DOMAIN 1: Security Principles

CIA Triad

When defining security, it is common to use the CIA Triad: Confidentiality, Integrity, and Availability

The purpose of these terms is to describe security using relevant and meaningful words that make security more understandable to management and users and define its purpose

Confidentiality: Confidentiality means permitting authorized access to information while at the same time protecting it from improper disclosure.

Integrity: Integrity is 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.

Availability: Availability means that systems and data are accessible at the time users need them. The purpose of these terms is to describe security using relevant and meaningful words that make security more understandable to management and users and define its purpose.

CIA Triad Deep Dive

Confidentiality:

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:

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:

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.

Authentication

Confidentiality
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 passphrases
- Something you have: Tokens, memory cards, smart cards
- Something you are: Biometrics, measurable characteristics

Methods of Authentication

There are two types of authentications. 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).

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

Multi-factor authentication:

Use of two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

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 entered some other secret value that only you know, then you have

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 creating information, approving information, or sending or receiving a message.

Non-repudiation is a legal term 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 impersonation of others or denial of an action (e.g., 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.

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.

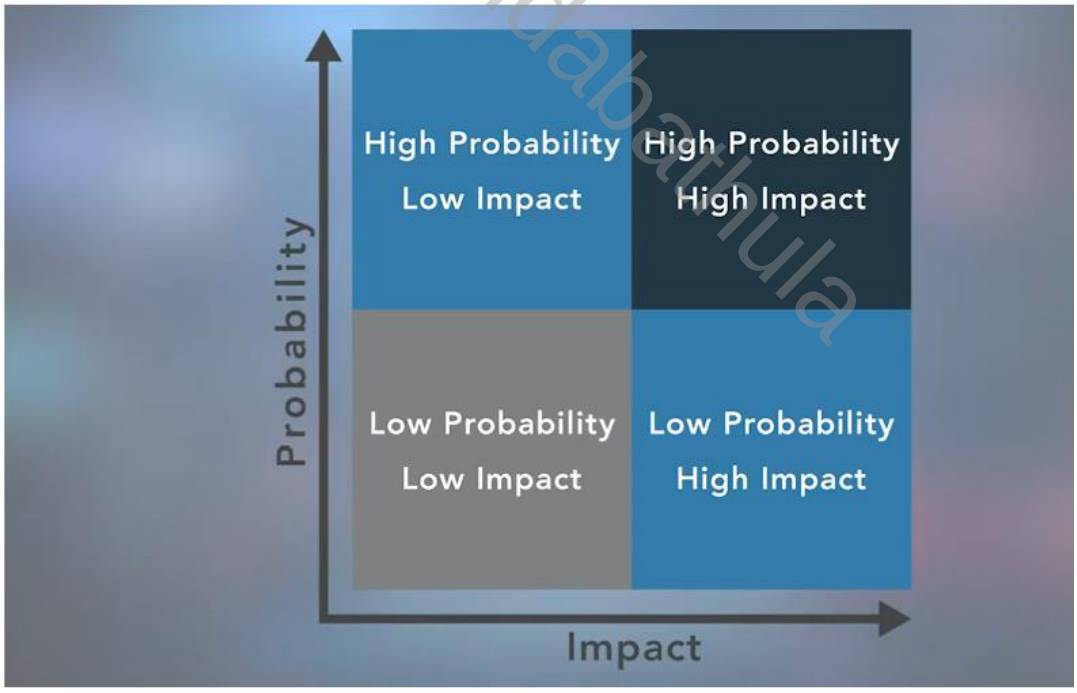
In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

(HIPAA in U.S)

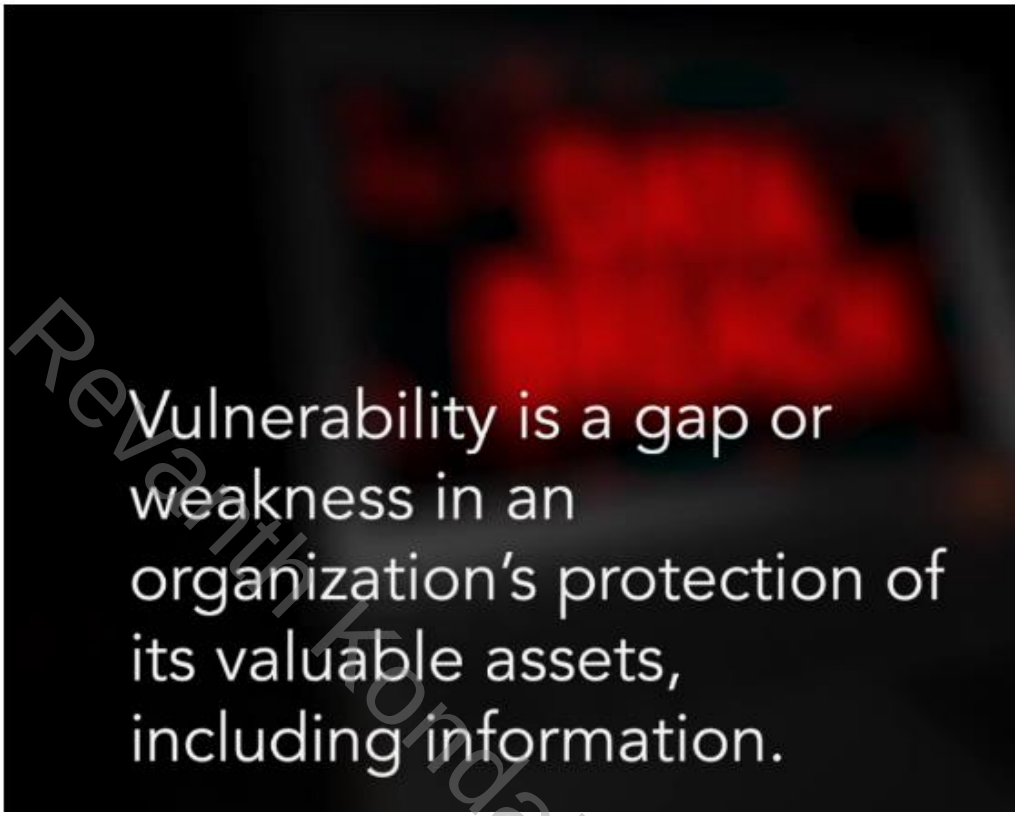
General Data Protection Regulation:

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.

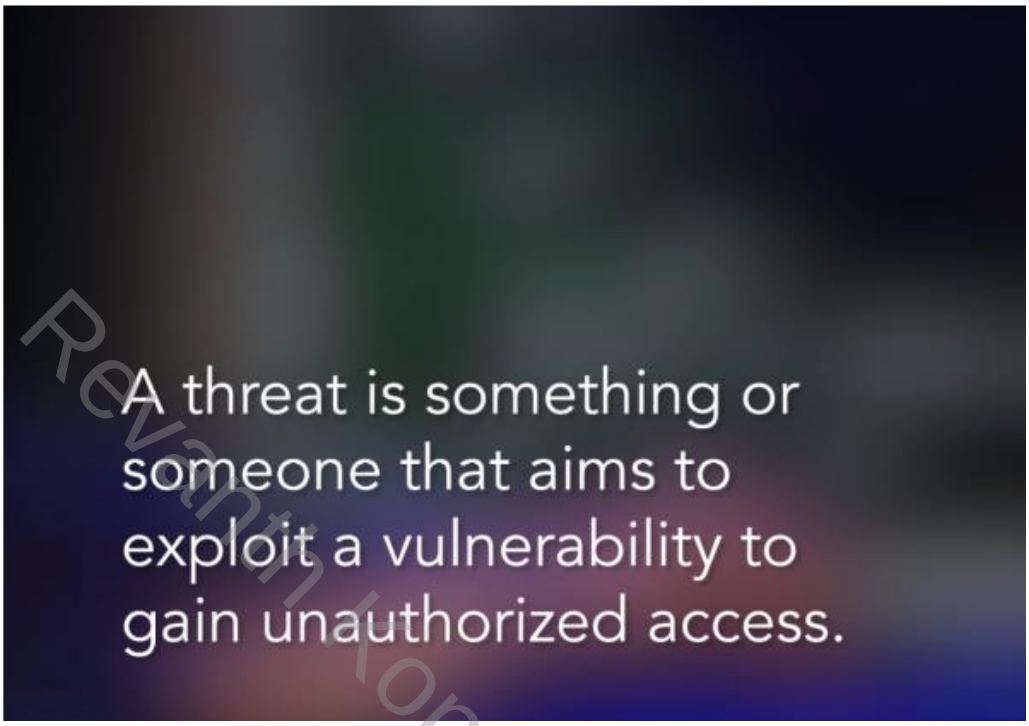
These laws, including national- and state-level laws, dictate that any entity anywhere in the world handling the private data of people in a particular legal jurisdiction must abide by its privacy requirements. It is important to understand how these laws apply to your organization. In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.



Importance of Risk Management



Importance of Risk Management



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.

- 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.

Terms such as threats, vulnerabilities, and assets are familiar to most cybersecurity professionals.

Risk Identification

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.

This involves looking at the organization 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.

Security professionals are likely to assist in risk assessment at a system level, focusing on process, control, monitoring, or incident response and recovery.

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

The analysis performed as part of risk management. A risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

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 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 centre 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 risk assessment to be performed by internal or external parties.

Risk Treatment

Risk treatment involves making decisions about the best actions to take regarding the identified and prioritized risk.

The decisions are dependent on the attitude of management toward risk and the availability—and cost—of risk mitigation.
The common risk treatment options are:

Risk Avoidance: It is the attempt to eliminate the risk entirely. This could include ceasing operation for some or all of the activities of the organization that leave it exposed to a particular risk. Leadership may choose risk avoidance if the potential impact of a given risk is too high or if the likelihood of the risk being realized is simply too great.

Risk acceptance: It is taking no action to reduce the likelihood of a risk occurring. Management may opt to conduct the business function 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.

Risk mitigation: It 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 such as security controls, policies, procedures, and standards to minimize adverse risk. Risk cannot always be mitigated, but mitigations such as safety measures should always be in place.

Risk transference: It 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 Priorities

When risks have been identified, it is time to prioritize and analyze core risks through **qualitative risk analysis** and/or **quantitative risk analysis**.

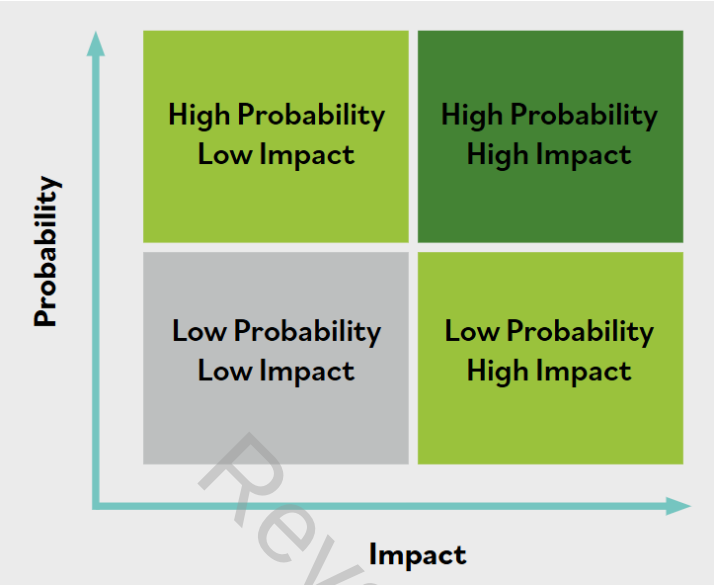
This is necessary to determine the root cause and narrow down apparent risks and core risks. Security professionals work with their teams to conduct both qualitative and quantitative analysis.

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.

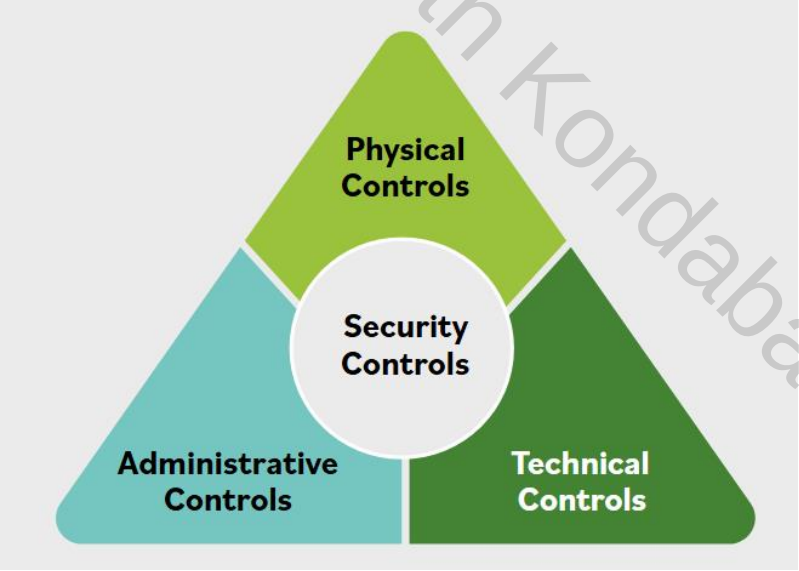
Often, risk tolerance is dictated by geographic location. For example, companies in Iceland plan for the risks that nearby volcanoes impose on their business. Companies that are outside the projected path of a lava flow will be at a lower risk than those directly in the path.

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 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

What are Security Controls?



Security controls pertain to the physical, technical, and administrative mechanisms that act as safeguards or countermeasures to protect the confidentiality, integrity, and availability of the system and its information.

The implementation of controls should reduce risk to an acceptable level.

Physical Controls

Physical controls address security needs using physical hardware devices, such as badge readers, architectural features of buildings and facilities, and specific security actions taken by staff.

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 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, door release mechanisms, and identity management and access control systems into a more seamless security system.

Technical Controls

Technical controls (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.

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 behaviour and should cover the entire scope of the organization's activities and its interactions with external parties and stakeholders.

Administrative controls can and should be powerful, effective tools for achieving information security. Even the simplest security awareness policy can be an effective control if it is implemented 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 references 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

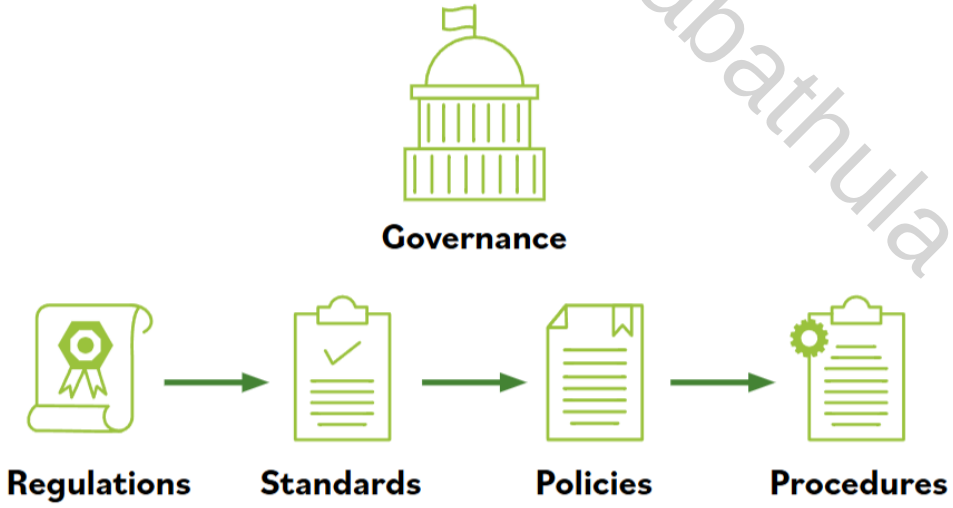
Governance Elements

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 non-compliance.



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 HIPAA 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 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 the 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.

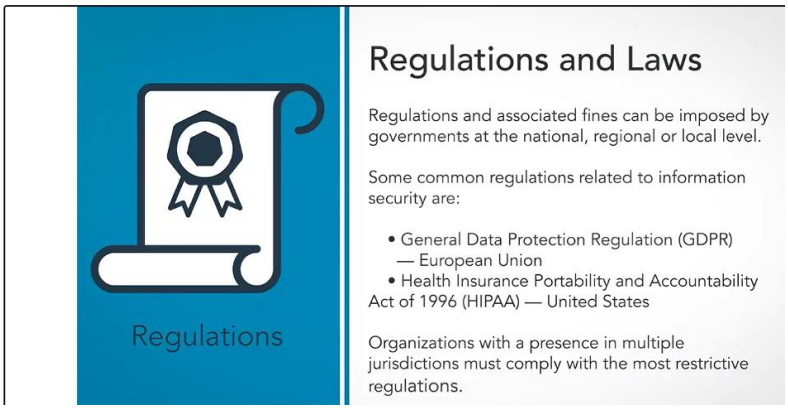
Policies are often written at many levels across the organization. High-level governance policies are used by senior executives to shape and control decision-making processes.

