The CIA Triad

Confidentiality: is a difficult balance to achieve when many system users are guests or customers, and it is not known if they are accessing the system from a compromised machine or vulnerable mobile application. So, the security professional's obligation is to regulate access—protect the data that needs protection, yet permit access to authorized individuals.
Personally Identifiable Information (PII) is a term related to the area of confidentiality. It pertains to any data about an individual that could be used to identify them. Other terms related to confidentiality are **protected health information (PHI)** , which is information regarding one's health status, and **classified or sensitive information**, which includes trade secrets, research, business plans and intellectual property.

Another useful definition is **sensitivity**, which is a measure of the importance assigned to information by its owner, or the purpose of denoting its need for protection. Sensitive information is information that if improperly disclosed (confidentiality) or modified (integrity) would harm an organization or individual. In many cases, sensitivity is related to the harm to external stakeholders; that is, people or organizations that may not be a part of the organization that processes or uses the information.

Integrity: measures the degree to which something is whole and complete, internally consistent and correct. The concept of integrity applies to:

information or data
systems and processes for business operations
organizations
people and their actions

Data integrity is the assurance that data has not been altered in an unauthorized manner. This requires the protection of the data in systems and during processing to ensure that it is free from improper modification, errors or loss of information and is recorded, used and maintained in a way that ensures its completeness. Data integrity covers data in storage, during processing and while in transit.

Information must be accurate, internally consistent and useful for a stated purpose. The internal consistency of information ensures that information is correct on all related systems so that it is displayed and stored in the same way on all systems. Consistency, as part of data integrity, requires that all instances of the data be identical in form, content and meaning.

System integrity refers to the maintenance of a known good configuration and expected operational function as the system processes the information. Ensuring integrity begins with an awareness of state, which is the current condition of the system. Specifically, this awareness concerns the ability to document and understand the state of data or a system at a certain point, creating a baseline. For example, a baseline can refer to the current state of the information—whether it is protected. Then, to preserve that state, the information must always continue to be protected through a transaction.

Going forward from that baseline, the integrity of the data or the system can always be ascertained by comparing the baseline with the current state. If the two match, then the integrity of the data or the system is intact; if the two do not match, then the integrity of the data or the system has been compromised. Integrity is a primary factor in the reliability of information and systems.

The need to safeguard information and system integrity may be dictated by laws and regulations. Often, it is dictated by the needs of the organization to access and use reliable, accurate information.

Availability: can be defined as (1) timely and reliable access to information and the ability to use it, and (2) for authorized users, timely and reliable access to data and information services.

The core concept of availability is that data is accessible to authorized users when and where it is needed and in the form and format required. This does not mean that data or systems are available 100% of the time. Instead, the systems and data meet the requirements of the business for timely and reliable access.

Some systems and data are far more critical than others, so the security professional must ensure that the appropriate levels of availability are provided. This requires consultation with the involved business to ensure that critical systems are identified and available. Availability is often associated with the term criticality, because it represents the importance an organization gives to data or an information system in performing its operations or achieving its mission.

CIA IN THE REAL WORLD

It's important to have a comprehensive approach to maintaining the CIA Triad: confidentiality, integrity, and availability. These are the foundations of the cybersecurity domain.

Confidentiality means that no private information has been disclosed to unauthorized individuals. We need to ensure that personally identifiable information, also known as PII, is protected. If you are part of a security team, your goal is to protect the assets or the information of large corporations or multiple individuals. For example, if you work in banking, health care or insurance companies, you have multiple personal identifiers to protect.

Integrity ensures that this information is not being corrupted or changed without the information owner's permission. It confirms that the information being maintained is complete and accurate and consistent with the legitimate use of that information.

Interfering with the integrity of information can have serious ramifications. For example, someone without authority changes someone's medical information, and now a patient may be in jeopardy because someone changed that vital information.

Our job is to maintain the security of that information so that no one, unless authorized to do so, changes any part of the information we are protecting.

Availability is critical because it is essential that authorized users have access to important information in a timely manner. Cyberattacks that disrupt services often target the availability of data. A business cannot function if its employees and customers cannot access their information in a timely manner. A ransomware attack, for example, may lock up a system and block access to vital information and services. That access will not be restored until a payment is made.

Authentication

When users have stated their identity, it is necessary to validate that they are the rightful owners of that identity. This process of verifying or proving the user's identification is known as **authentication**. Simply put, authentication is a process to prove the identity of the requestor.

There are three common methods of authentication:

Something you know: Passwords or paraphrases
Something you have: **Tokens**, memory cards, smart cards
Something you are: **Biometrics** , measurable characteristics

Methods of authentication

There are two types of authentication. Using only one of the methods of authentication stated previously is known as **single-factor authentication (SFA)** . Granting users access only after successfully demonstrating or displaying two or more of these methods is known as **multi-factor authentication (MFA)** .

Common best practice is to implement at least two of the three common techniques for authentication:

Knowledge-based
Token-based
Characteristic-based

Knowledge-based authentication uses a passphrase or secret code to differentiate between an authorized and unauthorized user. If you have selected a personal identification number (PIN), created a password or some other secret value that only you know, then you have experienced knowledge-based authentication. The problem with using this type of authentication alone is that it is often vulnerable to a variety of attacks. For example, the help desk might receive a call to reset a user's password. The challenge is ensuring that the password is reset only for the correct user and not someone else pretending to be that user. For better security, a second or third form of authentication that is based on a token or characteristic would be required prior to resetting the password. The combined use of a user ID and a password consists of two things that are known, and because it does not meet the requirement of using two or more of the authentication methods stated, it is not considered MFA.

Non-repudiation: The inability to deny taking an action, such as sending an email message. It is a legal term and is defined as the protection against an individual falsely denying having performed a particular action. It provides the capability to determine whether a given individual took a particular action, such as created information, approved information or sent or received a message.

In today's world of e-commerce and electronic transactions, there are opportunities for the impersonation of others or denial of an action, such as making a purchase online and later denying

it. It is important that all participants trust online transactions. Non-repudiation methodologies ensure that people are held responsible for transactions they conducted.

Proving Identity: Let us explore authentication a little more. Many of us are already accustomed to different ways of proving who we are, and we do it perhaps without even knowing it. Usually, we are asked to authenticate our identities by using something that we know, such as a password or passphrase.

That is one factor of authentication. Then we use something that only we have, such as a token or card. That gives us two different factors of authentication. When you go to the bank and use your ATM card, you may have a username and password or a specific code, such as a PIN. You HAVE the card, and you KNOW the PIN. So that is one form of multifactor authentication. Someone with just the card cannot access the money.

Then, increasingly, we also provide something that we are, with biometrics. This can be a fingerprint or another type of measurable characteristic, such as facial recognition or an iris scan. We see these elements of the authentication process on a daily basis. This adds another layer of multi-factor authentication.

Privacy

Privacy is the right of an individual to control the distribution of information about themselves. While security and privacy both focus on the protection of personal and sensitive data, there is a difference between them. With the increasing rate at which data is collected and digitally stored across all industries, the push for privacy legislation and compliance with existing policies steadily grows. In today's global economy, privacy legislation and regulations on privacy and data protection can impact corporations and industries regardless of physical location. Global privacy is an especially crucial issue when considering requirements regarding the collection and security of personal information. There are several laws that define privacy and data protection, which periodically change. Ensuring that protective security measures are in place is not enough to meet privacy regulations or to protect a company from incurring penalties or fines from mishandling, misuse, or improper protection of personal or private information. An example of a law with multinational implications is the European Union's **General Data Protection Regulation (GDPR)** which applies to all organizations, foreign or domestic, doing business in the EU or any persons in the EU. Companies operating or doing business within the United States may also fall under several state legislations that regulate the collection and use of consumer data and privacy. Likewise, member nations of the EU enact laws to put GDPR into practice and sometimes add more stringent requirements. These laws, including national- and state-level laws, dictate that any entity anywhere in the world handling the private data of people in a particular legal jurisdiction must abide by its privacy requirements. As a member of an organization's data protection team,

you will not be required to interpret these laws, but you will need an understanding of how they apply to your organization.

Privacy in the work environment

Privacy is a major component of information security. Once we know how private the information is, we know what appropriate controls can be implemented. A number of standards, policies and procedures govern privacy in the working environment, and these vary by geographic region. In the United States, HIPAA, the Health Insurance Portability and Accountability Act, controls how the privacy of medical information must be maintained. In the European Union (EU), the General Data Protection Regulation gives anyone within the borders of the EU control over what personal information companies can compile and retain about them. As a security professional, it's important to be aware of privacy laws and regulations in all jurisdictions where your company conducts business. When doing business in other countries, we must be aware of their privacy standards and regulations and act accordingly.

Protecting Information

Sometimes, a collection of data might be considered PII, while the distinct data elements, each by itself, would not. For example, a date of birth alone can be shared by many individuals and is not considered PII. However, when combined with a name or other piece of information, it would significantly narrow the possibility of association with more individuals.

Cybersecurity professionals take on the obligation of protecting many kinds of organizational data and personal information. We all have PII, and it needs to be protected. The three elements of the CIA Triad play out in our everyday lives. The next time you go to your physician, open your email or check the balance of your checking account, think about how the people who are entrusted to protect it accomplish this responsibility. It is a different way of thinking, and one you will develop as you progress in your cybersecurity career.

Understand the risk management process

Risks and security-related issues represent an ongoing concern of businesses as well as the field of cybersecurity, but far too often organizations fail to proactively manage risk. Assessing and analyzing risk should be a continuous and comprehensive exercise in any organization. As a member of an organization's security team, you will work through risk assessment, analysis, mitigation, remediation and communication. There are many frameworks and models used to facilitate the risk managementprocess, and each organization makes its own determination of what constitutes risk and the level of risk it is willing to accept. However, there are commonalities among the terms, concepts and skills needed to measure and manage risk. This module gets you started by presenting foundational terminology and introducing you to the risk management process. First, a definition of risk is a measure of the extent to which an entity is threatened by a potential circumstance or event. It is often expressed as a combination of:

1. the adverse impacts that would arise if the circumstance or event occurs, and
2. the likelihood of occurrence.

Information security risk reflects the potential adverse impacts that result from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems. This definition represents that risk is associated with threats, impact and likelihood, and it also indicates that IT risk is a subset of business risk.

Introduction to risk management

Information assurance and cybersecurity are greatly involved with the risk management process.

The level of cybersecurity required depends on the level of risk the entity is willing to accept; that is, the potential consequences of what's going on in our environment. Once we evaluate this risk, then we will implement security controls to mitigate the risk to the level that we find acceptable.

Risks can be from cyberattacks, such as malware, social engineering, or denial-of-service attacks, or from other situations that affect our environment, such as fire, violent crime, or natural disasters. With well-designed risk management technologies, we can recognize vulnerabilities and threats, and calculate the likelihood and the potential impact of each threat.

Importance of risk management

What do we mean when we say threats and vulnerabilities? A vulnerability is a gap or weakness in an organization’s protection of its valuable assets, including information. A threat is something or someone that aims to exploit a vulnerability to gain unauthorized access.

By exploiting a vulnerability, the threat can harm an asset. For example, a natural disaster, such as a major storm, poses a threat to the utility power supply, which is vulnerable to flooding. The IT environment where production takes place is an asset. If the utility power supply is cut off by a storm, the asset might be made unavailable, because the IT components won’t work without power. Our job is to evaluate how likely it is that an event will take place and take appropriate actions to mitigate the risk.

Risk management terminology

Security professionals use their knowledge and skills to examine operational risk management, determine how to use risk data effectively, work cross-functionally and report actionable information and findings to the stakeholders concerned. Terms such as threats, vulnerabilities and assets are familiar to most cybersecurity professionals.

> An asset is something in need of protection.

A vulnerability is a gap or weakness in those protection efforts.
A threat is something or someone that aims to exploit a vulnerability to thwart protection efforts.

Risk is the intersection of these terms. Let's look at them more closely.

Threats

A threat is a person or thing that takes action to exploit (or make use of) a target organization’s system vulnerabilities, as part of achieving or furthering its goal or objectives. To better understand threats, consider the following scenario: Tourists are popular targets for pickpockets. The existence of pickpockets in a crowded tourist spot is a threat to the people gathered there. That threat applies to everyone in the vicinity, even other pickpockets. If you are in the vicinity and the pickpocket has identified you as a target, you are facing a threat actor whether you know it or not.

The approach and technique taken by the pickpocket is their threat vector.

In the context of cybersecurity, typical **threat actors** include the following:

Insiders (either deliberately, by simple human error, or by gross incompetence).
Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
Formal entities that are nonpolitical (such as business competitors and cybercriminals).
Formal entities that are political (such as terrorists, nation-states, and hacktivists).
Intelligence or information gatherers (could be any of the above).
Technology (such as free-running **bots** and **artificial intelligence** , which could be part of any of the above).

*****Threat Vector:*** *The means by which a threat actor carries out their objectives.*

Vulnerabilities

A **vulnerability** is an inherent weakness or flaw in a system or component, which, if triggered or acted upon, could cause a risk event to occur. Consider the pickpocket scenario from below.

An organization's security team strives to decrease its vulnerability. To do so, they view their organization with the eyes of the threat actor, asking themselves, "Why would we be an attractive target?" The answers might provide steps to take that will discourage threat actors, cause them to look elsewhere or simply make it more difficult to launch an attack successfully. For example, to protect yourself from the pickpocket, you could carry your wallet in an inside pocket instead of the back pant pocket or behave alertly instead of ignoring your surroundings. Managing vulnerabilities starts with one simple step: Learn what they are.

Let's say the pick pocket chooses you as a target because they see that it will be easier or more profitable to steal from you. Maybe you are distracted, have jewelry that is easy to snatch, or appear weak and less likely to put up a struggle. In other words, you appear more vulnerable than the other tourists and the pick pocket feels that they can exploit that vulnerability or weakness.

Likelihood

When determining an organization's vulnerabilities, the security team will consider the **probability**, or **likelihood** , of a potential vulnerability being exploited within the construct of the organization's threat environment. **Likelihood of occurrence** is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.

Finally, the security team will consider the likely results if a threat is realized and an event occurs. **Impact** is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Think about the impact and the chain of reaction that can result when an event occurs by revisiting the pickpocket scenario: How do the pickpocket's actions affect your ability to continue your journey? If you appear to be a weak

target and the pickpocket chooses to take your money by brute force, will you be able to obtain more cash to complete your vacation or even return home? The downstream impact must also be considered. What if you are injured and require medical treatment or even hospitalization? Impact does not often stop with the incident itself.

Risk identification

How do you identify risks? Do you walk down the street watching out for traffic and looking for puddles on the ground? Maybe you've noticed loose wires at your desk or water on the office floor? If you're already on the lookout for risks, you'll fit with other security professionals who know it's necessary to dig deeper to find possible problems.

In the world of cyber, identifying risks is not a one-and-done activity. It's a recurring process of identifying different possible risks, characterizing them and then estimating their potential for disrupting the organization.

It involves looking at your unique company and analyzing its unique situation. Security professionals know their organization's strategic, tactical and operational plans.

Takeaways to remember about risk identification:

Identify risk to communicate it clearly.
Employees at all levels of the organization are responsible for identifying risk.
Identify risk to protect against it.

As a security professional, you are likely to assist in risk assessment at a system level, focusing on process, control, monitoring or incident response and recovery activities. If you're working with a smaller organization, or one that lacks any kind of risk management and mitigation plan and program, you might have the opportunity to help fill that planning void.

Risk assessment

Risk assessment is defined as the process of identifying, estimating and prioritizing risks to an organization's operations (including its mission,

functions, image and reputation), assets, individuals, other organizations and even the nation. Risk assessment should result in aligning (or associating) each identified risk resulting from the operation of an information system with the goals, objectives, assets or processes that the organization uses, which in turn aligns with or directly supports achieving the organization's goals and objectives.

A common risk assessment activity identifies the risk of fire to a building. While there are many ways to mitigate that risk, the primary goal of a risk assessment is to estimate and prioritize. For example, fire alarms are the lowest cost and can alert personnel to evacuate and reduce the risk of personal injury, but they won't keep a fire from spreading or causing more damage. Sprinkler systems won't prevent a fire but can minimize the amount of damage done. However, while sprinklers in a data center limit the fire's spread, it is likely they will destroy all the systems and data on them. A gas-based system may be the best solution to protect the systems, but it might be cost-prohibitive. A risk assessment can prioritize these items for management to determine the method of mitigation that best suits the assets being protected.

The result of the risk assessment process is often documented as a report or presentation given to management for their use in prioritizing the identified risk(s). This report is provided to management for review and approval. In some cases, management may indicate a need for a more in-depth or detailed risk assessment performed by internal or external resources.

Risk treatment

Risk treatment relates to making decisions about the best actions to take regarding the identified and prioritized risk. The decisions made are dependent on the attitude of management toward risk and the availability — and cost — of risk mitigation. The options commonly used to respond to risk are:

1. Risk avoidance is the decision to attempt to eliminate the risk entirely. This could include ceasing operation for some or all of the activities of the organization that are exposed to a particular risk. Organization leadership may choose risk avoidance when the potential impact of a given risk is too high or if the likelihood of the risk being realized is simply too great.

2. Risk acceptance is taking no action to reduce the likelihood of a risk occurring. Management may opt for conducting the business function that is associated with the risk without any further action on the part of the organization, either because the impact or likelihood of occurrence is negligible, or because the benefit is more than enough to offset that risk.
3. Risk mitigation is the most common type of risk management and includes taking actions to prevent or reduce the possibility of a risk event or its impact. Mitigation can involve remediation measures, or controls, such as security controls, establishing policies, procedures, and standards to minimize adverse risk. Risk cannot always be mitigated, but mitigations such as safety measures should always be in place.
4. Risk transference is the practice of passing the risk to another party, who will accept the financial impact of the harm resulting from a risk being realized in exchange for payment. Typically, this is an insurance policy.

Risk management process

As we mentioned before, an asset is something that we need to protect. It can be information, or it can be an actual physical piece of equipment, such as a rack in the server room or a computer or tablet or even a phone. A vulnerability is a weakness in the system. It can be due to lack of knowledge, or possibly outdated software. For example, perhaps we don't have a current operating system, or our awareness training is lacking. A threat is something or someone that could cause harm once they learn that we have a weakness. For example, if we have a back door open, either logically, in our website, or even physically in the back office, someone can exploit that weakness and take advantage of that gap in our defenses to access information.

The likelihood or the probability of that happening depends on the overall environment. In an environment that's extremely secure, such as a data center or a bank, the likelihood that someone can come in and rob the bank is very low. Whether they are seeking access through a web browser, or physically into the actual bank, their likelihood of success is not high because security is very strong.

In other situations, where we have fewer levels of security, the likelihood that the environment can be compromised is much higher. In our daily accounts, we often only have one username and a password and that is the extent of our defenses. Anyone who obtains that username and password can gain access; therefore, the likelihood that this environment can be compromised is very high.

As a first step in the risk management process, organizations need to figure out how much risk they are willing to take. This is called a risk appetite or risk tolerance. For a very trivial example, if you are a big fan of football or a particular TV program, you will have a low tolerance for having a power outage during a big game or your favorite program. You also need to have power when you are trying to access important documents or sites for your

business, so your risk appetite depends on how important that asset is. If your data is extremely sensitive, you will naturally be extremely averse to having any risk of a breach. To mitigate the risk, one option is to hire another company with the expertise to help you maintain the security of your environment. This will help reduce the risk. You would also consider implementing some security controls, which we will explore shortly.

If we don't have the competence or the means to protect sensitive information, sometimes we need to avoid the risk. This means removing ourselves from a situation that can result in problems and refraining from initiating risky activities until we achieve a certain level of comfort with our security. We can also share or transfer the risk by obtaining cybersecurity insurance, so the insurance company assumes the risk. While it is nearly impossible to remove all risk, once we have done enough to reduce or transfer the risk, and we are comfortable with the situation, then we can accept the level of risk that remains.

Risk in our lives

On a personal level, one example of a threat and its impact is unauthorized charges on your credit card. It’s a good idea not to store your credit information in your phone or on your web browser, even though that is convenient for online shopping. Most banks won’t charge you for unauthorized purchases, but it may result in your account being frozen when you are trying to use it, or the hassle of replacing a card that has been compromised and updating any subscriptions or bills that were paid directly with that card. If you identify a risk beforehand, you can mitigate it by adding layers of security, such as multifactor authorization. Most bank websites either require or at least encourage you to set up multifactor authentication when you access your account, so you need a username and password and also a code sent to your email or your cellphone.

Another example of handling risk is when you book a vacation. For example, you might be considering a Caribbean cruise where the weather can be a factor and your trip could be cancelled. In that case, you purchase travel insurance to transfer the risk, so you don’t lose out on your prepaid expenses and deposits if something happens to prevent the trip.

Other types of insurance are also ways to transfer risk. You might purchase additional health care coverage, to cover your expenses if you have an accident. If you are concerned about identity theft, there are companies that offer an insurance policy for managing your identity. These companies are involved in their own form of financial risk management, calculating that your premium payments or subscription payments will exceed the payouts they will have to make in the event of a claim.

Risk priorities

When risks have been identified, it is time to prioritize and analyze core risks through **qualitative risk analysis** and/or **quantitative risk analysis**. This is necessary to determine root cause and narrow down apparent risks and core

risks. Security professionals work with their teams to conduct both qualitative and quantitative analysis. Understanding the organization's overall mission and the functions that support the mission helps to place risks in context, determine the root causes and prioritize the assessment and analysis of these items. In most cases, management will provide direction for using the findings of the risk assessment to determine a prioritized set of risk-response actions.

One effective method to prioritize risk is to use a risk matrix, which helps identify priority as the intersection of likelihood of occurrence and impact. It also gives the team a common language to use with management when determining the final priorities. For example, a low likelihood and a low impact might result in a low priority, while an incident with a high likelihood and high impact will result in a high priority. Assignment of priority may relate to business priorities, the cost of mitigating a risk or the potential for loss if an incident occurs.

Decision making based on risk priorities

When making decisions based on risk priorities, organizations must evaluate the likelihood and impact of the risk as well as their tolerance for different sorts of risk. A company in Hawaii is more concerned about the risk of volcanic eruptions than a company in Chicago, but the Chicago company will have to plan for blizzards. In those cases, determining risk tolerance is up to the executive management and board of directors. If a company chooses to ignore or accept risk, exposing workers to asbestos, for example, it puts the company in a position of tremendous liability.

Risk tolerance

The perception management takes toward risk is often likened to the entity's appetite for risk. How much risk are they willing to take? Does management welcome risk or want to avoid it? The level of **risk tolerance** varies across organizations, and even internally: Different departments may have different attitudes toward what is acceptable or unacceptable risk. Understanding the organization and senior management's attitude toward risk is usually the starting point for getting management to take action regarding risks.Executive management and/or the Board of Directors determines what is an acceptable level of risk for the organization. Security professionals aim to maintain the levels of risk within management's

limit of risk tolerance. Often, risk tolerance is dictated by geographic location. For example, companies in Iceland plan for the risks that nearby volcanoes impose on their business. Companies that are outside the projected path of a lava flow will be at a lower risk than those directly in the path's flow. Similarly, the likelihood of a power outage affecting the data center is a real threat in all areas of the world. In areas where thunderstorms are common, power outages may occur more than once a month, while other areas may only experience one or two power outages annually. Calculating the downtime that is likely to occur with varying lengths of downtime will help to define a company's risk tolerance. If a company has a low tolerance of the risk of downtime, they are more likely to invest in a generator to power critical systems. A company with an even lower tolerance for downtime will invest in multiple generators with multiple fuel sources to provide a higher level of assurance that the power will not fail.

Risk tolerance drives decision making

Here are a few examples of how risk tolerance can drive decision making for organizations.

• An organization is required to build a bid package to gain a contract. The time and effort of personnel building a bid package will cost the organization $10,000 USD. If the organization wins the contract, the contract pays $2,000,000 USD. The organization decides to accept the risk of losing the cost of the bid package, because the benefit of winning the contract is appealing. The risk of losing the bid (and the cost of building the bid package) is within the organization's risk threshold.

• A trauma center has three critical-care units where patients are provided life- sustaining services (breathing and heart activity) through the use of machines. Inactivity of these machines could mean that people will die. The trauma center has zero tolerance for power failure, so creates redundant emergency power supplies, through the use of multiple utility power providers, battery backup, and multiple generators with secure fuel supplies and solid contracts with fuel providers to deliver additional fuel during emergency situations.

• Liza and Krith think they can build a business that is profitable and enjoyable; they decide to quit their jobs and start the business together. They tolerate the risk that their business might fail because the reward they perceive is significant.

Swimming with sharks (voices from the field) Podcast

Josh: Welcome to Dancing with Danger. A travel podcast about risk-loving people doing risky things. I'm Joshua Justin and today I'm talking with Sarah McMillan who runs the Swimming with Sharks attraction here in sunny Key West, Florida. Hi Sarah, how you doing today?

Sarah: It's a beautiful day to be swimming with sharks in Florida, Josh.
Josh: Some might disagree. Wouldn't you say this is a particularly risky thing to do? Downright

dangerous in fact.

the property. You are responsible for keeping track of your own belongings and your own kids and so on and so on. So people are quite used to accepting such conditions whenever they do just about anything. But we also have an insurance policy to handle any liability claims. This allows us to transfer our risk to another party. The insurance company is taking the gamble that our premiums and those of other businesses, will bring in more income than a potential claim would make them pay out.

Josh: So you've been in business here for a couple of years now.

Sarah: That's correct. About two years.
Josh: And in that time, have you had any liability claims?

Sarah: Not regarding the sharks. However, we did have a breach regarding our credit card information. That was a headache. Now we outsource our customer management system to a cloud based third party. So they assume the risk for cybersecurity. We discover that human sharks are a much bigger risk than marine sharks. The beach is safer than the breach, I guess you'd say.

Josh: I don't think I would, but thank you Sarah for taking the time to talk to our listeners today. I know we've learned a lot about shark related safety issues.

Sarah: You're welcome, Joshua. Thank you again for having me and let me know when you are ready to swim with the sharks.

Josh: That's all for today's Dancing with Danger episode. Tune into next week when we go bungee jumping with bears.

UNDERSTANDING SECURITY CONTROLS

What are security controls?

Security controls pertain to the physical, technical and administrative mechanisms that act as safeguards or counter measures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. The implementation of controls should reduce risk, hopefully to an acceptable level.

Physical control

Physical control address process-based security needs using physical hardware devices, such as badge readers, architectural features of buildings and facilities, and specific security actions to be taken by people. They typically provide ways of controlling, directing or preventing the movement of people and equipment throughout a specific physical location, such as an office suite, factory or other facility. Physical controls also provide protection and control over entry onto the land surrounding the buildings, parking lots or other areas that are within the

organization's control. In most situations, physical controls are supported by technical controls as a means of incorporating them into an overall security system. Visitors and guests accessing a workplace, for example, must often enter the facility through a designated entrance and exit, where they can be identified, their visit's purpose assessed, and then allowed or denied entry. Employees would enter, perhaps through other entrances, using company-issued badges or other tokens to assert their identity and gain access. These require technical controls to integrate the badge or token readers, the door release mechanisms and the identity management and access control systems into a more seamless security system.

