malware are called exploits, along with other types of attacks.

5.4 Protection Against Viruses and Other Malware

Malware (including viruses, worms, spyware, ransomware, and Trojan horses) are software exploits that take advantage of the computer's ability to shield the user from its activities. This is a design choice that makes computing accessible and simplifies the user experience, but it also gives the malware attacker the freedom to use computer resources unnoticed.

Malware design determines the method by which it spreads and how it uses the computer's resources, but the intention is the same in most instances, that is, to benefit from the infected environment. The method ranges from extortion of money, such as with ransomware, to the exfiltration of sensitive data with spyware. Some malware is designed to require an internet connection for proper functionality, but those that deny services or data may not require more than an internal network connection once they have infected a vulnerable computer.

Malware protection begins with a secure configuration of the computer and network equipment. Installing updates for the operating system and third-party software makes a significant improvement in safety, as does working with a regular user account whenever possible. Additional (and somewhat more technically demanding) actions are to configure network equipment to allow only necessary connectivity, as well as changing default passwords for network devices.

Virus scanners, as their name suggests, are an effective way to prevent malware infection by monitoring every file access and regularly checking all existing files for infection. Virus scanners use pre-defined malware code snippets to determine if a file or transmission has characteristics of known malicious software. Virus scanners require continuous updates to keep up with newly discovered malware, and they must be running any time the computer is on. All major vendors have integrated an automatic, web-based update function into their products as standard, so that the user needs to do little after the initial setup. Updates work on subscription methods, so there is often an annual fee associated with updates. Not all malware is known by the vendors of virus scanner software or can be protected against with fully updated software. Fortunately, user behaviors as listed in the email protection section of this course book are effective prevention against the entry of unfamiliar malware into the organization.

5.5 Protection Against Social Engineering Attacks

Social engineering is a security attack based around deception and persuasion. It uses the predictability of human interaction to influence the victim. The attacker's goal is to gather information or inspire actions that benefit themselves. While these attacks depend upon communication, they do not have to be carried out in person. Social engineering can be effective remotely, provided the victim is convinced that the attacker is acting in good faith. Common methods of social engineering are gaining entry through deception and phishing.

Gaining entry through deception is an in-person attack that takes advantage of the human tendency to assist other people in distress. By posing as someone in need of assistance, e.g., a new employee without a badge, or a delivery person who cannot locate their customer, the attacker persuades the victim to allow entry to restricted areas. Once the attacker is inside the protected area, they may go unchallenged by others who assume someone else authorized their entry. This allows free range as long as justified by the excuse for entry, perhaps only a few minutes for a delivery, but longer if one can skillfully pretend to be a new employee without drawing much attention. The attacker can choose from a variety of physical attacks during their time in the restricted area; theft of technology or information, shoulder surfing, planting wireless devices on the network, and installing microphones in offices are all possible after achieving unsupervised access.

Phishing is a remote social engineering attack with the aim of gathering sensitive information. Specialized forms of phishing take advantage of different technical methods, e.g., **vishing** for phone conversations and smishing for text messages (SMS), but they all aim to collect data that aid an attack. As with gaining entry, phishing uses the human tendency toward emotional reaction in response to distress. The content of attack varies based upon the target. Common scenarios are sending emails that threaten access to finances if action is not immediate; for instance, a personal bank account will be closed if no response is received within 24 hours. Other phishing attacks appeal to charitable impulses, often taking advantage of tragic, newsworthy events such as natural disasters, such as asking the victim to provide donations for aid to people displaced in the events. These examples are direct in their attack, asking outright for financial details.

Vishing
Variant phishing attacks may take their name through the delivery method, such as voice attacks through the phone (vishing) or text message (smishing).

Both of types of social engineering can be executed more subtly than in the above examples. The attacker may engage in long-term data gathering, leveraging each incremental gain in information. If the target is the password of a company's chief executive officer (CEO), the attacker may not wish to outright request it. Instead, they may gather sufficient intelligence to pose as a member of the CEO's administrative staff, asking for assistance during a crisis caused by the CEO's absence. This type of attack requires well-rounded knowledge about many parts of the organization, not limited to the IT helpdesk, the CEO, and the CEO's administrative staff. However, this work may be well worth the effort if the reward is access to information normally only possessed by the CEO.