Other high-level policies direct the behavior and activity of the entire organization as it moves toward 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.

Procedures

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



Professional Code of Conduct

All information security professionals who are certified by ISC2 recognize that certification is a privilege that must be both earned and maintained.

Every ISC2 member is required to commit to fully support the ISC2 Code of Ethics.

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 principles, and duty to each other require that we adhere and be seen to adhere to the highest ethical standards of behaviour.
● 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 principles.
● Advance and protect the profession.

Domain 2: Incident Response, Business Continuity and Disaster Recovery Concept

Incident Terminology

While security professionals strive to protect systems from malicious attacks or human carelessness, inevitably, 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.

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. **NIST SP 800-53 Rev. 5**

Event:

Any observable occurrence in a network or system. **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.

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. **IETF RFC 4949 Ver 2**

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. **NIST SP 800-30 Rev 1**

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**

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.

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.

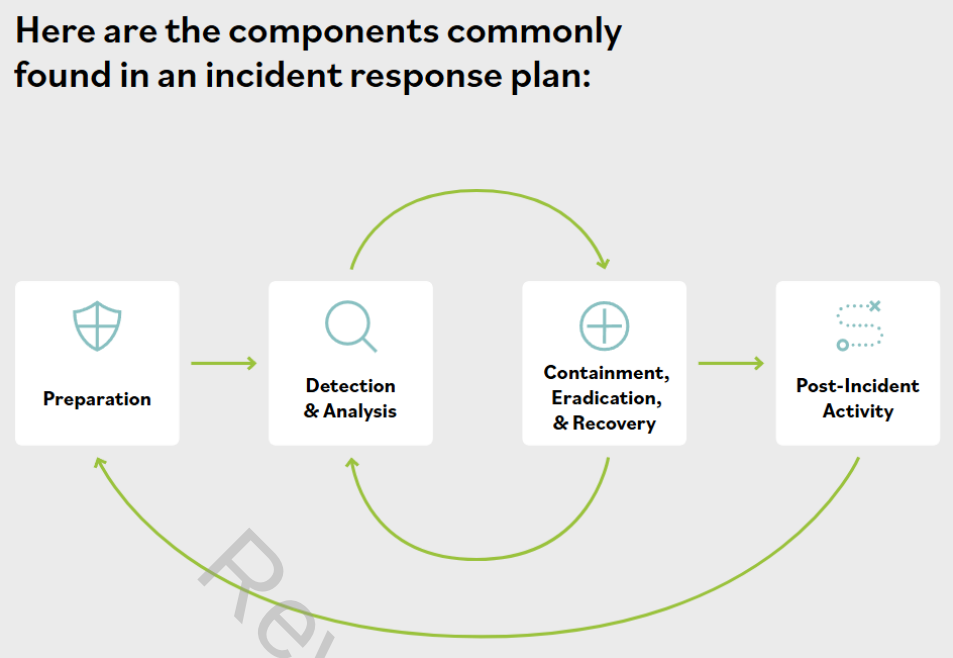
An event is any measurable occurrence, and most events are harmless. However, if the event has the potential to disrupt the business's mission, then it is called an incident. Every organization must have an incident response plan that will help preserve business viability and survival.

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. Incident response planning is a subset of the greater discipline of business continuity management (BCM).

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.



Preparation:

- Develop a policy approved by management.
- Identify critical data and systems and any single points of failure.
- Train staff on incident response.
- Implement an incident response team.
- Practice Incident Identification (first response).
- Identify roles and responsibilities.
- Plan the coordination of communication between stakeholders.
- Consider the possibility that a primary method of communication may not be available

Detection and Analysis:

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

Containment:

- 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.

Conduct a retrospective of:
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident Activity

Consulting with Management

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 managerial, 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.

Business Continuity in the Workplace

The Goal of 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.

The first step is to call the appropriate individuals and start to activate the business continuity plan. Management must be included because priorities can 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.

It is important 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 maintain essential activity.

The Goal of Disaster Recovery

Disaster recovery planning steps in where business continuity (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

It is vital to ensure 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.

Examples of disaster recovery in the real world:

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 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 manager
- 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 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 is 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.

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 imput from team members who are busy working on the recovery.

Domain 3: Access Control Concepts

Security Controls

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

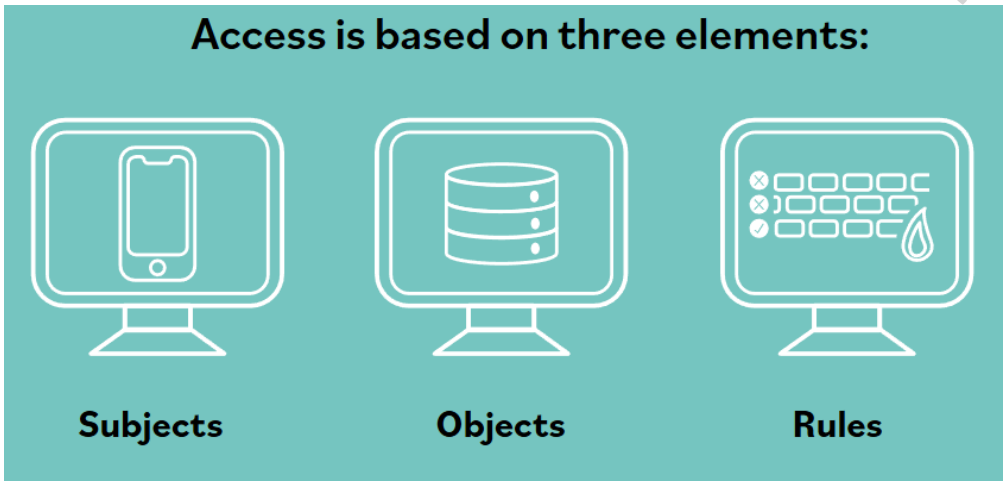
Access control involves limiting what objects can be available to what subjects according to what rules.

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. But in the end, security all comes down to who can get access to organizational assets (buildings, data, systems, etc.) and what they can 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.



Subjects

A subject can be defined as any entity that requests access to 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, or 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

Objects

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, a thread, or a process.
● Is anything that provides service to a user.
● Is passive.
● Responds to a request.
● May have a classification

Rules

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 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 re-purposed 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.

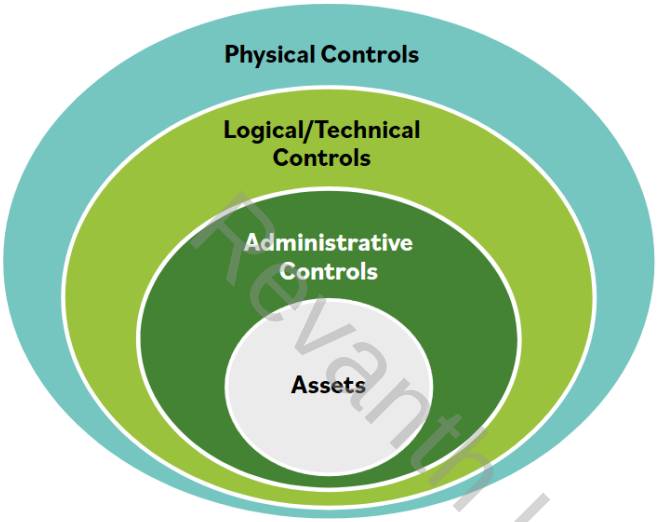
Defense in Depth

All-access permissions includes access to buildings, server rooms, networks, 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 an account, followed by a code sent to the user’s phone to verify their 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.

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 to only 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 example.

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.

This scenario illustrates 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 with 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, server, 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 managers, supervisors, leadership, or support staff 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. Even non-privileged 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 gaining those privileges. Just-in-time identity should also be considered a way to restrict the use of these privileges to specific tasks and the times at 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 non-disclosure 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

Consider the Help Desk role. In order to provide the level of service customers demand, it may be necessary for 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.

Separation of Duties

A core element of authorization is the principle of separation of duties (also known as segregation of duties).

Separation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish.

Separation 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 separation of duties to jointly commit fraud. This is called collusion.

Another implementation of separation 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 given authorized access to objects after they have been authenticated. 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, as the separated employee is unable to access company data after separation; 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.

The Benefit of Multiple Controls

Physical Security 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 Security Controls?

Physical access controls 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 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, enrolment 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
- Proximity
- Hybrid
- Magnetic stripe
- Smart

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 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 use characteristics unique to the individual seeking access. A biometric authentication solution entails two processes:

- **Enrollment**

During the enrolment process, the user's registered biometric code is stored either 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. Biometric takes two primary forms: physiological and behavioral

Physiological:
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:
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 present 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, monitoring personnel and equipment entering and leaving, and auditing and logging all physical events are primary elements in maintaining overall organizational security.

Monitoring Examples:

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

This section will concentrate 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.
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 to avoid missing 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 such as the closest fire department.
Finally, another common type of alarm system is 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.

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 subjects and objects in an information system.

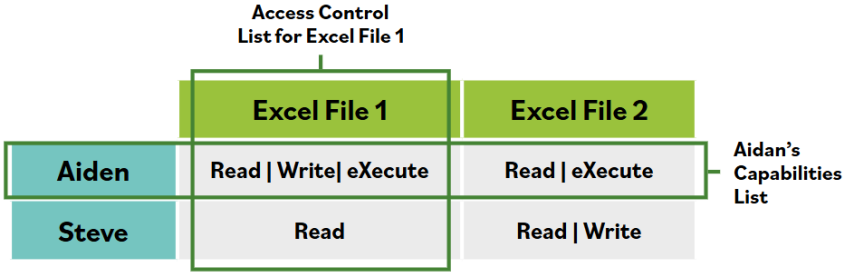
In DAC, the policy specifies that a subject who has been granted access to information can do one or more of the following:

● 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
● Change the rules governing access control; mandatory access controls restrict this capability

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. DAC can also be 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.

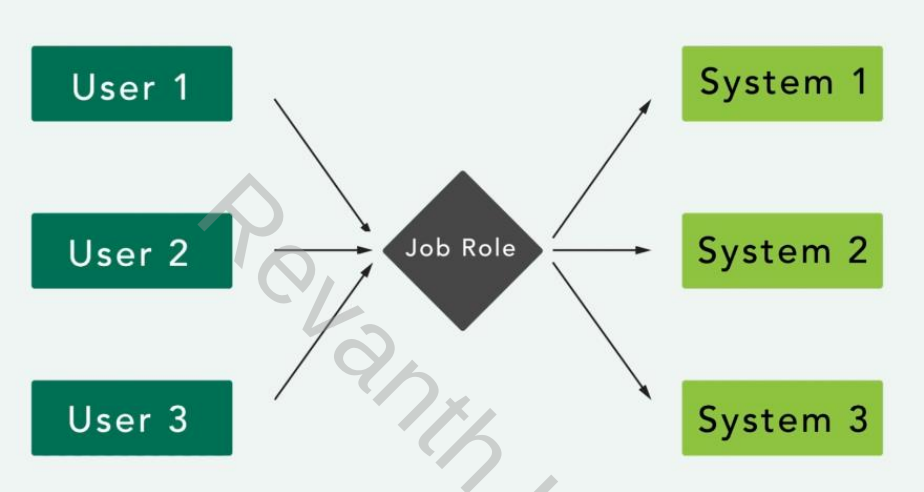
Mandatory Access Control (MAC) in the Workplace

Mandatory access control is determined by the owner of the assets, on an 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 the scope of work is limited and users do not have access to information that does not concern them. This separation of duties is also facilitated by **role-based access control.**

Role-Based Access Control



Role-Based Access Control (RBAC) in the Workplace

Role-based access control provides each worker privileges based on what role they have in the organization.
Only Human Resources has 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 one person's permissions are expanded for a specific reason—say, a junior worker's permissions might be expanded so they can temporarily act as the department manager—but their permissions aren't changed 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.

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.

Controls and Risks

A control serves to reduce the risk according to where it falls 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.

These controls together 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. Because there is a risk of a tall bookshelf toppling over and possibly hurting someone, local building codes or regulations might require bookshelves to be secured to a wall using a strap or a bracket.
In this case, the risk is the injury to people. An administrative control is the building code, and the actual attachment of the shelf to the wall is the physical control. Both administrative and physical controls work together to mitigate the risk.

Domain 4: Network Security

Networking

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 door 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

Hubs:

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.

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:

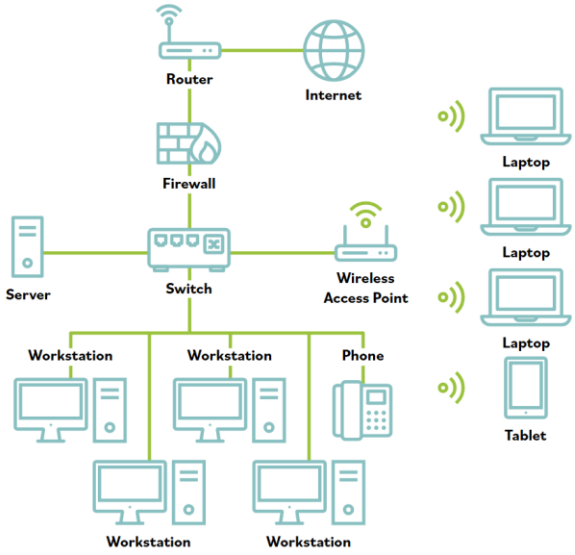
Every network device is assigned a Media Access Control (MAC) address. An example is 00-13-02-1F-58-F5. The first 3 bytes (24 bits) of the address denote the vendor or manufacturer of the physical network interface. No two devices can have the same MAC address in the same local network; otherwise an address conflict occur.

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 are192.168.1.1 and 2001:db8::ffff:0:1

Networking at a Glance

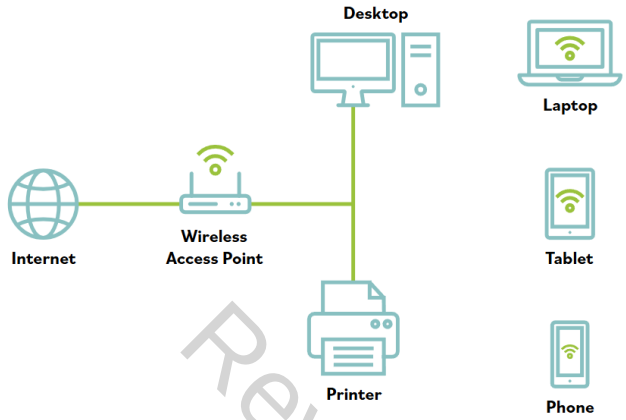
A Small Business Network



This diagram represents a small business network. 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.

A Typical Home Network



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.

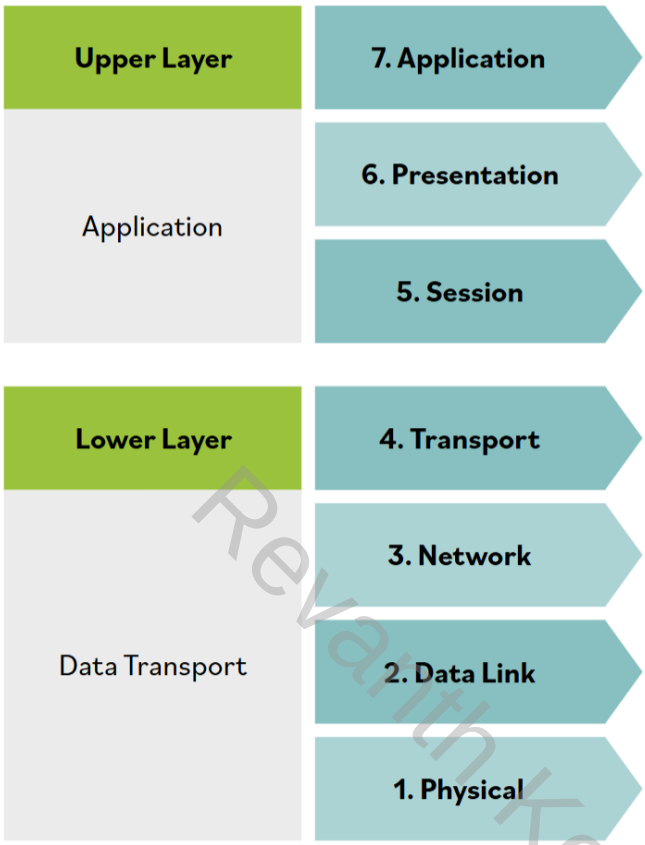
Networking Models

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:

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:

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 the buckets are 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 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, for example, 01010111, and sent across physical wires such as an ethernet cable.