Technical controls

Technical control (also called logical controls) are security controls that computer systems and networks directly implement. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations and support security requirements for applications and data. Technical controls can be configuration settings or parameters stored as data, managed through a software graphical user interface (GUI), or they can be hardware settings done with switches, jumper plugs or other means. However, the implementation of technical controls always requires significant operational considerations and should be consistent with the management of security within the organization. Many of these will be examined in more depth as we look at them in later sections in this chapter and in subsequent chapters.

Administrative controls

Administrative controls (also known as managerial controls) are directives, guidelines or advisories aimed at the people within the organization. They provide frameworks, constraints and standards for human behavior, and should cover the entire scope of the organization's activities and its interactions with external parties and stakeholders. It is vitally important to realize that administrative controls can and should be powerful, effective tools for achieving information security. Even the simplest security awareness policies can be an effective control, if you can help the organization fully implement them through systematic training and practice. Many organizations are improving their overall security posture by integrating their administrative controls into the task-level activities and operational decision processes that their workforce uses throughout the day. This can be done by providing them as in-context ready reference and advisory resources, or by linking them directly into training activities. These and other techniques bring the policies to a more neutral level and away from the decision-making of only the senior executives. It also makes them immediate, useful and operational on a daily and per-task basis.

Making connections

What sorts of activities can threaten the elements of the CIA Triad?

Consider a coworker sharing passwords. Perhaps Joe gives Joanne his password because he is home sick and needs Joanne to sign on to his work computer to get information he needs.

But later, Joanne is fired from her job. The employer cancels Joanne's credentials but isn't aware that Joanne also knows Joe's password. Joanne is disgruntled and decides to take revenge on her old company by using Joe's credentials to change or delete important files. Or in less hostile circumstances, improper use of the password could accidentally result in the introduction of unauthorized software that is riddled with malware.

Another example is the laptop of a remote worker being left unattended or unlocked in the worker's home. Children or other family members may decide to play games on the computer. They upload legal but contaminated software or files, leading to a corrupt workstation with compromised integrity.

The elements of the CIA Triad can also be compromised by ill-preparedness against acts of nature. For instance, a long-term power outage may lead to backup generators that run out of fuel or that suffer mechanical failures if not properly maintained.

As a final example, improper fire suppression methods can affect the CIA Triad by irreparably damaging or destroying both digital and analog information.

All these examples show that a comprehensive risk assessment of technical, human and environmental threats must be completed, then appropriate mitigation options must be put in place to protect the security and integrity of an organization's information.

Governance elements

Any business or organization exists to fulfill a purpose, whether it is to provide raw materials to an industry, manufacture equipment to build computer hardware, develop software applications, construct buildings or provide goods and services. To complete the objective requires that decisions are made, rules and practices are defined, and policies and procedures are in place to guide the organization in its pursuit of achieving its goals and mission.

When leaders and management implement the systems and structures that the organization will use to achieve its goals, they are guided by laws and regulations created by governments to enact public policy. Laws and regulations guide the development of standards, which cultivate policies, which result in procedures.

How are regulations, standards, policies and procedures related? It might help to look at the list in reverse.

Procedures are the detailed steps to complete a task that support departmental or organizational policies.

Policies are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulations.

Standards are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.

Regulations are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance.

Regulations and laws

Regulations and associated fines and penalties can be imposed by governments at the national, regional or local level. Because regulations and laws can be imposed and enforced differently in different parts of the world, here are a few examples to connect the concepts to actual regulations.

The **Health Insurance Portability and Accountability Act (HIPAA) of 1996** is an example of a law that governs the use of protected health information (PHI) in the United States. Violation of the HIPAA rule carries the possibility of fines and/or imprisonment for both individuals and companies.

The **General Data Protection Regulation (GDPR)** was enacted by the European Union (EU) to control use of Personally Identifiable Information (PII) of its citizens and those in the EU. It includes provisions that apply financial penalties to companies who handle data of EU citizens and those living in the EU even if the company does not have a physical presence in the EU, giving this regulation an international reach.

Finally, it is common to be subject to regulation on several levels. Multinational organizations are subject to regulations in more than one nation in addition to multiple regions and municipalities. Organizations need to consider the regulations that apply to their business at all levels—national, regional and local—and ensure they are compliant with the most restrictive regulation.

Standards

Organizations use multiple standards as part of their information systems security programs, both as compliance documents and as advisories or guidelines. Standards cover a broad range of issues and ideas and may provide assurance that an organization is operating with policies and procedures that support regulations and are widely accepted best practices.

The **International Organization for Standardization (ISO)** develops and publishes international standards on a variety of technical subjects, including information systems and information security, as well as encryption standards. ISO solicits input from the international community of experts to provide input on its standards prior to publishing. Documents outlining ISO standards may be purchased online.

The **National Institute of Standards and Technology (NIST)** is a United States government agency under the Department of Commerce and publishes a variety of technical standards in addition to information technology and information security standards. Many of the standards issued by NIST are requirements for U.S. government agencies and are considered recommended standards by industries worldwide. NIST standards solicit and integrate input from industry and are free to download from the NIST website.

Finally, think about how computers talk to other computers across the globe. People speak different languages and do not always understand each other. How are computers able to communicate? Through standards, of course!

Thanks to the **Internet Engineering Task Force (IETF)**, there are standards in communication protocols that ensure all computers can connect with each other across borders, even when the operators do not speak the same language.

The **Institute of Electrical and Electronics Engineers (IEEE)** also sets standards for telecommunications, computer engineering and similar disciplines.

Policies

Policy is informed by applicable law(s) and specifies which standards and guidelines the organization will follow. Policy is broad, but not detailed; it establishes context and sets out strategic direction and priorities. Governance policies are used to moderate and control decision-making, to ensure compliance when necessary and to guide the creation and implementation of other policies.

Policies are often written at many levels across the organization. High-level governance policies are used by senior executives to shape and control decision-making processes. Other high-level policies direct the behavior and activity of the entire organization as it moves toward specific or general goals and objectives. Functional areas such as human resources management, finance and accounting, and security and asset protection usually have their own sets of policies. Whether imposed by laws and regulations or by contracts, the need for compliance might also require the development of specific high-level policies that are documented and assessed for their effective use by the organization.

Policies are implemented, or carried out, by people; for that, someone must expand the policies from statements of intent and direction into step-by-step instructions, or procedures.

Procedure

Procedures define the explicit, repeatable activities necessary to accomplish a specific task or set of tasks. They provide supporting data, decision criteria or other explicit knowledge needed to perform each task. Procedures can address one-time or infrequent actions or common, regular occurrences. In addition, procedures establish the measurement criteria and methods to use to determine whether a task has been successfully completed.

Properly documenting procedures and training personnel on how to locate and follow them is necessary for deriving the maximum organizational benefits from procedures.

Importance of governance elements

Regulations and laws can affect the day-to-day operations of many organizations. As we mentioned before, one example of a law with a broad impact is t**he General Data Protection Regulation (GDPR),** which affords data protection and control to individuals within the territorial boundaries of the EU regardless of citizenship.

As another example, in the United States, patient medical information is governed by the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) and must be closely guarded. From the information security perspective, a high standard of professionalism is expected in safeguarding data on the patients' behalf. Information security is based on trust and credibility. If something goes wrong, the stakeholders' trust evaporates, and organizations' credibility is damaged—sometimes without cure. HIPAA also carries significant criminal and financial penalties for noncompliance for both the organization and the individuals involved.

Fortunately, there are published frameworks, or standards, to guide the organizational policies that support the compliance effort. Many departments or workgroups within the organization implement procedures that detail how they complete day-to-day tasks while remaining compliant. Among these groups is the International Organization for Standardization (ISO). ISO is an international standards body; one of the standards that ISO publishes is how to destroy data in a secure fashion.

Importance of a professional code of ethics (podcast)

Chad: Good morning, good afternoon, or good evening, depending on where and when you're listening. Welcome to the discussion on the role of ethics in cybersecurity. I'm your host, Chad Kliewer, holder of the CISSP and CCSP certifications, and current $(ISC)^2$ member, and I'll be facilitating our experience. I am extremely excited to welcome our special guest for today's discussion, Eder de Mattos, who holds the CISSP with the ISSAP endorsement, ISSMP, and CCSP credentials, and is also an active $(ISC)^2$ member. Eder joins us today from Brazil, where he's worked in communications, now works for an international cloud services organization, and he's also the treasurer for the $(ISC)^2$ Sao Paulo chapter. So let's get started. And today we'll start our discussion by illuminating an example code of ethics. So in this example, for all information security professionals who are certified by $(ISC)^2$, are required to adhere to $(ISC)^2$ Code of Ethics, there are only four canons, and we'll paraphrase them now. "To protect society, the common good, and infrastructure." The second one is "act honorably, honestly, justly, responsibly, and legally." And the third, "provide diligent and competent service to principals." And the final canon is "advance and protect the profession." So this is just one example of professional ethics, and it can take many forms. So, Eder, I'm curious, how do you define professional ethics, based on your experience?

Protect society, the common good, necessary public trust and confidence, and the infrastructure.
Act honorably, honestly, justly, responsibly and legally. =
Provide diligent and competent service to principals.
Advance and protect the profession.

Theoretical example- code of ethics

Here is an example of an ethical question that might come up for cyber security professionals. An organization handling Top Secret and other sensitive information was hiring new employees. At its facility, it used a retinal scanner to grant access to high-security areas, including where prospective employees were interviewed. Retinal scanners, unbeknownst to most people, can not only match blood vessels on an individual's retina, but they can also tell the difference between males and females. Further, they can tell whether a female is pregnant.

The organization used this information gathered by its access control system to discriminate against female candidates for the positions it was seeking to fill. Allowing this data to be accessed by those making hiring decisions was indisputably in violation of the $(ISC)_2$ Code of Ethics, which states that information security professionals must act honorably, honestly, justly, responsibly and legally.

Here is another example: The security manager for an organization heard from a network administrator who reported another user for violating the organization's acceptable use policy. When the security manager investigated the matter, he discovered several pertinent facts:

- The user did violate the policy.
- The violation was not a criminal matter.
- The network administrator had the IT permissions to monitor the user.
- The network administrator was not tasked with monitoring the user, nor was the administrator tasked with randomly monitoring all users.

• The network administrator would not say how the administrator came to learn that the user was violating policy.
• In talking with colleagues of both people, it became clear that there was a personal conflict between the administrator and the user.

In many jurisdictions, the organization can use any information, regardless of source, to make labor decisions. So yes, the organization could use this information against the user. The user violated the policy but did not break the law. Depending on how egregious the infraction was, the organization may choose to punish the user for the violation.

Because the administrator would not explain why he was monitoring the user, it makes his actions suspect at best, and nefarious at worst. The administrator violated the trust given to him by the organization; as an IT professional, the administrator was expected to use authority and permissions in an adult and objective manner. This situation is almost certainly an example of the administrator using authority to settle a personal grievance. The administrator

should be punished much more severely than the user (firing the administrator is not untoward; this person may have opened the organization up to a lawsuit for creating a hostile work environment, which may have an impact/risk that exceeds whatever policy violation the user committed).

Whether the administrator was terminated or not, his actions were in clear contradiction of the Code of Ethics.

Terms and definitions

Adequate Security - Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information. Source: OMB Circular A-130

Administrative Controls - Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.

Artificial Intelligence - The ability of computers and robots to simulate human intelligence and behavior.

Asset - Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

Authentication - Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single factor or SFA) or more (multi-factor authentication or MFA) factors of identification.

Authorization - The right or a permission that is granted to a system entity to access a system resource. NIST 800-82 Rev.2

Availability - Ensuring timely and reliable access to and use of information by authorized users.

Baseline - A documented, lowest level of security configuration allowed by a standard or organization.

Bot - Malicious code that acts like a remotely controlled “robot” for an attacker, with other Trojan and worm capabilities.

Classified or Sensitive Information - Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form.

Confidentiality - The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. NIST 800-66

Criticality - A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. NIST SP 800-60 Vol. 1, Rev. 1

Data Integrity - The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit. Source: NIST SP 800-27 Rev A

Encryption - The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

General Data Protection Regulation (GDPR) - In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

Governance -The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles, and procedures the organization uses to make those decisions.

Health Insurance Portability and Accountability Act (HIPAA) - This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individual's health information. Other provisions address fraud reduction, protections for individuals with health insurance and a wide range of other healthcare-related activities. Est. 1996.

Impact - The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

Information Security Risk - The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

Institute of Electrical and Electronics Engineers - IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.

Integrity - The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.

International Organization of Standards (ISO) - The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies.

Internet Engineering Task Force (IETF) - The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus. Source: NIST SP 1800-16B

Likelihood - The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

Likelihood of Occurrence - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.
Multi-Factor Authentication - Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.
National Institutes of Standards and Technology (NIST) - The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions.
Non-repudiation - The inability to deny taking an action such as creating information, approving information and sending or receiving a message.
Personally Identifiable Information (PII) - The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information.”
Physical Controls - Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.
Privacy - The right of an individual to control the distribution of information about themselves.
Probability - The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Source: NIST SP 800-30 Rev. 1
Protected Health Information (PHI) - Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).
Qualitative Risk Analysis - A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286
Quantitative Risk Analysis - A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain. Source: NISTIR 8286
Risk - A possible event which can have a negative impact upon the organization.
Risk Acceptance - Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.
Risk Assessment - The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations. The analysis performed as part of risk management

which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.
Risk Avoidance - Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.
Risk Management - The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.
Risk Management Framework - A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 4009
Risk Mitigation - Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.
Risk Tolerance - The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.
Risk Transference - Paying an external party to accept the financial impact of a given risk.
Risk Treatment - The determination of the best way to address an identified risk.
Security Controls - The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. Source: FIPS PUB 199
Sensitivity - A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Source: NIST SP 800-60 Vol 1 Rev 1
Single-Factor Authentication - Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.
State - The condition an entity is in at a point in time.
System Integrity - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. Source: NIST SP 800-27 Rev. A
Technical Controls - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.
Threat- Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
Threat Actor - An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.
Threat Vector - The means by which a threat actor carries out their objectives.

Token- A physical object a user possesses and controls that is used to authenticate the user's identity. Source: NISTIR 7711
Vulnerability - Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1

Incident terminology

While security professionals strive to protect systems from malicious attacks or human carelessness, inevitably, despite these efforts, things go wrong. For this reason, security professionals also play the role of first responders. An understanding of incident response starts with knowing the terms used to describe various cyberattacks.

Tab 1: Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Source: NIST SP 800-53 Rev. 5

Tab 2: Event

Any observable occurrence in a network or system. (Source: NIST SP 800-61 Rev 2)

Tab 3: Exploit

A particular attack. It is named this way because these attacks exploit system vulnerabilities.

Tab 4: Incident

An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

Tab 5: Intrusion

A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. Source: (IETF RFC 4949 Ver 2)

Tab 6: Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access,

destruction, disclosure, modification of information and/or denial of service. Source: NIST SP 800-30 Rev 1

Tab 7: Vulnerability

Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. NIST SP 800-30 Rev 1

Tab 8: Zero Day

A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

What does incident response in cybersecurity look like? No 911 calls have reported an incident. No ambulances or fire engines are coming to the rescue. It's up to the cybersecurity professionals to detect and respond to incidents.

The Goal of Incident Response

Every organization must be prepared for incidents. Despite the best efforts of an organization's management and security teams to avoid or prevent problems, it is inevitable that **adverse events** will happen that have the potential to affect the business mission or objectives. The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, always choose safety first.

The primary goal of incident management is to be prepared. Preparation requires having a policy and a response plan that will lead the organization through the crisis. Some organizations use the term "crisis management" to describe this process, so you might hear this term as well.

An event is any measurable occurrence, and most events are harmless. However, if the event has the potential to disrupt the business's mission, then it is called an incident. Every organization must have an **incident response plan** that will help preserve business viability and survival.

The incident response process is aimed at reducing the impact of an incident so the organization can resume the interrupted operations as soon as possible. Note that incident response planning is a subset of the greater discipline of business continuity management (BCM), which we will cover shortly.

Incident Response Priorities

Chad Kliewer: All right. Good morning, good afternoon, or good evening, depending on where in the world you're listening from. So welcome to the discussion on the importance of prioritizing responses to incidents. I'm your host, Chad Kliewer, holder of CISSP, CCSP, and

The incident response policy should reference an incident response plan that all employees will follow, depending on their role in the process. The plan may contain several procedures and standards related to incident response. It is a living representation of an organization's incident response policy. The organization's vision, strategy and mission should shape the incident response process. Procedures to implement the plan should define the technical processes, techniques, checklists and other tools that teams will use when responding to an incident. To prepare for incidents, here are the components commonly found in an incident response plan:

Preparation

- Develop a policy approved by management.
- Identify critical data and systems, single points of failure.
- Train staff on incident response.
- Implement an incident response team. (covered in subsequent topic)
- Practice Incident Identification. (First Response)
- Identify Roles and Responsibilities.
- Plan the coordination of communication between stakeholders.

Detection and analysis

- Monitor all possible attack vectors.
- Analyze incident using known data and threat intelligence.
- Prioritize incident response.
- Standardize incident documentation.

Containment, eradication and recovery

- Gather evidence.
- Choose an appropriate containment strategy.
- Identify the attacker.
- Isolate the attack.

Post incident activity

- Identify evidence that may need to be retained.
- Document lessons learned

Consulting with Management

The first part of preparation is identifying the critical information that needs protection and avoiding any single point of failure. This means that if we have something particularly important, but it is protected by just one door, we create multiple layers of protection to reduce the likelihood of a successful attack. We will talk more later about the principle of defense in depth, but like a fortress, the more layers of defense we have, the more difficult it will be for attackers who are trying to break through.

It is important to train staff in incident response so that everyone knows what to do. Training can include simulations and scenarios so teams can practice their response and learn to coordinate communication among the different stakeholders of the organization. That includes colleagues, superiors, the owners of the information and customers as well. We need to consider what types of communication will be available, because we cannot communicate the same information to everyone. Some material will be confidential, and some will be useful only to certain people and not to the press or outside individuals.

When it comes to detection and analysis, we need to monitor the attack vectors, how the attack was made and what technology was used. It is important to standardize the incident documentation, because in a group of people, each will have their own idea of how to record activities and procedures. For the consistency of the organization and our responsibility to the data owners, we need to have a standardized incident response, where each person knows exactly what needs to be done and in what sequence. This makes it easier to prioritize the response, because each person has their own tasks and knows how to take care of their own responsibilities then communicate appropriately with others concerned.

Next, we need to find the appropriate containment strategy, identify the attackers and how they penetrated our defenses, and isolate the attack, making sure it does not go any further or do additional damage. After the incident, we identify evidence that may need to be retained then, often, there is an internal audit of what occurred. External investigation may also be required, especially in major cyberattacks where law enforcement is involved. Lessons learned must be documented. Perhaps, it will be found that we responded better than during a previous attack, but we still need to improve preparation or detection analysis. Often, these post-incident activities are subject to regulatory requirements, and certain documentation must be submitted. This is especially important if the compromised critical information is protected by law.

Incident response team

Along with the organizational need to establish a **Security Operations Center (SOC)** is the need to create a suitable incident response team. A properly staffed and trained incident response team can be leveraged, dedicated or a combination of the two, depending on the requirements of the organization.

Many IT professionals are classified as first responders for incidents. They are the first ones on the scene and know how to differentiate typical IT problems from security incidents. They are similar to medical first responders who have the skills and knowledge to provide medical assistance at accident scenes and help get the patients to medical facilities when necessary. The medical first responders have specific training to help them determine the difference between minor and major injuries. Further, they know what to do when they come across a major injury.

Similarly, IT professionals need specific training so they can determine the difference between a typical problem that needs troubleshooting and a security incident that they need to report and address at a higher level.

A typical incident response team is a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident. Potential team members include the following:

Representative(s) of senior management
Information security professionals
Legal representatives
Public affairs/communications representatives
Engineering representatives (system and network)

Team members should have training on incident response and the organization's incident response plan. Typically, team members assist with investigating the incident, assessing the damage, collecting evidence, reporting the incident and initiating recovery procedures. They would also participate in the remediation and lessons learned stages and help with root cause analysis.

Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs). When an incident occurs, the response team has four primary responsibilities:

Determine the amount and scope of damage caused by the incident.
Determine whether any confidential information was compromised during the incident.
Implement any necessary recovery procedures to restore security and recover from incident-related damage.
Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

These are just a few examples of how a simple event could escalate and involve other teams. The organization's incident response procedure should be scalable from a single event to events causing system-wide outages, with appropriate personnel levels defined in the plan.

UNDERSTAND BUSINESS CONTINUITY

The importance of business continuity

The intent of a business continuity plan is to sustain business operations while recovering from a significant disruption. An event has created a disturbance in the environment, and now you need to know how to maintain the business.

A key part of the plan is communication, including multiple contact methodologies and backup numbers in case of a disruption of power or communications. Many organizations will establish a phone tree, so that if one person is not available, they know who else to call. Organizations will go through their procedures and checklists to make sure they know exactly who is responsible for which action. No matter how many times they have flown, without fail, pilots go through a checklist before take-off. Similarly, there must be established procedures and a thorough checklist, so that no vital element of business continuity will be missed.

We call the appropriate individuals and start to activate the business continuity plan. Management must be included, because sometimes priorities may change depending on the situation. Individuals with proper authority must be there to execute operations, for instance, if there are critical areas that need to be shut down.

We need to have at hand the critical contact numbers for the supply chain, as well as law enforcement and other sites outside of the facility. For example, a hospital may suffer a severe cyberattack that affects communications from the pharmacy, the internet or phone lines. In the United States, in case of this type of cyberattack that knocks out communications, specific numbers in specific networks can bypass the normal cell phone services and use military-grade networks. Those will be assigned to authorized individuals for hospitals or other critical infrastructures in case of a major disruption or cyberattack, so they can still maintain essential activity.

The goal of business continuity

Business continuity refers to enabling the critical aspects of the organization to function, perhaps at a reduced capacity, during a disruption caused by any form of disturbance, attack, infrastructure failure or natural disaster. Most incidents are minor and can be handled easily with minimal impact. A system requires a reboot for example, but after a few minutes the system is back in operation and the incident is over. But once in a while a major incident will interrupt business for an unacceptable length of time, and the organization cannot just follow an incident plan but must move toward business continuity.

Business continuity includes planning, preparation, response and recovery operations, but it does not generally include activities to support full restoration of all business activities and services. It focuses on the critical products and services that the organization provides and ensures those important areas can continue to operate even at a reduced level of performance until business returns to normal.

Developing a business continuity plan requires a significant organizational commitment in terms of both personnel and financial resources. To gain this commitment, organizational support for business continuity planning efforts must be provided by executive management or an executive sponsor. Without the proper support, business continuity planning efforts have little chance of success.

Components of a business continuity plan

Business continuity planning (BCP) is the proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization. Members from across the organization should participate in creating the BCP to ensure all systems, processes and operations are accounted for in the plan.

The term business is used often, as this is mostly a business function as opposed to a technical one. However, in order to safeguard the confidentiality, integrity and availability of information, the technology must align with the business needs.

Here are some common components of a comprehensive business continuity plan:

List of the BCP team members, including multiple contact methods and backup members
Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
Notification systems and call trees for alerting personnel that the BCP is being enacted
Guidance for management, including designation of authority for specific managers
How/when to enact the plan
Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners

Business Continuity in the work place

Obviously, the business continuity plan needs to be maintained somewhere where it can be accessed. Often, in modern organizations, everything is digital and not provided as a hard copy. This can be dangerous, just like storing everything within the main company building.

Some organizations have what is called the Red Book, which is given to the appropriate individual outside the facility. All the procedures are outlined in that document—in case, for example, a hurricane hits, the power is out and all the facilities are compromised and there is

no access to electronic backups. It is important to update this hard-copy Red Book any time the electronic copy is updated so both versions remain consistent.

Business continuity in action

What does business continuity look like in action?

Imagine that the billing department of a company suffers a complete loss in a fire. The fire occurred overnight, so no personnel were in the building at the time. A ***Business Impact Analysis (BIA)*** *was performed four months ago and identified the functions of the billing department as very important to the company, but not immediately affecting other areas of work. Through a previously signed agreement, the company has an alternative area in which the billing department can work, and it can be available in less than one week. Until that area can be fully ready, customer billing inquiries will be answered by customer service staff. The billing department personnel will remain in the alternate working area until a new permanent area is available.*

In this scenario, the BIA already identified the dependencies of customer billing inquiries and revenue. Because the company has ample cash reserves, a week without billing is acceptable during this interruption to normal business. Pre-planning was realized by having an alternate work area ready for the personnel and having the customer service department handle the billing department's calls during the transition to temporary office space. With the execution of the plan, there was no material interruption to the company's business or its ability to provide services to its customers—indicating a successful implementation of the business continuity plan.

UNDERSTAND DISASTER RECOVERY (DR)

Manny: No matter how good the incident response and business continuity plans are, it seems likely that some lasting damage is going to be done. Some data is going to be lost or some services delayed. How do we get things back to normal?

Tasha: That's where disaster recovery comes in. It picks up where business continuity left off. We discussed in the last module that business continuity is about maintaining critical business functions. These functions often rely on IT systems and communications. Disaster recovery planning is about restoring IT and communications back to full operation after a disruption, which we'll learn more about in this module.

The goal of disaster recovery

In the Business Continuity module, the essential elements of business continuity planning were explored. **Disaster recovery** planning steps in where BC leaves off. When a disaster strikes or an interruption of business activities occurs, the **Disaster recovery plan (DRP)**

guides the actions of emergency response personnel until the end goal is reached—which is to see the business restored to full last-known reliable operations.

Disaster recovery refers specifically to restoring the information technology and communications services and systems needed by an organization, both during the period of disruption caused by any event and during restoration of normal services. The recovery of a business function may be done independently of the recovery of IT and communications services; however, the recovery of IT is often crucial to the recovery and sustainment of business operations. Whereas business continuity planning is about maintaining critical business functions, disaster recovery planning is about restoring IT and communications back to full operations after a disruption.

Disaster recovery in the real world

We need to make sure that an organization's critical systems are formally identified and have backups that are regularly tested. Sometimes an incident is not recognized or detected until days or months later.

At a hospital in Los Angeles, it took 260 days (about 8 and a half months) to discover that there was a compromise. In this case, the hospital could not return to doing business by using the last backup because it was riddled with a time-based malware that would corrupt all the data on the system as soon as it was restored. The hospital needed to go back nearly a year prior to discovering the incident to restore the entire system, and then restore the remaining data piece-by-piece to avoid reinfection. This scenario highlights the need for multiple levels of backup and retention periods to address the needs of the organization.

Complex systems can often store valuable information across several servers. While at its most basic level, disaster recovery plans include backing up data at a server level, it is also necessary to consider the database itself, as well as any dependencies on other systems. In this more complex scenario, data is entered by users into one system and database and is then distributed to other systems. This is common in large enterprises where multiple systems need to talk to each other to maintain common data. In another hospital example, the radiology department used a different system than the laboratory. In this case, a separate routine copied the patient data from the registration system to the laboratory and the radiology systems, which technically use separate databases. It is important to understand the flow of data and the intricate dependencies of one system on another to properly document and implement a disaster recovery plan that will be successful when it is needed.