As social engineering takes advantage of human nature, there are few technology solutions. Instead, protections against social engineering should focus on security awareness and reporting. The following information should be included in any security awareness training:

- Escort anyone without an entry badge to the check-in desk or security guard. If there is no one in a similar role, ask who they are visiting. Even if the visit is authorized, escort the visitor to their contact.

- Do not provide internal or sensitive information when requested by an unsolicited contact. Verify the identity and affiliation of the requester. Even better, refuse to engage. Instead, initiate the transaction yourself, using an independent source for the method (such as a published helpdesk number or physical address).
- Do not use email to transmit sensitive information, and do not follow links in emails that request sensitive information.
- Use multi-factor authentication wherever it is offered. This prevents third parties from accessing your accounts if they do not also possess the second authenticator.
- Check to ensure that uniform resource locators (URLs) are legitimate. Search for the correct web site, ensure that the address begins with “https,” and look for the padlock in the address bar indicating that information is transmitted securely.

SUMMARY

Security has many different aspects reflected in our everyday lives. Although IT and information security personnel deal with complex security concepts, the front-line user activities in security have the best chance of allowing a compromise to take place. Cyber security is greatly enhanced when all of an organization’s personnel are familiar with their security responsibility.

An objectively strong password consists of a minimum length and varied characters. The administrator of a computer or and application is responsible for ensuring that minimum security requirements are enforced on user-chosen passwords. Users are responsible for managing their passwords securely, remembering them, and for keeping the passwords confidential.

Data backups should be executed based on the criticality and amount to be stored. Most enterprise data backups should be performed in a schedule of both comprehensive full-data backups and incremental change backups. Critical enterprise-level data can be “mirrored” so that every change is immediately written to a perfect copy.

Email security is mostly the responsibility of the IT department or cyber security department, but users can behave in helpful ways. User behavior is critical in the fight against malware delivered through email. Constructive behaviors require that the email recipients think about any unexpected email attachments, links from external sources, and other suspicious characteristics.

Viruses and pests can be controlled, though not completely eradicated, with actively updated malware protection and fully patched computer systems. Zero-day attacks include malware, and virus scanners do not protect against malicious software that it cannot detect. Social engineering is the use of common human responses to manipulate a situation.

Social engineering attacks often focus on gaining entry to restricted areas. Another common social engineering attack is the use of emotional reaction to gather information, such as taking advantage of goodwill or anger.

UNIT 6

NETWORK AND COMMUNICATION SECURITY

STUDY GOALS

On completion of this unit, you will have learned …

- the definition of a firewall and its use.
- what decisions are made when separating networks.
- which types of networks are available to an organization.
- what security technology is available to protect wide-area and mobile networks.

6. NETWORK AND COMMUNICATION SECURITY

Introduction

Encryption protects data at rest and in transit, but an organization must protect its infrastructure along with the traffic that flows through it. Firewalls are security devices that enforces choices about which network connections to accept, deny, disregard (drop), or limit. They may be either network-hosted or host-based; either model executes the same function of limiting network connections, and either firewall is usually an application deployed on an information system. The network-based firewall does not typically share its host with any other application, whereas the host-based firewall is not the main function of the hosting system. It serves to protect the main function.

There is no absolute standard for configuration of a firewall; it must be aligned with the policies and goals of the organization. Updates are also common—as threats on the internet change, the configuration of a firewall may change to defend against new attacks. If possible, organizational security policies should require that firewalls block all traffic that is not necessary. This makes it easier to follow standardized configurations. It also prevents a constant scramble to adjust firewalls based on new threats.

6.1 Firewall Technology

At its most basic, a firewall is a communication monitor for network traffic. It determines whether communication is allowed between two points. Like a router, it is an independent device that separates the traffic from the networks or network segments that it monitors. A firewall offers protection against unauthorized data transmission by analyzing each incoming and outgoing packet and (according to predefined rules) forwarding the packet or preventing it from being forwarded.

A firewall controls the data traffic at particularly critical points in or between networks. This is sometimes within a subdivision of a single internal network, such as between production and development environments. The most crucial point to deploy a firewall is between the internet and an internal network. For example, a firewall should always be in place between the organization's corporate workstations and the internet. Otherwise, internal networks and systems would be continuously and directly attacked.