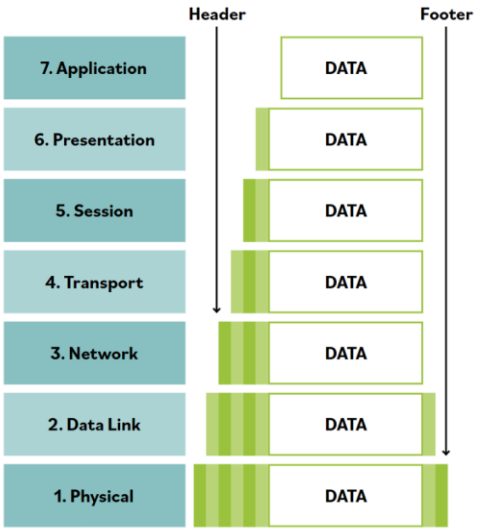
It's worth mapping some common networking terminology to the OSI Model so you can see the value in the conceptual model.

Consider the following examples:

- When referencing image file like a JPEG or PNG, we are talking about presentation layer (6).
- When discussing routers that are sending packets, we are discussing the network layer (3).
- When discussing switches, bridges, or WAPs sending frames, we are discussing data link layer (2).
- 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)

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 number of resources and is relatively easy to hack into because it was designed for ease of use rather than for security.
At the Application Layer, TCP/IP protocols include Telnet, File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), and Domain Name Service (DNS).

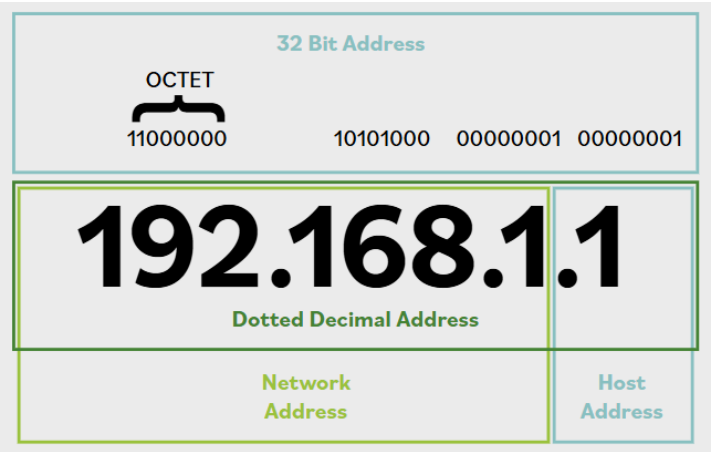
The two primary transport layer protocols of TCP/IP are TCP and UDP. TCP is a full-duplex connection-oriented protocol, whereas UDP is a simplex connectionless protocol. In the internet layer, Internet

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.

<table>
<tr><th>OSI Model Layers</th><th>TCP/IP Protocol Architecture</th><th colspan="4">TCP/IP Protocol Suite</th></tr>
<tr><td>Application Layer</td><td rowspan="3">Application Layer</td><td>FTP</td><td>Telnet</td><td>SNMP</td><td>LPD</td></tr>
<tr><td>Presentation Layer</td><td rowspan="2">TFTP</td><td rowspan="2">SMTP</td><td rowspan="2">NFS</td><td rowspan="2">X Window</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Network Layer</td><td>Internet Layer</td><td>ICMP</td><td colspan="2">IP</td><td>ICMP</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Network Interface Layer</td><td rowspan="2">Ethernet</td><td rowspan="2">Fast Ethernet</td><td rowspan="2">Token Ring</td><td rowspan="2">FDDI</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

Internet Protocol (IPv4 and IPv6)

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



IP hosts/devices associate an address with a unique logical address. An IPv4 address is expressed as four octets separated by a dot (.), for example, 216.12.146.140

Each octet may have a value between 0 and 255. However, 0 is the network itself (not a device on that network), and 255 is generally reserved for broadcast purposes. Each address is subdivided into

two parts: the network number and the host. The network number assigned by an external organization, such as the Internet Corporation for Assigned Names and Numbers (ICANN), represents the organization's network. The host represents the network interface within the network.
To ease network administration, networks are typically divided into subnets. Because subnets cannot be distinguished with the addressing scheme discussed so far, a separate mechanism, the subnet mask, is used to define the part of the address used for the subnet. The mask is usually converted to decimal notation like 255.255.255.0.

With the ever-increasing number of computers and networked devices, it is clear that IPv4 does not provide enough addresses for our needs. To overcome this shortcoming, IPv4 was subdivided into public and private address ranges. Public addresses are limited with IPv4, but this issue was addressed in part with private addressing. Private addresses can be shared by anyone, and it is highly likely that everyone on your street is using the same address scheme.
The nature of the addressing scheme established by IPv4 meant that network designers had to start thinking in terms of IP address reuse. IPv4 facilitated this in several ways, such as its creation of the private address groups; this allows every LAN in every small office/home office (SOHO) situation to use addresses such as 192.168.2.xxx for its internal network addresses, without fear that some other system can intercept traffic on their LAN.

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

Range
10.0.0.0 to 10.255.255.254
172.16.0.0 to 172.31.255.254
192.168.0.0 to 192.168.255.254

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

IPv6 is a modernization of IPv4, which addressed a number of weaknesses in the IPv4 environment:
● A much larger address field: IPv6 addresses are 128-bits, which supports 2128 or 340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 hosts. This ensures that we will not run out of addresses.
● Improved security: IPsec is an optional par of IPv4 networks, but a mandatory component of IPv6 networks. This will help ensure the integrity and confidentiality of IP packets and allow communicating partners to authenticate each other.
● Improved quality of service (QoS): This will help services obtain an appropriate share of a network's bandwidth

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

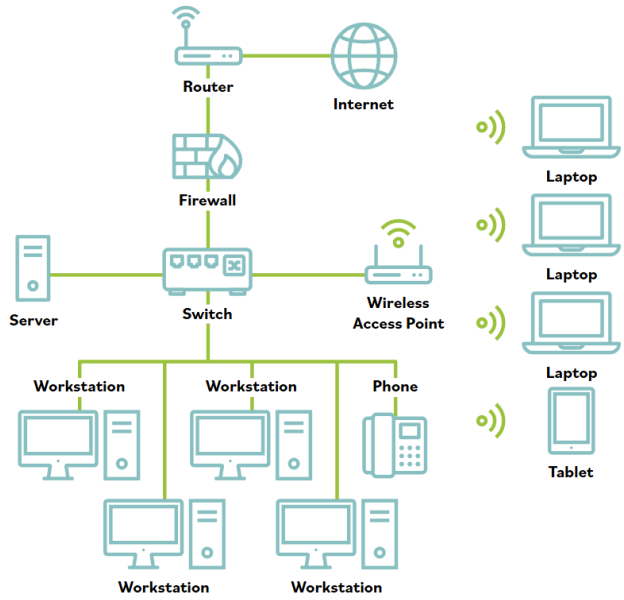
- ::1 is the local loopback address, used the same as 127.0.0.1 in IPv4.
- The range 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff is reserved for documentation use, just like in the examples above. fc00:: to fdff: ffff:ffff:ffff:ffff:ffff:ffff:ffff are addresses reserved for internal network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

Wi-Fi

Wireless networking is a popular method of connecting corporate and home systems because of the ease of deployment and relatively low cost.

It has made networking more versatile than ever before. Workstations and portable systems are no longer tied to a cable but can roam freely within the signal range of the deployed wireless access points. However, with this freedom comes additional vulnerabilities.

Wi-Fi range is generally wide enough for most homes or small offices, and range extenders may be placed strategically to extend the signal for larger campuses or homes. Over time the Wi-Fi standard has evolved, with each updated version faster than the last.
In a LAN, threat actors need to enter the physical space or immediate vicinity of the physical media itself. For wired networks, this can be done by placing sniffer taps onto cables, plugging in USB devices, or using other tools that require physical access to the network. By contrast, wireless media intrusions can happen at a distance.



Security of the Network

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

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

Ports and Protocols (Applications/Services)

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

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

Logical Ports:

When a communication connection is established between two systems, it is done using ports. A logical port (also called a socket) is little more than an address number that both ends of the communication link agree to use when transferring data.

Ports allow a single IP address to support multiple simultaneous communications, each using a different port number. In the application layer of the TCP/ IP Model, which includes the session, presentation, and application layers of the OSI Model, resides numerous application- or service-specific protocols. Data types are mapped using port numbers associated with services. For example, web traffic (or HTTP) is port 80. Secure web traffic (or HTTPS) is port 443. Table 5.4 highlights some of these protocols and their customary or assigned ports. Note that in several cases a service or protocol may have two ports assigned, one secure and one nonsecure.

When in doubt, systems should be implemented using the most secure version of a protocol and its services.

● Well-known ports (0–1023):

These ports are related to the common protocols that are at the core of the Transport Control Protocol/Internet Protocol (TCP/IP) model, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc.

● Registered ports (1024–49151):

These ports are often associated with proprietary applications from vendors and developers. While they are officially approved by the Internet Assigned Numbers Authority (IANA), in practice many

vendors simply implement a port of their choosing. Examples include Remote Authentication Dial-In User Service (RADIUS) authentication (1812), Microsoft SQL Server (1433/1434) and the Docker REST API (2375/2376).

● Dynamic or private ports (49152–65535):
Whenever a service is requested that is associated with well-known or registered ports, those services will respond with a dynamic port that is used for that session and then released.

Secure Ports

Some network protocols transmit information in clear text, meaning it is not encrypted and should not be used. Clear text information is subject to network sniffing. This tactic uses software to inspect packets of data as they travel across the network and extract text such as usernames and passwords.

Network sniffing could also reveal the content of documents and other files if they are sent via insecure protocols. The table below shows some of the insecure protocols along with recommended secure alternatives.

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

23-Telnet				
Insecure Port	**Description**	**Protocol**	**Secure Alternative Port**	**Protocol**
23-Telnet	Port 23, telnet, is used by many Linux systems and any other systems as a basic text-based terminal. All information to and from the host on a telnet connection is sent in plaintext and can be intercepted by an attacker. This includes username and password as well as all information that is being presented on the screen, since this interface is all text. Secure Shell (SSH) on port 22 uses encryption to ensure that traffic between the host and terminal is not sent in a plaintext format.	Telnet	22*-SSH	Secure Shell

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

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

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

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

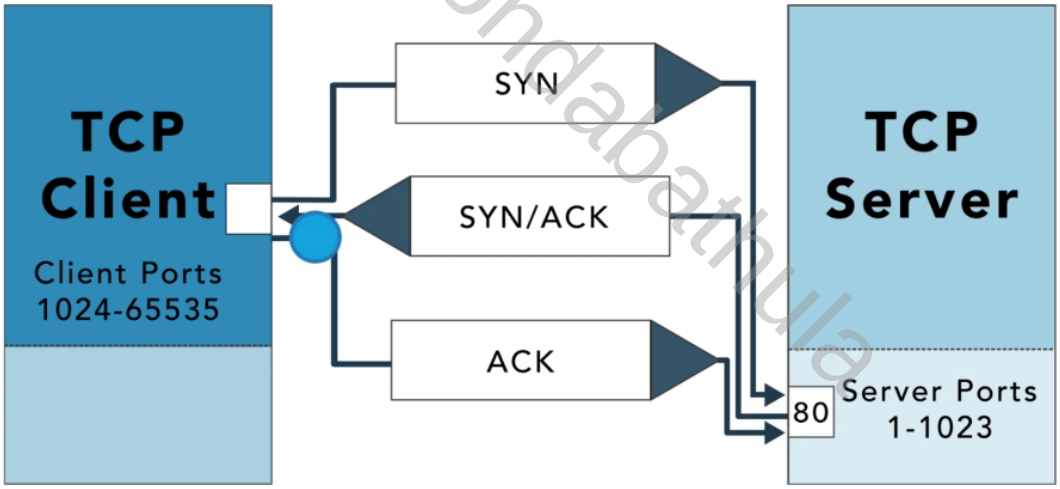
143-IMAP				
Insecure Port	**Description**	**Protocol**	**Secure Alternative Port**	**Protocol**
143-IMAP	Port 143, Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing. The secure alternative is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

161/162-SNMP				
Insecure Port	**Description**	**Protocol**	**Secure Alternative Port**	**Protocol**
161/162-SNMP	Ports 161 and 162, Simple Network Management Protocol, are commonly used to send and receive data used for managing infrastructure devices. Because sensitive information is often included in these messages, it is recommended to use SNMP version 2 or 3 (abbreviated SNMPv2 or SNMPv3) to include encryption and additional security features. Unlike many others discussed here, all versions of SNMP use the same ports, so there is not a definitive secure and insecure pairing. Additional context is needed to determine whether information on ports 161 and 162 is secured.	Simple Network Management Protocol	161/162-SNMP	SNMPv3

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

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

SYN, SYN-ACK, ACK Handshake



Types of Threats

Spoofing:

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

Phishing:

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

DOS/DDOS:

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

Virus:

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

Worm:

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

Trojan:

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

On-path Attack:

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

Side-channel:

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

Advanced Persistent Threat (APT):

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

Insider Threat:

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

Malware:

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

Ransomware:

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

Tools to Identify and Prevent Threats

Tools	Description	Identifies Threats	Prevent Threats
Intrusion Detection System (IDS)	A form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures.	✓	
Host-basaed IDS (HIDS)	Monitors activity on a single computer.	✓	
Network-based IDS (NIDS)	Monitors and evaluates network activity to detect attacks or event anomalies.	✓	
SIEM	Gathers log data from sources across an enterprise to understand security concerns and apportion resources.	✓	
Anti-malware/Antivirus	Seeks to identify malicious software or processess.	✓	✓
Scans	Evaluates the effectiveness of security controls.	✓	
Firewall	Filters network traffic - manages and controls network traffic and protects the network.	✓	✓
Intrusion Protection System (IPS-NIPS/HIPS)	An active IDS that automatically attempts to detect and block attacks before they reach target systems.	✓	✓

Intrusion Detection System (IDS)

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resources.

Intrusion detection is a specific form of monitoring that monitors recorded information and real-time events to detect abnormal activity indicating a potential incident or intrusion.

An intrusion detection system (IDS) automates the inspection of logs and real-time system events to detect intrusion attempts and system failures.

An IDS is intended as part of a defense-in-depth security plan. It will work with, and complement, other security mechanisms such as firewalls, but it does not replace them.

IDSs can recognize attacks that come from external connections, such as an attack from the internet, and attacks that spread internally, such as a malicious worm. Once they detect a suspicious event, they respond by sending alerts or raising alarms. A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions.

Intrusion detection and prevention refer to capabilities that are part of isolating and protecting a more secure or more trusted domain or zone from one that is less trusted or less secure. These are natural functions to expect of a firewall, for example.

IDS types are commonly classified as host- based and network-based. A host-based IDS (HIDS) monitors a single computer or host. A network-based IDS (NIDS) monitors a network by observing network traffic patterns.

Host-based Intrusion Detection System (HIDS):

A HIDS monitors activity on a single computer, including process calls and information recorded in system, application, security, and host-based firewall logs. It can often examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack. It can also track processes employed by the attacker. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect.

For example, a HIDS can detect infections where an intruder has infiltrated a system and is controlling it remotely. HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration. A HIDS cannot detect network attacks on other systems.

Network Intrusion Detection System (NIDS):

A NIDS monitors and evaluates network activity to detect attacks or event anomalies. It cannot monitor the content of encrypted traffic but can monitor other packet details. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console. These sensors can monitor traffic at routers, firewalls, network switches that support port mirroring, and other types of network taps.

A NIDS has very little negative effect on the overall network performance, and when it is deployed on a single-purpose system, it doesn't adversely affect performance on any other computer. A NIDS is usually able to detect the initiation of an attack or ongoing attacks, but they can't always provide information about the success of an attack. They won't know if an attack affected specific systems, user accounts, files, or applications. Intrusion Detection Systems.

Security Information and Event Management (SIEM):

Security management involves the use of tools that collect information about the IT environment from many disparate sources to better examine the overall security of the organization and streamline security efforts.

These tools are generally known as security information and event management (or SI-E-M, pronounced "SIM") solutions. The general idea of a SIEM solution is to gather log data from various sources across the enterprise to better understand potential security concerns and apportion resources accordingly.

