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.

Sarah: Everything is risky, Josh, from driving in a car to giving your credit card number to a telemarketer. Well in our business, people are lowered into the water in steel cages to observe and photograph sharks. Obviously this has some risk attached. The key is that we take risk very seriously and we take steps to make our attraction as safe as possible, both for the participants and for those who have invested in the business. If something were to happen, the bad publicity and the legal liability would take a big bite out of our livelihood. If you pardon the pun.

Josh: I don't actually, but tell me more about the different ways you address the dangers of your enterprise. Like, the sharks are tame or mechanical or something, right?

Sarah: No, these are absolutely real wild sharks. That's what's exciting about it. And part of the fun is the danger, or the perception of danger.

Josh: So it's only a perception?
Sarah: No, of course not. Well, mostly.
Josh: I don't think I'm following. Is it dangerous or not?

Sarah: Okay. Okay. We're going to accept that there are some risks involved here, right? If we weren't willing to accept a little danger we wouldn't be in this business and the customers wouldn't be signing up to participate. Customers who aren't feeling very brave can obviously avoid the risk by not participating. We have a video feed so they can watch other people in the cages. So they get to share the experience. We also avoid risk by not going out in certain weather conditions or when particularly dangerous shark activity has been observed. We keep a very close eye both on the weather and the animal's behavior so we don't take unnecessary chances with our crew or our customers or even our equipment.

Josh: So you don't go out unless conditions are ideal. What other safeguards do you take?

Sarah: We mitigate our risk by having very strong cages and testing them often. And we train our crews rigorously to adhere to our safety policies and procedures and to abide by Florida laws and federal safety regulations.

Josh: What if something happens in spite of all your preparation? People love to sue businesses when accidents happen.

Sarah: That's why all our participants are required to sign waivers. That serves to mitigate the risk of liability.

Josh: Do people object to the waivers?

Sarah: Not really. This sort of risk management approach is very common. Everything you do has fine print, from downloading an app to flying in a plane or staying at a hotel. Even at other attractions, like those run by animated mice and ducks that we will not name, the ticket includes a disclaimer in the fine print that the park is not responsible for theft or accidents on 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?

Eder: Hi, Chad. Hi, everyone. Thank you for this, for inviting me for this session. It's a pleasure to be here with you today. And about this question, I think it's, ethics is mandatory for everyone in cybersecurity nowadays. And we are in face of a lot of different situations. And we need to have a strong feeling of ethics, because dealing with different conditions, I think what I learn about (ISC)$_2$, and with complementary, with my background, ethics are fundamental to keep working in our area nowadays. I think (ISC)$_2$ gives us a solid pillars, for pillars about ethics. And during my profession or in my career, I was learning that it's important, incorporate these conditions about (ISC)$_2$, reinforce in every certification, in every document, in every publication, and join with feelings about what I learned when I was a kid, about my father told me in the past, my family, I think it's a, the role is a, we need to join any point that you learn, and apply in our market, in cybersecurity. I think it's the main point.

Chad: Okay, great. And I would like to hear a little bit more about, in your experience, and how those ethics influence your concept of right and wrong?

Eder: A lot, a lot. Because the market and the conditions of economic and wars and stuff like that, we have different situations for dealing about this point. Recently, last year, I received a bribery. Someone invite me to disclose sensitive informations, and will pay a huge amount of money. And no, no thanks. It was a very different situation for me. And I call the legal authorities here in Brazil, and I sent them all the informations about the communication. I was invited by email, you know, it's a point that, it's me. My honor is not on sale. And I think this point is mandatory. And in the profession, we have daily, we are in face with these situations daily, because we have many criminal organizations interesting in achieve our information, because we are in face of customers' information, company information. And in the black market, these information have paramount value. It's a, it's this. I think that's it.

Chad: And that's a great story. And that's part of why I was so excited to talk to you, and talk to you about ethics, is so we could gather more of the international perspective. And you mentioned that somebody had contacted you through the mail for a bribe. Is that something, and I don't want to single out Brazil, and say this only happens in Brazil, because I know it happens other places, it happens here in the U.S. as well, but is that something, do you think that's more commonplace in Brazil, or is it still somewhat rare to happen?

Eder: I think in Brazil, happens a lot, because we have problem with our society here. It's a society that, if someone have the opportunity to achieve advantage, or some gifts or whatever, the people are in face, and sometimes they accept the offer. It's not my case in this situation. And as I mentioned, my honor is not for sale, but here in Brazil we have this difficulty, because the corruption in our society is, it's hard.

Chad: Yeah, absolutely, so I'm trying to figure, you know, I'm really curious, does that, you know, you said it's something that does happen often in Brazil. So is it also something that, is it, I want to say people from Brazil that are making those bribery offers, is it something that seems to be domestic, or is it international, is it other countries that are, and you don't need to name other countries if that's the case, I'm just curious if that's something that's internal to the country, or something that's other countries?

Eder: We have both scenarios here. We have competitors here. We have scenarios of malware or ransom groups. It's like criminal groups, like Conti or other groups responsible for hijacking or ransom inside main companies, very important companies around the world. And it's common in both cases, from international and from internal national, internal nation here, because the culture here is a point for difficult dealing. And we have specific areas in our police departments, and fiscalizations for avoid corruption and bribery. It's a sad point, present in our society here in Brazil.