The most advanced firewalls can assign each incoming and outgoing packet to a data stream, verify the application protocol, and determine both the sender and the recipient beyond any doubt (Mishra, 2019). Those that do so can, if least privilege is applied in their configuration, provide very effective protection. Firewalls may also have the ability to decrypt TLS/SSL connections if provided with the correct encryption secrets. This provides a layer of data loss prevention, allowing the organization to determine if illicit traffic is being sent outside of their network boundaries. However, this functionality of a firewall may lead to difficulties since it breaks any possible end-to-end encryption.

Stateless Firewall

The most basic network firewall is the stateless firewall. Stateless firewalls ignore sessions, i.e., ongoing conversations. Each packet is measured solely against the rules configured in the firewall. While this is a simple firewall to understand, it does not work well with modern architectures that allow dynamic port assignment.

The main reason to avoid stateless firewalls is inflexibility. Statelessness refers to the inability to assign packets to an established communication session (Mishra, 2019). For instance, a user from inside a corporate network may wish to browse a web site. In order for the users to do so, they must be able to send and receive packets in exchange with the web server. Every port, internet protocol (IP) address, and protocol must align with the firewall rules. The stateless firewall must be configured to allow all potential web traffic in that connection, whether it includes changing port numbers or protocols, or even redirection. On an enterprise scale, configuration of least necessary access on a stateless firewall becomes extremely challenging (Mishra, 2019).

Stateful Firewall

Stateful firewalls, though more processing-intensive, provide greater security for the organization and a better administrative experience. A firewall is stateful when it can retain information about the communication sessions it allows. If the initial communication passes the firewall requirements, the response and ongoing exchange will be allowed to continue. Once allowed, the session does not need to be explicitly allowed with both incoming and outgoing rules for each point of communication. The administrator can create a smaller number of specific firewall rules without concern that communication will be too narrow to support the intended experience. The maintenance of rules is significantly reduced. Additionally, the stateful firewall supports more secure communication, requiring fewer accommodations for incoming traffic to the internal network.

6.2 Network Separation

An organization’s private networks are collectively referred to as “the intranet.” However, the intranet is usually made up of several different, potentially interconnected networks. These networks should be separated from the Internet by at least one firewall, and they are usually separated from each other by network devices and firewalls as well. Corporate networks host the business transactions and the workers’ functions that make the enterprise run. Production networks host the processing for an enterprise’s money-making critical functions. Development networks are usually present for developing and testing new applications before they are deployed into production networks. Demilitarized zones

(DMZs) are networks that host intranet systems that must be exposed to the internet, such as a web server. Therefore, a DMZ is connected to both the main intranet and the internet, and protected with firewalls at either end.

Common network separation points where the intranet is split into subnets thus are the DMZ separation from all other networks, production information technology (IT) from development, and corporate workstations from IT development and production. In large organizations, there may be additional separation points, such as vendor networks, IT laboratories, or IT administrative networks.

Why Separate Networks?

Separating networks provides security and operational advantages. Each network will carry less traffic, and connections between networks can be limited to only that absolutely required. Fewer users and workstations may have access to each network. In some cases, servers and workstations may be almost entirely inaccessible from the internet. Network separation is also called network segregation or subnetting.

Security advantages of separated networks

Lateral movement
An intruder who can create or access a machine inside the target network will often begin attacking computers on that same network. When these attacks successfully allow access to new systems, it is called lateral movement.

Separating networks allows less traffic on each network, as there are fewer computers communicating. A primary security benefit is therefore the lower amount of traffic that can be eavesdropped upon as it passes through the network. It also allows less opportunity for **lateral movement**, as there is a smaller number of targets once an intruder has gained network access (MITRE, 2019). The lower amount of network traffic equates to fewer unrelated log entries to review in the event of a network-related security incident. Smaller networks also mean fewer access rules per firewall. Each additional access rule is a potential route for malicious traffic between networks. By separating networks into smaller subnetworks, the number of computers at risk due to a lax or misconfigured firewall rule is lowered (MITRE, 2020).

Operational advantages of separated networks

Broadcast traffic
This is network traffic that is sent to every accessible computer on the same network as the source.