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

Preventing Threats

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

- **Keep systems and applications up to date.** Vendors regularly release patches to correct bugs and security flaws, but these only help when they are applied. Patch management ensures that systems and applications are kept up to date with relevant patches
- **Remove or disable unneeded services and protocols.** If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system. As an extreme contrast, imagine a web server is running every available service and protocol. It is vulnerable to potential attacks on any of these services and protocols.
- **Use intrusion detection and prevention systems.** Intrusion detection and prevention systems observe activity, attempt to detect threats, and provide alerts. They can often block or stop attacks.
- **Use up-to-date anti-malware software**. A primary countermeasure is anti-malware software
- **Use firewalls.** Firewalls can prevent many different types of threats. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems

Antivirus

The use of antivirus products is strongly encouraged as a security best practice and is a requirement for compliance with the Payment Card Industry Data Security Standard (PCI DSS).

There are several antivirus products available, and many can be deployed as part of an enterprise solution that integrates with several other security products.

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

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

Scans

Regular vulnerability and port scans are a good way to evaluate the effectiveness of security controls used within an organization.

They may reveal areas where patches or security settings are insufficient, where new vulnerabilities have developed or become exposed, and where security policies are either ineffective or not being followed. Attackers can exploit any of these vulnerabilities.

Firewalls

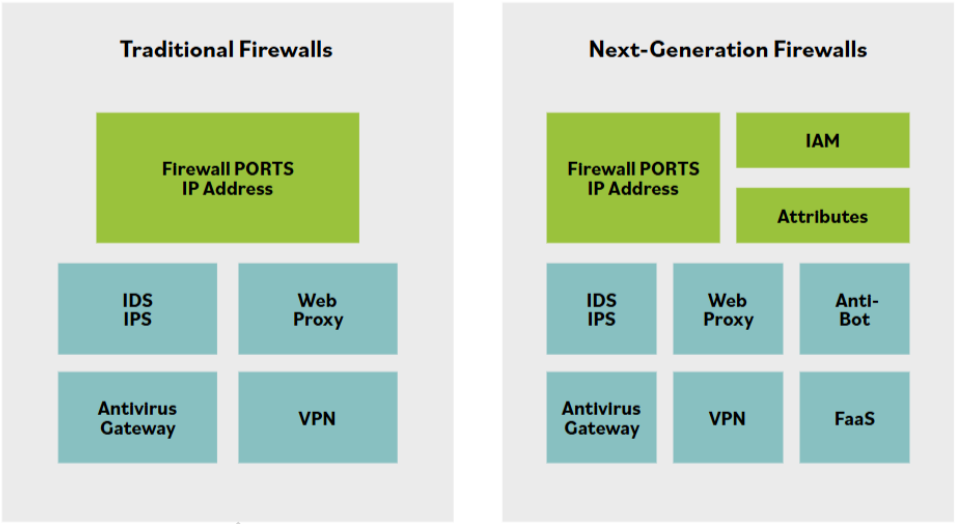
In building construction or vehicle design, a firewall is a specially built physical barrier that prevents the spread of fire from one area of the structure to another or from one compartment of a vehicle to another.

Early computer security engineers borrowed that name for the devices and services that isolate network segments from each other, as a security measure. As a result, firewalling refers to the process of designing, using, or operating different processes in ways that isolate high-risk activities from lower-risk ones.

Firewalls enforce policies by filtering network traffic based on a set of rules. While a firewall should always be placed at internet gateways, other internal network considerations and conditions determine where a firewall would be employed, such as network zoning or segregation of different levels of sensitivity.

Firewalls have rapidly evolved over time to provide enhanced security capabilities. This growth in capabilities can be seen in the graphic below, which contrasts an oversimplified view of traditional and next- generation firewalls.

It integrates a variety of threat management capabilities into a single framework, including proxy services, intrusion prevention services (IPS) and tight integration with the identity and access management (IAM) environment to ensure only authorized users are permitted to pass traffic across the infrastructure. While firewalls can manage traffic at Layers 2 (MAC addresses), 3 (IP ranges) and 7 (application programming interface (API) and application firewalls), the traditional implementation has been to control traffic at Layer 4.



Intrusion Prevention System (IPS)

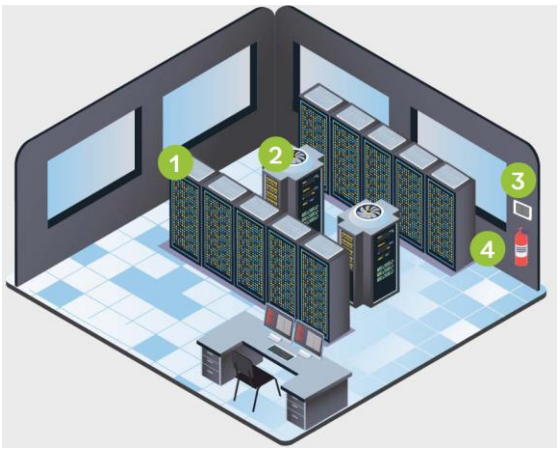
An intrusion prevention system (IPS) is a special type of active IDS that automatically attempts to detect and block attacks before they reach target systems.

A distinguishing difference between an IDS and an IPS is that the IPS is placed in line with the traffic.

In other words, all traffic must pass through the IPS and the IPS can choose what traffic to forward and what traffic to block after analyzing it. This allows the IPS to prevent an attack from reaching a target. Since IPS systems are most effective at preventing network- based attacks, it is common to see the IPS function integrated into firewalls. Just like IDS, there are Network-based IPS (NIPS) and Host-based IPS (HIPS).

On-Premises Data Centers

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



1. Data Center/Closets

The facility wiring infrastructure is integral to overall information system security and reliability. Protecting access to the physical layer of the network is impor□ant in minimizing intentional or unintentional damage. Proper protection of the physical site must address these sor□s of security challenges.

Data centers and wiring closets may include the following:
● Phone, network, special connections
● ISP or telecommunications provider equipment
● Servers
● Wiring and/or switch components

2. Heating, Ventilation, and Air Conditioning (HVAC) / Environmental

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

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

3. Power

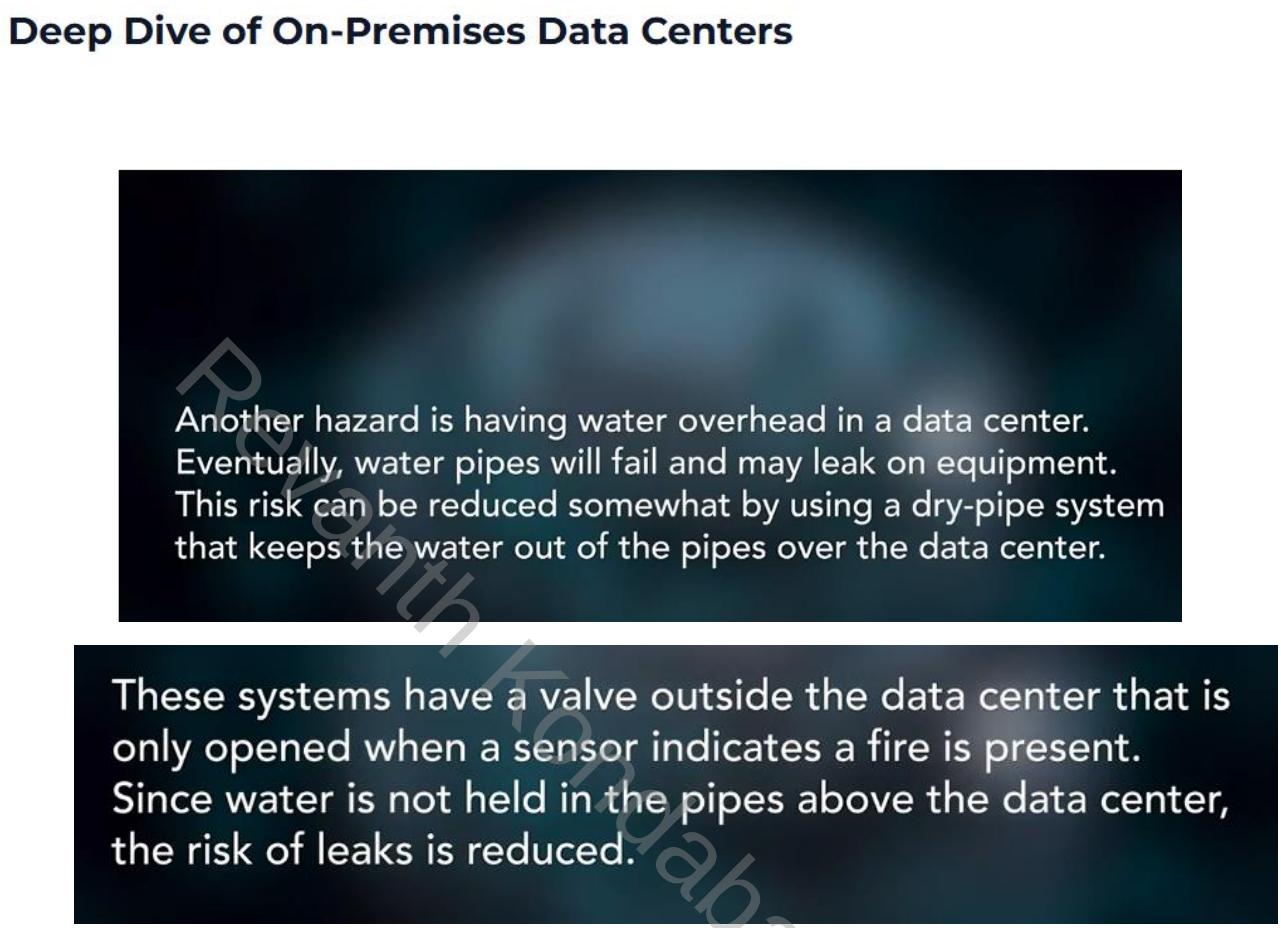
Data centers and information systems in general consume a tremendous amount of electrical power, which needs to be delivered both constantly and consistently. Wide fluctuations in the quality of power affect system lifespan, while disruptions in supply completely stop system operations.

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

4. Fire Suppression

For server rooms, appropriate □ire detection/suppression must be considered based on the size of the room, typical human occupation, egress routes, and risk of damage to equipment.

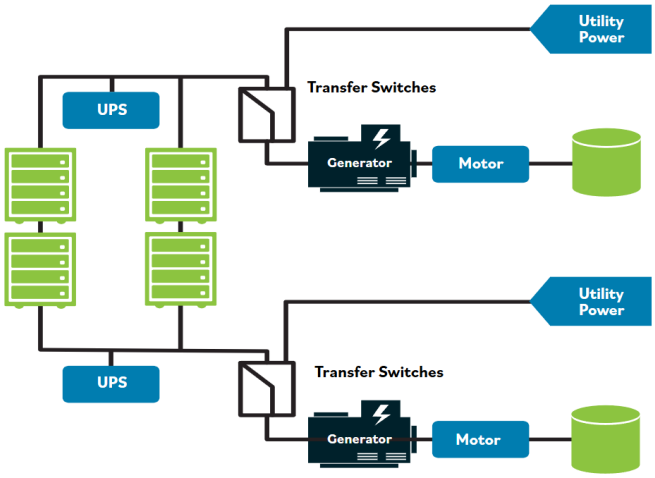
For example, water used for fire suppression would cause more harm to servers and other electronic components. Gas-based fire suppression systems are more friendly to the electronics, but can be toxic to humans.



Redundancy

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

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



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

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

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

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

The difference between an MOA or MOU and a service-level agreement (SLA) is that an MOU is more directly related to what can be done with a system or the information.

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

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

Cloud Computing

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

Cloud computing is similar to the electrical or power grid. It is provisioned in a geographic location and is sourced using an electrical means that is not necessarily obvious to the consumer. However, when you want electricity, it's available via a common standard interface and you pay only for what you use.

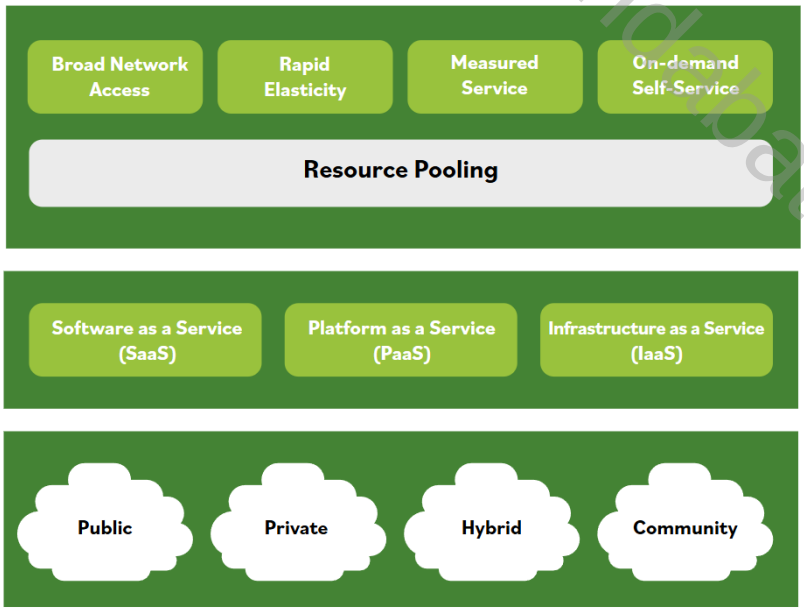
Cloud computing is scalable, elastic, and easy-to-use for the provisioning and deployment of Information Technology (IT) services.

There are various definitions of what cloud computing means per leading standards, including NISTs.

This NIST definition is commonly used around the globe, cited by professionals to clarify what the term "cloud" means:

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

This image depicts cloud computing characteristics, service, and deployment models.



Cloud Characteristics

Cloud-based assets include any resources that an organization accesses using cloud computing. Cloud computing refers to on-demand access to computing resources available from almost

anywhere, and cloud computing resources are highly available and easily scalable. Organizations typically lease cloud-based resources from outside the organization.

Cloud computing has many benefits for organizations, which include but are not limited to:

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

Service Models

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

There are varying levels of responsibility for assets depending on the service model. This includes maintaining the assets, ensuring they remain functional, and keeping the systems and applications up to date with current patches.

In some cases, the cloud service provider is responsible for these steps. In other cases, the consumer is responsible.

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

Deployment Models

There are four cloud deployment models. The cloud deployment model also a fects the breakdown of responsibilities of the cloud-based assets.

The four cloud models available are public, private, hybrid, and community.

Public:

Public clouds are commonly referred to as clouds for the public user. It is easy to access a public cloud. There is no real mechanism, other than applying for and paying for the cloud service. It is open to the public and is, therefore, a shared resource that many people can use as part of a resource pool.

A public cloud deployment model includes assets available for any consumers to rent or lease and is hosted by an external cloud service provider (CSP). Service-level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization.

Private:

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

Hybrid:

A hybrid cloud deployment model is created by combining two forms of cloud computing deployment models, typically a public and private cloud. Hybrid cloud computing is gaining popularity with organizations by providing them with the ability to retain control of their IT environments, conveniently allowing them to use public cloud service to fulfill non-mission- critical workloads, and taking advantage of flexibility, scalability, and cost savings.

Important drivers or bene its of hybrid cloud deployments include: Retaining ownership and oversight of critical tasks and processes related to technology, Reusing previous investments in technology within the organization, Control over most critical business components and systems, and cost-effective means to fulfilling noncritical business functions.

Community:

Community clouds can be either public or private. What makes them unique is that they are generally developed for a particular community. An example could be a public community cloud focused primarily on organic food, or maybe a community cloud focused specifically on financial services.

The idea behind the community cloud is that people of like minds or similar interests can get together, share IT capabilities and services, and use them in a way that is beneficial for the particular interests that they share.

Managed Service Provider (MSP)

A managed service provider (MSP) is a company that manages information technology assets for another company. Small and medium-sized businesses commonly outsource par□ or all of their information technology functions to an MSP to manage day-to-day operations or to provide expertise in areas the company does not have. Organizations may also use an MSP to provide network and security monitoring and patching services.

Today, many MSPs o fer cloud-based services augmenting SaaS solutions with active incident investigation and response activities. One such example is a managed detection and response (MDR) service, where a vendor monitors firewall and other security tools to provide expertise in triaging events.