Chad: Okay, great. And from what you've talked about so far, you definitely believe in the (ISC)$_2$ code of ethics. You obviously have your own code of ethics that might be apart from what your country is. And obviously you have been in cybersecurity for a while, and you are a great cybersecurity practitioner, but what do you think makes your chosen profession, a professional? What makes you a professional in cybersecurity?

Eder: About describing about my roles or my activities or why I chose working for cybersecurity, is this question?

Chad: Yes.

Eder: I think I start working for cybersecurity, or for security area, because cybersecurity doesn't exist 10 years ago. When I start working for this area, why, for why, or why I decided to work in this area, because, the first point, in security you have people with strong feelings about what is correct. And this is my point. My father recommend me in the past for become a judge, because I, to enforce the correctness, enforce the correct points about situations. But it's too many papers. No, it's not for me. In cybersecurity, you have a lot of papers, these documentation policies and whatever, but it's more applicable, or it's feasible with our reality. Apply something and affect a lot of people and companies about this point. And this is for, this is, was, this was my mainly reason for decide for cybersecurity, because strong feeling about what's correct, enforce the correctness, enforce what is possible. And yes, now we have some situations that are not totally correct, but we are in face of risk and risk analysis. And we need to deal about a project in face of our appetite of risk. And I think this point.

Chad: All right, and that's a great story. And we are so glad you chose cybersecurity over being a judge, because we're happy to have you here today. And we might not be talking if you had chosen that judge path. So that's great. I'm curious, though, in your perception, what makes the code of ethics in cybersecurity different from those in other professions?

Eder: I think in cybersecurity, we need to follow in more restrict way all points of ethics, because we are in face about the whole information, the company's, because we are security area. And security area needs to protect the company. In this case, we need to be a simple example for other people inside the company, as strong professionals, professionals that have a very good position in face of any problems or any circumstance that is not following the right way. I think it's, and security area, cybersecurity area, we enforce all points about ethics for other areas. About courses, about internal communication, about trainings for other areas that's not in face daily with problems with security or whatever, but show them about ethics, and why is important to keep ethics in current work, day to day.

Chad: That is great. And I really like that you see cybersecurity professionals as being a basically a role model in the world of ethics. And that's super, I really like that. So I want to know if you can share a specific situation, and I know you already shared one with us, about the bribery, but if you can share a situation where ethics played an impactful role in your decision making.

Eder: Yes, of course, in many projects the teams ask me, "Oh, let's forget these points about security, because will impact our work. We need to work a lot for compliance with these points. It's possible to forget this point." No. Because we need to enforce all points for security. And in every project, someone tries to resume the way of security, not implement all features, or avoid some important point. And I used to tell these guys, "No, if you commit some mistake here, or you produce a code without a compliant, without a wrong, a right check about this code, probably we will have a large problem in front." And is not the case, we need to have a strong feeling about security, about ethics, about condition for improve security, not for reduce security. I think this is the condition that I'm facing in many situations nowadays.

Chad: Yep, you are absolutely right. And that's something that we constantly, as cybersecurity professionals, have to apply our ethics to, to produce, or basically to make our decisions based on what may be best for the company, not necessarily what's best for the cybersecurity professional.

Eder: Yes.

Chad: And I think that's something that oftentimes is very difficult for the cybersecurity professional to do. Sometimes we have to, you know, sometimes we do have to make those decisions that are better for the organization than maybe for us personally, or make our life a little bit more difficult to better protect the organization.

Eder: Yes, yes. I agree, I agree.
Chad: Yep. You are absolutely right. Ethics play a huge part in that. Go ahead.

Eder: Yes, in another case, when some project, "No, we are not able to fill all security points." In this case, we produce a letter about risks, and request approval for a senior manager, senior management, or director, or vice president, or yes, if you are not compliant and you need to go ahead with this project, with this poor condition of security, you need to agree with this point, and agree that this is your responsibility. If you have some fail or some problem in the future, you are charged about this point.

Chad: Yep. Absolutely. And I think we, you know, for our listeners, I think we did cover part of that in our risk management section, we'll cover that. In talking about, you know, when there is risk, when we're introducing new risk, part of our ethics are to make sure that we are raising the awareness of that risk, and making sure that the business owners fully understand that risk. Whether it makes us popular or not, doesn't matter. Sometimes we have to take the unpopular road, and at least raise that up. So that's some great discussion, and we're gonna wrap up here in just a moment, Eder. It's been great talking to you, but I do want to give you one last chance, if you have anything else you'd like to say to our listeners.

Eder: Yes, I think for anyone that is interesting in starting cybersecurity, cybersecurity is a code of life, because someone that start working for cybersecurity, or someone that worked for a long time in cybersecurity, we use these concepts in our life, in our society. And we are advocates. We are people to transmit security and cybersecurity and ethic codes for people around us. And I think it's a point to everyone that is starting cybersecurity, pay attention in the code of ethics, and strong feeling about what is right. I think it's the main point, and our society needs this condition, a strong, or improve these values now.