The same effects of subnetting provide operational advantages along with the security improvements. **Broadcast traffic** travels only on its own subnet, and the lower amount of traffic frees network capacity for local traffic (Grimmick, 2021). As with the security advantage, smaller logs and fewer devices on the smaller network make troubleshooting network problems simpler.

6.3 Security in WLAN, Mobile Networks, Bluetooth, and NFC

When securing networks, the administrator must consider how it is extended by wireless technologies. Wireless local area networks (WLAN), mobile phone connectivity, and ranged communications between devices, such as Bluetooth and near-field communication (NFC), blur the formerly defined edges of the organization network. Some of these, such as WLANs, can be protected through organizational efforts. Other wireless networks, such as temporary mobile phone WiFi networks, are managed by end users without oversight from network administrators. The administrator should consider whether allowing user-owned mobile devices to connect to the corporate network is advisable and if they can be appropriately contained to protect the enterprise.

Wireless Local Area Networks (WLANs)

As with other networks, wireless LANs are vulnerable to attackers that can join the network and eavesdrop upon the traffic. An additional complication for wireless LANs is that machines joining the network do not require a space to plug in to the infrastructure. In fact, unauthorized users do not have to be on the same floor or in the same building as the organization. Attackers can connect wherever they can obtain a signal, and capturing traffic becomes trivial. This inability to police the systems physically necessitates an approach that implements network security through authentication of devices. Awareness of the media access control (MAC) address, which is a unique identifier of any computer on a network, can allow the WLAN to limit connectivity to only known and authorized machines (Cyber Security & Infrastructure Security Agency, 2020). Alternative requirements can be used instead, such as individual certificates assigned to each authorized computer, or requirements for user authentication in order for a connection to take place.

Along with device authentication, WLANs should ensure that unbroken encryption is applied to all transactions in its network. If an attacker should find a way to join the network in order to observe traffic, any information obtained will still be unusable unless encryption keys are also available to them. The use of modern encryption standards and secure handling of encryption keys are critical components of WLAN protection.

Mobile Networks

Unlike WLAN protection, mobile communication protection (as needed for cellular telephones) is outside of the hands of the users and administrators for devices. Newer standards, such as Long-Term Evolution (LTE) and 5G, provide greater security than the older Universal Mobile Telecommunications System (UMTS) communication standards. UMTS uses weak encryption, which allows interception and eavesdropping on user communications (Cichonski et al., 2017).

LTE provides **mutual authentication** between the mobile device and the network, ensuring both that the device is authorized and that the network is an expected connection point. This, coupled with better encryption than UMTS, enhances the privacy of the user's communication. However, LTE is subject to several compromise scenarios, including the ability for an attacker to force the LTE-capable device to downgrade its communication to UMTS.

Mutual authentication
Computers can be set to allow communications only with other devices that can prove their identity. Requirements that computers must provide this proof prior to further communication is mutual authentication.

Outside of the forced downgrade, LTE traffic may be jammed or intercepted by an attacker. Fortunately, jamming attacks require physical access or specific hardware to enact. Interception attacks are more easily pursued, but alerts or mitigation of these attacks are available to the carrier. The security value of LTE is a significant improvement on UMTS, and users should ensure that their connection is LTE prior to transmitting sensitive information via a mobile connection (Cichonski et al., 2017).

Bluetooth

Bluetooth security implementation is also largely outside the control of the device user or the enterprise administrator. Vulnerability management consists of choosing a device that has reliable security built in. Part of the choice to manage Bluetooth security is in determining the software version. When possible, limit Bluetooth device purchases to the newest version. At the time of writing, this means those with version 5.0 or above.

Bluetooth accessories require a short-distance wireless connection with the system, and establishing this connection is called pairing. An additional security control is often available within the pairing requirements for a Bluetooth device. Options range from automatic pairing to any nearby device with Bluetooth enabled to mutual authentication in which the user takes part. For example, a pairing action may require that the computer, car, mobile phone, or other system display or announce a numeric personal identification number (PIN). That PIN is then entered by the user into the Bluetooth accessory. Without the human in the middle, with access to both devices, the connection does not take place. Without appropriate security, Bluetooth connections are prey to the vulnerabilities listed for WLANs. Devices may be connected without proper authorization, or unencrypted information sent through authorized connections may be subject to eavesdropping or interference (Bartock et al., n.d.).