Components of a disaster recovery plan

Depending on the size of the organization and the number of people involved in the DRP effort, organizations often maintain multiple types of plan documents, intended for different audiences. The following list includes various types of documents worth considering:

- Executive summary providing a high-level overview of the plan
- Department-specific plans

Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
Full copies of the plan for critical disaster recovery team members
Checklists for certain individuals:
Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster.
IT personnel will have technical guides helping them get the alternate sites up and running.
Managers and public relations personnel will have simple-to-follow, high-level documents to help them communicate the issue accurately without requiring input from team members who are busy working on the recovery.

Disaster recovery in action

An example of disaster recovery in action is the use of system backups. The timeline in this image looks backward in time from the moment of incident detection (on the right) as a way of identifying the amount of work that will be lost by reloading from a backup. Transaction processing events (the triangles) and some backup events (shown as database symbols) have been numbered as events 1 through 21 from left to right along the timeline. The green transactions (events 1 through 14) are ones that were fully processed prior to the intrusion or the start of the incident. Presumably, and if antivirus and other systems are working correctly, this may be a safe assumption. These transactions were not exposed to possible loss of integrity, authenticity, privacy, or any other required security attributes.

The database symbols shown in gray (events 2, 5, 9, and 13—all prior to the event) represent some form of system and data backup that may have captured the changes to the system as a result of properly completing the green transactions.

It is events 15 through 21, however, that are in doubt. They may be okay, or they may represent a lack of integrity if the data was compromised. The database backup symbols in orange, between the time of the incidence occurrence and it's being detected, are clearly in doubt as to their integrity or safety. They may contain bogus, corrupted data or they may even contain malware in a variety of forms. Moving backward in time from the detection of the incident, it's not until we get to that right most gray database symbol—event 13 the backup just before the incident occurs—that we have our last clean, trustworthy backup.

Three sets of work that were lost since the incident started to occur can be identified: all transactions or changes prior to that last good backup that were not part of that backup—if it was an incremental or partial backup and not a full backup—events 15, 17 through 19 and 21; all transactions and other changes processed or attempted from that backup forward in time until after the incident was detected, not started to occur; and all transactions changes, etc. that would normally have been processed from the time the incident was detected until the system was fully operational again, but were not able to be processed at all due to the disruption.

When lightening strikes

Manny: During a bad lightning storm last night, JavaSip experienced a power surge that damaged the company computer.

Sandra: (Groaning) Oh, I can't believe it. The power surge killed the computer. It won't even turn on. Now what are we going to do?

Keith: Seems like we need a new computer.
Sandra: Well, that's the least of our worries. What about everything that's on the computer?

Everything we need to run this coffee shop is on the computer.

Keith: It's okay, Mom. Remember? As part of our disaster recovery plan, Nate and I have been backing up the system every night after we close.

Sandra: Are you serious? You have everything backed up?
Keith: Everything. It's all on an external hard drive that we take home every night after we

close.
Sandra: (Laughing) Thank goodness. I'm so proud of you. See, we need you here at JavaSip.

Keith: Aw, thanks, Mom. Glad I can help. It's just too bad I couldn't predict a power surge that'd impact the business like this. But look, you go get a new computer and get a surge protector while you're at it.

Sandra: I agree. We do not want anything like this to ever happen again.
Keith: I'll call Nate. He'll bring the backup, and we'll upload and restore everything up until last

night. *Sandra:* Okay.

CHAPTER 2 TERMS AND DEFINITION

Adverse Events - Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.
Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Source: NIST SP 800-53 Rev. 5
Business Continuity (BC) - Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.
Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption.
Business Impact Analysis (BIA) - An analysis of an information system’s requirements, functions, and interdependencies used to characterize system

contingency requirements and priorities in the event of a significant disruption. Reference: https://csrc.nist.gov/glossary/term/business-impact-analysis

Disaster Recovery (DR) - In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, disruption or disturbance of any kind or scale.

Disaster Recovery Plan (DRP) - The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. A disaster is when an organization’s critical business function(s) cannot be performed at an acceptable level within a predetermined period following a disruption.

Event - Any observable occurrence in a network or system. Source: NIST SP 800-61 Rev 2

Exploit - A particular attack. It is named this way because these attacks exploit system vulnerabilities.

Incident - An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

Incident Handling - The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response (IR) - The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response Plan (IRP) - The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization’s information systems(s). Source: NIST SP 800-34 Rev 1

Intrusion - A security event, or combination of security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. Source: IETF RFC 4949 Ver 2

Security Operations Center - A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

Vulnerability - Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-128.

Zero Day - A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

UNDERSTAND ACCESS CONTROL CONCEPTS

Manny: In the last module, we covered all the planning that goes into incident response and disaster recovery. But how do security professionals protect information from falling into the wrong hands in the first place?

Tasha: That's the topic of our next module. Information security professionals are like gatekeepers, controlling who gets access to which systems and data, why they get certain permissions or not, and how. Let's find out more about these access control concepts.

What is a security control

A control is a safeguard or countermeasure designed to preserve Confidentiality, Integrity and Availability of data. This, of course, is the CIA Triad.

Access control involves limiting what objects can be available to what subjects according to what rules. We will further define objects, subjects and rules later in this chapter. For now, remember these three words, as they are the foundation upon which we will build.

One brief example of a control is a firewall, which is included in a system or network to prevent something from the outside from coming in and disturbing or compromising the environment. The firewall can also prevent information on the inside from going out into the Web where it could be viewed or accessed by unauthorized individuals.

Controls overview

It can be argued that access controls are the heart of an information security program. Earlier in this course we looked at security principles through foundations of risk management, governance, incident response, business continuity and disaster recovery. But in the end, security all comes down to, “who can get access to organizational assets (buildings, data, systems, etc.) and what can they do when they get access?”

Access controls are not just about restricting access to information systems and data, but also about allowing access. It is about granting the appropriate level of access to authorized personnel and processes and denying access to unauthorized functions or individuals.

Access is based on three elements:

A **subject** can be defined as any entity that requests access to our assets. The entity requesting access may be a user, a client, a process or a program, for example. A subject is the initiator of a request for service; therefore, a subject is referred to as “active.”

A subject:

Is a user, a process, a procedure, a client (or a server), a program, a device such as an endpoint, workstation, smartphone or removable storage device with onboard firmware.
Is active: It initiates a request for access to resources or services.
Requests a service from an object.
Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.

By definition, anything that a subject attempts to access is referred to as an **object**. An object is a device, process, person, user, program, server, client or other entity that responds to a request for service. Whereas a subject is active in that it initiates a request for a service, an object is passive in that it takes no action until called upon by a subject. When requested, an object will respond to the request it receives, and if the request is wrong, the response will probably not be what the subject really wanted either.

Note that by definition, objects do not contain their own access control logic. Objects are passive, not active (in access control terms), and must be protected from unauthorized access by some other layers of functionality in the system, such as the integrated identity and access management system. An object has an owner, and the owner has the right to determine who or what should be allowed access to their object. Quite often the rules of access are recorded in a rule base or access control list.

An object:

> Is a building, a computer, a file, a database, a printer or scanner, a server, a communications resource, a block of memory, an input/output port, a person, a software task, thread or process.
> Is anything that provides service to a user.
> Is passive.
> Responds to a request.
> May have a classification.

An access **rule** is an instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list. One example of a rule is a **firewall** access control list. By default, firewalls deny access from any address to any address, on any port. For a firewall to be useful, however, it needs more rules. A rule might be added to allow access from the inside network to the outside network. Here we are describing a rule that allows access to the object “outside network” by the subject having the address “inside network.” In another example, when a user (subject) attempts to access a file (object), a rule validates the level of access, if any, the user should have to that file. To do this, the rule will contain or reference a set of attributes that define what level of access has been determined to be appropriate.

A rule can:

> Compare multiple attributes to determine appropriate access.
> Allow access to an object.
> Define how much access is allowed.
> Deny access to an object.
> Apply time-based access.

Controls and risks

Narrator: A control serves to reduce the risk to where it is within the risk tolerance of the individual or organization. A physical control would be a seat belt. An administrative control would be a law requiring the use of the seatbelt. Both of these serve to reduce the risk of driving to a degree that is acceptable to the driver and to society.

Another non-technical example is that of a tall bookshelf. Since there is a risk of a tall bookshelf toppling over and possibly hurting someone, many local building codes or regulations require bookshelves to be secured to a wall using a strap or a bracket. In this case, the risk is the injury to people. A logical control is the building code, and the actual attachment of the shelf to the wall is the physical control. Both logical and physical controls work together to mitigate the risk.

Control assessments

Risk reduction depends on the effectiveness of the control. It must apply to the current situation and adapt to a changing environment.

Consider a scenario where part of an office building is being repurposed for use as a secure storage facility. Due to the previous use of the area, there are 5 doors which must be secured before confidential files can be stored there. When securing a physical location, there are several things to consider. To keep the information the most secure, it might be recommended to install biometric scanners on all doors. A site assessment will determine if all five doors need biometric scanners, or if only one or two doors need scanners. The remaining doors could be permanently secured, or if the budget permits, the doors could be removed and replaced with a permanent wall. Most importantly, the cost of implementing the controls must align with the value of what is being protected. If multiple doors secured by biometric locks are not necessary, and the access to the area does not need to be audited, perhaps a simple deadbolt lock on all of the doors will provide the correct level of control.

Defense in depth

As you can see, we are not just looking at system access. We are looking at all access permissions including building access, access to server rooms, access to networks and applications and utilities. These are all implementations of access control and are part of a layered defense strategy, also known as defense in depth, developed by an organization.

Defense in depth describes an information security strategy that integrates people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization. It applies multiple countermeasures in a layered fashion to fulfill security objectives. Defense in depth should be implemented to prevent or deter a cyberattack, but it cannot guarantee that an attack will not occur.

A technical example of defense in depth, in which multiple layers of technical controls are implemented, is when a username and password are required for logging in to your account, followed by a code sent to your phone to verify your identity. This is a form of multi-factor authentication using methods on two layers, something you have and something you know. The combination of the two layers is much more difficult for an adversary to obtain than either of the authentication codes individually.

Another example of multiple technical layers is when additional firewalls are used to separate untrusted networks with differing security requirements, such as the internet from trusted networks that house servers with sensitive data in the organization. When a company has information at multiple sensitivity levels, it might require the network traffic to be validated by rules on more than one firewall, with the most sensitive information being stored behind multiple firewalls.

For a non-technical example, consider the multiple layers of access required to get to the actual data in a data center. First, a lock on the door provides a physical barrier to access the data storage devices. Second, a technical access rule prevents access to the data via the network. Finally, a policy, or administrative control defines the rules that assign access to authorized individuals.

Defense in depth practice

Narrator: A data center might have multiple layers of defense. We would have administrative controls, such as policies and procedures. Then logical or technical controls, which include programming to limit access. There are also physical controls, which we sometimes forget about in our highly technical world. Regardless of how much we focus on cloud computing and virtualization, there is always a physical location where information is being stored or processed in a physical hard drive in a physical computer. Even in a data center in a large organization that provides cloud computing services, for example, there is still a physical aspect of information storage and processing.

Principle of least privilege

The **Principle of Least Privilege** is a standard of permitting only minimum access necessary for users or programs to fulfill their function. Users are provided access only to the systems and programs they need to perform their specific job or tasks.

Tasha: Gabriela is a recent new hire at JavaSip, and she's reached out to Nate for some help.

Gabriela: Hey Nate?

Nate: Yep?

Gabriela: I accidentally submitted my timecard already, and I can't get into the payroll system to fix it.

Nate: Well, of course you can’t get into the system. Only the manager, that's me, can get into the payroll system. Otherwise, we'd risk everyone giving themselves raises, not to mention having access to other employees' confidential information. Here, let me show you. There it is.

Gabriela: Oh. Yeah. *Nate:* All good. *Gabriela:* Thanks! *Nate:* Welcome.

Tasha: Nate explains to Gabriela that her access to the system is limited by her role. She doesn't have the proper permissions to make changes to her timecard, just to complete and submit it. That's all she needs to do in her position, so she is restricted from other functions in the system, but he's happy to help and reassures Gabriela that he will make the necessary changes.

Examples of least privilege

To preserve the confidentiality of information and ensure that it is only available to personnel who are authorized to see it, we use privileged access management, which is based on the principle of least privilege. That means each user is granted access only to the items they need and nothing further.

For example, only individuals working in billing will be allowed to view consumer financial data, and even fewer individuals will have the authority to change or delete that data. This maintains confidentiality and integrity while also allowing availability by providing administrative access with an appropriate password or sign-on that proves the user has the appropriate permissions to access that data.

Sometimes it is necessary to allow users to access the information via a temporary or limited access, for instance, for a specific time period or just within normal business hours. Or access rules can limit the fields that the individuals can have access to. One example is a healthcare environment. Some workers might have access to patient data but not their medical data. Individual doctors might have access only to data related to their own patients. In some cases, this is regulated by law, such as HIPAA in the United States, and by specific privacy laws in other countries.

Systems often monitor access to private information, and if logs indicate that someone has attempted to access a database without the proper permissions, that will automatically trigger an alarm. The security administrator will then record the incident and alert the appropriate people to take action.

The more critical information a person has access to, the greater the security should be around that access. They should definitely have multi-factor authentication, for instance.

Privileged access management

Privileged access management provides the first and perhaps most familiar use case. Consider a human user identity that is granted various create, read, update, and delete privileges on a database. Without privileged access management, the system's access control would have those privileges assigned to the administrative user in a static way, effectively "on" 24 hours a day, every day. Security would be dependent upon the login process to prevent misuse of that identity. Just-in-time privileged access management, by contrast, includes role-based specific subsets of privileges that only become active in real time when the identity is requesting the use of a resource or service.

Consider this scenario explaining why privileged access management is important:

*ABC, Inc., has a small IT department that is responsible for **user provisioning** and administering systems. To save time, the IT department employees added their IDs to the Domain Admins group, effectively giving them access to everything within the Windows server and workstation environment. While reviewing an invoice that was received via email, they opened an email that had a malicious attachment that initiated a **ransomware** attack. Since they are using Domain Admin privileges, the ransomware was able to **encrypt** all the files on all servers and workstations. A privileged access management solution could limit the damage done by this ransomware if the administrator privileges are only used when performing a function requiring that level of access. Routine operations, such as daily email tasks, are done without a higher level of access.*

Privileged accounts

Privileged accounts are those with permissions beyond those of normal users, such as managers and administrators.

Broadly speaking, these accounts have elevated privileges and are used by many different classes of users, including:

- Systems administrators, who have the principal responsibilities for operating systems, applications deployment and performance management.
- Help desk or IT support staff, who often need to view or manipulate endpoints, servers and applications platforms by using privileged or restricted operations.
- Security analysts, who may require rapid access to the entire IT infrastructure, systems, endpoints and data environment of the organization.

Other classes of privileged user accounts may be created on a per-client or per-project basis, to allow a member of that project or client service team to have greater control over data and applications.

These few examples indicate that organizations often need to delegate the capability to manage and protect information assets to various managerial, supervisory, support or leadership people, with differing levels of authority and responsibility. This delegation, of course, should be contingent upon trustworthiness, since misuse or abuse of these privileges could lead to harm for the organization and its stakeholders.

Typical measures used for moderating the potential for elevated risks from misuse or abuse of privileged accounts include the following:

- More extensive and detailed **logging** than regular user accounts. The record of privileged actions is vitally important, as both a deterrent (for privileged account holders that might be tempted to engage in untoward activity) and an administrative control (the logs can be **audited** and reviewed to detect and respond to malicious activity).
- More stringent access control than regular user accounts. As we will see emphasized in this course, even nonprivileged users should be required to use MFA methods to gain access to organizational systems and networks. Privileged users—or more accurately, highly trusted users with access to privileged accounts—should be required to go through additional or more rigorous authentication prior to those privileges. Just-in-time identity should also be considered as a way to restrict the use of these privileges to specific tasks and the times in which the user is executing them.
- Deeper trust verification than regular user accounts. Privileged account holders should be subject to more detailed background checks, stricter nondisclosure agreements and acceptable use policies, and be willing to be subject to financial investigation. Periodic or event-triggered updates to these background checks may also be in order, depending on the nature of the organization's activities and the risks it faces.
- More auditing than regular user accounts. Privileged account activity should be monitored and audited at a greater rate and extent than regular usage.

Explore privileged access management further

Let's consider the Help Desk role. In order to provide the level of service customers demand, it may be necessary for your Help Desk personnel to reset passwords and unlock user accounts. In a Windows environment, this typically requires "domain admin" privileges. However, these two permissions can be granted alone, giving the Help Desk personnel a way to reset passwords without giving them access to everything in the Windows domain, such as adding new users or changing a user's information. These two actions should be logged and audited on a regular basis to ensure that any password resets were requested by the end user. This can be done by automatically generating a daily list of password resets to be compared to Help Desk tickets. This scenario allows the Help Desk personnel to resolve password-related issues on the first call while doing so in a safe and secure manner.

Segregation of duties

A core element of authorization is the principle of segregation of duties (also known as separation of duties). Segregation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish. Segregation of duties

breaks the transaction into separate parts and requires a different person to execute each part of the transaction. For example, an employee may submit an invoice for payment to a vendor (or for reimbursement to themselves), but it must be approved by a manager prior to payment; in another instance, almost anyone may submit a proposal for a change to a system configuration, but the request must go through technical and management review and gain approval, before it can be implemented.

These steps can prevent fraud or detect an error in the process before implementation. It could be that the same employee might be authorized to originally submit invoices regarding one set of activities, but not approve them, and yet also have approval authority but not the right to submit invoices on another. It is possible, of course, that two individuals can willfully work together to bypass the segregation of duties, so that they could jointly commit fraud. This is called collusion.

Another implementation of segregation of duties is dual control. This would apply at a bank where there are two separate combination locks on the door of the vault. Some personnel know one of the combinations and some know the other, but no one person knows both combinations. Two people must work together to open the vault; thus, the vault is under dual control.

Two-person integrity
The two-person rule is a security strategy that requires a minimum of two people to be in an area together, making it impossible for a person to be in the area alone. Many access control systems prevent an individual cardholder from entering a selected high-security area unless accompanied by at least one other person. Use of the two-person rule can help reduce **insider threats** to critical areas by requiring at least two individuals to be present at any time. It is also used for life safety within a security area; if one person has a medical emergency, there will be assistance present.

Authorized versus unauthorized personnel
Subjects are authorized access to objects after they have been authenticated. Remember from earlier sections that authentication is confirming the identity of the subject. Once a subject has been authenticated, the system checks its authorization to see if it is allowed to complete the action it is attempting. This is usually done via a security matrix accessed by the system controlling the access, based on pre-approved levels. For example, when a person presents an ID badge to the data center door, the system checks the ID number, compares that to a security matrix within the system, and unlocks the door if the ID is authorized. If the ID is not authorized to unlock the door, it will remain locked. In another example, a user attempts to delete a file. The file system checks the permissions to see if the user is authorized to delete the file. If the user is authorized, the file is deleted. If the user is not authorized, an error message is displayed, and the file is left untouched.

How users are provisioned
Other situations that call for provisioning new user accounts or changing privileges include:

Susan: So, will this make things complicated when Dimitra returns to work? Oh, I see. Even though the account is disabled, but not otherwise modified, it will be easy to reactivate it once she returns. That's great news, because I'm going to need her up and running as soon as she gets back.

The benefit of multiple controls

Narrator: A control is a safeguard or countermeasure designed to preserve Confidentiality, Integrity and Availability of data. We also discussed defense-in-depth as an implementation of multiple technical controls. Now, we will look at a scenario that uses multiple controls across the spectrum, including physical, technical and administrative controls.

Payroll is one area in nearly every organization that requires multiple levels of controls to ensure money is not mishandled. Most will agree that just a single control is too risky, so multiple controls are often implemented.

To prevent payroll personnel from creating a fictional employee and processing a check for that employee, a logical (or technical) control is to ensure that a person who processes payroll is not able to create a new employee record AND process the check print file. A physical control that helps reinforce that technical control is to ensure the actual paper media that checks are printed on is secured in a place that is not accessible to the person processing payroll. Both of these controls can be further enforced by creating an administrative control (or policy) that regularly audits the technical and physical controls by reviewing new employees added to the system and by logging and verifying the number on physical checks.

Small and medium businesses have a particular challenge when it comes to technical controls, as they often do not have sufficient personnel to separate the duties within the payroll system. In this case, it may become necessary to implement only physical and logical controls that align with the business needs.

UNDERSTAND PHYSICAL ACCESS CONTROLS

Manny: We've talked a lot about protecting systems from being accessed by unauthorized users or bad actors, but isn't there a risk of losing information through methods other than technology like break-ins and stolen laptops?

Tasha: That's right. Simply locking your doors is a great start when protecting data. If a thief can't get into your building, then there's less opportunity for unauthorized access to your equipment, files, and personal information. In this module, we will explore and compare the most common physical access controls employed by organizations to safeguard buildings, property, and people.

What are physical access controls?

Physical access controls are items you can physically touch. They include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas

within a facility. Examples of physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles, and alarms.

Physical access controls are necessary to protect the assets of a company, including its most important asset, people. When considering physical access controls, the security of the personnel always comes first, followed by securing other physical assets.

Why have physical access controls?

Physical access controls include fences, barriers, turnstiles, locks and other features that prevent unauthorized individuals from entering a physical site, such as a workplace. This is to protect not only physical assets such as computers from being stolen, but also to protect the health and safety of the personnel inside.

Types of physical access controls

Many types of physical access control mechanisms can be deployed in an environment to control, monitor and manage access to a facility. These range from deterrents to detection mechanisms. Each area requires unique and focused physical access controls, monitoring and prevention mechanisms. The following sections discuss many such mechanisms that may be used to control access to various areas of a site, including perimeter and internal security.

Badge Systems and Gate Entry

Physical security controls for human traffic are often done with technologies such as **turnstiles**, **mantraps** and remotely or system-controlled door locks. For the system to identify an authorized employee, an access control system needs to have some form of enrollment station used to assign and activate an access control device. Most often, a badge is produced and issued with the employee's identifiers, with the enrollment station giving the employee specific areas that will be accessible. In high-security environments, enrollment may also include biometric characteristics. In general, an access control system compares an individual's badge against a verified database. If authenticated, the access control system sends output signals allowing authorized personnel to pass through a gate or a door to a controlled area. The systems are typically integrated with the organization's logging systems to document access activity (authorized and unauthorized)

A range of card types allow the system to be used in a variety of environments. These cards include:

- Bar code
- Magnetic stripe
- Proximity
- Smart

Hybrid

Environmental Design

Crime Prevention through Environmental Design (CPTED) approaches the challenge of creating safer workspaces through passive design elements. This has great applicability for the information security community as security professionals design, operate and assess the organizational security environment. Other practices, such as standards for building construction and data centers, also affect how we implement controls over our physical environment. Security professionals should be familiar with these concepts so they can successfully advocate for functional and effective physical spaces where information is going to be created, processed and stored.

CPTED provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware) and natural design (architectural and circulation flow) methods. By directing the flow of people, using passive techniques to signal who should and should not be in a space and providing visibility to otherwise hidden spaces, the likelihood that someone will commit a crime in that area decreases.

Biometrics

To authenticate a user's identity, biometrics uses characteristics unique to the individual seeking access. A biometric authentication solution entails two processes.

> Enrollment—during the enrollment process, the user's registered biometric code is either stored in a system or on a smart card that is kept by the user.
> Verification—during the verification process, the user presents their biometric data to the system so that the biometric data can be compared with the stored biometric code.

Even though the biometric data may not be secret, it is personally identifiable information, and the protocol should not reveal it without the user's consent. Biometrics takes two primary forms, physiological and behavioral.

Physiological systems measure the characteristics of a person such as a fingerprint, iris scan (the colored portion around the outside of the pupil in the eye), retinal scan (the pattern of blood vessels in the back of the eye), palm scan and venous scans that look for the flow of blood through the veins in the palm. Some biometrics devices combine processes together—such as checking for pulse and temperature on a fingerprint scanner—to detect counterfeiting.

Behavioral systems measure how a person acts by measuring voiceprints, signature dynamics and keystroke dynamics. As a person types, a keystroke dynamics system measures behavior such as the delay rate (how long a person holds down a key) and transfer rate (how rapidly a person moves between keys).

Biometric systems are considered highly accurate, but they can be expensive to implement and maintain because of the cost of purchasing equipment and registering all users. Users may also be uncomfortable with the use of biometrics, considering them to be an invasion of privacy or presenting a risk of disclosure of medical information (since retina scans can disclose medical conditions). A further drawback is the challenge of sanitization of the devices.

Monitoring

The use of physical access controls and monitoring personnel and equipment entering and leaving as well as auditing/logging all physical events are primary elements in maintaining overall organizational security.

CAMERAS

Cameras are normally integrated into the overall security program and centrally monitored. Cameras provide a flexible method of surveillance and monitoring. They can be a deterrent to criminal activity, can detect activities if combined with other sensors and, if recorded, can provide evidence after the activity They are often used in locations where access is difficult or there is a need for a forensic record.

While cameras provide one tool for monitoring the external perimeter of facilities, other technologies augment their detection capabilities. A variety of motion sensor technologies can be effective in exterior locations. These include infrared, microwave and lasers trained on tuned receivers. Other sensors can be integrated into doors, gates and turnstiles, and strain-sensitive cables and other vibration sensors can detect if someone attempts to scale a fence. Proper integration of exterior or perimeter sensors will alert an organization to any intruders attempting to gain access across open space or attempting to breach the fence line.

LOGS

In this section, we are concentrating on the use of physical logs, such as a sign-in sheet maintained by a security guard, or even a log created by an electronic system that manages physical access. Electronic systems that capture system and security logs within software will be covered in another section.

A log is a record of events that have occurred. Physical security logs are essential to support business requirements. They should capture and retain information as long as necessary for legal or business reasons. Because logs may be needed to prove compliance with regulations and assist in a forensic investigation, the logs must be protected from manipulation. Logs may also contain sensitive data about customers or users and should be protected from unauthorized disclosure.

The organization should have a policy to review logs regularly as part of their organization’s security program. As part of the organization’s log processes, guidelines for log retention must

be established and followed. If the organizational policy states to retain standard log files for only six months, that is all the organization should have.

A **log anomaly** is anything out of the ordinary. Identifying log anomalies is often the first step in identifying security-related issues, both during an audit and during routine monitoring. Some anomalies will be glaringly obvious: for example, gaps in date/time stamps or account lockouts. Others will be harder to detect, such as someone trying to write data to a protected directory. Although it may seem that logging everything so you would not miss any important data is the best approach, most organizations would soon drown under the amount of data collected.

Business and legal requirements for log retention will vary among economies, countries and industries. Some businesses will have no requirements for data retention. Others are mandated by the nature of their business or by business partners to comply with certain retention data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires that businesses retain one year of log data in support of PCI. Some federal regulations include requirements for data retention as well.