Some other common MSP implementations are:

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

Service-Level Agreement (SLA)

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

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

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

Other important SLA points to consider include the following:

- Cloud system infrastructure details and security standards
- Customer right to audit legal and regulatory compliance by the CSP
- Rights and costs associated with continuing and discontinuing service use
- Service availability
- Service performance
- Data security and privacy
- Disaster recovery processes
- Data location
- Data access
- Data portability
- Problem identification and resolution expectations
- Change management processes
- Dispute mediation processes
- Exit strategy

Network Design

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

Network Segmentation:

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

DMZ:

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

VLAN:

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

VPN:

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

NAC:

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

Defense in Depth

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

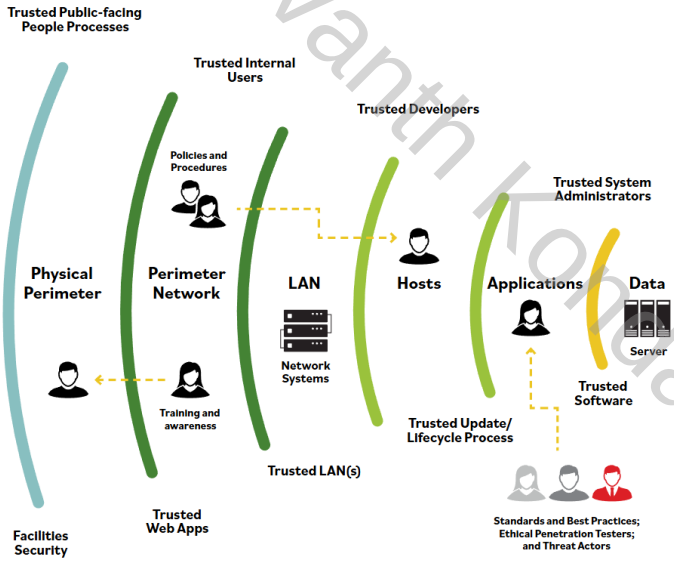
Defense in depth uses a layered approach when designing the security posture of an organization. Think about a castle that holds the crown jewels. The jewels will be placed in a vaulted chamber in a central location watched over by security guards. The castle is built around the vault with additional layers of security—soldiers, walls, and a moat.

The same approach is true when designing the logical security of a facility or system. Using layers of security will deter many attackers and encourage them to focus on other, easier targets.

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

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

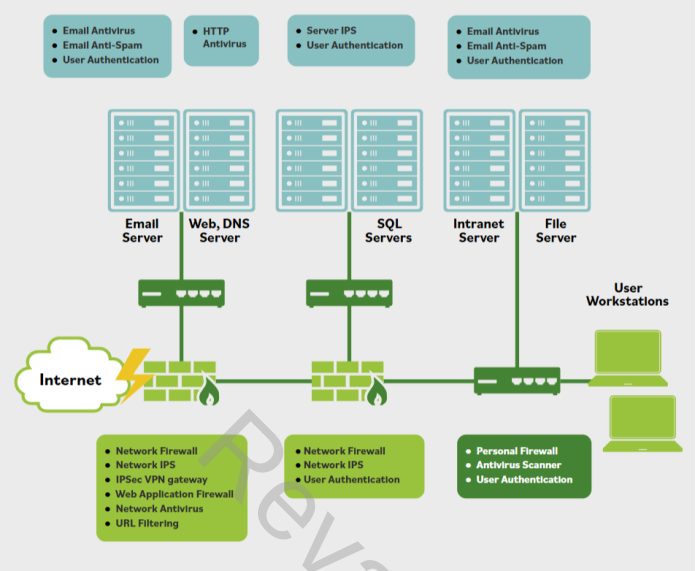
- **Data:** Controls that protect the actual data with technologies such as encryption, data leak prevention, identity and access management and data controls.
- **Application:** Controls that protect the application with technologies such as data leak prevention, application firewalls and database monitors.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



Zero Trust

Zero trust networks are often microsegmented networks, with firewalls at nearly every connecting point. Zero trust encapsulates information assets, the services that apply to them, and their security properties.

This concept recognizes that once inside a trust-but-verify environment, a user has perhaps unlimited capabilities to roam around, identify assets and systems, and potentially find exploitable vulnerabilities. Placing a greater number of firewalls or other security boundary control devices throughout the network increases the number of opportunities to detect a troublemaker before harm is done. Many enterprise architectures are pushing this to the extreme of microsegmenting their internal networks, which enforces frequent reauthentication of a user ID, as depicted in this image.



Consider a rock music concert. If traditional perimeter controls, such as firewalls, are employed, you would show your ticket at the gate and have free access to the venue, including backstage where the real rock stars are.

In a zero-trust environment, additional checkpoints are added. Your identity (ticket) is validated to access the floor level seats, and again to access the backstage area. Your credentials must be valid at all three levels to meet the stars of the show.

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

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

Network Access Control (NAC)

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

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

Considering just IoT for a moment, it is impor ant to understand the range of devices that might be found within an organization. They include heating, ventilation and air conditioning (HVAC) systems that monitor the ambient temperature and adjust the heating or cooling levels automatically, or air

monitoring systems, to security systems, sensors, and cameras, right down to vending and co□fee machines. Look around your own environment and you will quickly see their scale of use.

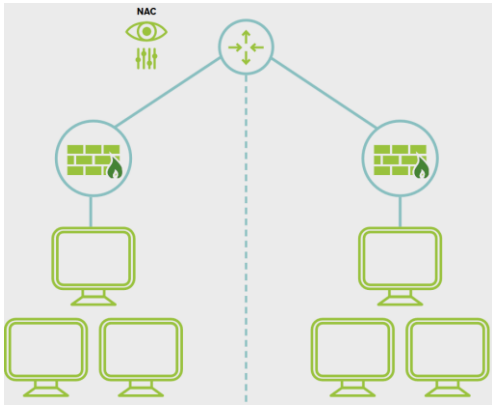
Having identified the need for a NAC solution, you need to identify what capabilities a solution may provide. As you know, everything begins with a policy. The organization's access control policies and associated security policies should be enforced via the NAC devices. Remember, of course, that an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

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

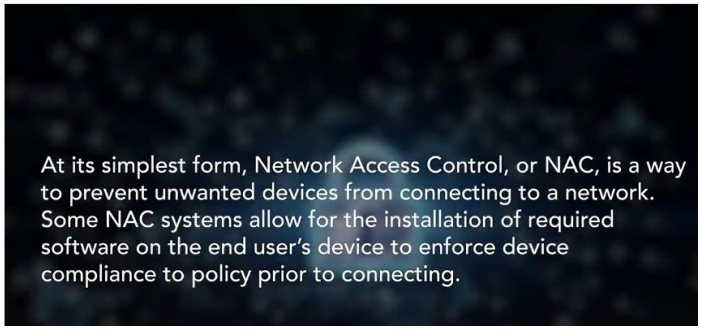
Let's consider some possible use cases for NAC deployment:

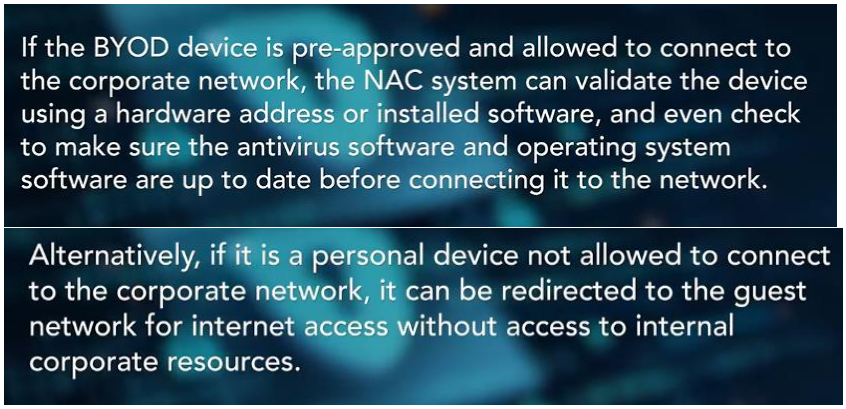
- Medical devices
- IoT devices
- BYOD/mobile devices (e.g., laptops, tablets, smar phones)
- Guest users and contractors

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



Network Access Control (NAC) Deeper Dive

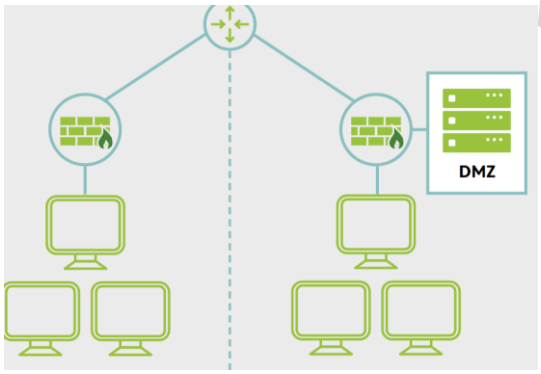




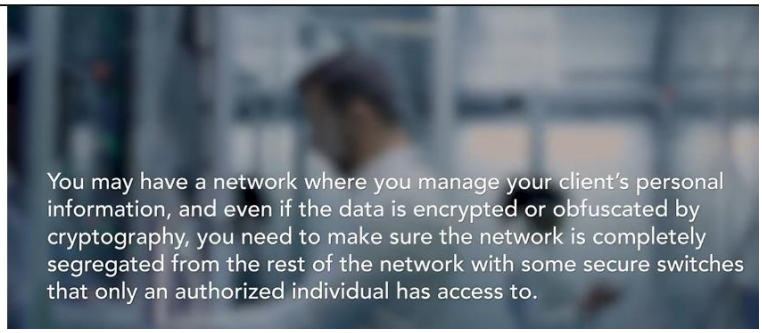
Network Segmentation: Demilitarized Zone (DMZ)

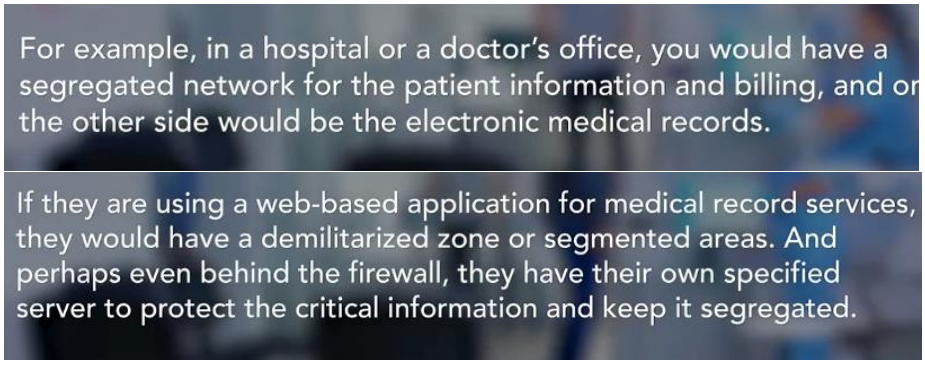
Network segmentation is an effective way to achieve defense in depth for distributed or multitiered applications. The use of a demilitarized zone (DMZ), for example, is a common practice in security architecture.

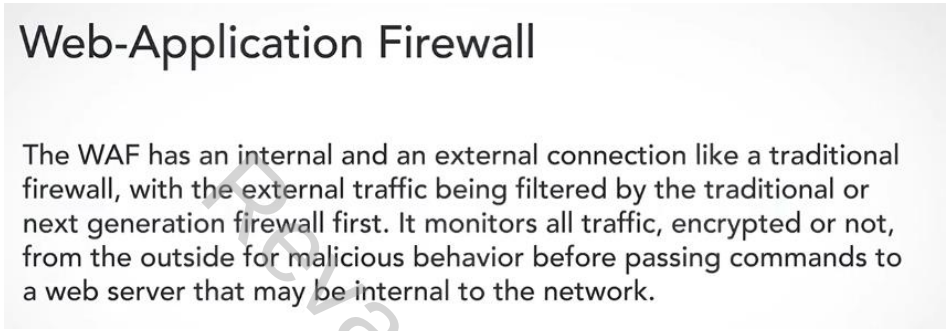
With a DMZ, host systems that are accessible through the irewall are physically separated from the internal network by means of secured switches or by using an additional irewall to control tra ic between the web server and the internal network. Application DMZs (or semi-trusted networks) are frequently used today to limit access to application servers to those networks or systems that have a legitimate need to connect.



DMZ (Demilitarized Zone) Deeper Dive







Segmentation for Embedded Systems and IoT

An embedded system is a computer implemented as part of a larger system. The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it is a component.

Examples of embedded systems include network-attached printers, smart TVs, HVAC controls, smart appliances, smart thermostats and medical devices. Segmentation for Embedded Systems and IoT

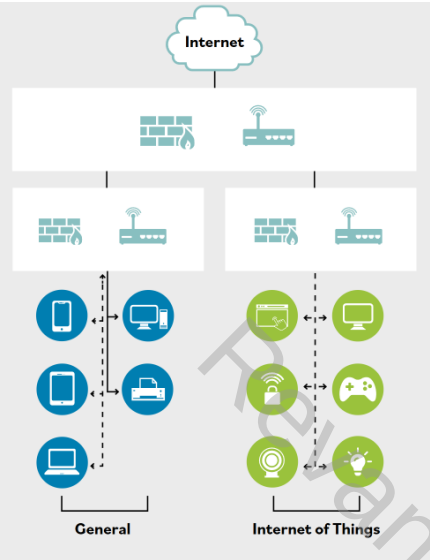
Network-enabled devices are any type of portable or non-portable device that has native network capabilities. This generally assumes the network in question is a wireless type of network, typically provided by a mobile telecommunications company. Network-enabled devices include smartphones, mobile phones,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

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

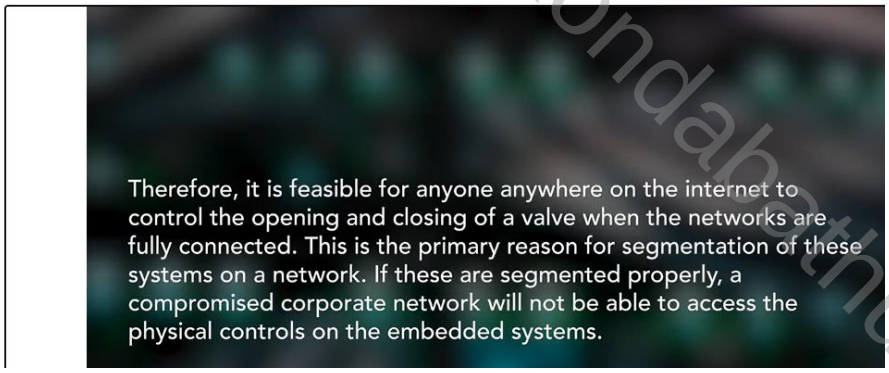
Embedded systems and network-enabled devices that communicate with the internet are considered IoT devices and need special attention to ensure that communication is not used in a malicious manner.

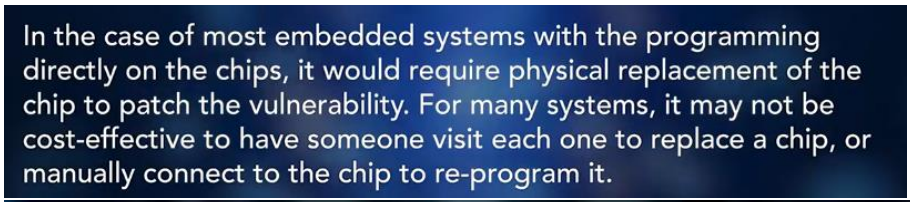
Because an embedded system is often in control of a mechanism in the physical world, a security breach could cause harm to people and property. Since many of these devices have multiple access

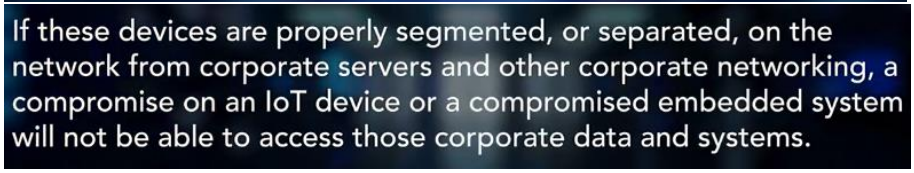
routes, such as ethernet, wireless, or Bluetooth, special care should be taken to isolate them from other devices on the network. You can impose logical network segmentation with switches using VLANs, or through other traffic-control means, including MAC addresses, IP addresses, physical ports, protocols, or application filtering, routing, and access control management. Network segmentation can be used to isolate IoT environments.