Near Field Communication (NFC)

Near field communication (NFC) is a very short-range form of data transmission that relies upon radio frequency waves to connect the communicating devices. NFC is available in many of the same devices as Bluetooth connectivity, but it can also be found in non-technical constructs such as credit cards. Contactless payment options for credit cards and mobile devices, such as smart watches, use NFC (NFC, n.d.-a).

Near field communication relies upon close proximity for data communication. This has a side-effect of preventing long-ranger eavesdropping attacks. Some implementations of NFC establish a secure, encrypted channel which foils eavesdropping and interception or data manipulation attempts. Again, similar to Bluetooth, the only security management available to the user of NFC technology is vendor choice (NFC, n.d.-b). Where possible, users of NFC should look for vendors that offer strong encryption and communication configurations that address known vulnerabilities in the technology.

SUMMARY

Communications security is provided by oversight and additional technology that is added to a network infrastructure. Networks are most secure when they are segmented into smaller groupings, and when there is security at each communication edge. Firewalls provide protection and are essential to network security, but they are not in themselves sufficient for all network concerns. Stateful and stateless firewalls each have advantages, but enterprises will find that stateful firewalls offer far better security and less demanding management.

Mobile technologies have significant security drawbacks. Most are subject to some form of interception, eavesdropping, or data manipulation. These issues are rarely within the control of the consumer or the organization administrators. When adding mobile connectivity to the enterprise, vendor considerations must include built-in security offerings.

UNIT 7

CYBER SECURITY IN THE DEVELOPMENT OF SOFTWARE SYSTEMS

STUDY GOALS

On completion of this unit, you will have learned …

- the definition of Common Criteria.
- what threats apply to application code development environments.
- which security challenges arise in application development.
- what resources are available to improve application code security.

7. CYBER SECURITY IN THE DEVELOPMENT OF SOFTWARE SYSTEMS

Introduction

Application security is key to protecting the organization, and one of the least understood by those who implement it. Security teams routinely implement configuration requirements for servers, commercially purchased software, and networks, and these configurations are easily tested. However, application developers may be untrained in security, and their delivery goals may not include information security as a quality measure.

Organizations reasonably prioritize the production environment, where sensitive data and systems live. They must also consider the protection of their development environment, to protect intellectual property, integrity of code, and the prevention of attacks based inside their own infrastructure. Development environments, such as production, should be provided to a standard merited by their sensitivity and the need for uninterrupted usage.

7.1 Protection of the Development Environment

The development environment, where application code is created and tested for functionality, may have fewer security controls in place than the production environment. This makes sense for efficiency and cost savings; why protect a network area that does not contain sensitive information and is not used to run business-critical systems? Is it safe to say that this environment has little or no value to an attacker?

Why Protect the Development Environment?

It seems logical to pose these questions. However, their underlying assumptions are doubtful. Many organizations find that developers move sensitive data into these environments in order to perform comprehensive and accurate software testing. Fewer organizations find that business-critical services are run from development, but customer sales demonstrations may take place in this arena.

Potential gain for an attacker doesn’t only lie with immediate access to sensitive data. Environments with less security are ideal bases from which to launch internal and external attacks. A poorly monitored development environment can be turned into a collection of externally controlled attack servers. Organizations that do not review outgoing network traffic from the development environment may be surprised when their servers are used to break into third parties or perform distributed denial of service (DDOS) attacks.

Application code itself also has value for the organization. If the code is considered valuable **intellectual property**, the sale of application code in development may be profitable. When code is not salable, it will still have value based on its distribution and targeted use. Attackers residing in the development environment may review the code for vulnerabilities that can be used after its release. They could also seek to insert malicious functionality that will be passed on to the organization's customers.

Intellectual property
This refers to original creations of a person or organization to which ownership rights can be applied. Computer code is considered intellectual property.

Security Hygiene for Development Environments

Basic computer **security hygiene** is crucial for all computers and networks, including development environments. An organization should determine the controls that are necessary to implement minimum acceptable baseline assurance measures. Technical security should include, without fail, network firewalls; least privilege for access; security, application, and system log monitoring; rigorous security patching for operating systems and software; and virus protection for each computer. Additional security measures can be chosen based upon the data that are resident in the environment and the uses they may have besides creation of application code.