If a business has no business or legal requirements to retain log data, how long should the organization keep it? The first people to ask should be the legal department. Most legal departments have very specific guidelines for data retention, and those guidelines may drive the log retention policy.

ALARM SYSTEMS

Alarm systems are commonly found on doors and windows in homes and office buildings. In their simplest form, they are designed to alert the appropriate personnel when a door or window is opened unexpectedly.

For example, an employee may enter a code and/or swipe a badge to open a door, and that action would not trigger an alarm. Alternatively, if that same door was opened by brute force without someone entering the correct code or using an authorized badge, an alarm would be activated.

Another alarm system is a fire alarm, which may be activated by heat or smoke at a sensor and will likely sound an audible warning to protect human lives in the vicinity. It will likely also contact local response personnel as well as the closest fire department.

Finally, another common type of alarm system is in the form of a panic button. Once activated, a panic button will alert the appropriate police or security personnel.

SECURITY GUARDS

Security guards are an effective physical security control. No matter what form of physical access control is used, a security guard or other monitoring system will discourage a person from masquerading as someone else or following closely on the heels of another to gain access. This helps prevent theft and abuse of equipment or information.

UNDERSTAND LOGICAL ACCESS CONTROLS

Manny: It's pretty easy to picture physical controls, and we've all used passwords and other kinds of access controls, but what are logical access controls?

Tasha: This gets a little more technical. The parameters that are set up within a system can affect who has access to certain information and what they can do with it. For example, a system could be configured so that anyone who has permission to edit a file also has permission to copy it and share it with someone else.

Manny: We'll learn more in this module about different types of logical controls.

What are Logical Access Controls?

Whereas physical access controls are tangible methods or mechanisms that limit someone from getting access to an area or asset, logical access controls are electronic methods that limit someone from getting access to systems, and sometimes even to tangible assets or areas. Types of logical access controls include:

- Passwords
- Biometrics (implemented on a system, such as a smartphone or laptop)
- Badge/token readers connected to a system

These types of electronic tools limit who can get logical access to an asset, even if the person already has physical access.

Discretionary Access Control (DAC)

Discretionary access control (DAC) is a specific type of access control policy that is enforced over all su
following:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes on subjects, objects, information systems or system components
- Choose the security attributes to be associated with newly created or revised objects; and/or
- Change the rules governing access control; mandatory access controls restrict this capability

Most information systems in the world are DAC systems. In a DAC system, a user who has access to a file
Rule-based access control systems are usually a form of DAC.

DAC Example

Discretionary access control systems allow users to establish or change these permissions on files they create or otherwise have ownership of.

Steve and Aidan, for example, are two users (subjects) in a **UNIX environment** operating with DAC in place. Typically, systems will create and maintain a table that maps subjects to objects, as shown in the image. At each intersection is the set of permissions that a given subject has for a specific object. Many operating systems, such as Windows and the whole Unix family tree (including **Linux**) and **iOS**, use this type of data structure to make fast, accurate decisions about authorizing or denying an access request. Note that this data can be viewed as either rows or columns:

> An object's access control list shows the total set of *subjects* who have any permissions at all for that specific object.
> A subject's capabilities list shows each object in the system that said subject has any permissions for.

This methodology relies on the discretion of the owner of the access control object to determine the access control subject's specific rights. Hence, security of the object is literally up to the discretion of the object owner. DACs are not very scalable; they rely on the access control decisions made by each individual object owner, and it can be difficult to find the source of access control issues when problems occur.

DAC in the Workplace

Most information systems are DAC systems. In a DAC system, a user who has access to a file is able to share that file with or pass it to someone else. It is at the discretion of the asset owner whether to grant or revoke access for a user. For access to computer files, this can be shared file or password protections. For example, if you create a file in an online file sharing platform you can restrict who sees it. That is up to your discretion. Or it may be something low-tech and temporary, such as a visitor's badge provided at the discretion of the worker at the security desk.

Mandatory Access Control (MAC)

A **mandatory access control (MAC)** policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system. In simplest terms, this means that only properly designated security administrators, as trusted subjects, can modify any of the security rules that are established for subjects and objects within the system. This also means that for all subjects defined by the organization (that is, known to its integrated identity management and access control system), the organization assigns a subset of total privileges for a subset of objects, such that the subject is constrained from doing any of the following:

Passing the information to unauthorized subjects or objects
Granting its privileges to other subjects
Changing one or more security attributes on subjects, objects, the information system or system components
Choosing the security attributes to be associated with newly created or modified objects
Changing the rules governing access control

Although MAC sounds very similar to DAC, the primary difference is who can control access. With Mandatory Access Control, it is mandatory for security administrators to assign access rights or permissions; with Discretionary Access Control, it is up to the object owner's discretion.

MAC in the Workplace

Mandatory access control is also determined by the owner of the assets, but on a more across-the-board basis, with little individual decision-making about who gets access.

For example, at certain government agencies, personnel must have a certain type of security clearance to get access to certain areas. In general, this level of access is set by government policy and not by an individual giving permission based on their own judgment.

Often this is accompanied by separation of duties, where your scope of work is limited and you do not have access to see information that does not concern you; someone else handles that information. This separation of duties is also facilitated by role-based access control, as we will discuss next.

Role-Based Access Control (RBAC)

Role-based access control (RBAC), as the name suggests, sets up user permissions based on roles. Each role represents users with similar or identical permissions.

Narrator: A role is created and assigned the access required for personnel working in that role. When a user takes on a job, the administrator assigns them to the appropriate role. If a user leaves that role, the administrator removes that user and then access for that user associated with that role is removed. RBAC works well in an environment with high staff turnover and multiple personnel with similar access requirements.

RBAC in the Workplace

Role-based access control provides each worker privileges based on what role they have in the organization. Only Human Resources staff have access to personnel files, for example; only Finance has access to bank accounts; each manager has access to their own direct reports and their own department. Very high-level system administrators may have access to everything; new employees would have very limited access, the minimum required to do their jobs.

Monitoring these role-based permissions is important, because if you expand one person's permissions for a specific reason—say, a junior worker's permissions might be expanded so they can temporarily act as the department manager—but you forget to change their permissions back when the new manager is hired, then the next person to come in at that junior level might inherit those permissions when it is not appropriate for them to have them. This is called privilege creep or permissions creep. We discussed this before, when we were talking about provisioning new users.

Having multiple roles with different combinations of permissions can require close monitoring to make sure everyone has the access they need to do their jobs and nothing more. In this world where jobs are ever-changing, this can sometimes be a challenge to keep track of, especially with extremely granular roles and permissions. Upon hiring or changing roles, a best practice is to not copy user profiles to new users. It is recommended that standard roles are established, and new users are created based on those standards rather than an actual user. That way, new employees start with the appropriate roles and permissions.

PODCAST

Chad Kliewer: All right. Good morning, good afternoon, or good evening, depending on where in the world you're listening from. Welcome to this discussion on access controls. I'm your host Chad Kliewer, holder of the CISSP and CCSP and current (ISC)2 member. And I'll be facilitating your experience today, and I'm extremely excited to welcome our special guest for today's discussion, Daisha Pennie, who's also a CISSP and an (ISC)2 member. And Daisha comes to us with more than 15 years of IT experience practicing within public state university. So, let's get started. So, we're going to start this discussion today on access control by defining what access control is in a simple way, and simply put, it's the process of permitting or restricting access to applications or data at a granular level such as per user, per group, or per resources. And Daisha, as you're aware, access control strategy and implementation is much more difficult in an organizational setting than really what it is in a textbook. It's a whole lot more difficult when we put those human connections in place. And that's what we want to try to do today. And we know that every employee needs enough access to do the job. And every time you give an employee more access it introduces more risk to the organization and to the systems. So how do you strike a balance in that?

Daisha Pennie: Well, I would definitely say, you know, the key word in your definition is process. It's all about processes. I think, you know, if you can identify the categories of your user base that's going to be the easiest way to build your process to have some access control. So, I think a lot of times there's this concern that you're going to get one to one, you're going to have each individual user's going to have their different access needs, and that creates a whole lot of burden and overhead for your administration to deal with. So, it's really about streamlining, which goes beyond your access control processes and into your organization, and making sure that everyone has an idea, like, 'This is how we define this role, and this is the access that that role needs.' So, it's kind of an organization wide issue.

Kliewer: But that's the overall goal. So, to our listeners, I hope you all have enjoyed this discussion. I know I definitely have, and again, many, many, many thanks to our special guest Daisha Pennie for volunteering to share her time and her experience with us today. Thank you very much.

Pennie: Happy to be here.

CHAPTER 3 TERMS AND DEFINITIONS

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. NIST SP 1800-15B
Crime Prevention through Environmental Design (CPTED) - An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.
Defense in Depth - Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. Source: NIST SP 800-53 Rev 4
Discretionary Access Control (DAC) - A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. NIST SP 800-192
Encrypt - To protect private information by putting it into a form that can only be read by people who have permission to do so.
Firewalls - Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.
Insider Threat - An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. NIST SP 800-32
iOS - An operating system manufactured by Apple Inc. Used for mobile devices.
Layered Defense - The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.
Linux - An operating system that is open source, making its source code legally available to end users.
Log Anomaly - A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.
Logging - Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks. NIST SP 1800-25B.
Logical Access Control Systems - An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different

individuals depending on their roles and responsibilities in an organization. NIST SP 800-53 Rev.5.

Mandatory Access Control - Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Mantrap - An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

Object - Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See subject. Source: NIST SP 800-53 Rev 4

Physical Access Controls - Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Principle of Least Privilege - The principle that users and programs should have only the minimum privileges necessary to complete their tasks. NIST SP 800-179

Privileged Account - An information system account with approved authorizations of a privileged user. NIST SP 800-53 Rev. 4

Ransomware - A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid.

Role-based access control (RBAC) - An access control system that sets up user permissions based on roles.

Rule - An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

Segregation of Duties - The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties.

Subject - Generally an individual, process or device causing information to flow among objects or change to the system state. Source: NIST SP800-53 R4

Technical Controls - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Turnstile - A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

Unix - An operating system used in software development.

User Provisioning - The process of creating, maintaining and deactivating user identities on a system.

NETWORK SECURITY

Understand computer networking

Manny: One of the biggest issues in cybersecurity is that computers are all linked together, sometimes by physical networks within a building, and almost always via the Internet, so it's easy for viruses and other threats to move rapidly through networks.

Tasha: That's right, and cyber threats and attacks are getting more sophisticated all the time. This aspect of cybersecurity is always evolving. Let's find out more.

What is Networking

A network is simply two or more computers linked together to share data, information or resources.

To properly establish secure data communications, it is important to explore all of the technologies involved in computer communications. From **hardware** and **software** to **protocols** and **encryption** and beyond, there are many details, standards and procedures to be familiar with.

Types of Networks

There are two basic types of networks:

Local area network (LAN) - A local area network (LAN) is a network typically spanning a single floor or building. This is commonly a limited geographical area.
Wide area network (WAN) - Wide area network (WAN) is the term usually assigned to the long-distance connections between geographically remote networks.

Network Devices

Hub

Hubs are used to connect multiple devices in a network. They’re less likely to be seen in business or corporate networks than in home networks. Hubs are wired devices and are not as smart as switches or routers.

Switch

Rather than using a hub, you might consider using a switch, or what is also known as an intelligent hub. Switches are wired devices that know the addresses of the devices connected to them and route traffic to that port/device rather than retransmitting to all devices.

Offering greater efficiency for traffic delivery and improving the overall throughput of data, switches are smarter than hubs, but not as smart as routers. Switches can also create separate **broadcast** domains when used to create **VLANs**, which will be discussed later.

Router

Routers are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between them. Routers can be wired or wireless and can connect multiple switches. Smarter than hubs and switches, routers determine the most efficient “route” for the traffic to flow across the network.

Firewall

Firewalls are essential tools in managing and controlling network traffic and protecting the network. A firewall is a network device used to filter traffic. It is typically deployed between a private network and the internet, but it can also be deployed between departments (segmented networks) within an organization (overall network). Firewalls filter traffic based on a defined set of rules, also called filters or access control lists.

Server

A server is a computer that provides information to other computers on a network. Some common servers are web servers, email servers, print servers, database servers and file servers. All of these are, by design, networked and accessed in some way by a client computer. Servers are usually secured differently than workstations to protect the information they contain.

Endpoint

Endpoints are the ends of a network communication link. One end is often at a server where a resource resides, and the other end is often a client making a request to use a network resource. An endpoint can be another server, desktop workstation, laptop, tablet, mobile phone or any other end user device.

Other Networking Terms

Ethernet

Ethernet (IEEE 802.3) is a standard that defines wired connections of networked devices. This standard defines the way data is formatted over the wire to ensure disparate devices can communicate over the same cables.

Device Address

Media Access Control (MAC) Address - Every network device is assigned a Media Access Control (MAC) address. An example is 00-13-02-1F-58-F5. The first 3 **bytes** (24 bits) of the address denote the vendor or manufacturer of the physical network

interface. No two devices can have the same MAC address in the same local network; otherwise an address conflict occurs.
Internet Protocol (IP) Address - While MAC addresses are generally assigned in the firmware of the interface, IP hosts associate that address with a unique logical address. This logical IP address represents the network interface within the network and can be useful to maintain communications when a physical device is swapped with new hardware. Examples are 192.168.1.1 and 2001:db8::ffff:0:1.

Networking at a Glance

This diagram represents a small business network, which we will build upon during this lesson. The lines depict wired connections. Notice how all devices behind the firewall connect via the network switch, and the firewall lies between the network switch and the internet.

The network diagram below represents a typical home network. Notice the primary difference between the home network and the business network is that the router, firewall, and network switch are often combined into one device supplied by your internet provider and shown here as the wireless access point.

Networking Models

Many different models, architectures and standards exist that provide ways to interconnect different hardware and software systems with each other for the purposes of sharing information, coordinating their activities and accomplishing joint or shared tasks.

Computers and networks emerge from the integration of communication devices, storage devices, processing devices, security devices, input devices, output devices, operating systems, software, services, data and people.

Translating the organization’s security needs into safe, reliable and effective network systems needs to start with a simple premise. The purpose of all communications is to exchange information and ideas between people and organizations so that they can get work done.

Those simple goals can be re-expressed in network (and security) terms such as:

Provide reliable, managed communications between hosts (and users)
Isolate functions in layers
Use **packets** as the basis of communication
Standardize routing, addressing and control
Allow layers beyond internetworking to add functionality
Be vendor-agnostic, scalable and resilient

In the most basic form, a network model has at least two layers:

Upper Layer/ host or application layer

The upper layer, also known as the host or application layer, is responsible for managing the integrity of a connection and controlling the session as well as establishing, maintaining and terminating communication sessions between two computers. It is also responsible for transforming data received from the Application Layer into a format that any system can understand. And finally, it allows applications to communicate and determines whether a remote communication partner is available and accessible.

Lower Layer or media or transport layer

The lower layer is often referred to as the media or transport layer and is responsible for receiving bits from the physical connection medium and converting them into a frame. Frames are grouped into standardized sizes. Think of frames as a bucket and the bits as water. If the buckets are sized similarly and the water is contained within the buckets, the data can be transported in a controlled manner. Route data is added to the frames of data to create packets. In other words, a destination address is added to the bucket. Once we have the buckets sorted and ready to go, the host layer takes over.

Open Systems Interconnection (OSI) Model

The OSI Model was developed to establish a common way to describe the communication structure for interconnected computer systems. The OSI model serves as an abstract framework, or theoretical model, for how protocols should function in an ideal world, on ideal hardware. Thus, the OSI model has become a common conceptual reference that is used to understand the communication of various hierarchical components from software interfaces to physical hardware.

The OSI model divides networking tasks into seven distinct layers. Each layer is responsible for performing specific tasks or operations with the goal of supporting data exchange (in other words, network communication) between two computers. The layers are interchangeably referenced by name or layer number. For example, Layer 3 is also known as the Network Layer. The layers are ordered specifically to indicate how information flows through the various levels of communication. Each layer communicates directly with the layer above and the layer below it. For example, Layer 3 communicates with both the Data Link (2) and Transport (4) layers.

The Application, Presentation, and Session Layers (5-7) are commonly referred to simply as data. However, each layer has the potential to perform encapsulation. **Encapsulation** is the addition of header and possibly a footer (trailer) data by a protocol used at that layer of the OSI model. Encapsulation is particularly important when discussing Transport, Network and Data Link layers (2-4), which all generally include some form of header. At the Physical Layer (1), the data unit is converted into binary, i.e., 01010111, and sent across physical wires such as an ethernet cable.

It's worth mapping some common networking terminology to the OSI Model so you can see the value in the conceptual model.

Consider the following examples:

When someone references an image file like a JPEG or PNG, we are talking about the Presentation Layer (6).
When discussing logical ports such as NetBIOS, we are discussing the Session Layer (5).
When discussing TCP/UDP, we are discussing the Transport Layer (4).
When discussing routers sending packets, we are discussing the Network Layer (3).
When discussing switches, bridges or WAPs sending frames, we are discussing the Data Link Layer (2).

Encapsulation occurs as the data moves down the OSI model from Application to Physical. As data is encapsulated at each descending layer, the previous layer's header, **payload** and footer are all treated as the next layer's payload. The data unit size increases as we move down the conceptual model and the contents continue to encapsulate.

The inverse action occurs as data moves up the OSI model layers from Physical to Application. This process is known as **de-encapsulation** (or decapsulation). The header and footer are used to properly interpret the data payload and are then discarded. As we move up the OSI model, the data unit becomes smaller. The encapsulation/de-encapsulation process is best depicted visually below:

Transmission Control Protocol/Internet Protocol (TCP/IP)

The OSI model wasn't the first or only attempt to streamline networking protocols or establish a common communications standard. In fact, the most widely used protocol today, **TCP/IP**, was developed in the early 1970s. The OSI model was not developed until the late 1970s. The TCP/IP protocol stack focuses on the core functions of networking.

TCP/IP Protocol Architecture Layers	
Application Layer	Defines the protocols for the transport layer.
Transport Layer	Permits data to move among devices.
Internet Layer	Creates/inserts packets.
Network Interface Layer	How data moves through the network.

The most widely used protocol suite is TCP/IP, but it is not just a single protocol; rather, it is a protocol stack comprising dozens of individual protocols. TCP/IP is a platform-independent protocol based on open standards. However, this is both a benefit and a drawback. TCP/IP can be found in just about every available operating system, but it consumes a significant amount of resources and is relatively easy to hack into because it was designed for ease of use rather than for security.

Transmission Control Protocol/Internet Protocol (TCP/IP)

At the Application Layer, TCP/IP protocols include Telnet, **File Transfer Protocol (FTP)**, **Simple Mail Transport Protocol (SMTP)**, and **Domain Name Service (DNS)**.

The two primary Transport Layer protocols of TCP/IP are TCP and UDP. TCP is a full-duplex connection-oriented protocol, whereas UDP is a simplex connectionless protocol. In the Internet Layer, **Internet Control Message Protocol (ICMP)** is used to determine the health of a network or a specific link. ICMP is utilized by ping, traceroute and other network management tools.

The ping utility employs ICMP echo packets and bounces them off remote systems. Thus, you can

use ping to determine whether the remote system is online, whether the remote system is responding promptly, whether the intermediary systems are supporting communications, and the level of performance efficiency at which the intermediary systems are communicating.

Internet Protocol (IPv4 and IPv6)

IP is currently deployed and used worldwide in two major versions. IPv4 provides a 32-bit address space, which by the late 1980s was projected to be exhausted. IPv6 was introduced in December 1995 and provides a 128-bit address space along with several other important features.

IP hosts/devices associate an address with a unique logical address. An IPv4 address is expressed as four octets separated by a dot (.), for example, 216.12.146.140. Each octet may have a value between 0 and 255. However, 0 is the network itself (not a device on that network), and 255 is generally reserved for broadcast purposes. Each address is subdivided into two parts: the network number and the host. The network number assigned by an external organization, such as the Internet Corporation for Assigned Names and Numbers (ICANN), represents the organization's network. The host represents the network interface within the network.
To ease network administration, networks are typically divided into subnets. Because subnets cannot be distinguished with the addressing scheme discussed so far, a separate mechanism, the subnet mask, is used to define the part of the address used for the subnet. The mask is usually converted to decimal notation like 255.255.255.0.
With the ever-increasing number of computers and networked devices, it is clear that IPv4 does not provide enough addresses for our needs. To overcome this shortcoming, IPv4 was sub-divided into public and private address ranges. Public addresses are limited with IPv4, but this issue was addressed in part with private addressing. Private addresses can be shared by anyone, and it is highly likely that everyone on your street is using the same address scheme.
The nature of the addressing scheme established by IPv4 meant that network designers had to start thinking in terms of IP address reuse. IPv4 facilitated this in several ways, such as its creation of the private address groups; this allows every LAN in every SOHO (small office, home office) situation to use addresses such as 192.168.2.xxx for its internal network addresses, without fear that some other system can intercept traffic on their LAN.

This table shows the private addresses available for anyone to use:

Range
10.0.0.0 to 10.255.255.254
172.16.0.0 to 172.31.255.254
192.168.0.0 to 192.168.255.254

The first octet of 127 is reserved for a computer's loopback address. Usually, the address 127.0.0.1 is used. The loopback address is used to provide a mechanism for self-diagnosis and troubleshooting at the machine level. This mechanism allows a network administrator to treat a local machine as if it were a remote machine and ping the network interface to establish whether it is operational.

IPv6 is a modernization of IPv4, which addressed a number of weaknesses in the IPv4 environment:

A much larger address field: IPv6 addresses are 128 bits, which supports 2128 or 340,282,366,920,938,463,463,374,607,431,768,211,456 hosts. This ensures that we will not run out of addresses.

Improved security: IPsec is an optional part of IPv4 networks, but a mandatory component of IPv6 networks. This will help ensure the integrity and confidentiality of IP packets and allow communicating partners to authenticate with each other.

Improved quality of service (QoS): This will help services obtain an appropriate share of a network's bandwidth.

An IPv6 address is shown as 8 groups of four digits. Instead of numeric (0-9) digits like IPv4, IPv6 addresses use the hexadecimal range (0000-ffff) and are separated by colons (:) rather than periods (.). An example IPv6 address is 2001:0db8:0000:0000:0000:ffff:0000:0001. To make it easier for humans to read and type, it can be shortened by removing the leading zeros at the beginning of each field and substituting two colons (::) for the longest consecutive zero fields. All fields must retain at least one digit. After shortening, the example address above is rendered as 2001:db8::ffff:0:1, which is much easier to type. As in IPv4, there are some addresses and ranges that are reserved for special uses:

::1 is the local loopback address, used the same as 127.0.0.1 in IPv4.
The range 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff is reserved for documentation use, just like in the examples above.
fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff are addresses reserved for internal network use and are not routable on the internet.

What is WiFi?

Wireless networking is a popular method of connecting corporate and home systems because of the ease of deployment and relatively low cost. It has made networking more versatile than ever before. Workstations and portable systems are no longer tied to a cable but can roam freely within the signal range of the deployed wireless access points. However, with this freedom comes additional vulnerabilities.

Wi-Fi range is generally wide enough for most homes or small offices, and range extenders may be placed strategically to extend the signal for larger campuses or homes. Over time the Wi-Fi standard has evolved, with each updated version faster than the last.

In a LAN, threat actors need to enter the physical space or immediate vicinity of the physical media itself. For wired networks, this can be done by placing sniffer taps onto cables, plugging in USB devices, or using other tools that require physical access to the network. By contrast, wireless media intrusions can happen at a distance.

Security of the Network

TCP/IP's vulnerabilities are numerous. Improperly implemented TCP/IP stacks in various operating systems are vulnerable to various **DoS/DDoS attacks**, **fragment attacks**, **oversized packet attacks**, **spoofing attacks**, and **man-in-the-middle attacks**.

TCP/IP (as well as most protocols) is also subject to passive attacks via monitoring or sniffing. Network monitoring, or sniffing, is the act of monitoring traffic patterns to obtain information about a network.

Ports and Protocols (Applications/Services)

There are physical ports that you connect wires to and logical ports that determine where the data/traffic goes.

Physical ports
Physical ports are the ports on the routers, switches, servers, computers, etc. that you connect the wires, e.g., fiber optic cables, Cat5 cables, etc., to create a network.

Logical ports

When a communication connection is established between two systems, it is done using ports. A logical port (also called a socket) is little more than an address number that both ends of the communication link agree to use when transferring data. Ports allow a single IP address to be able to support multiple simultaneous communications, each using a different port number. In the Application Layer of the TCP/IP model (which includes the Session, Presentation, and Application Layers of the OSI model) reside numerous application- or service-specific protocols. Data types are mapped using port numbers associated with services. For example, web traffic (or HTTP) is port 80. Secure web traffic (or HTTPS) is port 443. Table 5.4 highlights some of these protocols and their customary or assigned ports. You'll note that in several cases a service (or protocol) may have two ports assigned, one secure and one insecure. When in doubt, systems should be implemented using the most secure version as possible of a protocol and its services.

Well-known ports (0–1023): These ports are related to the common protocols that are at the core of the Transport Control Protocol/Internet Protocol (TCP/IP) model, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc.
Registered ports (1024–49151): These ports are often associated with proprietary applications from vendors and developers. While they are officially approved by the Internet Assigned Numbers Authority (IANA), in practice many vendors simply implement a port of their choosing. Examples include Remote Authentication Dial-In User Service (RADIUS) authentication (1812), Microsoft SQL Server (1433/1434) and the Docker REST API (2375/2376).
Dynamic or private ports (49152–65535): Whenever a service is requested that is associated with well-known or registered ports, those services will respond with a dynamic port that is used for that session and then released.

Secure Ports

Some network protocols transmit information in clear text, meaning it is not encrypted and should not be used. Clear text information is subject to network sniffing. This tactic uses software to inspect packets of data as they travel across the network and extract text such as usernames and passwords. Network sniffing could also reveal the content of documents and other files if they are sent via insecure protocols. The table below shows some of the insecure protocols along with recommended secure alternatives.

Insecure port	description	protocol	secure altve port	protocol
21 - FTP	Port 21, File Transfer Protocol (FTP) sends the username and password using plaintext from the client to the server. This could be intercepted by an attacker and later used to retrieve confidential information from the server. The secure alternative, SFTP, on port 22 uses encryption to protect the user credentials and packets of data being transferred.	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol

25 - SMTP	Port 25, Simple Mail Transfer Protocol (SMTP) is the default unencrypted port for sending email messages. Since it is unencrypted, data contained within the emails could be discovered by network sniffing. The secure alternative is to use port 587 for SMTP using Transport Layer Security (TLS) which will encrypt the data between the mail client and the mail server.	Simple Mail Transfer Protocol	587 - SMTP	SMTP with TLS

23 - Telnet	Port 23, telnet, is used by many Linux systems and any other systems as a basic text-based terminal. All information to and from the host on a telnet connection is sent in plaintext and can be intercepted by an attacker. This includes username and password as well as all information that is being presented on the screen, since this interface is all	Telnet	22* - SSH	Secure Shell

	text. Secure Shell (SSH) on port 22 uses encryption to ensure that traffic between the host and terminal is not sent in a plaintext format.			