Chad: All right, absolutely. Thank you. And I think it is just absolutely great the way you put that, that underline and that highlight, that ethics really does lie underneath everything we do as cybersecurity professionals. And I thank you very much for helping us put an international eye on this. So we can see, a lot of times we think of terms in our own country, and how things happen in our own countries. And that's part of what (ISC)2 strives to do, not only here, but for the cybersecurity profession as a whole, to make sure that we are one team and we have one common goal, one common set of ethics across the world. But I thank you many, many times, Eder, thank you for spending time with us today. Thanks for sharing your knowledge and your perspective on ethics, and everybody, please join me in thanking Eder de Mattos for volunteering his time with us here today. Thank you very much.

Eder: Thank you. Thank you, Chad. It was a pleasure to be here. And thank you, guys, and enjoy the cybersecurity.

PROFESSIONAL CODE OF CONDUCT

ISC2 code of ethics preamble

The Preamble states the purpose and intent of the ISC2 Code of Ethics.

> The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
> Therefore, strict adherence to this Code is a condition of certification.

ISC2 code of ethics canons

The Canons represent the important beliefs held in common by the members of ISC2. Cybersecurity professionals who are members of ISC2 have a duty to the following four entities in the Canons.

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 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, Daniel Hernandez. I invited Daniel here today because he has perspectives very close to you, our listeners. Daniel's currently working towards his CISSP and has a history of about five years as a CIS admin and about a year as an information security analyst.

So, I'm going to dive right in here and say, lay a little bit of groundwork on this first one here, and say that I think we talked, in our courses, that security exists to support the business operations, something that's a very important point to make for us here at (ISC)2. You know, security is important, there are a lot of technical components to the security, but ultimately security is there to support the business and make sure the business can continue to operate safely and securely. So, what we're going to dive into specifically is a business continuity plan or BCP. And what that is really trying to do is to create an easy-to-use actionable solution to help prepare for the impact of an actual incident or even the broad range of threats occurring to an organization. Now, the business continuity plan and what it takes to keep a business operating applies—you know, we think of that often and we think of disasters often in the term of natural disasters (tornadoes, floods, hurricanes you name it), but this also, of course, includes global pandemics, it includes accidents. It could include acts of terrorism. So, when we're thinking about a business continuity plan, we're really trying to make sure that we can plan and keep the business operating from a technical perspective, but providing that technical support to the business to keep them operating with the systems, either working or not working, as effective as possible. So, we're looking at how these hazards can cause the failure and how we can keep these operating in terms of system equipment software.

So, Daniel, I know you're very aware of how the BCP keeps incident response and disaster recovery in place. So, what we're here to really talk about is how, when that business continuity plan and the incident response plans fail, is how we start with disaster recovery. So, I'm just wondering, and we're speaking of disasters and I'm going to turn a little bit of a different one and I don't know how familiar you are with the, and we're going to call it a disaster, but the 2017 Equifax breach and how that impacted more than 150 million consumers. And really, Canada, US, and Britain, but from all over the world. So how do you feel, you know, and what kind of a plan do you have in place, or have you thought about, either personally or professionally, and how can you protect and how can you make sure you can continue business in the face of a breach such as Equifax?

Daniel Hernandez: Well, you know, I think one of the most important pieces there in your incident response plan would be the communications portion, right? How do you communicate to those affected by the incident or the disaster that occurred? So, I think those are—that's probably one of my focal points is having clear and good communication with, you know, everyone that is affected by it and, you know, just all the stakeholders within your incident response planning. I think that's a very important piece of it, too, just understanding who are the stakeholders that you need to communicate with or inform of the different stages that are there. So does that kind of—?

Kliewer: Absolutely, it really does. And I think you bring out a really important part, because most of us that are looking at a career in security or are already in a career in security are very much technical-minded. We're not necessarily thinking about those non-technical pieces and it's a great point to bring that in. Absolutely, communication is key. "Communicate early, communicate often," I think is what a lot of people say about that. The other trick to that is to make sure we get those communications on the right level, to make sure we're communicating with people and not communicating to people. Now, I understand—and since we got off kind of on this communication tangents and one of the reasons, I was excited to have you as a guest, is I understand you've got some, we'll say some background or history, not necessarily in security area, but you've got some background in how to adjust that communication for the different audiences. Would you want to share that with us?

Hernandez: Yeah, for sure. So, you know, growing up, often I was tasked with translating from Spanish to, or from English to Spanish and Spanish to English, you know, my parents not being native language speakers, and they relied on me for a whole lot of that. So, you know, I felt that, for the longest time, I've always been that middleman between two different parties, you know, just for a long time. And so, I think I've developed those skills throughout the years. And translating them, I mean, even from just a technical perspective, being able to, you know, communicate different issues to non-technical individuals, and now, you know, as I moved onto the security realm, now communicating the security issues to technical individuals that don't understand, you know, risk may be one of those things that they don't quite understand, and translating it into their own languages is kind of important. And I think it's something that is good to have in the field is being able to communicate to different levels, you know, doing that translation for them.

Kliewer: Okay, absolutely. And I think that is absolutely key to this whole process is, like I said, that communication at the right level. And to make sure that that communication is absolutely included in the business continuity plan, incident response plans, and disaster recovery plans, which all tie in together. So, great insight there. So, I want to talk a little bit more, maybe, on the security side of things for a minute now. And I'm wondering, and as close as you can get without naming any organizations, other than we all know what the big breach is out there and that, but without naming any of your organizations or giving away any real secrets there, what kind of incident or disruption have you seen within your career and how do you think that response was?

Hernandez: Well, are we allowed to talk about the “S” one?

Kliewer: Absolutely, I think everybody knows all about SolarWinds.

Hernandez: Yeah, so SolarWinds, you know, that was quite, I think it was something that, it was a revelation to the industry as a whole, and, well, maybe even the nation, you know, because it

revealed that we're susceptible to being attacked from, you know, our trusted parties. So, you know, I think, for a lot of us, it told us that we need to do a better job at vetting our suppliers of software and hardware as part of our business continuity planning and third-party risk management. It is a big portion, you know. You have to take into account that, whenever you're doing your incident response, you have to look at, okay, you know, what is the criticality of this piece of software that has been compromised? If you need to isolate a machine that is hosting, you know, SolarWinds, how does that impact the business as a whole? You know, from us in critical infrastructure, we have to monitor our equipment continuously, so it is a great impact to not be able to have those eyes to, you know, understand what equipment is up and running, so.

Kliewer: Absolutely, and I want to pick on something you said there, Daniel, just talking about being in critical infrastructure and talking about the impact. And what I want to be real clear about there is the impact and what you've got to do with that business continuity plan, that disaster recovery plan, is how does that really affect your business and how do these different pieces affect your business? It will be absolutely different for every business, I guarantee. I've also had a lot of conversations about SolarWinds with different groups. A lot of people, when that stuff happened, they said, "Okay, we just ripped it all out and we went with a different vendor." That's not always an option. If you're an internet provider, you operate a very large network, it's absolutely crucial to your operations. It's not just a monitor to see what's working and what's not, or to help you deploy patches. It's a lot more than that. It's very integral to your daily operations. So, I think our lesson there is to really look at how it integrates to your daily operations and understand that. And that's the biggest part of that business continuity plan. Remember, the business word comes first. So how does this keep the business running and how does the business keep running when you don't have it, or if you don't have it. So, do you think that that incident changed? I can tell it definitely changed the way you think about keeping, I don't want to get up on a supply chain tangent here, but I can tell it changes the way you think about the business continuity and the way we use and the way we evaluate things. Do you think that had any impact on the organization as a whole into how people think about how we use things?

Hernandez: Yes, absolutely. You know, I think because, you know, working in a small, rural, you know, telecom, perspective of things may be different throughout the organization, but once they all understand what's at stake and what are some of the risks that imply or are implied with, you know, having a breach or, you know, things like that. I think it has, you know, gone all the way up to our general manager and our board, you know, to help them understand that yes, there is a priority that needs to be addressed with security, you know, and how we handle just security for the whole organization, that there's a place on the table for, you know, all of the business leaders who deal with the day-to-day operations and management of the organization, that there is a need for them to understand risk, you know, and the different risks that cybersecurity has brought in into their eyes.

Kliewer: Okay, awesome. And I want to turn the conversation just a little bit, and once again, I'll lay a little bit of groundwork here. And I'm going to talk just a second about the National Institute for Standards and Technology and how they define incident response. They define preparation, detection and analysis, containment and recovery, and post-incident activities. We've talked mostly about preparation, the business continuity plan, which we know is of the ultimate importance. We're going to kind of skip the middle two because we talked, you know, I talked with some of those in a different podcast about incident response and actual incidents. But what I want to do now is fast forward to those post-incident activities. And I'm going to say this because we're mostly technical people, we like to get in, we like to fix things, we like to get out. “It's fixed now, what else is there for me to do?” So, what I'm curious about, Daniel, is I want to hear your perspective a little bit more on why the post-incident activities and what happens after you've contained an incident, after you've resumed operations—you know, when we've got to do that after-incident report or whatever. Help me understand the importance of that.

Hernandez: So, you know, often, I compare security with raising a child or the upbringing of a child. So, you know, I'm a new dad, you know, nine months or so. And when an incident happens where, you know, my daughter falls and at the end, I let her go through the whole process of, you know, you have to cry and, you know, it's okay, you pamper her and do this and that, but at the end, there needs to be some growth. And so, the post-work of an incident is probably, you know, as important as the prep work that is done at the beginning, you know, that we already talked about. I believe the learning really happens there for a lot of people, is after they realize what went wrong, then the learning really happens because you have their attention fully. And at that point, you know, you can really provide them with the tools that they need to make sure that this type of incident does not happen again, because you have a timeline, and you have history to look back on and make sure that they don't forget that.

Kliewer: Absolutely, because what are we doing? And it's not easy for us to do, but so what are we doing? We're looking at—when you're talking about post-incident, we're like, "Where did we mess up? What happened? Why did this happen? It shouldn't have happened." But most importantly, we're looking to feed that back to our business continuity plan to say, "Where did we miss that? What can we do to shore up our planning ahead and our business continuity first?" I think that's a great way to do it. And of course, I'm going to throw back in there again, just like what you were talking about, translating not necessarily English to Spanish and back and forth, but translating back and forth between the technical teams and the business teams to make sure that the goal on both sides are being met. And I think that's an awesome point to have.

So finally, I'm going to kind of wrap up with one question and I'll give you an opportunity to share anything you want to after that. So really, one final question, and I'm curious how you feel, being part of critical infrastructure in the United States, how do you feel that entities like, and I'm going to use the example of the US-CERT, and I know there are other ones and the names are not coming to me right now, but I know there are other ones worldwide, such as the UK has another agency, Japan has their agency that handles these kind of things. And I know other countries do as well. But I'm curious how you feel that the roles that those government agencies play in your incident response and in what, you know, how do you feel their role is, and how does that plug into your plan?

Hernandez: That's a good question. And I think, you know, from all the work that I've done in the last year or so, I've come to really—you know, when it comes to something critical and a critical incident or an incident that relates to a piece of either data or a system that is critical to our industry or to our organization, you know, we have to have a trust relationship with government at some point, because we, as critical infrastructure phase threats from overseas that are not local and we can't just report to the police and, you know, just that it'll actually have an impact on the threat that we're looking at. So, I believe that having those relationships with the FBI and with CISA is making sure that you can trust, you understand who are your contacts, is just of the most importance, I believe. And to have that contact information within your incident response, make sure that you have the information available for when you need it, because timeliness is, something that is critical for incident response is making sure you shorten that time. It makes a big difference at the end.

Kliewer: Absolutely correct. And I'm going to put a big exclamation point after that and say, especially, not necessarily US-CERT, but when you're talking about people like the FBI or CISA within the US, or whatever your agency is in other countries, be sure you know who your contacts are and don't be afraid to document that. I'm not going to say don't be afraid, do document it. Definitely do. Because I'll guarantee you, I don't care how many times you think about it, how many times you think you have incidents or whatever. Until that incident hits you and until you find out you have a breach, or you have a large incident sitting in front of you, you realize that no matter what you thought about, it just went out the window. And if you don't have that documented, you're still going to run around in circles and wonder what to do. So, when you say that and having those steps documented is absolutely key as part of the business continuity and your incident response and your disaster recovery. So, make sure you've got those documented and where you're going with those. So that's a great note to wrap up on, Daniel. Do you have any last-minute pieces of advice that you'd want to share?

Hernandez: Just keep going, that's all I got to say. You know, because I think a big portion of your audience may be entry level. And I just want to say, you know, don't be afraid that, you know, you don't have to know all of it from the get-go. You know, there's always great mentors like Chad himself and information security that you can look up to and gain a lot from, you know, as you continue your journey in information security. It is a great field to be in. It's very rewarding for a lot of us. So that's all I got.

Kliewer: I love that, to finish up on a positive note. After we talked about all the bad stuff, it's always great to say, yeah, absolutely, using Daniel's words, "Keep pressing forward. Keep moving forward." Things will happen, just make sure you learn from them and move on. I think that's a great piece of advice. And with that, we're going to wrap up here and I hope you've enjoyed our discussion. And again, I want to say many, many thanks to our special guest, Daniel Hernandez, for volunteering his time and to share his experiences with us here today. And thank you very much for listening.

Components of the incident response plan

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.

Incident response in action

Tasha: It's a slow day at the coffee shop, and Keith notices that Nate seems distracted and worried.

Keith: What's wrong? You don't seem like yourself today.
Nate: Oh. Well, I just got a lot on my mind. Did you hear what happened to our neighbors?
Keith: What do you mean?

Nate: Well, last Friday night when that storm was happening, some water got into the hardware store and damaged their front cash register. I mean, they were trying to open Saturday morning, and then when they couldn't, they had to close the shop and wait for it to be repaired. Could you imagine closing the store for an entire weekend?

Keith: No, that's our busiest time. *Nate:* Mm-hmm.

Keith: Huh, if only the hardware store had an extra cash register, they could have used that instead of having to close it down.

Nate: Exactly, and then on top of that, there was a break-in at the bakery. Their laptop got stolen. I mean, think about all the banking and customer information that was on that thing.

Keith: Yeah, that's scary. *Nate:* Yeah.

Keith: I wonder if they would've had the laptop in the safe, it wouldn't have got stolen. I just hope the data on the laptop was encrypted or a password or a passcode was needed to decrypt it.

Nate: Wait, wait, what are you talking about?
Keith: Oh, it's just talk with Susan about securing data. Anyway, I wonder where that laptop is

now.

Nate: Who knows? But, you know, it got me thinking what we can do to kind of make sure things like that don't happen here.

Keith: Huh. Susan says it's inevitable that adverse events can happen that will affect the business. You know what we need? An incident response plan.

Nate: What is that?

Keith: Don't worry about it. I got it.
Nate: Okay.
Tasha: Later that day, Keith gets Nate and Sandra together.

Keith: Hey all, thanks for coming. Look. This is what we have here. Well, first of all, Susan taught me that we need to be prepared with an incident response plan so we can reduce the impact of an incident. So, I've written one, and the three of us get to be the incident response team.

Sandra: Okay, Keith. Thanks. Uh, so what do you need us to do?

Keith: Well, when an incident occurs, the three of us will determine the amount and scope out any damage, including whether or not any confidential information was leaked. Then, we'll have to implement recovery procedures and restore any damage that occurred. It's all in the plan here.

Nate: Cool, Keith. Hey, thanks for taking this on. I really look forward to reading it. *Sandra:* Yeah, me too.

Keith: Great. Great. Because we all have to be familiar with this plan. I made a checklist for every employee, and it lets them know what they're responsible for in case of an incident and how to contact each other.

Nate: You know, we can make this the agenda for our next staff meeting.
Keith: Yes. I actually want to schedule some training sessions for everyone, so we all know how

to communicate if an incident occurs.
Sandra: This is such a relief. Thank you, Keith. I feel much better about things now. *Nate:* Yeah, good job, man.

Application of Incident response

How do you recognize an incident and then identify the first response? Until an analysis has been performed, you cannot. Organizations with mature security programs will have defined procedures. For example, employees tasked with detecting suspicious activity will ascertain the facts and relay them to the organization’s security office or response team.

Let us look at the response to a malware alert. First, a Security Operations Center (SOC) Analyst receives an alert of anomalous behavior at a workstation. Since the alert is for only one workstation, the SOC Analyst begins triaging the event. Further investigation shows that the alert was for behavior by a known user that did not pose a threat to the organization.

However, had the event involved software that is explicitly not allowed by the organization, the incident response plan would include escalation to a manager to address noncompliance with company policy. Further, if the event involved more than one computer, it might require escalation to a network or systems team to help isolate the event. If the event escalates further, additional teams such as executive management or public relations, or even law enforcement, might need to be involved.

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:

A new employee—When a new employee is hired, the hiring manager sends a request to the security administrator to create a new user ID. This request authorizes creation of the new ID and provides instructions on appropriate access levels. Additional authorization may be required by company policy for elevated permissions.

Change of position—When an employee has been promoted, their permissions and access rights might change as defined by the new role, which will dictate any added privileges and updates to access. At the same time, any access that is no longer needed in the new job will be removed.

Separation of employment—When employees leave the company, depending on company policy and procedures, their accounts must be disabled after the termination date and time. It is recommended that accounts be disabled for a period before they are deleted to preserve the integrity of any audit trails or files that may be owned by the user. Since the account will no longer be used, it should be removed from any security roles or additional access profiles. This protects the company, so the separated employee is unable to access company data after separation, and it also protects them because their account cannot be used by others to access data.

NOTE: Upon hiring or changing roles, a best practice is to not copy user profiles to new users, because this promotes "permission or privilege creep." For example, if an employee is given additional access to complete a task and that access is not removed when the task is completed, and then that user's profile is copied to create a new user ID, the new ID is created with more permissions than are needed to complete their functions. It is recommended that standard roles are established, and new users are created based on those standards rather than an actual user.

Tasha: Whether a user is authorized or unauthorized depends on their user provisioning, which is an identity management process for creating and managing access to resources and information systems.

Manny: While we usually think of user provisioning as creating new accounts, there are several different situations which require action by a security administrator who is responsible for provisioning user accounts.

Tasha: In fact, Susan finds herself in a situation that requires changes to a user's provisioning. Let's check in with her as she notifies the security administrator of this change.

Susan is talking to her securityadministrator.

Susan: One of my employees will be taking a temporary leave of absence. Dimitra, she's going to be taking a sabbaticalfrom work and she's not going to need access to the systems

Manny: Since Dimitra will not be accessing the systems, the security admin recommends disabling her accounts while she is not at work. This reduces the risk that her account could be used by an unauthorized person while she is on leave. He tells Susan to make the request, and then, according to the company policy and procedures, he will disable Dimitra's login account, so she is not allowed to log in to the company systems while out on leave.

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: All right, and I love the way you're already leading into role-based access, and we're going to get more into role-based access down the road here in just a little bit. One of the things I wanted to talk about a little bit before we get there is talking about, you know, a time when an operation or when an access control strategy failed, and it failed quite miserably. So, one example that we pulled up was an access control failure in the UK which resulted in the loss of the confidential information of 25 million people, or about the population of the state of Texas here in the US. And revenue and customs information was lost when an employee mailed a copy of an entire database, and it was lost somewhere in transit. So, it was something that was a physical copy that was mailed maybe on a USB drive, maybe on a disk or some sort, and was lost in transit. So, it didn't make it to its destination. And then we were at the center, you know, then her Majesty's revenue and customs was at the center of the media ridicule and the government faced huge embarrassment. And the worst part is, is there were only a couple thousand records that were even requested, and the entire database was sent. So, what parts did you pick out of there that could have been done better?

Pennie: Well, you know, honestly when they went back, they did a review and they found there were some key issues. One of which is kind of goes back to my point about organization wide. So, they found that there was a cultural issue at their organization, or in this case this a

government agency, but organization culture around security was they had policies, but they weren't really, they were kind of bureaucratic and they weren't very operational. So, they had policy, not necessarily procedure. And so it goes back to those processes that you have to have. And so, they didn't have the appropriate, for example, they could have had some approval processes to make sure there's an additional check to make sure that they were sending the appropriate database to whoever had requested it. And they could have had, you know, just a whole variety of processes to ensure that they were getting the right information or access to the individual that requested it, or a vetting process. They could have had a vetting process. There's a whole variety of ways you can control access that I don't think a lot of times we just think it's you request it and then you get it, or it's removed when you leave. We don't really think about the whole variety of ways that we can actually control access, be it fine grain control, like you mentioned before with your definition also. So, I think that was one of the breakdowns that they found. And then they also did kind of an audit process to ensure that their procedures that they did develop were actually being followed and were effective. So that's also kind of that continuous monitoring that has to happen.

Kliewer: Okay. And I don't know about you, but I'm already starting to hear a little bit of a of a trend here in our discussion. And once again, when we're talking about data control, we're talking about access control, that data or once again, we've got to connect the people to the practices.

Pennie: Yep.
Kliewer: And sounds to me like they had some pretty good practices in place textbook wise.

Maybe they had some good policies, but they never connected the people part of it. *Pennie:* No. Yeah.

Kliewer: So that sounds like a really good point to bring up there. So, it kind of segues that into another question that I had, and it is similar but a little bit different, but what are some ways that we can leverage the different access control methods or strategies to prevent unintentional or even intentional insider threats?

Pennie: So, you know, when it comes to insider threats, because that's a really great question, the intentional insider threat in some ways I think is easier sometimes, I think they both have their downsides and their ups on controlling them. The unintentional is really about fine grain access control, and it goes back to that streamlining. I think what ends up happening, kind of like I mentioned before, you end up with this one to one, this individual wears four hats and so they need four different roles access but one of those or two of those four may have additional access that they don't actually need. So, you end up with this access creep, and then that also happens when, you know, someone changes positions, and they hold onto some access and then they just start building access over time. So that's one of the ways that an insider threat unintentionally can happen where you can accidentally, especially in like a HIPAA situation where you can accidentally breach some data because it's really a minimum necessary failure.

So, on the other side of it with an intentional, I'm thinking that, you know, you have to classify your data really well. And then you can apply some process around your data with regards to access. So, if you know that there's sensitive data in this location or all those locations of sensitive data then you can build your processes to be more robust around those locations and more fine grain so that you can give just what they need and not any more than that. Always least privilege, right?

Kliewer: Okay. Awesome. And that leads us right into our discussion that I said just a little bit ago that we were going to have as we get on down the road, because I heard you kind of leading into it again, but that's when we start talking about the role based access control and I'm going to be honest, that's something that in a textbook is really hard to explain and really hard to get the bigger picture of, and that's part of what our discussion here today is, is to help explain that to our listeners and to help, you know, how do we really break down that role-based access control into a way that's understood and something that's easy for our learners as well as why it's so challenging. And I'm going to ask you your question for challenging here in just a moment, but it definitely is a challenge for that role-based access, because it's just like you said, what people want to do is they want to have individual access. This individual needs access to this. I know I personally have been in organizations where they said there is no way that you can create roles because we have too many people doing too many different jobs and helping out here and there. And that is one of the biggest challenges. And I'm curious if you've seen that challenge in your career and how you were able to work around that.

Pennie: Sure. I found that, you know, I've seen it so many times in so many different areas, you know, be it in your HR area where, you know, they need access to all employee data, but does each individual HR employee need that access—that's questionable. So, what I've done in the past is focus on separation of duties. If they have, you know, certain access that's needed that's higher leveled or more privileged than others then I might separate that access out, one person can have these two, you know, privileges, but they can't have these other two, and give those other two to someone else, separating things out, making it more difficult to act especially going back to your intentional insider threat or otherwise separating those out is really a, I have found, to be the best approach. Even if you have just two people, right? If you're talking about one individual who's just got to have a lot of access which I've seen in my past organizations where we have some smaller groups that have just one individual doing a lot of people's jobs, in that case the best you can do is really do monitoring, auditing of their access, auditing of sensitive data locations, and just you know, doing some alerts because what's the point of an audit if you're not alerting on it. And what's the point of alert if no one's reviewing any reports on that. So that would be kind of a step in those processes as well.

Kliewer: Awesome. So, I want to dive just a little bit deeper into what you were talking about, and you led right into the separation of duties. To me one of the easiest places to explain that separation of duties is in payroll and the separation a lot of times between human resources and payroll.

Pennie: Yeah.

Kliewer: And when you're talking about the separation and duties within a system, it really should be set up to where, and the one example I'm going to use is a person in payroll should not be able to enter a new employee into the system.

Pennie: Right.
Kliewer: Or set up payment for that employee. But payroll does, I mean, that's what they do,

they issue payment, right? *Pennie:* Mm-hmm.

Kliewer: So, what we're talking about here, we're talking about putting steps into the processes and where we can do that technically, we want to do that technically, you know, we want to prevent that person from being able to enter that new employee in the system. Ultimately, if you can you want to prevent the person that prints payroll checks from being able to update pay rates and that kind of stuff because that opens the door for that insider threat.

Pennie: Yep.

Kliewer: Whether it be intentional or not intentional, it still opens that door.

Pennie: I've also looked at, sorry go ahead-

Kliewer: Go ahead.

Pennie: I've also looked at, you know, the person who can create an account can't or an employee can't remove it as well, because that's also a risk there.

Kliewer: Yep, absolutely. But I'm going to add on there. I've seen a place and I've been in a place where we only had one payroll person who happened to be our accounts payable clerk as well. You know, so very small organization, those are difficult to do. Those are really difficult. We could still separate out the new employee, but when it came to separating out the payroll processes it just wasn't possible. I mean, we didn't have the granular ability within the system to do that. So, I can tell you what we ended up doing there was we ended up putting some manual checks in place. And when I say manual checks, that sounds really bad. I'm talking about payroll; I'm talking about manual checks but not those kinds of checks. I'm talking about the checks and balances kind of checks not the money kind. But what happened is we had to put some steps in place where basically that payroll clerk had to go to the CFO get a physical signature on that register that somebody else had reviewed it before it was processed. The downside of that is it doesn't actually prevent the fraud, but it does create an audit trail to show that things have been checked. So, the important part of that story is you can't always control everything technically. We'd like to think we can, but we know better, we know better than that.

Pennie: That's why it goes back to your point about process. It's all about process.

Kliewer: Yep, absolutely. It's where we got to connect those people. So that leads me right into the other people part of this conversation. So how have you found interdepartmental cooperation, such as partnering with HR to build more effective access control? How have you found good partnerships there?

Pennie: Well, what I've seen and really recently is kind of a looking at how we can build our roles from the beginning. Whenever we classify an employee’s position and identifying those commonalities and in access. And then once we have identified these categories of job class I guess is what I would call it, then we would, you know, kind of assign access to just those areas and then maybe some optional access that they may or may not need. That way we can have some kind of flexibility when we assign access and approve access. And also, some automation. You can automate a lot easier when you define things from the beginning, it goes back to that classifying data. But in this case, classifying your position so that, you know, when someone comes in it's a streamlined process, you can automate it. You know if they're in this role, they're already approved for this particular base access. And it just really speeds things up. It makes it more user friendly all around and it reduces that burden on your HR side for approving access or any other area who may have to approve some access. So those are some of the things that I've seen recently is just kind of a classifying your user, your employee base and your position, starting with your positions.

Kliewer: All right. Very good. And I'm going to back that off for our listeners just a little bit. At the very highest level, your relationship with HR, of course you know, everybody knows there there's two departments in any organization that you're always friends with. The first one is HR and payroll. The second one is IT. As long as you're friends with those two departments, you're going to do just fine in any company. But the biggest key information you can get from your HR and payroll departments is new hires and employee terminations. That's the number one most basic connection that you can make there. Make sure you know when somebody new is coming on board so hopefully you can be prepared as a security professional. You can be prepared for that employee coming on board, know what access they need, know when somebody leaves so you can terminate that access. So, we don't have a bunch of access left out there. Those are the most basic levels.

But you talked about being able to tie these security roles to what a person actually does. And I'll tell you the first time I sat down and thought about that, I'm like you know, how can we do that? How do we know what each person does? I sure wish I knew what Daisha did every day for her job, you know, so I could figure out what access that I think she needs. You know once again, that's what I think we have to work together to figure that out and know for sure what you need, but I got to figure like how can I ever figure that out? And then it finally dawned on me one day, you know what, somebody actually has all this information, and they wrote it down on a piece of paper, and that's HR and their job descriptions. And those job descriptions should absolutely align to what we do in security.

Pennie: Mm-hmm.

Kliewer: And when we're looking, you know, because HR is looking to categorize people mostly for pay purposes, but maybe for that job code and for certain departments and information security is also looking to categorize those people into what kind of access they need in the systems and those two very much align. And if you can build those, if you can build those synergies between your HR, your payroll, between your job descriptions and connect the people through those managers to build those roles and to create that role-based access control.

Pennie: Yeah.

Kliewer: It is absolutely priceless. So, we're just about out of time here Daisha. I do want to give you an opportunity if there's any last-minute words, you'd like to give our listeners on access controls or anything else I want to give you the chance to do that.

Pennie: Well, I think you made a good point about partnerships because it really is an organization wide process that you build around all of your access. So, each and every step of the way I think sometimes in IT we get very kind of narrow focused, and we think we can just technically, like you mentioned, solve all the problems, but sometimes it's definitely a lot of times, especially with security, it's a people business. So, you’ve got to get in and make those relationships and build those partnerships so that you can develop processes that are effective. And that's what that UK breach found. It's a cultural thing. It's an organizational thing. That's where access control really comes together effectively.

Kliewer: Absolutely. And thank you much for that. And I'm going to summarize our statements there because that that was a great conversation that we had on that. And we definitely have to remember to stay in touch. Although we tend to think technically, we tend to think it's access allowed, access denied, but we've got to connect that to the people and without connecting it to the people the access control is exactly that, it's control, and control is not what we're trying to do here, but we're trying to make sure the right people have the right access to the right information at the right time.

Pennie: That's it.
Kliewer: That's a whole lot of rights. *Pennie:* Yes.

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.