Security hygiene
Computer security should be performed at a level of diligence appropriate to the criticality of the system function. Every information system should be subjected to a basic minimum of security.

7.2 Secure Development

Application security is another key component of organizational security. Vulnerabilities in applications have the potential to introduce enormous problems into the organization's environment, as they are often designed for internet exposure. Developer training does not routinely include secure programming techniques, which has led to the need for niche tools such as application firewalls that protect against exploitation of code insecurities. While the availability of these tools is helpful, it is important for every organization to educate its application creators about security practices and the critical code flaws that result from their absence.

OWASP and the Top Ten Application Security Vulnerabilities

The Open Web Application Security Project (OWASP) is an international, community-based organization dedicated to improvement of application security. It originally only considered web applications but now also works on the security of applications in general. OWASP provides advice and education on code security in order to encourage organizations and developers to improve the overall state of internet security (OWASP, n.d.-a).

The OWASP top ten list, last updated in 2021, consists of the following ten vulnerabilities that are often seen in web applications (Open Web Application Security Project, 2021):

- A1:2021—Broken Access Control: restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws so that they can have unauthorized functionality and/or data, such as access to other users' accounts and sensitive files, the ability to modify other users' data, or permission to change access rights.

- A2:2021—Cryptographic Failures: many web applications and APIs do not properly protect sensitive data such as financial, healthcare, and PII, applying cryptography either incorrectly or not at all. For example, they use algorithms and protocols that are weak or inadequate to the task, or weak keys. Attackers may steal or modify such weakly protected data to commit credit card fraud, identity theft, or other crimes. Without extra protection such as encryption at rest or in transit, sensitive data may be compromised and require special precautions when exchanged with the browser.

- A3:2021—Injection: injection flaws such as SQL, NoSQL, OS, and LDAP injection may occur when untrusted data is sent to an interpreter as part of a command or query. usually after passing on data from some user input field without verification. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. Cross-site scripting (XSS) attacks, where an attacker manages to cause malicious scripts to be executed on other clients visiting the same website, are now counted as a special case of injection attacks by OWASP.

- A4:2021—Insecure Design: even a perfect implementation of a web application will be insecure if it is not based on a secure design, for example leaving out important security controls. To achieve a secure design, tools such as threat modeling, secure design patterns and principles, and reference architectures should be used.

- A5:2021—Security Misconfiguration: security misconfiguration usually is a result of insecure default configurations, unnecessarily open ports or services, misconfigured HTTP headers, and verbose error messages containing sensitive information. All operating systems, frameworks, libraries, and applications must be securely configured, as well as patched and upgraded in a timely fashion.

- A6:2021—Vulnerable and Outdated Components: components such as libraries, frameworks, and other software modules run with the same privileges as the application itself. If a vulnerable or outdated component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

- A7:2021—Identification and Authentication Failures: application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws in order to assume other users' identities temporarily or permanently. Examples involve allowing weak passwords, permitting brute force or other automated attacks, and weak processes for forgotten passwords.

- A8:2021—Software and Data Integrity Failures: if software and data are transferred between environments, their integrity must be verified, e.g. using signatures. This applies e.g. to moving code along the CI/CD pipeline, downloading updates, or insecure **deserialization**.

Serialization and deserialization
Serialization is the process of converting objects into a linear (serial) format such as a text string.

- A9:2021—Security Logging and Monitoring Failures: insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, move on to additional systems, and tamper, extract, or destroy data. Most breach studies show that the time it takes to detect a breach is over 200 days, and they are typically detected by external parties rather than by internal processes or monitoring.

Deserialization is the process of converting such a linear format back into the object.

- A10:2021—Server-Side Request Forgery (SSRF): in SSRF, an insecure server is used to send HTTP requests to some system that the attacker cannot access directly. For example, the server is induced to connect to an external system and leak information such as login credentials to the attacker. Commonly, an SSRF attack can be performed if the server is trusted by a third system to send requests that contain an URL. In such a case, an attacker may try to modify the URL or some other part of the request, causing the recipient server (which may be the same as the original insecure server) to read or modify internal resources.