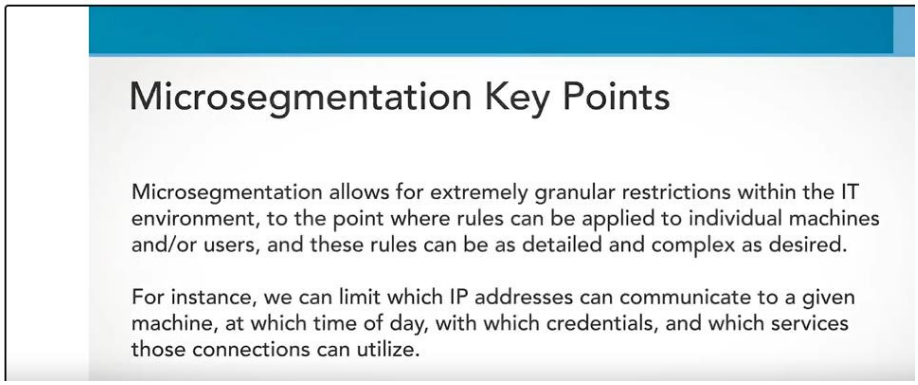
Segmentation for Embedded Systems and IoT Deeper Dive







Microsegmentation Characteristics



Microsegmentation Key Points

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

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

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

Microsegmentation allows the organization to limit which business functions/units/offices/departments can communicate with others, in order to enforce the concept of least privilege.

For instance, the Human Resources office probably has employee data that no other business unit should have access to, such as employee home address, salary, medical records, etc. Microsegmentation, like VLANs, can make HR its own distinct IT enclave, so that sensitive data is not available to other business entities, thus reducing the risk of exposure.

In modern environments, microsegmentation is available because of virtualization and software-defined networking (SDN) technologies. In the cloud, the tools for applying this strategy are often called "virtual private networks (VPN)" or "security groups."

Even in your home, microsegmentation can be used to separate computers from smart TVs, air conditioning, and smart appliances which can be connected and can have vulnerabilities.

Virtual Local Area Network (VLAN)

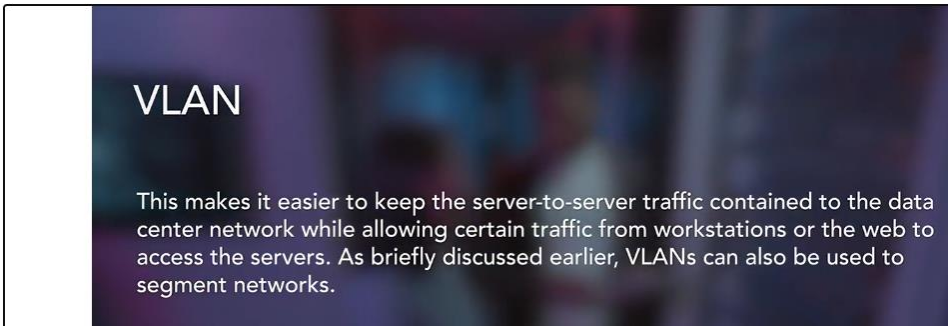
Virtual local area networks (VLANs) allow network administrators to use switches to create software-based LAN segments, which can segregate or consolidate traffic across multiple switch ports.

Devices that share a VLAN communicate through switches as if they were on the same Layer 2 network. The image below shows different VLANs—red, green, and blue—connecting separate sets of ports together, while sharing the same network segment consisting of the two switches and their connection.

Since VLANs act as discrete networks, communications between VLANs must be enabled. Broadcast traffic is limited to the VLAN, reducing congestion and reducing the effectiveness of some attacks. Administration of the environment is simplified, as the VLANs can be reconfigured when individuals change their physical location or need access to different services. VLANs can be configured based on switch port, IP subnet, MAC address, and protocols.

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

Virtual Local Area Network (VLAN) Segmentation



Virtual Private Network (VPN)

A virtual private network (VPN) is not necessarily an encrypted tunnel. It is simply a point-to-point connection between two hosts that allows them to communicate.

Secure communications can, of course, be provided by the VPN, but only if the security protocols have been selected and correctly configured to provide a trusted path over an untrusted network, such as the internet.

Remote users employ VPNs to access their organization's network, and depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. As an alternative to expensive dedicated point-to-point connections, organizations use gateway-to- gateway VPNs to securely transmit information over the internet between sites or even with business partners.

Microsegmentation

The toolsets of current adversaries are polymorphic in nature and allow threats to bypass static security controls.

Modern cyber attacks take advantage of traditional security models to move easily between systems within a data center. Microsegmentation aids in protecting against these threats.

A fundamental design requirement of microsegmentation is to understand the protection requirements for traffic within a data center and traffic to and from the internet traffic flows.

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

Microsegmentation Characteristics:

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

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

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

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

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

● In modern environments, microsegmentation is available because of virtualization and software-defined networking (SDN) technologies. In the cloud, the tools for applying this strategy are often called "virtual private networks (VPN)" or "security groups."

● Even in your home, microsegmentation can be used to separate computers from smart TVs, air conditioning, and smart appliances, which can be connected and have vulnerabilities

Data Handling

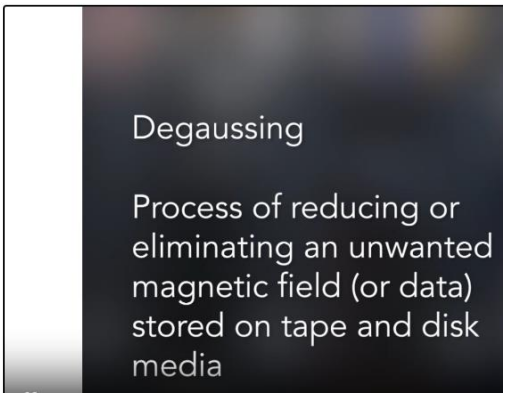
Data goes through its own life cycle as users create, utilize, share, and modify it. Many different models of the life of a data item can be found, but they all have some basic operational steps in common.

The data security life cycle model is useful because it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal). It also helps put the different data states of in use, at rest and in motion, into context. Let's take a closer look.

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

Create: Creating the knowledge, which is usually tacit knowledge at this point.
Store: Storing or recording it in some fashion that makes it explicit.
Use: Using the knowledge, which may cause the information to be modified, supplemented, or partially deleted
Share: Sharing the data with other users, whether as a copy or by moving the data from one location to another.
Archive: Archiving the data when it is temporarily not needed.
Destroy: Destroying the data when it is no longer needed

Data Handling Deep Dive



Data Handling Practices

Data has value and must be handled appropriately.

We will explore the basics of classifying and labeling data to ensure it is treated and controlled in a manner consistent with the sensitivity of the data. In addition, we will complete the data life cycle by documenting retention requirements and ensuring data that is no longer in use is destroyed.

Classification:

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

Before any labels can be attached to sets of data that indicate its sensitivity or handling requirements, the potential impact or loss to the organization needs to be assessed.

This is our first definition: Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality, integrity and availability. Information is then labeled and handled accordingly.

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

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

Labeling:

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

Data Sensitivity Levels and Labels

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

Typically, two or three classifications are manageable, and more than four tend to be difficult.

● Highly restricted: Compromise of data with this sensitivity label could possibly put the organization’s future existence at risk. Compromise could lead to substantial loss of life, injury, or property damage, and litigation and claims would follow.

● Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.

● Low sensitivity (sometimes called “internal use only”): Compromise of data with this sensitivity label could cause minor disruptions, delays, or impacts.

● Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure

Retention:

Information and data should be kept only for as long as it is beneficial, no more and no less. For various types of data, certain industry standards, laws and regulations define retention periods. When such external requirements are not set, it is an organization’s responsibility to define and implement its own data retention policy. Data retention policies are applicable both for hard copies and for electronic data, and no data should be kept beyond its required or useful life.

Security professionals should ensure that data destruction is performed when an asset has reached its retention limit. For the security professional to succeed in this assignment, an accurate inventory must be maintained, including the asset location, retention period requirement, and destruction requirements. Organizations should conduct a periodic review of retained records to reduce the volume of information stored and to ensure that only necessary information is preserved.

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

● Personnel understand the various retention requirements for data of different types throughout the organization.

● The organization appropriately documents the retention requirements for each type of information.

● The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer

A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary “noise” when searching or processing information in search of relevant records.

It may also be in violation of externally mandated requirements such as legislation, regulations or contracts, which may result in fines or other judgments. Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be considered.

Destruction:

Data that might be left on media after deleting is known as remanence and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level.

This can be done by one of several means:

● Clearing the device or system, which usually involves writing multiple patterns of random values throughout all storage media such as main memory, registers and fixed disks. This is sometimes called “overwriting” or “zeroizing” the system, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.

● Purging the device or system, which eliminates, or greatly reduces, the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual “ghosts” of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, degaussing may not be sufficient.

● Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.

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

Logging and Monitoring Security Events

Logging is the primary form of instrumentation that attempts to capture signals generated by events.

Events are any actions that take place within the systems environment and cause measurable or observable change in one or more elements or resources within the system.

Logging imposes a computational cost but is invaluable when determining accountability. Proper design of logging environments and regular log reviews remain best practices regardless of the type of computer system.

Major controls frameworks emphasize the importance of organizational logging practices.

Information that may be relevant to being recorded and reviewed include, but is not limited to:

- User IDs
- System activities
- Dates/times of key events (e.g., logon and logo□□)
- Device and location identity
- Successful and rejected system and resource access attempts
- System configuration changes and system protection activation and deactivation events

Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems, detecting compromises and providing a record of how systems are used.

Robust logging practices provide tools to effectively correlate information from diverse systems to fully understand the relationship between one activity and another.

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

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

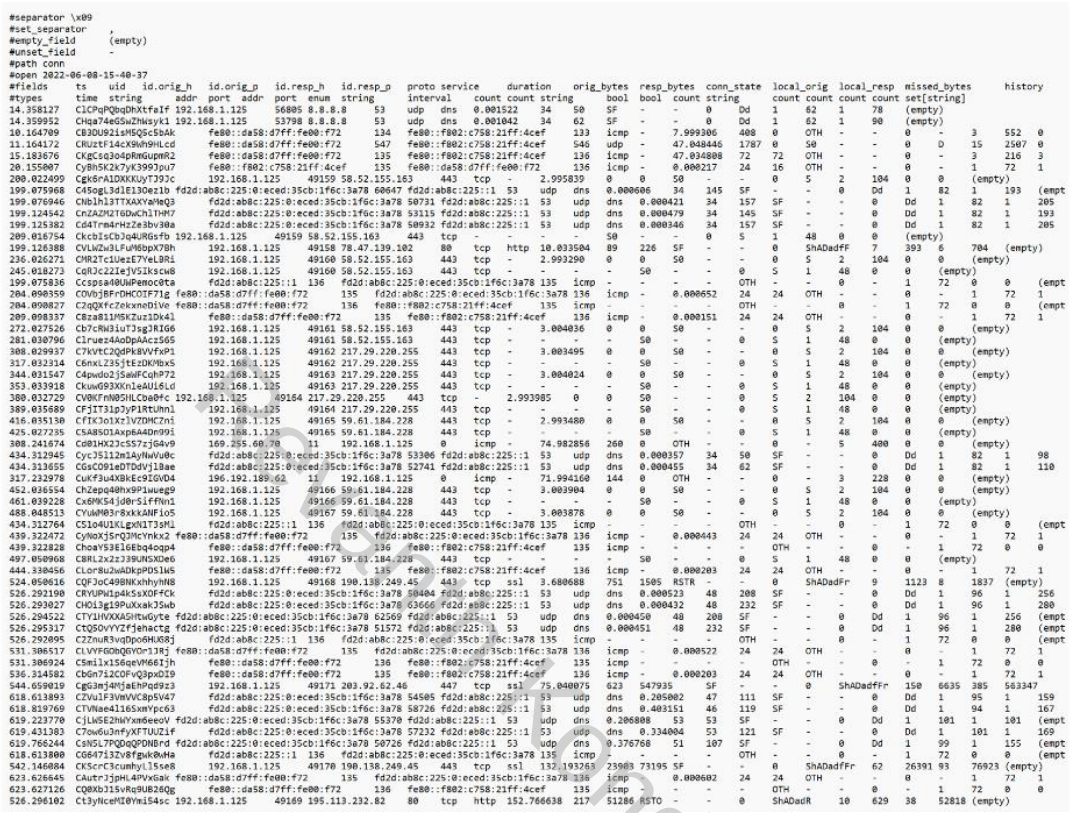
Controls are implemented to protect against unauthorized changes to log information. Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded. Organizations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

Data Security Event Example

Here is a data security event example. It's a raw log, and it is one way to see if someone tried to break into a secure file and hijack the server.

Of course, there are other systems now that are more user-friendly. But security engineers get familiar with some of these codes and can figure out exactly who was trying to log it, was it a secure port or a questionable port that they were trying to use to penetrate our site.

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



```
#separator \x09
#set_separator    ,
#empty_field      (empty)
#unset_field      -
#path conn
#open 2022-06-08-15-40-37
#fields     ts    uid   id.orig_h   id.orig_p   id.resp_h   id.resp_p   proto service     duration    orig_bytes  resp_bytes  conn_state  local_orig  local_resp  missed_bytes      history
#types      time  string      addr  port  addr  port  enum  string      interval    count count string      bool  bool  count string      count count count count set[string]
14.358127   CiCPqPQbqDhXtfaIf 192.168.1.125     56805 8.8.8.8     53    udp   dns   0.001522    34    50    SF    -     -     0     Dd    1     62    1     78    (empty)
14.359952   CHqa74eGSwZhWsyk1 192.168.1.125     53798 8.8.8.8     53    udp   dns   0.001042    34    62    SF    -     -     0     Dd    1     62    1     90    (empty)
10.164709   CB3DU92isM5QSc5bAk      fe80::da58:d7ff:fe00:f72      134   fe80::f802:c758:21ff:4cef     133   icmp  -     7.999306    408   0     OTH   -     -     0     -     3     552   0
11.164172   CRUztF14cX9Wh9HLcd      fe80::da58:d7ff:fe00:f72      547   fe80::f802:c758:21ff:4cef     546   udp   -     47.048446   1787  0     S0    -     -     0     D     15    2507  0
15.183676   CKgCsqJo4pRmGupmR2      fe80::da58:d7ff:fe00:f72      135   fe80::f802:c758:21ff:4cef     136   icmp  -     47.034808   72    72    OTH   -     -     0     -     3     216   3
20.155007   CyBhSK2k7yK399Jpu7      fe80::f802:c758:21ff:4cef     135   fe80::da58:d7ff:fe00:f72      136   icmp  -     0.000217    24    16    OTH   -     -     0     -     1     72    1
200.022409  CgK6rAlDXKKUyTJ92c 192.168.1.125     49159 58.52.155.163     443   tcp   -     2.995839    0     0     S0    -     -     0     S     2     104   0     0     (empty)
199.075968  C45ogL3dlEl3Oez1b fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 60647 fd2d:ab8c:225::1  53    udp   dns   0.000606    34    145   SF    -     -     0     Dd    1     82    1     193   (empt
199.076946  CNblhl3TTXAXYaMeQ3      fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 50731 fd2d:ab8c:225::1  53    udp   dns   0.000421    34    157   SF    -     -     0     Dd    1     82    1     205
199.124542  CnZAZM2T6DwChlTHM7      fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 53115 fd2d:ab8c:225::1  53    udp   dns   0.000479    34    145   SF    -     -     0     Dd    1     82    1     193
199.125382  Cd4Trm4rHzZe3bv30a      fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 50932 fd2d:ab8c:225::1  53    udp   dns   0.000346    34    157   SF    -     -     0     Dd    1     82    1     205
209.016754  CkcbIsCbJq4URGsfb 192.168.1.125     49159 58.52.155.163     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
199.126388  CVLWZw3LFuM8bpX78h       192.168.1.125     49158 78.47.139.102     80    tcp   http  10.033504   89    226   SF    -     -     0     ShADadfF    7     393   6     704   (empty)
236.026271  CMR2Tc1UezE7YeL8Ri       192.168.1.125     49160 58.52.155.163     443   tcp   -     2.993290    0     0     S0    -     -     0     S     2     104   0     0     (empty)
245.018273  CqRJc22IejV5Iksciw8      192.168.1.125     49160 58.52.155.163     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
199.075836  Ccspsa40UwPemoc0ta      fd2d:ab8c:225::1  136   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0     (empt
204.090359  COVbj8FrDHCOIF71g fe80::da58:d7ff:fe00:f72      135   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 136   icmp  -     0.000652    24    24    OTH   -     -     0     -     1     72    1
204.090827  C2qQKfcZekxneDiVe fe80::da58:d7ff:fe00:f72      136   fe80::f802:c758:21ff:4cef     135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0     (empt
209.098337  C8za81M5KZuz1Dk4l       fe80::da58:d7ff:fe00:f72      135   fe80::f802:c758:21ff:4cef     136   icmp  -     0.000151    24    24    OTH   -     -     0     -     1     72    1
272.027526  Cb7cRW3iuTJsgJRIG6      192.168.1.125     49161 58.52.155.163     443   tcp   -     3.004036    0     0     S0    -     -     0     S     2     104   0     0     (empty)
281.030796  C1ruez4AoDpAAcz565      192.168.1.125     49161 58.52.155.163     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
308.029937  C7kVtC2QdPk8VVfxP1      192.168.1.125     49162 217.29.220.255    443   tcp   -     3.003495    0     0     S0    -     -     0     S     2     104   0     0     (empty)
317.032314  C6nxLZ35jtEzDKMbxS      192.168.1.125     49162 217.29.220.255    443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
344.031547  C4pwdoJj5aWFCuh972       192.168.1.125     49163 217.29.220.255    443   tcp   -     3.004024    0     0     S0    -     -     0     S     2     104   0     0     (empty)
353.033918  CkuwG93XKnleAUl6Ld      192.168.1.125     49163 217.29.220.255    443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
380.032729  CV0KFnN05HLCba0fc 192.168.1.125     49164 217.29.220.255    443   tcp   -     2.993985    0     0     S0    -     -     0     S     2     104   0     0     (empty)
389.035689  CFjIT3lpJyP1RtUhnl      192.168.1.125     49164 217.29.220.255    443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
416.035138  CfIKJoiXrlVZDMCZni      192.168.1.125     49165 59.61.184.228     443   tcp   -     2.993480    0     0     S0    -     -     0     S     2     104   0     0     (empty)
425.027235  CSA8SOIAxpbA4Dn99i       192.168.1.125     49165 59.61.184.228     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
308.241674  Cd01HX2Jc557zjG4v9       169.255.60.70     11    192.168.1.125     0     icmp  -     74.982856   260   0     OTH   -     -     0     -     5     400   0     0     (empty)
434.312945  CycJ5l12m1AyNwVu0c       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 53306 fd2d:ab8c:225::1  53    udp   dns   0.000357    34    50    SF    -     -     0     Dd    1     82    1     98
434.313655  CGsCO91eDTDdVjl8ae      fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 52741 fd2d:ab8c:225::1  53    udp   dns   0.000455    34    62    SF    -     -     0     Dd    1     82    1     110
317.232978  CuKf3u4XBkEc9IGVD4       196.192.189.62    11    192.168.1.125     0     icmp  -     71.994160   144   0     OTH   -     -     0     -     3     228   0     0     (empty)
452.036554  ChZepq40hx9P1wueg9      192.168.1.125     49166 59.61.184.228     443   tcp   -     3.003904    0     0     S0    -     -     0     S     2     104   0     0     (empty)
461.039228  Cx6MKS4jdOrSiFfNn1       192.168.1.125     49166 59.61.184.228     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
488.048513  CYuWM03r8xkkANFio5       192.168.1.125     49167 59.61.184.228     443   tcp   -     3.003878    0     0     S0    -     -     0     S     2     104   0     0     (empty)
434.312764  C51o4U1KLgxNlT3sM1       fd2d:ab8c:225::1  136   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0     (empt
439.322472  CyNoXjSrQ3McYnkx2 fe80::da58:d7ff:fe00:f72      135   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 136   icmp  -     0.000443    24    24    OTH   -     -     0     -     1     72    1
439.322828  ChoaY53El6Ebq4oqp4      fe80::da58:d7ff:fe00:f72      136   fe80::f802:c758:21ff:4cef     135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0
497.050968  C8RL2x2zJJ9UNSXDe6       192.168.1.125     49167 59.61.184.228     443   tcp   -     -           -     -     S0    -     -     0     S     1     48    0     0     (empty)
444.330456  CLor8u2w6DkpPDSlW5       fe80::da58:d7ff:fe00:f72      135   fe80::f802:c758:21ff:4cef     136   icmp  -     0.000203    24    24    OTH   -     -     0     -     1     72    1
524.050616  CQFJoC49BNKxhhyhN8       192.168.1.125     49168 190.138.249.45    443   tcp   ssl   3.680688    751   1505  RSTR  -     -     0     ShADadFr    9     1123  8     1837  (empty)
526.292190  CRYUPW1p4kSsXOFfCk       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 50404 fd2d:ab8c:225::1  53    udp   dns   0.000523    48    208   SF    -     -     0     Dd    1     96    1     256
526.293027  CHOi3g19PuXxakJSwb       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 63666 fd2d:ab8c:225::1  53    udp   dns   0.000432    48    232   SF    -     -     0     Dd    1     96    1     280
526.294522  CTY1HVXXASHtwGyte fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 62569 fd2d:ab8c:225::1  53    udp   dns   0.000450    48    208   SF    -     -     0     Dd    1     96    1     256   (empt
526.295317  CtQ5OvYYZfjehactg fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 51572 fd2d:ab8c:225::1  53    udp   dns   0.000451    48    232   SF    -     -     0     Dd    1     96    1     280   (empt
526.292095  C2ZnuR3vqDpo6HUXRj       fd2d:ab8c:225::1  136   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0     (empt
531.306517  CLVYFGObQGYOn1JRj fe80::da58:d7ff:fe00:f72      135   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 136   icmp  -     0.000522    24    24    OTH   -     -     0     -     1     72    1
531.306924  C5mil1S6qeVM66Tjh       fe80::da58:d7ff:fe00:f72      136   fe80::f802:c758:21ff:4cef     135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0
536.314582  CbGn7i2COFvQ3pxDI9       fe80::da58:d7ff:fe00:f72      135   fe80::f802:c758:21ff:4cef     136   icmp  -     0.000203    24    24    OTH   -     -     0     -     1     72    1
544.659019  CgG3mj4MjaEhPqd9z3       192.168.1.125     49171 203.92.62.46      447   tcp   ssl   75.040075   623   547935    SF    -     -     0     ShADadfFr   150   6635  385   563347
618.613893  CZVu1F3VmVVC8pSV47       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 54505 fd2d:ab8c:225::1  53    udp   dns   0.205002    47    111   SF    -     -     0     Dd    1     95    1     159
618.819769  CTVNae4l16SvmYpc63       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 58726 fd2d:ab8c:225::1  53    udp   dns   0.403151    46    119   SF    -     -     0     Dd    1     94    1     167
619.223770  CjLW5E2hWYxm6eeoV fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 55370 fd2d:ab8c:225::1  53    udp   dns   0.206808    53    53    SF    -     -     0     Dd    1     101   1     101   (empt
619.431303  C7ow6uJnfyXFTUUZif       fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 57232 fd2d:ab8c:225::1  53    udp   dns   0.334004    53    121   SF    -     -     0     Dd    1     101   1     169
619.766244  CsN5L7PQDqQPDN8rd fd2d:ab8c:225:0:eced:35cb:1f6c:3a70 50726 fd2d:ab8c:225::1  53    udp   dns   0.376768    51    107   SF    -     -     0     Dd    1     99    1     155   (empt
618.613800  CG647i3Zv8fgwk0xHa       fd2d:ab8c:225::1  136   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0     (empt
542.146084  CK5crC3cumhyL15xe8       192.168.1.125     49170 190.138.249.45    443   tcp   ssl   132.193265  23903 73195 SF    -     -     0     ShADadfFr   62    26391 93    76923 (empty)
623.626645  CAutrjjpHL4PVxGak fe80::da58:d7ff:fe00:f72      135   fd2d:ab8c:225:0:eced:35cb:1f6c:3a78 136   icmp  -     0.000602    24    24    OTH   -     -     0     -     1     72    1
623.627126  CQ0XbJ15vRq9UB26Qg       fe80::da58:d7ff:fe00:f72      136   fe80::f802:c758:21ff:4cef     135   icmp  -     -           -     -     OTH   -     -     0     -     1     72    0     0
526.296102  Ct3yNceMI0Ymi54sc 192.168.1.125     49169 195.113.232.82    80    tcp   http  152.766638  217   51286 RSTO  -     -     0     ShADadR     10    629   38    52818 (empty)
```

Event Logging Best Practices

Different tools are used depending on whether the risk from the attack is from traffic coming into or leaving the infrastructure.

Ingress monitoring:

Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts.

Devices and tools that offer logging and alerting opportunities for ingress monitoring include:

- Firewalls
- Gateways
- Remote Authentication Servers
- IDS/IPS Tools
- SIEM Solutions
- Anti-Malware solutions

Egress monitoring:

Egress monitoring is used to regulate data leaving the organization's IT environment.

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

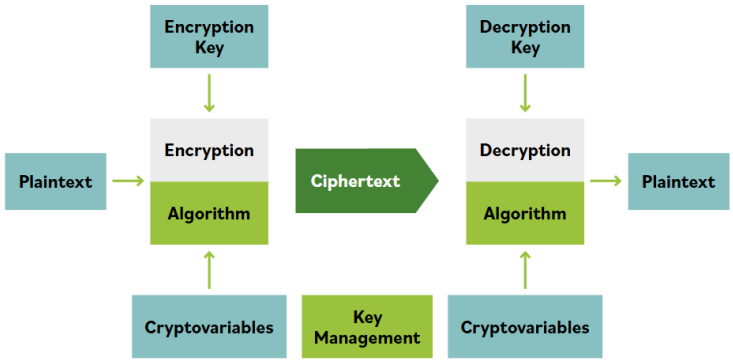
- Email (content and attachments)
- Copy to portable media
- File Transfer Protocol (FTP)
- Posting to web pages/websites
- Applications/application programming interfaces (APIs)

Encryption Overview

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

Confidentiality:
Cryptography provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient. Confidentiality keeps information secret from those who are not authorized to have it

Integrity:
Hash functions and digital signatures can provide integrity services that allow a recipient to verify that a message has not been altered by malice or error. These include simple message integrity controls. Any changes made by the sender or the recipient, either deliberate or accidental, will result in two different results.



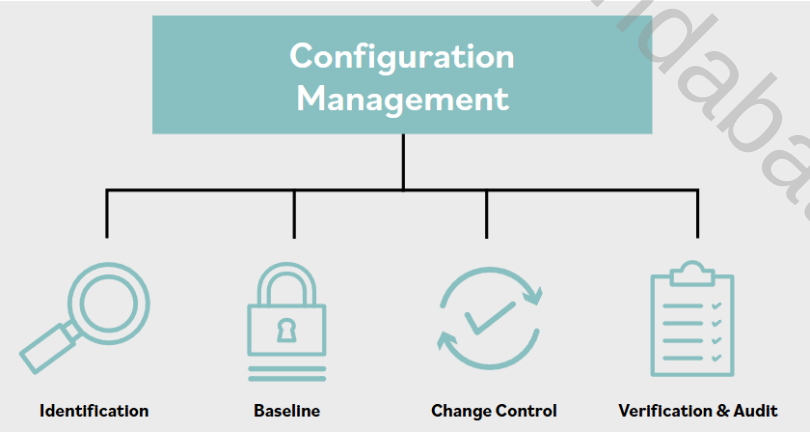
Encryption System
An encryption system is a set of hardware, so ware, algorithms, control parameters, and operational methods that provide a set of encryption services.

Plaintext:
Plaintext is the data or message in its normal, unencrypted form and format. Its meaning or value to an end user (a person or a process) is immediately available for use. Plaintext can be:
● Image, audio, or video files in their raw or compressed forms
● Human-readable text and numeric data, with or without markup language elements for formatting and metadata
● Database files or records and fields within a database
● Anything else that can be represented in digital form for computer processing, transmission, and storage It is important to remember that plaintext can be anything and that much of it is not readable to humans

Configuration Management Overview

Configuration management is a process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated.

It is both a decision-making process and a set of control processes. If we look closer at this definition, the basic configuration management process includes components such as identification, baselines, updates, and patches.



Identification:

Baseline identi□ication of a system and all its components, inter□aces and documentation.

Baselines:

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

Change Control:

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

Verification and Audit:

A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

Inventory

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

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

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

Baseline

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

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

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

Updates

Repairs, maintenance actions and updates are frequently required on almost all levels of systems elements, from the basic infrastructure of the IT architecture on up through operating systems, applications platforms, networks and user interfaces. Such modifications must be acceptance tested to verify that newly installed or repaired functionality works as required.

They must also be regression tested to verify that the modifications did not introduce other erroneous or unexpected behaviors in the system. Ongoing security assessment and evaluation testing evaluates whether the same system that passed acceptance testing is still secure.

Patches

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

There are some issues with the use of patches. Many organizations have been affected by a flawed patch from a reputable vendor that affected system functionality. Therefore, an organization should test the patch before rolling it out across the organization. This is often complicated by the lack of a testing environment that matches the production environment. Few organizations have the budget to maintain a test environment that is an exact copy of production.

There is always a risk that not everything will be tested, and problems may appear in production that were not apparent in the test environment. To the extent possible, patches should be tested to ensure they will work correctly in production.

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

Many vendors offer a patch management solution for their products. These systems often have certain automated processes, or unattended updates, that allow the patching of systems without interaction from the administrator. The risk of using unattended patching should be weighed against the risk of having unpatched systems in the organization’s network. Unattended (or automated) patching might result in unscheduled outages as production systems are taken offline or rebooted as part of the patch process.

Common Security Policies

All policies must support any regulatory and contractual obligations of the organization.

Sometimes it can be challenging to ensure the policy encompasses all requirements while remaining simple enough for users to understand. Here are six common security-related policies that exist in most organizations:

Data Handling Policy:

This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles, or can be made public to anyone outside the organization. In addition, some data has associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations.

For example, classifying credit card data as confidential can help ensure compliance with the PCI DSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard

Password Policy:

Every organization should have a password policy in place that defines expectations of systems and users.

The password policy should describe senior leadership's commitment to ensuring secure access to data, outline any standards that the organization has selected for password formulation, and identify who is designated to enforce and validate the policy.

Acceptable Use Policy (AUP):

The acceptable use policy (AUP) defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action. It should detail the appropriate and approved usage of the organization's assets, including the IT environment, devices and data. Each employee (or anyone having access to the organization's assets) should be required to sign a copy of the AUP, preferably in the presence of another employee of the organization, and both parties should keep a copy of the signed AUP.

Policy aspects commonly included in AUPs:

- Data access
- System access
- Data disclosure
- Passwords
- Data retention

● Internet usage

● Company device usage

Bring Your Own Device (BYOD) Policy:

An organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business use. This is sometimes called bring your own device (BYOD). Another option is to present the teleworker or employee with a list of approved equipment and require the employee to select one of the products on the trusted list.

Letting employees choose the device that is most comfortable for them may be good for employee morale, but it presents additional challenges for the security professional because it means the organization loses some control over standardization and privacy.

If employees are allowed to use their phones and laptops for both personal and business use, this can pose a challenge if, for example, the device has to be examined for a forensic audit. It can be hard to ensure that the device is configured securely and does not have any backdoors or other vulnerabilities that could be used to access organizational data or systems.

All employees must read and agree to adhere to this policy before any access to the systems, network, or data is allowed. If and when the workforce grows, so too will the problems with BYOD. Certainly, the appropriate tools will be necessary to manage the use of and security around BYOD devices. The organization needs to establish clear user expectations and set the appropriate business rules.

Privacy Policy:

Often, personnel have access to personally identifiable information (PII), also referred to as electronic protected health information (ePHI) in the health industry. It is imperative that the organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling that type of information and are made aware of the legal repercussions of improper protection. This type of documentation is similar to the AUP but is specific to privacy-related data.

The organization's privacy policy should stipulate which information is considered PII/ePHI, the appropriate handling procedures and mechanisms used by the organization, how the user is expected to perform in accordance with the stated policy and procedures, any enforcement mechanisms and punitive measures for failure to comply, as well as references to applicable regulations and legislation to which the organization is subject.

This can include national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries such as HIPAA and Gramm–Leach–Bliley Act (GLBA) in the United States; or local laws in which the organization operates.

The organization should also create a public document that explains how private information is used, both internally and externally. For example, it may be required that a medical provider present

patient with a description of how the provider will protect their information, or a reference to where they can find this description, such as the provider's website.

Change Management Policy:

Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management focuses on making the decision to change and results in the approvals to systems support teams, developers, and end users to make the directed alterations.

Throughout the system life cycle, changes made to the system, its individual components, and its operating environment all have the capability to introduce new vulnerabilities and thus undermine the security of the enterprise. Change management requires a process to implement the necessary changes so they do not adversely affect business operations.

Common Security Policies Deeper Dive

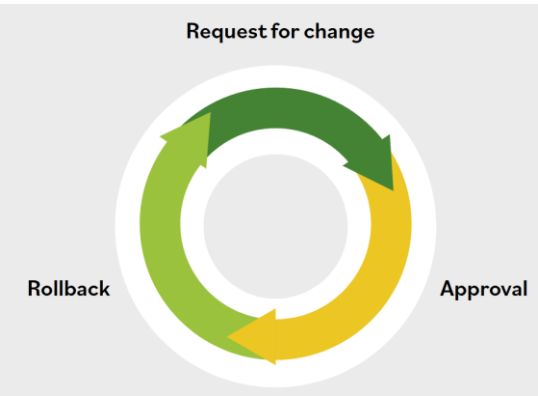
Policies will be set according to the needs of the organization and its vision and mission. Each of these policies should have a penalty or a consequence attached in case of noncompliance.

The first time may be a warning; the next might be a forced leave of absence or suspension without pay, and a critical violation could even result in an employee's termination.

All of this should be outlined clearly during onboarding, particularly for information security personnel. It should be made clear who is responsible for enforcing these policies, and the employee must sign off on them and have documentation saying they have done so. This process could even include a few questions in a survey or quiz to confirm that the employees truly understand the policy. These policies are part of the baseline security posture of any organization.

Any security or data handling procedures should be backed up by the appropriate policies.

Change Management Components



The change management process includes the following components:

Documentation:

All of the major change management practices address a common set of core activities that start with a request for change (RFC) and move through various development and test stages until the change is released to the end users. From first to last, each step is subject to some form of formalized management and decision-making; each step produces accounting or log entries to document its results.

Approval:

These processes typically include: Evaluating the RFCs for completeness, assignment to the proper change authorization process based on risk and organizational practices, stakeholder reviews, resource identification and allocation, appropriate approvals or rejections, and documentation of approval or rejection.

Rollback:

Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: scheduling the change, testing the change, verifying the rollback procedures, implementing the change, evaluating the change for proper and effective operation, and documenting the change in the production environment.

Rollback authority would generally be defined in the rollback plan, which might be immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.

Security Awareness Training

The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out whether there is any carelessness or complacency that may pose a risk to the organization.

Let's start with a clear understanding of the three different types of learning activities that organizations use, whether for information security or for any other purpose:

● Education: The overall goal of education is to help learners improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways.

● Training: Focuses on building proficiency in a specific set of skills or actions, including sharpening the perception and judgment needed to make decisions as to which skill to use, when to use it and how to apply it. Training can focus on low-level skills, an entire task, or complex work□lows consisting of many tasks.

● Awareness: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem, or need.

Notice that none of these have an expressed or implied degree of formality, location, or target audience.

Think of a newly hired senior executive with little or no exposure to the specific compliance needs your organization faces; first, someone has to get their attention and make them aware of the need to understand. The rest can follow.

Security Awareness Training Example

Let's look at an example of security awareness training by using an organization's strategy to improve fire safety in the workplace.

● Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms, and their interactions with electrical power, lighting and ventilation systems.

● Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities.

● Awareness activities would include not only posting the appropriate signage, floor, or doorway markings, but also other indicators to help workers detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

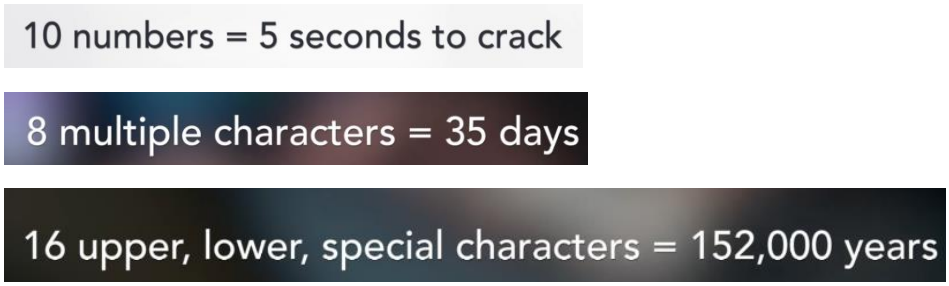
Translating that into an anti-phishing campaign might be done by:

● Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques.

● Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email.

● Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing"), and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking.

Password Advice and Examples



Password Protection

We all use multiple passwords and systems. Many password managers store passwords so that a user does not have to remember all their security codes for multiple systems.

The greatest disadvantage of these solutions is the risk of compromise of the password manager.

These password managers may be protected by a weak password or passphrase chosen by the user and easily compromised. There have been many cases where a person's private data was stored by a cloud provider but easily accessed by unauthorized persons through password compromise.

Organizations should encourage the use of different passwords for different systems and should provide a recommended password management solution for its users.

Examples of poor password protection that should be avoided are:

- Reusing passwords for multiple systems, especially using the same password for business and personal use.
- Writing down passwords and leaving them in unsecured areas.
- Sharing a password with tech support or a co-worker.

Hashing

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

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

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

● Useful: It is easy to compute the hash value for any given message

● Nonreversible: It is computationally infeasible to reverse the hash process or otherwise derive the original plaintext of a message from its hash value, unlike an encryption process, for which there must be a corresponding decryption process.

● Content integrity assurance: It is computationally infeasible to modify a message such that reapplying the hash function will produce the original hash value.

● Unique: It is computationally infeasible to ind two or more di ferent, sensible messages that hash to the same value.

● Deterministic: The same input will always generate the same hash, when using the same hashing algorithm

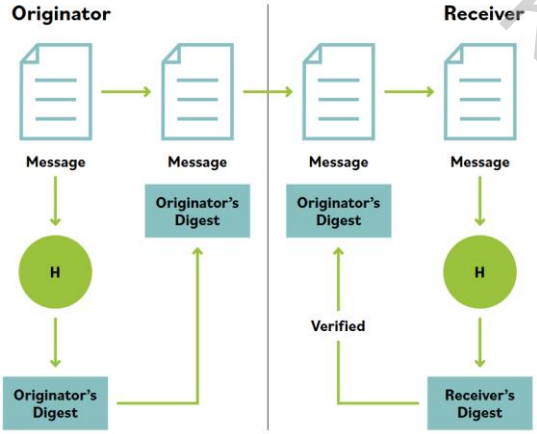
Cryptographic hash functions have many applications in information security, including digital signatures, message authentication codes, and other forms of authentication.

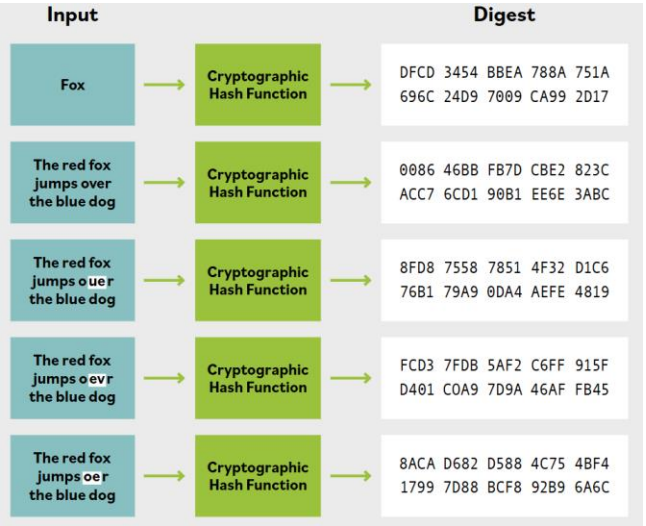
They can also be used for fingerprinting, to pinpoint duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. The operation of a hashing algorithm is demonstrated in the image below.

This is an example of a simple hashing function. The originator wants to send a message to the receiver and ensure that the message is not altered by noise or lost packets as it is transmitted. The originator runs the message through a hashing algorithm that generates a hash, or a digest of the message.

The digest is appended to the message and sent together with the message to the recipient. Once the message is delivered, the receiver will generate their own digest of the received message using the same hashing algorithm. The digest of the received message is compared with the digest sent by the originator. If the digests are the same, the received message is the same as the sent message.

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





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

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

Hashing Deep Dive

Hashing puts data through a hash function or algorithm to create an alphanumeric set of figures, or a digest that means nothing to people who might view it.

No matter how long the input is, the hash digest will be the same number of characters.

Any minor change in the input, a misspelling or an upper-case or lower-case error, will create a completely different hash digest. So you can use the hash digest to confirm that the input exactly matches what is expected or required—for instance, a password.

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

Before we go live with a so□□ware product provided by a third par□y, for instance, we have to make sure no one has changed anything since it was tested by you and the programmer. They will usually send you the digest of their code and you compare that to the original. This is also known as a checksum.

If you see a discrepancy, that means something has changed. Then the security coders will compare the original one and the new one, and sometimes it's very tedious, but they have software that can do it for them. If it's something a little more intricate, they may need to go line by line and find out where the bugs are or if some lines need to be fixed. Often these problems are not intentional; they sneak in when you are making final adjustments to the software.

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

Phishing

The use of phishing attacks to target individuals, entire departments, and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend against.

Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments, and other delivery mechanisms.

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as **whaling attacks.**

Asymmetric Encryption

Asymmetric encryption uses one key to encrypt and a different key to decrypt the input plaintext. This is in stark contrast to symmetric encryption, which uses the same key to encrypt and decrypt.

For most security professionals, the math of asymmetric encryption can be left to the cryptanalysts and cryptographers to know.

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

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

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

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

The problem, however, has been that asymmetric cryptography is extremely slow compared with its symmetric counterpart. Asymmetric cryptography is impractical for everyday use in encrypting large amounts of data or for frequent transactions where speed is required.

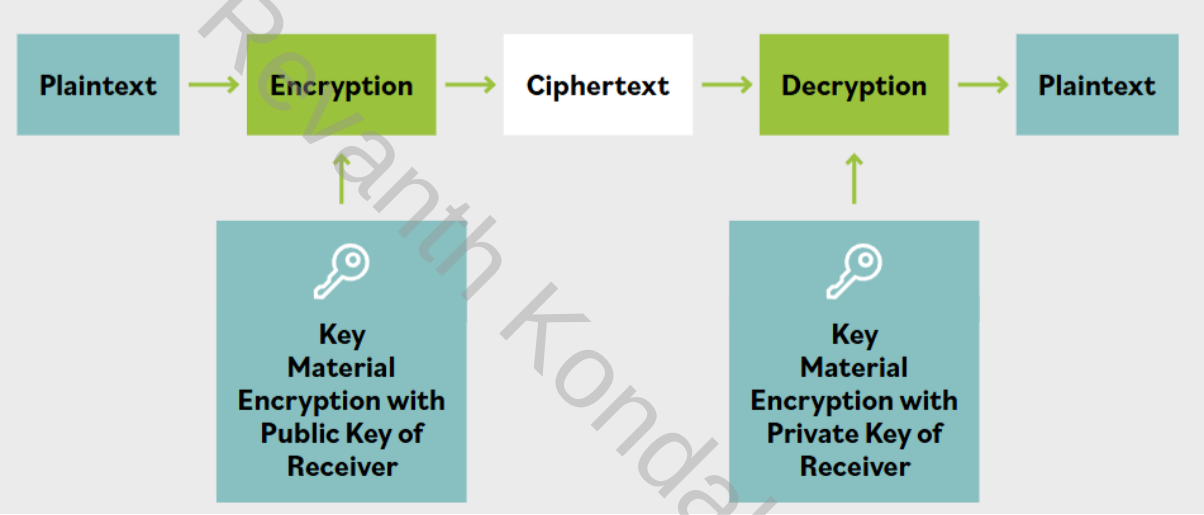
This is because asymmetric key cryptography handles much larger keys and is mathematically intensive, thereby reducing the speed significantly.

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

The two keys (private and public) are a key pair; they must be used together. This means that any message that is encrypted with a public key can only be decrypted with the corresponding other half of the key pair, the private key.

Similarly, signing a message with a sender's private key can only be verified by the recipient decrypting its signature with the sender's public key. Therefore, as long as the key holder keeps the private key secure, there exists a method of transmitting a message confidentially. The sender would encrypt the message with the public key of the receiver. Only the receiver with the private key would be able to open or read the message, providing confidentiality.

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



Symmetric Encryption

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

The same key is used for both the encryption and decryption processes. This means that the two parties communicating need to share knowledge of the same key.

This type of algorithm protects data, as a person who does not have the correct key would not be able to read the encrypted message. Because the key is shared, however, this can lead to several other challenges:

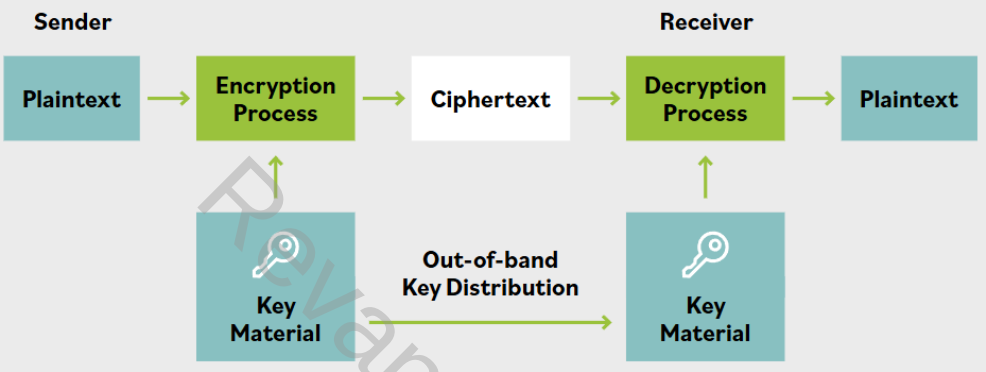
● If two parties suspect a specific communication path between them is compromised, they obviously can't share key material along that path. Someone who has compromised communications between the parties would also intercept the key.

● Distribution of the key is difficult, because the key cannot be sent in the same channel as the encrypted message, or the man- in-the-middle (MITM) would have access to the key. Sending the key through a different channel (band) than the encrypted message is called out-of-band key

distribution. Examples of out-of-band key distribution would include sending the key via courier, fax, or phone.

● Any party with knowledge of the key can access—and therefore change—the message.

● Each individual or group of people wishing to communicate would need to use a different key for each individual or group they want to connect with. This raises the challenge of scalability—the number of keys needed grows quickly as the number of different users or groups increases. Under this type of symmetric arrangement, an organization of 1,000 employees would need to manage 499,500 keys if every employee wanted to communicate confidentially with every other employee.



Primary uses of symmetric algorithms:

● Encrypting bulk data (e.g., backups, hard drives, portable media)

● Encrypting messages traversing communications channels (e.g., IPsec, TLS)

● Streaming large-scale, time-sensitive data (e.g., audio/video materials, gaming)

Other names for symmetric algorithms:

● Same key
● Single key
● Shared key

● Secret key
● Session key

Symmetric Encryption Via Decoding Ring Other names for symmetric algorithms:

An example of symmetric encryption is a substitution cipher, which involves the simple process of substituting letters for other letters, or more appropriately, substituting bits for other bits, based upon a cryptovariable. These ciphers involve replacing each letter of the plaintext with another that may be further down the alphabet. Plaintext Key Material Key Material Plaintext Encryption Process Out-of-band Key Distribution Sender Receiver Ciphertext.

Social Engineering

Social engineering is an important part of any security awareness training program for one simple reason: bad actors know that it works.

For cyber attackers, social engineering is an inexpensive investment with a potentially high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.

One of the most important messages to deliver in a security awareness program is the real and powerful threat of social engineering. Employees must become familiar with types of social engineering so that they can recognize and resist these attacks.

Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives.

A short list of the tactics that we see across cyberspace currently includes:

● **Phone phishing or vishing**: Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution's IVR system. For example, the victim is prompted through a phishing email to call in to a "bank" via a provided phone number to verify information such as account numbers, account access codes, or a PIN and to confirm answers to security questions, contact information, and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.

● **Quid pro quo**: A request for your password or login credentials in exchange for some compensation, such as a "free gift," a monetary payment, or access to an online game or service. If it sounds too good to be true, it probably is.

● **Pretexting**: The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a co-worker, the police, a tax authority, or some other seemingly legitimate person. The goal is to gain access to a computer and information.

● **Tailgating**: The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating occurs when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when they are actually installing malicious software onto your device.

Social engineering works because it plays on human tendencies. Education, training, and awareness work best to counter or defend against social engineering because they underscore that every person in the organization plays a role in information security.