37 - Time	Port 37, Time Protocol, may be in use by legacy equipment and has mostly been replaced by using port 123 for Network Time Protocol (NTP). NTP on port 123 offers better error-handling capabilities, which reduces the likelihood of unexpected errors.	Time Protocol	123 - NTP	Network Time Protocol

53 - DNS	Port 53, Domain Name Service (DNS), is still used widely. However, using DNS over TLS (DoT) on port 853 protects DNS information from being modified in transit.	Domain Name Service	853 - DoT	DNS over TLS (DoT)

80 - HTTP	Port 80, HyperText Transfer Protocol (HTTP) is the basis of nearly all web browser traffic on the internet. Information sent via HTTP is not encrypted and is susceptible to sniffing attacks. HTTPS using TLS encryption is preferred, as it protects the data in transit between the server and the browser. Note that this is often notated as SSL/TLS. Secure Sockets Layer (SSL) has been compromised is no longer considered secure. It is now recommended for web servers and clients to use Transport Layer Security (TLS) 1.3 or higher for the best protection.	HyperText Transfer Protocol	443 - HTTPS	HyperText Transfer Protocol (SSL/TLS)

143 - IMAP	Port 143, Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing. The secure alternative is to use port 993 for IMAP, which adds SSL/TLS security to encrypt the data between the mail client and the mail server.	Internet Message Access Protocol	993 - IMAP	IMAP for SSL/TLS

161/162 - SNMP	Ports 161 and 162, Simple Network Management Protocol, are commonly used to send and receive data used for managing infrastructure devices. Because sensitive information is often included in these messages, it is recommended to use SNMP version 2 or 3 (abbreviated SNMPv2 or SNMPv3) to include encryption and additional security features. Unlike	Simple Network Management Protocol	161/162 - SNMP	SNMPv3

	many others discussed here, all versions of SNMP use the same ports, so there is not a definitive secure and insecure pairing. Additional context will be needed to determine if information on ports 161 and 162 is secured or not.			

445 - SMB	Port 445, Server Message Block (SMB), is used by many versions of Windows for accessing files over the network. Files are transmitted unencrypted, and many vulnerabilities are well-known. Therefore, it is recommended that traffic on port 445 should not be allowed to pass through a firewall at the network perimeter. A more secure alternative is port 2049, Network File System (NFS). Although NFS can use encryption, it is recommended that	Server Message Block	2049 - NFS	Network File System

	NFS not be allowed through firewalls either.			

389 - LDAP	Port 389, Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from servers to clients. This can be an address book for email or usernames for logins. The LDAP protocol also allows records in the directory to be updated, introducing additional risk. Since LDAP is not encrypted, it is susceptible to sniffing and manipulation attacks. Lightweight Directory Access Protocol Secure (LDAPS) adds SSL/TLS security to protect the information while it is in transit.	Lightweight Directory Access Protocol	636 - LDAPS	Lightweight Directory Access Protocol Secure

SYN, SYN-ACK, ACK Handshake

Narrator: Between the client and the server, there is a system for synchronizing and acknowledging any request that is known as a three-way handshake. This handshake is used to establish a TCP connection between two devices.

Here, we will take a simplified look at how communications are established to a web server. Depending on the exact protocol, there may be additional connection negotiation taking place.

First, the client sends synchronization (SYN) packet to the web server's port 80 or 443. This is a request to establish a connection.

The web server replies to the SYN packet with an acknowledgement known as a SYN/ACK.

Finally, the client acknowledges the connection with an acknowledgement (ACK). At this point, the basic connection is established, and the client and host will further negotiate secure communications over that connection.

Understand Network (Cyber) Threats and Attacks

Chad Kliewer: I'll say greetings and welcome to the discussion on cyberattacks. I'm your host, Chad Kliewer, holder of a CISSP and CCSP, and current $(ISC)_2$ member. I'll be facilitating our experience. And I'm extremely excited to welcome our special guest, Joe Sullivan, CISSP, and also an $(ISC)_2$ member. Joe's a former CISO in the banking and finance industry, who now specializes in forensics, incident response and recovery. So, Joe, you ready to get started?

Joe Sullivan: I am looking forward to this. I'm excited.
Kliewer: All right. Anything else you'd like to add about your background? I didn't give you much

opportunity to do that.

Sullivan: Just a brief overview. I've been in information security for 2 years now in various aspects as you've mentioned.

Kliewer: Okay, awesome. Thank you much. So, I'm going to dive right into some content here. Because part of what we're trying to do is we're trying to look at how we prevent attacks, and then once those attacks happen, how they really impact the business and how they impact the companies. We all hear about these attacks constantly, but we never really look so much at how they impact each individual business. So, we're going to start out just talking a little bit and say, if we can't detect any future ongoing attack, how are we going to remediate that, and how are we going to stop it? And the one point we want to make here is how important it is to make sure that

we're aggregating all that data using this Security Information Event Management system or SIEM, S-I-E-M. And what are your thoughts on using a SIEM to make actional intelligence, Joe?

Sullivan: Integrating a SIEM for actionable intelligence, I think you have to take a step back and think about, when do we trigger incident response, typically? Over the course of my career, incident response is usually triggered after something bad happens. They're on the network, or we see and exploit, or we've been compromised or there's a knock on the door that says, Hey, your data's out there. If we have a SIEM or user behavior analytics, whatever the case may be properly optimized and tuned, we can pick up on those indicators of compromise before the bad things happen. And when I say indicators of compromise, I'm referring to things like scanning, malicious email attachments, web application, enumeration and things like that. Attackers spend the majority of their time in the recon phase. If we can detect those recon activities, that's actionable intelligence where we can block IPs, block tools and things like that before they actually get on the network. Even once they get on a network, recon still takes place. I get on a machine, what's the vendor? What software am I running on this machine? What applications are installed? What's the network look like? And still, we're not to the point where a breach is actually taking place yet. Again, if we're detecting an activity in our SIEM with the appropriate logging, monitoring and alerting, we can trigger incident response well before the actual breach takes place.

Kliewer: So, what are your thoughts on the actionable intelligence and how we prevent threats? Do you think most of the threats or most of the, well, we'll say incidents, are actually detected by internal systems, or do you think they're mostly the result of receiving the indicators of compromise from a third-party organization, such as a government entity or something like that?

Sullivan: If you look at as far as detection, we have events determining what's malicious and what's just an event or a false positive is the challenge here. When you have lean running security teams, who don't have the time to go in and tune and optimize this (but then again, something is better than nothing) a well operationalized security program with the appropriate headcount has the chance of detecting these and getting those alerts and indicators of compromise and acting on those earlier; whereas, if you have a lean running program (a two- to three-headcount security department that are wearing many different hats) it's a little bit more challenging to tune and optimize that. It's in scenarios like that where it might be beneficial to outsource that to a third-party SOC or something, and let them say, “Hey, we've detected this going on in your network, it doesn't look like a false positive, you should go check this out.”

Kliewer: Awesome. So, I'm going to paraphrase a little bit and read between the lines and say that I didn't hear one thing in there about, ‘You need to buy this software product to detect all the incidents.’

Sullivan: You don't really need to buy a software product to detect all the incidents. You know, if you look at like the CIS controls in this CSF, this cybersecurity framework, or even this 853, if you implement those and get your logs where you just have some visibility into them monitoring something, you can detect these. It doesn't really need to have a high-dollar SIEM or something like that. Network segmentation, we'll look at that. Host-based firewalls does a lot of good for limiting the impact of an incident.

Kliewer: Okay, awesome. So now I want to kind of roll that just a little bit more, and we kind of talked about that that's more the processes to log retention, so do you think what we've talked about so far still holds true when it's cloud-based software products or even cloud-based, and I'm going to say cloud-based SIEM, like a lot of them are?

Sullivan: The concept still holds true, right? We still want to aggregate the logs. The challenging cloud is the threat surface is a little bit different. I have all these different authentication portals and command line tools that can be used in public cloud services. And your threat model is things like permissions and IAM—identity and access management—if you don't have the appropriate permissions set up, you don't know what a user can do (like in some cases with a particular public cloud service I won't name) if you have a certain permission where you can actually roll back permissions, but you're limited, you can actually roll back your own policy and do something where you had permission at an earlier date, but you don't now. It's those little gotchas like that that you need to be aware of. And then there is provisioning cloud services,

depending on how you provision certain virtual machines, RDP and SSH is enabled by default facing the internet, so you want to be aware of what's the context of if I provision that here or from the command line tool?

The logging, monitoring, and alerting, you can have a cloud-based SIEM third party, or a lot of public cloud providers have their own tools. It's a little bit different approach, a little bit different aggregating those logs and reading them, setting up the alerts, so there might be a learning curve there. And then there's things like the instance metadata service, which if you get in contact with that, you can actually—it's like getting all the metadata on your VMs, your hosts, your disk drives, your backups and things like that, and gives you a wealth of information. And we're seeing older attacks like server-side request forgery coming back. In the Capital One breach a while back in a public cloud service, we've seen that take place. And there's various controls and mitigations they put in place to mitigate the IMDS attacks, and you need to be aware of what those are and how you can prevent those from happening. So, it's a little bit different, a little bit more comprehensive. It's not the same as your traditional on-prem resources, so there's a learning curve going through there. It's a little bit more challenging at first, but I think overall, it's the same approach, you just have a different way of implementing it.

Kliewer: Awesome. So, thanks for answering that. Since you mentioned the recent Capital One breach that involved the cloud service, can you kind of give our listeners an overview, we'll say about a 15,000-foot view of that breach and what happened?

Sullivan: The Capital One breach was actually an insider threat. They actually had access to this system, had worked with it before, and the instance metadata service—so you hit the web application, which caused a URL on the back end to get data, allocate resources, authentication and things like that. Like say, you have data in an S3 bucket, you can actually hit that IMDS and get that information back. That server-side request forgery attack let that person enumerate those resources and get access to them and download them. So, they had to go back and determine, "Well, how can we prevent this from happening?" And implemented things like now you need a token to send to the IMDS to actually get that information back, or we're going to limit the response

from the IMDS into one hop, that way it doesn't go past the machine out to the internet. So, an attacker can't actually get that.

Kliewer: Okay. Awesome. Thanks for covering that for us. I want to shift gears just a little bit, and we're talking about an attack here that involved some cloud components, but not necessarily in the cloud. And I wanted to talk just a little bit, because it was such a widespread incident—I mean, it can be called a cyberattack, we'll call it an incident with SolarWinds—it was one that was very widespread, gained a lot of notoriety because it was one that affected a lot of US government agencies, and I'm guessing probably a lot of other government agencies as well. And this was a very good example of a supply chain attack, where some malicious code or malicious programs were embedded within the supply chain or within an update package. So,

would you like to kind of lead us through a little bit, Joe, and just once again at a real high level of what steps that SolarWinds attack really took? I'm going to preface it by saying the reason it has such a huge impact was because it went undetected for so long. It went undetected, I think for at least, I'm going to say at least six to eight months that we know of, possibly quite longer. But if you could give our listeners an overview of that SolarWinds attack and how they actually utilized the cloud components.

Sullivan: Sure, no problem there. SolarWinds was a really, really clever attack. The initial foothold, we're not sure. They gained access to the internal network. We don't know if it was a spear phishing attack. There had also been rumor that a password was leaked as well. It could have been someone had set up a site for a watering hole attack. However, they did it, once they got access to the network, they focused on the build server where the actual code is compiled. And instead of actually implementing their malicious code in the build process, in the build, they coded as the output of the build process, that way it got packaged in and signed with the SolarWind software. They took that approach because, one, it keeps them off the radar for code scanning and code review. They're not going to see that code. And once they get signed, it's trusted at that point. So, once they got pushed out to the update server, all these individual companies who were running Orion SolarWinds download that, it gets on their network, but the attack didn't start or that malware didn't trigger for two weeks. And once it started triggering, it communicated with cloud resources where they set up their C2 network with AWS, GCP, Azure, GoDaddy and services like that and actually mimicked the Orion syntax. So, it looked like regular Orion traffic going back and forth. And that gave them access to the network. They could read email, obtain documents. They even got certificates where they could impersonate users. And it wasn't detected for a long time. It was a really sophisticated attack. They were very patient, and this was a really crafty attack.

Kliewer: Awesome. And just to point out there, because I want to point out in a little bit for our listeners and our learners in our courses that we've talked about some of these different components. I think we talked about C2, the command and control, which is what they're actually using to actually go back and obtain that information out of the host networks once they're compromised. And the fact that these command-and-control networks were propagated or stored in not just one cloud network infrastructure, but they used multiple cloud infrastructures and multiple cloud providers to do this, and all of that stuff helped them evade detection basically. So, like I said, I wanted to point that out a little bit. And I can tell you as one person who was part of an

organization, who was named in that SolarWinds attack, and one of the initial organizations that were listed as compromised—I'm going to back this up to our SIEM conversation earlier and say that SIEM was absolutely priceless in showing us that, yes, we did establish the initial communication with their command and control, but nothing happened past that point. We can show beyond a shadow of a doubt that we did not exfiltrate data, that there was no other data that went back and forth between our internal network and that command-and-control service. So that's where that whole SIEM ties into it.

So, Joe, I wanted to talk about one other thing, which I know is one of those areas that's kind of near and dear to your heart as a hacker kind of guy, not to use that in a negative component, but I'd like to hear your thoughts on threat hunting versus pen testing, vulnerability scanning, and malicious actors. I mean, how do you know the difference between somebody that's out there doing threat hunting or vulnerability assessment across the internet versus somebody who's a real malicious actor or a real threat?

Sullivan: Well, I think when you look at threat hunting, pen testing and vulnerability scanning, if you're doing it internally, obviously you know this is happening. If you're a third-party performing this for another organization, obviously you're doing it with permission so they're aware of it; whereas if you see these activities taking place, then you haven't given anyone permission, they're not going on internally, you have bigger issues. And these are often used interchangeably today. Threat hunting, in my mind, in my experience is I'm actually going to look at my network and act like there's a potential attacker here, we've been breached and we're going to treat it like that. We're going to look at our business-critical systems. We're going to capture memory. We're going to do packet captures. We're looking for indicators of compromise to see if do we actually have a bad actor on the network? This is beneficial because of your attack dwell time, right? You don't always detect the attacker immediately. Hopefully you do, but usually there's four to six weeks or something like that where they're on the network. This helps shorten that time period if you perform regular threat hunting. Whereas pen testing, I want to know, can you actually get into my network? Is it possible to compromise my software, my configurations, my people? Can you get access into the building? And that tells you, like I say, people ask me, what do you do? Well, I hack networks and break into buildings to keep people from hacking networks and breaking into buildings. If you have a good idea of how this takes place, you can better shore up your defenses in those particular areas. Vulnerability scanning is something every organization should be doing. I'm running regular scans with whatever vulnerability scanner you like that fits into your particular context, that identifies these vulnerabilities as they take place or as they get released and you can set up a remediation plan to patch those.

Kliewer: Awesome. I think that is a great breakdown of those different pieces. So, I'm trying to figure out here if we have any other questions. And I want to take just a couple minutes here to—I want to roll back a little bit, and it's not so much in a cloud context, but still help define some of the rules and regulations we have in place today. But what I wanted to do, Joe, is I want to back up and talk a little bit about the T.J. Maxx incident. Happened quite a few years back, and I think it's probably used in a lot of textbooks. But there was an incident with T.J. Maxx, or basically, somebody was able to access their networks and use network sniffers, you name it, to siphon off

credit card numbers, flowing from their front-end systems to their backend systems, and then turn around and sell those numbers on the dark web, you name it. Does that about sum that up? Do you have a better summary of it?

Sullivan: Yeah, this one's going way back aways, right? The T.J. Maxx hack is, if I remember right, was primarily, the initial foothold was they had an unsecured wireless network. Once they got on that wireless network, there was no network segmentation, so they were able to move freely. I think they got 94 million people or so credit cards. It was a huge breach, but yes, that's basically from a high level, what the T.J. Maxx attack was.

Kliewer: Awesome. And the reason I bring that up, because I wanted talk about that for our listeners a little bit, because everybody's also familiar with the PCI DSS or the Payment Card Industry Data Security Standards. And ultimately, that was one of the incidents and one of the cyberattacks that really led up to that PCI rule. And I want to be clear. It is a rule, not necessarily a regulation or a law, it's something that's set forth by industry. I mean, what are the pieces that PCI covers, Joe? I heard you mention several causes of that T.J. Maxx incident. Can you help us connect the dots between that incident and PCI?

Sullivan: Sure. Just to kind of step back and kind of recap what you were saying about PCI, a lot of times, it's misstated that this is a regulation or a law. It's actually a contractual obligation between you and the credit card companies. And the credit card companies got together and did all this because they wanted to avoid government regulation. So, they said, “Hey, we actually police ourselves, we don't need you to get in our business here.” So, they came up with PCI. The T.J. Maxx incident impacted PCI. They looked at what happened at T.J. Maxx, and they said, “You know what? You really need to better secure your wireless networks and need to be separate from your regular network, and your systems, actually whole PCI data, those have to be segmented. They have to have network access control as well. And you need to use the appropriate encryption to encrypt all this in transit and at rest.” And so, we came up with more strict PCI requirements, and you get into the network segmentation. And you don't want to apply PCI to all your resources, right. on the network (your systems, your servers, your devices) because then everything has to be PCI compliant. The secret to becoming PCI compliant is narrowing the scope, applying it just to those credit card related systems. There was something else on that one too. Just totally train crashed there. Oh, they also recommend using a higherlevel agnostic security or control framework, and then scoping down to your PCI system. So, then you're looking at something like the CIS controls or this cyber security framework as well.

Kliewer: All right. And I think that's a great point to make there is regardless of what country you are or geolocation, whatever, the PCI pretty much applies worldwide, but there are other frameworks and other tools you can use depending on your geographic location that can help implement those same regulations and rules, and I think that's a great connection to make there. And all right, I want to kind of start wrapping things up here just a little bit, Joe. Are there any other real last minute or overarching things that you'd like to talk about on the attack surface or what you'd like our listeners to know when it comes to the cyberattacks and what happens out there?

Sullivan: I think I'm going to sound like a broken record on this one, right? It still goes back to doing those basic things like you see in the CIS controls. Notice where you're at with asset inventory, know what assets you have, know what are business-critical assets, know where the crown jewels are, segment those, appropriate logging, monitoring, alerting, patch management, vulnerability scanning. In fact, it was June of last year, the White House actually came out with a document that said, these are the things you should be doing to protect your information security program—regular backups, penetration testing, vulnerability management. These things still hold true. And that was very much a watershed event. I don't remember a time where the White House actually came out and said, “Hey, this is what you needed to do to secure your network.” Why did they do that? Because you see organizations like SolarWinds getting government organizations breached, and you see the Colonial Pipeline, which is supplying oil to the United States, and the meat packing processing plant, which also got ransomware at that time—provides food and meat to people in the US. It's where these incidents, these cyber events and these ransomware attacks aren't just affecting individual companies now, they're affecting people across the nation when you get to this level. So that really changed the criticality of what you need to be doing to secure your network. And you see, CISA came out with supply chain guidelines to protect your organization against those. I guess what I'm getting at is do the basics and determine what your context is. Do I need to focus on supply chain? Do I need to focus on vulnerability scanning, penetration testing—are my backups in place? And take care of the basics and build on top of that.

Kliewer: Awesome, great advice, Joe. And I want to take just a moment here. To our listeners, I hope you've enjoyed this discussion. I hope you found this useful, and I hope you found it helpful as the official training that you've been taking. And again, I want to offer many, many, many thanks to our special guest, Joe Sullivan for volunteering his time to share his experience with us.

Sullivan: Oh, good to be here, Chad, I enjoyed it. Good conversation.

Types of Threats

There are many types of cyber threats to organizations. Below are several of the most common types:

Spoofing

An attack with the goal of gaining access to a target system through the use of a falsified identity. Spoofing can be used against IP addresses, MAC address, usernames, system names, wireless network SSIDs, email addresses, and many other types of logical identificatio

Phishing

An attack that attempts to misdirect legitimate users to malicious websites through the abuse of URLs or hyperlinks in emails could be considered phishing.

DoS/DDoS

A denial-of-service (DoS) attack is a network resource consumption attack that has the primary goal of preventing legitimate activity on a victimized system. Attacks involving numerous unsuspecting secondary victim systems are known as distributed denial-of-service (DDoS) attacks.

Virus

The computer virus is perhaps the earliest form of malicious code to plague security administrators. As with biological viruses, computer viruses have two main functions—propagation and destruction. A virus is a self-replicating piece of code that spreads without the consent of a user, but frequently with their assistance (a user has to click on a link or open a file).

Worm

Worms pose a significant risk to network security. They contain the same destructive potential as other malicious code objects with an added twist—they propagate themselves without requiring any human intervention.

Trojan

Named after the ancient story of the Trojan horse, the Trojan is a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network. For example, ransomware often uses a Trojan to infect a target machine and then uses encryption technology to encrypt documents, spreadsheets and other files stored on the system with a key known only to the malware creator.

On-path attack

In an on-path attack, attackers place themselves between two devices, often between a web browser and a web server, to intercept or modify information that is intended for one or both of the endpoints. On-path attacks are also known as man-in-the-middle (MITM) attacks.

Side-channel

A side-channel attack is a passive, noninvasive attack to observe the operation of a device. Methods include power monitoring, timing and fault analysis attacks.

Advanced persistent threat

Advanced persistent threat (APT) refers to threats that demonstrate an unusually high level of technical and operational sophistication spanning months or even years. APT attacks are often conducted by highly organized groups of attackers.

Insider threat

Insider threats are threats that arise from individuals who are trusted by the organization. These could be disgruntled employees or employees involved in espionage. Insider threats are not always willing participants. A trusted user who falls victim to a scam could be an unwilling insider threat.

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system or otherwise annoying or disrupting the victim.

Ransomeware

Malware used for the purpose of facilitating a ransom attack. Ransomware attacks often use cryptography to "lock" the files on an affected computer and require the payment of a ransom fee in return for the "unlock" code.

A viral threat

Tasha: Before her shift starts, Gabriela attempts to upload a school assignment on her iPad, but the device is not responding.

Gabriela: Ugh, why is nothing working? This stupid thing. I need to turn in this assignment. *Keith:* What is it?
Gabriela: It just spins and spins.
Keith: Have you updated recently?

Gabriela: Yes.
Keith: Have you clicked on any new links?

Gabriela: Oh, no. That strange email from the other day! It said I won a gift certificate, but when I clicked the link, it didn't go anywhere.

Keith: It's okay. Sounds like you have a virus though. But we can ask Susan for help. Have you backed it up to the cloud?

Gabriela: I have.
Keith: Great, everything will be all right then.

Identify Threats and Tools Used to Prevent Them

So far in this chapter, we have explored how a TCP/IP network operates, and we have seen some examples of how threat actors can exploit some of the inherent vulnerabilities. The remainder of this module will discuss the various ways these network threats can be detected and even prevented.

While there is no single step you can take to protect against all attacks, there are some basic steps you can take that help to protect against many types of attacks.

Here are some examples of steps that can be taken to protect networks.

> If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system.
> Firewalls can prevent many different types of attacks. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems.

Narrator: This table lists tools used to identify threats that can help to protect against many types of attacks, like virus and malware, Denial of Service attacks, spoofing, on-path and side- channel attacks. From monitoring activity on a single computer, like with HIDS, to gathering log data, like with SIEM, to filtering network traffic like with firewalls, these tools help to protect entire networks and individual systems.

These tools, which we will cover more in depth, all help to identify potential threats, while anti-malware, firewall and intrusion protection system tools also have the added ability to prevent threats.

Intrusion Detection System (IDS)

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resources. Intrusion detection is a specific form of monitoring that monitors recorded information and real-time events to detect abnormal activity indicating a potential incident or intrusion. An intrusion detection system (IDS) automates the inspection of logs and real-time system events to detect intrusion attempts and system failures. An IDS is intended as part of a defense-in-depth security plan. It will work with, and complement, other security mechanisms such as firewalls, but it does not replace them. IDSs can recognize attacks that come from external connections, such as an attack from the internet, and attacks that spread internally, such as a malicious worm. Once they detect a suspicious event, they respond by sending alerts or raising alarms. A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions.
Intrusion detection and prevention refer to capabilities that are part of isolating and protecting a more secure or more trusted domain or zone from one that is less trusted or less secure. These are natural functions to expect of a firewall, for example.
IDS types are commonly classified as host-based and network-based. A host-based IDS (HIDS) monitors a single computer or host. A network-based IDS (NIDS) monitors a network by observing network traffic patterns.

NOTE: **Identify.** An Intrusion Detection System helps to identify threats, but does not have the capability to prevent them.

Host-based Intrusion Detection System (HIDS)

A HIDS monitors activity on a single computer, including process calls and information recorded in system, application, security and host-based firewall logs. It can often examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack. It can also track processes employed by the attacker. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect. For example, a HIDS can detect infections where an intruder has infiltrated a system and is controlling it remotely. HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration. A HIDS cannot detect network attacks on other systems.

NOTE: **Identify.** A Host Intrusion Detection System helps to identify threats to a host system, but does not prevent them.

Network Intrusion Detection System (NIDS)

A NIDS monitors and evaluates network activity to detect attacks or event anomalies. It cannot monitor the content of encrypted traffic but can monitor other packet details. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console. These sensors can monitor traffic at routers, firewalls, network switches that support port mirroring, and other types of network taps. A NIDS has very little negative effect on the overall network performance, and when it is deployed on a single-purpose system, it doesn't adversely affect performance on any other computer. A NIDS is usually able to detect the initiation of an attack or ongoing attacks, but they can't always provide information about the success of an attack. They won't know if an attack affected specific systems, user accounts, files or applications.

NOTE: **Identify.** A Network Intrusion Detection System helps to identify threats based on network traffic, but does not prevent them.

Security Information and Event Management (SIEM)

Security management involves the use of tools that collect information about the IT environment from many disparate sources to better examine the overall security of the organization and streamline security efforts. These tools are generally known as security information and event management (or S-I-E-M, pronounced "SIM") solutions. The general idea of a SIEM solution is to gather log data from various sources across the enterprise to better understand potential security concerns and apportion resources accordingly.

SIEM systems can be used along with other components (defense-in-depth) as part of an overall information security program.

NOTE: **Identify.** A Security Incident and Event Management system identifies threats by correlating and storing logs from multiple systems, but does not take action to prevent the threats from materializing.

Identifying threats

Narrator: Here we see an example of an Intrusion Detection System (IDS) alert. This is being provided as an example of how threats are identified, Some of the concepts in this scenario are more advanced than this course, so don't be alarmed if you don't understand everything discussed here.

We'll start by reviewing the main points of the data that is presented to us. Note that in this example, the hostname and username fields have been removed to maintain anonymity.