Types of Application Security Tools

Application security tools are gaining traction in development environments. These tools may be difficult to automate and their output difficult to understand, but it is even more difficult to thoroughly test an application's security manually. Application security tools may be classified as static application security testing (SAST) and dynamic application security testing (DAST). These two types of tools should both be incorporated into a code development program, as they work within two different paradigms in code review.

Static application security testing (SAST) tools are used early in the code lifecycle. As blocks of application code are completed, the SAST can be run against them. The SAST checks indications of vulnerability in the code itself. There is no need for the code to be deployed or running on an information system in order to get SAST feedback (Phadke, 2016).

Dynamic application security testing (DAST) tools are used when code has been deployed and is running in an environment, preferably first in the development environment. The DAST checks executes code with the intention of finding and exploiting security-related flaws. These tools are capable of testing without access to the application code itself, and they provide evidence of vulnerabilities by showing the output of the commands that were executed (Phadke, 2016).

7.3 Common Criteria

Common Criteria, formally referred to as "Common Criteria for Information Technology Security Evaluation," is an information security standard published by the International Standards Organization (ISO) as ISO/IEC 15408. All three sections of the standard are available to the public at no cost. Auditors can use the Common Criteria to standardize evaluations for security products. Entities that wish to provide assurance of that their security product meets specific qualifications can use the Common Criteria to define evaluation targets and protection profiles, i.e., the objectives and implementation, of their security (ISO, n.d.-q).

Content of Common Criteria

The Common Criteria is not a traditional security measurement standard; it does not provide a new set of control requirements. In contrast to security management standards such as ISO/IEC 27001, the common criteria address the security of products rather than a security management system. It provides the context in which the review of a security product takes place, as well as the criteria to be used in such a review. ISO/IEC 15408:2009 is separated into the following three sections, each of which is published as a single document:

1. ISO/IEC 15408-1 serves as an introduction to the standard. It provides an overview of the common criteria system and models protection profiles (PP). It also gives an overview of the evaluation process (ISO, n.d.-q).
2. ISO/IEC 15408-2 covers measurement for security functional components, defining different kinds of security functionality (such as “authentication” or “rollback”) and the relevant functional requirements of the target of evaluation (TOE). They provide the mechanism to defend against threats that are inherent in the technology (ISO, n.d.-r).
3. ISO/IEC 15408-3 covers measurement for security assurance components. When choosing security products, the consumer has an interest in the consistency and reliability of their performance. Common Criteria for security assurance measure the vendor’s compliance to their stated security measures for products. For this purpose, they define different Evaluation Assurance Levels (EAL) from EAL1 “functionally tested” to EAL7 “formally verified design and tested” (ISO, n.d.-s). Put more simply, part two defines what functionality security products may provide, and part three defines how well this functionality is implemented.

Criticism

Quality of Common Criteria measurement, much like other audits of security, is limited by the rigor of its implementation. The organization being measured sets the scope of the audit and the protection profile to which they are being measured. Therefore, there may be critical infrastructure, operations, or administration that are not in scope. Those items in scope will be measured to a standard set by the organization. When a customer considers a vendor’s security products, they should routinely examine the compliance with performance and assurance standards. Common Criteria is an appropriate standard by which to evaluate a potential vendor product’s security, but the customer must also review the **audit scope** to ensure it covers the applicable service to a depth that meets their level of security requirement.

Audit scope
When conducting a security audit, the scope indicates all objects and processes that are to be examined in the audit.

SUMMARY

Security requirements for the development environment diverge from other networks, as the protection profile is different. While development systems should not host sensitive data or run business-critical applications, the security owner of the environment cannot assume this is the case without auditing its contents. Concerns for the development environment should center around enforcement of security hygiene and network perimeter protection.

Security for code development is driven by the high likelihood that applications will be hosted in an internet-available format and therefore be subject to frequent attack. Injection and cross-site-scripting issues are common, and they are caused when the system accepts unsanitized, malicious input from a remote attacker. The consequences of cross-site-scripting are mostly borne by the system's other users.

Common Criteria is the name of an ISO standard that establishes audit criteria for vendors of security products. It helps establish and communicate needs for both the security functionality of the product and assurance of the vendor's security program. The drawback of Common Criteria is the ability for a vendor to set their own audit criteria and scope. In order to ensure the suitability of a product audited under Common Criteria, the consumer should review the coverage of the audit as well as the result.