This tells us that the IDS detected the use of software called Advanced IP Scanner that can be used by attackers to enumerate, or look through the network, scanning addresses to see what services are running on the computers in the local network. This software is also used by network or system administrators to inventory a local network for troubleshooting purposes. Finally, this top section of the alert screen tells us that the event was reported by an endpoint agent, meaning that it was generated by a Host Intrusion Detection System (HIDS) solution, not a Network Intrusion Detection System (NIDS).

This line identifies the host that is running the suspicious process as a Windows system.

This process section identifies the start time, process name and ID (or pid) number that correlates to the process in the Windows Task Manager. This can be helpful in a couple of ways. First, the start time tells us how long the process has been running. The pid can also give some clues, as lower pid numbers may indicate a process that started running during the boot sequence and higher numbers indicate something that was started much later.

These lines give us the details of the executable file, including the path to the file itself as well as the actual command line that was used to run the executable. These are important contextually as they show the program executed from a Temp folder under the user's ID, which typically does not require administrative privileges in a Windows system. In other words, they could be run by any average user. The command line used shows additional context, including that the application is running as a portable application, meaning that it doesn't have to be formally installed on the machine to execute.

In this case, there is not enough context to really know if this process is being used in a malicious manner. Like many security alerts, this one relies on some human interaction, so you should contact the end user assigned to this asset to inquire whether they are, in fact, running this software and if they have a legitimate business reason to do so. If you discover that this was intended, it might be a good place to explain to that you were alerted because this legitimate

software can be used by threat actors to conduct reconnaissance on the local network to determine where there might be weaknesses to exploit.

Preventing Threats

While there is no single step you can take to protect against all threats, there are some basic steps you can take that help reduce the risk of many types of threats.

Keep systems and applications up to date. Vendors regularly release patches to correct bugs and security flaws, but these only help when they are applied. Patch management ensures that systems and applications are kept up to date with relevant patches.

Remove or disable unneeded services and protocols. If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system. As an extreme contrast, imagine a web server is running every available service and protocol. It is vulnerable to potential attacks on any of these services and protocols.

Use intrusion detection and prevention systems. As discussed, intrusion detection and prevention systems observe activity, attempt to detect threats and provide alerts. They can often block or stop attacks.

Use up-to-date anti-malware software. We have already covered the various types of malicious code such as viruses and worms. A primary countermeasure is anti-malware software.

Use firewalls. Firewalls can prevent many different types of threats. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems. This chapter included a section describing how firewalls can prevent attacks.

Antivirus

The use of antivirus products is strongly encouraged as a security best practice and is a requirement for compliance with the **Payment Card Industry Data Security Standard (PCI DSS)**. There are several antivirus products available, and many can be deployed as part of an enterprise solution that integrates with several other security products.

Antivirus systems try to identify malware based on the signature of known malware or by detecting abnormal activity on a system. This identification is done with various types of scanners, pattern recognition and advanced machine learning algorithms.

Anti-malware now goes beyond just virus protection as modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware. Many endpoint solutions also include software firewalls and IDS or IPS systems.

NOTE: **Both.** Anti-malware/Antivirus helps to both identify and prevent threats by identifying malicious software and stopping the processes before they fully execute.

Scans

Here is an example scan from **Zenmap** showing open ports on a host.

Regular vulnerability and port scans are a good way to evaluate the effectiveness of security controls used within an organization. They may reveal areas where patches or security settings are insufficient, where new vulnerabilities have developed or become exposed, and where security policies are either ineffective or not being followed. Attackers can exploit any of these vulnerabilities.

NOTE: **Identify.** Scans help to identify threats, often by conducting a vulnerability analysis, and may suggest action to mitigate the threats, but does not prevent them.

Firewalls

In building construction or vehicle design, a firewall is a specially built physical barrier that prevents the spread of fire from one area of the structure to another or from one compartment of a vehicle to another. Early computer security engineers borrowed that name for the devices and services that isolate network segments from each other, as a security measure. As a result, firewalling refers to the process of designing, using or operating different processes in ways that isolate high-risk activities from lower-risk ones.

Firewalls enforce policies by filtering network traffic based on a set of rules. While a firewall should always be placed at internet gateways, other internal network considerations and conditions determine where a firewall would be employed, such as network zoning or segregation of different levels of sensitivity. Firewalls have rapidly evolved over time to provide enhanced security capabilities. This growth in capabilities can be seen in Figure 5.37, which contrasts an oversimplified view of traditional and next-generation firewalls. It integrates a variety of threat management capabilities into a single framework, including proxy services, intrusion prevention services (IPS) and tight integration with the identity and access management (IAM) environment to ensure only authorized users are permitted to pass traffic across the infrastructure. While firewalls can manage traffic at Layers 2 (MAC addresses), 3 (IP ranges) and 7 (**application programming interface (API)** and application firewalls), the traditional implementation has been to control traffic at Layer 4.

NOTE: **Both.** Most modern firewalls both identify and prevent threats by automatically adjusting rules to block malicious traffic from entering a secured network.

Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) is a special type of active IDS that automatically attempts to detect and block attacks before they reach target systems. A distinguishing difference between an IDS and an IPS is that the IPS is placed in line with the traffic. In other words, all traffic must pass through the IPS and the IPS can choose what traffic to forward and what traffic to block after analyzing it. This allows the IPS to prevent an attack from reaching a target. Since IPS systems are most effective at preventing network-based attacks, it is common to see the IPS function integrated into firewalls. Just like IDS, there are Network-based IPS (NIPS) and Host-based IPS (HIPS).

NOTE: **Both.** Intrusion Prevention Systems both identify and prevent threats.

Manny: In this section, we are going to be exploring the concepts and terminology around data centers and the cloud. Sounds exciting!

Tasha: It can be, Manny. This is where a lot of the future applications of cybersecurity will come from. As threats evolve, so does the technology to improve data protection, wherever that data is stored and however it's transmitted.

On-Premises Data Centers

When it comes to data centers, there are two primary options: organizations can outsource the data center or own the data center. If the data center is owned, it will likely be built on premises. A place, like a building for the data center is needed, along with power, HVAC, fire suppression and redundancy

Fire Suppression

For server rooms, appropriate fire detection/suppression must be considered based on the size of the room, typical human occupation, egress routes and risk of damage to equipment. For example, water used for fire suppression would cause more harm to servers and other electronic components. Gas-based fire suppression systems are more friendly to the electronics, but can be toxic to humans.

Power

Data centers and information systems in general consume a tremendous amount of electrical power, which needs to be delivered both constantly and consistently. Wide fluctuations in the quality of power affect system lifespan, while disruptions in supply completely stop system operations.

Power at the site is always an integral part of data center operations. Regardless of fuel source, backup generators must be sized to provide for the critical load (the computing resources) and the supporting infrastructure. Similarly, battery backups must be properly sized to carry the critical load until generators start and stabilize. As with data backups, testing is necessary to ensure the failover to alternate power works properly.

Heating, Ventilation and Air Conditioning (HVAC) / Environmental

High-density equipment and equipment within enclosed spaces requires adequate cooling and airflow. Well-established standards for the operation of computer equipment exist, and equipment is tested against these standards. For example, the recommended range for optimized maximum uptime and hardware life is from 64° to 81°F (18° to 27°C), and it is recommended that a rack have three temperature sensors, positioned at the top, middle and bottom of the rack, to measure the actual operating temperature of the environment. Proper management of data center temperatures, including cooling, is essential.

Cooling is not the only issue with airflow: Contaminants like dust and noxious fumes require appropriate controls to minimize their impact on equipment. Monitoring for water or gas leaks, sewer overflow or HVAC failure should be integrated into the building control environment, with appropriate alarms to signal to organizational staff. Contingency planning to respond to the warnings should prioritize the systems in the building, so the impact of a major system failure on people, operations or other infrastructure can be minimized.

Data Center/Closets

The facility wiring infrastructure is integral to overall information system security and reliability. Protecting access to the physical layer of the network is important in minimizing intentional or unintentional damage. Proper protection of the physical site must address these sorts of security challenges. Data centers and wiring closets may include the following:

Phone, network, special connections
ISP or telecommunications provider equipment
Servers
Wiring and/or switch components

Deeper Dive of On-Premises Data Centers

Narrator: Now that we have looked at some of the primary components that must be considered when building an on-premises data center, we should take a deeper dive into some of the components.

First, we consider the air conditioning requirements of a data center. Servers and other equipment generate a lot of heat which must be handled appropriately. This is not just to make it comfortable when humans are present, but to ensure the equipment is kept within its operating parameters. When equipment gets too hot, it can lead to quicker failure or a voided warranty. Most equipment is programmed to automatically shut down when a certain temperature threshold is met. This helps to protect the equipment, but a system that is shut down is not available to the users. An abnormal system shutdown can also lead to the loss or corruption of data.

Another consideration for the on-premises data center is the fire suppression systems. In the United States, most commercial buildings are required to have sprinkler systems that are activated in a fire. These sprinklers minimize the amount of damage caused to the building and keep the fire from spreading to adjacent areas, but they can be detrimental to electronic equipment, as water and electricity don’t mix. While most water-based fire suppression systems don’t work like they do in the movies, where a fire in one part of the building turns on the sprinklers for the entire building, another hazard is having water overhead in a data center. Eventually, water pipes will fail and may leak on equipment. This risk can be reduced somewhat by using a dry-pipe system that keeps the water out of the pipes over the data center. These systems have a valve outside the data center

that is only opened when a sensor indicates a fire is present. Since water is not held in the pipes above the data center, the risk of leaks is reduced.

Redundancy

The concept of redundancy is to design systems with duplicate components so that if a failure were to occur, there would be a backup. This can apply to the data center as well. Risk assessments pertaining to the data center should identify when multiple separate utility service entrances are necessary for redundant communication channels and/or mechanisms.

If the organization requires full redundancy, devices should have two power supplies connected to diverse power sources. Those power sources would be backed up by batteries and generators. In a high-availability environment, even generators would be redundant and fed by different fuel types.

Narrator: In addition to keeping redundant backups of information, you also have a redundant source of power, to provide backup power so you have an uninterrupted power supply, or UPS. Transfer switches or transformers may also be involved. And in case the power is interrupted by weather or blackouts, a backup generator is essential. Often there will be two generators connected by two different transfer switches. These generators might be powered by diesel or gasoline or another fuel such as propane, or even by solar panels. A hospital or essential government agency might contract with more than one power company and be on two different grids in case one goes out. This is what we mean by redundancy.

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)

Some organizations seeking to minimize downtime and enhance BC (Business Continuity) and DR (Disaster Recovery) capabilities will create agreements with other, similar organizations. They agree that if one of the parties experiences an emergency and cannot operate within their own facility, the other party will share its resources and let them operate within theirs in order to maintain critical functions. These agreements often even include competitors, because their facilities and resources meet the needs of their particular industry.

For example, Hospital A and Hospital B are competitors in the same city. The hospitals create an agreement with each other: if something bad happens to Hospital A (a fire, flood, bomb threat, loss of power, etc.), that hospital can temporarily send personnel and systems to work inside Hospital B in order to stay in business during the interruption (and Hospital B can relocate to Hospital A, if Hospital B has a similar problem). The hospitals have decided that they are not going to compete based on safety and security—they are going to compete on service, price and customer loyalty. This way, they protect themselves and the healthcare industry as a whole.

These agreements are called joint operating agreements (JOA) or memoranda of understanding (MOU) or memoranda of agreement (MOA). Sometimes these agreements are mandated by regulatory requirements, or they might just be part of the administrative safeguards instituted by an entity within the guidelines of its industry.

The difference between an MOA or MOU and an SLA is that a Memorandum of Understanding is more directly related to what can be done with a system or the information.

The service level agreement goes down to the granular level. For example, if I'm outsourcing the IT services, then I will need to have two full-time technicians readily available, at least from Monday through Friday from eight to five. With cloud computing, I need to have access to the information in my backup systems within 10 minutes. An SLA specifies the more intricate aspects of the services.

We must be very cautious when outsourcing with cloud-based services, because we have to make sure that we understand exactly what we are agreeing to. If the SLA promises 100 percent accessibility to information, is the access directly to you at the moment, or is it access to their website or through their portal when they open on Monday? That's where you'll rely on your legal team, who can supervise and review the conditions carefully before you sign the dotted line at the bottom

Cloud

Cloud computing is usually associated with an internet-based set of computing resources, and typically sold as a service, provided by a cloud service provider (CSP).

Cloud computing is very similar to the electrical or power grid. It is provisioned in a geographic location and is sourced using an electrical means that is not necessarily obvious to the consumer. But when you want electricity, it’s available to you via a common standard interface and you pay only for what you use. In these ways, cloud computing is very similar. It is a very scalable, elastic and easy-to-use “utility” for the provisioning and deployment of Information Technology (IT) services.

There are various definitions of what cloud computing means according to the leading standards, including NIST. This NIST definition is commonly used around the globe, cited by professionals and others alike to clarify what the term “cloud” means:

“a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” NIST SP 800-145

This image depicts cloud computing characteristics, service and deployment models, all of which will be covered in this section and by your instructor.

Narrator: Many organizations have moved from hard-wired server rooms to operations that are run by cloud-based facilities, because it provides both security and flexibility. Cloud service providers have different availability zones, so that if one goes down, activities can shift to another. You don't have to maintain a whole data center with all the redundancy that entails – the cloud service provider does that for you.

There are several ways to contract with a cloud service provider. You can set up the billing so that it depends on the data used, just like your mobile phone. And you have resource pooling, meaning you can share in the resources of other colleagues or similar types of industries to provide data for artificial intelligence or analytics.

Cloud Characteristics

Cloud-based assets include any resources that an organization accesses using cloud computing. Cloud computing refers to on-demand access to computing resources available from almost anywhere, and cloud computing resources are highly available and easily scalable. Organizations typically lease cloud-based resources from outside the organization. Cloud computing has many benefits for organizations, which include but are not limited to:

Usage is metered and priced according to units (or instances) consumed. This can also be billed back to specific departments or functions.
Reduced cost of ownership. There is no need to buy any assets for everyday use, no loss of asset value over time and a reduction of other related costs of maintenance and support.
Reduced energy and cooling costs, along with "green IT" environment effect with optimum use of IT resources and systems.
Allows an enterprise to scale up new software or data-based services/solutions through cloud systems quickly and without having to install massive hardware locally.

Service Models

Some cloud-based services only provide data storage and access. When storing data in the cloud, organizations must ensure that security controls are in place to prevent unauthorized access to the data.

There are varying levels of responsibility for assets depending on the service model. This includes maintaining the assets, ensuring they remain functional, and keeping the systems and applications up to date with current patches. In some cases, the cloud service provider is responsible for these steps. In other cases, the consumer is responsible for these steps.

Types of cloud computing service models include **Software as a Service (SaaS)** , **Platform as a Service (PaaS)** and **Infrastructure as a Service (IaaS)**.

Software as a Service (SaaS)

Software as a Service (SaaS): A cloud provides access to software applications such as email or office productivity tools. SaaS is a distributed model where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources. SaaS is a widely used and adopted form of cloud computing, with users most often needing an internet connection and access credentials to have full use of the cloud service, application and data. SaaS has many benefits for organizations, which include but are not limited to: Ease of use and limited/minimal administration. Automatic updates and patch management. The user will always be running the latest version and most up-to-date deployment of the software release, as well as any relevant security updates, with no manual patching required. Standardization and compatibility. All users will have the same version of the software release.

Platform as a Service (PaaS)

Platform as a Service (PaaS): A cloud provides an environment for customers to use to build and operate their own software. PaaS is a way for customers to rent hardware, operating systems, storage and network capacity over the internet from a cloud service provider. The service delivery model allows customers to rent virtualized servers and associated services for running existing applications or developing and testing new ones. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application-hosting environment configurations. A PaaS cloud provides a toolkit for conveniently developing, deploying and administering application software that is structured to support large numbers of consumers, process very large quantities of data and potentially be accessed from any point on the internet. PaaS clouds will typically provide a set of software building blocks and a set of development tools such as programming languages and supporting run-time environments that facilitate the construction of high-quality, scalable applications. Additionally, PaaS clouds will typically provide tools that assist with the deployment of new applications. In some cases, deploying a new software application in a PaaS cloud is not much more difficult than uploading a file to a web server. PaaS clouds will also generally provide and maintain the computing resources (e.g., processing, storage and networking) that consumer applications need to operate. PaaS clouds provide many benefits for developers, including that the operating system can be changed and upgraded frequently, along with associated features and system services.

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS): A cloud provides network access to traditional computing resources such as processing power and storage. IaaS models provide basic computing resources to consumers. This includes servers, storage, and in some cases, networking resources. Consumers install operating systems and applications and perform all required maintenance on the operating systems and applications. Although the consumer has use of the related equipment, the cloud service provider retains ownership and is ultimately responsible for hosting, running and maintenance of the hardware. IaaS is also referred to as hardware as a service by some customers and providers. IaaS has a number of benefits for organizations, which include but are not limited to: Ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure. Retain system control at the operating system level.

Deployment Models

There are four cloud deployment models. The cloud deployment model also affects the breakdown of responsibilities of the cloud-based assets. The four cloud models available are **public**, **private**, **hybrid** and **community** .

Public

Public clouds are what we commonly refer to as the cloud for the public user. It is very easy to get access to a public cloud. There is no real mechanism, other than applying for and paying for the cloud service. It is open to the public and is, therefore, a shared resource that many people will be able to use as part of a resource pool. A public cloud deployment model includes assets available for any consumers to rent or lease and is hosted by an external cloud service provider (CSP). Service level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization.

Private

Private clouds begin with the same technical concept as public clouds, except that instead of being shared with the public, they are generally developed and deployed for a private organization that builds its own cloud. Organizations can create and host private clouds using their own resources. Therefore, this deployment model includes cloud-based assets for a single organization. As such, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party and split maintenance requirements based on the service model (SaaS, PaaS or IaaS). Private clouds provide organizations and their departments private access to the computing, storage, networking and software assets that are available in the private cloud.

Hybrid

A hybrid cloud deployment model is created by combining two forms of cloud computing deployment models, typically a public and private cloud. Hybrid cloud computing is gaining popularity with organizations by providing them with the ability to retain control of their IT environments, conveniently allowing them to use public cloud service to fulfill non-mission-critical workloads, and taking advantage of flexibility, scalability and cost savings. Important drivers or benefits of hybrid cloud deployments include: Retaining ownership and oversight of critical tasks and processes related to technology, Reusing previous investments in technology within the organization, Control over most critical business components and systems, and Cost-effective means to fulfilling noncritical business functions (utilizing public cloud components).

Community

Community clouds can be either public or private. What makes them unique is that they are generally developed for a particular community. An example could be a public community cloud focused primarily on organic food, or maybe a community cloud focused specifically on financial services. The idea behind the community cloud is that people of like minds or similar interests can

get together, share IT capabilities and services, and use them in a way that is beneficial for the particular interests that they share.

Managed Service Provider (MSP)

A managed service provider (MSP) is a company that manages information technology assets for another company. Small- and medium-sized businesses commonly outsource part or all of their information technology functions to an MSP to manage day-to-day operations or to provide expertise in areas the company does not have. Organizations may also use an MSP to provide network and security monitoring and patching services. Today, many MSPs offer cloud-based services augmenting SaaS solutions with active incident investigation and response activities. One such example is a managed detection and response (MDR) service, where a vendor monitors firewall and other security tools to provide expertise in triaging events.

Some other common MSP implementations are:

Augment in-house staff for projects
Utilize expertise for implementation of a product or service
Provide payroll services
Provide Help Desk service management
Monitor and respond to security incidents
Manage all in-house IT infrastructure

Service-Level Agreement (SLA)

The cloud computing service-level agreement (cloud SLA) is an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing– specific terms to set the quality of the cloud services delivered. It characterizes quality of the cloud services delivered in terms of a set of measurable properties specific to cloud computing (business and technical) and a given set of cloud computing roles (cloud service customer, cloud service provider, and related sub-roles).

Think of a rule book and legal contract—that combination is what you have in a service-level agreement (SLA). Let us not underestimate or downplay the importance of this document/ agreement. In it, the minimum level of service, availability, security, controls, processes, communications, support and many other crucial business elements are stated and agreed to by both parties.

The purpose of an SLA is to document specific parameters, minimum service levels and remedies for any failure to meet the specified requirements. It should also affirm data ownership and specify data return and destruction details. Other important SLA points to consider include the following:

Cloud system infrastructure details and security standards
Customer right to audit legal and regulatory compliance by the CSP
Rights and costs associated with continuing and discontinuing service use
Service availability

Service performance
Data security and privacy
Disaster recovery processes
Data location
Data access
Data portability
Problem identification and resolution expectations
Change management processes
Dispute mediation processes
Exit strategy

Network Design

The objective of network design is to satisfy data communication requirements and result in efficient overall performance.

Network segmentation

Network segmentation involves controlling traffic among networked devices. Complete or physical network segmentation occurs when a network is isolated from all outside communications, so transactions can only occur between devices within the segmented network.

Demilitarized zone (DMZ)

A DMZ is a network area that is designed to be accessed by outside visitors but is still isolated from the private network of the organization. The DMZ is often the host of public web, email, file and other resource servers.

Virtual local area network VLAN

VLANs are created by switches to logically segment a network without altering its physical topology.

Virtual private network VPN
A virtual private network (VPN) is a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network.

Defense in depth
Defense in depth uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security stance.

Network access control

Network access control (NAC) is a concept of controlling access to an environment through strict adherence to and implementation of security policy.

Defense in Depth

Defense in depth uses a layered approach when designing the security posture of an organization. Think about a castle that holds the crown jewels. The jewels will be placed in a vaulted chamber in a central location guarded by security guards. The castle is built around the vault with additional layers of security—soldiers, walls, a moat. The same approach is true when designing the logical security of a facility or system. Using layers of security will deter many attackers and encourage them to focus on other, easier targets.

Defense in depth provides more of a starting point for considering all types of controls—administrative, technological, and physical—that empower insiders and operators to work together to protect their organization and its systems.

Here are some examples that further explain the concept of defense in depth:

Data: Controls that protect the actual data with technologies such as encryption, data leak prevention, identity and access management and data controls.
Application: Controls that protect the application itself with technologies such as data leak prevention, application firewalls and database monitors.
Host: Every control that is placed at the endpoint level, such as antivirus, endpoint firewall, configuration and patch management.
Internal network: Controls that are in place to protect uncontrolled data flow and user access across the organizational network. Relevant technologies include intrusion detection systems, intrusion prevention systems, internal firewalls and network access controls.
Perimeter: Controls that protect against unauthorized access to the network. This level includes the use of technologies such as gateway firewalls, honeypots, malware analysis and secure demilitarized zones (DMZs).
Physical: Controls that provide a physical barrier, such as locks, walls or access control.
Policies, procedures and awareness: Administrative controls that reduce insider threats (intentional and unintentional) and identify risks as soon as they appear.

Zero Trust

Zero trust networks are often microsegmented networks, with firewalls at nearly every connecting point. Zero trust encapsulates information assets, the services that apply to them and their security properties. This concept recognizes that once inside a trust-but-verify environment, a user has perhaps unlimited capabilities to roam around, identify assets and systems and potentially find exploitable vulnerabilities. Placing a greater number of firewalls or other security boundary control devices throughout the network increases the number of opportunities to detect a troublemaker before harm is done. Many enterprise architectures are pushing this to the extreme of microsegmenting their internal networks, which enforces frequent re-authentication of a user ID, as depicted in this image.

Consider a rock music concert. By traditional perimeter controls, such as firewalls, you would show your ticket at the gate and have free access to the venue, including backstage where the real rock stars are. In a zero-trust environment, additional checkpoints are added. Your identity (ticket) is validated to access the floor level seats, and again to access the backstage area. Your credentials must be valid at all 3 levels to meet the stars of the show.

Zero trust is an evolving design approach which recognizes that even the most robust access control systems have their weaknesses. It adds defenses at the user, asset and data level, rather than relying on perimeter defense. In the extreme, it insists that every process or action a user attempts to take must be authenticated and authorized; the window of trust becomes vanishingly small.

While **microsegmentation** adds internal perimeters, zero trust places the focus on the assets, or data, rather than the perimeter. Zero trust builds more effective gates to protect the assets directly rather than building additional or higher walls.

Network Access Control (NAC)

An organization's network is perhaps one of its most critical assets. As such, it is vital that we both know and control access to it, both from insiders (e.g., employees, contractors) and outsiders (e.g., customers, corporate partners, vendors). We need to be able to see who and what is attempting to make a network connection.

At one time, network access was limited to internal devices. Gradually, that was extended to remote connections, although initially those were the exceptions rather than the norm. This started to change with the concepts of bring your own device (BYOD) and Internet of Things (IoT).

Considering just IoT for a moment, it is important to understand the range of devices that might be found within an organization. They include heating, ventilation and air conditioning (HVAC) systems that monitor the ambient temperature and adjust the heating or cooling levels automatically or air monitoring systems, through security systems, sensors and cameras, right down to vending and coffee machines. Look around your own environment and you will quickly see the scale of their use.

Having identified the need for a NAC solution, we need to identify what capabilities a solution may provide. As we know, everything begins with a policy. The organization's access control policies and associated security policies should be enforced via the NAC device(s). Remember, of course, that an access control device only enforces a policy and doesn't create one.

The NAC device will provide the network visibility needed for access security and may later be used for incident response. Aside from identifying connections, it should also be able to provide isolation for noncompliant devices within a quarantined network and provide a mechanism to "fix" the noncompliant elements, such as turning on endpoint protection. In short, the goal is to ensure that all devices wishing to join the network do so only when they comply with the requirements laid out in the organization policies. This visibility will encompass internal users as well as any temporary users such as guests or contractors, etc., and any devices they may bring with them into the organization.

Let's consider some possible use cases for NAC deployment:

Medical devices
IoT devices
BYOD/mobile devices (laptops, tablets, smartphones)
Guest users and contractors

Deep dive in NAC

As we have established, it is critically important that all mobile devices, regardless of their owner, go through an onboarding process, ideally each time a network connection is made, and that the device is identified and interrogated to ensure the organization's policies are being met.

Narrator: At its simplest form, Network Access Control, or NAC, is a way to prevent unwanted devices from connecting to a network. Some NAC systems allow for the installation of required software on the end user's device to enforce device compliance to policy prior to connecting.
A high-level example of a NAC system is hotel internet access. Typically, a user connecting to the hotel network is required to acknowledge the acceptable use policy before being allowed to access the internet. After the user clicks the acknowledge button, the device is connected to the network that enables internet access. Some hotels add an additional layer requiring the guest to enter a special password or a room number and guest name before access is granted. This prevents abuse by someone who is not a hotel guest and may even help to track network abuse to a particular user.

A slightly more complex scenario is a business that separates employee BYOD devices from corporate-owned devices on the network. If the BYOD device is pre-approved and allowed to connect to the corporate network, the NAC system can validate the device using a hardware address or installed software, and even check to make sure the antivirus software and operating system software are up to date before connecting it to the network. Alternatively, if it is a personal device not allowed to connect to the corporate network, it can be redirected to the guest network for internet access without access to internal corporate resources.

Network Segmentation (Demilitarized Zone (DMZ))

Network segmentation is also an effective way to achieve defense in depth for distributed or multi-tiered applications. The use of a demilitarized zone (DMZ), for example, is a common practice in security architecture. With a DMZ, host systems that are accessible through the firewall are physically separated from the internal network by means of secured switches or by using an additional firewall to control traffic between the web server and the internal network. Application DMZs (or semi-trusted networks) are frequently used today to limit access to application servers to those networks or systems that have a legitimate need to connect.

DMZ deeper dive

Narrator: A web front end server might be in the DMZ, but it might retrieve data from a database server that is on the other side of the firewall.

For example, you may have a network where you manage your client's personal information, and even if the data is encrypted or obfuscated by cryptography, you need to make sure the network is completely segregated from the rest of the network with some secure switches that only an authorized individual has access to. Only authorized personnel can control the firewall settings and control the traffic between the web server and the internal network. For example, in a hospital or a doctor's office, you would have a segregated network for the patient information and billing, and on the other side would be the electronic medical records. If they are using a web-based application for medical record services, they would have a demilitarized zone or segmented areas. And perhaps even behind the firewall, they have their own specified server to protect the critical information and keep it segregated.

It is worth noting at this point that while this course will not explore the specifics, some networks use a web application firewall (WAF) rather than a DMZ network. The WAF has an internal and an external connection like a traditional firewall, with the external traffic being filtered by the traditional or next generation firewall first. It monitors all traffic, encrypted or not, from the outside for malicious behavior before passing commands to a web server that may be internal to the network.

Segmentation for Embedded Systems and IoT

An embedded system is a computer implemented as part of a larger system. The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it is a component. Examples of embedded systems include network-attached printers, smart TVs, HVAC controls, smart appliances, smart thermostats and medical devices.

Network-enabled devices are any type of portable or nonportable device that has native network capabilities. This generally assumes the network in question is a wireless type of network, typically provided by a mobile telecommunications company. Network-enabled devices include smartphones, mobile phones, tablets, smart TVs or streaming media players (such as a Roku Player, Amazon Fire TV, or Google Android TV/Chromecast), network-attached printers, game systems, and much more.

The Internet of Things (IoT) is the collection of devices that can communicate over the internet with one another or with a control console in order to affect and monitor the real world. IoT devices might be labeled as smart devices or smart-home equipment. Many of the ideas of industrial environmental control found in office buildings are finding their way into more consumer-available solutions for small offices or personal homes.

Embedded systems and network-enabled devices that communicate with the internet are considered IoT devices and need special attention to ensure that communication is not used in a malicious manner. Because an embedded system is often in control of a mechanism in the physical world, a security breach could cause harm to people and property. Since many of these devices have multiple access routes, such as ethernet, wireless, Bluetooth, etc., special care should be taken to isolate them from other devices on the network. You can impose logical network segmentation with switches using VLANs, or through other traffic-control means, including MAC addresses, IP addresses, physical ports, protocols, or application filtering, routing, and access control management. Network segmentation can be used to isolate IoT environments.

Segmentation for embedded systems and ioT deeper dive

Narrator: The characteristics that make embedded systems operate efficiently are also a security risk. Embedded systems are often used to control something physical, such as a valve for water, steam, or even oil. These devices have a limited instruction set and are often hard- coded or permanently written to a memory chip. For ease of operating the mechanical parts, the embedded system is often connected to a corporate network since and may operate using the TCP/IP protocol, yes, the same protocol that runs all over the internet. Therefore, it is feasible for anyone anywhere on the internet to control the opening and closing of a valve when the networks are fully connected. This is the primary reason for segmentation of these systems on a network. If these are segmented properly, a compromised corporate network will not be able to access the physical controls on the embedded systems.

The other side of the embedded systems, which also applies to IoT devices, is the general lack of system updates when a new vulnerability is found. In the case of most embedded systems with the programming directly on the chips, it would require physical replacement of the chip to patch the vulnerability. For many systems, it may not be cost-effective to have someone visit each one to replace a chip, or manually connect to the chip to re-program it.

We buy all these internet connected things because of the convenience. Cameras, light bulbs, speakers, refrigerators, etc. all bring some sort of convenience to our lives, but they also introduce risk. While the reputable mainstream brands will likely provide updates to their devices when a new vulnerability is discovered, many of the smaller companies simply don’t plan to do that as they seek to control the costs of a device. These devices, when connected to a corporate network, can be an easy internet-connected doorway for a cyber criminal to access a corporate network. If these devices are properly segmented, or separated, on the network from corporate servers and other corporate networking, a compromise on an IoT device or a compromised embedded system will not be able to access those corporate data and systems.

Microsegmentation

The toolsets of current adversaries are polymorphic in nature and allow threats to bypass static security controls. Modern cyberattacks take advantage of traditional security models to move easily between systems within a data center. Microsegmentation aids in protecting against these threats. A fundamental design requirement of microsegmentation is to understand the protection requirements for traffic within a data center and traffic to and from the internet traffic flows.

When organizations avoid infrastructure-centric design paradigms, they are more likely to become more efficient at service delivery in the data center and become apt at detecting and preventing advanced persistent threats.

Microsegmentation deeper dive

Narrator: Some key points about microsegmentation:

Microsegmentation allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users, and these rules can be as detailed and complex as desired. For instance, we can limit which IP addresses can communicate to a given machine, at which time of day, with which credentials, and which services those connections can utilize.

These are logical rules, not physical rules, and do not require additional hardware or manual interaction with the device (that is, the administrator can apply the rules to various machines without having to physically touch each device or the cables connecting it to the networked environment).

This is the ultimate end state of the defense-in-depth philosophy; no single point of access within the IT environment can lead to broader compromise.

This is crucial in shared environments, such as the cloud, where more than one customer’s data and functionality might reside on the same device(s), and where third-party personnel (administrators/technicians who work for the cloud provider, not the customer) might have physical access to the devices.

Microsegmentation allows the organization to limit which business functions/units/offices/departments can communicate with others, in order to enforce the concept of least privilege. For instance, the Human Resources office probably has employee data that no other business unit should have access to, such as employee home address, salary, medical records, etc. Microsegmentation, like VLANs, can make HR its own distinct IT enclave, so that sensitive data is not available to other business entities, thus reducing the risk of exposure.

In modern environments, microsegmentation is available because of virtualization and software-defined networking (SDN) technologies. In the cloud, the tools for applying this strategy are often called “virtual private networks (VPN)” or "security groups.”
Even in your home, microsegmentation can be used to separate computers from smart TVs, air conditioning, and smart appliances which can be connected and can have vulnerabilities.

Virtual Local Area Network (VLAN)

Virtual local area networks (VLANs) allow network administrators to use switches to create software-based LAN segments, which can segregate or consolidate traffic across multiple switch ports. Devices that share a VLAN communicate through switches as if they were on the same Layer 2 network. This image shows different VLANs — red, green and blue — connecting separate sets of ports together, while sharing the same network segment (consisting of the two switches and their connection). Since VLANs act as discrete networks, communications between VLANs must be enabled. Broadcast traffic is limited to the VLAN, reducing congestion and reducing the effectiveness of some attacks. Administration of the environment is simplified, as the VLANs can be reconfigured when individuals change their physical location or need access to different services. VLANs can be configured based on switch port, IP subnet, MAC address and protocols.

VLANs do not guarantee a network's security. At first glance, it may seem that traffic cannot be intercepted because communication within a VLAN is restricted to member devices. However, there are attacks that allow a malicious user to see traffic from other VLANs (so-called VLAN hopping). The VLAN technology is only one tool that can improve the overall security of the network environment.

Narrator: VLANS are virtual separations within a switch and are used mainly to limit broadcast traffic. A VLAN can be configured to communicate with other VLANs or not, and may be used to segregate network segments.

There are a few common uses of VLANs in corporate networks. The first is to separate Voice Over IP (VOIP) telephones from the corporate network. This is most often done to more effectively manage the network traffic generated by voice communications by isolating it from the rest of the network.

Another common use of VLANs in a corporate network is to separate the data center from all other network traffic. This makes it easier to keep the server-to-server traffic contained to the data center network while allowing certain traffic from workstations or the web to access the servers. As briefly discussed earlier, VLANs can also be used to segment networks. For example, a VLAN can separate the payroll workstations from the rest of the workstations in the network. Routing rules can also be used to only allow devices within this Payroll VLAN to access the servers containing payroll information.

Earlier, we also discussed Network Access Control (NAC). These systems use VLANs to control whether devices connect to the corporate network or to a guest network. Even though a wireless access controller may attach to a single port on a physical network switch, the VLAN associated with the device connection on the wireless access controller determines the VLAN that the device operates on and to which networks it is allowed to connect.

Finally, in large corporate networks, VLANs can be used to limit the amount of broadcast traffic within a network. This is most common in networks of more than 1,000 devices and may be separated by department, location/building, or any other criteria as needed.

The most important thing to remember is that while VLANs are logically separated, they may be allowed to access other VLANs. They can also be configured to deny access to other VLANs.

Virtual Private Network (VPN)

A **virtual private network** (VPN) is not necessarily an encrypted tunnel. It is simply a point-to-point connection between two hosts that allows them to communicate. Secure communications can, of course, be provided by the VPN, but only if the security protocols have been selected and correctly configured to provide a trusted path over an untrusted network, such as the internet. Remote users employ VPNs to access their organization's network, and depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. As an alternative to expensive dedicated point-to-point connections, organizations use

gateway-to-gateway VPNs to securely transmit information over the internet between sites or even with business partners.

Chapter 4 terms and definitions

Application programming interface (API) - A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

Bit - The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model.

Broadcast - Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

Byte - The byte is a unit of digital information that most commonly consists of eight bits.

Cloud computing - A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST 800-145

Community cloud - A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. NIST 800-145

De-encapsulation - The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

Denial-of-Service (DoS) - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) Source: NIST SP 800-27 Rev A

Domain Name Service (DNS) - This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

Encapsulation - Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.

Encryption - The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

File Transfer Protocol (FTP) - The internet protocol (and program) used to transfer files between hosts.

Fragment attack - In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

Hardware - The physical parts of a computer and related devices.

Hybrid cloud - A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise’s private cloud while other data is stored and accessible from a public cloud storage provider.

Infrastructure as a Service (IaaS) - The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.
Internet Control Message Protocol (ICMP) - An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.
Internet Protocol (IPv4) - Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. CNSSI 4009-2015
Man-in-the-Middle - An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. Source: NISTIR 7711
Microsegmentation - Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places firewall at every connection point.
Oversized Packet Attack - Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly.
Packet - Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.
Payload - The primary action of a malicious code attack.
Payment Card Industry Data Security Standard (PCI DSS) - An information security standard administered by the Payment Card Industry Security Standards Council that applies to merchants and service providers who process credit or debit card transactions.
Platform as a Service (PaaS) - The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.
Private cloud - The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.
Protocols - A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems. NIST SP 800-82 Rev. 2
Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. NIST SP 800-145
Simple Mail Transport Protocol (SMTP) - The standard communication protocol for sending and receiving emails between senders and receivers.
Software - Computer programs and associated data that may be dynamically written or modified during execution. NIST SP 80-37 Rev. 2

Software as a Service (SaaS) - The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Derived from NIST 800-145

Spoofing - Faking the sending address of a transmission to gain illegal entry into a secure system. CNSSI 4009-2015

Transport Control Protocol/Internet Protocol (TCP/IP) Model - Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data between hosts), and Application Layer, where other protocols and user applications programs make use of network services.

Virtual Local Area Network (VLAN) - A logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.

VPN - A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks.

Wireless Area Network (WLAN) - A group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi is network is a type of WLAN.

Zenmap - The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information.

Zero Trust - Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.

UNDERSTAND DATA SECURITY

Manny: It's hard to imagine the sheer volume of data that's flying around the world right now.

Tasha: Right, and information security, as a process and discipline, provides a structure for protecting the value of data. As an organization creates, stores, shares, uses, modifies, archives, and finally destroys that data.

Manny: Writing information down on paper, a whiteboard, or a flash drive, or putting it in a file on Cloud creates data that is a tangible asset. The organization has to protect both the ideas and the data.

Tasha: Yes, and all the copies of it in papers, books, conversation logs, computer files, database records and the network packets which help move that information from one location or user to another.

Manny: Wow, that's an important job. *Tasha:* It sure is.

Data Handling

Data itself goes through its own life cycle as users create, use, share and modify it. Many different models of the life of a data item can be found, but they all have some basic operational steps in common. The data security life cycle model is useful because it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal). It also helps put the different data states of in use, at rest and in motion, into context. Let's take a closer look.

All ideas, data, information or knowledge can be thought of as going through six major sets of activities throughout its lifetime. Conceptually, these involve:

Create

Creating the knowledge, which is usually tacit knowledge at this point.

Store

Storing or recording it in some fashion (which makes it explicit).

Use

Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.

Share

Sharing the data with other users, whether as a copy or by moving the data from one location to another.

Archive

Archiving the data when it is temporarily not needed.

Destroy

Destroying the data when it is no longer needed.

Data Hnadling deeper dive

Narrator: Data handling is extremely important. As soon as we receive the assets, the data we need to protect, we need to make sure we know the best practices for handling this data.

First, we need to recognize which assets we need to protect. This is based on the value of the data according to the owner of that data. Based on that, we see what kind of risk we are facing with respect to the likelihood that this information could be compromised, destroyed or changed by any means, and what vulnerabilities exist that we need to account for. This is the life cycle of data handling, from create, to store, to use, to share, to archive and finally to destroy. And at any point there are different risks to the data and different practices for handling it. Some of these procedures are mandated by government standards.

For example, in the US, the Occupational Safety and Health Administration (OSHA) is the federal government agency that protects the well-being of workers. Under the rules of the Healthcare Insurance Portability and Accountability Act (HIPAA), medical records need to be kept for 10 years, but under OSHA, if we have a medical record of an on-the-job injury, that record needs to be maintained for over 30 years, even after the last day of work in that particular organization. That's a regulatory requirement, and if you don't know that or don't abide by it, you can find yourself in trouble as the result of an audit. So you can see that we have to be very cautious when deciding how to handle data, as there may be multiple regulations that apply to a single piece of data.

Also in the US there are also specific guidelines related to the Payment Card Industry Data Security Standards (PCI DSS) requirements regarding credit card information and how to maintain that information securely. In the European Union, the GDPR also has specific requirements regarding the handling of financial data. In order to protect the data properly, you need to know all the relevant requirements for the type of data being protected in the various geographic areas.

Many countries and other jurisdictions have regulations that require certain data protections throughout every stage of the data's life cycle. These govern how the data is acquired, processed, stored, and ultimately destroyed. And when looking at the life cycle of the data, we need to keep a watchful eye and protect the information at every stage, even if it's ready to be legally destroyed at the end of the life cycle. In some cases, multiple jurisdictions may impose rules affecting the data we are charged with protecting. In these instances, we need to be aware of any and all regulations that affect us.

Some data handling practices include classification and labeling, where you determine the sensitivity of the data, what is available to everyone and what needs to be restricted, and label the information accordingly so that your access controls will allow the correct level of access. Retention is how long we store the information and where, based on the requirements of our organization and perhaps regulatory agencies as well. And then there needs to be defensible destruction, meaning that we have the regulatory mandate backing up our decision to destroy the data. Destruction can be physical, of hard drives or computer chips, or destruction of digital records, which can be done under a number of methodologies. We need to make sure we

understand the secure destruction of the data, because often we think we can just empty the virtual trash can to delete the data. But when we do that, old emails and other data may never be erased. To completely erase the data on physical media, you need to use some technical equipment for **degaussing**, such as powerful magnets to erase the data stored on tape and disk media such as computer and laptop hard drives, diskettes, reels, cassettes and cartridge tapes. However, an individual with sophisticated equipment could potentially still retrieve that information, at least partially. So we must make sure we understand what recovery tools are available, because if you are subject to regulatory compliance, you have to follow through with specific protocols and processes to destroy that information as required so that it can no longer be accessed in any way.

Data Handling Practices

Data itself has value and must be handled appropriately. In this section, we will explore the basics of classifying and labeling data to ensure it is treated and controlled in a manner consistent with the sensitivity of the data. In addition, we will complete the data life cycle by documenting retention requirements and ensuring data that is no longer in use is destroyed.

Classification

Businesses recognize that information has value and others might steal their advantage if the information is not kept confidential, so they classify it. These classifications dictate rules and restrictions about how that information can be used, stored or shared with others. All of this is done to keep the temporary value and importance of that information from leaking away. Classification of data, which asks the question “Is it secret?” determines the labeling, handling and use of all data.

Before any labels can be attached to sets of data that indicate its sensitivity or handling requirements, the potential impact or loss to the organization needs to be assessed. This is our first definition: **Classification** is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality, integrity and availability. Information is then labeled and handled accordingly.

Classifications are derived from laws, regulations, contract-specified standards or other business expectations. One classification might indicate “minor, may disrupt some processes” while a more extreme one might be “grave, could lead to loss of life or threaten ongoing existence of the organization.” These descriptions should reflect the ways in which the organization has chosen (or been mandated) to characterize and manage risks.

The immediate benefit of classification is that it can lead to more efficient design and implementation of security processes, if we can treat the protection needs for all similarly classified information with the same controls strategy.

Labeling

Security labels are part of implementing controls to protect classified information. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. This spectrum of needs is useful, but it should not be taken to mean that clear and precise boundaries exist between the use of “low sensitivity” and “moderate sensitivity” labeling, for example.

Data Sensitivity Levels and Labels

Unless otherwise mandated, organizations are free to create classification systems that best meet their own needs. In professional practice, it is typically best if the organization has enough classifications to distinguish between sets of assets with differing sensitivity/value, but not so many

classifications that the distinction between them is confusing to individuals. Typically, two or three classifications are manageable, and more than four tend to be difficult.

Highly restricted: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.
Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.
Low sensitivity (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.
Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

Retention
Information and data should be kept only for as long as it is beneficial, no more and no less. For various types of data, certain industry standards, laws and regulations define retention periods. When such external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy. Data retention policies are applicable both for hard copies and for electronic data, and no data should be kept beyond its required or useful life. Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit. For the security professional to succeed in this assignment, an accurate inventory must be maintained, including the asset location, retention period requirement, and destruction requirements. Organizations should conduct a periodic review of retained **records** in order to reduce the volume of information stored and to ensure that only necessary information is preserved.

Records retention policies indicate how long an organization is required to maintain information and assets. Policies should guarantee that:

Personnel understand the various retention requirements for data of different types throughout the organization.
The organization appropriately documents the retention requirements for each type of information.
The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer.

A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary "noise" when searching or processing information in search of relevant records. It may also be in violation of externally mandated requirements such as legislation, regulations or contracts (which may result in fines or other judgments). Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be considered.

Destruction
Data that might be left on media after deleting is known as **remanence** and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level. This can be done by one of several means:

Clearing the device or system, which usually involves writing multiple patterns of random values throughout all storage media (such as main memory, registers and fixed disks). This is sometimes called “overwriting” or “zeroizing” the system, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.
Purging the device or system, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual “ghosts” of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, **degaussing** may not be sufficient.
Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.

In many routine operational environments, security considerations may accept that clearing a system is sufficient. But when systems elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

Logging and Monitoring Security Events

Logging is the primary form of instrumentation that attempts to capture signals generated by events. Events are any actions that take place within the systems environment and cause measurable or observable change in one or more elements or resources within the system. Logging imposes a computational cost but is invaluable when determining accountability. Proper design of logging environments and regular log reviews remain best practices regardless of the type of computer system.

Major controls frameworks emphasize the importance of organizational logging practices. Information that may be relevant to being recorded and reviewed include (but is not limited to):

user IDs
system activities
dates/times of key events (e.g., logon and logoff)
device and location identity
successful and rejected system and resource access attempts
system configuration changes and system protection activation and deactivation events

Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems, detecting compromises and providing a record of how systems are used. Robust logging practices provide tools to effectively correlate information from diverse systems to fully understand the relationship between one activity and another.

Log reviews are an essential function not only for security assessment and testing but also for identifying security incidents, policy violations, fraudulent activities and operational problems near the time of occurrence. Log reviews support audits – forensic analysis related to internal and external investigations – and provide support for organizational security baselines. Review of historic audit logs can determine if a vulnerability identified in a system has been previously exploited.

It is helpful for an organization to create components of a log management infrastructure and determine how these components interact. This aids in preserving the integrity of log data from accidental or intentional modification or deletion and in maintaining the confidentiality of log data.

Controls are implemented to protect against unauthorized changes to log information. Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded. Organizations must maintain adherence to retention policy for logs as prescribed by law, regulations and corporate governance. Since attackers want to hide the evidence of their attack, the organization's policies and procedures should also address the preservation of original logs. Additionally, the logs contain valuable and sensitive information about the organization. Appropriate measures must be taken to protect the log data from malicious use.

Data Security Event Example

Here is a data security event example. It's a raw log, and it is one way to see if someone tried to break into a secure file and hijack the server. Of course, there are other systems now that are a little more user-friendly. But security engineers get very familiar with some of these codes and can figure out exactly who was trying to log it, was it a secure port or a questionable port that they were trying to use to penetrate our site.

Information security is not something that you just plug in as needed. You can have some patching on a system that already exists, such as updates, but if you don't have a secure system, you can't just plug in something to protect it. From the very beginning, we need to plan for that security, even before the data is introduced into the network.

Event Logging Best Practices

Different tools are used depending on whether the risk from the attack is from traffic coming into or leaving the infrastructure. **Ingress monitoring** refers to surveillance and assessment of all inbound communications traffic and access attempts. Devices and tools that offer logging and alerting opportunities for ingress monitoring include:

- Firewalls

Gateways
Remote authentication servers
IDS/IPS tools
SIEM solutions
Anti-malware solutions

Egress monitoring is used to regulate data leaving the organization's IT environment. The term currently used in conjunction with this effort is **data loss prevention (DLP)** or data leak protection. The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including:

Email (content and attachments)
Copy to portable media
File Transfer Protocol (FTP)
Posting to web pages/websites
Applications/application programming interfaces (APIs)

Encryption Overview

Almost every action we take in our modern digital world involves cryptography. Encryption protects our personal and business transactions; digitally signed software updates verify their creator's or supplier's claim to authenticity. Digitally signed contracts, binding on all parties, are routinely exchanged via email without fear of being repudiated later by the sender.
Cryptography is used to protect information by keeping its meaning or content secret and making it unintelligible to someone who does not have a way to decrypt (unlock) that protected information. The objective of every encryption system is to transform an original set of data, called the plaintext, into an otherwise unintelligible encrypted form, called the ciphertext.
Properly used, singly or in combination, cryptographic solutions provide a range of services that can help achieve required systems security postures in many ways:

Confidentiality: Cryptography provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient. Confidentiality keeps information secret from those who are not authorized to have it.
Integrity: **hash functions** and **digital signatures** can provide integrity services that allow a recipient to verify that a message has not been altered by malice or error. These include simple message integrity controls. Any changes, deliberate or accidental, will result in the two results (by sender and by recipient) being different.

An **encryption system** is the set of hardware, software, algorithms, control parameters and operational methods that provide a set of encryption services.

Plaintext is the data or message in its normal, unencrypted form and format. Its meaning or value to an end user (a person or a process) is immediately available for use.

Plaintext can be:

image, audio or video files in their raw or compressed forms
human-readable text and numeric data, with or without markup language elements for formatting and metadata
database files or records and fields within a database
or anything else that can be represented in digital form for computer processing, transmission and storage

It is important to remember that plaintext can be anything—much of which is not readable to humans in the first place.

The central characteristic of a symmetric algorithm is that it uses the same key in both the encryption and the decryption processes. It could be said that the **decryption** process is just a mirror image of the encryption process. This image displays how symmetric algorithms work.

The same key is used for both the encryption and decryption processes. This means that the two parties communicating need to share knowledge of the same key. This type of algorithm protects data, as a person who does not have the correct key would not be able to read the encrypted message. Because the key is shared, however, this can lead to several other challenges:

If two parties suspect a specific communication path between them is compromised, they obviously can't share key material along that path. Someone who has compromised communications between the parties would also intercept the key.
Distribution of the key is difficult, because the key cannot be sent in the same channel as the encrypted message, or the man-in-the-middle (MITM) would have access to the key. Sending the key through a different channel (band) than the encrypted message is called out-of-band key distribution. Examples of out-of-band key distribution would include sending the key via courier, fax or phone.
Any party with knowledge of the key can access (and therefore change) the message.
Each individual or group of people wishing to communicate would need to use a different key for each individual or group they want to connect with. This raises the challenge of scalability — the number of keys needed grows quickly as the number of different users or groups increases. Under this type of symmetric arrangement, an organization of 1,000 employees would need to manage 499,500 keys if every employee wanted to communicate confidentially with every other employee.

Primary uses of symmetric algorithms:

Encrypting bulk data (backups, hard drives, portable media)
Encrypting messages traversing communications channels (IPsec, TLS)
Streaming large-scale, time-sensitive data (audio/video materials, gaming, etc.)

Other names for symmetric algorithms, which you may encounter, include:

Same key

Single key
Shared key
Secret key
Session key

An example of **symmetric encryption** is a substitution cipher, which involves the simple process of substituting letters for other letters, or more appropriately, substituting bits for other bits, based upon a cryptovariable. These ciphers involve replacing each letter of the plaintext with another that may be further down the alphabet.

Asymmetric Encryption

Asymmetric encryption uses one key to encrypt and a different key to decrypt the input plaintext. This is in stark contrast to symmetric encryption, which uses the same key to encrypt and decrypt. For most security professionals, the math of asymmetric encryption can be left to the **cryptanalysts** and cryptographers to know.

A user wishing to communicate using an asymmetric algorithm would first generate a key pair. To ensure the strength of the key generation process, this is usually done by the cryptographic application or the public key infrastructure (PKI) implementation without user involvement. One half of the key pair is kept secret; only the key holder knows that key. This is why it is called the private key. The other half of the key pair can be given freely to anyone who wants a copy. In many companies, it may be available through the corporate website or access to a key server. Therefore, this second half of the key pair is referred to as the public key.

Note that anyone can encrypt something using the recipient's public key, but only the recipient —with their private key—can decrypt it.

Asymmetric key cryptography solves the problem of key distribution by allowing a message to be sent across an untrusted medium in a secure manner without the overhead of prior key exchange or key material distribution. It also allows for several other features not readily available in symmetric cryptography, such as the non-repudiation of origin and delivery, access control and data integrity.

Asymmetric key cryptography also solves the problem of scalability. It does scale well as numbers increase, as each party only requires a key pair, the private and public keys. An organization with 100,000 employees would only need a total of 200,000 keys (one private and one public for each employee). This is less than half of the number of keys that would be required for symmetric encryption.

The problem, however, has been that asymmetric cryptography is extremely slow compared with its symmetric counterpart. Asymmetric cryptography is impractical for everyday use in encrypting large amounts of data or for frequent transactions where speed is required. This is because asymmetric key cryptography is handling much larger keys and is mathematically intensive, thereby reducing the speed significantly.

Let’s look at an example that illustrates the use of asymmetric cryptography to achieve different security attributes.

The two keys (private and public) are a key pair; they must be used together. This means that any message that is encrypted with a public key can only be decrypted with the corresponding other half of the key pair, the private key. Similarly, signing a message with a sender’s private key can only be verified by the recipient decrypting its signature with the sender’s public key. Therefore, as long as the key holder keeps the private key secure, there exists a method of transmitting a message confidentially. The sender would encrypt the message with the public key of the receiver. Only the receiver with the private key would be able to open or read the message, providing confidentiality.

This image shows how asymmetric encryption can be used to send a confidential message across an untrusted channel.

Narrator: Examples of encryption persist throughout human history, from early cryptic depictions by cave dwellers of Magura Cave in Bulgaria to the Pyramids at Giza. Even then, each group had its own primitive cryptographic approach, so that members of the tribe or group could communicate with one another while keeping secrets from the rival tribes regarding hunting grounds or sources of water and food.

It is part of human nature to encrypt information. You start with clear text, which is the information that you and I could easily read, and then you use an algorithm, which is often a form of software that can be embedded in the system. But that needs to be activated with an encryption key. A very simple example is if you are trying to encrypt a PDF document; for example, perhaps your accountant is sending you some documents to sign before submitting your taxes. Encryption would create a ciphertext, which no one can use, and you and your accountant would have set up a preset encryption key so that you could retrieve the information at either end of the communication. You need to have good key management, which means you safeguard the information, because imagine if you have thousands of keys in a commercial environment. There is often a third party or external server where the keys will be separately stored and managed, so you don’t have all your eggs in one basket, so to speak. It will be protected through a hashing system, which we will explore in a moment, and no one else can have access to those keys.

Asymmetric encryption is more secure because the sender and receiver each uses a unique code, often a certificate, so you can confirm that the information has been sent from the sender to the recipient in a secure manner.

Hashing

Hashing takes an input set of data (of almost arbitrary size) and returns a fixed-length result called the hash value. A hash function is the algorithm used to perform this transformation. When used with cryptographically strong hash algorithms, this is the most common method of ensuring message integrity today.

Hashes have many uses in computing and security, one of which is to create a **message digest** by applying such a hash function to the plaintext body of a message.

To be useful and secure, a cryptographic hash function must demonstrate five main properties:

> Useful: It is easy to compute the hash value for any given message.
> Nonreversible: It is computationally infeasible to reverse the hash process or otherwise derive the original plaintext of a message from its hash value (unlike an encryption process, for which there must be a corresponding decryption process).
> Content integrity assurance: It is computationally infeasible to modify a message such that re-applying the hash function will produce the original hash value.
> Unique: It is computationally infeasible to find two or more different, sensible messages that hash to the same value.
> Deterministic: The same input will always generate the same hash, when using the same hashing algorithm.

Cryptographic hash functions have many applications in information security, including digital signatures, message authentication codes and other forms of authentication. They can also be used for fingerprinting, to detect duplicate data or uniquely identify files, and as **checksums** to detect accidental data corruption. The operation of a hashing algorithm is demonstrated in this image.

This is an example of a simple hashing function. The originator wants to send a message to the receiver and ensure that the message is not altered by noise or lost packets as it is transmitted. The originator runs the message through a hashing algorithm that generates a hash, or a digest of the message. The digest is appended to the message and sent together with the message to the recipient. Once the message is delivered, the receiver will generate their own digest of the received message (using the same hashing algorithm). The digest of the received message is compared with the digest sent by the originator. If the digests are the same, the received message is the same as the sent message.

The problem with a simple hash function like this is that it does not protect against a malicious attacker that would be able to change both the message and the hash/digest by intercepting it in transit. The general idea of a cryptographic hash function can be summarized with the following formula:

variable data input + hashing algorithm

= fixed bit size data output (the digest)

As seen in this image, even the slightest change in the input message results in a completely different hash value.

Hash functions are very sensitive to any changes in the message. Because the size of the hash digest does not vary according to the size of the message, a person cannot tell the size of the message based on the digest.

Hashing Deep Dive

Hashing puts data through a hash function or algorithm to create an alphanumeric set of figures, or a digest, that means nothing to people who might view it. No matter how long the input is, the hash digest will be the same number of characters. Any minor change in the input, a misspelling, or upper case or lower case, will create a completely different hash digest. So you can use the hash digest to confirm that the input exactly matches what is expected or required, for instance, a password.

For example, we pay our rent through automatic withdrawal, and it's $5,000 a month. Perhaps someone at the bank or at the rental office thinks they can just change it to $50,000 and keep the extra money. They think no one will notice if they just add another zero to the number. However, that change will completely change the digest. Since the digest is different, it will indicate that someone corrupted the information by changing the value of the automatic withdrawal, and it will not go through. Hashing is an extra layer of defense.

Before we go live with a software product provided by a third party, for instance, we have to make sure no one has changed anything since it was tested by you and the programmer. They will usually send you the digest of their code and you compare that to the original. This is also known as a Checksum. If you see a discrepancy, that means something has changed. Then the security coders will compare the original one and the new one, and sometimes it's very tedious, but they have software that can do it for them. If it's something a little more intricate, they may need to go line by line and find out where the bugs are or if some lines need to be fixed. Often these problems are not intentional; they sneak in when you are making final adjustments to the software.

An incident occurred at the University of Florida many years ago, where a very reputable software source, Windows 2000 or Millennium, was provided to 50,000 students via CD-ROMs, and the copies were compromised. The problems were detected when the digests did not match on a distribution file.

Narrator: Often your password will be stored as a fixed hash value or digest, so that the system can tell if your password matches without the password itself ever being visible.

A more secure password with alphanumeric and special characters will generate a different type of hash digest. However, this system of password management is already becoming obsolete. Often, for security purposes, you will be asked to generate a new password with a minimum number of characters, and the software behind it will recognize the hash function and tell you if the password is sufficiently secure to be used, or it will prompt you to create a better password.

Attackers can use password hashes to “guess” your password offline. If an attacker can copy the password file, which is usually hashed, from a compromised workstation or server, and they know the algorithm that is used to hash the password, they can use a computer to try random sequences of letters and number combinations to try to match the known password hash.

UNDERSTANDING SYSTEM HARDENING

Manny: With so much data to work with, and so many different software applications required to handle it, how do companies keep track of everything?

Tasha: It's a challenge all right, that's why we need configuration management. It's part of cybersecurity in that it protects the confidentiality, integrity, and availability of data by making sure that only authorized and validated changes are made to a system. Every change also needs to be tested to make sure it doesn't cause any disruption to any other part of the system.

Manny: I can understand that. It seems like every time we upgrade our computer systems at the high school, something else stops working.

Tasha: Let's find out how cybersecurity professionals work to prevent that from happening.

Configuration Management Overview

Configuration management is a process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated. It is both a decision-making process and a set of control processes. If we look closer at this definition, the basic configuration management process includes components such as identification, baselines, updates and patches.

Identification

Baseline identification of a system and all its components, interfaces and documentation.

Baseline

A security baseline is a minimum level of protection that can be used as a reference point. Baselines provide a way to ensure that updates to technology and architectures are subjected to the minimum understood and acceptable level of security requirements.

Change Control

An update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. A review and approval process for all changes. This includes updates and patches.

Verification and Audit

A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that

the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

Effective use of configuration management gives systems owners, operators, support teams and security professionals another important set of tools they can use to monitor and oversee the configuration of the devices, networks, applications and projects of the organization. An organization may mandate the configuration of equipment through standards and baselines. The use of standards and baselines can ensure that network devices, software, hardware and endpoint devices are configured in a consistent way and that all such devices are compliant with the security baseline established for the organization. If a device is found that is not compliant with the security baseline, it may be disabled or isolated into a quarantine area until it can be checked and updated.

Inventory
Making an inventory, catalog or registry of all the information assets that the organization is aware of (whether they already exist, or there's a wish list or need to create or acquire them) is the first step in any asset management process. It requires that we locate and identify all assets of interest, including (and especially) the information assets:

You can't protect what you don't know you have.

It becomes even more challenging to keep that inventory, and its health and status with respect to updates and patches, consistent and current, day in and day out. It is, in fact, quite challenging to identify every physical host and endpoint, let alone gather the data from them all.

Baselines
A commercial software product, for example, might have thousands of individual modules, processes, parameter and initialization files or other elements. If any one of them is missing, the system cannot function correctly. The baseline is a total inventory of all the system's components, hardware, software, data, administrative controls, documentation and user instructions.

Once controls are in place to mitigate risks, the baselines can be referenced. All further comparisons and development are measured against the baselines.

When protecting assets, baselines can be particularly helpful in achieving a minimal protection level of those assets based on value. Remember, if assets have been classified based on value, and meaningful baselines have been established for each of the classification levels, we can conform to the minimum levels required. In other words, if classifications such as high, medium and low are being used, baselines could be developed for each of our classifications and provide that minimum level of security required for each.

Updates
Repairs, maintenance actions and updates are frequently required on almost all levels of systems elements, from the basic infrastructure of the IT architecture on up through **operating systems**, applications platforms, networks and user interfaces. Such modifications must be acceptance tested to verify that newly installed (or repaired) functionality works as required. They must also be regression tested to verify that the modifications did not introduce other erroneous or unexpected behaviors in the system. Ongoing security assessment and evaluation testing evaluates whether the same system that passed acceptance testing is still secure.

Patch

Patch management mostly applies to software and hardware devices that are subject to regular modification. A **patch** is an update, upgrade or modification to a system or component. These patches may be needed to address a vulnerability or to improve functionality. The challenge for the security professional is maintaining all patches, since they can come at irregular intervals from many different vendors. Some patches are critical and should be deployed quickly, while others may not be as critical but should still be deployed because subsequent patches may be dependent on them. Standards such as the PCI DSS require organizations to deploy security patches within a certain time frame.

There are some issues with the use of patches. Many organizations have been affected by a flawed patch from a reputable vendor that affected system functionality. Therefore, an organization should test the patch before rolling it out across the organization. This is often complicated by the lack of a testing environment that matches the production environment. Few organizations have the budget to maintain a test environment that is an exact copy of production. There is always a risk that the testing will not always be able to test everything, and problems may appear in production that were not apparent in the test environment. To the extent possible, patches should be tested to ensure they will work correctly in production.

If the patch does not work or has unacceptable effects, it might be necessary to roll back to a previous (pre-patch) state. Typically, the criteria for rollback are previously documented and would automatically be performed when the rollback criteria were met.

Many vendors offer a patch management solution for their products. These systems often have certain automated processes, or unattended updates, that allow the patching of systems without interaction from the administrator. The risk of using unattended patching should be weighed against the risk of having unpatched systems in the organization’s network. Unattended (or automated) patching might result in unscheduled outages as production systems are taken offline or rebooted as part of the patch process.

The risks of change

Narrator: You have to make sure you have a robust change management process and make sure you test in model environments before you make any change in a production or live environment. Even with extensive planning and testing, there are sometimes unintended consequences, so you must make sure there is a rollback plan. A rollback is restoring the system to the state it was in before the change was made. To the point where we know it was working properly before we introduced changes into the environment. We need to make sure we review and test all the patches and can restore the previous configuration.

Maintaining a separate testing environment can be a logistical challenge for many organizations; as such, many do not have separate production and testing environments to properly vet all patches and system updates. In this case, they may rely on vendor third party testing to certify a

new software release based on a generic set of data. The rollback plan is important in all environments, but it is absolutely critical in those who are unable to fully test a change.

Understand best practice security policy

Manny: What kind of policies can organizations establish to help their employees or members protect their data?

Tasha: Policies can include password requirements, limits on personal devices, and all kinds of other policies to ensure privacy and security. In this module, we'll explore the most common security policies found in organizations and identify some components of these policies.

Common Security Policies

All policies must support any regulatory and contractual obligations of the organization. Sometimes it can be challenging to ensure the policy encompasses all requirements while remaining simple enough for users to understand.

Here are six common security-related policies that exist in most organizations.

Data handling policy
Appropriate use of data: This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization. In addition, some data has associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations. For example, classifying credit card data as confidential can help ensure compliance with the PCI DSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard.

Password policy
Every organization should have a password policy in place that defines expectations of systems and users. The password policy should describe senior leadership's commitment to ensuring secure access to data, outline any standards that the organization has selected for password formulation, and identify who is designated to enforce and validate the policy.

Acceptable use policy (AUP)
The acceptable use policy (AUP) defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action. It should detail the appropriate and approved usage of the organization's assets, including the IT environment, devices and data. Each employee (or anyone having access to the organization's assets) should be required to sign a copy of the AUP, preferably in the presence of another employee of the organization, and both parties should keep a copy of the signed AUP.

Policy aspects commonly included in AUPs:

- Data access
- System access
- Data disclosure
- Passwords
- Data retention
- Internet usage
- Company device usage

Bring your own device (BYOD) policy

An organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use. This is sometimes called bring your own device (BYOD). Another option is to present the teleworker or employee with a list of approved equipment and require the employee to select one of the products on the trusted list.

Letting employees choose the device that is most comfortable for them may be good for employee morale, but it presents additional challenges for the security professional because it means the organization loses some control over standardization and privacy. If employees are allowed to use their phones and laptops for both personal and business use, this can pose a challenge if, for example, the device has to be examined for a forensic audit. It can be hard to ensure that the device is configured securely and does not have any backdoors or other vulnerabilities that could be used to access organizational data or systems.

All employees must read and agree to adhere to this policy before any access to the systems, network and/or data is allowed. If and when the workforce grows, so too will the problems with BYOD. Certainly, the appropriate tools are going to be necessary to manage the use of and security around BYOD devices and usage. The organization needs to establish clear user expectations and set the appropriate business rules.

Privacy policy

Often, personnel have access to personally identifiable information (PII) (also referred to as electronic protected health information [ePHI] in the health industry). It is imperative that the organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling of that type of information and are made aware of the legal repercussions of handling such sensitive data. This type of documentation is similar to the AUP but is specific to privacy-related data.

The organization's privacy policy should stipulate which information is considered PII/ePHI, the appropriate handling procedures and mechanisms used by the organization, how the user is expected to perform in accordance with the stated policy and procedures, any enforcement mechanisms and punitive measures for failure to comply as well as references to applicable regulations and legislation to which the organization is subject. This can include national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries

such as HIPAA and Gramm–Leach–Bliley Act (GLBA); or local laws in which the organization operates.

The organization should also create a public document that explains how private information is used, both internally and externally. For example, it may be required that a medical provider present patients with a description of how the provider will protect their information (or a reference to where they can find this description, such as the provider's website).

Change management policy
Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management focuses on making the decision to change and results in the approvals to systems support teams, developers and end users to start making the directed alterations.

Throughout the system life cycle, changes made to the system, its individual components and its operating environment all have the capability to introduce new vulnerabilities and thus undermine the security of the enterprise. Change management requires a process to implement the necessary changes so they do not adversely affect business operations.

Common Security Policies Deeper Dive

Policies will be set according to the needs of the organization and its vision and mission. Each of these policies should have a penalty or a consequence attached in case of noncompliance. The first time may be a warning; the next might be a forced leave of absence or suspension without pay, and a critical violation could even result in an employee's termination. All of this should be outlined clearly during onboarding, particularly for information security personnel. It should be made clear who is responsible for enforcing these policies, and the employee must sign off on them and have documentation saying they have done so. This process could even include a few questions in a survey or quiz to confirm that the employees truly understand the policy. These policies are part of the baseline security posture of any organization. Any security or data handling procedures should be backed up by the appropriate policies.

Change Management Components

The change management process includes the following components.

Documentation

All of the major change management practices address a common set of core activities that start with a **request for change (RFC)** and move through various development and test stages until the change is released to the end users. From first to last, each step is subject to some form of formalized management and decision-making; each step produces accounting or log entries to document its results.

Approval

These processes typically include: Evaluating the RFCs for completeness, Assignment to the proper change authorization process based on risk and organizational practices, Stakeholder reviews, resource identification and allocation, Appropriate approvals or rejections, and Documentation of approval or rejection.

Rollback

Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: Scheduling the change, Testing the change, Verifying the rollback procedures, Implementing the change, Evaluating the change for proper and effective operation, and Documenting the change in the production environment. Rollback authority would generally be defined in the rollback plan, which might be immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.

Change management components in the workplace

Narrator: Change management happens in a cycle. There is no real stopping point; it is continuously going. This means that there must be continuous monitoring of that environment. So, if you or anyone should request a change, it needs to go through the appropriate approvals. The organization must be prepared for rollback if necessary, meaning that if that particular change did not work, we need to be able to roll back to the legacy system.

While change management is an organization-wide process, it often falls on Information Security professionals to coordinate the effort and maybe to provide oversight and governance. Depending on the size of the organization, it may also fall under an IT or development area. In organizations that have a quality or risk management department, it would be a great fit in either of those areas too. The common theme is that change management acknowledges and incorporates input from the end users as well as all areas of IT, Development, Information Security and most importantly Management, to ensure that all changes are properly tested, approved and communicated prior to being implemented.

Supporting security policy with procedures

Narrator: Different organizations will have different goals for their acceptable use policies. Some organizations encourage employees to make wide personal use of the organization’s IT assets, to

improve morale and reduce interruptions between the user's personal life and work. Some organizations encourage users to use organizational assets to perform personal educational tasks, as well—this way, the employee gets the benefit of the assets, and the organization gets a higher-trained and happier employee. Some organizations severely limit users' personal use of IT assets, in order to reduce risk within the organization.

All security related policies should align with the organization's risk tolerance while ensuring that regulatory requirements are met. An organization that does not store confidential data on a laptop or workstation is likely to be more relaxed in their acceptable use policy, while a healthcare facility, research institution or defense contractor may be much stricter, as they have data that can be potentially devastating if compromised.

Understand security awareness trainaning

Manny: So what's the most important tool for cybersecurity, Tasha?
Tasha: I'd say the most important tool is your human resources—your people. *Manny:* People more so than technology, firewalls, passwords, and all that stuff?

Tasha: Yes, Manny. It's people who develop that technology, install those firewalls, create those passwords. Even more so, everyone must follow best practices and policies to ensure the secure handling of the data they work with every day. That's why security awareness training is so important. Your people must know what to look for and what to do when they see it. They must stay vigilant. Complacency is the enemy when it comes cybersecurity.

Manny: If you see something, say something. *Tasha:* Exactly. Let's find out more.

Purpose

The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization. We will be able to align the information security goals with the organization's missions and vision and have a better sense of what the environment is.

What is Security Awareness Training?

Let's start with a clear understanding of the three different types of learning activities that organizations use, whether for information security or for any other purpose:

Education: The overall goal of education is to help learners improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways.
Training: Focuses on building proficiency in a specific set of skills or actions, including sharpening the perception and judgment needed to make decisions as to which skill to use,

when to use it and how to apply it. Training can focus on low-level skills, an entire task or complex workflows consisting of many tasks.
Awareness: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.

You'll notice that none of these have an expressed or implied degree of formality, location or target audience. (Think of a newly hired senior executive with little or no exposure to the specific compliance needs your organization faces; first, someone has to get their attention and make them aware of the need to understand. The rest can follow.)

The one that got away

Gabriela: So, something really weird happened. I got a text this morning saying that I won $1000 from Amazon.

Keith: Wow. Did you respond?

Gabriela: Well, I was going to, but then at the last minute I noticed that it was from Amazoon, not Amazon. I mean, a company wouldn't misspell its own name, would it? And then it got me thinking about that one time that I accidentally downloaded a virus, and I thought that I would just wait to talk to you about it, since I know you've been studying cybersecurity and phishing and all that.

Keith: Congrats You passed. That was a fake link I sent you to see if you would click on it.

Gabriela: (sighs) Well, I guess that security awareness training you've been doing has finally paid off. But I still kind of feel like someone owes me $1,000.

(People chattering)
Tasha: Susan arrives at the coffee shop in time to hear Keith and Gabrielle's conversation. (People chattering)
Susan: Well, look at how far you've come since we first started talking about cybersecurity. Keith: Well, at first I figured I didn't have the technical skills.

Susan: Ah, but what it really comes down to is you have curiosity, and you're a good communicator, and you work well as part of a team. You're also analytical. You're good at identifying patterns, you know, seeing the bigger picture, but also the smaller details. You are actually perfect for cybersecurity work.

Keith: I guess it is pretty interesting, understanding data and how to keep people's data safe.

Susan: And it's always changing. There are so many opportunities in this field and different directions you can take. I'm proud to say that I am a System Security Certified Practitioner, and I'm even thinking about earning my CISSP from (ISC)2.

Keith: What's that?

Susan: It's a Certified Information System Security Professional, a globally recognized cybersecurity certification.

Keith: Wow, that is so cool. It seems like cybersecurity never gets boring or stale. I'd always be growing, unlike here.

Susan: Hey, do not let your mom hear you say that. she has coffee running in her veins.

Keith: Gabriela can take over for me, right? I mean, you know more about customers' data and how to keep it safe.

Gabriela: I mean, that would be great, Keith, but I might consider a future in cybersecurity myself.

Keith: I'm ready to start now. What do I need to do to get a job like yours?
Susan: I might just be able to point you in the right direction. What have we got here? Keith: Oh, we're working on...

The impotence of security training

Narrator: Why does everyone need security training? The weakest link in any organization is the human, and each one of us, regardless of if we are the new intern or the executive in the corner office, each one of us has our own responsibilities about security. Everyone contributes to improving the security environment, administratively, physically and technically.

Employees cannot follow policies and procedures if they have not received training on what the policies and procedures are. This is especially important for topics like data handling and emergency response activities. For instance: fire drills are crucial to protect health and human safety, and train users how to implement the process of protecting themselves from danger.

Security Awareness Training Examples

Let’s look at an example of security awareness training by using an organization’s strategy to improve fire safety in the workplace:

> Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms and their interactions with electrical power, lighting and ventilation systems.
> Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities.

> Awareness activities would include not only posting the appropriate signage, floor or doorway markings, but also other indicators to help workers detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

Translating that into an anti-phishing campaign might be done by:

> Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques.
> Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email.
> Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing) and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking.

Let's look at some common risks and why it's important to include them in your security awareness training programs.

Phishing

The use of phishing attacks to target individuals, entire departments and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend against. Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments and many other delivery mechanisms.

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as **whaling attacks** .

Social Engineering

Social engineering is an important part of any security awareness training program for one very simple reason: bad actors know that it works. For the cyberattackers, social engineering is an inexpensive investment with a potentially very high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.

One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.

Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives. A short list of the tactics that we see across cyberspace currently includes:

Phone phishing or vishing: Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted through a phishing email to call in to the "bank" via a provided phone number to verify information such as account numbers, account access codes or a PIN and to confirm answers to security questions, contact information and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.
Pretexting: The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to your login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a coworker, the police, a tax authority or some other seemingly legitimate person. The goal is to gain access to your computer and information.
Quid pro quo: A request for your password or login credentials in exchange for some compensation, such as a "free gift," a monetary payment or access to an online game or service. If it sounds too good to be true, it probably is.
Tailgating: The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating would occur when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when he or she is actually installing malicious software onto your device.

Social engineering works because it plays on human tendencies. Education, training and awareness work best to counter or defend against social engineering because they help people realize that every person in the organization plays a role in information security.

Password Protection

We use many different passwords and systems. Many password managers will store a user's passwords for them so the user does not have to remember all their passwords for multiple systems. The greatest disadvantage of these solutions is the risk of compromise of the password manager.

These password managers may be protected by a weak password or passphrase chosen by the user and easily compromised. There have been many cases where a person's private data was stored by a cloud provider but easily accessed by unauthorized persons through password compromise.

Organizations should encourage the use of different passwords for different systems and should provide a recommended password management solution for its users.

Examples of poor password protection that should be avoided are:

Reusing passwords for multiple systems, especially using the same password for business and personal use.
Writing down passwords and leaving them in unsecured areas.
Sharing a password with tech support or a co-worker.

Password advice and example

Narrator: Going back to the subject of the password. If you have a 10-number password, then with software with the cryptographic calculation to brute force attack your environment, it will take 5 seconds to crack. Most people think 8 characters with multiple different characters is pretty secure, and that's kind of standard for password requirements. But if someone really wants it, it may take them 35 days. We'd rather be more secure than that.

If you have 16 characters with one upper case and one special character, for example, this is more secure, because you have upper and lowercase characters and special characters. To crack this, it will take about 152,000 years.

So just by following a good password policy and appropriate procedures, we can improve our password security immensely.

Best practices for security awareness training

Narrator: We have to make sure we have appropriate communications about current and potential threats to keep awareness high. We could even encourage friendly competition between departments to spot the most phishing attempts. We can offer friendly reminders, like a little squishy stress ball that says, "Lock your computer." There are also automatic systems that lock the computer automatically when you step away.

It is important to make sure we get positive feedback about our training, ensuring it is appropriate and understood. Make sure the organization's leaders understand the importance of training and working to promote and improve the information security environment of the organization. And provide the opportunity for personnel to practice what they've learned, with exercises and simulations. Occasionally send simulated phishing emails, for example, and give them positive feedback for reporting it.
Depending on the organization's culture and risk profile, awareness training should be a positive experience for everyone and not punitive unless it is absolutely necessary.

Chapter five terms and definitions

Application Server - A computer responsible for hosting applications to user workstations. NIST SP 800-82 Rev.2
Asymmetric Encryption - An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.
Checksum - A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.
Ciphertext - The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret.
Classification - Classification identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. In short, classification is focused first and foremost on maintaining the confidentiality of the data, based on the data sensitivity.
Configuration management - A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated.
Cryptanalyst - One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.
Cryptography - The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning.
Data Loss Prevention (DLP) - System capabilities designed to detect and prevent the unauthorized use and transmission of information.
Decryption - The reverse process from encryption. It is the process of converting a ciphertext message back into plaintext through the use of the cryptographic algorithm and the appropriate key for decryption (which is the same for symmetric encryption, but different for asymmetric encryption). This term is also used interchangeably with the “deciphering.”
Degaussing - A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.
Digital Signature - The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. NIST SP 800-12 Rev. 1
Egress Monitoring - Monitoring of outgoing network traffic.
Encryption - The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.
Encryption System - The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability.
Hardening - A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and

software, including operating system, web server, application server, application, etc. Hardening is normally performed based on industry guidelines and benchmarks, such as those provided by the Center for Internet Security (CIS).

Hash Function - An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. NIST SP 800-152

Hashing - The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. Source CNSSI 4009-2015

Ingress Monitoring - Monitoring of incoming network traffic.

Message Digest - A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated. NISTIR-8011 Vol.3

Operating System - The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations. NIST SP 800-44 Version 2

Patch - A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. Source: ISO/IEC 19770-2

Patch Management - The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. Source: CNSSI 4009

Plaintext - A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

Records - The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). NIST SP 800-53 Rev. 4

Records Retention - A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed.

Remanence - Residual information remaining on storage media after clearing. NIST SP 800-88 Rev. 1

Request for change (RFC) - The first stage of change management, wherein a change in procedure or product is sought by a stakeholder.

Security Governance - The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

Social engineering - Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building.
Symmetric encryption - An algorithm that uses the same key in both the encryption and the decryption processes.
Web Server - A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an “intranet server.” NIST SP 800-44 Version 2
Whaling Attack - Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities.