CYBER SECURITY

UNIT-1:-

Cybersecurity Best Practices:

Password reuse continues to be a threat to companies everywhere—a recent report found that 64% of people continue to use passwords that have been exposed in a breach. Poor password hygiene by end-users can open up your organization to security breaches and make your company's sensitive data vulnerable to cyber-attack.

Preventing cybersecurity attacks starts with preparing your frontline of defense: your employees. Cybersecurity awareness training helps them become more aware, alert, and knowledgeable against the latest cyber threat tactics targeting end-users.

While it can be difficult to prevent all users' "bad" behavior, there are several cybersecurity best practices to train and regularly remind your employees of.

Secure End-User Accounts:

Credential-based endpoints are the most vulnerable attack surface in any organization. Securing end-user accounts with these 4 best practices is important to protecting your entire organization from risk.

1. Enforce password policy compliance:

Employees should have no choice but to comply with the password policy rules of your organization. With Specops Password Policy, for instance, organizations can enforce length and complexity requirements to ensure that their password is as strong as possible while blocking over 3 billion known breached passwords.

2. Utilize MFA whenever possible:

To further secure end-user accounts, the implementation of multifactor authentication (MFA) should be mandatory for end-users logging into work

apps, or making a change like resetting their passwords. When it comes to the MFA process, the more ways you can verify your identity when logging in, the harder it is for someone to steal your information.

3. Don't leave information unprotected:

Another best practice pertaining to account information is to encourage employees to lock their screens when they're not around. Leaving screens unlocked increases the risk of someone viewing or accessing sensitive data.

4. Use a password manager:

It's also important for your organization to encourage the use of a password manager, not only for the individual end-user but to utilize shared vault features to prevent insecure password sharing among employees.

Protect Company Equipment:

It's easy, especially in a software-lead organization, to forget the importance of secure hardware. But as the IT pros in manufacturing or healthcare will tell you, it's vital to secure your device infrastructure as well as your network.

When it comes to employees protecting their equipment from cybersecurity threats, there are a few ways internal training and strong policies can help.

5. All hardware should come from IT:

To start, all new purchases should come directly through the IT department. IT is responsible for not only setting up the employee on the company's network, but also for making sure the computer is properly equipped with security and OS or system support. This initial setup helps the IT department remotely maintain your computer to ensure your software is up to date and is set up to auto update.

6. Mobile devices need encryption too:

Phones should have a lock screen and enable message encryption. This policy protects critical texts such as MFA security codes from being visible on a

locked screen. This way, only those who can identify themselves with the correct password can read the messages.

7. Shut down devices properly, and often:

It's common for employees to keep their computers running throughout the work week, but shutting them down is essential for the health—and security—of the equipment. Most software updates require you to restart your computer in order to run successfully, so shutting down equipment is necessary for regular software maintenance.

8. Don't disable built-in protections:

Employees should also be encouraged to keep firewalls enabled. Firewalls are put in place to block certain types of network traffic which keeps your system safe from external threats. Disabling the firewall opens up the organization to malicious attacks which rely on open network ports.

Finally, as an additional layer of protection, employees should always enable antivirus. Antivirus software offers real-time protection by scanning new files and will immediately alert the user if it detects any threats.

Data Privacy and Storage Policies:

Data privacy is another huge piece of the IT security infrastructure. Encouraging these data storage best practices, as well as implementing a zero-trust framework in your organization, can ensure none of your end-users are invertedly putting your data at risk.

9. No personal data storage:

Many companies encourage employees to send everything to the cloud, whether for file sharing or storage. The cloud offers more control over who can access internal information. If this is the policy at your company, then there shouldn't be any company information saved on a user's personal storage.

10. Discourage USBs:

Additionally, make it a point to discourage the use of USB drives. USBs are not only small and easy to lose, but they're usually not encrypted. This means that if a user plugs one into a personal or public computer that isn't secure, and then uses it on work equipment, the USB can then transfer and introduce a virus into your network.

If an end-user needs a USB and there is no other option, make sure it's being purchased and looked over by your IT department

11. Beware of suspicious emails and texts:

Employees should also be encouraged to pay close attention to suspicious-looking emails – and always send them to IT if unsure. The IT department can conduct anti-phishing campaigns to help train employees on security awareness and what to look out for when it comes to suspicious emails.

12. Consider the environment, and your data security:

All employees should also avoid printing anything with company data. Loose papers can end up in the wrong hands once they leave the employee's home or the office.

While printing should be limited, there are cases where you may need to print a document—in which case employees should be encouraged to shred anything they're no longer using.

Handle Software & Licensing Responsibly:

Lastly, end-user education in cybersecurity 101 should include the risks of software on work devices. Organizations should have clear guidelines on how and when end-users can download or license anything that doesn't come standard-issue on their work computers. A few guidelines include:

13. Express IT permission for all new downloads:

New software downloads should be limited, but if users have to download a program, even a web-based application, they should clear it with IT first.

This is especially important if there isn't any web application security already in place.

14. MFA on external software is non-optional:

Additionally, all external software needs MFA for even greater password protection and security.

You'd be shocked to find out how many work-related apps' built-in security measures don't stack up. MFA can help mitigate any 3rd party risk.

Cybersecurity training is a constant practice and a team effort. With regular reminders, training sessions, and support from IT, users can generate more awareness of cybersecurity threats and help protect internal information.

Security Standards:

To make cybersecurity measures explicit, the written norms are required. These norms are known as cybersecurity standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cybersecurity strategy.

1. ISO:

ISO stands for International Organization for Standardization. International Standards make things to work. These standards provide a world-class

specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard is officially established On 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

ISO 27000 Series:

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorized into many types. They are-

ISO 27001- This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

ISO 27000- This standard provides an explanation of terminologies used in ISO 27001.

ISO 27002- This standard provides guidelines for organizational information security standards and information security management practices. It includes the selection, implementation, operating and management of controls taking into consideration the organization's information security risk environment(s).

ISO 27005- This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is capable for all kind of organizations such as non-government organization, government agencies, and commercial enterprises.

ISO 27032- It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

2. IT Act:

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of United Nations. This act is also used to check misuse of cyber network and computer in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitate electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act

3. Copyright Act:

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not covers the following-

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic ornamentation, lettering, or coloring

4.Patent Law:

Patent law is a law that deals with new inventions. Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

- Not a natural object or process
- New
- Useful
- Not obvious.

5. IPR:

Intellectual property rights is a right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

What is a Cybersecurity Plan:

Small businesses are the favorite target of cyber-criminals. As a matter of fact, ransomware attacks in 2017 caused nearly a quarter of small and medium-sized businesses to completely halt operations. Recent statistics also show that around 60 percent of small and medium businesses forced to suspend operations after a cyber-attack never reopen for business.
According to Cyrus Walker, Managing Principal at Data Defenders, there are two key mistakes small companies make that leave them vulnerable to cyber-attacks. The first key mistake is that small businesses assume they won't be targeted. The second key mistake, which is as a result of the first, is that they don't provide any cybersecurity training for their employees. These two mistakes eventually result in serious cybersecurity threats to small businesses. Employees sometimes give cyber-criminals access into the defense networks of businesses due to ignorance on how to handle activities in accordance with cybersecurity best practices. This is why a cybersecurity plan is very important.
A cybersecurity plan is a written document containing information about an organization's security policies, procedures, and countermeasures. The objective of this plan is to ensure the integrity of operations and security of your company's assets.

Developing Your Cybersecurity Plan:

Once you've understood best practices in cybersecurity and have assessed your organization's cybersecurity structure, you're ready to start building your cybersecurity roadmap. How do you develop a cybersecurity plan

1. Identify Key Assets And Threats:

The first step in developing a cybersecurity plan is to identify the assets you're protecting. This step involves active consideration of your business' context, as well as asset/risk assessment and threat management processes.

2. Prioritize Assets, Risks, and Threats:

After assessing your assets, threats and risks, the next step is to prioritise them with the right approach depending on the context of your organisation. Here are three questions you need to answer to help you identify top risks:

- What are the risks or threats in your organization?
- What are the main concerns of your organization regarding cybersecurity
- Which risks and threats would harm your organization more?

You can then go on to determine countermeasures and treatments for each risk or threat identified. Classify them from the easy wins to the hardest to achieve.

3. Set Achievable Goals:

It's cool to aim high on your goals, but achievable goals are more important to your company than a long list of policies and procedures that don't help. While a cybersecurity plan should identify all activities that you'd like to undertake, you need to identify those goals that will be truly achievable. Some companies at the beginning of the year set goals of completing a task in 6 months but they never complete it in over a year.

Start with the basics; the goals that are easily achievable. Remember, cybersecurity policies are a strong foundation that will drive the rest of your cybersecurity efforts. Focus on the most important and high-risk areas first and get them out of the way as they are a matter of priority.

4. Document Your Cybersecurity Policies:

It's a known fact that small businesses often operate more by word of mouth and intuitional knowledge rather than operating out of the books. Cybersecurity is one area where it's essential to document your protocols, processes, policies, and every procedure. Having a cybersecurity plan avails you the opportunity to have a detailed toolkit that is in line with cybersecurity best practices and policies.
Writing these policies may be a herculean task, however, some organisations are best known for their expertise in technical and business writing. You can hire the services of any of these organizations.

5. Link Goals To Business Objectives:

Identify the business reason for each goal earlier highlighted. For example, it's better to indicate that a firewall is needed, not just for the sakes of it, but so staff can easily access the data they need to do their jobs. Don't ignore the business side of your cybersecurity plan because every of your plans will have an impact on your organization.

6. Test For Vulnerabilities:

Having done all, don't forget to have a test run. You need to find out if your cybersecurity plan works or not. Waiting to find out when a cybercrime occurs will be too late and too risky. Therefore, test your plan.
How do you do this? At least once in a year, hire a cybersecurity expert to perform a full assessment on your security to make sure that your plan is still relevant, up to date, and effective. Some organizations even hire ethical

hackers to attempt to breach their system. Cyber-threats are always evolving, so your computer security plan should evolve also.

The Cyber Security Governance Principles:

1. Set clear roles and responsibilities:

An essential component of setting up cyber security protocols is establishing a cybersecurity team within your organisation – with each member having a clearly defined role and responsibility.

The cybersecurity team will be responsible for engaging with management and keeping the board informed on cybersecurity measures and trends. Within that team, there should be a clear line of management responsibility for cyber security.

It's also vital that board members regularly include cyber risk and strategy in their agendas. Boards should also review their skills annually to ensure that directors have a minimum understanding of cyber security risk.

External experts also play critical roles in maximising the cybersecurity team's capabilities. External experts can provide advice and assurance to boards and identify areas for improvement. They can also help establish policies that will assist with implementing a cyber security framework. An external review and validation of an organisation's cyber risk controls and strategy are essential to a robust cyber security policy.

When reporting to the board on cyber risks, ensure your reporting is easy to digest – free of excessive jargon and technical terms.

2. Develop, implement and evolve a comprehensive cyber strategy:

A cyber strategy, overseen by the board of directors and implemented by management, can identify opportunities for an organisation to build cyber resilience — thus proactively addressing threats.

A cyber strategy should exist in the form of a formal document. A robust cyber strategy includes the following:

- Identifying the key digital assets and data of an organisation—and who has access to them;
- Considering the impact of third-party suppliers: Both in terms of their importance and their potential risks;
- A data governance framework that outlines how your organisation collects holds, protects, and ultimately destroys data; and
- A process for assessing and ensuring the cyber security controls of suppliers, vendors, and other relevant stakeholders.

Finally, your organisation's cyber strategy and risk controls must be subject to internal and external evaluation. As cyber security threats constantly evolve, your plan to mitigate the risk of a security breach should also evolve.

3. Embed cyber security in existing risk management practices:

While cyber security is a hot-button issue for organisations, it is important to remember that cyber risk is yet another risk (albeit a significant one) that should fall under your organisation's existing risk management plan.

And as with other risks, the board should regularly assess the effectiveness of their cyber controls to ensure they match the ever-evolving nature of cyber threats.

And even though you cannot reduce your cyber risk to zero, there are several accessible and low-cost ways that all organisations can protect themselves.

Cyber security should be in the fabric of your organisation. Organisations often make the mistake of relying on the cybersecurity controls of their service providers. Over-reliance on external experts means you are underprepared internally if something were to go wrong.

4. Promote a Culture of "cyber resilience":

Creating a culture of cyber resilience involves regular, relevant training of key staff in your organisation – including specific training for directors.

Cyber security training should involve simulated cyber-attack exercises that ensure that your team has the playbook and "match-fitness" to respond to a breach.

Furthermore, your organisation's leaders should reinforce the importance of cybersecurity and "cyber resilience" to all staff. Without reinforcement from leadership, many staff see cyber security as an issue for frontline staff to manage and, therefore, not their problem.

To that end, it is vital your organisation's leaders "walk the walk" by actively engaging with all aspects of your organisation's cyber security processes and procedures.

As staff buy-in to cyber resilience is a top-down exercise, your organisation must include cyber security considerations in key leaders' job descriptions and KPIs

5. Prepare for a cyber attack:

Underpinning your organisation's cyber security measures should be the adage: "Prepare for the worst, expect the best".

And in preparing for the worst, your organisation must prepare for a significant cyber attack.

As mentioned above, your leadership team must fully prepare your staff for the possibility of a cyber-attack by conducting a range of simulation exercises. These training drills will ensure all staff are fully aware of their roles and responsibilities during a breach.

It is imperative to document processes and lessons from these simulation exercises. Documentation ensures your organisation systemises effective responses – and the resulting blueprints will help to alleviate the additional pressure of a real-life attack.

Furthermore, your organisation needs a pre-determined crisis communications strategy so that you are in a position to deliver timely, relevant communication to stakeholders in the event of a breach. Clear, transparent communications with all key stakeholders can help mitigate the reputational damage of a significant cyber-attack – boosting your prospects of a speedy recovery.

Components of cyber security:

1. Application security:

Application security represents a core component of cyber security. The purpose of application security is to guard against security vulnerabilities that could permit system access and modification. Types of application security features include authentication, authorization, encryption, logging and application security testing.

Organizations may wish to automate application security and API protection with tools powered by contextual AI. This can reduce the need to manually fine-tune rules. With modern security solutions, it's possible to engage in precision threat-prevention without any human intervention. Other network-level application security tools include firewalls, antivirus, encryption techniques, and web application firewalls.

Because mobile devices also rely on applications, enterprises may also wish to add a layer of mobile application security. For example, IT admins can provide employees with mobile device VPN options.

2. Information security:

Information security functions as a means of preventing and defending against unapproved access, use, interruption, modification or deletion of information. A core concept in information security includes the CIA triad – Confidentiality, Integrity and Availability. Learn more about this component of cyber security here:

Confidentiality:

This refers to the guarding of proprietary business and client information. In accomplishing this, organizations commonly implement zero trust and other access safeguards. Confidentiality means that unauthorized persons cannot access important business data. It also means that users who do need to access sensitive information can do so as needed.

Protecting corporate proprietary information exfiltration from competitors or nation-states must be a high priority for small businesses and, in the case of US government subcontractors, security compliance requirements are detailed and specified in CMMC and NIST 800-171. In combating confidentiality breaches and moving beyond zero trust, organizations may wish to encrypt data, use multi-factor authentication and educate users around data access policies.

Integrity:

In cyber security, the concept of integrity refers to maintaining consistency, accuracy and completeness of information. Information owners cannot move or alter information in ways that the parent organization has not approved. In addition, data integrity means continually ensuring that external parties have not disturbed data in any way. For example, if a given organization presents information about executives on its website, the information must meet certain unspoken integrity standards. IT administrators need to ensure that this information is not tampered with by persons of nefarious intent. Cyber criminals could potentially hack an organization's website and manipulate the descriptions under executives' profile photos or the photos themselves.

Availability:

Data is largely dead weight unless it is available to employees within an organization, approved third-parties and relevant customers. In the CIA triad, availability refers to the notion that applications, systems, and networks must function effectively at all times. Users should be able to obtain necessary information without interference and with efficiency. In ensuring the availability of data, organizations commonly build redundancies into networks. Organizations also enhance availability by staying up-to-date in relation to software updates and security system updates.

3. Network security:

Network security is designed to protect a network and data from breaches, intrusions and other threats. Network security functions as a vast and overarching system that protects configurations, accessibility and more. It generally involves access control, virus and antivirus software, network analytics, endpoint security, firewalls, encryption and more.

Network security is critical when it comes to protecting information. In other words, it keeps data secure, protects from viruses, and assists with network performance by reducing overhead expenses. It can also limit losses from data breaches. In the long run, network security plays a role in saving enterprises both time and financial resources.

4. Disaster recovery and business continuity planning:

In thinking about disaster recovery, images of generators, life jackets and space blankets likely come to mind. In cyber security, disaster recovery refers to tools and procedures used to recover from disruptions to information technology systems.

A "disaster" consists of any event that interrupts data access, apps, networks or data availability. This can range from a power outage to a DDoS or ransomware attack. Disaster recovery and business continuity plans are designed to assist organizations in overcoming these unexpected challenges.

Within disaster recovery plans, organizations commonly include recovery point objectives, recovery time objectives, remote data backup information, and accountability charts.

Disaster recovery plans are not the same as business continuity plans. The former help organizations recover *from* a disaster. The latter assist organizations in maintaining operations *despite* a disaster. For organizations with the capacity to create them, disaster recovery and business continuity plans easily justify the cost.

5. Operational security:

Operational security encourages security professionals to adopt the mindset of a cyber adversary. This component of security prevents sensitive information from actually reaching attackers. It also helps organizations highlight weak points that could accidentally open the doors to persons with nefarious intent.

The idea of operational security (OpSec) was first introduced by the military. Since then, OpSec has become popular throughout the private sector. The process involved in operational security can be described in five distinctive steps:

- **Identification of data:** This involves determining what data a given organization needs to protect. For example, organizations may need to

protect intellectual property, financial statements, customer information and employee information.

- **Identification of possible threats:** For every type of data, organizations need to determine what types of threats remain likely. Are third-party threats a concern? Intellectual property theft?…etc.

- **Security weakness analysis:** In this step, organizations must assess current safeguards and determine which weaknesses could see exploit for the purpose of gaining access to sensitive data.

- **Appraisal of risk associated with vulnerabilities:** At this stage in the game, cyber security professionals need to rank vulnerabilities, determine damage potential and calculate recovery times, if breached. The greater the likelihood of an attack and the higher the level of damage, the more important it is for organizations to prioritize mitigation of associated risk.

- **Implementing prevention and defense:**The final step involved in operational security consists of implementing security technologies and best practices. For some organizations, mitigation and defense measures must meet industry compliance standards. This represents a key factor in determining what type or types of security a given organization needs to implement.

6. Testing and tabletop exercises:

Cyber security testing and tabletop exercises are core elements in demonstrating cyber security maturity. Many types of testing and exercises exist. All offer opportunities to prove effective cyber security risk management and to fine-tune components of cyber security. Testing and exercises may show gaps, weaknesses, or cyber security challenges in other regards.

Testing and tabletop exercises also enable cyber security professionals to strengthen working relationships with peers. And, they can improve organizational and individual outlooks and attitudes around cyber security preparedness.

7. Quarterly risk discussions and planning:

Regular risk discussions and planning represent core components of cyber security programs. In these discussion and planning meetings, experts recommend discussing immediate and long-term cyber security needs, a layered approach to cyber security, and the incident response playbook.

8. Optimization and continual improvement:

The final component of the cyber security lifecycle consists of determining whether or not there are any areas that can be improved upon. Organizations need to both continually add value to the business and also continually add value for customers. The continual service improvement (CSI) stage can be broken down into a multi-step process, making CSI possibilities clearer and easier to manage.

Approaches:

A security model is a computer model which can be used to analyze and enforce security policies. It does not require some previous formation and it can be organized on the access right model or inspecting computing model or computation model.

A security model is a mechanism in which a security policy is produced. The development of this security policy is regulate to a definite setting or example of a policy.

A security policy depends upon authentication, but construct within the confines of a security model. For instance, it is designing a security model depends upon authentication and authorization. It can consider the 4-factor model of security, including authentication, authorization, availability, and reliability.

A security model makes the external component for the inspection of security issues

in general, and provides the context for database application, including implementation and application.

Information security models bridge the gap among security policy declarations and it can represent which customer should have access to information. The operating system implementation which enables an administration to organize access control.

The models supports map analytical goals onto numerical relations that strengthen whichever implementation is definitely preferred. There are several approaches of information security models which are as follows −

No Security − In this fundamental method, the approach can be a decision to perform no security at all.

Security through obscurity − In this structure, a system is protected simply because nobody understand about its continuation and elements. This approach cannot operate for too long, as there are some methods an attacker can come to understand about it.

Hot Security − In this model, the security for every host is required separately. This is a secure approach, but the difficulty is that it cannot scale well. The difficulty and diversification of current sites/organizations creates the service even harder.

Network Security − Host security is complex to obtain as organizations become larger and develop into more diverse. In this approach, the target is to control network approach to multiple hosts and their services, instead of individual host security. This is a very effective and extensible model.

Information Systems Security (INFOSEC) − Security of information systems next to unauthorized access to or modification of data, whether in storage, processing, or transit, and against the denial of service to authorized users, addition those measures important to recognize, documents, and explanation such threats.

Technical Reference Model (TRM) − An element-driven, high-tech framework that represent the standards and technologies to provide and enable the delivery of service elements and capabilities. The important security framework that lies away from a business represented border, but provide its IA and IA-authorized products, its security position and its risk management plan.

Information Risk Management:

Information risk management is crucial to effective cybersecurity. While information security and risk management relate, the two have subtle, critical differences. Information security deals with technology, whereas information risk management comprises accounting for all of the policies, procedures, guidelines, and human behaviors that constitute the risk environment around data.

There are three primary components to understanding information risk management:

- The overall purpose of information risk management in cybersecurity
- The benefits of a custom-tailored information risk management framework
- The general process of information risk management in cybersecurity

We'll touch on all of these below, along with ways in which a quality managed security service provider (MSSP) can optimize your implementation of an information risk management program.

The Process of Information Risk Management in Cybersecurity:

There are various approaches to information risk management. No single information risk management framework will work perfectly for all organizations; however, similar routine activities can be identified within all effective IRM frameworks.
One approach particularly effective for baseline IRM strategizing is managed detection and response (MDR), which comprises four major components that form a simple, cyclical, stepwise process for IRM:

1. Detection and identification
2. Comprehensive response
3. Root cause analysis (RCA)
4. Compliance and continuity

1: Detection and Identification:

Vulnerabilities and threats need to be identified before they can be mitigated or otherwise managed. Therefore, the first and most essential process is ongoing scanning across all system components for any known vulnerabilities, threats, or indications thereof.
Public threat intelligence, such as the common vulnerabilities and exposures (CVE) list, should be cross-referenced with more specific data from your organization and other, comparable entities.
For example, and returning to the healthcare examples above, covered entities and business associates should optimize their internal threat intelligence to threats specific to PHI.

2: Comprehensive Response

When a threat is identified, the catalog of threat intelligence enables instant identification and inventory logging. Ideally, these should be followed by automated response protocols, a thorough process of manual assignment, and escalation to eradicate the threat.
Identified threats and vulnerabilities should be responded to before developing into a full-on attack, leak, or another cybersecurity incident. To reduce the strain of incident response, threats and vulnerabilities should be accounted for as incidents and managed accordingly. One way this relates to the HIPAA examples above is that, strictly speaking, even a minor breach of the Privacy Rule could be interpreted as a data breach—all threats need to be taken seriously.

3: Root Cause Analysis (RCA)

One crucial difference between responding to an incident and responding to a risk is that the former involves a recovery process, whereas the latter typically does not. In its place, however, organizations should conduct deep-dive analyses into the root causes that led to the vulnerability or threat manifesting. These may include:

- Faulty security architecture planning or implementation
- Missing or incomplete patches to software or hardware
- Inappropriate user behavior due to ignorance or malice

Whatever a threat's source or extent of materialization, its mitigation is incomplete if root causes are unknown.

4: Compliance and Continuity

Vulnerabilities, threats, and risks cause volatility in both the short and long term with respect to an organization's ability to maintain service and good delivery. This is why the final consideration in MDR is both making sure that end-user-facing functions remain as *available* as possible—despite threats—and that systems are prepared for the long-term work of reporting and maintaining compliance.

Without thorough, *proactive* information risk management, any individual threat can do irreversible harm.

Advantages of Risk Management:

1. It encourages the firm to think about its threats. In particular, risk management encourages it to analyze risks that might otherwise be overlooked.

2. In clarifying the risks, it encourages the firm to be better prepared. In other words, it helps the firm to manage itself better.

3. It lets the organization prioritize its investment and reduces internal disputes about how money should be spent.

4. It reduces duplication of systems. Integration of environmental and health and safety systems are one instance.

Disadvantages of Risk Management:

1. Qualitative risk assessment is subjective and lacks consistency.

2. Unlikely events do occur but if the risk is unlikely enough to occur is maybe better to simply retain the risk and deal with the result if the loss does in fact occur.

3. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably.

Asset Identification:

Asset identification is a critical process for any business because knowing which equipment you have is essential to being able to track it. If your assets are labeled incorrectly, or if you have duplicate labels, you risk facing compliance issues, falling behind with preventive maintenance, and putting your assets at risk of being stolen or lost. Utilizing asset identification best practices with fixed and movable physical assets is the foundation of efficient asset tracking for your business.

Methods of Asset Identification:

The most common method of asset identification is asset tags. Also known as asset labels, asset tags can be used to identify a range of physical assets, including equipment, tools, racks, and machines. These asset tags include serial numbers that serve as unique identification numbers. Asset tags may be made of foil, aluminum, premium polyester, or vinyl.
You can use barcode label asset tags to identify your assets. Barcodes also are assigned a unique identification number, which can be scanned into an asset tracking software solution with handheld scanners or mobile devices. All of the asset data is contained within the program, empowering users to locate a specific asset quickly and easily. Some programs also include maintenance schedules, warranty information, and maintenance history for assets.
Radio Frequency Identification (RFID) asset tags also are an option for asset identification. Unlike barcode tags, RFID tags do not have to be directly in the line of sight of scanners to be detected because RFID readers send out radio waves detected by the antenna within the tag. One disadvantage of RFID asset tags is their cost. Not only do RFID labels cost more than barcode labels, but RFID readers are more expensive than barcode scanners.

Asset Identification Best Practices:

To maximize your fixed asset identification efforts, implement best practices across your organization. To be cost-effective, prioritize identifying high-value assets including those that depreciate. You also should identify moveable assets and those requiring regular maintenance, repairs, or replacement parts

like equipment and machinery. Thus, you should label IT hardware like computers and servers, audio-visual equipment like projectors, fixed assets, critical equipment like machines and tools, and furniture like desks and filing cabinets.
Another asset identification best practice is implementing an asset tracking solution. No matter which type of asset identification your company chooses to use, you will benefit from eliminating manual data entry that can be rife with error. Scanning automates processes and makes asset identification and tracking much more reliable and efficient.

Success factor asset identification:

The main goal of cybersecurity is to protect the mission-critical assets that keep the business running and growing. However, you need to know what you need to protect. Here are some actionable approaches to identifying assets and avoiding a corporate heart attack.

«Assets» include anything that is relevant to a specific business purpose in a particular context and therefore essential for survival. Therefore, it is key to protect the assets to ensure their confidentiality, integrity and availability.What is considered an «asset», however, is a question of perspective: For a company manager, an asset is, for example, established customer trust, for the cybersecurity specialist it is the IT systems, for the information security officer it is information of all kinds, and for the data privacy officer it is personal data.

Knowing one's assets – why is it so important?

Only if you know and understand the assets you want to protect, you will be able to assess and manage your risks. Unfortunately, there is little practical guidance on how to collect assets so that they are fully mapped and changes can be quickly identified.

Identifying assets in everyday life:

Usually, assets are collected in close and regular collaboration with those responsible for applications and specialist areas in the company.

Many information security managers are unhappy with this, as they believe they cannot rely on the completeness and timeliness of the assets documented in this way. In fact, most companies do not know in detail which systems, information and data they have where and in which processes which data is used.

Even inventory solutions often only serve to provide transparency per se, are based on a very limited understanding of «assets» or are unsuitable for putting assets into a corporate risk context and deriving protective measures.

Principles and challenges:

For assets to be useful as a basis for risk analysis, it is crucial to determine them systematically and to observe the following principles:

1. Capture assets in a granular and detailed way so as not to miss valuable components
2. Describe assets as what needs to be protected rather than reducing them to their attack surface
3. Include assets that cannot be derived from process descriptions
4. Try to detect changes in the asset and system landscape at an early stage

Identify assets in a targeted manner for a solid cybersecurity foundation:

For the most complete and up-to-date determination of assets, a combination of different approaches is recommended:

1. Start from the IAM solutions and derive what the people or devices managed in them can access
2. Start from all inventories and merge this information about assets
3. Start from existing documentation of the system landscape, network structure, IT architectures and processes
4. Start from the knowledge of the process and application managers
5. Start from the real data traffic to understand which systems and assets are accessed

Clearly, identifying assets requires a wide range of expertise, experience and resources – which is often lacking within the company. However, the money would be well invested here, as cybersecurity has moved from being a pure IT issue to an urgent business issue.

Thread Identification:

The threat identification process examines IT vulnerabilities and determines their capacity to compromise your system. It's a key element of your organization's risk management program. Identifying threats allows your organization to take preemptive actions. You receive the information you need to obstruct unauthorized users and prevent system breaches. At Ward IT

Security Consulting Group, we provide the specialized knowledge and the experience necessary for effective threat identification.

We understand your organization's risk profile:

Each IT system environment is unique. Some threats will in some ways be a part of a common set of threats to all organizations with public-facing web portals. Other vulnerabilities may be specific only to your organization. That's why we work collaboratively with your staff and begin our evaluation with an in-depth understanding of your organization and operations.

- Analyzing and understanding the particular threat portfolio specific to your organization and its operation.
- Effectively prioritizing the evaluation of your system vulnerabilities.
- Determining how those vulnerabilities may be exploited by a specific threat actor or actions.
- Providing a report of findings with detailed information that allows your organization to implement preemptive risk management actions.

Assurance of the threat identification

Assurance evidence for threat identification is derived primarily from the use of relevant checklists and from traceability links between the elements of the integrated system model. Individual threat identification strategies (injury argument, entry point argument, threat argument, and vulnerability argument) all provide unique perspectives on threat. Assurance of threat identification is done by cross-correlating the results of these approaches. In addition, the identified components of threats are linked to the system elements, which allows for additional cross-correlation. (If a certain system element is associated with one of the threat components, are all similar elements also associated with threat components?) An additional backing argument is based on using qualified and experienced personnel to perform threat identification. The threat identification activity involves verification and validation tasks, as well as the assurance task.

How Do You Identify Cyber Security Threats

These assessments are used to identify vulnerabilities, estimate cyber security threats, and prioritize operations based on risk levels. To do this, they look at

the way the business operates, the systems it uses, and the information it stores.

This process will normally start with a number of basic goals:

- Identify the organization's most important information technology assets
- Decide what data breach would have the greatest impact on the business
- Identify cyber security threats
- Evaluate the potential impact of each threat
- Highlight internal and external vulnerabilities
- Evaluate the likelihood each threat will be exploited
- Identify types of attacks that are likely to affect the business's ability to function
- Decide what level of risk the organization is comfortable taking

Advantages of threads:

1. We can execute multiple tasks of an application at a time
2. Reduces the complexity of a big applications
3. Helps to improve the performance of an application drastically
4. Utilizes the max resources of multiprocessor systems
5. Better user interface in case of GUI based applications
6. Reduces the development time of an application
7. All the threads are independent , any unexpected exception happens in any of the thread will not lead to an application exit.

Disadvantages of threads

1. Thread synchronization is an extra over head to the developers
2. Shares the common data across the threads might cause the data inconsistency or thread sync issues
3. Threads blocking for resources is more common problem
4. Difficult in managing the code in terms of debugging or writing the code

Vulnerability Identification:

Vulnerability Identification is vital to proactively protect your IT system rather than reactively cleaning up after an attack. The vulnerability identification process enables you to identify and understand weaknesses in your system, underlying infrastructure, support systems, and major applications. It allows you to analyze the potential exposures generated by your supply chain and your business partners.

When vulnerabilities remain unidentified, attackers can use them to damage your applications, produce a deniable service, or create the circumstances for a breach. Attackers manipulate vulnerabilities to exfiltrate confidential and proprietary data that are vital to your business operations and to your professional reputation.
At Ward IT Security Group, we approach vulnerability identification from the analytical perspective of a potential attacker. Our team has the expertise to evaluate mission-critical applications hosted by our clients. We implement proactive protections by identifying weaknesses and opportunities before an attacker has an opportunity to exploit them.

IT Applications:

Public-facing web applications are one of the primary threat factors by which attackers can infiltrate your organization's IT system. The Ward Group has extensive experience in evaluating, assessing, and providing remediation recommendations for the spectrum of web applications. We have provided critical security assessments for applications hosting or providing portals for such highly attractive targets as health insurance exchanges, business and personal tax information, and primary eligibility management portals for state governments.
Our IT experts are meticulous when evaluating your organization's applications. We bring to each security task a thorough understanding of applications, how they are attached and constructed, and how platforms are configured. We recognize that the inherent weaknesses built into many deployed applications are due to the development process and the tools used to produce them.

Cloud Systems:

When your organization operates applications and stores data in a cloud system, your security concerns are similar to traditional IT systems only more complex. You retain accountability for system operations, data privacy, regulatory compliance, user authentication, access, and authority, yet these and other aspects of system security are often out of your direct control. Evaluating and assessing vulnerabilities can present procedural and technical difficulties.
At Ward Group, we understand the inherent challenges of cloud computing security. We analyze your exposures by assessing both the client side and the cloud side for compliance with required guidelines and standards. Our team reviews legal and regulatory issues and determines the extent of existing and missing safeguards. We evaluate your ability to access information related to privacy enforcement, data protection, security incidents, and other cloud environment factors that may be of your control.

Network Security:

Unexposed vulnerabilities in your network provide attackers with easy access to your IT system. Ward Group works proactively to reveal existing network vulnerabilities before they become a problem. We dissect network traffic flows, analyze network device configuration, and evaluate the design and allocation of address space within the access controls to critical network subnets. Our team complies with standards and guidelines for public cloud computing as outlined in NIST Special Publication 800-144.

Physical Security:

Ward has performed comprehensive independent physical and environmental assessments of some of the most critical data center sites in the Northeast. Our evaluation methodology is modular and ensures compliance with multiple regulatory environments and physical site variations. In evaluating your data center's physical security risks, we provide you with the assurance that all control capabilities impacting compliance will be thoroughly investigated, evaluated, and documented.
Our experts work directly on-site with your organization management, IT team, and support staff. We use a collaborative methodology which guarantees a transparent end effective knowledge transfer process to your staff.

Supply Chain Security:

Sources of supply chain risk can vary from third-party vendors, compromised software or hardware, embedded malware, or a wide variety of other origins. IT security best practices recognize that any systems evaluation should be based on breach inevitability, considering not if your system will be breached but when.
When the Ward Group evaluates and assesses your supply chain risk, we address aspects of data breach mitigation as well as prevention. Our team considers all potential sources of supply chain risk. We then work with your organization to establish security controls, identify vulnerabilities and security issues, and address vendor access concerns.

Policy and Procedures:

Policies and procedures are an important element of the vulnerability identification process. Once security issues have been detected and remediated, it's imperative to establish a written plan to manage the risk, prevent future problems, and monitor for ongoing compliance.

The Ward Group has the experience and integrity to review and upgrade your existing IT security policies and procedures. We can identify and assess policy weaknesses which may have allowed vulnerabilities to exist unabated. Our team works collaboratively with your staff to implement policies and procedures that address your vulnerabilities and system security requirements. We review your physical security, IT policies, and procedures. When we discover system vulnerabilities we verify them with evidence and artifacts. We report vulnerabilities with assigned threat levels that allow you to prioritize remediation solutions based on risk.

Common types of cybersecurity vulnerabilities:

When building a vulnerability management program, there are several key cybersecurity vulnerabilities that you must be aware of. Below are six of the most common types of cybersecurity vulnerabilities:

1. System misconfigurations:

System misconfigurations occur as a result of network assets having vulnerable settings or disparate security controls. A common tactic cybercriminals use is to probe networks for system misconfigurations and gaps that can be exploited. As more organizations adopt digital solutions, the likelihood of network misconfigurations grows, so it is important to work with experienced security professionals when implementing new technologies.

2. Out of date or unpatched software:

Unpatched vulnerabilities can be exploited by cybercriminals to carry out attacks and steal valuable data. Similar to system misconfigurations, cyber adversaries will probe networks looking for unpatched systems they can compromise. To limit this risk, It is important to establish a patch management schedule so that all new system patches are implemented as soon as they are released.

3. Missing or weak authorization credentials:

A common tactic attackers employ is to brute force their way into a network by guessing employee credentials. It is important to educate employees on cybersecurity best practices so that their login information cannot be easily exploited to gain access to a network.

4. Malicious insider threats:

Whether unknowingly or with malicious intent, employees who have access to critical systems can share information that allows cybercriminals to breach a network. Insider threats can be difficult to track since all actions taken by

employees will appear legitimate and therefore raise little to no red flags. To help combat these threats, consider investing in network access control solutions, and segment your network based on employee seniority and expertise.

5. Missing or poor data encryption:

Networks with missing or poor encryption allow attackers to intercept communication between systems, leading to a breach. When poorly or unencrypted information is interrupted, cyber adversaries are able to extract critical information and inject false information onto a server. This can undermine an organization's cybersecurity compliance efforts and lead to substantial fines from regulatory bodies.

6. Zero-day vulnerabilities:

Zero-day threats are specific software vulnerabilities that are known to the attacker but have not yet been identified by an organization. This means that there is no available fix since the vulnerability has not yet been reported to the system vendor. These are extremely dangerous as there is no way to defend against them until after the attack has been carried out. It is important to remain diligent and continuously monitor your systems for vulnerabilities in order to limit the likelihood of a zero-day attack.

Risk assessment:

A cybersecurity risk assessment is an assessment of an organization's ability to protect its information and information systems from cyber threats.

The purpose of a cybersecurity risk assessment is to identify, assess, and prioritize risks to information and information systems. A cybersecurity risk assessment helps organizations identify and prioritize areas for improvement in their cybersecurity program. It also helps organizations communicate their risks to stakeholders and make informed decisions about how to allocate resources to reduce those risks.

There are many cybersecurity risk assessment frameworks and methodologies available, but they all share a common goal.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of the most popular risk assessment frameworks. It provides a flexible and structured approach for organizations to assess their cybersecurity risks and prioritize actions to reduce those risks.

Another popular risk assessment framework is the ISO 27001:2013 standard. This standard provides a comprehensive approach to information security management, including requirements for risk assessment and risk treatment.

Organizations can also develop their own customized risk assessment frameworks and methodologies. Whatever approach an organization chooses, the goal should be to identify, assess, and prioritize risks to information and information systems.

The 4 steps of a successful security risk assessment model:

1. **Identification:** Determine all critical assets of the technology infrastructure. Next, diagnose sensitive data that is created, stored, or transmitted by these assets. Create a risk profile for each.
2. **Assessment:** Administer an approach to assess the identified security risks for critical assets. After careful evaluation and assessment, determine how to effectively and efficiently allocate time and resources towards risk mitigation. The assessment approach or methodology must analyze the correlation between assets, threats, vulnerabilities, and mitigating controls.
3. **Mitigation:** Define a mitigation approach and enforce security controls for each risk.
4. **Prevention:** Implement tools and processes to minimize threats and vulnerabilities from occurring in your firm's resources.

Risk Assessment Methodologies:

Organizations can take several approaches to assess risks—quantitative, qualitative, semi-quantitative, asset-based, vulnerability-based, or threat-based. Each methodology can evaluate an organization's risk posture, but they all require tradeoffs.

Quantitative: Quantitative methods bring analytical rigor to the process. Assets and risks receive dollar values. The resulting risk assessment can then be presented in financial terms that executives and board members easily understand. Cost-benefit analyses let decision makers prioritize mitigation options.

However, a quantitative methodology may not be appropriate. Some assets or risks are not easily quantifiable. Forcing them into this numerical approach requires judgment calls—undermining the assessment's objectivity.

Quantitative methods can also be quite complex. Communicating the results beyond the boardroom can be difficult. In addition, some organizations do not have the internal expertise that quantitative risk assessments require. Organizations often take on the added cost to bring in consultants' technical and financial skills.

Qualitative: Where quantitative methods take a scientific approach to risk assessment, qualitative methods take a more journalistic approach. Assessors meet with people throughout the organization. Employees share how, or whether, they would get their jobs done should a system go offline. Assessors use this input to categorize risks on rough scales such as High, Medium, or Low.

A qualitative risk assessment provides a general picture of how risks affect an organization's operations.

People across the organization are more likely to understand qualitative risk assessments. On the other hand, these approaches are inherently subjective. The assessment team must develop easily-explained scenarios, develop questions and interview methodologies that avoid bias, and then interpret the results.

Without a solid financial foundation for cost-benefit analysis, mitigation options can be difficult to prioritize.

Semi-Quantitative: Some organizations will combine the previous methodologies to create semi-quantitative risk assessments. Using this approach, organizations will use a numerical scale, such as 1-10 or 1-100, to assign a numerical risk value. Risk items that score in the lower third are

grouped as low risk, the middle third as medium risk, and the higher third as high risk.

Blending quantitative and qualitative methodologies avoids the intense probability and asset-value calculations of the former while producing more analytical assessments than the latter. Semi-quantitative methodologies can be more objective and provide a sound basis for prioritizing risk items.

Asset-Based: Traditionally, organizations take an asset-based approach to assessing IT risk. Assets are composed of the hardware, software, and networks that handle an organization's information—plus the information itself. An asset-based assessment generally follows a four-step process:

- Inventory all assets.
- Evaluate the effectiveness of existing controls.
- Identify the threats and vulnerabilities of each asset.
- Assess each risk's potential impact.

Asset-based approaches are popular because they align with an IT department's structure, operations, and culture. A firewall's risks and controls are easy to understand.

However, asset-based approaches cannot produce complete risk assessments. Some risks are not part of the information infrastructure. Policies, processes, and other "soft" factors can expose the organization to as much danger as an unpatched firewall.

Vulnerability-Based: Vulnerability-based methodologies expand the scope of risk assessments beyond an organization's assets. This process starts with an examination of the known weaknesses and deficiencies within organizational systems or the environments those systems operate within.

From there, assessors identify the possible threats that could exploit these vulnerabilities, along with the exploits' potential consequences.

Tying vulnerability-based risk assessments with an organization's vulnerability management process demonstrates effective risk management and vulnerability management processes.

Although this approach captures more of the risks than a purely asset-based assessment, it is based on known vulnerabilities and may not capture the full range of threats an organization faces.

Threat-Based: Threat-based methods can supply a more complete assessment of an organization's overall risk posture. This approach evaluates the conditions that create risk. An asset audit will be part of the assessment since assets and their controls contribute to these conditions.
Threat-based approaches look beyond the physical infrastructure.

By evaluating the techniques threat actors use, for example, assessments may re-prioritize mitigation options. Cybersecurity training mitigates social engineering attacks. An asset-based assessment may prioritize systemic controls over employee training. A threat-based assessment, on the other hand, may find that increasing the frequency of cybersecurity training reduces risk at a lower cost.

Adavantages:

Pro #1: It is more than an automated vulnerability scan.

A vulnerability scan is a crucial component of this security risk assessment. Still, it's only one of the tools your security team uses to discover the risks and vulnerabilities within your network.

Even more important than the vulnerability assessment is the manual review the security team will perform on every component of your IT environment.

The combination of these tools is what makes the defensive IT security risk assessment so comprehensive.

Pro #2: You'll know how to make your security posture stronger.

A defensive IT security risk assessment doesn't just uncover your vulnerabilities.

Your security team will take their findings and put them into a list with risk ratings to inform you on which problems pose the most significant threat to your IT environment.

This will be in your security risk assessment report, along with a list of risk reduction recommendations, to help you plan for reducing the number of risks in your network.

Pro #3: Your security team is comprised of experts.

Regardless of who you hire for a defensive IT security risk assessment, the team should include cybersecurity experts.

At The KR Group, our internal Certified Information Systems Security Professional (CISSP) leads our team. As a customer, this means you can expect us to approach your IT environment with decades of experience looking for a variety of risks and providing effective solutions.

Disadvantages:

Con #1: It may not fit into your budget.

Since our security risk assessments are thorough and led by a team of experts, the cost can be prohibitive for some businesses.

Compared to a less extensive vulnerability risk assessment, which is an automated scan, the price tag of a defensive IT security risk assessment can appear steep.

We urge you to remember all this assessment encompasses. However, if the cost is still above your budget, talk with your IT security adviser about other options they have.

A defensive IT security risk assessment is only one of the types of security assessments available from IT consultants, including The KR Group.

Con #2: Remediation actions can be technical.

Providing risk remediation actions is essential to a security risk assessment. However, those actions aren't always straightforward.

A good security adviser will recommend the most efficient ways to address gaps in your security, but at times, they'll be technical.

You may need to hire an external IT expert to assist with the actions or anticipate your internal IT department will be extremely busy for several weeks.

Additionally, the risk reduction actions with or without external help aren't always free.

Con #3: Reviewing your security findings is a lengthy process.

Your security team will compile information about what areas of your environment they analyzed, what they found, what your top risks are, and recommendations to address those risks. This makes for a comprehensive and lengthy report.

Along with a large document with the details of your security risk assessment, the security team also reviews this information during a presentation. To hit all the important points within the report, your security adviser will spend several hours discussing what they found.

This process can be daunting, but we encourage you to stick through it and understand it will ultimately benefit your business

Risk Assessment: Likelihood & Impact:

Every organization is unique, so the risks they each face are not the same. In order to make a plan of action to protect your business, you need to first understand where the threats against you are. Once you know those risks and gaps, you can start to identify the likelihood of them occurring and the impact they could have on your organization.

Because of this**,** an information security risk assessment forms the cornerstone of any cybersecurity policy**.** Clear risk knowledge is crucial when making risk-based decisions for your company. Without full knowledge of where, how, and why a threat could occur, you won't be able to stop it. That's why understanding likelihood and impact for any given threat are both important factors in the risk assessment process.

Pratum's consultants perform information security risk assessments using a clear four-step process based on a clear formula. Start thinking about your risks by reviewing the basic threat likelihood/impact formula below.

Formula to Determine Risk Likelihood and Impact:

The standard described in NIST SP 800-53 implies that a realistic assessment of risk requires an understanding of these areas:

- Threats to an organization
- Potential vulnerabilities within the organization
- Likelihood and impacts of successfully exploiting the vulnerabilities with those threats

For handling the most basic level of risk assessment, risk managers can follow this simple formula:

Risk = (Threat x Vulnerabilities) x Impact

The first part of the formula **(Threats x Vulnerabilities)** identifies the likelihood of a risk. For example, if there's a known security flaw in older versions of software you use, there's the threat of hackers exploiting that particular vulnerability to compromise your system. But if you've applied the latest software patches that fix the problem, then the vulnerability cannot be exploited, and the threat has been eliminated.

Impact measures how much disruption you'll face if the threat actually occurs. Combining likelihood and impact produces a residual risk rating of Low, Medium or High. Each organization's residual risk rating may differ based on the likelihood and impact that each control deficiency introduces.

You could also represent this concept with a simple chart like this one:

For example, let's consider the risk of a hacker getting access to a folder containing all of your public-facing marketing materials. That event may have a medium likelihood, but it has a very low impact. Those materials are already publicly available on your website, etc., so unauthorized access to them does no harm. That risk gets a Low rating.

But the formula changes if the risk is an employee in the Accounts Payable department clicking a phishing link. There's at least a medium likelihood of one of those employees making this mistake. And the impact would be very high if a hacker got access to a user account that controls financial transactions. That risk gets a High rating.

Keep in mind that a very High impact rating could make a risk a top priority, even if it has a low likelihood. If a breach could shut down a hospital's life-support equipment, for example, that risk obviously deserves serious consideration on your priority list.

If you'd like to read detailed guidelines on how to rate risks by various factors, consult NIST SP 800-30.

Drilling Down on Specific Residual Risk:

Now that you know the formulas for determining likelihood and impact during a risk assessment, it's time to focus on specific risks.

1. Inherent risk – This is the risk level and exposure your system faces without taking into account any mitigating measures or controls that are actively in place. Where is your system at its weakest when no other security measures are in place to protect them? Which risks deserve the highest rating based on their likelihood and potential impact?

2. Residual risk – An area with a higher likelihood and impact of a threat on the organization, from an inherent risk level, may need additional controls to reduce the level of risk to an acceptable level. After you apply those controls, you are left with what we call "residual risk." If the residual risk level after mitigating controls is still higher than you prefer, then additional risk management measures and techniques should be introduced.

Mitigating measures you may apply include:

- **Avoidance –** Elimination of the cause of the risk. You could, for example, prevent employees from accessing certain parts of your system on mobile devices.

- **Mitigation –** Reduction of the probability of a risk's occurrence or of its impact. Adding multifactor authentication, for example, greatly reduces the probability of a hacker getting into a user's account.
- **Transfer –** Sharing of risk with partners, such as through insurance or other ventures.
- **Acceptance –** Formal acknowledgement of the presence of risk with a commitment to monitor it.

Finding Help When You Need It:

Reading through how to determine likelihood and impact can help you understand first steps in your risk assessment process. But you'll probably still need help from cybersecurity consultants to carry out a full assessment. These experts look over a number of key factors you may not have considered.

Cybersecurity consultants analyze your organization's structure, policies, standards, technology, architecture, controls, and more to determine the likelihood and impact of potential risks. They will also review your current controls and evaluate their effectiveness.

For example, a financial management company turned to Pratum when it realized that investors were choosing portfolio managers based, in part, on a company's strength of cybersecurity. The management firm asked Pratum's consultants to take a deep dive into its administrative, physical and technical controls. Pratum guided the company in developing a clear summary of its high and moderate risks along with recommendations for remediation.

Consultants also assess any gaps between your current security posture and where you want your organization to be. A core part of that process will be determining accountability and assigning risk ownership at the appropriate level and to the appropriate team. It's important to have the right security measures in the right hands.

End Goal: An Acceptable Level of Risk:

The end goal is to get to a level of risk that is satisfactory to your management team. It's important to evaluate and be aware of the risk in your environment so you can implement appropriate controls to mitigate this risk and secure sensitive information. Evaluating risk means understanding the biggest factors of any security threat, likelihood and impact.

If you're looking for a security partner to address your risk assessment needs, please contact a Pratum Consultant at any time for more details on ways you can secure your business.

Risk Determination:

Risk determination assesses threats and vulnerabilities to consider the likelihood that known threat sources will be able to exploit identified vulnerabilities to cause one or more adverse events and the consequences if such events occur. Depending on the type of threat under analysis and the nature of the risk assessment being performed, likelihood and impact may be

determined using relative ratings or quantitative estimates. Many factors contribute to likelihood, including some that are difficult to measure accurately, such as ease of exploitation, skill level or sophistication of adversaries, visibility of the organization, and attractiveness of the organization or its assets to attack [51]. Accurate quantitative risk determination requires sufficient historical observations or other evidence to support calculation of probabilities, and also requires impact to be expressed in numeric terms, such as dollar values. Organizations may characterize the nature and severity of adverse impacts according to what aspect of security is impacted, the extent of disruption to operations, the resources lost, or the consequences to mission execution or organizational stakeholders. Whether stated in absolute or relative terms, determinations of risk enable risk managers to compare and prioritize risk—within a specific information system or operational context or across the organization—and represent key inputs to risk response decisions.

Risk Determination provides a quantitative risk value representing the systems exposure to a threat exploiting a particular vulnerability after current controls have been considered. This quantitative value is in the form of a Risk Score. A risk score basically follows the following formula:

RISK= IMPACT x LIKELIHOOD

The computation for the risk value is a fairly straightforward multiplication of the Impact and Likelihood scores. This computation was performed for all threat and vulnerability pairs for all systems that were in scope for this assessment. An example of what this looks like for one of the hypothetical in scope systems is captured below:

Application: Hospital Information System

Threat (Agent and Action)		Vulnerability	Impact Score	Likelihood Score	Risk Score
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	5	2	10
External Intruders,	System intrusion and	Possible Weak Passwords	5	2	10

Application: Hospital Information System

Threat (Agent and Action)		Vulnerability	Impact Score	Likelihood Score	Risk Score
Malicious Insiders, Malicious Code	unauthorized system access	due to lack of password complexity controls			
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	2	10
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	3	15
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5	2	10
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	5	1	5

The following risk categorization table was then used to categorize the distinct system risk scores into risk classification "buckets" of High, Moderate, or Low Risk:

For all system risk scores and risk classifications please refer to the Data Collection and Computation matrix in the Appendices of this report.
Based on the risk scores, what follows are aggregate views resulting from the risk determination phase. This table presents a ranking of applications based on their aggregate risk scores (sum of all risk scores for all threat and vulnerability pairs). In theory, the higher the aggregate risk score, the greater the risk to the system.

Risk Rank	Application	Aggregate Risk Score
1	HIS	60
2	HR Payroll	50
3	Cardio Research DB	47
4	Email	46
5	Imaging	45

Finally based on the aggregation and categorization effort in the previous tables, the following table identifies the high risk systems for each of the risks represented by a threat and vulnerability pair:

Threat Agent	Threat Action	Vulnerability	Score	High Risk Systems
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	59	Imaging, Email
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible weak Passwords due to lack of password complexity controls	57	HR Payroll
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	44	HIS
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	41	None
Non-Specific, Natural	Loss of power	Lack of redundant power supply	26	None
Natural	Equipment damage or destruction due	Lack of environmental	21	None

Threat Agent	Threat Action	Vulnerability	Score	High Risk Systems
	to natural causes (fire, water, etc.)	controls		

As seen in the template, the structure of the Risk Determination section follows a very similar pattern as the three intermediary sections (Impact, Likelihood, and Control Analysis) whereby the full results are referenced in a container as it is not feasible to put everything in the body of the report. A key differentiator is that by virtue of it being the final stage of the computation, there are certain aggregate tables that can be presented.

Risk Evaluation Definition:

Risk evaluation is defined by the Business Dictionary as: “Determination of risk management priorities through establishment of qualitative and/or quantitative relationships between benefits and associated risks.”

Performing a Risk Evaluation:

A risk evaluation can be performed in five simple steps.

1. Identify and prioritize assets: Consider all the different types of data, software applications, servers, and other assets that are managed. Determine which of these is the most sensitive or would be the most damaging to the company if compromised.

2. **Locate assets:** Find and list the source of those assets. Be it desktop office computers, mobile devices, internal servers, or anything else, you’ll want to trace each asset back to its source.

3. **Classify assets:** Categorize each asset as either public information, sensitive internal information, non-sensitive internal information, compartmentalized internal information, or regulated information.

4. **Perform a threat modeling exercise:** Identify and rate all the threats faced by your top-rated assets. Microsoft’s STRIDE method is a popular one.

5. **Finalize data and make a plan:** Once you have your evaluation, it’s time to start tackling those risks, beginning with the most critical.

RISK ASSESSMENT PROCESS / RISK EVALUATION PROCESS:

Risk evaluation process or risk assessment involves the following steps:

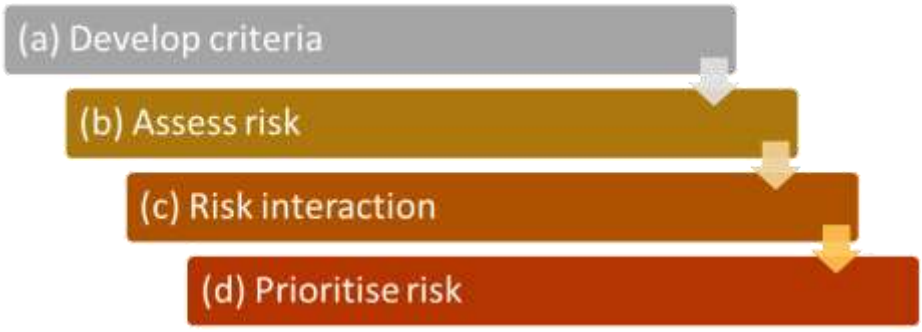
RISK IDENTIFICATION:

The first step in risk assessment is Risk identification. It is necessary to identify the risk involved in a particular project or business. It is must to manage the risk. If the risk managers are not able to identify the risk, then it is impossible to manage the risk. Thus, it is must for every risk manager to identify all kinds of risks (financial, operational, strategic etc.) and sub categories of risk like market, credit, liquidity etc. The risk managers have to identify key risk involved in a particular project.

RISK ASSESSMENT:

The next step in risk evaluation process is to assess the quantity of risk by checking the likelihood and severity of impact of risk in a particular project or business. The likelihood of risk event determines the probability of occurrence of an event. The risk manager will have to identify the risk with highest probability and its impact on business.

The risk assessment process further involves four steps:



(a) Develop Criteria:

The first step in Risk assessment process is to develop the criteria or base on which the risk is assessed or prioritised of a particular firm or project. The criteria set a benchmark on basis of which the comparison on company basis, industry basis is done.

(b) Assess Risk:

After developing criteria, risk is assessed with the help of various qualitative and quantitative techniques.

(c) Risk Interactions:

The third step within risk assessment is to determine risk interactions. Risk do not interact in isolation but its effects get magnified when it gets interacted with the environment in which the business survives. Thus, it is very essential to study and assess risk interactions. There are various techniques like bow-tie diagrams, risk interaction matrices, fault trees and event trees etc.

(d) Prioritise Risk:

The fourth and the last step is to prioritise the risk assessed or evaluated. These rankings are essential to manage the risk. The risk manager can pay more attention to those risks which are significant in the nature. The prioritisation of the risk is done in two steps:

1. They are ranked according to one or more criteria like its impact, likelihood or vulnerabilities etc.
2. Then these ranks are revised in the light of other factors.

On the basis of this, a hierarchy is formed which has to be managed in a proper or systematic manner. These risks are then plotted on the risk map or heat map which further clarifies the situation. The risk map can give detailed analysis of likelihood and impact of risk event on an ordinal scale of high, low medium etc.

RESPOND TO RISKS:

The last step in the risk assessment process or risk evaluation process is to minimise the risk by responding to the risks evaluated in a very rational manner. Various response options such as accept, reject or avoid are examined in the light of the above analysis and the cost benefit analysis is done to reach at the conclusion.

During risk evaluation, you'll compare the results you came up with during your risk analysis and compare those to your organization's existing risk criteria to determine if you'll need to do more to treat the risk(s) you're assessing.

During risk evaluation, your organization may choose to:

- Do nothing
- Consider implementing other risk treatments
- Reconsider your organization's objectives
- Return to the risk analysis phase to develop a more thorough understanding of the risk at hand

The importance of risk evaluation and perception:

Risk evaluation attempts to define what the estimated risk actually means to people concerned with or affected by the risk. A large part of this evaluation will be the consideration of how people perceive risks. This section of the book provides an overview of the psychometric and cultural approaches underpinning risk perception, offering an insight into the reasons why risks are perceived in different ways.

Risk Treatment:

Risk treatment is a collective term for all the tactics, options, and strategies chosen to respond to a specific risk, bound to achieve the desired outcome concerning the threat.
Consequently, risk treatment is not a concept functioning on its own. On the contrary, it should always be examined, understood, and implemented as part of a bigger whole, i.e., risk management.

Simply put, the **risk management** process is a firm's policy, composed of different steps taken to ensure proper management of occurring threats. In general, risk management's actions include:

- **Risk identification:** The inspection process allows you to identify the organisation's potential risks to ensure all the threats are recognised.
- **Risk assessment and evaluation**: The analysis is bound to reveal the threat's consequences, outcome, likelihood, and severity. Thus, the analysis examines both the risk factor and the harm that it is bound to produce.
- **Risk treatment**: The plan of implementing various strategies, activities, and actions to appropriately deal with the threat and manage it in a possibly profitable way.

- **Risk monitoring**: The implementation of a continuous control system over the threat after treating it.

Five Steps Of Risk Treatment:

In the risk treatment process, it's recommended to follow five main steps to ensure the correct logistics and effectiveness of the strategy:

- Brainstorming and selecting the right risk treatment option.
- Planning and use of options chosen.
- Examining the effectiveness of the chosen tactics.
- Deciding whether the level of the remaining risk, i.e., residual risk, is acceptable or not.
- If it's not acceptable, implementing new risk treatment activities to reduce the residual risk.

Risk Treatment Options:

There are several risk treatment strategies to deal with the risks. Notably, one kind of treatment cannot apply to all possible threats. It's crucial to review each threat individually to predict the effect of each solution.

The risk treatment options include:

- Risk Avoidance
- Risk Reduction
- Risk Transfer
- Risk Retention

RISK AVOIDANCE:

If the risk assessment concludes that the risk is too high to be mitigated, it's possible to avoid the risk by resigning from performing specific actions or processes. The avoidance strategy is linked to interpreting the risk as unfavourable to the point that it should be excluded entirely. To avoid the risk,

the company might choose to perform another action instead, as the alternative generates a lower threat.

RISK REDUCTION:

Risk reduction is an important risk treatment strategy because it requires taking action to reduce the impact of a given risk while maximising the benefits obtained from taking such action(s).

To reduce the likelihood of risk or to bring its consequences down to an acceptable level, the company might implement safeguards or controls, carefully chosen from the range of the available control processes. By diminishing the risk to the required level, this option ensures the needed level of security.

There are two steps to reduce risk as part of the risk treatment plan. The first one is using preventive methods, such as:

- Human resources and staff training
- Legislation compliance
- Quality control measures
- Auditing
- Regular maintenance
- Security systems installation

The second method to reduce risk involves the implementation of certain procedures upon the occurrence of a risk event:

- Data backups
- Emergency procedures
- Minimise exposure to highest-rated risks

RISK TRANSFER:

Transferring risk is related to passing a specific portion of the threat to another party to reduce its likelihood or impact on the organisation. However, it's vital that another party - for example, an insurance company - is informed about

the consequences of the sharing, the impact of the risk, and the expected transfer cost.

This type of risk treatment might be executed by signing a contract with a service provider or purchasing an error insurance.

Notably, this option does not mitigate the risk itself, as it deals only with its consequence. Thus, the transfer treatment should be typically implemented along with other risk treatment plans.

There are various forms of implementing this particular risk treatment option, such as the following:

- Hedging strategies
- Contractual agreements
- Hiring a security company
- Properly vetting suppliers and vendors

RISK RETENTION:

Suppose the analysis concludes that the risk rating is at acceptable levels, or the mitigation cost of the implemented strategy is higher than the expected damage. Only after the cost-benefit analysis is performed should you decide to choose risk retention as your best risk treatment option.

In that case, the appropriate treatment might be to accept the risk and not take any actions to treat it. However, you must only choose this treatment option assuming the risk should always go hand in hand with implementing a system that would continuously control and monitor the given risk, along with its possible development.

Security Management:

Security management covers all aspects of protecting an organization's assets – including computers, people, buildings, and other assets – against risk. A security management strategy begins by identifying these assets, developing and implementing policies and procedures for protecting them, and maintaining and maturing these programs over time.

Below, we discuss what security management means to organizations, types of security management, and review some considerations for security management when choosing a cyber security solution.

Purpose of Security Management:

The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy. The information and procedures developed as part of security management processes will be used for data classification, risk management, and threat detection and response.

These procedures enable an organization to effectively identify potential threats to the organization's assets, classify and categorize assets based on their importance to the organization, and to rate vulnerabilities based on their probability of exploitation and the potential impact to the organization.

Types of Security Management:

Security management can come in various different forms. Three common types of security management strategies include information, network, and cyber security management.

#1. Information Security Management:

Information security management includes implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/IEC 27000 family of standards. Information security management programs should ensure the confidentiality, integrity, and availability of data.

Many organizations have internal policies for managing access to data, but some industries have external standards and regulations as well. For example, healthcare organizations are governed by the Health Insurance Portability and Accessibility Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) protects payment card information.

#2. Network Security Management:

Network security management is a vital component of a network management strategy. The network is the vector by which most cyberattacks reach an organization's systems and its first line of defense against cyber threats. Network security management includes deploying network monitoring and defense solutions, implementing network segmentation, and controlling access to the network and the devices connected to it.

#3. Cybersecurity Management:

Cybersecurity management refers to a more general approach to protecting an organization and its IT assets against cyber threats. This form of security management includes protecting all aspects of an organization's IT infrastructure, including the network, cloud infrastructure, mobile devices, Internet of Things (IoT) devices, and applications and APIs.

Security Management Architecture:

A scalable and sustainable security management strategy is one that is built using an integrated framework and the right tools rather than a disconnected set of standalone policies and strategies. A security management architecture enables an organization to consistently enforce its security policies across its entire IT ecosystem. This requires an array of integrated security solutions that enable centralized management and control of an organization's entire security infrastructure.

Impact of DevSecOps on Security Management:

A shift is on to automate security management using DevOps. There are many security tasks that are repetitive and take time to complete when using a management user interface. Security automation is a valuable tool for reducing the time spent completing tasks.

Examples of security management tasks that could benefit from automation include:

- Adding rules and objects to a security policy to complete a new project.
- Responding to a security incid/ent by validating threat indicators, mitigating the threat by isolating the infected host, and searching logs for other infected hosts using Indicators of Compromise (IoC) returned from the security incident analysis.
- Provisioning new cloud infrastructures, including the firewalls and the security policy for the firewalls protecting the new infrastructure.
- Cloud applications of DevSecOps include container image scanning, code scanning, Infrastructure as a Code (IaC) scanning, and scanning for credential exposure.

Security Management with Check Point:

Security management has always been one of Check Point's core competencies, and we continually work to evolve security and management capabilities to meet the evolving needs of the market and our customers. Check Point security management can be deployed on the platform of your choice; turn-key security management appliances, open server hardware, in public and private cloud environments, and as a hosted cloud service. Check Point's security management solutions are based on four key pillars, including:

- Security Automation into CI/CD Pipelines: Integrating security into CI/CD pipelines via automation reduces configuration errors, makes rapid deployments possible, and allows operational processes to be orchestrated.
- Security Consolidation: Consolidated security improves efficiency, reduces capital and operational expenditure (CAPEX and OPEX), and achieves improved visibility and context by integrating security policy and events management within a single solution.

- Solution Agility: Security management solutions must be agile and dynamic to keep up with the evolving cyber threat landscape. An example is an object in the security policy that defines private or public cloud addresses or users. As these external entities change, so does the security policy.
- Efficient Operations: Security should be a business enabler, not a roadblock.

  Security management solutions must be efficient to not inhibit security innovation. For example, easy to use management that unifies security and event management and enables delegated access to multiple admins at the same time enables security staff to do more in less time.

Feature of Security Management System:

- Security management relates to the physical safety of buildings, people, and products.
- Security management is the identification of the organization's assets.
- Generally, Security Management System is provided to any enterprise for security management and procedures as information classification, risk assessment, and risk analysis to identify threats, categorize assets, and rate.

Understand the 5 Pillars of the Security Management:

1. Physical Security:

Physical Security relates to everything that is tangible in your organization.

- Access to Buildings
- Physical Assets
- IT Hardware
- Vehicle Fleet

Responsibility for Physical Security lies with: Operations Manager, Security Staff.

2. People Security:

Humans typically present the greatest threat to an organisation's security, be it through human error or by malicious intent. People Security is about mitigating risk by monitoring and controlling the access and flow of people.

- Permanent & Contract Staff

- Partners
- 3rd Party Employees
- Visitors
- Special Events Security

Responsibility for People Security lies with: HR, Security Staff.

3. Data Security:

Data can be both an asset and a liability. Whether it is the Intellectual Property (IP) of your organization, or the personal data of employees and customers, protected by privacy regulations such as the GDPR, it needs to be handled with care. Appropriate data protection policies and procedures must be implemented to manage data storage, processing and compliance.

- Trade Secrets
- Employee Data
- Database
- Customer Data

Responsibility for Data Security lies with: HR, IT Teams & Managers.

4. Infrastructure Security:

Information Security refers to the intangible assets of your organization, where data is stored and controlled. These must be protected to prevent security breaches and leaks.

- Networks
- Remote Sites
- Application Security
- Website
- Intranet

Responsibility for Infrastructure Security lies with: IT Team & Managers.

5. Crisis Management:

Effective Crisis Management depends on an organization's ability to be prepared for any eventuality. Policies and protocols must be continuously tested and revised to mitigate exposure.

- Documentation & Work Procedures
- Emergency Response Plans
- Business Continuity Plans
- Disaster Recovery Plans

Responsibility for Crisis Management lies with: Operation Manager, IT Team & HR.

Security Policies:

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies:

1) It increases efficiency

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

1. Virus and Spyware Protection policy:

This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy:

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy

This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies. This policy requires that the client system must have installed antivirus.

8. Information Technology Purchasing Policy

The reason for this strategy is to characterize norms, methods, and limitations for the acquisition of all IT equipment, programming, PC-related parts, and specialized administrations bought with organization reserves. Acquisition of innovation and specialized administrations for the organization should be supported and facilitated through the IT Department.

9. Web Policy

The reason for this policy is to set up guidelines for the utilization of the organization’s Internet for access to the Internet or the Intranet.

10. Log Management Policy

Log management is often of great benefit during a sort of scenario, with proper management, to reinforce security, system performance, resource management, and regulatory compliance.

11. Password Policy

The concept of usernames and passwords has been a fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity. The purpose of this policy is to determine a typical for the creation of strong passwords, the protection of these passwords, and therefore the frequency of changing passwords must be followed.

12.Cloud Computing Adoption

The purpose of this policy is to make sure that the corporate can potentially make appropriate cloud adoption decisions and at an equivalent time doesn't use, or allow the utilization of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed during this policy.

13. Server Security Policy

The purpose of this policy is to define standards and restrictions for the bottom configuration of internal server equipment owned and/or operated by or on the company's internal network(s) or related technology resources via any channel.

14. Systems Monitoring And Auditing Policy

System monitoring and auditing are employed to work out if inappropriate actions have occurred within a data system. System monitoring is employed to seem for these actions in real-time while system auditing looks for them after the very fact.

15. Vulnerability Assessment

The purpose of this policy is to determine standards for periodic vulnerability assessments. This policy reflects the company's commitment to spot and implementing security controls, which can keep risks to data system resources at reasonable and appropriate levels.

Acceptable Use Policy:

An acceptable use policy, also called an AUP, is an agreement between two or more parties that outlines the appropriate use of access to a corporate network or the internet. This document describes what users may and may not do when accessing this network.

An AUP is useful for businesses and educational facilities that provide internet access to employees or students. Before they are granted access to the network, they must agree to these terms and conditions. Likewise, when you sign up with an internet service provider, they usually have you sign an AUP that requires you to follow a certain set of stipulations.

What Is Covered in an Acceptable Use Policy:

Companies and other facilities use an AUP to protect their networks from bad players. The purpose of an AUD is to ensure everyone is only using internet access for appropriate tasks. Limiting what users can do can help these internet providers uphold the law and protect other users from cybersecurity threats. Here are a few stipulations you may find in an AUP:

- Avoid violating the law while using the service
- Do not attempt to hack the security of the network or users on the network
- Do not attempt to send spam or junk mail
- Do not attempt to crash a website's server with spam or mass emails

- Report any suspicious behavior you may see on the network

Why Is an Acceptable Use Policy Important

If your business provides internet access, then you need an AUP for these reasons:

Preventing Cybersecurity Threats: Businesses and institutions want to have some sort of control over what activity takes place on their networks. Limiting what users can browse, download, and search on the internet is all a part of keeping a safe network . If a student or employee were to open a suspicious attachment or visit unsecured websites, they could make your network vulnerable to hackers and viruses.

Ensure Users are Avoiding Illegal Activity:

An AUP can help ensure users are following the law. For instance, an AUP may strictly prohibit users from pirating music, movies, or other files. It may outline that if a user is violating these rules, they will be banned from the network. Having users break the law on your network can become a liability for your business, which is why outlining these prohibited activities in your AUP is so essential.

Focus on Productivity:

Schools may also use an AUP to ensure their students are focusing on classwork rather than looking up things for fun on the web. Also, when young people are using the internet, schools need to make parameters to protect children from any inappropriate websites. Businesses can use it to ensure their employees are working on their tasks rather than browsing social media or tending to personal communications.

Creating an Acceptable Use Policy:

When creating an AUP for your business, you need to consider these key factors:

Acceptable Internet Use:

Employers should have an internet use policy to ensure their employees are staying on task during working hours. The level of freedom your team gets should depend on the type of work they do. For instance, creative teams may need a larger scope of access to be able to check out social media trends and pop culture. Other teams may need access to the news or local reports to do their job right.

When deciding what's allowed, remember that your employees want to be treated like adults. An overly restrictive AUP may hinder their work and make them feel that you can't trust them. Many businesses choose to restrict the following type of websites:

- Social media
- Streaming
- Shopping
- News
- Personal email/communications
- Pornography
- Gambling
- Illegal activity

Cybersecurity:

Protecting sensitive information is at the heart of most AUPs. It's crucial that you outline which at-risk behaviors employees should avoid when using your

network. A data breach could cost your business and employees a lot of time and money, so use your AUP to outline these common security policies:

- Keep all passwords private, and change them regularly
- Do not use public Wi-Fi on company devices
- Never open email attachments or links that you are not expecting. When something appears suspicious, contact the IT department
- Sign up for two-factor authentication
- Social media is only allowed for business purposes

Private Information:

Employees need to be able to send confidential information to one another securely. In your AUP, outline how employees can safely send, view, and store company data. If there happens to be a data breach, an AUP can also tell employees how to handle such a situation. Outline how to report an incident, who to report it to, and any other important protocols for when an employee is experiencing a network issue.

Guest Users:

Many businesses have a separate network for their guests. When a guest logs on, they usually have to sign an AUP. In this document, it's wise to make your policies even stricter for those who are not employees. Make sure guests cannot access internal files or information.

Security Management Best Practices:

Security management now is more complex and the top 10 security management best practices are now a must for CIOs and CSOs

Too many companies have found out the hard way that their most valuable assets are exposed and vulnerable to hacker attracts, theft and destruction. They now have learned a very expensive lesson, a company's valuable information cannot be undone, and also often leads to significant damage to your company's reputation.

10 Security Management Best Practices

- **Centralize Malware Management -** Centralize malware monitoring, incident responses, assessing and reporting operational impacts from end point to perimeter with regard to ensuring activation and standard use, monitoring and reviewing malware activity, and most importantly, responding to issues. Include all sources
    - anti-malware applications,
    - anti-virus,
    - anti-trojan,
    - spam filtering,
    - web filtering and
    - website scanners.
- **Establish Boundary Control -** Consolidate monitoring of access activity from boundary defenses including firewalls, routers, VPNs and other network resources. Setup analysis of cross-correlating network flows with other operational data to identify suspicious behavior and potential security threats. Understand boundary definitions in each organization in terms of levels of risk, appropriate access grants and monitoring interests.
- **Centralize Provisioning and Authorization Management -** Establish firm rules, alerts and reporting to consolidate all provisioning and authorization management - monitor successful logins, subsequent secondary logins and user/system activities to facilitate investigations. Eliminate shared credentials. Monitor failures in addition to successful accesses to monitor and investigate insider threats including privileged users and consultants.
- **Implement Acceptable Use Policy -** Publish Acceptable Use policies so which users better understand when, where and how best to use and protect corporate assets and information. Create watch lists used to facilitate monitoring processes for the acceptable use of critical resources, user roles and specific acceptable use policy violations. Include monitoring for after hour and focus on non-typical uses.
- **Build Security into Applications Starting in the Design Phase -** Design security into applications. That includes both new applications and existing ones. Go beyond the perimeter, network and host security defenses and include application platform monitoring, resource monitoring, web application defenses and database activity monitoring. Incorporate web application firewalls (WAF) to inspect and filter HTTP traffic at the application layer to monitor web and mobile applications. .
- **Understand and implement all compliance and audit requirements –** understand applicable industry, regulatory and legal obligations for security and risk management. Compliance reports and dashboards should be defined to support security analysts, internal and external auditors and the CIO or CSO.

- **Implement Monitoring and reporting processes** - Define monitoring and reporting requirements including objectives, targets, capacity requirements, compliance reports, implementation and work flow with key constituents prior to deployment of any technical tools.
- **Manage security deployment and infrastructure processes** - Manage the deployment in phases, maintain source activation and consistent delivery of event and log data and refine the system continuously. On-going maintenance costs and growth plans need to be incorporated as part of the overall planning to obtain a true Total Cost of Ownership (TCO).
- **Implement network and host defenses** - Aggregate IDS/IPS alerting and filter IDS/IPS false positives and facilitate incident management.
- **Constantly validate network and system resource integrity** - Manage the infrastructure, from deployed devices, systems, applications to configuration, vulnerability and patch details to assure and maintain operating integrity.

Security model :

A security model is a computer model which can be used to identify and impose security policies. It does not need some prior formation it can be founded on the access right model or analysing computing model or computation model.

A security model is a statement that framework the requirements necessary to properly provide and implement a specific security policy. If a security policy indicates that some users should be identified, dependable, and recognized before accessing network resources, the security model can lay out an access control matrix that should be constructed so that it accomplish the requirements of the security policy.

Security model characteristics:

An organization defines a security model to meet its business needs. The model serves as a basis to define the requirements and actual implementation of a security system.

Some characteristic objectives of a security model include:

- Verifying the identity of users, provided by authentication systems that include password strength and other factors.
- Enabling authorized users to access resources, provided by authorization systems that define request or role-based processes, and related provisioning. Resources, for example, include accounts,

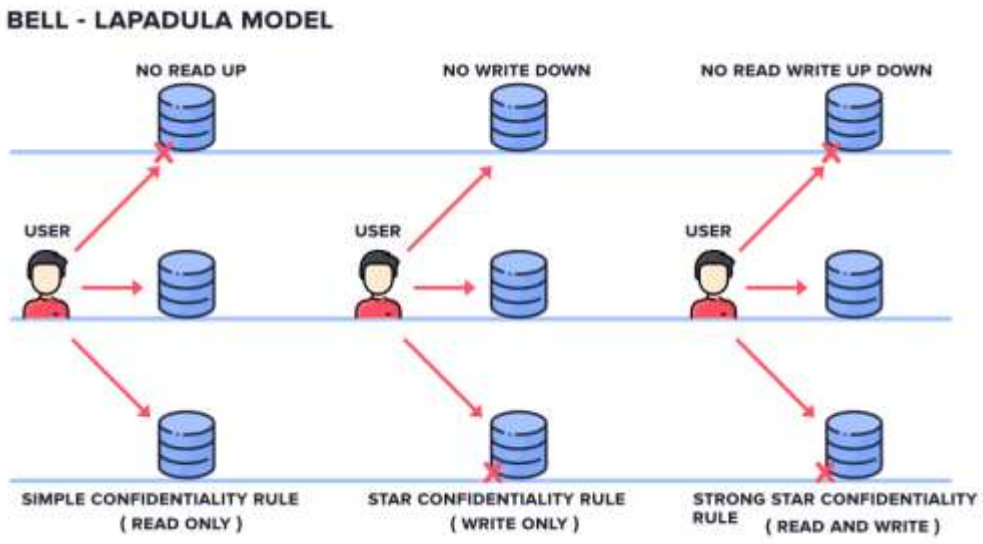
services, user information, and IBM Security Identity Manager functions.

A security model also requires additional provisioning processes to select the resources that users are permitted to access.

- Administering which operations and permissions are granted for accounts and users.
- Delegating a user's list of activities to other users, on a request or assignment basis.
- Protecting sensitive information, such as user lists or account attributes.
- Ensuring the integrity of communications and data.

1. Bell-LaPadula

This Model was invented by Scientists **David Elliot Bell** and **Leonard .J. LaPadula**.Thus this model is called the Bell-LaPadula Model. This is used to maintain the **Confidentiality** of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy.



It has mainly 3 Rules:

- **SIMPLE CONFIDENTIALITY RULE**: Simple Confidentiality Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO READ-UP
- **STAR CONFIDENTIALITY RULE**: Star Confidentiality Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the

Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO WRITE-DOWN

- **STRONG STAR CONFIDENTIALITY RULE**: Strong Star Confidentiality Rule is highly secured and strongest which states that the Subject can Read and Write the files on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as NO READ WRITE UP DOWN

he **Bell-Lapadula Model** of protection systems deals with the control of *information flow*. It is a linear non-discretionary model. This model of protection consists of the following components:

- A set of *subjects*, a set of *objects,* and an access control matrix.
- Several ordered security levels. Each subject has a clearance and each object has a classification which attaches it to a security level. Each subject also has a current clearance level which does not exceed its clearance level. Thus a subject can only change to a clearance level below its assigned clearance level.

The set of access rights given to a subject are the following:

- **Read-Only**: The subject can only read the object.
- **Append** : The subject can only write to the object but it cannot read.
- **Execute** : The subject can execute the object but can neither read nor write.
- **Read-Write**: The subject has both read and write permissions to the object.

Control Attribute: This is an attribute given to the subject that creates an object. Due to this, the creator of an object can pass any of the above four access rights of that object to any subject. However, it cannot pass the control attribute itself. The creator of an object is also known as the *controller* of that object.

Restrictions imposed by the Bell-Lapadula Model:

The following restrictions are imposed by the model:

- **reading down**: A subject has only read access to objects whose security level is below the subject's current clearance level. This prevents a subject from getting access to information available in security levels higher than its current clearance level.

- **writing up**: A subject has append access to objects whose security level is higher than its current clearance level. This prevents a subject from passing information to levels lower than its current level.

Clearance and Classification Levels

There are two types of levels in the Bell-LaPadula model: classification and clearance levels.

Classification levels are used to protect information from unauthorized disclosure. These levels are used to assign a security label to an object. The security labels are used to control access to the object. Examples of classification levels in the Bell-LaPadula model could include Top Secret, Secret, Confidential, and Unclassified, with Top Secret holding the highest level of trust/classification and unclassified being the lowest (available to the public).

Clearance levels are used to protect information from unauthorized modification and unauthorized use/access. These levels are used to assign a security level to a subject. The clearance levels mimic the classification levels in their structure. For example:

- **Top Secret:** Subjects with this clearance level would have access to all objects with a classification level of Top Secret and below.
- **Secret:** Subjects with this clearance level have access to all objects with a classification level of Secret and below.
- **Confidential:** Subjects with this clearance level would have access to all objects with a classification level of Confidential or Unclassified.
- **Unclassified:** Subjects with this clearance level could only access unclassified/public information. They would have no access to information classified as Top Secret, Secret, or Confidential.

Problems with Bell-La Padula:

- Focus on Confidentiality, not much else.
- The process of assigning and enforcing security classifications for each file and user is glossed over in the model, and is hard to implement in real life.
- Classification of data data changes over time; how will you deal with this?
- Since data tends to migrate into "higher" security classifications (due to the write-up property), a trusted user has to continually "downgrade" it.
- Bruce Schneier: "Data sometimes have a higher classification in aggregate than each datum does individually: An individual telephone number at the NSA is Unclassiffied, but the entire NSA phone book is classified Confidential." (Secrets and Lies, page 126).
- Too complex

Properties of Bell-LaPadula:

In Bell-LaPadula, we have two security properties that define how information can flow to and from the resource.

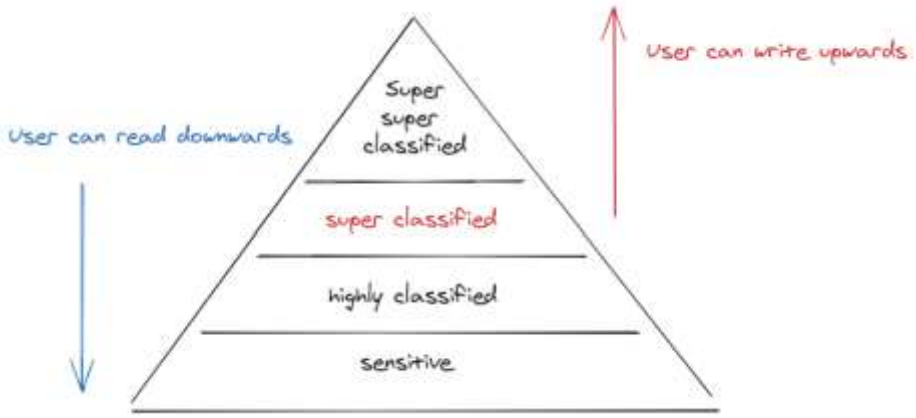
1.The Simple Security Property: The level of access granted to an individual must be at least as high as the classification of the resource in order for the individual to be able to access it.

2.The *Property: Anyone accessing a resource can only write its contents to one classified at the same level or higher.

Example of Bell-LaPadula Model:

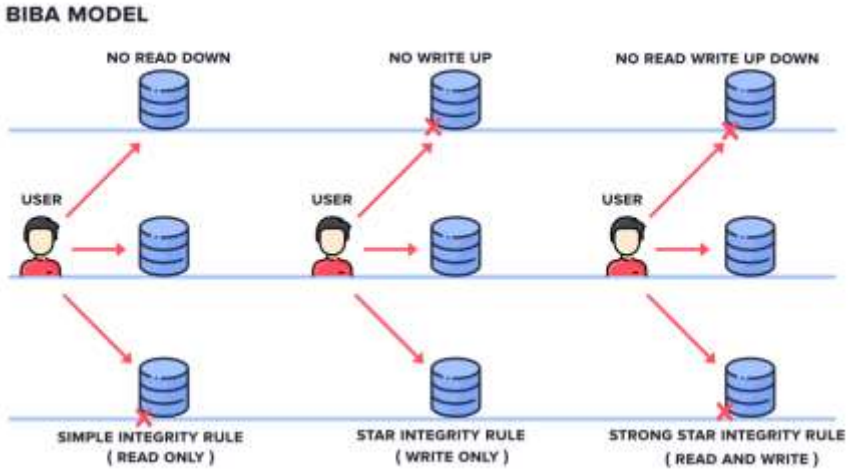
A great example is a secret agent wanting to send a message back to headquarters. This rule can be thought of as “no write down”.

Together, the Bell-LaPadula Model can be summarized as *no reading up, no writing down.* If you do this, you’re enforcing confidentiality.



Biba Model:

This Model was invented by Scientist Kenneth .J. Biba. Thus this model is called Biba Model. This is used to maintain the Integrity of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy. This works the exact reverse of the Bell-LaPadula Model.



It has mainly 3 Rules:

- **SIMPLE INTEGRITY RULE**: Simple Integrity Rule states that the Subject can only **Read** the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as **NO READ DOWN**
- **STAR INTEGRITY RULE**: Star Integrity Rule states that the Subject can only **Write** the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as **NO WRITE-UP**

- **STRONG STAR INTEGRITY RULE**

Biba Integrity Model:

The Biba paper defines three different mandatory integrity models:

1. Low-Water Mark Policy
2. Ring Policy
3. Strict Integrity Policy

The **Low-Water Mark Policy** is a dynamic policy with three rules that basically amount to:

1. the new integrity level of a subject is the minimum of the previous integrity level of the subject and the integrity level of the currently accessed object
2. for all subjects s, and all objects o, a subject can modify an object iff the integrity level of the object is dominated by the integrity level of the subject.
3. for all subjects s1 and s2, s1 may invoke s2 iff the integrity level of s2 is dominated by the integrity level of s1.

The **Ring Policy** is a more flexible policy that only provides two rules:

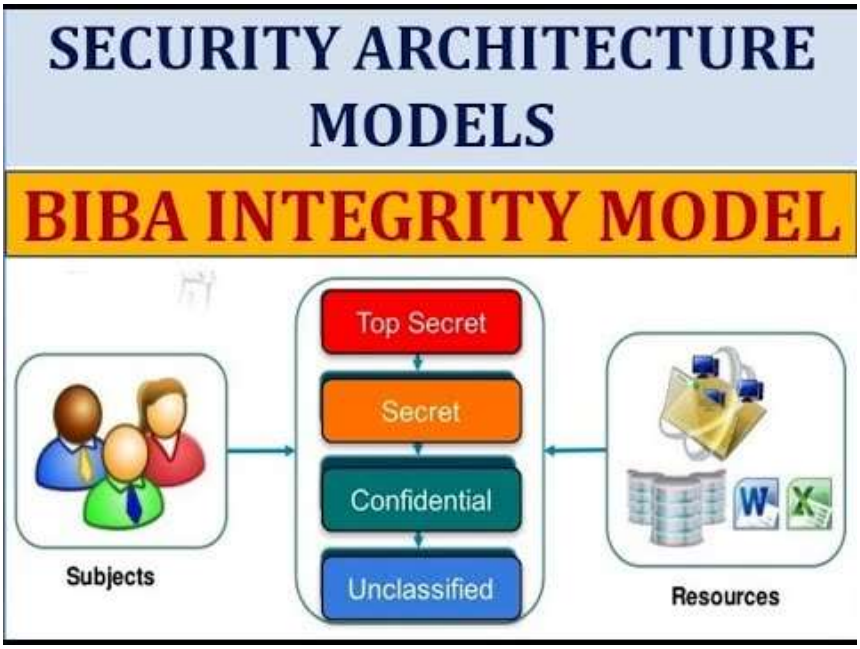
1. for all objects o and all subjects s, s may modify o iff the integrity level of the object is dominated by the integrity level of the subject. *(This is very close to Pfleeger's statement of the simple integrity property.)*
2. for all subjects s1 and s2, s1 may invoke s2 iff the integrity level of s2 is dominated by the integrity level of s1

The **Strict Integrity Policy** is 'considered a "complement" or "dual" of the security policy' (p32). This is the policy that states the two axioms which correspond to the Bell-La Padula model. This gives three rules/axioms:

1. for all subjects s and all objects o, s may observe o iff the integrity level of s is dominated by the integrity level of o
2. for all subjects s and all objects o, s may modify o iff the integrity level of o is dominated by the integrity level of s
3. for all subjects s1 and s2, s1 may invoke s2 iff the integrity level of s2 is dominated by the integrity level of s1

The Biba model addresses the issue of integrity, i.e. whether information can become corrupted. A new label is used to gauge integrity. If a high security object comes into contact with a low-level information, or be handled by a low-level program, the integrity level can be downgraded. For instance, if one used an insecure program to

view a secure document, the program might covertly copy it to another part of the system.



Integrity is usually characterized by the tree following goals:

1. The data are protected from any modification by unauthorized users
2. The data are protected from unauthorized modification by authorized users (which raises the question -- what is unauthorized modification; for example for logs this is deletion or altering of records, while adding records is permitted)
3. The data are internally and externally consistent. Again thing about integrity of logs as an example.

The model specifies three integrity axioms:

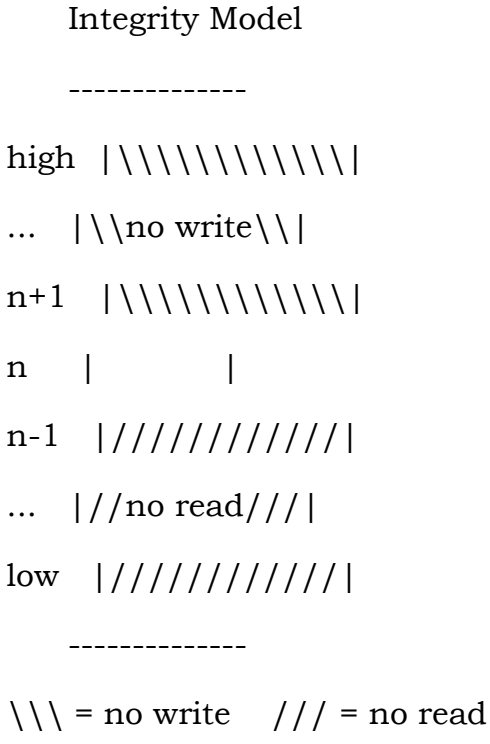
- **simple integrity axiom**
  - ***"no read down"***. What (I think) the model is saying is that since the criteria for the lower clearance level is less restrictive than your clearance level you cannot trust the data from the lower level.
  - ***"no write up"*** you can't introduce the data for lower security level to any document that you create at your level (and thus propagating possibly insecure or inaccurate information).
- A subject at one level of integrity cannot invoke a subject at higher level of integrity.

The main focus of the **Biba Model** is preserving integrity and is also governed by two axioms:

Fred Cohen & Associates

The Biba integrity model [Biba77] was published at Mitre one year after the B-L model. When Biba noticed that the B-L policy did not provide protection against a user at level X writing information at level Y when X was a lower security level than Y. Thus a low security user could overwrite highly classified documents unless some sort of integrity policy were in place.

Biba chose the mathematical dual of the B-L policy wherein there are a set of integrity levels, a relation between them, and two rules which, if properly implemented, have been mathematically proven to prevent information at any given integrity level from flowing to a higher integrity level. Typical integrity levels are "untrusted", "slightly trusted", "trusted", "very trusted", "so trusted that we don't need a higher level of



The Biba integrity model is the mathematical dual of the Bell-LaPadula model for sensitivity:

Every subject(process) and object(e.g. file) of the system is assigned an integrity label which consists of a hierarchical component and a non-hierarchical, set based component.

In Trusted IRIX/B the hierarchical component is referred to as the grade, and the non-hierarchical, set based component as the division set.

New objects are created with the same integrity label as the process which created them. Thus, a process can never give data a higher integrity than it had before.

A process can downgrade the integrity of data by reading data with a higher integrity than the process and writing it to a new file, which gets the integrity of the process.

EXAMPLES OF BEHAVIORS THAT LACK INTEGRITY

Examples of behaviors that lack integrity include, but are not limited to:

- Giving, taking, or receiving unauthorized information to/from another person during any type of assignment or test.
- Obtaining or providing without authorization questions or answers prior to the time of an assignment or test.
- Using unauthorized sources for answers during any assignment or test.
- Taking part in or arranging for another person to complete an assignment or to take a test in place of another.
- Giving or receiving answers by use of signals or electronic communication during a test.
- Altering answers on a scored test and submitting it for a higher grade.
- Collaborating with others in a required assignment without the approval of the instructor.
- Stealing class assignments or portions of assignments, including electronic files, and submitting them as one's own.

The Chinese Wall Model:

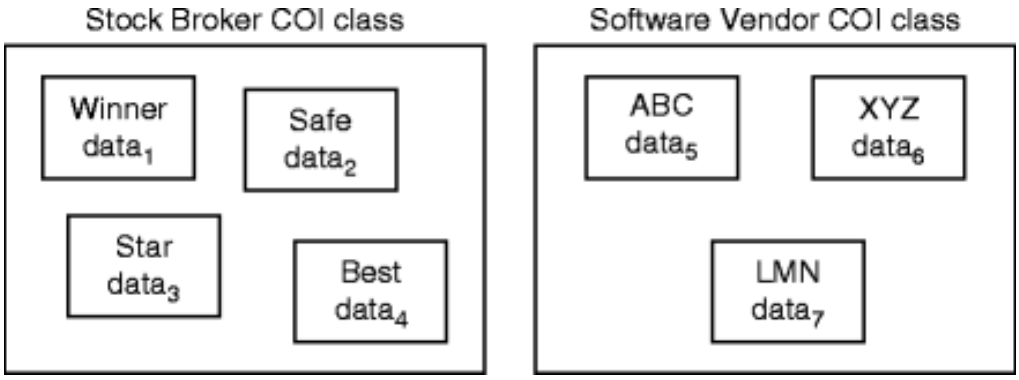
Definition:

The Chinese Wall model is a security model that concentrates on confidentiality and finds itself application in the commercial world. The model bases itself on the principles defined in the Clark Wilson security model.

Background:

The Chinese Wall model was introduced by Brewer and Nash in 1989. The model was built on the UK stock brokerage operations. The stock brokers can be consulted by different companies that are in competition. This causes a conflict of interest, which should be prevented with lawfully enforceable policies. Similar to the UK brokerage system, the Chinese Wall model assumes

impenetrable Chinese Walls among company data sets, so that no conflict of interest occurs on the same side of the wall. According to the model, subjects are only granted access to data that is not in conflict with other data they possess.



The Chinese Wall Security Policy:

The 1989 Brewer and Nash published paper titled "The Chinese Wall Security Policy" is an authoritative voice in the information security realm. It is essentially an access control policy that addresses a very specific security issue: *conflict of interest*.
It aims to protect the confidentiality and, through extension, the integrity of a set of data, by mandating rules around its access and availability.
Data sets in the Brewer-Nash abstraction model could be any one of the following three types-

- **Objects –** This is the same as the objects of the Bell-LaPadula model and is essentially the ungrouped basic units of information
- **Company Dataset –** This is the collection of all objects belonging to a single organization or company
- **Conflict of Interest Class –** This is a collection of companies that are in competition with each other

The security policy builds on three levels of abstraction. Objects such as files. Objects contain information about only one company.

Chinese Wall properties:

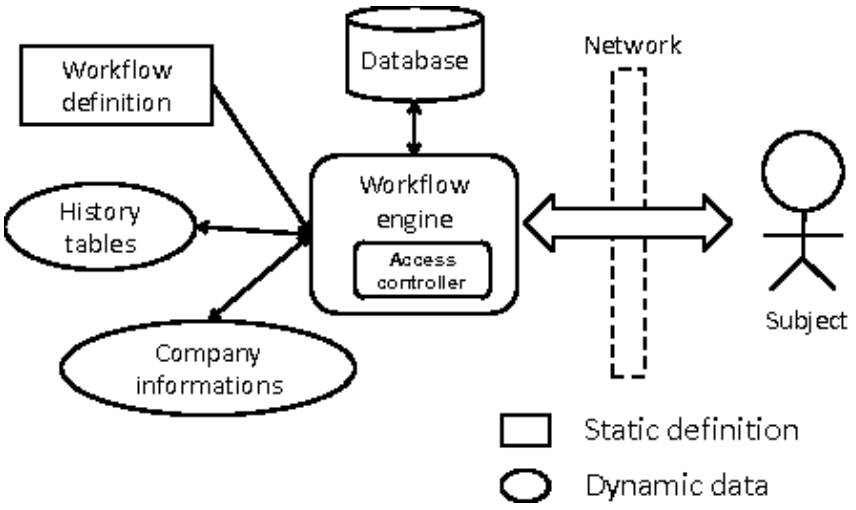
Formally, the policy restricts access according to the following two properties:

- (Chinese Wall) Simple Security Rule: A subject s can be granted access to an object o only if the object:
  - is in the same company datasets as the objects already accessed by s, that is, "within the Wall,"or
  - belongs to an entirely different conflict of interest class.

- (Chinese Wall) *-property: Write access is only permitted if:
  - access is permitted by the simple security rule, and
  - no object can be read which is:
    - in a different company dataset than the one for which write access is requested, and
    - contains unsanitized information.
    - Unlike previous policies, Brewer and Nash's Chinese Wall Policy is designed to address a very specific concern: conflicts of interest by a consultant or contractor.
    - This illustrates that security policies can be crafted to solve very specialized problems.
    - The Chinese Wall is an access control policy in which accesses are sensitive to the history of past accesses.

Implementing the Chinese Wall Security Model in Workflow Management Systems:

The Chinese wall security model (CWSM) was designed to provide access controls that mitigate conflict of interest in commercial organizations, and is especially important for large-scale interenterprise workflow applications. This paper describes how to implement the CWSM in a WfMS. We first demonstrate situations in which the role-based access control model is not sufficient for this, and we then propose a security policy language to solve this problem, also providing support for the intrinsic dynamic access control mechanism defined in the CWSM (i.e., the dynamic binding of subjects and elements in the company data set). This language can also specify several requirements of the dynamic security policy that arise when applying the CWSM in WfMSs. Finally we discuss how to implement a run-time system to implement CWSM policies specified by this language in a WfMS.



Example of chinese Model:

For example, consider the following conflict classes:

Company groups collect all objects concerning a particular company.

Conflict classes cluster the groups of objects for competing companies.

{ Ford, Chrysler, GM } { Bank of America, Wells Fargo, Citicorp } { Microsoft }

We have a simple access control policy: A subject may access information from any company as long as that subject has never accessed information from a different company in the same conflict class.
For example, if you access a file from GM, you subsequently will be blocked from accessing any files from Ford or Chrysler. You are free to access files from companies in any other conflict class. Notice that permissions change dynamically. The access rights that any subject enjoys depends on the history of past accesses.

UNIT-2:-

People Management:

People management refers to the practice of recruiting, training, engaging, and retaining people to optimize their talent and maximize their productivity. A subcategory of Human Resource Management (HRM), people management includes:

- Training and development
- Recruitment
- Compensation and benefits
- Performance management
- Organization
- Engagement and retention
- Safety and wellness

People management strategies address people's needs, unique talents, and career objectives while supporting their alignment with company goals and values.

Why should HR leaders care about people management?

HR leaders and managers must have people management skills to communicate, inspire, and direct talent effectively. Successful people management practices help motivate people to work productively and passionately, leading to increased engagement and retention.

Tips and best practices for effective people management:

Effective people management demands that HR leaders embody several essential work habits. Here are five core practices HR leaders can incorporate to promote successful people management:

Lead by example: By demonstrating a high level of emotional intelligence, HR leaders can set the tone for a productive and dynamic work environment. Exemplifying essential characteristics such as empathy and resilience at work shows people how they should aim to behave in the workplace.

Gauge team members' personalities: Knowing and understanding each person's unique personality and motivations enables managers to connect with people on a personal level and strategically maximize their work potential. HR coach Katherine Giacalone emphasizes the importance of identifying and mentally categorizing each person's personality for effective management.

Communicate respectfully: Clear and considerate communication is the foundation of any type of successful relationship. Encouraging people and managers to practice active listening builds trust and healthy interpersonal connections, which promote a positive culture and foster productivity. Furthermore, active listening can help managers acquire valuable, constructive feedback to improve the employee experience.

Conflict resolution: Approaching conflict with respect for the individuals involved allows managers to resolve challenging situations with integrity. Instead of passively letting a conflict spiral out of control, managers can empathetically approach people, ultimately strengthening interpersonal relationships and elevating the work community.

Offer development opportunities for managers: HR leaders can help managers develop their skills by providing development training. They can also team up with finance team leaders to introduce budgets that enable managers to take certification and knowledge courses. HR leaders can also offer mentorship programs that provide a framework for managers to learn one-on-one with internal or external management coaches.

People Management Skills:

To excel in people management, HR leaders must cultivate the following abilities:

1.Empathy: If there is a number one must-have skill for people management, it's empathy. The ability to put yourself in others' shoes and feel what they are feeling will make talent feel more heard and recognized. It will also improve HR decision-making and communication, helping create a better employee experience.

2.Leadership: Successfully managing others requires a range of abilities that can be bundled together under the umbrella of leadership skills, including trust-building, motivating, conflict resolution, and empowerment.

3.Organization and analytical thinking: While much of people management requires applying soft skills, the modern organization requires HR professionals to employ an equal measure of analysis and data savviness. HR technology has become a crucial part of people management. Tech literacy and data analysis are now essential competencies for modern HR professionals.

4. Communication: Communication is key to succeeding in many roles, and people management is no different. Successful people managers can communicate clearly with their coworkers in various circumstances. They balance candor with politeness to get their message across to many people.

5. Active listening: It's essential to listen to employees and coworkers. When active listening, people managers listen to the whole person. Before responding, they note what the other person says verbally, along with any physical cues that might otherwise go unnoticed.

6. Creativity: Every person is slightly different: Each employee has different needs and drivers. Discovering these differences is one thing, and acting upon this information is quite another. It takes creative thinking to solve people problems. So having out-of-the-box problem-solving strategies can be an asset in people management.

Human Resource Security:

Human Resources Security is a set of processes designed to ensure that all employees, suppliers, and contractors are qualified for and understand their engagement/job tasks and responsibilities, and that access is revoked after the engagement is finished.

The Human Resource Security discipline is designed to examine key controls applied before, during, and after the hiring of human resources. These controls include but are not limited to the definitions of roles and responsibilities, recruitment, contracting terms and conditions, awareness, education and training, disciplinary processes, and termination.

METRICS:

Human resource professionals must establish meaningful safety and security metrics to determine how safety and security programs and practices contribute to the business. Relevant metrics may include the following:

- Injury and illness rates.
- Workers' compensation costs per employee.
- Workers' compensation incidence rates.
- Workers' compensation severity rate.
- Safety and security team initiatives completion rate.
- At-risk behavior reduction.
- Observation of safety behavior.
- Compliance trainings.
- Near-miss responses.
- Safety and security committee activities.
- Six sigma.
- Trend analysis.

Continuous improvement in the workplace safety and security function can be achieved only when safety and security systems are measured and connected to established goals. Metrics can demonstrate that security risk reduction, accident prevention and associated investments are having a positive impact on the business. *See* Developing Effective Safety Management Programs.

Guide to ISO 27001 Human Resource Security:

HR departments process vast amounts of sensitive information, so organisations must take appropriate steps to secure that data.

Annex A.7 of **ISO 27001** sets out the framework for organisations to do that. ISO 27001 is the international standard that describes best practice for implementing an ISMS (information security management system), and Annex A.7 addresses human resource security specifically.

It's broken down into three sections:

- **Annex A.7.1**, which covers activities before employment.
- **Annex A.7.2**, which contains guidelines to ensure that employees and contractors fulfil their information security responsibilities.
- **Annex A.7.3**, which covers the termination and change of employment.

This blog explains each clause within Annex A.7, helping you understand human resource security and ISO 27001.

A.7.1.1 Screening:

Employee screening is the process of verifying an applicant's credentials and ensuring that they meet the conditions for employment.

The screening process should, for example, establish whether the applicant has concealed or falsified information, such as their qualifications and job history.

Annex A.7.1.1 advises organisations to adjust the stringency of employee screening based on the role that they are applying for.

Applicants whose jobs involve accessing sensitive information should be subject to more extensive screening.

Organisations must document the screening process to demonstrate which procedures are carried out.

A.7.1.2 Terms and conditions of employment:

An employment contract must include a section related to the information security responsibilities of the organisation and the employee.

This is a compliance requirement of ISO 27001 and the GDPR (General Data Protection Regulation).

A.7.2.1 Management responsibilities:

Managers should ensure that employees who report to them understand information security threats and that appropriate controls are in place to mitigate risks.

Managers must also ensure that employees complete regular information security staff awareness training. This is addressed further in Annex A.7.2.2.

A.7.2.2 Information security awareness, education and training:

Employees and relevant contractors must receive information security staff awareness training.

These training courses should be retaken at regular intervals to refresh employees' knowledge and account for changes in how the organisation operates.

A.7.2.3 Disciplinary process:

Organisations must create and document a disciplinary process for when an employee violates their employment contract.

Annex A.7.2.3 focuses on action related to information security breaches, but there doesn't need to be a separate process. Organisations can use the same framework for information security breaches as they would for disciplinary actions related to other violations.

A.7.3.1 Termination or change of employment responsibilities:

The final clause of Annex A.7 addresses what happens when an employee leaves their job. This includes staff who have left voluntarily, been fired or changed roles.

Annex A.7.3.1 recognises that some information security responsibilities are applicable after the employee has left the role.

For example, they are still expected to protect confidential information, and they are prohibited from keeping sensitive information belonging to the employer.

Organisations must define the responsibilities that come with the termination of or change in employment, communicate them to the employee and make sure they are enforced.

Additionally, there are steps that employees must take when they leave their role, such as returning company equipment and keys, fobs, passes, etc. to the premises.

Annex A.7.3.1 also specifies what organisations must do if an employee moves to another position within the same company.

For example, if an employee moves to a different department, the organisation must ensure that they no longer have access to information assets that aren't required for their new role.

Security Awareness:

The Definition of Security Awareness:

Security awareness has long been a goal of organizations that strive to provide a safe and secure environment for their employees, customers, and those who want to defend precious assets.

Security awareness is a formal process for training and educating employees about IT protection. It involves:

- Programs to educate employees
- Individual responsibility for company security policies
- Measures to audit these efforts

Obviously, the first bullet point is the main component of a security awareness program, but it's just as important that employees are held accountable and steps are taken to gauge the effectiveness of an organization's security measures.

Security awareness can be broken down into four stages:

- Determining the current status
- Developing and crafting a security awareness program
- Deploying said program to employees
- Measuring the progress made by the program and revising as necessary

Before we begin describing the various types of security awareness, let's take a look at the history that has brought us to this current point.

A Brief History of Security Awareness:

The history of cyber security goes back almost as far as the Internet itself. Indeed, from the very beginning of the World Wide Web becoming a mainstream resource, criminals have been using it to their advantage.

The government was quick to respond to this new threat. Laws like the Computer Fraud and Abuse Act were passed in order to prevent and punish attempts by these malicious parties. The Computer Emergency Response Team was also formed in an effort to investigate the growing number of hacks and potential methods of protection.

This and subsequent attacks are of interest because they were the impetus for much of what we think of as cyber security today. CERTs (computer emergency response teams) were created as a result. With this attack, companies began realizing how vulnerable they truly were. An adage we now hear all the time in the cyber security community, "Prevention is better than a cure," was coined around this time.

The Rise of Modern Hacking:

It was really in the early to late 2000s that hacking evolved into the widespread problem that we know today. Again, much of this goes back to the proportional increase in targets (e.g., more and more people using the Internet).

At the same time, hacking was becoming much simpler. Gone were the days when the only people who were able to execute these attacks had technical skills equal to or better than the foremost programmers in the world.

There was also a proliferation of information about how to hack. Someone who had never even attempted a cyber attack could become a real threat in under a month.

Modern-Day Security Awareness:

As you're probably well aware, cyber attacks have not slowed down. In 2013, the breach of Target's security measures was another shocking reminder to the world of just how vulnerable even the largest corporations were. Some 40 million customers spent the days following Thanksgiving checking their accounts to see if they had money stolen.

The other reason the Target attack is being brought up here is because the level of sophistication used is another milestone in the history of cyber security. As opposed to the direct attack on TJX, the criminals who succeeded with Target knew the importance of a direct approach.
The hackers also realized there was a precise moment when they'd have to strike. Credit card numbers were present and unencrypted in the memory of the system for just a short time.

Types of Security Awareness:

With the above in mind, it should be very clear that companies must take security awareness seriously. There is, of course, a place for digital security and the professionals who are able to install and run it.

However, more and more, hackers are succeeding because of phishing attacks and similar versions that rely on companies' employees to open the door for them.

The Top-down Approach: One very important feature of security awareness is that it can't simply be the duty of the employees to learn the measures they need to take and apply them. That's important and we'll cover that in more detail in a moment, but it should be obvious that a top-down approach is required.

Again, the Target attack made this abundantly clear when the company's CEO actually fell on his sword as a result of the breach.

For one thing, anyone from a manager up to an executive is going to be an easy target if they are not aware of the potential for attacks and how they can be successful.

This knowledge, though, must also carry over to ensuring that each and every employee is also aware and also capable of keeping the company safe.

Budgeting for Security Awareness: One good indication of whether or not a company is taking security awareness seriously can be found in their budget. How are they treating security awareness as a priority? How does it measure up to other ways funds are allocated?

If your company's idea of security awareness consists of an email every now and then to remind people of the possibility of an attack, you have to expect that you'll soon be a victim.

To be clear, security awareness is just one piece of a viable protection plan. Other pieces would include:

- Creating a security policy
- Assessing your company's vulnerabilities

- Investing in security technology

However, nothing is more important than security awareness. Companies should be spending as much on this investment as they do on the software and other forms of security tech. None of that will be remotely helpful if your people are easy targets for phishing attacks.

An Organizational Structure Dedicated to Security Awareness: This type of security awareness is vital because it affects everyone in the company. Much like the top-down approach, having an organizational structure built around security will make everyone's job simpler.

If at all possible, you should have a team of people who are responsible for implementing your security awareness program. At the very least, an individual at your organization must take this job.

Create a Plan and Related Documentation: The plan for every company is going to be a little different, but this is an important type of security awareness that deserves some attention here. Features of your plan should include some version of the following:

- Outlining the security awareness team and the roles involved
- A mission statement of the security awareness program that explains its necessity
- A calendar of activities for the entire year that involves regular activities – not just reminder emails – designed to make sure employees understand common threats and what their role is for preventing them
- Programs for new employees that explain the security awareness program and their roles
- References to company security procedures and policies

Using Different Forms of Media to Reinforce the Message: We've touched on reminder emails about security awareness a couple of times. That's not to say that emails are a bad thing. They're perfectly fine and everyone needs reminder from time to time.

That being said, you should use multiple forms of media to make sure your company's messages about security awareness never go ignored.

For example, your calendar of events should involve a security expert at your company getting up in front of people and explaining important topics. Videos can be sent out over email, as well. Tests can be used. Physical reminders around the office may work. The list goes on and on, but the point is not to become complacent about how you deliver the messages about security awareness.

Highlight Recent Attacks in the News: This is an extremely important form of security awareness. However, make sure you're highlighting all kinds of attacks, not just the ones that make national news. The goal with this approach is to show your employees how prevalent these attacks are, how easily one could succeed with your company, and what the fallout entails.

For this reason, don't simply highlight the stories that make national news. It's all too easy for an employee to think, "Yeah, but we're not Target. No one would bother with us."

Find the stories about companies your size and/or in your industry. Sadly, it doesn't look like there is going to be any lack of these incidents going forward.

Seek the Services of a Professional: If you have absolutely no security awareness measures in place at the moment, it's worth thinking about taking on the services of a professional. They'll help you get up and running and make sure you quickly make up for lost time.

Even if you have invested in a security awareness policy and other measures, it's still not a bad idea to bring on an independent consultant from time to time to see if there are areas where you can improve.

Security education:

Security education refers to the process of teaching individuals and organizations about various aspects of security, both physical and digital. It covers a wide range of topics, from cybersecurity to physical security measures, and aims to raise awareness about potential threats and vulnerabilities. In today's increasingly connected world, security education is crucial for protecting sensitive information, maintaining privacy, and ensuring the safety of people and assets.

Importance of Security Education:

Understanding Cybersecurity:

Cybersecurity is a major concern for individuals, businesses, and governments alike. Cyber attacks can lead to significant financial loss, reputational damage, and even physical harm. Security education helps individuals understand the risks associated with using digital technologies and how to mitigate them. By learning about common threats, such as malware, phishing, and ransomware, people can better protect their digital assets and prevent unauthorized access to sensitive information.

Physical Security

Physical security is equally important, as it focuses on protecting people, property, and assets from harm. This can include measures such as surveillance systems, access control, and alarm systems. Security education teaches individuals how to identify potential risks, implement appropriate security measures, and respond effectively to incidents.

Components of Security Education:

Training

Training is a critical component of security education. It involves teaching employees and individuals about security best practices, policies, and procedures. Training sessions can be conducted in-person, online, or through a combination of both methods. Topics covered in security training may include password management, securing devices, and recognizing phishing attempts.

Awareness Programs

Security awareness programs aim to create a culture of security within an organization or community. They are designed to keep security issues at the forefront of people's minds and encourage them to stay vigilant. Awareness programs may include regular communication about security updates, posters and signage, or events such as cybersecurity awareness month.

Simulated Exercises

Simulated exercises, such as mock phishing campaigns or incident response drills, can be an effective way to test and improve security awareness. These exercises help individuals and organizations identify areas of weakness and refine their security practices.

Implementing Security Education:

Identifying the Target Audience

Before implementing a security education program, it is essential to identify the target audience. This can include employees, customers, or other stakeholders who need to be aware of security best practices. Identifying the target audience will help tailor the content and delivery method for maximum effectiveness.

Creating a Security Education Plan

A well-structured security education plan should outline the objectives, content, and delivery methods for the program. The plan should also include a timeline for implementation and any necessary resources, such as trainers, materials, and budget.

Evaluating and Improving Security Education

Regular evaluation of security education programs is essential for ensuring their effectiveness. This can be done through surveys, feedback sessions, or by measuring key performance indicators such as the number of security incidents or changes in employee behavior. Based on the evaluation, improvements can be made to the program to ensure it remains relevant and effective.

Cloud Security

Cloud computing allows users to store and access data and applications over the internet, rather than on local hardware. Should address the unique challenges and risks associated with cloud computing, such as data breaches, loss of data control, and insider threats. Best practices for securing cloud environments, selecting cloud providers, and ensuring data privacy should also be covered.

Network Security

Network security involves protecting computer networks and the data they transmit from unauthorized access, misuse, or destruction. hould cover topics such as network segmentation, firewall configuration, and intrusion detection and prevention systems.

Mobile Device Security

As smartphones and tablets become increasingly common, it is essential to address mobile device security. Should teach individuals how to protect their devices from theft, unauthorized access, and malware. This may include guidance on securing app downloads, enabling device encryption, and setting up remote wipe capabilities.

Internet of Things (IoT) Security

The Internet of Things (IoT) refers to the network of interconnected devices that communicate and share data with each other. As IoT devices become more prevalent in homes and workplaces, security education should cover IoT-related risks and best practices for securing these devices

Information Management:

Information management is the collection, storage, management and maintenance of data and other types of information. It involves the gathering, dissemination, archiving and destruction of information in all its forms. Information management covers the procedures and guidelines organizations adopt to manage and communicate information among different individuals, departments and stakeholders.

Information management focuses on the level of control an organization has over the information it produces. It requires building dedicated information management systems designed to help the company use its resources to support business processes.

Information management also deals with how the organization shares and delivers information to diverse recipients. This includes the format, such as digital and physical information, and the medium, including computers, servers, websites, social media, mobile devices and applications.

Information management and its role in the workplace:

Information management allows an organization to achieve various goals. It improves compliance, reduces risk and controls access to vital business information. Here's why information management is important in the workplace:

1. Controls creation of records

An effective information management system can help an organization control the creation and growth of records. Without a defined strategy for creating and recording information, the workplace can produce excessive paper and paperless records.

This can increase time for retrieving records and increase costs of managing information resources. To prevent this, information management protocols set limits to creating and destruction of information to improve productivity and efficiency.

2. Ensures regulatory compliance

Many organizations have to work within regulations regarding how they handle client and business data. An effective information management system

provides guidelines that enforce compliance with laws and regulations, allowing the company to avoid legal and financial penalties that could result from accidental breaches.

3. Reduces operating costs

Workplaces need an efficient information management system to reduce the cost of record keeping. Data collection, analysis, information storage, sharing and destruction are capital-intensive activities, especially for large organizations. Information management prioritizes the most important records, reducing expenses throughout the information life cycle.

4. Adopts new technologies

Information management provides the capability to adopt newer and more efficient technologies for managing information. It can be automation, enterprise solutions, artificial intelligence or any technological product or service that will help the company derive more benefits from its information.

5. Improves productivity and efficiency

A great information management system can improve how employees store and retrieve information required during their daily activities. It can also make it easier to disseminate information to diverse recipients via multiple channels, allowing teams to collaborate and communicate easily across time zones and locations. An effective information management system can help the organization extract actionable insights from its records to guide decision-making.

6. Reduces risks

An important function of information management is to reduce the risk of legal and financial punishments against the organization. It achieves this with a well-defined protocol for recording, storing, disseminating and destroying data. This reduces the chance of breaches and improves compliance with regulations.

7. Protects proprietary information and preserves corporate memory

Organizations need a process to safeguard their vital information from competitors and unauthorized access. Information management provides a system for protecting proprietary information from intruders, system failures and natural disasters. It helps protect the confidentiality and integrity of vital

information assets, allowing the owner to derive maximum benefits from their trade secrets.

Information management also helps an organization create a reliable institutional memory it can use for planning and making important strategic decisions.

How to create an information management system:

Use these eight steps to create an information management system:

1. Identify information requirements

The first step when creating an information management system is to identify information requirements. This can be in the form of an internal study or company-wide survey to determine the scope of the system in relation to the business, its operations, stakeholders and regulatory requirements. A simple way to achieve this step is to ask employees and management the amount and type of information they need to perform their duties.

2. Outline objectives

For the system to be successful, the organization needs to define its objectives in the form of guidelines or protocols that will guide implementation. Consider the overall management principles that will serve as a user manual when the system becomes operational.

3. Determine information sources

Organizations can collect information from diverse sources, including employees, internal departments, competitor research, market intelligence and regulatory agencies. The objectives of the system often determine the sources of information.

4. Determine collection and classification methods

Once you have determined the sources of information, the next step is to identify methods of collecting and classifying the information. This involves outlining the amount of information collection and the frequency, location and time. For classification, determine which information is quantitative, qualitative, technical, demographic, financial, legal and other categories. This step also involves the storage of current information and archiving when it becomes obsolete.

5. Determine dissemination method

Next, you'll identify the information recipients, the format and the channels of distribution. You'll also decide when to provide data access and other control measures to prevent breaches.

6. Perform a cost-benefit analysis

The cost of an information management system will include expenses for setting up the infrastructure, training staff, daily operations and maintenance. An effective information management system will deliver benefits that outweigh the costs.

7. Implement and evaluate

If the cost-benefit analysis is positive, you'll begin setting up the system and providing training and operational guidelines. You want employees who use the system to improve their productivity and efficiency at work.

You should assess the performance of the system after some months to determine how it's met objectives, including ensuring that the benefits continue to outweigh costs. Shorter periods for recording and retrieving information and increased use of data for decision-making are also signs the system is working.

If there are lapses in the company's information management strategy, an evaluation can help identify ways to improve the system for more effectiveness.

8. Maintain and improve

An evaluation will show how to improve the system's effectiveness and also provides an opportunity to upgrade infrastructure and retrain staff. Continuous improvements can contribute positively to the company's ability to achieve short- and long-term goals.

Information Classification:

Information classification is a process used in information security to categorize data based on its level of sensitivity and importance. The purpose of classification is to protect sensitive information by implementing appropriate security controls based on the level of risk associated with that information.

There are several different classification schemes that organizations can use, but they generally include a few common levels of classification, such as:

- **Public:** Information that is not sensitive and can be shared freely with anyone.
- **Internal:** Information that is sensitive but not critical, and should only be shared within the organization.
- **Confidential:** Information that is sensitive and requires protection, and should only be shared with authorized individuals or groups.
- **Secret:** Information that is extremely sensitive and requires the highest level of protection, and should only be shared with a select group of authorized individuals.
- **Top Secret:** Information that if disclosed would cause exceptionally grave damage to the national security and access to this information is restricted to a very small number of authorized individuals with a need-to-know.
- Information classification also includes a process of labeling the information with the appropriate classification level and implementing access controls to ensure that only authorized individuals can access the information. This is done through the use of security technologies such as firewalls, intrusion detection systems, and encryption.

Information classification is a crucial aspect of information security as it helps to ensure that sensitive information is protected and only accessible by authorized individuals, which can help organizations to protect their sensitive information, maintain compliance with relevant regulations, and keep their data and systems safe from cyber threats.

The initial step of data characterization is doling out worth to every data resource, contingent upon the gamble of misfortune or damage in the event that the data gets uncovered. In view of significant worth, data is arranged as:

1. **Confidential Data –** data that is safeguarded as secret by all substances included or affected by the data. The most elevated level of safety efforts ought to be applied to such information.
2. **Classified Data –** data that has limited admittance according to regulation or guideline.
3. **Restricted Data –** data that is accessible to the vast majority of representatives.
4. **Internal Data –** data that is available by all workers
5. **Public Data** – data that everybody inside and outside the association can get to

Most companies follow the following steps to make things easier:

The first step of information classification is assigning value to each information asset, depending on the risk of loss or harm if the information gets disclosed. Based on value, information is sorted as:

- **Confidential Information –** information that is protected as confidential by all entities included or impacted by the information. The highest level of security measures should be applied to such data.
- **Classified Information – i**nformation that has restricted access as per law or regulation.
- **Restricted Information –** information that is available to most but not all employees.
- **Internal Information –** information that is accessible by all employees
- **Public Information –** information that everyone within and outside the organization can accessorization of information on the basis of different organizations and different parameters. Information in an organization should be categorized and must be kept confidential and that's why information security comes into the picture, and it plays a vital role for any organization.

The main reason for classifying information is that not all data/information has the same level of importance or the same level of relevance/critical to an organization. Some data are more valuable to people who make strategic decisions (senior management) because they aid them in making long-run or short-range business direction decisions.

Thus, it is obvious that information is used to prevent unauthorized disclosure and the resultant failure of confidentiality.

Schemes for Information Classifications as follows.

1. **Government Organization**
2. **Private Organizations**

Levels in Government organization for Information Classification :

1. **Unclassified –** Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.
2. **Sensitive but Unclassified –** Information that has been designed as a major secret but may not create serious damage if disclosed.
3. **Confidential –** The unauthorized disclosure of confidential information could cause some damage to the country's national security
4. **Secret –** The unauthorized disclosure of this information could cause serious damage to the countries national security.
5. **Top Secret –** It is the highest level of information classification. Any unauthorized disclosure of top-secret information will cause grave damage to the country's national security.

Levels in Private Organizations for Information Classification :

1. **Public –** Information that is similar to unclassified information. However, if it is disclosed, it is not expected to seriously impact the company.

2. **Sensitive –** Information that required a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from loss of integrity owing to an unauthorized alteration.
3. **Private –** Typically, this is the information i.e. considered of a personal nature and is intended for company use only, its disclosure could adversely affect the company or its employee salary levels and medical information could be considered as examples of "private information".

Criteria for Information Classification :

1. **Value –** It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization it needs to be classified.
2. **Age –** The classification of the information may be lowered if the information value decreases over time.
3. **Useful Life –** Information will be more useful if it will be available to make the changes as per requirements than, it will be more useful.
4. **Personal association –** If the information is personally associated with a specific individual or is addressed by a privacy law then it may need to be classified.

Advantahes and Disadvantages :

Advantages of information classification in information security include:

- Improved security: By classifying information based on its level of sensitivity, organizations can ensure that the appropriate security controls are in place to protect that information.
- Compliance: Information classification can help organizations to meet compliance requirements, by ensuring that sensitive information is protected in accordance with relevant regulations.
- Risk management: By identifying and classifying sensitive information, organizations can better manage the risks associated with that information.
- Better resource management: By classifying information, organizations can ensure that their resources are used efficiently, by focusing on protecting the most sensitive information first.
- Increased efficiency: By implementing information classification, organizations can ensure that their information security processes are streamlined and efficient.

Disadvantages of information classification in information security include:

- Cost: Implementing information classification can be costly, as it may require additional resources, such as security experts, to manage the process.
- Time-consuming: The classification process can be time-consuming, especially for organizations that have a large amount of data to classify.

- Complexity: The classification process can be complex, especially for organizations that have not previously used this framework.
- Inflexibility: The classification process is a structured process, which can make it difficult for organizations to respond quickly to changing security needs.
- Limited Adaptability: The classification process is predefined, which is not adaptable to new technologies, it may require updating or revising to accommodate new technology.

Information Handling:

It is important that individuals receiving care, education and support have the right to confidentiality. Each organisation that handles information should have a code of practice outlining the steps to be taken in order to ensure that confidential information is handled appropriately. The code will help organisations to ensure that there are rules to be followed in relation to handling information.

Handling information To handle information it is necessary to:

● decide what information is required for decision making and management purposes;

● identify the relevant data that is readily available and where and how it can be obtained;

● identify where any data at present unavailable can be obtained and decide whether the value of the data justifies the effort and cost of getting it;

● take steps to convert the raw data that has been made available into information which has 'meaning and purpose' in accordance with specified requirements;

● establish how best to record, analyse and present the information in ways which ensure that it serves a useful purpose. These actions inform the development of a computerized system for providing information as well as carrying out various administrative tasks as described below. They also provide guidance on the statistical methods which can be used to analyse and present the information.

Tips for Handling Confidential Information:

When handling confidential information in your business, whether it's relating to your customers or employees, you have a duty to take the necessary steps to protect it. Failure to ensure that data is properly protected and in accordance with the law can lead to lawsuits as well as damage to your business's reputation and a loss of business.

Below are some of the best ways to better protect the confidential information that your business handles.

1. Control access:

For any information that's stored digitally it's incredibly important that you control access to it by using passwords, firewalls and encryption. This is especially important when the information is contained on smaller storage devices such as USB drives that are easily misplaced.

When using passwords to control access to confidential information, you must ensure that they're both secure and changed regularly. Using easy-to-guess passwords is a mistake that many businesses make and something that you should avoid doing if you want to keep your confidential information secure. The best type of passwords to use are a combination of upper and lower case letters and as well as special characters.

2. Use confidential waste bins and shredders

As prominent as digital data has become, most businesses still deal with a lot of paperwork on a day-to-day basis. If you need to dispose of sensitive documents, then be sure to shred them or use a confidential waste bin. Issues such as identity theft mean that you should never assume that because a document has been put in the bin, it will not be viewed by anyone else.

3. Lockable document storage cabinets

If you need to permanently destroy confidential documents, then a shredder works well but what about documents you need to keep on hand? In this case the best option is to have lockable storage cabinets that only a few select people have the key for.

To provide an added level of protection, it's also a good idea to keep any lockable storage cabinets in a locked room that cannot be accessed by everyone.

4. Secure delivery of confidential documents

Storing confidential documents safely on your own premises is one thing but if they need to be delivered then it's extremely important that this is done in a secure manner. If it's physical documents that need to be delivered, then it's a good idea to use a trusted courier service or ideally have them delivered by someone you trust within your organisation.

For digital documents that need to be sent to a third party, you can either email or use a file sharing program. If you use a file sharing program, then it's very important to encrypt the documents and make sure you use a trusted service provider.

5. Employee training

When it comes to confidential data being leaked, often it's a company's own employees who are the biggest risk. This isn't necessarily due to malicious reasons either; often it's simply because the right training was not provided.

When training your employees about protecting confidential information, it's a good idea to start first with explaining why data confidentiality is so important and then provide training about the practical aspects of data protection i.e. using secure passwords, destroying of documents etc.

Information Handling Policy:

1. Purpose

The purpose of this policy is to seek to ensure staff and students understand how information in their possession should be protected, and how information should be shared with other parties. UWE Bristol generates and holds a wide variety of information that must be protected against unauthorized access, disclosure, modification, or other misuse.

This document forms part of the Information Security Policy Toolkit, and underpins the overarching Information Security Policy. Adherence to this policy will provide everyone with guidance to help ensure that correct information classification and handling methods are applied to their day-to-day activities and managed accordingly.

2. Scope

This policy applies to all information assets generated or processed by UWE Bristol, including those created prior to the publishing of this policy. This includes electronic information as well as information on paper and information shared orally or visually (such as telephone and video conferencing). Where UWE Bristol holds information on behalf of another

organisation with its own classification system, agreement shall be reached as to which handling policy shall apply.

3. Responsibility

It is the responsibility of UWE Bristol to ensure that adequate data storage and processing facilities are available to enable compliance with the Information Handling Policy. Individuals have a personal responsibility to ensure the correct management and protection of information, and may be personally liable for any breaches in information security that arise from a failure to take appropriate measures to do so.

4. Consequences of Policy Violation

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply may lead to the immediate cancellation of a contract. Where appropriate, breaches of the law will be reported to the authorities. Sensitive personal data ("special categories" under GDPR) includes disability status, ethnicity, medical information (both physical and mental) and details of criminal convictions, and may require heightened security measures such as encryption and stricter access controls.

5. Information Classification

All information generated or processed by UWE Bristol is subject to classification. This is to assist information owners in determining the different levels of security required. The following classifications are used by UWE Bristol:

Public- Information that is available to any member of the public without restriction. This however should not be automatically placed into the public domain without a specific reason, unless the information was originally intended for public disclosure

Restricted- Non-confidential information where dissemination is restricted to specific groups or individuals for policy, operational or contractual reasons, for example: some committee minutes; procurement documents; or internal reports. Typically, if this level of information was leaked outside of the University, it could be viewed as inappropriate or ill-timed

Confidential- Information which requires additional protection because it is sensitive personal data, commercial or legal information, under embargo prior to wider release, or which could not be disclosed under Freedom of Information legislation

Privacy:

Privacy can be defined as an individual or a group's ability to cloister the data about them and then reveal it selectively.

It means that privacy is applied to sensitive or crucial information. The privacy domain overlaps moderately with security that can add the concepts of proper use and protection of data.

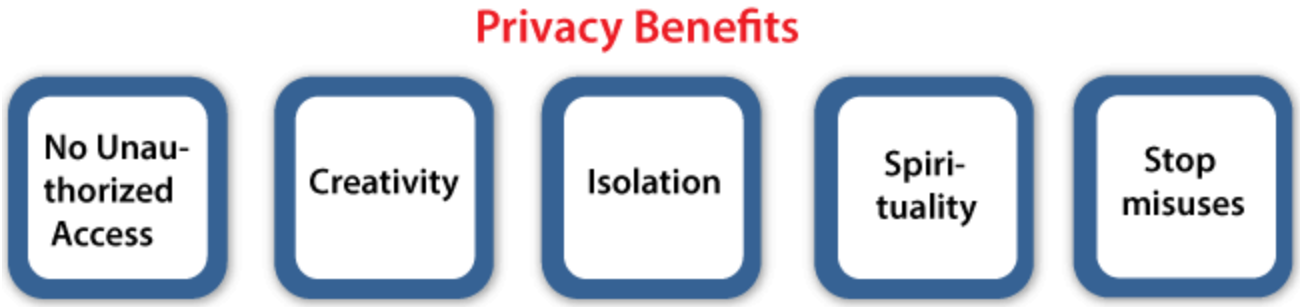
The concept of global specific privacy is a modern concept mainly associated with Western culture (North American and British in particular) and remained unknown virtually within a few cultures. Most cultures identify the ability of persons to withhold some parts of personal information through wider society.

In the organizational world, an individual can volunteer secret details to receive a few sorts of profit. Public figures can be subject to regulations and rules on its interest. Secret information of a person that is shared voluntarily and misused can subsequently cause **identity theft**.

Privacy Benefits

The benefits are listed below:

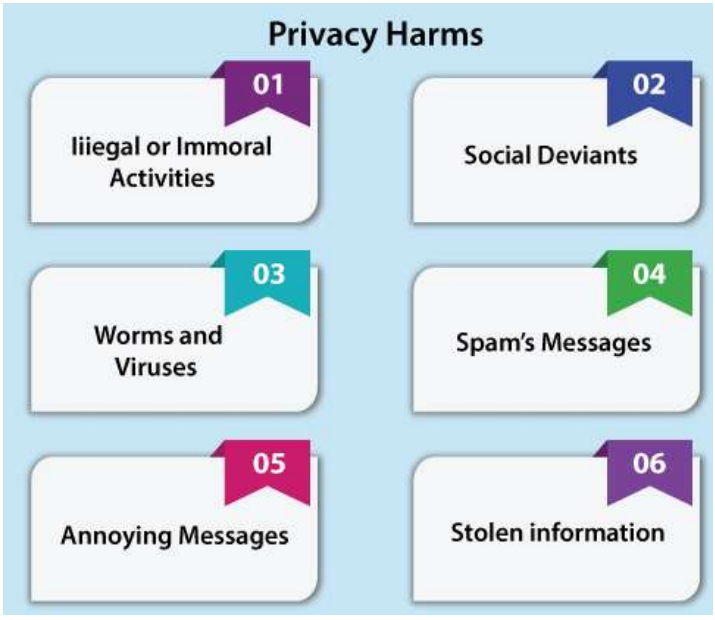
- Unauthorized users cannot access our personal data.
- All aspects of our life are not transparent.
- Creativity
- Privacy can be defined as the "moral capital."
- Isolation
- Spirituality
- Different relationships with distinct people.
- It makes users feel protected about their data and information.
- No misuse or unwanted attacks.
- Encourages customers for sharing and shopping information with organizations.



Privacy harms

Let's discuss the threats to our privacy:

- Can cause illegal or immoral activities
- Social deviants
- Worms and viruses
- Spam's messages
- Annoying messages
- Stolen various card information
- Family violence
- May lead to unhappiness
- Trapped/caught in relationships



Privacy is something about user identity's safeguarding.

Privacy can be harder to specify because user-specific information can be secure information as well.

Example: It might limit the record access of patient health to particular staff members of the hospital, like medical assistants, nurses, and doctors.

Document management:

Document management can help your organization control all its content, and records management helps ensure your information stays confidential and secure. While there is some overlap between the two, document and records management are distinct.
Document management is the process of organizing and controlling your organization's documents.

Under this definition, documents are defined as "information created for the organization to operate." Per the standard, documents can take any format, come from any source, and be of any media type.

With that in mind, here's a partial list of materials that fall into the category of documents:

- Emails that acknowledge receipt of an invoice or confirm an appointment time
- To-do lists
- Draft communications
- Contracts
- Marketing copy
- Product descriptions and specifications
- Executive orders
- Wills
- Invoices

A document can be in any media format, including:

- Photographs
- Video
- Text
- Paper

Organizations have countless documents in many formats. These documents evolve as people edit or alter them. It's important to keep track of documents to ensure they don't get lost and unauthorized changes don't get passed

along. That's where having a document management system can prove invaluable.

Document management process:

The document management process typically involves multiple steps, from creating a document to its eventual storage. The process looks something like this.

1. Creation

How a document gets created depends on the media used and the format of the file. If it's a text-based document, creation can involve opening and saving a word processing document. If it's a video or image-based document, creation can involve uploading video or image files to the document management system.

2. Drafting and review

The created document gets shared with collaborators, who might add edits or comments. Ideally, the document management process will allow collaborators to work on the same document without overriding each other's work. Features like track changes and document locking help to minimize mistakes and streamline the collaborative process. Document version control makes it easy to go back and see what changes were made and by whom.

A document management system can also include automation that makes it easy to review documents. Automated features might include auto-tags on files and spelling or grammar checkers

3. Assembly and approval

Some documents are more complex than others and might need to be assembled before they are complete. A document management system can assemble a document using custom metadata so all related pages are included. The assembly process can ensure the document meets any regulatory requirements and abides by the company's standards. For example, an employment contract or nondisclosure agreement might need to contain certain clauses to be valid.

Once the document is drafted and assembled, the next step is approval. The approval process can involve collecting signatures on the document. An organization can use e-signature software to streamline this step.

4. Storage and access

Approved documents need to live somewhere. In the past, it was common to print out paper versions or gather physical copies of documents in the form of tapes, DVDs, or photographs. Physical formats need a physical location for storage, such as a filing room or off-site storage facility.

Cloud storage eliminates the need for physical filing cabinets and a dedicated room or facility. A cloud-based document management system means a user can access a document from almost anywhere and the document can be downloaded on any internet-connected device.

5. Disposal

While some documents need to live forever, not all do. A document management system should include an effective option for deleting or disposing of documents that are no longer needed (or that must be deleted to comply with regulation or policy). Based on your organization's industry and compliance regulations, your system should comply with any disposition requirements that might apply.

Records management:

A record is slightly different from a document.. Records, according to ISO 9000:2015, are documents that provide evidence of activities performed or that state results achieved. They can be used as evidence of verification, corrective action, or preventive action. They can also formalize traceability.

The United Nations (U.N.) defines a record as "information created, received, and maintained as evidence and information by an organization or person, pursuance of legal obligations or in the transaction of business."

Examples of records include:

- Confirmation emails
- Spreadsheets with budgetary decisions
- Photographs
- Final reports

One way to differentiate between records and documents is that records are generally more formal than documents. They need to be managed much closely, as they can act as a form of evidence if needed. While a document can continue to evolve over the course of its life, a record is complete. Once a piece of content has been called a record, there is no way to change it without creating a new, separate record.

Records management process:

Initially, the records management process is similar to the documents management process. It involves the following:

1. Creation

Records often begin their lives as documents. They can take many forms, such as contracts, photos, and videos. Depending on the type of record, there might be multiple components that need to be created. For example, a medical record might include X-rays of a patient, a written medical history, a list of medications, and written or audio commentary from a physician. A record of an auto accident might include the police report, recordings of eyewitnesses, and photos of the damage.

2. Drafting, review, and revision

Depending on the type of record being created, there might be a drafting, review, and revision process, just as there is during document management. At this point, it's important to assign user permissions and track who is working on the record at any time to avoid overriding edits and keep the record as accurate as possible.

3. Approval

A record might also need to be approved, which can take multiple forms. For instance, the appropriate parties can sign the record or a court can approve it.

4. Storage

Records need to be stored securely to protect their integrity. Often, a retention schedule is connected to records storage. Depending on the record type, an organization might need to retain it for months, a year, or forever. The retention schedule would also determine where a record is stored.

For example, say a university needs to store student records. How long the school keeps each record is determined by the relationship the school had with the student. Applicant records for students who applied but weren’t accepted typically don't need to be retained for long. A school might store their records for a year, then archive or dispose of them.

5. Disposal

Although there are rules regarding how long an organization needs to keep records, they don't necessarily last forever. Records can be disposed of when the time is right. An organization's record management system should outline the proper steps for disposing of records to ensure the process is handled correctly.

Capabilities of records management:

An effective records management system needs to have certain capabilities to ensure compliance. The capabilities should be customizable based on your organization's industry and needs. They include:

- Record registration: After creation, a record is assigned a unique identifier, ensuring consistency throughout its life
- Stringent access controls: Records might need to be restricted, meaning only users with certain permission levels can edit or access them
- Retention rules: A records management system needs rules that define how long records can be kept, where they should be stored, and the disposal process at the end of a record's lifecycle
- Audit functionality: Audits show how the records were created, who handled them, how they were stored, and how they were disposed of

Physical Asset Management:

Physical asset management is a strategy for implementing efficient and effective upkeep of a manufactured item or property throughout its entire lifecycle. Activities facilitated by physical asset management include maintenance, repair, upgrades, and end-of-life disposition of the asset.

Also called service asset management, this strategy is often applied to equipment, machinery, devices, vehicles, and other complex assets that are characterized by relatively long product lifecycles. The purpose of physical asset management is to increase the performance, efficiency, and life of assets during their operational use.

Physical asset management is typically carried out by asset management software, which is part of a service lifecycle management (SLM) system. Asset management software connects service activities with an asset’s history, operational status, unplanned downtime, regulated maintenance requirements, current configuration, and more.

Physical asset management software gathers and maintains updated asset-specific information as services are performed. The software also provides an open ecosystem visible and accessible to OEMs, customers, and third parties involved in delivering effective service of managed assets.

The Primary Aim of Physical Asset Management:

The primary aim of Physical Asset Management is to maximize the value of physical assets while minimizing the risks associated with owning and operating them. An AM strategy helps ensure that physical assets are:

- Available when needed
- Reliable and fit for purpose
- Cost-effective to operate and maintain
- Compliant with regulations and standards
- Safely and sustainably managed

Two Types of Asset Management:

There are two types of Asset Management that companies can use to manage their physical assets: Reactive Asset Management and Proactive Asset Management.

1. **Reactive Asset Management:** This approach is based on fixing assets after they fail or break down. This type of Asset Management is costly and can lead to unplanned downtime, lost revenue, and safety hazards.
2. **Proactive Asset Management:** This approach involves monitoring assets in real-time, predicting potential failures before they occur, and conducting preventative maintenance to avoid downtime and costly repairs. This type of Asset Management reduces risks, increases reliability, and maximizes the value of physical assets.

Maintance of physical assests:

Maintaining physical assets involves several steps, including:

- Conducting regular inspections and assessments
- Identifying potential failures and risks
- Prioritizing maintenance activities based on criticality and impact
- Scheduling and executing preventative maintenance
- Recording and tracking maintenance data
- Continuously monitoring asset performance and condition
- Training employees on proper maintenance procedures and safety protocols is also crucial for maintaining physical assets.

Importantance:

To comprehend why physical asset management is significant, you need to see how the assets are utilized in the business and improving the assets to capitalize on them before they are decommissioned.

The stock should be seen to guarantee it doesn't run its timeframe of realistic usability prior to being sold. Gear should be kept up with and adjusted so it doesn't cause vacation when it breaks.

Physical asset management utilizes procedures and cycles that spotlights forestalling these conceivable outcomes while as yet helping your association bring down the complete expense of possession.

It is an extremely modern cycle that should be managed by experts who will consistently search for approaches to further develop it.

When appropriately conveyed, you will get a drawn-out advantage that impacts your primary concern as well as the wellbeing and dependability of all your actual assets.

Benefits of physical asset management:

- Early identification of material or logistics issues
- Greater assurance that compliance requirements are met
- Reduced inventory costs and reduced scrap rates of unneeded parts
- Improved efficiency in developing and maintaining parts catalogs
- Improved traceability and clarity of service impacts across the enterprise
- Increased asset availability and reliability
- Reduced downtime and repair cost
- Improved safety and compliance
- Enhanced efficiency and cost-effectiveness
- Extended asset life and improved sustainability
- Better risk management and decision-making

Examples of Physical Assests management:

Physical assets can vary depending on the industry and the company’s operations. Here are some examples of physical assets in various industries:

- **Manufacturing:** Machinery, equipment, and tools
- **Energy:** Power plants, pipelines, and transmission lines
- **Transportation:** Vehicles, planes, and infrastructure
- **Real Estate:** Buildings and land
- **Utilities:** Water treatment plants, reservoirs, and distribution systems

We tend to differentiate Asset Management of an organization's tangible assets, such as machinery, equipment, vehicles, buildings, and infrastructure, as a separate discipline from Investment asset management which is closer aligned with financial services, however both disciplines share core principles.

Physical or Infrastructure Asset management involves planning, acquiring, maintaining, operating, and disposing of these assets in the most efficient and cost-effective manner possible, with the purpose of delivering the Organization's strategic objectives.

Office Equipment :

Office Equipment is a term used to refer all the modern technology equipment and supplies used by today's businesses, from a small shop to big stores and from the government to private sectors.

They play a major role in making your day to day business activity quite easy. Well in older days, there was a very less use of such equipment and the work done manually. But as time has passed technology is improving and new equipment has come into the market.

•Control of office equipment must be local—a department or area manager is usually the appropriate person to be assigned this responsibility.

•Where high-risk and critical equipment is used or stored, involve your organization's security representative in a formal risk assessment and in the design of appropriate security measures.

•The best way to reduce risk to office equipment is the consistent application of site access control procedures that are in accordance with your organization's policy.

•Minimize the number of points where material is received and removed.

•Place all office equipment on your fixed assets list.

Suggested Minimum Security Requirements:

✓Inventory all equipment and place it on the fixed assets list.
✓Prevent unauthorized use of equipment.

✓Control access in accordance with your organization's policy.
✓Develop and use a proprietary pass system for equipment that may be removed from the area.
✓Lock all desks, storage cabinets, and equipment when not in use and during non-business hours.
✓Assign one person the responsibility for equipment movement and accountability.

Essential Types of Office Equipment:

Office equipment is an essential part of every business. It keeps operations running smoothly, and in many cases, a business relies on their equipment so much that an equipment failure would significantly impact or cripple their ability to operate. This is why regular office equipment maintenance is so important. Here are 4 types of office equipment that you definitely do not want to neglect.

1.Dictation Machines

One piece of equipment that may not seem essential to many people is the dictation machine. Although speech recognition software continues to evolve, it is not without pitfalls. Executives who need to draft letters, memos, and reports are best off dictating the copy and recording it, since speaking is much faster than writing and can be done while performing other tasks. The type of equipment chosen depends on the preferences of the dictators, number of users, frequency of use, and budget. Some dictation equipment uses cassette tapes, while more modern versions record digitally and even use a phone system for recording. However the audio is recorded, this file is then processed by another employee, who transcribes the audio into a written document and saves, emails, or prints it.

2. Printers

Any office that runs even one PC needs a printer to create hard copies of electronic documents and files. Despite the promises of paperless offices in the

future, that era has not yet arrived. All sorts of business documentation needs to be printed, whether the business is a product- or service-oriented industry. Examples of common office documents include invoices, packing slips, flyers, and letters. Printers can be used not just to generate transfer electronic files to paper but also to create composite documents containing digital information and scanned images.

3.Document Scanners

While the fax machine was once considered an indispensable piece of office equipment, electronic copies of just about any document are now possible with the help of a scanner. A scanner copies an image of papers that were not created electronically and converts them into digital images so that they can be stored on a computer or emailed. Examples of items that might need to be scanned include photographs, pages from print publications, cash register receipts, drawings, and forms that have been filled out by hand. Even a letter that was created in a computer software program might have been received in hard copy and so would need to be scanned into a storage system if the digital file was not available. Before the invention of the scanner, the best that could be done with miscellaneous materials was to photocopy and file them, a practice which is still followed today in some places.

4.Laminate Machines

Laminating machines are generally underutilized in most offices. When someone has gone to the trouble to print or copy a document, that document can be preserved by heat-sealing two thin layers of clear plastic over each side. A piece of paper is inserted into a laminating sheet, which is generally is twice the size of a standard document but then folded in half. Enough of a margin remains on all sides of the document so that the plastic melts to itself and creates a permanent seal. The document and plastic are inserted into a special laminating sleeve that enables the document to pass through the machine smoothly and keeps the melted plastic from getting stuck between the hot

rollers.
Laminators can be used to

- Create signage
- Produce ID badges
- Preserve photos
- Create long-lasting business cards
- Reinforce pages in a flip chart or spiral-bound booklet

Once an office obtains a laminator, the personnel may come up with many more creative uses for this equipment

5.Computer Projector For Presentation or Meeting

A projector or image projector is an optical device that projects an image (or moving images) onto a surface, commonly a projection screen. Most projectors create an image by shining a light through a small transparent lens, but some newer types of projectors can project the image directly, by using lasers. A virtual retinal display, or retinal projector, is a projector that projects an image directly on the retina instead of using an external projection screen.
The most common type of projector used today is called a video projector. Video projectors are digital replacements for earlier types of projectors such as slide projectors and overhead projectors. These earlier types of projectors were mostly replaced with digital video projectors throughout the 1990s and early 2000s, but old analog projectors are still used at some places. The newest types of projectors are handheld projectors that use lasers or LEDs to project images.

6.Office Essential Business Materials Printing

Design custom print essential business materials that introduce and distinguish your business.
Create consistent branding on business cards, labels, and envelopes.

- Make correspondences official with customized letterheads and notepads.

- Stock up on personalized notebooks, calendars, and notepads.

7.Network Equipments

full line of powerful enterprise class networking solutions for all your network needs at simple subscription service. By combining these solutions with cloud-management service, customers can address today's highest networking priorities, from bandwidth expansion, VoIP, BYOD, to network security.

8.Servers

For companies that have gone "all-in" on the cloud, there may not be a single server to be found in the office.

More commonly, a few servers run in-house databases such as ERP systems, document management systems, and data marts.

Servers are also used for file sharing and as a local data backup location for individual computers. Of course, there should be an off-site component to a comprehensive data backup strategy.

9. Multi-Function Printers

A multi-function printer (MFP) is a vital office equipment item for many small businesses.

These devices print, copy and scan at high speeds and high resolutions.

With the right type of MFP and a properly configured network, anyone can walk over to the MFP and scan documents directly to a desktop application on their computer. No need for everyone to have their own scanner.

A quality MFP is the first leg of an entire digital document management process for law firms and CPAs.

10. A Projector or a Big Screen TV

Given a choice between a projector and a big-screen TV, many businesses are selecting the latter. TVs are quiet, the image is crisper, there's no bulb to burn out, and a shadow can't be cast on the screen.

All TVs have multiple HDMI ports standard and most new projectors include an HDMI port. This means that devices such as Apple TV, Chromecast with Google TV, or Airtame can be plugged into the TV or projector. This, in turn, means that almost any device can be wirelessly connected to either a TV or a projector.

Industrial Control System (ICS):

ICS assets are the digital devices that are used in industrial processes. This includes all of the various components of critical infrastructure (power grid, water treatment, etc.), manufacturing, and similar applications.

- A number of different devices are classified as ICS. Some examples include:
- Programmable Logic Controllers (PLCs)
- Remote Terminal Units (RTUs)
- Human-Machine Interfaces (HMIs)
- Supervisory Control and Data Acquisition (SCADA)

ICS has been around for a while, and, although they have been networked together for decades, they were often “air gapped” from the Internet. This helped to protect them from cyber threats by making them more difficult to remotely access and exploit.

In recent years, the air gap has eroded. Now, it is common to use Internet-connected smart and IoT devices for remote monitoring and management of ICS. While this increases efficiency and usability, it also introduces new cybersecurity risks. With this new paradigm, ICS and IoT security solutions are required to protect the safety and functionality of these newly Internet-connected systems.

Challenges of ICS Security:

While industrial control systems have the same security challenges as traditional IT environments, they have their own unique challenges as well, including:

High Availability Requirements: For ICS systems in critical infrastructure, manufacturing, and other industries, availability and uptime are of the utmost importance. This makes securing these systems difficult as they cannot be easily taken down to install security updates.

Insecure and Proprietary Protocols: ICS uses a variety of proprietary protocols, including many that were designed decades ago to support long-lived components. These protocols often lack basic security features (such as encryption and access control) and cannot be updated.

Focus on Detection Over Prevention: ICS's high availability requirements mean that the potential that legitimate operations will be blocked is a significant concern. For this reason, the ICS security is often set to detect attacks rather than attempting to prevent them.

Overcoming these challenges requires ICS security solutions designed to operate in ICS's unique environment.

Threats to Industrial Control Systems:

Attacks against ICS devices can intentionally or unintentionally cause loss of availability. Attackers can gain access to these systems in a number of ways, including:

- Lateral movement from IT network
- Direct access to Internet-facing systems
- Phishing attacks to compromise legitimate OT account credentials
- Exploitation of vulnerable IoT and Internet-connected systems

An ICS security solution must provide comprehensive protection against these and other ICS attack vectors.

ICS Security Best Practices:

ICS systems commonly lag behind IT systems in terms of protection against cyber threats. To start bringing ICS system security up to speed, implement these best practices:

- **Perform ICS Asset Discovery:** Many organizations lack full visibility into their complete ICS infrastructure. A full understanding of ICS assets and their network connectivity is essential to security.
- **Monitor Network Baselines:** ICS networks should be fairly static as the devices connected to them rarely change. These networks should be monitored to establish a baseline, then to detect and alert on any network anomalies or new devices connected to the network.
- **Perform Network Segmentation:** Historically, ICS networks were protected by air gaps, but this is no longer the case. Securing systems that were not designed to be connected to the Internet requires network segmentation with firewalls that understand ICS protocols.
- **Implement Least Privilege:** Many ICS protocols do not implement access controls, allowing inappropriate access to privileged and dangerous functionality. ICS protocol-aware firewalls should be used to enforce access controls on ICS network traffic.
- **Deploy an Intrusion Prevention System (IPS):** Detection-focused ICS security leaves an organization in the position of responding to existing malware infections and security incidents. An IPS should be used to identify and block attempted exploitation of known vulnerabilities in ICS systems and the legacy operating systems that they run on.
- **Secure Remote Access:** Remote access is often necessary for monitoring and management of ICS assets at geographically distributed sites. However, this access should be implemented using strong authentication, access control, and encryption to protect against unauthorized access to and exploitation of these systems.
- **Secure Physical Access:** Physical access to ICS assets can threaten their availability and enable defenses to be bypassed. ICS should be protected by both cyber and physical security measures.

Industrial control systems are complex and vulnerable, but they are also a vital part of critical infrastructure, manufacturing, and related industries. Protecting these systems against attack without interrupting normal operations makes ICS-aware security essential.

Critical Aspects of Industrial Control Systems (ICS) Security:

Industrial Control Systems (ICS) is one of the most important areas of business. They can help automate tasks, improve performance, and ensure safety. However, they can also be abused if not properly managed. Here are a few critical aspects to consider for ICS security:

- Ensure that all components of the system are compatible with each other
- Make sure that devices and controls are tested before they're used
- Keep track of who has access to the system and how it's used
- Limit access to specific users or groups

What Are the Benefits of Industrial Control Systems (ICS)

Industrial Control Systems (ICS) can help businesses save time and money. For example, they can help reduce the number of steps needed to complete a task, or they can automate tasks that would otherwise require human interaction. Industrial Control Systems (ICS) can also save money by reducing the cost of goods and services.

What Are the Risks in Industrial Control Systems (ICS)

Industrial Control Systems (ICS) can pose a number of risks to businesses and individuals. These include:

- Unauthorized use of equipment or data, which could result in loss of data or damage to equipment.

- Accidental release of dangerous chemicals or explosives from control systems.

- Human error could lead to accidents or injuries caused by faulty controls.

Mobile Device Security:

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. With more than half of business PCs now mobile, portable devices present distinct challenges to network security, which must account for all of the locations and uses that employees require of the company network. Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen.

Mobile device security, or mobile device management, provides the following:

- Regulatory compliance
- Security policy enforcement
- Support of “bring your own device” (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup

Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.
How does Mobile Device Security work?

Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

To get started, here are some mobile security best practices:

- **Establish, share, and enforce clear policies and processes**

Mobile device rules are only as effective as a company's ability to properly communicate those policies to employees. Mobile device security should include clear rules about:

1. What devices can be used
2. Allowed OS levels
3. What the company can and cannot access on a personal phone
4. Whether IT can remote wipe a device
5. Password requirements and frequency for updating passwords

- **Password protection**

One of the most basic ways to prevent unauthorized access to a mobile device is to create a strong password, and yet weak passwords are still a persistent problem that contributes to the majority of data hacks. Another common security problem is workers using the same password for their mobile device, email, and every work-related account. It is critical that employees create strong, unique passwords (of at least eight characters) and create different passwords for different accounts.

- **Leverage biometrics**

Instead of relying on traditional methods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable biological characteristics, such as face, fingerprint, voice, or iris recognition for identification and access. Multiple biometric authentication methods are now available on smartphones and are easy for workers to set up and use.

- **Avoid public Wi-Fi**

A mobile device is only as secure as the network through which it transmits data. Companies need to educate employees about the dangers of using public Wi-Fi networks, which are vulnerable to attacks from hackers who can easily

breach a device, access the network, and steal data. The best defense is to encourage smart user behavior and prohibit the use of open Wi-Fi networks, no matter the convenience.

- **Beware of apps**

Malicious apps are some of the fastest growing threats to mobile devices. When an employee unknowingly downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data. To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

- **Mobile device encryption:**
  Most mobile devices are bundled with a built-in encryption feature. Users need to locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorized access.

What are the different types of Mobile Device Security:

There are many aspects to a complete security plan. Common elements of a mobile security solution include the following:

- **Enterprise Mobile Management platform:** In addition to setting up internal device policies that protect against unauthorized access, it's equally important to have an Enterprise Mobile Management (EMM) platform that enables IT to gather real-time insights to catch potential threats.
- **Email security:** Email is the most popular way for hackers to spread ransomware and other malware. To combat such attacks, it's critical for businesses to be armed with advanced email security that can detect, block, and address threats faster; prevent any data loss; and protect important information in transit with end-to-end encryption.

- **Endpoint protection:** This approach protects enterprise networks that are remotely accessed by mobile devices. Endpoint security protects companies by ensuring that portable devices follow security standards and by quickly alerting security teams of detected threats before they can do damage. Endpoint protection also allows IT administrators to monitor operation functions and data backup strategies.
- **VPN:** A virtual private network, or VPN, extends a private network across a public network. This enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs' encryption technology allows remote users and branch offices to securely access corporate applications and resources.
- **Secure web gateway:** A secure web gateway protects against online security threats by enforcing company security policies and defending against phishing and malware in real-time. This is especially important for cloud security as this type of protection can identify an attack on one location and immediately stop it at other branches.
- **Cloud access security broker:** A cloud access security broker (CASB) is a tool that sits between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications. CASBs help organizations extend the security controls of their on-premises infrastructure to the cloud.

Importance of mobile device security:

With more than half of business PCs now mobile, portable devices present distinct challenges to network security, which must account for all of the locations and uses that employees require of the company network. Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen. To avoid a security breach, companies should take clear, preventative steps to reduce the risk.

Benefits of Mobile Device Security:

Mobile device security, or mobile device management, provides the following:

- Regulatory compliance
- Security policy enforcement
- Support of "bring your own device" (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup

Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

To get started, here are some mobile security best practices:

- **Establish, share, and enforce clear policies and processes**

Mobile device rules are only as effective as a company's ability to properly communicate those policies to employees. Mobile device security should include clear rules about:

1. What devices can be used
2. Allowed OS levels
3. What the company can and cannot access on a personal phone
4. Whether IT can remote wipe a device
5. Password requirements and frequency for updating passwords

- **Password protection**

One of the most basic ways to prevent unauthorized access to a mobile device is to create a strong password, and yet weak passwords are still a persistent problem that contributes to the majority of data hacks. Another common security problem is workers using the same password for their mobile device, email, and every work-related account. It is critical that employees create

strong, unique passwords (of at least eight characters) and create different passwords for different accounts.

- **Leverage biometrics**

Instead of relying on traditional methods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable biological characteristics, such as face, fingerprint, voice, or iris recognition for identification and access. Multiple biometric authentication methods are now available on smartphones and are easy for workers to set up and use.

- **Avoid public Wi-Fi**

A mobile device is only as secure as the network through which it transmits data. Companies need to educate employees about the dangers of using public Wi-Fi networks, which are vulnerable to attacks from hackers who can easily breach a device, access the network, and steal data. The best defense is to encourage smart user behavior and prohibit the use of open Wi-Fi networks, no matter the convenience.

- **Beware of apps**

Malicious apps are some of the fastest growing threats to mobile devices. When an employee unknowingly downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data. To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

- **Mobile device encryption:**

  Most mobile devices are bundled with a built-in encryption feature. Users need to locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorized access.

The Different types of Mobile Device Security:

There are many aspects to a complete security plan. Common elements of a mobile security solution include the following:

- **Enterprise Mobile Management platform:** In addition to setting up internal device policies that protect against unauthorized access, it's equally important to have an Enterprise Mobile Management (EMM) platform that enables IT to gather real-time insights to catch potential threats.
- **Email security:** Email is the most popular way for hackers to spread ransomware and other malware. To combat such attacks, it's critical for businesses to be armed with advanced email security that can detect, block, and address threats faster; prevent any data loss; and protect important information in transit with end-to-end encryption.
- **Endpoint protection:** This approach protects enterprise networks that are remotely accessed by mobile devices. Endpoint security protects companies by ensuring that portable devices follow security standards and by quickly alerting security teams of detected threats before they can do damage. Endpoint protection also allows IT administrators to monitor operation functions and data backup strategies.
- **VPN:** A virtual private network, or VPN, extends a private network across a public network. This enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs' encryption technology allows remote users and branch offices to securely access corporate applications and resources.
- **Secure web gateway:** A secure web gateway protects against online security threats by enforcing company security policies and defending against phishing and malware in real-time. This is especially important for cloud security as this type of protection can identify an attack on one location and immediately stop it at other branches.

- **Cloud access security broker:** A cloud access security broker (CASB) is a tool that sits between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications. CASBs help organizations extend the security controls of their on-premises infrastructure to the cloud.

Possible mobile Phone malware threats:

As a security specialist, it is essential to know about the types of malware associated with mobile devices.

- **Mobile spyware:** Spyware is malicious software that can creep into apparently compassionate programs and, in secret, monitor your activity, track your geo-location, as well as steal sensitive passwords.
- **Mobile banking Trojans:** These are mobile banking viruses that target and steal your bank details. In the year 2017, mobile banking Trojans hit around 260,000 users across 160+ countries. They acted as if they are legitimate bank applications and then stolen all users' bank and account
- details.
- **Rooting malware:** These types of malware try to gain root access to any mobile devices for providing its creators or cybercriminals the administrative privileges as well as access to that victim's files.

Components of a Mobile Security Solution:

- Mobile security is complex because of the large number of potential attack vectors – devices can be targeted at multiple levels:

- **Applications:** Malware can be developed and deployed as malicious apps that users unwittingly install on their devices. Mobile security solutions should be able to detect and block downloads of these malicious apps.

- **Network:** Mobile devices and the legitimate apps that run on them can be targeted at the network level. Man-in-the-Middle, phishing, and other attacks take advantage of network connectivity to steal data or deliver malicious content. Mobile security involves blocking these network-level attacks.

- **OS:** Both iOS and Android operating systems can contain exploitable vulnerabilities, which are used for jailbreaking/rooting devices either by users or by malware. This provides an attacker with advanced permissions on the device, breaking its security model. Mobile security incorporates real-time risk assessments, configuration monitoring, and other tools to detect exploitation of device vulnerabilities.

System Development:

Systems development is the procedure of defining, designing, testing, and implementing a new software application or program. It comprises of the internal development of customized systems, the establishment of database systems, or the attainment of third party developed software. In this system, written standards and techniques must monitor all information systems processing functions. The management of company must describe and execute standards and embrace suitable system development life cycle practise that manage the process of developing, acquiring, implementing, and maintaining computerized information systems and associated technology.

System development methodologies are promoted in order to improve the management and control of the software development process, structuring and simplifying the procedure, and standardizing the development process and product by stipulating actions to be done and methods to be used. It is often implicitly presumed that the use of a system development methodology will increase system development output and excellence.

7 Stages of the System Development Life Cycle:

There are seven primary stages of the modern system development life cycle. Here's a brief breakdown:

- Planning Stage
- Feasibility or Requirements of Analysis Stage

- Design and Prototyping Stage
- Software Development Stage
- Software Testing Stage
- Implementation and Integration
- Operations and Maintenance Stage

Now let’s take a closer look at each stage individually.

Planning Stage:

Before we even begin with the planning stage, the best tip we can give you is to take time and acquire proper understanding of app development life cycle.

The planning stage (also called the feasibility stage) is exactly what it sounds like: the phase in which developers will plan for the upcoming project.

It helps to define the problem and scope of any existing systems, as well as determine the objectives for their new systems.

By developing an effective outline for the upcoming development cycle, they'll theoretically catch problems before they affect development.

And help to secure the funding and resources they need to make their plan happen.

Perhaps most importantly, the planning stage sets the project schedule, which can be of key importance if development is for a commercial product that must be sent to market by a certain time.

Analysis Stage

The analysis stage includes gathering all the specific details required for a new system as well as determining the first ideas for prototypes.

Developers may:

- Define any prototype system requirements
- Evaluate alternatives to existing prototypes
- Perform research and analysis to determine the needs of end-users

Furthermore, developers will often create a software requirement specification or SRS document.

This includes all the specifications for software, hardware, and network requirements for the system they plan to build. This will prevent them from overdrawing funding or resources when working at the same place as other development teams.

Design Stage:

The design stage is a necessary precursor to the main developer stage.

Developers will first outline the details for the overall application, alongside specific aspects, such as its:

- User interfaces
- System interfaces
- Network and network requirements
- Databases

They'll typically turn the SRS document they created into a more logical structure that can later be implemented in a programming language. Operation, training, and maintenance plans will all be drawn up so that developers know what they need to do throughout every stage of the cycle moving forward.

Once complete, development managers will prepare a design document to be referenced throughout the next phases of the SDLC.

Development Stage

The development stage is the part where developers actually write code and build the application according to the earlier design documents and outlined specifications.

This is where Static Application Security Testing or SAST tools come into play.

Product program code is built per the design document specifications. In theory, all of the prior planning and outlined should make the actual development phase relatively straightforward.

Developers will follow any coding guidelines as defined by the organization and utilize different tools such as compilers, debuggers, and interpreters.

Programming languages can include staples such as C++, PHP, and more. Developers will choose the right programming code to use based on the project specifications and requirements.

Testing Stage

Building software is not the end.

Now it must be tested to make sure that there aren't any bugs and that the end-user experience will not negatively be affected at any point.

During the testing stage, developers will go over their software with a fine-tooth comb, noting any bugs or defects that need to be tracked, fixed, and later retested.

t's important that the software overall ends up meeting the quality standards that were previously defined in the SRS document.

Depending on the skill of the developers, the complexity of the software, and the requirements for the end-user, testing can either be an extremely short phase or take a very long time. Take a look at our top 10 best practices for software testing projects for more information.

Implementation and Integration Stage:

After testing, the overall design for the software will come together. Different modules or designs will be integrated into the primary source code through developer efforts, usually by leveraging training environments to detect further errors or defects.

The information system will be integrated into its environment and eventually installed. After passing this stage, the software is theoretically ready for market and may be provided to any end-users.

Maintenance Stage:

The SDLC doesn't end when software reaches the market. Developers must now move into a maintenance mode and begin practicing any activities required to handle issues reported by end-users.

Furthermore, developers are responsible for implementing any changes that the software might need after deployment.

This can include handling residual bugs that were not able to be patched before launch or resolving new issues that crop up due to user reports. Larger systems may require longer maintenance stages compared to smaller systems.

Role of System Analyst:

An SDLC's system analyst is, in some ways, an overseer for the entire system. They should be totally aware of the system and all its moving parts and can help guide the project by giving appropriate directions.

The system analyst should be:

- An expert in any technical skills required for the project
- A good communicator to help command his or her team to success

- A good planner so that development tasks can be carried out on time at each phase of the development cycle

Thus, systems analysts should have an even mix of interpersonal, technical, management, and analytical skills altogether. They're versatile professionals that can make or break an SDLC.

Their responsibilities are quite diverse and important for the eventual success of a given project. Systems analysts will often be expected to:

- Gather facts and information
- Make command decisions about which bugs to prioritize or what features to cut
- Suggest alternative solutions
- Draw specifications that can be easily understood by both users and programmers
- Implement logical systems while keeping modularity for later integration
- Be able to evaluate and modify the resulting system as is required by project goals
- Help to plan out the requirements and goals of the project by defining and understanding user requirements

Incorporate security into the software development life cycle(SDLC):

With the persistence of security issues in software development, there is an urgent need for software development companies to prioritize security in the software development life cycle.

Apart from helping them maintain a good reputation and avoid a declining customer base, integrating security in the software development life cycle (SDLC) is also key to protecting organizations from data breaches and other cyberattacks. Therefore, software engineers should take a proactive approach to security during each phase of the SDLC.

Understanding secure software development life cycle:

The software development life cycle is not a one-off process that software developers can implement in a linear form. Instead, there are phases of the SDLC that intertwine into many loops where thorough checks are carried out to ensure the proper outcome of the software.

However, it's not just enough to loop through the phases of SDLC without the proper integration of security checks in each phase. So, what, then, makes a secure software development life cycle?

First, a secure SDLC must incorporate security measures such as code review, penetration testing and architecture analysis. In addition to that, some other security measures that make for a secure SDLC include threat modeling, risk assessment and static analysis.

Ways to incorporate security into the SDLC:

In the software development life cycle, there are certain standards software developers can adopt to ensure a secure SDLC. Some of them are highlighted below alongside the SDLC phases.

1. Requirements gathering phase

Critical security questions that should be asked during the requirement gathering phase include: How quickly can the software recover from a security attack? and What security techniques can protect the software from security attacks?

When you answer these questions at this stage, the security requirements for the software will be clear for the developers.

2. Design phase:

The design phase is crucial for security integration in software development. Common software vulnerabilities are usually caused by adopting the wrong technologies in software development.

In this phase, there should be a threat modeling process to ensure possible threats are detected as well as a mitigation plan to protect the software against threats. It's important to note at this stage that the earlier potential threats are detected, the easier it is for software engineers to come up with a plan to address them.

3. Development phase:

Program development designs should be properly assessed at this phase, utilizing internal and external software teams and software development tools. Initial testing, user training, deployment, acceptance testing and management

approval are just a few issues that should be described and documented at this stage.

4. Implementation phase:

During this implementation phase, the attention should be on automated technology tools and guidelines that will make code reviews easy. Tools that automate code review can be deployed at this phase for thorough code analysis. One of such tools is the static application security testing (SAST) tool. In addition, if your developers intend to make the software open source, then using Software Composition Analysis (SCA) tools can also help them inspect and analyze their codes for vulnerabilities.

5. Testing phase:

Developers should adopt some security testing techniques to successfully integrate security at this phase. Some of the security testing techniques to use include:

- **Penetration Testing:** Using a variety of manual and/or automated testing via DAST tools, testers look for weaknesses in network, application and computer systems that an attacker can take advantage of.
- **Fuzz Testing:** In fuzz testing, testers can send malformed inputs to the software to enable them to find possible vulnerabilities.
- **Interactive Application Security Testing (IAST):** As a combination of DAST and SAST testing techniques,

6. Deployment phase:

The deployment phase is also critical to improving the software's security posture. From a security standpoint, deployment in cloud settings poses extra issues. For example, database parameters, private certificates and any other deployment-related sensitive configuration parameters should always be saved in secret management solutions like key vaults made available to programs during runtime.

7. Post-deployment and maintenance:

When the software development process reaches this point, it enters maintenance mode. At this phase, monitor the new program's performance regularly. In addition to that, try to make necessary changes without causing major production delays by making a schedule for patching and system shutdowns for maintenance, hardware updates and disaster recovery tasks.

Furthermore, developers can use security scan tools to check for vulnerabilities in applications or networks. These solutions can run continuous security scans and alert you if any dangers are discovered. However, it's worth noting that security scanners should be utilized responsibly. Use these scanners only with the consent of the owners of the infrastructure or applications.

Mitigate threats early in the software development life cycle:
There is no doubt that the world will continue to battle with the incidence of security attacks. However, if security is given a first-class treatment in the software development life cycle, it will go a long way to averting some security vulnerabilities in software tools. That said, the pointers above are intended to help companies and software engineers incorporate the best security practices in the software development life cycle.

Things to keep in mind while incorporating security into SDLC

- **Awareness of secure coding practices**

It is important to educate your team on secure coding practices and to use the available framework for security while building and planning for test cases. Use code scanning tools such as Code Sight, AppScan Source, and Coverity.

- **Performing gap analysis**

It is helpful to perform a gap analysis to find out the effectiveness of your organization's current activities and policies.

- **Threat Modeling**

Threat modeling for software components is done to identify and manage the threats in the early development lifecycle. It is all about planning for the appropriate mitigation before it becomes more harmful. There can be different approaches for this activity, such as protecting specific critical processes, exploiting weaknesses, or focusing on the system design.

- **Secured design with team review**

The development team should include security features while building software with developers including security design review when reviewing functional feature design. It is important to review code and developers need to be aware and follow a checklist of the most common coding security risks

- **Open-Source Analysis**

Open-Source Analysis reduces vulnerabilities with the dependencies. The open-source analysis goes through the entire codebase and pulls out all the dependencies used and indicates the non-safe versions of them. There are many tools available that you can use for open-source analysis such as WhiteSource, SourceClear, and Sync.

Most used secure SDLC models are:

- **MS Security development lifecycle (MS SDL)**

It is one of the first secured SDLC models of its kind, proposed by Microsoft in association with the phases of a classic SDLC.

- **NIST 800-64**

It was developed by the National Institute of Standards and technology to provide security measures within the SDLC.

The Benefits of Secure SDLC:

As Secure Software Development Lifecycle integrates security tightly into all phases of the lifecycle there are benefits throughout the lifecycle, making security everybody's responsibility and enabling software development that is secure from its inception. Some of the biggest benefits are as follows:

- **Reduced Costs**: Thanks to early identification of security concerns allowing the embedding of controls in parallel. No more patching post-deployment.
- **Security-First:** Secure SDLC builds security-focussed cultures, creating a working environment where security comes first, and everyone's eyes are on it. Improvements happen across the organization.
- **Development Strategy:** Defining security criteria from the outset improves technology strategy, making all team members aware of the security criteria of the product, and ensuring developer security throughout the lifecycle.
- **Better Security:** Once Secure SDLC processes are embedded, security posture improves across the whole organization. Organizations that are security aware reduce their risk of cyberattack significantly.

Possible Drawbacks of SDLC:

However, just like any other software development approach, the SDLC models might have drawbacks that can significantly impact the client's final decision. The probable disadvantages of the software development lifecycle system can be:

- Increased time and costs for the project development
- All the details should be specified in advance
- Low flexibility (especially in the final stages of the project development)
- The high volume of documentation
- The attraction of different specialists
- High involvement of the client
- Testing might be too complicated for certain teams of developers

Disaster management:

The organization, planning and application of measures preparing for, responding to and recovering from disasters.

Annotation: Disaster management may not completely avert or eliminate the threats; it focuses on creating and implementing preparedness and other plans to decrease the impact of disasters and "build back better". Failure to create and apply a plan could lead to damage to life, assets and lost revenue.

Emergency management is also used, sometimes interchangeably, with the term disaster management, particularly in the context of biological and technological hazards and for health emergencies. While there is a large degree of overlap, an emergency can also relate to hazardous events that do not result in the serious disruption of the functioning of a community or society.

The role of cybersecurity in disaster management:

From checking the weather app to using satnav, our everyday lives are surrounded by satellite information. However, satellites can be helpful beyond mundane activities. Rescuers, for example, can use satellite data to tackle natural disasters and manage emergency situations.

As with any other technological infrastructure, satellites are, however, at the mercy of cyber-attacks. Following October's International Day for Disaster Risk Reduction, we take a look at cybersecurity and what ESA is doing to avoid hacks and safeguard disaster management services.

How satellites help with managing disasters:

In 2014, a hack interfered with the US National Weather Service, which had to seal off data vital for disaster planning, aviation and shipping. According to NOAA officials, the services were made available shortly after, and forecasts were resumed. However, the lack of forecasting data, even for a short time, can put lives at risk.

Floods and hurricanes are two of the extreme events that, coming unannounced, can have devastating consequences for human life. This is why services that use satellite data to monitor disasters are vital, like the Copernicus Emergency Management Service. All over the world, entities and organisations active in emergency management can use the Copernicus Emergency Management Service to map areas that may be affected by natural disasters, humanitarian crises or human-made emergency events. The service uses reliable data from satellites and locations where a disaster may occur to rapidly map an area within hours of an event.

Satellite data can also help prevent a humanitarian crisis occurring in the first place. Earlier this year, the Portuguese island São Jorge received threatening levels of seismic activity – 1800 small tremors were registered in just four days. These could have indicated an imminent volcanic eruption, so local authorities used satellite data to map the potential lava flow and protect people and infrastructure accordingly. Fortunately, no volcanic eruption occurred, but the

local population was ready for the worst-case scenario thanks to the help of space technology.

The Scope of Disaster Management:

Disaster management has a broad scope. To understand what disaster management is, it is useful to study prevention, preparedness, and response and recovery.

Prevention:

Mitigation and prevention efforts aim to reduce the potential damage and suffering that disasters can cause. While disaster management cannot prevent disasters, it can prevent them from becoming compounded as a result of neglecting causal factors and manageable risks. Mitigation specifically refers to actions taken that can lessen the severity of a disaster's impact. Investing in measures that limit hazards can greatly reduce the burden of disasters.

Strategies that disaster management professionals implement to protect vulnerable communities and limit hazards include the following:

- Raising awareness about potential hazards and how to address them
- Educating the public about how to properly prepare for different types of disaster
- Installing and strengthening prediction and warning systems

Managing hazards and risks means planning to minimize a community's vulnerability to disasters. This can involve:

- Encouraging community members to buy appropriate insurance to protect their properties and belongings
- Educating families and businesses on how to create effective disaster plans
- Promoting the use of fire-retardant materials in construction
- Advocating for capital works initiatives, such as the construction and maintenance of levees
- Building partnerships between sectors and agencies at the federal, state, and local levels to collaborate on mitigation projects

Disaster management professionals working on mitigation efforts also focus on the following:

Land Use and Building Codes:

Building schools, hospitals, and neighborhoods in flood-prone areas increases their exposure to disasters. Disaster management spotlights these risks and presents ideas to use land in safer ways.

For example, rather than constructing homes in floodplains, community planners can designate those areas as places for outdoor recreation, wildlife attractions, or hiking trails. They can also urge people to avoid these areas during flood season. These measures make residents and their homes less vulnerable to harm.

Additionally, mitigation efforts can do the following:

- Address ways to engineer bridges to sustain earthquakes
- Enforce building codes that safeguard buildings during hurricanes

Critical Infrastructure:

Protecting critical infrastructure during a disaster can mean the difference between life and death. Critical infrastructure, which comprises the systems and assets vital to a community's economy, security, and public health, deserves special attention as regards disaster management mitigation.

Setting up protective measures that limit damage to water and wastewater systems or nuclear plants, for example, can prevent serious repercussions.

As an example, Japan experienced devastating physical and psychological consequences after a 2011 earthquake triggered a tsunami. The inundation of water cut off the power supply to the cooling system for Fukushima Daiichi reactors, leading to a massive nuclear accident.

Preparedness:

Well-coordinated responses to disasters require prior planning. This helps ensure fast, effective response efforts and limits duplicated efforts.

Disaster preparedness plans:

- Identify organizational resources
- Designate roles and responsibilities
- Create procedures and policies
- Organize activities that improve disaster readiness

Anticipating the needs of communities that disasters affect improves the quality of the response efforts. Building the capacities of volunteers, personnel, and disaster management teams to respond to disasters also makes the response efforts more effective.

Plans may include the following:

- Emergency shelter sites
- Evacuation routes
- Emergency energy and water sources

They may also address:

- Chains of command
- Training programs
- Communication procedures
- Emergency supply distribution
- Stockpile needs

Response and Recovery:
During and immediately after an emergency, disaster management focuses on delivering help and interventions that can save lives, safeguard health, and protect buildings, animals, and community property. Following an initial response, efforts shift toward supporting communities as they rebuild emotionally, economically, and physically.

Disaster Relief
Disaster relief addresses the immediate and short-term needs of disaster-affected communities. It can include evacuations, search and rescue missions, and emergency medical assistance.

Examples of disaster relief are:

- Setting up temporary shelters that provide a safe place to sleep, food, and emotional support from trained personnel
- Delivering meals and water
- Distributing emergency supplies and necessities, such as toiletries for hygiene and tarps, shovels, trash bags for cleanup efforts
- Providing emergency health services, such as first aid for injuries and prescription medication replacements

Rebuilding
Emergency management helps communities rebuild their lives after trauma. This involves longer-term efforts to restore:

- Housing
- Economies
- Infrastructure systems
- Individual and community health

Federal agencies and supporting organizations help communities with problem-solving and finding resources as they redevelop and revitalize.

Recovery assistance may include the following:

- Unemployment assistance
- Housing assistance
- Legal services
- Mental health counseling
- Disaster case management

Incident Response Plan:

An incident response plan is a set of written instructions that outline your organization's response to data breaches, data leaks, cyber attacks and security incidents.

Incident response planning contains specific directions for specific attack scenarios, avoiding further damages, reducing recovery time and mitigating cybersecurity risk.

Incident response procedures focus on planning for security breaches and how organization's will recover from them.

Without a formal IR plan in place, organizations may not detect attacks or may not know what to do to contain, clean up and prevent attacks when detected.

Importantance of Incident Response Plan:

Incident response planning is important because it outlines how to minimize the duration and damage of security incidents, identifies stakeholders, streamlines digital forensics, improves recovery time, reduces negative publicity and customer churn.

Even small cybersecurity incidents, like a malware infection, can snowball into bigger problems that ultimately lead to data breaches, data loss and interrupted business operations.

A proper incident response process allows your organization to minimize losses, patch exploitable vulnerabilities, restore affected systems and processes and close the attack vector that was used.

Incident response encompasses preparation for unknown and known cyber threats, reliably identifying root causes of security incidents and post-incident disaster recovery.

Responsible for Incident Response Planning:

Organizations should form a computer security incident response team (CSIRT) who is responsible for analyzing, categorizing and responding to security incidents.

Incident response teams can include:

- **Incident response manager:** oversees and prioritizes actions during detection, containment and recovery of an incident. They may also be required to convey high-severity incidents to the rest of the organization, customers, law enforcement, regulations and the public where applicable.
- **Security analysts:** support and work directly with affect resources, as well as implementing and maintaining technical and operational controls.
- **Threat researchers:** provide threat intelligence and context around security incidents. They may use third-party tools and the Internet to understand current and future threats. Organizations will often outsource this function if the expertise does not exist in-house. If this is your organization, look for tools or services that can automatically monitor for leak credentials, data leaks and third-party and fourth-party vendor security posture.

Tools are Available for Incident Response Teams:

There are tools and industry standards that can be helpful to incident response teams. Tools can be split into three categories:

1. Prevention
2. Detection
3. Response

For prevention, an organization may employ a security scanner and a data leak detection tool to prevent leaked credentials and other sensitive data being exposed due to poor S3 security or a lack of configuration management.

Detection could be covered by antivirus software, network intrusion detection systems, security incident and event management (SIEM) software or a vulnerability scanner that checks CVE.

A common response tool is remediation workflows where incident response teams can request remediation, track and close third-party attack vectors.

Reasons You Need an Incident Response Plan:

A strong incident response process can dramatically reduce the damage caused to an organization when disaster strikes. An incident response plan helps codify and distribute the incident response plan across the organization.

Here are the main reasons you must have a strong incident response plan in place:

1. **Prepares you for emergency**—security incidents happen without warning, so it's essential to prepare a process ahead of time
2. **Repeatable process**—without an incident response plan, teams cannot respond in a repeatable manner or prioritize their time
3. **Coordination**—in large organizations, it can be hard to keep everyone in the loop during a crisis. An incident response process can help achieve this
4. **Exposes gaps**—in mid-sized organizations with limited staff or limited technical maturity, an incident response plan exposes obvious gaps in the security process or tooling which can be addressed before a crisis occurs
5. **Preserves critical knowledge**—an incident response plan ensures critical knowledge and best practices for dealing with a crisis are not forgotten over time and lessons learned are incrementally added
6. **Practice makes perfect**—an incident response plan creates a clear, repeatable process that is followed in every incident, improving coordination and effectiveness of response over time
7. **Documentation and accountability**—an incident response plan with clear documentation reduces an organization's liability—it allows you to demonstrate to compliance auditors or authorities what was done to prevent the breach

UNIT-3:-

Business application management:

A business application is a collection of components that provides a business functionality that you can use internally, externally, or with other business applications. You can create business applications of individual components, which are related to each other.

For example, Order Management, Inventory Management, and Billing are business applications that might use individual components such as a Java EE application server, LDAP, and a database that runs on the Solaris server.

Business application is a type of a custom collection. You can also create the following types of custom collections:

- Collection, which is a group of any resources that you can select according to your needs.
- Access collection, which is a collection that is used to control the access to configuration items (CIs) and permissions to modify configuration items. You can create access collections only when data-level security is enabled.

The following methods are provided for creating business applications:

- By using grouping patterns in Data Management Portal.
- By using application descriptors.
- By using grouping patterns that are created with Java API and loaded by the bulk load program.

There are several stakeholder groups in AM, who should work as a team to reach critical decisions such as build or buy, whether an application should be modernized or replaced, or where the application should be hosted.

Some key stakeholders in AM are:

- **Application Manager/Application Analyst**: Owns the AM process and thus manages the overall application lifecycle. Typically, there would be one Application Analyst or a team of Application Analysts for each major application. Also responsible for performing skills gap analysis and acquiring needed skills or staff.
- **Business Unit Owners**: Business-level staff members who view applications and AM in terms of bottom-line benefits, increased productivity, impact on revenue, and improved competitive stance.
- **Developers/DevOps/DevSecOps**: This group of IT professionals are charged with the design, development, deployment, integration, security, and maintenance of applications.
- **Application users**: Users provide feedback on productivity and performance, and key concerns for users include privacy, and security of the applications.

Importance Of Business Application management:

Application management is a key factor in a business' ability to innovate. By ensuring that business functions are being properly addressed with modern applications, business process solutions can be brought to market more efficiently, quickly, and at a lower total cost. When applications are efficiently managed, more IT resources are available to focus on new business challenges and competitive issues.

Additionally, effectively managed applications are more reliable and less prone to failure that could lead to loss of functionality. Thus, application management can reduce the risk of downtime and improve overall business continuity.

By incorporating new capabilities and monitoring user issues, application management can provide an enhanced end-user experience, which not only increases productivity but also helps accelerate the adoption of new applications or features.

Work Of Business Application Management:

Traditionally, AM was part of the IT Infrastructure Library (ITIL) processes, specifically as part of the ITIL Process Map as outlined in the process overview of ITIL Application Management.

Once the build-vs-buy decision for a given application is made, AM stakeholders collaborate with technical teams including DevSecOps to ensure the requisite skills to design, test, manage, and improve the application's services are on hand or acquired and constantly refined to meet changing environment and needs. Note that the exact functions of an application management system are constantly evolving, just as application development methodologies have evolved from waterfall to agile to cloud-native.

Corporate Business Application Security:

To allow organizations using enterprise business applications to determine an achievable, tailored-to approach defining actionable targets and measurable results, with the capability to scale by strengthening people, leveraging processes, and enhancing the use of tools. The Core Business Application Security (CBAS) project is designed to combine different industry standards and expertise from various security professionals to provide a comprehensive framework to align enterprise application security measures with the organization's security strategy. As a result, a framework is created to improve the security governance of enterprise application technology.

Core business applications or enterprise business applications are beneficial to organizations in several ways. Some of these benefits include:

- Combining different business processes under one solution
- Improving business performance
- Higher productivity by eliminating redundant processes
- Flexibility and mobility
- Easier collaboration between different organizational teams
- Centralized data

Even though there are numerous benefits that these solutions have, security threats have not decreased. Maintaining, implementing, and deploying security controls and/or information security standards around such solutions is still facing challenges. Some of these challenges include:

- Little to no understanding of the solutions in place
- Security professionals not involved in the initial phases of deploying and implementing such solutions
- Security controls being built after the solution is operational and functional; causing a blow back from business units

Reasons Application Security is a Must for Your Business:

In this new digital world, every company is now a tech company. Whether it's an off-the-shelf software or custom-made ones, companies are using applications to help increase the efficiency of their processes. Because of this, investing in tech-related initiatives is a crucial step in a business's success.

However, all becomes moot when these applications and software are left in a vulnerable state. That's why prioritizing application security for your business is a must.

Let's go over in finer detail seven reasons every business needs to prioritize application security.

1. Every company is now a software company

Following the trends of going digital, companies have started to adopt different applications in their day-to-day operations. Over 100 billion hours have been spent on shopping apps in the retail industry, generating an 18% year-over-year increase. This upward trend can be seen in other industries as well, including banking and fintech, travel, health and fitness, restaurants, and entertainment.

With most things going online, businesses rely on software to help them stay on top of their tasks and upgrade their efficiency. Because of this, having robust application security can help your business do away with the inconveniences of insecure applications.

2. Hackers are always evolving

Technological advancements continue to push through as the world moves forward into the digital age. These have greatly shaped how people live their daily lives and organizations conduct their business.

However, malicious entities have also been adapting to the changes, threatening the cybersecurity of the business landscape. In fact, 2021 saw a 31% increase in security attacks compared to 2020.

Despite the cybersecurity enhancements and innovations, hackers find ways to adapt and create new strategies to overcome them. This has urged companies to employ stricter security measures in their business applications since these are where most vulnerabilities can be exploited.

3. **If you get hacked, you will pay (a lot more)**

Your business may face many repercussions with every data breach and other forms of cyber threats that occur. Based on projections, cybercrime costs may increase by 15% every year, amounting to $10.5 trillion by 2025.

Many factors can contribute to this rise in costs. For example, your business may experience a loss in revenue due to stolen data, loss of consumer trust, and even investors. Cyberthreats that have successfully infiltrated your systems may also cause brand damage, potentially causing customers to cut ties with your organization.

4. Automated AppSec can improve your team's workflow

Creating an application is already difficult, especially since developers have to create apps quickly to keep up with changing markets.

Often, a higher priority is given to the quality of critical business functions. The goal is toward the best user experience, leaving behind security measures at the back of their minds. Because of this, security teams are faced with a growing pile of issues they need to address.

Automated app security platforms like GuardRails can help secure your business as fast and as frictionless as possible. GuardRails' platform ensures the integrity of your applications and provides your team with a better workflow with fewer bugs to fix.

5. **Foster customer trust and confidence with AppSec**

Now more than ever, consumers are entrusting their sensitive data with their chosen merchants. For example, online shops and retail store applications include a database of their clients' credit or debit card information.

Unfortunately, this practice makes them vulnerable to data breaches and other types of cyber threats. In fact, approximately 1,243 security incidents resulted in a breach of 5.1 billion records in 2021.

Customers may become hesitant to give you sensitive information if your company does not have a robust system for cybersecurity. Application security can put your customers' worries at ease, knowing that you have the right measures to protect their data.

6.**AppSec keeps your business compliant with security regulations**

Apart from instilling customer trust and confidence, AppSec enables you to stay compliant with security regulations. Governments have become stricter with their enforcement of cybersecurity regulations such as HIPAA, PCI-DSS, and more, especially for organizations handling sensitive customer data.

Integrating AppSec in your workflow is a must since not doing so may leave your organization vulnerable to cyber attacks. When that happens, you may find yourself facing forensic investigations that may hamper other business activities. AppSec can also save you from fines and fees you may incur from not meeting the necessary security standards.

7. **Digital transformation is the next step**

The fast-changing business landscape has paved the way for many to integrate software and other necessary apps into their daily operations. For instance, businesses have started to digitalize their finance department to help their team become more efficient with their task. They have automated tasks that are tedious and prone to human error.

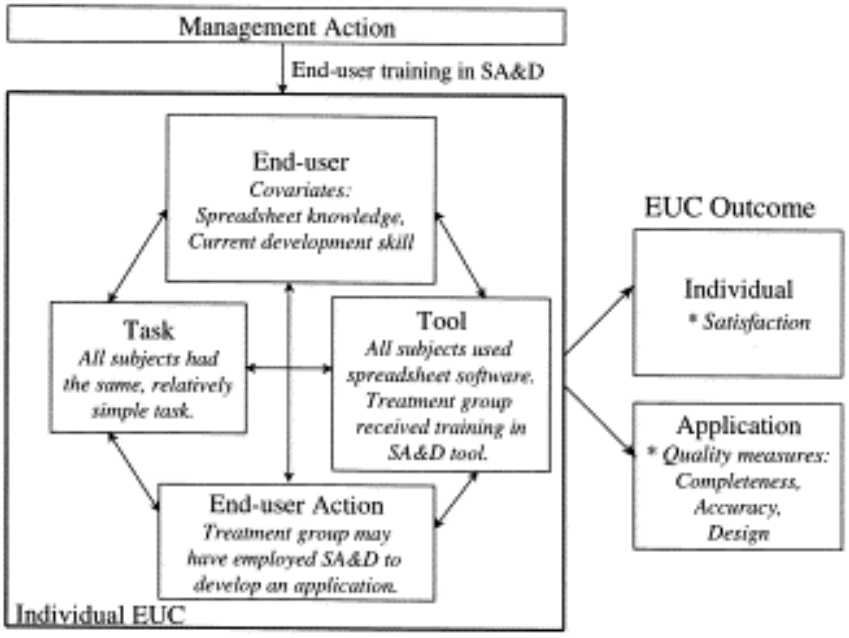
Enlisting the help of an application security provider can accelerate this digital transformation across the board by providing real-time visibility into your networks, apps, data, and more. As such, you can identify potential risks and vulnerabilities while gaining insights on how to best prepare and defend against cyber attacks.

End user Developed Applications:

End-user development refers to activities and tools that allow end-users – people who are not professional software developers – to create or modify system software.

User-Developed Applications (UDAs) typically consist of spreadsheets and databases created and used by end users to extract, sort, calculate, and compile organizational data to analyze trends, make business decisions, or summarize operational and financial data and reporting results:

Due to their unrestricted nature, User-Developed Applicatons allow relatively un-sophisticated computer users to write programs that represent complex data models, while shielding them from the need to learn lower-level programming languages. However, once end users are given freedom to extract, manipulate, summarize, and analyse their UDA data without assistance from IT personnel, end users inherit risks once controlled by IT.



These risks associated with User-Developed Applications

- Data security i.e. data confidentiality, integrity and availability.
- Data download issues
- Lack of structured development processes and change management controls
- Increasing complexity of the application
- Inefficient or ineffective development practices
- Lack of version control leading to multiple versions of the same application
- Lack of documentation

- Lack of support
- Limited input and output controls
- Lack of formal testing and acceptance

BUSINESS RISK OF USER DEVELOPED APPLICATIONS:

EUDAs present a significant business risk as they are very difficult to control.

- Employees typically work on Excel spreadsheets on their desktop computers which are manually downloaded and re-uploaded to file-sharing services.
- Two or more employees cannot work on the same document simultaneously.
- If systems to review and approve changes exist - they are typically manual and open to user error.
- Those reviewing EUDAs do not have strong tooling to track changes - monitoring changes to these documents is manual, painstaking work.
- It is difficult to make many small changes atomistically because of cumbersome review and approval processes.
- More complex EUDAs can take a long time to process and are prone to crashing due to logic errors or running out of memory.
- There is no effective way to separately test discrete logical components of an EULA.
- Unstructured development and lack of control for changes result outputs that are difficult to trust.
- Complexity increases as the business grows. If the business is successful it will outgrow its spreadsheet.
- No version control and regression testing resulting hard coded fixes and workarounds
- Lack or absence of documentation
- Lack or absence of internal data integrity checks
- Lack or absence of formal testing

Benefits of End User Development

There are perhaps thousands of distinct EUD platforms in common use, each with its own unique qualities. That said, there are some common traits that many of them share.

Easy for Beginners

EUD platforms usually present a low barrier to entry for those with fledgling technical skills. That means little or no coding background required and no need to grapple with intimidating technical documentation.

Programming by Example

Programming by example works by recording end users' actions. You simply “show” the application what to do in a certain context by performing the relevant actions, and the system is able to play them back in a repeatable way and even generalize the process to new cases.

Simple Presentation of Development Principles

In many cases, important software concepts are simplified. For example, common Excel functions like SUM, SUMIF, COUNT, COUNTIF, and VLOOKUP use conventional programming constructs like loops and conditional statements under the hood, but this is invisible to the user.

EUD is Often Visual

Some EUD platforms mainly rely on graphical interfaces. For example, you may work with visual elements like spreadsheet cells rather than abstract data types. Alternatively, there are entirely visual languages to represent programming logic, such as in Scratch.

A Diverse Ecosystem

End-user development is a catch-all term for a variety of different approaches for integrating development tools into user-friendly platforms. What counts as an "end user" can vary greatly as well. Moreover, sometimes standard programming languages are used for end-user development purposes.

Photoshop's support for JavaScript and other scripting languages is a good example. Another is system administrators' use of scripting languages like Perl or Python, which are powerful general-purpose programming languages, for routine automation of administrative tasks. The database query language SQL is used by professional software developers and database administrators to create and maintain databases used by complex systems and applications, but also by less technical business analysts (end users in this case) making simple queries to retrieve some data they would like to work on.

Disadvantages:

- Duplication or effort and waste of resources
- Greatly increased costs
- Loss of control over data
- Loss of control of quality in both programs and data
- Incompatibles prevent sharing
- Can be used to circumvent control processes, such as the steering committee
- Generally produces narrow, inflexible systems with short lives

Examples

- As mentioned above, Microsoft Excel is probably the most widely-used end-user development application. Workers around the world make use of functions, macros, and other tools every day.
- Adobe Photoshop has rich scripting functionality that you can use to automate common tasks or implement more complex functionality. The supported languages include JavaScript, AppleScript, and VBScript.
- Simple video game engines like RPG Maker are accessible to non-programmers.
- A variety of tools collectively known as **"no code" platforms** make it possible to develop apps without programming knowledge of any kind.

System Access:

System access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of system access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

How is access to IT systems and data controlled?

Over time the ways in which IT systems can be accessed has grown, and the job of securing those system and their data has become increasingly more complex. High-profile breaches have spawned a host of compliance regulations that further expanded the ways – and thus the complexities - in which organizations needed to secure their systems and protect sensitive data.

Access control systems perform identification authentication and authorization of users and entities by:

- Strengthening logon security through multi-factor authentication

- Restricting user privilege through elevated authority management solutions
- Granting requests for access to systems and data based on the identity of the user and the context of the request.

A complete system access control solution requires a layered defense to protect access control systems.

How is system access control performed?

System access control solutions determine how users are allowed to interact with specific systems and resources. A robust system access control regime gives an organization the ability to manage, restrict, and monitor user activity while protecting sensitive systems and data.

A robust system access control solution will intercept every request for access through network protocols, open source database protocols, communications ports, SQL statement, command lines and more, determine whether to grant or deny the request based on precise rules, and log both accepted and rejected access attempts.

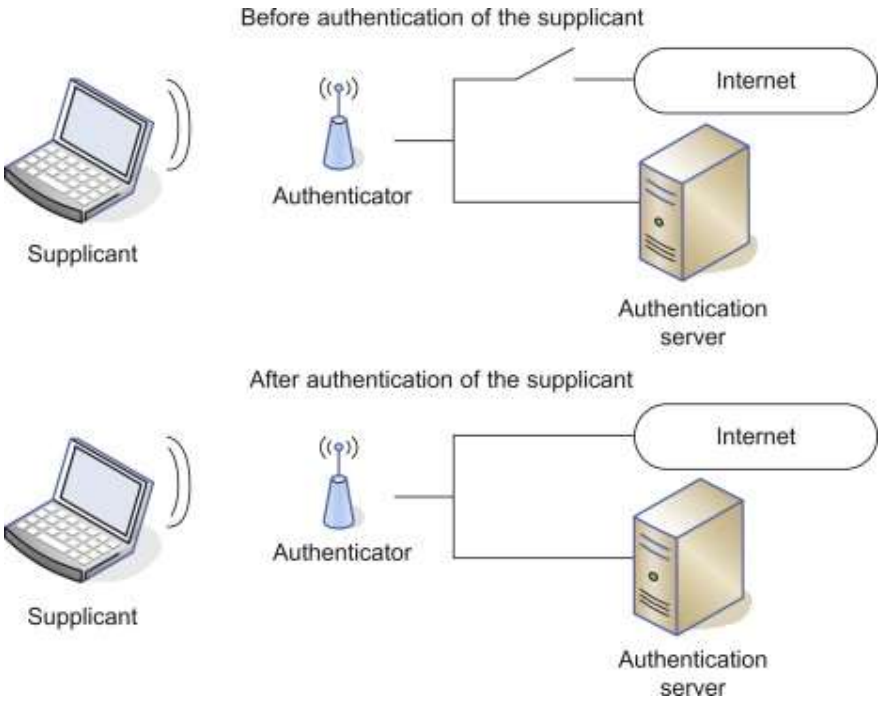
Authentication Mechanisms:

Authentication

Security Access Manager provides user authentication functions that allow for simple and complex authentication scenarios.

The users who want to access your protected resources can be challenged to provide credentials to authenticate with the various authentication technologies that are supported by Security Access Manager. The component responsible for this capability is called the Authentication Service. The Authentication Service consists of a framework you can use to enforce the execution of various supported authentication mechanisms to authenticate users.

Authentication mechanisms are modules that authenticate the user with a specific challenge or authentication technology, such as user name and password and one-time password. The order on which the authentication mechanisms are run is controlled by an authentication policy. An authentication policy is an XML document that you create with the authentication policy editor. The authentication policy dictates the order of authentication mechanisms to execute.



Authentication mechanisms

Security Access Manager provides the following authentication mechanisms:

One-time password authentication mechanisms

A one-time password is a password that is generated for an authentication event and is valid for one use. The one-time password authentication capability in Security Access Manager provides the following features:

- One-time password generation and validation with support for various implementations as provided.
- One-time password delivery with email and short message service (SMS) implementation.
- Time-based, counter-based, and RSA one-time password generation and validation that requires no delivery mechanism.

Username and Password mechanism

Users provide a user name and password.

HTTP Redirect mechanism

Use this mechanism to integrate a custom authentication mechanism into the workflow of an authentication policy. Users provide credentials that are required by the custom authentication mechanism.

Consent to device registration mechanism

Users provide consent to allow their device to be registered.

FIDO Universal 2nd Factor mechanism

Users authenticate through the use of registered FIDO Universal 2nd Factor tokens.

Authentication policies

By grouping the provided authentication mechanisms into the workflow of an authentication policy, you can achieve several types of authentication:

- **Simple authentication**

  Users provide basic identifying information such as a user name and password.

- **Step-up authentication**

  Users provide a specific type of credential usually to access sensitive resources. The users might be challenged to authenticate and provide an extra set of credentials to prove that they are allowed to access sensitive resources.

- **Multi-factor authentication**

  Users provide more than one type of credential to access a protected resource.

Each authentication policy has a unique identifier that you can use with an access policy or to start the authentication service directly without any prior access policy invocation.

Access Control:

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

Implementing access control is a crucial component of web application security, ensuring only the right users have the right level of access to the right resources. The process is critical to helping organizations avoid data

breaches and fighting attack vectors, such as a buffer overflow attack, KRACK attack, on-path attack, or phishing attack.

The most common types of access control systems:

Mandatory access control (MAC)

The mandatory access control system provides the most restrictive protections, where the power to permit access falls entirely on system administrators. That means users cannot change permissions that deny or allow them entry into different areas, creating formidable security around sensitive information.

It even restricts the resource owner's ability to grant access to anything listed in the system. Once an employee enters the system, they're tagged with a unique connection of variable "tags"—like a digital security profile—that speaks to what level of access they have. So depending on what tags a user has, they will have limited access to resources based on the sensitivity of the information contained in it. This system is so shrewd, in fact, that it's commonly used by government entities because of its commitment to confidentiality.

Discretionary access control (DAC)

A discretionary access control system, on the other hand, puts a little more control back into leadership's hands. They determine who can access which resources, even if the system administrator created a hierarchy of files with certain permissions. All it takes is the right credentials to gain access.

The only disadvantage, of course, is giving the end-user control of security levels requires oversight. And since the system requires a more active role in managing permissions, it's easy to let actions fall through the cracks. Where the MAC approach is rigid and low-effort, a DAC system is flexible and high-effort.

Role-based access control (RBAC)

Role-based access control attributes permissions to a user based on their business responsibilities. As the most common access control system, it determines access based on the user's role in the company—ensuring lower-level employees aren't gaining access to high-level information.

Access rights in this method are designed around a collection of variables that map back to the business—such as resources, needs, environment, job, location, and more. Many executives like this approach because it's simple to group employees based on the kind of resources to which they need access. For

example, someone in human resources does not need access to private marketing materials, and marketing employees don't need access to employee salaries. RBAC provides a flexible model that increases visibility while maintaining protection against breaches and data leaks.

ACCESS CONTROL PRINCIPLES:

Guiding principles that provide rules for all implementations of access to networks, systems, information and data. This can include principles relating to:

- Access approval by a registered owner (e.g. an information, business or system owner)
- The sharing of personal data
- Role and group based access

Components of Access Control:

Access control is managed through several components:

1. Authentication

Authentication is the initial process of establishing the identity of a user. For example, when a user signs in to their email service or online banking account with a username and password combination, their identity has been authenticated. However, authentication alone is not sufficient to protect organizations' data.

2. Authorization

Authorization adds an extra layer of security to the authentication process. It specifies access rights and privileges to resources to determine whether the user should be granted access to data or make a specific transaction.

For example, an email service or online bank account can require users to provide two-factor authentication (2FA), which is typically a combination of something they know (such as a password), something they possess (such as a token), or something they are (like a biometric verification). This information can also be verified through a 2FA mobile app or a thumbprint scan on a smartphone.

3. Access

Once a user has completed the authentication and authorization steps, their identity will be verified. This grants them access to the resource they are attempting to log in to.

4. Manage

Organizations can manage their access control system by adding and removing the authentication and authorization of their users and systems. Managing these systems can become complex in modern IT environments that comprise cloud services and on-premises systems.

5. Audit

Organizations can enforce the principle of least privilege through the access control audit process. This enables them to gather data around user activity and analyze that information to discover potential access violations.

Access Control Models:

1. **Attribute-based Access Control (ABAC):** In this model, access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.
2. **Discretionary Access Control (DAC):** In DAC, the owner of data determines who can access specific resources.
3. **History-Based Access Control (HBAC):** Access is granted or declined by evaluating the history of activities of the inquiring party that includes behavior, the time between requests and content of requests.
4. **Identity-Based Access Control (IBAC):** By using this model network administrators can more effectively manage activity and access based on individual requirements.
5. **Mandatory Access Control (MAC):** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
6. **Organization-Based Access control (OrBAC):** This model allows the policy designer to define a security policy independently of the implementation.
7. **Role-Based Access Control (RBAC):** RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
8. **Rule-Based Access Control (RAC):** RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.

Examples of access control systems:

- **Password** - A word or set of letters, numbers, and symbols.
- **Access card** - Size of a credit card, with a magnetic strip or computer chip, swiped through or placed next to a card reader.
- **Security fob** - A device with a RF security chip inside, placed next to security fob reader.

- **Fingerprint reader** - Scans a person's fingerprint, which is different for each person.
- **Palm reader** - Scans the palm of a person's hand, which is unique for each person.
- **Voice recognition** - Usually requires a person to say their name, a specific sentence or series of words, to recognize the person's unique voice pattern.
- **Retina scan** - A scan of the eye, specifically the retina, which is unique for each person.
- **DNA scan** - Much more sophisticated and futuristic, requiring sample of saliva or blood to check for and verify the person's DNA.

Systems management:

Systems management is the facilitation of IT systems throughout a company, office, data center, or other organization. The IT team overseeing systems management is responsible for everything from ordering computer equipment and maintaining networks to troubleshooting and setting up automation. In short, systems management is the brain working behind the scenes to ensure your important IT functions are firing on all cylinders.

The purpose of systems management:

The purpose of systems management is to keep networks, technology, and overall IT infrastructures running smoothly.

In a basic office setting, systems management could be as simple as having a single IT person who works on the website, keeps software updated across the office, and supports the rest of the staff's tech needs. On a more complex level, it could include a whole team responsible for managing servers, setting up robotic process automation, and programming AI.

Systems management covers a variety of tasks, including:

- **Security:** Systems management includes data- and network security-related operations and assets like firewalls, virus protection software, 2FA, password/login standards, phishing detection, and even the physical security of hardware.

- **Asset inventory:** An organization's hardware, software, and digital assets also fall under systems management, including servers, computers, files, and product licenses.
- **User management:** All the logins, permissions, and subscriptions for the SaaS products, applications, devices, and software used across an organization fall into this category.
- **Backup and recovery:** Systems management also covers fail-safety measures like data backup and recovery procedures.
- **Data analytics:** Processes for extracting, logging, transferring, synthesizing, and analyzing data also fall under systems management.
- **Automation:** IT teams work together with other teams in an organization to set up and refine triggers that automatically execute tasks and processes like reporting, notifications, emailing, and logging data.
- **Capacity forecasting:** Will your current data center support your needs in 10 years? Five years? Next year? Systems managers can assess your infrastructure at scale to help sustain your growth.
- **Cloud management:** Whether it's public, private, or both, whatever your cloud computing needs are, good systems management can ensure you've got the security, utility, and capacity you need.
- **Help desk:** For organizations with client-facing support ticketing, systems management includes issue resolution processes.
- **Interoperability:** Effective systems management ensures that all of your separate software and applications play well together and fit neatly into your workflows.
- **Education:** IT teams help train team members on how to use software and hardware and can train them on security best practices.

- **Compliance:** Each of these responsibilities also has to maintain compliance, and IT teams have to be particularly cognizant of compliance as it relates to user data.

Common challenges when implementing systems management:

Just like implementing a change in mindset, systems management implementations can cause a little friction. Here are a few potential challenges you might face when implementing a new system or IT management approach.

- **Learning curve:** Any changes that come along with systems management may need additional training to execute. Within IT teams affected by those systems or changes that come from them, there may be resistance to alterations in job roles or processes.
- **Added complexity:** It's often easier not to implement systems management strategies like automation or enhanced security, but the more complex workflows can be well worth it. Systems that lead to more efficiency should even simplify workflows down the road.
- **Cost:** Good systems management costs money. Period. Specialized hires for IT teams may fetch high salaries, and the software and hardware needs required to scale can also add up.
- **Implementation:** As systems management needs grow, organizations may run into roadblocks with existing applications and utilities. Interoperability can become an issue if changes aren't carefully considered early on.
- **Strain on current IT team:** Existing teams may become overburdened by growing systems management needs.

Systems management best practices

No matter what your IT needs are, you can promote sound systems management with these strategies:

- **Consult IT teams on requirements:** Nobody knows your systems management requirements better than your IT team. They can advise on network, interoperability, hardware, and utilization requirements to set a baseline.
- **Consult IT teams on budgets:** Decision-makers should never assume their current teams have all the resources they need for continued growth. By consulting IT managers, they can solidify timelines and budgets for putting systems management plans into action.
- **Consider frameworks:** Like a template, an established framework can help keep teams on track with a proven, pre-set structure like FCAPS for network security, FMEA for compliance, or COBIT for IT governance.
- **Align goals with strategic vision:** Communicate across teams to understand overall strategic visions and organizational growth goals so that systems management goals can help advance them.
- **Set attainable goals:** Since goals should be both attainable and measurable, consider another framework like ITIL for setting values and measurables. Including IT teams will help ensure their viability and timelines.

choosing a systems management software

Thinking about upgrading software or adding a new application? Consider consulting with your IT team or network admin on these points:

- **IT budget:** Will licensing fees, registration costs, necessary hardware, or network upgrades fit into the budget? Will you need new hires?

Budgeting for systems needs can be complex, and costs can add up quickly.

- **Timelines:** You may need lengthy runways to account for onboarding, training, and early troubleshooting that could eat into productivity.
- **Existing resources:** Take stock of all your current resources like applications, hardware, and staff certifications and skills. Make sure they can support your new software before committing to it.
- **Interoperability potential:** If there are applications you depend on that would be a headache to change, your new software should be able to integrate with them.
- **Size and scale:** The size of your organization, the number of users who will need accounts for the new software, and your scale plans should all factor into the software choice and its pricing model.

Systems management tools and ITSM products

Integrating the right systems management tools can help your IT team operate more efficiently, which in turn helps the rest of your organization. IT support management (ITSM) products can help:

- Alleviate IT pain points
- Improve network reliability and performance
- Maximize automation and AI capabilities
- Enhance security
- Cut operating costs

Advantages

Below are some advantages of using the systems approach to management:

Simplicity: With only five components and a few foundational principles, it's easy to understand this approach. The basic concept of interconnectedness is also quite intuitive and can make sense.

Comprehensive troubleshooting: If you encounter a problem with one aspect of an organisation, systems theory dictates that it might have a cause elsewhere or that its effects might impact other areas of the organisation. This makes it much less likely that you'd adopt a narrow view when troubleshooting.

Transparency: When you and others in the organisation agree that everything is interrelated, there's a greater incentive for cooperation and transparency.

Disadvantages

Below are some of the key disadvantages of this framework:

Vague: This approach is so simple that it's hard to refute. While this makes it more convincing, it does limit its utility in more complex scenarios.

Inadequate for complex organisations: In smaller organisations, you can usually identify the components of a system quite easily. Conversely, in large organisations with large departments performing multiple functions, the distinction between these components becomes less clear.

Limited: Although it can describe the basics of organisational structure and function, it excludes a lot of elements that you may want to understand or explain, such as organisational hierarchies or inequalities. It, therefore, provides no techniques or solutions, only a framework for describing system elements.

Virtual Servers:

A virtual server replicates the same functionality as a physical server. However, multiple virtual servers can be applied to a pool of servers. Virtual servers may be applied against a bare metal computer which allows for its operating system and interfaces to integrate into the physical server's resources.
There are many services today that allow for a physical to virtual (P2V) server migration to occur. These can range from simple and free, to quite expensive and feature rich.

A virtual server re-creates the functionality of a dedicated physical server. It exists transparently to users as a partitioned space inside a physical server. Virtual servers makes it easy to reallocate resources and adapt to dynamic workloads. Ultimately, a virtual server is meant to make the best use of the overall physical compute resources, thus providing a better return on investment for each organization.

Types of virtual servers:

There are a few different methods of providing a virtual server, these are known in the industry as type-1 and type-2. Type-1 is a native or bare-metal virtual server that runs directly on the host server's hardware to control, manage the resources and the guest operating systems. Popular examples of this would be something like VMWare ESXi or Microsoft Hyper-V, and Oracle VM.

Type-2 is a hosted solution that runs on a conventional operating system, the same as other programs do. This means that the guest operating system runs on top of the host operating system. Examples of this are Parallels Desktop, VirtualBox, and VMWare Workstation.

1.Full virtualization:

This is outlined above as a type-1 method. This full virtualization will run directly on the machine's physical hardware. There isn't an underlying operating system. This provides the virtual server with direct access to the hardware without any other software getting in the way. Because of this, system administrators and IT professionals often find that this is the most efficient way of performing virtualization. The type-1 or full virtualization is how most enterprise organizations run their virtual servers.

Type-1 virtual servers are often more secure because the hypervisor that controls the virtualization runs directly on the physical hardware.

2.OS-level virtualization:

This is outlined above as the type-2 method. Type 2 is sometimes called a hosted hypervisor or an OS-level virtualization. This is because the overall virtual server relies on the existing host machine's operating system to run.

This has an impact on computer resources such as processing, memory, storage, and networking resources.
You're unlikely to see a large enterprise running type-2 hypervisors and are normally reserved for client systems or end-user systems.

These solutions are often used because the cost of entry is significantly less. Sometimes, IT professionals use type-2 virtual servers to create virtual desktops.

3.Para-virtualization:

There is a possible third option; para-virtualization. Para-virtualization also uses a hypervisor, but the virtual servers do not fully emulate the physical host's hardware. Instead, a para-virtualization hypervisor will take advantage of an application programming interface (API) – typically integrated into modern servers – and it directly exchanges calls to the host and virtual server operating systems. The resulting virtual servers recognize their environment as an extension of the host's resources.

4. Hardware-Assisted Virtualization:

With hardware-assisted virtualization, the division of resources needed to support multiple VMs is already built into the CPU of the host server. This allows virtual machines to communicate directly to the main server rather than entirely through the hypervisor. It's a way to partially cut out the middleman, though a hypervisor is still needed. Since the path between the virtual machines and the physical server is more direct, the hypervisor uses a very significant amount of the server's resources. This makes it seem like the virtual machines are running directly on the server.

5. Hypervisor-Based Virtualization:

With hypervisor-based virtualization, software (the hypervisor) virtually emulates the hardware of the main server, basically acting like the physical machine on which operating systems can run. The hypervisor allocates resources of the physical server across the various guest virtual machines.

Full virtualization and para-virtualization are types of hypervisor-based virtualization. Hardware-assisted virtualization is a type of hybrid virtualization that is hypervisor-based as well as hardware-based.

Virtual server management best practices:

There are different ways to manage and maintain your virtual server but here are some of the best practices that I've found over the past 20 years:

- Ensure that all the hardware used in the solution is on the hardware compatibility list for that specific version of your hypervisor. There is nothing worse than going to a client site or working on a slow hypervisor because non-compatible hardware has been used.

- Ensure that the hardware choice meets your minimum configuration requirements. 'Measure twice and cut once' is the old saying and this is very true here. Make sure that you don't under specify the hardware required. It's always better to have too much than too little.

- When building virtual servers for production and enterprise systems, it's best practice to test the memory for 72 hours to make sure there aren't any hardware issues.

- Always make sure your software is kept up to date. Most modern solutions will support N-1, that being N=the current version and -1 being one

- previous. This helps with the performance, security, and supportability of the virtual servers.

Advantages :

Virtual server advantages

- Reduction of cost and cost efficiencies: By partitioning physical servers and increasing the number of virtual servers running on a single box. The roles and responsibilities increase dramatically.

- Resource isolation can occur: By supplying more than one set of services, virtual servers can be spun up quickly, development and pre-production

environments can be created at a moment's notice. The testing within independent environments ensures that things like software and development aspects don't affect all users.

- It's good for the environment. The reduction of physical hardware means that it's less likely to wind up in landfills, less likely to be running at low utilization, less likely to require upgrading constantly on a rolling lease or outright purchase. It's cheaper and more efficient to run a well-specified server at a higher utilization than it is to run several physical servers at nearly zero.

Disadvantages:

Virtual server disadvantages

- Spinning up virtual servers has similar limitations as a physical one, particularly if a single or a group of virtual servers are very hard working. This leads to something called resource hogging; too many servers running on a single or pool of virtual servers causes it to limit the amount of processing power available to it. The good news is that with a correctly designed solution this doesn't occur. Correctly setting up the solution and with forethought in the design will ensure that capacity isn't going to be an issue when your servers grow to scope the size of your business.

Network Storage Systems:

Network attached storage (NAS) is a centralized, file server, which allows multiple users to store and share files over a TCP/IP network via Wifi or an Ethernet cable. It is also commonly known as a NAS box, NAS unit, NAS server, or NAS head. These devices rely on a few components to operate, such as hard drives, network protocols, and a lightweight operating system (OS).

• **Hard drives or hard disk drives (HDDs):** HDDs provide storage capacity for a NAS unit as well as an easy way to scale. As more data storage is needed, additional hard disks can be added to meet the system demand, earning it the name "scale-out" NAS. More modern systems leverage flash storage in combination with HDDs or as a standalone configuration. The use case for the NAS device usually determines the type of HDD used. For example, sharing

large media files, such as streaming video, across an organization requires more resources than a file system for a single user at home.

• **Network Protocols:** TCP/IP protocols –i.e. Transmission Control Protocol (TCP) and Internet Protocol (IP)—are used for data transfer, but the network protocols for data sharing can vary based on the type of client. For example, a Windows client will typically have a server message block (SMB) protocol while a Linux or UNIX client will have a network file system (NFS) protocol.

• **Operating System:** While standard operating systems can handle thousands of requests, the NAS OS restricts the system to two types of requests, data storage and file sharing.

As businesses also seek to leverage emerging technologies, such as AI, machine learning, and edge computing, these workloads will need to be stored together to facilitate insights and learning. Finally, NAS systems are also commonly used to support cloud storage providers, acting as a data backup, archiving, and disaster recovery system.

Importantance of network storage:

It is accepted that data is a critical asset for companies

Without access to their corporate data, companies may not be capable of serving their customers with the expected level of service. Poor customer service, loss of sales, or even business liquidation can be the result of corporate information not being available.

But it is equally true that in most businesses, the focus is not on the storage, but on the applications that consume it. Additionally, small businesses find themselves faced with other demands such as:

- Simplified operation (many small businesses do not have IT staff)
- Accessibility, reliability and availability of applications and systems for day-to-day operations
- Easy to use security, backup and recovery to protect application data
- Availability of a wide range of applications to support their business needs

NAS implementations:

- There are two types of NAS implementations: integrated and gateway. The integrated NAS device has all of its components and storage system

in a single enclosure (package). In gateway implementation, NAS head shares its storage with SAN environment.

1. Integrated NAS:

- An integrated NAS device has all the components of NAS, such as the NAS head and storage, in a single enclosure, or frame. This makes the integrated NAS a self-contained environment. The NAS head connects to the IP network to provide connectivity to the clients and service the file I/O requests. The storage consists of a number of disks that can range from low-cost ATA to high throughput FC disk drives. Management software manages the NAS head and storage configurations.
- An integrated NAS solution ranges from a low-end device, which is a single enclosure, to a high-end solution that can have an externally connected storage array.
- A low-end appliance-type NAS solution is suitable for applications that a small department may use, where the primary need is consolidation of storage, rather than high performance or advanced features such as disaster recovery and business continuity. This solution is fixed in capacity and might not be upgradable beyond its original configuration. To expand the capacity, the solution must be scaled by deploying additional units, a task that increases management overhead because multiple devices have to be administered.
- In a high-end NAS solution, external and dedicated storage can be used. This enables independent scaling of the capacity in terms of NAS heads or storage. However, there is a limit to scalability of this solution.

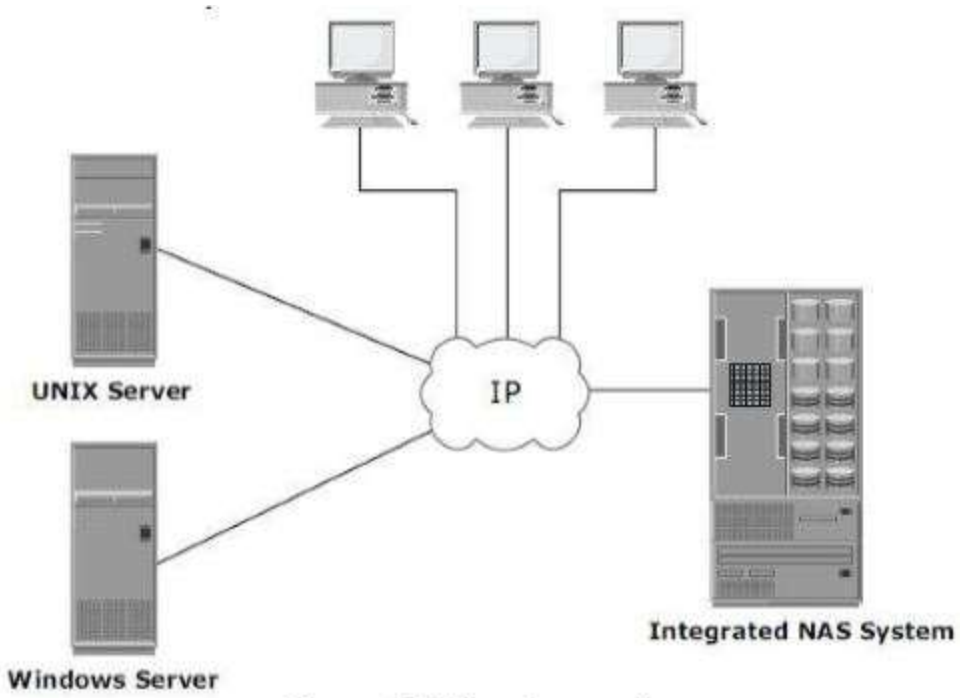


Figure: NAS implementation

2. Gateway NAS:

- A gateway NAS device consists of an independent NAS head and one or more storage arrays. The NAS head performs the same functions that it does in the integrated solution; while the storage is shared with other applications that require block-level I/O. Management functions in this type of solution are more complex than those in an integrated environment because there are separate administrative tasks for the NAS head and the storage. In addition to the components that are explicitly tied to the NAS solution, a gateway solution can also utilize the FC infrastructure, such as switches, directors, or direct-attached storage arrays.
- The gateway NAS is the most scalable because NAS heads and storage arrays can be independently scaled up when required. Adding processing capacity to the NAS gateway is an example of scaling., adding capacity on the SAN independently of the NAS head. Administrators can increase performance and I/O processing capabilities for their environments without purchasing additional interconnect devices and storage. Gateway NAS enables high utilization of storage capacity by sharing it with SAN environment.

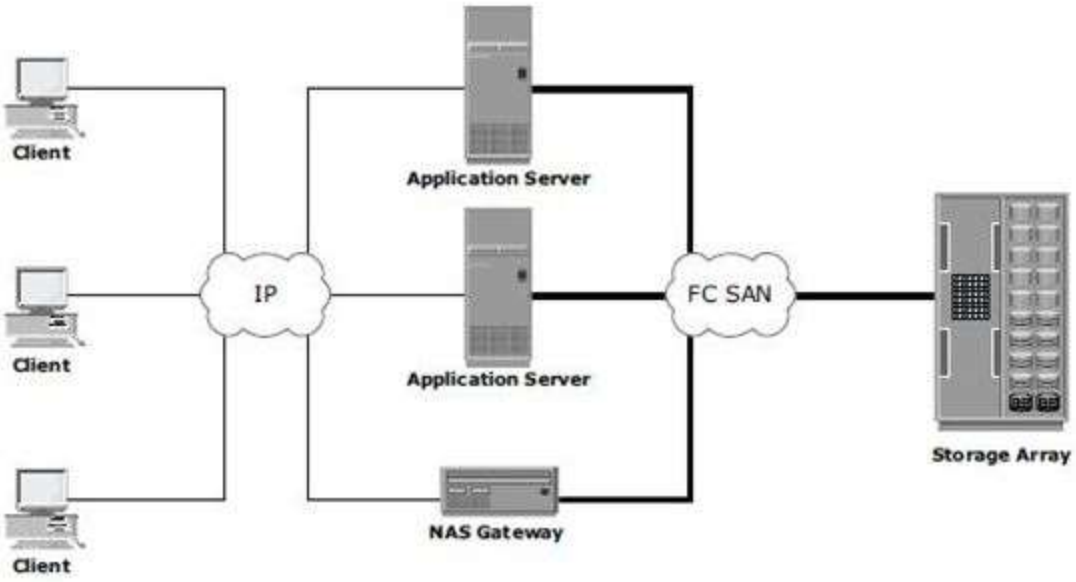


Figure: Gateway NAS connectivity

Advantages of NAS:

- Relatively inexpensive
- A self-contained solution
- Ease of administration
- It is multi-protocol
- A wide array of system and size to choose from
- Drive failure tolerant storage volumes
- Automatic backup to other devices and the cloud.
- Easy to install and configure
- 24/7 and remote data availability
- More flexible than DAS
- It requires some knowledge of computer network to use them efficiently
- Universal client access
- With NAS you will get the same speed of data transfer as DAS that is faster
- The user who wants their data processed directly because will need to do it through installed OS

Disadvantages of NAS:

- Performance depends on the protocol
- Slow down for video application or multiple large files

- It is file oriented
- Increased LAN traffic
- The file transfer speed is not as fast as DAS
- Limited scalability
- Additional Input-output processing
- System available features depend upon the NAS chip and firmware
- For using NAS device people should know some basic knowledge about computer networking

Network Management Concepts:

- Network management includes all of the tools, processes, and procedures that are used to monitor, configure, and maintain an organization's network infrastructure. Network management systems continuously poll network elements to improve reliability, performance and security of the network. Here we discuss what network management is, and demonstrate the importance of an integrated network security solution.
- Network management refers to two related concepts. First is the process of configuring, monitoring, and managing the performance of a network. Second is the platform that IT and NetOps teams use to complete these ongoing tasks.

Network configuration is the process of assigning network settings, policies, flows, and controls. In a virtual network, it's easier to make network configuration changes because physical network devices appliances are replaced by software, removing the need for extensive manual configuration.

Network configuration

Network configuration can also be automated and managed via a centralized configuration manager network configuration manager, further reducing manual IT workload and making it easier to:

- **Maintain** a network
- **Make** configuration changes
- **Relaunch** devices
- **Track** and report data

Some network configuration basics include switch/router configuration, host configuration, software and firewall configuration, and network topology which can be controlled through rest APIs.

configure a network switch and router

When setting up a network switch and router, it's important to customize settings and apply all necessary configurations to ensure that your network will work properly. Some of the configurable settings on a network switch and router include:

- **IP address**—for identification
- **Password**—for added security
- **Channel and band selection**—to improve performance
- **Default gateway**—to make the device visible to network management tools
- **Neighbor discovery**—for added visibility
- **Correct time**—for proper troubleshooting and detailed error logs

A network configuration manager is the easiest way to perform network switch configuration and apply these settings consistently to every device on your enterprise network.

Network monitoring:

Network monitoring is the process of constantly monitoring a computer network for problems such as slow traffic or component failure. Network Monitoring tools are always scanning the network and are designed to automatically notify network administrators via text, email, or other application such as Slack when a problem occurs. Network monitoring software differs from network security or intrusion detection systems in that network monitoring is focused on internal network issues such as overloaded routers, server failures, or network connection issues that could impact other devices.

Network monitoring solutions can also initiate failover to remove problem device or circuits from duty until remediation can be performed to repair the issue. Ideally, a proactive network monitoring solution will prevent downtime or

failures before they occur by identifying anomalies that could lead to outage if unchecked.

Network Monitoring should provide:

- Visualization of the organization's complete IT and network infrastructure
- Monitoring, troubleshooting, and remediation of network performance issues.
- Root cause analysis tools when problems occur.
- Dashboard with clear visualization tools and reports

Network managing

Networks are managed via a centralized network management solution. This solution is responsible for monitoring the state of the network and taking action to improve network security and performance.

Elements of a Network

- Network management solutions deal with all aspects of a network, such as:

- **Network Devices:** Network devices are all of the systems that are connected to the corporate network. This includes user workstations, servers, and security solutions like firewalls.
- **Network Types:** Network management solutions apply to all different "types" of networks, including LANs, WANs, and VPNs.
- **Network Structures:** Network management requires understanding network communications using models, such as the OSI model of network layers.

How Networks Are Managed

It accomplishes this by periodically polling devices on the network for data of interest. After collecting this data, the management station processes the collected information to determine the current state of the network as a whole

and the individual devices connected to it. Based on this information, the network management platform can take action to correct issues or otherwise ensure the performance and security of the network.

Network management is a solution that bridges the gaps between various vendors, devices, and environments. In order to achieve the visibility needed, network management platforms use vendor-neutral protocols like the simple network management protocol (SNMP) to communicate with all systems on the network. Another option is to gather information from an agent installed on the device.

Common Network Management Tasks

Network management consists of a variety of different tasks. The ISO Telecommunications Management Network model breaks network management tasks into five categories:

- **Fault:** Fault management is designed to identify, track, and manage fault events to minimize potential disruption to the network.

- **Configuration:** Configuration management includes both setting up initial configuration settings for a network and performing change management of network configurations over time.
- **Accounting:** Accounting tasks involve collection of usage statistics to help improve the utility of the network.
- **Performance:** Performance management is focused on ensuring that the network meets service level agreements (SLAs) and otherwise operates at an acceptable level.
- **Security:** Network security management is designed to control access to the corporate networks and the assets and data linked to it.

Each of these categories includes a number of different sub-tasks. For example, network security management incorporates tasks like the deployment

of next-generation firewalls (NGFWs) and implementing encryption of sensitive data in the corporate network.

Features

There are various features of network management which are as follows −

Network automation

One defining feature of a modern network management system is network automation. This is the procedure of automating the configuring, handling, testing, deploying, and operating of physical and virtual devices inside a network. Network service availability increases when everyday network tasks and functions are automated and repetitive processes are controlled and managed automatically.

Network administration

Network administration encompasses tracking network resources, including switches, routers, and servers. It also includes performance monitoring and software updates.

Network Operation

This contains smooth network functioning as created and intended, including close monitoring of activities to quickly and effectively address and fix problems as they occur and preferably even before users are aware of the problem.

Network assurance

Network assurance features are often included in modern network management systems. These features help improve network performance, customer experience, and security. Assurance systems help network analytics, application analytics, and policy analytics, as well as AI and ML, to achieve full network assurance.

Network provisioning

Network provisioning involves network resource configuration for the purposes of supporting any given service, like voice functions or accommodating additional users.

Network maintenance

Network maintenance covers upgrades and fixes to network resources. It also consists of proactive and remediation activities executed by working with network administrators, such as replacing network gear like routers and switches.

Network analytics

Network analytics is a software tool that compares incoming information against preprogrammed operational models and makes functional decisions for improving network performance.

Advantages:

1. **Network Visibility**

   Among the primary benefits of network management is that it provides visibility into the network. Having the ability to monitor a network is a foundational component of good IT best practices.

2. **Downtime Detection**

   The ability to detect if part or the whole network is down is another key benefit of network management. Downtime is a business-critical event for organizations and being able to quickly detect and remedy network downtime is of utmost importance.

3. **Performance Optimization**

   A slow network can also have a significant effect on an organization. The ability to identify and optimize network performance is another benefit of network management technology and its tools.

Disadvantages:

1. **Ephemeral IP Addresses**

   Identifying network devices and users was traditionally done via an IP address. With virtualized and container-based applications, the use of ephemeral or elastic IP addresses can represent a challenge for identifying users, applications and services.

2. **Multi-site Network Administration**

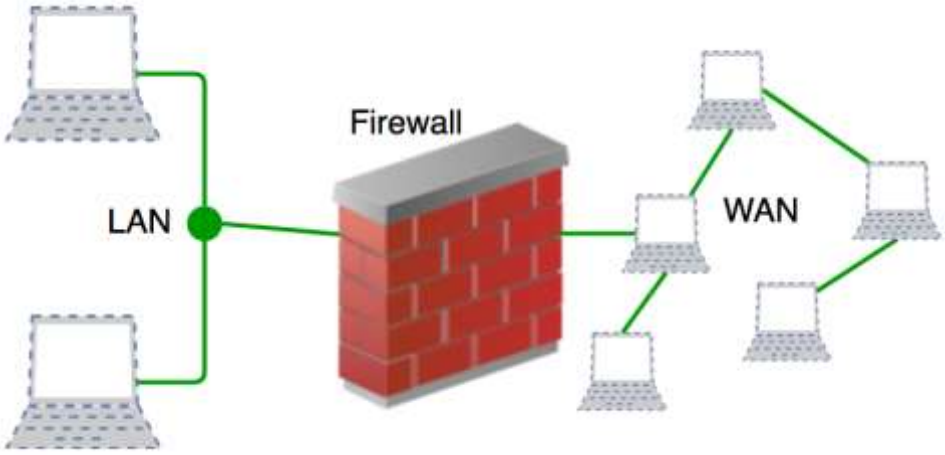
   Larger networks that span multiple physical and virtual deployments can be complex to manage.

3. **Cloud and Hybrid Deployments**

   Modern organizations typically use a mix of on-premises and cloud services. Having visibility and control over both types of networks in a unified approach can be a challenge.

Firewall:

A Firewall is a network security device that monitors and filters incoming andoutgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sitsbetween a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.



.

Its purpose is to create a barrier between your internal network and traffic that flows in from external sources – like the rest of the internet. This blocks hackers, viruses and other malicious traffic.

There are pre-set rules to analyze and filter traffic, rerouting data that comes from suspicious or unsecured sources in order to prevent attacks on your network.

Firewalls protect your website against the following:

- **Brute Force Attacks:** Hackers who try hundreds of username and password combos to discover your login credentials.
- **DDoS Attacks:** An attack that sends thousands (or even millions) of fake packets to cause server overload and take your site down.
- **Intrusions:** Unauthorized users who try to access your computer or server.

- **Malware:** Attackers who want to infect your device or server with malware, which can steal your personal information, harm your computer and even spread to other devices.

Protecting a own server firewall:

If a hacker makes their way into a web server, they can change your website login credentials, ruin or remove your website and even add malware to your site that will infect your visitors' devices. You can kiss traffic and sales goodbye if that happens.

Unless you're protecting your own server, these are the types of firewalls to look for:

Personal:

Instead of being for a network or web server, a personal firewall is meant for just one computer. You probably already have this – it usually comes standard with a Mac or Windows computer, as well as with antivirus software.

Personal firewalls do the following:

- Analyze all incoming and outgoing traffic, as well as whether or not the connection with your device's apps is safe.
- Protect the ports that you use when connecting with websites and applications. The attackers can't see that those ports are open when they're in use.
- Prevent hackers from accessing and taking control of your computer.
- Defend against attacks that happen to get through.

Web Application

Even if a firewall monitors network traffic, it may not detect traffic that comes from an app, service or software. That's what application firewalls are for – to catch malicious attempts against software or older firewalls.

Web application firewalls (WAFs) work in a similar way, but they're specifically designed to monitor web apps, not computer apps. Examples of web apps are third-party forms and shopping cart plugins. When a web app gets hacked, malware is sent to the server.

WAFs are usually cloud-based, making them easier to set up because you don't have to do anything on the server level, but they may also be part of a

hardware firewall. Also, remember that application monitoring is often part of a next-generation firewall.

Different types of firewalls:

Proxy firewall
An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall
Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall
A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Next-generation firewall (NGFW)
Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.
According to Gartner, Inc.'s definition, a next-generation firewall must include:

- Intelligence-based access control with stateful inspection
- Integrated intrusion prevention system (IPS)
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats
- URL filtering based on geolocation and reputation

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
- Better detect evasive or suspicious activity with network and endpoint event correlation
- Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
- Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

Virtual firewall

A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (Amazon Web Services or AWS, Microsoft Azure, Google Cloud Platform or GCP, Oracle Cloud Infrastructure or OCI) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software-defined networks (SDN).

Learn about Cisco virtual firewalls for public cloud and private cloud.

Cloud Native Firewall

Cloud native firewalls are modernizing the way to secure applications and workload infrastructure at scale. With automated scaling features, cloud native firewalls enable networking operations and security operations teams to run at agile speeds.

How Does a Firewall Work?

How does a firewall work? Firewalls work by inspecting packets of data and checking them for threats to enhance network security. They can check the contents of the data, the ports it uses to travel, and its origin to see if it poses a danger. Further, next-generation firewalls (NGFWs) use machine learning to detect patterns of data behavior that may signify anomalous—and dangerous—activity. These capabilities can prevent several kinds of attacks.

Backdoors

Backdoors are a form of malware that allow hackers to access an application or system remotely. Firewalls can detect and stop data that contains backdoors.

Denial of Service

Denial-of-service (DoS) attacks overwhelm a system with fake requests. You can use a network firewall with an access control list (ACL) to control which kinds of traffic are allowed to reach your applications. You can also use a web application firewall (WAF) to detect DoS-style traffic and stop it from impacting your web app.

Macros

Macros can be used by hackers to destroy data on your computer. A firewall can detect files with malicious macros and stop them from entering your system.

Remote Logins

Firewalls can prevent people from remotely logging in to your computer, which can be used to control it or steal sensitive information.

Spam

Spam, which involves unwanted emails being sent without the consent of the recipient, can also be stopped by firewalls. An email firewall can inspect incoming messages and detect spam using a predesigned assortment of rules.

Viruses

Viruses copy themselves and spread to adjacent computers on a network. Firewalls can detect data packets containing viruses and prevent them from entering or exiting the network.

Advantages of Cloud Native Firewalls

- Agile and elastic security
- Multi-tenant capability
- Smart load balancing

Advantages of using Firewall

1. **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known

malware or other security concerns, assisting in the defense against these kinds of attacks.

3. **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
4. **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.
5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **Complexity:** Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.
2. **Limited Visibility:** Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.
3. **False sense of security:** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.
4. **Limited adaptability:** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
5. **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.
6. **Limited scalability:** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
7. **Limited VPN support:** Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.
8. **Cost:** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

IP Security:

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection

.

Components of IP Security

It has the following components:

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

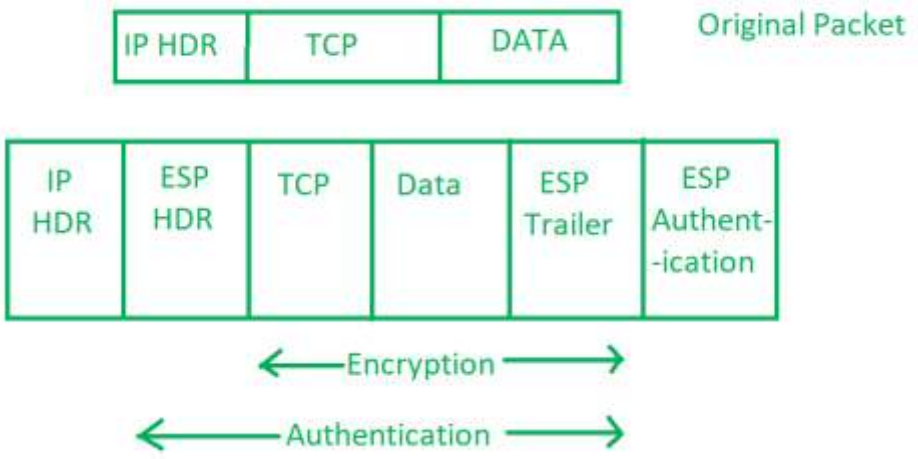
1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

(IP Header)

3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet

Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.

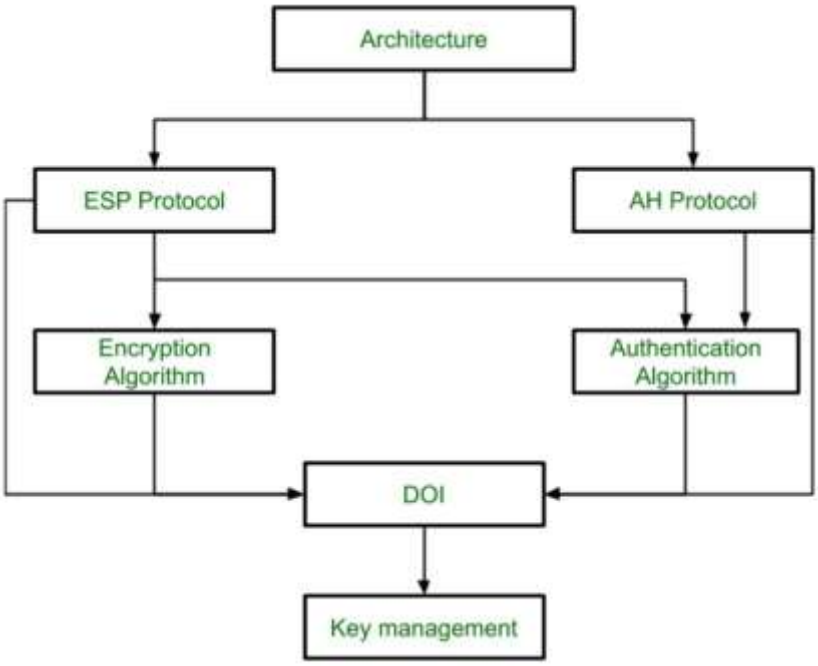


(Packets in Internet Protocol)

IP Security Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authenticity
- Integrity



(IP Security Architecture)

Working on IP Security

- The host checks if the packet should be transmitted using IPsec or not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
- Then IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode provides greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
- The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
- Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms.
- Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
- When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both hosts.

Features of IPSec

1. **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
2. **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
3. **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
4. **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
5. **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
6. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
7. **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Advantages of IPSec

1. **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2. **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4. **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5. **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

1. **Configuration complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
2. **Compatibility issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3. **Performance impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4. **Key management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.

5. **Limited protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

Electronic Communications:

Electronic communication can be defined as, the communication which uses electronic media to transmit the information or message using computers, e-mail, telephone, video calling, FAX machine, etc. This type of communication can be developed by sharing data like images, graphics, sound, pictures, maps, software, and many things.
Because of this e-communication, there is a lot of changes have occurred in work areas, society, etc. Thus, people can simply access global communication with no physical movement. Please refer to this link to know about – Electronic Communication Protocols

Types of Electronic Communication

Electronic communication can be classified into different types like messaging, voice call, e-mail, social media, etc. We know that e-communication has changed due to the way public interact and communicate with each other for different purposes like personal or business. By using this, it is very simple to communicate with the world.

E-Mail
E-Mail or electronic mail is the most used type of electronic communication. By using this communication, one can send a message to another person through a mail immediately. For that, we need to create an account to send an e-mail, media files, photos, documents, etc. This type of communication has replaced many conventional types of communication due to many benefits.

So this type of communication is more suitable for different methods of communication. The benefits of this communication are ease of usage, completely free, etc. Additionally, this type of electronic communication doesn't affect the surroundings.

Messaging
This type of communication allows people to interact with others who are far away from us. This is possible only due to technology as well as usage of the internet. There are different types of messengers are available like Skype, Windows Live, Gmail, etc. These messengers help in chatting or sending messages to our beloved ones or friends.

There are many benefits by using this kind of communication like the message which we sent & the response are immediate. But in some cases, some files include nil although bug can stop the functioning of your computer by giving you lots of trouble.

Blogging

At present, blogging is the most preferable communication method. This is a type of online journaling, which can be updated daily, or many times a day. It covers all the information or a particular topic.

By using such blogs, one can share, follow, or even post comments. This kind of communication is extremely suitable. This is the reason why people utilize blogs very often. Additionally, by using the internet, people can access, read & follow it worldwide.

Video Chat

This type of communication can be done by adding web cameras for video calling application. By using this application, one can communicate with others and also they can observe with whom they are speaking. The webcam can be connected to the computer externally and also we need to use applications like Skype, Hangouts, etc.

There are many benefits to using video chatting. We can contact anybody immediately. We can communicate with more than one person at a time by using the feature like business conference feature. Also, we can share PPTs, data sheets online.

Social Networking

Social media is one kind of communication between people, which is used with their general advantage otherwise for relationships. In this, mostly Facebook, as well as LinkedIn, give places for people to work together, sometimes in real-time. There is a Micro-blogging service namely Twitter, which allows the short message of more than 140 characters to be transmitted to a huge audience.

Not like text messages, it sends to simply tiny groups. The posts like Microblog are intended to be seen by all the followers and users can repost texts that they desire to share with their followers. Therefore, a microblog post can reach rapidly and a viral post is s message which reports widely.

Telex

This is a significant device for current electronic communication. This system uses a teleprinter to communicate from one position to another using a machine. It includes mainly two parts like keyboard transmitter as well as a receiver.

Whenever a text is to be sent, then the user presses a push-button, and stays for the call tone, calls the number preferred & enters the massage on a tiny paper strip at the end of receiver end because it is entered within the creating office. This method is the quickest & most exact methods for exchanging written posts.

Fax

The Fax machine is a kind of communications and use of this is increasing gradually to transmit materials which are visual like illustrations, diagrams, picture, etc. Here, this machine can be connected using a telephonic.

The transmitted document can be fed throughout the machine, after that it is scanned electronically & signals are broadcasted to the end of receiver wherever an equal document copy is replicated on a plain paper sheet using the receiving machine.

This machine has made it achievable to send important documents copies which include testimonials, certificates, degrees, contracts, agreements from one location to another in a telephone call speed. Because of this reason, it is a commonly used technique for communication.

Multimedia

The multimedia is one kind of communication system and it is an excellent innovation to improve the communication system. This is a blend of several media which bring mutually to transmit messages. The multimedia mainly includes a photo, graphics, voice, music, animation, and message. Whenever all these media are located jointly otherwise computer screen then becomes multimedia. This can be used efficiently for marketing and advertising campaigns.

IMPORTANCE OF ELECTRONIC COMMUNICATION IN BUSINESS

Electronic communication can be achieved by finding the right tool for communication. Moving from paper to electronic communications can actually help your business connect easier, while saving time and money.

Email, instant messaging, websites, blogs, text messaging, voicemail and video messaging are a few examples of electronic communication. Electronic communication has changed the way businesses communicate with each other. Electronic communication can be very beneficial if used effectively. Knowing the strengths and weaknesses will help businesses conduct effective electronic communication.

One weakness of electronic communication is the lack of communication support. In a face-to-face conversation nonverbal communication, such as tone of voice and body language, help to clarify the message you are sending. This lack of communication support can lead to messages becoming misinterpreted.

ADVANTAGES OF ELECTRONIC COMMUNICATION

- **Speedy transmission**: It requires only a few seconds to communicate through electronic media because it supports quick transmission.
- **Wide coverage**: The world has become a global village and communication around the globe requires only a second.
- **Low cost**: Electronic communication saves time and money. For example, text SMS is cheaper than the traditional letter.
- **Exchange of feedback**: Electronic communication allows the instant exchange of feedback. So communication becomes perfect using electronic media.
- **Managing global operation**: Due to the advancement of electronic media, business managers can easily control operation across the globe. Video or teleconferencing e-mail and mobile communication are helping managers in this regard.

DISADVANTAGES OF ELECTRONIC COMMUNICATION

- **The volume of data:** The volume of telecommunication information is increasing at such a fast rate that business people are unable to absorb it within the relevant time limit.
- **The cost of development:** Electronic communication requires huge investment for infrastructural development. Frequent change in technology also demands further investment.
- **Legal status:** Data or information, if faxed, may be distorted and will cause zero value in the eye of law.
- **Undelivered data:** Data may not be retrieved due to system error or fault with the technology. Hence required service will be delayed.
- **Dependency:** Technology is changing every day and therefore poor countries face the problem as they cannot afford the new or advanced technology. Therefore poor countries need to be dependent towards developed countries for sharing global network.

Case study on OWASP vulnerabilities using OWASP ZAP tool:

Case study on OWASP vulnerabilities:

#1. Broken Access Control

Access control systems are intended to ensure that only legitimate users have access to data or functionality. Vulnerabilities in the broken access control category include any issue that allows an attacker to bypass access controls or that fails to implement the principle of least privilege. For example, a web application might allow a user to access another user's account by modifying the provided URL.

#2. Cryptographic Failures

Cryptographic algorithms are invaluable for protecting data privacy and security; however, these algorithms can be very sensitive to implementation or configuration errors. Cryptographic failures include a failure to use encryption at all, misconfigurations of cryptographic algorithms, and insecure key management. For example, an organization might use an insecure hash algorithm for password storage, fail to salt passwords, or use the same salt for all stored user passwords.

#3. Injection

Injection vulnerabilities are made possible by a failure to properly sanitize user input before processing it. This can be especially problematic in languages such as SQL where data and commands are intermingled so that maliciously malformed user-provided data may be interpreted as part of a command. For example, SQL commonly uses single (') or double (") quotation marks to delineate user data within a query, so user input containing these characters might be capable of changing the command being processed.

#4. Insecure Design

Vulnerabilities can be introduced into software during the development process in a couple of different ways. While many of the vulnerabilities on the OWASP Top Ten list deal with implementation errors, this vulnerability describes failures in design that undermine the security of the system. For example, if the design for an application that stores and processes sensitive data does not include an authentication system, then a perfect implementation of the software as designed will still be insecure and fail to properly protect this sensitive data.

#5. Security Misconfiguration

In addition to its design and implementation, the security of an application is also determined by how it is configured. A software manufacturer will have default configurations for their applications, and the users may also enable or disable various settings, which can improve or impair the security of the system. Examples of security misconfigurations could include enabling unnecessary applications or ports, leaving default accounts and passwords active and unchanged, or configuring error messages to expose too much information to a user.

Ways to Plan a Vulnerability Test Over a Web Application Using OWASP ZAP:

The world has seen a substantial rise in web applications in the last few years. Many of these applications may carry vulnerabilities that can threaten their security. OWASP ZAP (Zed Attack Proxy) is a popular application security testing tool that can be used to find such vulnerabilities in a web application. Some of the common issues detected by OWASP ZAP web application testing include SQL injection, data exposure, broken authentication, and cross-site scripting. Maintained by a team of non-profit expert volunteers at OWASP (Open Web Application Security Project), the tool is open-source and free for all.

Some Key Features of The OWASP ZAP Scanner

1. The OWASP ZAP vulnerability scanner is a dynamic tool that can work in both test and production environments. This means that you do not have to wait for the deployment of an app before you can scan it for security issues. It is a time-saver if you are looking to build and test at the same time.
2. Secondly, it is designed in such a way that even non-security professionals such as developers and functional testers can use it. It is a flexible cross-platform product that can be used with either Windows, Linux, or Mac OS. And because it is an open-source project, it is always improving and enhancing its repository.

How to Use the OWASP ZAP Vulnerability Scanner to Plan A Vulnerability Test?

The OWASP ZAP tool captures the request just before hitting the network, which allows to analyze the various parameters, header values in the request. It then explores and attacks it to find security issues that need redressal. In the process, it records the requests and responses on every page and sends out alerts when it encounters an issue.

Below are the steps on how to initiate the OWASP ZAP penetration testing using a Windows system:

1. Starting the OWASP ZAP UI

To start a vulnerability test using the OWASP ZAP web application scanner, you need to download the tool and install it. It is platform agnostic and hence you can set it up on either Windows, Mac OS, or Linux. However, if you are using Windows or Linux, you should also have Java 8+ already installed on your system. After installation, click on the OWASP ZAP icon on your desktop. Now, click on the 'start' button on the start-up dialog box, to launch the ZAP UI.

Upon running the interface, a pop-up window will ask if you want to save the session. For a new session, choose the default option 'No, I do not want to persist the session'.

2. Initiating a Scan

You can start scanning your web application by using the QuickStart automated scan. With QuickStart, you can scan an application just by entering its URL and pushing the 'attack' button, which makes it quite simple to execute.

You can use passive scanning as well, which is one of the most interesting features of the OWASP ZAP scanner. The tool records all the requests received by the application and its responses. It then issues an alert if any anomaly is observed with either the request or the response. However, it cannot detect an issue such as an SQL injection attack. Instead, you can use the active scanning feature to find out the vulnerabilities not found through passive scanning. During an active scan, ZAP can simulate a real attack against some specific areas of your application to understand the response.

Additionally, the ZAP scanner can be used in different modes like:

- The standard mode which allows you to use every feature of the tool
- You can also use attack mode to run active scans.
- The safe mode turns off the harmful features while the protected mode lets you scan chosen websites within a defined scope.

The OWASP ZAP scanner can also spider or crawl all over a web app and create a map for it. Spidering allows you to look for issues that get missed when you are not scanning all the aspects of your web app. The tool provides the best results when spidering is combined with manual scanning.

Manual scanning can be started by clicking on the 'manual explore' button and entering the destination URL in the 'URL to explore' text box. Then, you must select the browser and click on the 'launch browser' action button. You will then be ready to explore the web application through the browser, while the tool also passively scans and reports for any issues as you explore.

There are several more options with the OWASP ZAP scanner that you can explore to increase the level of security of your web applications. To understand how to keep your web and mobile applications safe, reach out to a reliable security advisor like Indusface now.

UNIT-4:-

Supply Chain Management:

Supply chain management is the management of the flow of goods and services and includes all processes that transform raw materials into final products. It involves the active streamlining of a business's supply-side activities to maximize customer value and gain a competitive advantage in the marketplace.

- Supply chain management (SCM) is the centralized management of the flow of goods and services and includes all processes that transform raw materials into final products.
- By managing the supply chain, companies can cut excess costs and deliver products to the consumer faster and more efficiently.
- Good supply chain management keeps companies out of the headlines and away from expensive recalls and lawsuits.
- The five most critical elements of SCM are developing a strategy, sourcing raw materials, production, distribution, and returns.
- A supply chain manager is tasked with controlling and reducing costs and avoiding supply shortages.
- Supply chain management is the process of integrating the supply and demand management, not only within the organization, but also across all the various members and channels in the supply chain so they work together most efficiently and effectively.
- There are **five basic components in a supply chain management system**:
- **1. Planning**
- To meet customer demands, supply chain managers have to plan ahead. This means **forecasting demand**, designing the supply chain intentionally, and determining how the organization will measure the supply chain to ensure it is performing as expected in terms of efficiency, delivering value for customers and helping to achieve organizational goals.
- **2. Sourcing**
- Selecting suppliers who will provide the goods, raw materials, or services that create the product is a critical component of the supply chain. Not only does this include creating the contracts that govern the suppliers, but also managing and monitoring existing relationships. As part of **strategic sourcing**, supply chain managers must oversee the processes for ordering, receiving, managing inventory and authorizing invoice payments for suppliers.

- **3. Making**
- Supply chain managers also need to help coordinate all the steps involved in creating the product itself. This includes reviewing and accepting raw materials, manufacturing the product, quality testing and packaging. Generally, businesses evaluate the quality, production output and employee productivity to ensure overall standards are upheld.

- **4. Delivering**
- Ensuring the products reach the customers is achieved through **logistics and it's fundamental to supply chain success**. This includes coordinating the orders, scheduling delivery, dispatching, invoicing, and receiving payments. Generally, a fleet of vehicles must be managed to ship the products—from tankers bringing product manufactured overseas to fleet trucks and parcel services handling last mile delivery. In some cases, organizations outsource the delivery process to other organizations who can oversee special handling requirements or home delivery.

- **5. Returning**
- Supply chain managers also need to develop a network that supports returning products. In some cases, this may include scrapping or re-producing a defective product; in others, it may simply mean returning a product to the warehouse. This network needs to be responsible and flexible to support customer needs.
- The foundation for each of these components is a solid network of supporting processes that can effectively monitor the information across the supply chain and assure adherence to laws and regulations. This involves a wide number of departments, including HR, IT, quality assurance, finance, product design and sales, according to **CIO**.

Types of Supply Chain Models

Supply chain management does not look the same for all companies. Each business has its own goals, constraints, and strengths that shape what its SCM process looks like. In general, there are often six different primary models a company can adopt to guide its supply chain management processes.

- **Continuous Flow Model:** One of the more traditional supply chain methods, this model is often best for mature industries. The continuous flow model relies on a manufacturer producing the same good over and over and expecting customer demand will little variation.
- **Agile Model:** This model is best for companies with unpredictable demand or customer-order products. This model prioritizes flexibility, as a company may have a specific need at any given moment and must be prepared to pivot accordingly.

- **Fast Model:** This model emphasizes the quick turnover of a product with a short life cycle. Using a fast chain model, a company strives to capitalize on a trend, quickly produce goods, and ensure the product is fully sold before the trend ends.
- **Flexible Model:** The flexible model works best for companies impacted by seasonality. Some companies may have much higher demand requirements during peak season and low volume requirements in others. A flexible model of supply chain management makes sure production can easily be ramped up or wound down.
- **Efficient Model:** For companies competing in industries with very tight profit margins, a company may strive to get an advantage by making their supply chain management process the most efficient. This includes utilizing equipment and machinery in the most ideal ways in addition to managing inventory and processing orders most efficiently.
- **Custom Model:** If any model above doesn't suit a company's needs, it can always turn towards a custom model. This is often the case for highly specialized industries with high technical requirements such as an automobile manufacturer.

Supply Chain Manager Responsibilities:

The supply chain manager coordinates, organizes and manages all logistics involved in the production and distribution process of a company's goods. According to the BLS, supply chain managers oversee the entire life cycle of a product. The following are their main responsibilities:

• Create business relationships with suppliers and clients. Supply chain managers must be excellent networkers and understand the demands of the client in order to meet their needs.

• Direct allocation of materials, supplies, and products. Supply chain managers must be successful leaders to lead teams, manage a financial budget, and develop a product that meets the needs of current and future clients.

• Develop high-quality products. Supply chain managers need to develop and deliver high-quality products as efficiently as possible. They are required to continuously review logistical functions and identify areas of improvement. It is their responsibility to propose strategies to minimize the cost of time required to deliver goods.

Importantance:

Supply chain management is crucial for any organization because doing it well can introduce several benefits to the organization; however, poor supply chain management can result in very expensive delays, quality issues, or reputation. In some cases, poor supply chain management can also cause legal issues if suppliers or processes are not compliant. Technology advances have unlocked huge potential for supply chain management, enabling supply chain managers

to work closely – and in real time – with members of the supply chain. With supply chain management, organizations can:

- Anticipate problems
- Dynamically adjust prices
- Improve inventory and fulfillment

Examples of Supply Chain Management

For example, Walmart linked its POS system to notify its distribution centers to send additional products to the stores when individual P&G products ran low. If the distribution center fell below its threshold, an automatic alert was sent to the P&G distribution center to ship additional product.

This constant cycle of communication helps balance manufacturing so inventory can meet demand without reaching excess and enables billing and payment to become automated processes.

Benefits of Supply Chain Management

Effective supply chain management provides **three primary benefits to an organization**, according to MSU's online Supply Chain Management I course.

1. Lowered Costs

By integrating supliers and applying technology, organizations can lower operating costs by responding more dynamically to customer needs. For example, managing based on demand keeps organizations from over-producing, which not only reduces labor and raw materials costs, but also cuts down on inventory management costs and transportation costs.

2. Increased Revenue

When organizations use technology to stay closer to customer demand and respond more quickly (as in the Walmart example keeping shelves stocked), it's more likely products remain available for customers to purchase. When manufacturing is streamlined to produce just enough, labor and materials can be devoted to developing new items to offer the customer and expand the product mix. Outside the product realm, this may mean offering additional services customers.

3. Asset Utilization

With effective supply chain management, organizations can use capitol assets, like production or transportation equipment, most effectively. Rather than

adding wear and tear to manufacturing equipment needlessly, businesses can produce to the need.

Supply chain management allows organizations to deliver more quickly, ensure products are available, reduce quality issues, and navigate returns with ease, ultimately improving value, both within the organization and for the customers.

The Disadvantages of Utilizing Improper Supply Chain Management

The main disadvantages of utilizing improper supply chain management (SCM) pertains to the following:

- **Improper Implementation** - Changing a supply chain management system requires three things: financial investment, time, and human resources. If implementation is not conducted properly, there will be wasted labor, service redundancy, and missed deadlines that may be potentially result in significant costs. In order to avoid these costs, high-quality logistics providers will complete a thorough analysis before implementing changes to the supply chain. This ensures that they fully understand the client's freight schedule, consolidation opportunities, and last-mile logistics needs before they develop and implement a new system.
- **Inadequate Training** - Inadequate training is by far one of the most common mistakes that companies can make when implementing a new system into a working supply chain. In order to avoid this mistake, make sure and spend money and time on a detailed and planned training program for employees to ensure that they understand what exactly is needed. This will ensure that there are no costly mistakes and will decrease excessive employee turnover within your manufacturing operation.
- **"One & Done" Mentality** - Short-sighted logistics providers miss out on consolidation opportunities and other ways to potentially improve their clients supply chain efficiency. The initial savings are realized, but any additional savings or growth opportunities will get neglected. A company that relies on this form of provider will eventually fall behind competitors. In order to avoid this, focus on continual analysis. This pushes you to always look for new methods to reduce their clients' supply chain expenses and improve efficiency.

Cloud Security:

Cloud security is a discipline of cyber security dedicated to securing cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms. Securing these systems involves the efforts of cloud providers and the clients that use them, whether an individual, small to medium business, or enterprise uses.

Cloud providers host services on their servers through always-on internet connections. Since their business relies on customer trust, cloud security methods are used to keep client data private and safely stored. However, cloud security also partially rests in the client's hands as well. Understanding both facets is pivotal to a healthy cloud security solution.

At its core, cloud security is composed of the following categories:

- Data security
- Identity and access management (IAM)
- Governance (policies on threat prevention, detection, and mitigation)
- Data retention (DR) and business continuity (BC) planning
- Legal compliance

Cloud security is the whole bundle of technology, protocols, and best practices that protect cloud computing environments, applications running in the cloud, and data held in the cloud. Securing cloud services begins with understanding what exactly is being secured, as well as, the system aspects that must be managed.

The full scope of cloud security is designed to protect the following, regardless of your responsibilities:

- **Physical networks** — routers, electrical power, cabling, climate controls, etc.
- **Data storage** — hard drives, etc.
- **Data servers** — core network computing hardware and software
- **Computer virtualization frameworks** — virtual machine software, host machines, and guest machines
- **Operating systems (OS)** — software that houses
- **Middleware** — application programming interface (API) management,
- **Runtime environments** — execution and upkeep of a running program
- **Data** — all the information stored, modified, and accessed
- **Applications** — traditional software services (email, tax software, productivity suites, etc.)
- **End-user hardware** — computers, mobile devices, Internet of Things (IoT) devices, etc.

Types of Cloud Security Tools:

Various types of cloud security tools and technologies exist within the cloud to ensure straightforward and reliable data protection.

Various types of cloud security tools and technologies exist within the cloud to ensure straightforward and reliable data protection.

1. 2-Factor Authentication

With 2-Factor Authentication (2FA) cloud users can validate all logins and passwords from any geographic location using their personal devices. This extra level of protection ensures that only those approved by the organization can access cloud data. As the workforce continues to migrate to remote or hybrid models, 2FA allows for enhanced security without requiring employees to access material from specific locations or devices.

2. Encryption

Encryption is an incredibly advantageous piece of cloud security. The encryption process transforms data into unreadable formats before transferring and storing it in the cloud. Without an encryption key, content on the cloud becomes indecipherable to attackers and, therefore, ineffective.

3. Data Loss Prevention

Data loss prevention (DLP) ensures your organization's data stays safe, at rest and in transit, from both internal and external threats. DLP also protects data from accidental exposure. DLP solutions provide visibility and control in SaaS and IaaS applications.

4. Privileged Access Management

The rise in contractors and remote workers means organizations don't need to share a single workspace or account. Thus, privileged access has begun to expand its parameters. Along with 2FA, privileged access management can help validate and verify users and their activity.

5. Cloud Security Monitoring & Vulnerability Management

Cloud security monitoring solutions allow you to supervise both on-premises and virtual servers to increase visibility across the infrastructure. These services provide continuous data monitoring, integrating seamlessly with your organization's existing services to identify threats and vulnerabilities.

Cloud security challenges:

Since data in the public cloud is being stored by a third party and accessed over the internet, several challenges arise in the ability to maintain a secure cloud. These are:

- **Visibility into cloud data** — In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.
- **Control over cloud data** — In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.
- **Access to cloud data and applications** —Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.
- **Compliance** — Use of cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may need to adhere to regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as requirements from internal teams, partners and customers. Cloud provider infrastructure, as well as interfaces between in-house systems and the cloud are also included in compliance and risk management processes.
- **Cloud–native breaches** – Data breaches in the cloud are unlike on-premises breaches, in that data theft often occurs using native functions of the cloud. A Cloud-native breach is a series of actions by an adversarial actor in which they "land" their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, "expand" their access through weakly configured or protected interfaces to locate valuable data, and "exfiltrate" that data to their own storage location.
- **Misconfiguration** – Cloud-native breaches often fall to a cloud customer's responsibility for security, which includes the configuration of the cloud service. Research shows that just 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as the front door to a Cloud-native breach, allowing the attacker to successfully land and then move on to expand and exfiltrate data. Research also shows 99% of misconfigurations go unnoticed in IaaS by cloud customers. Here's an

excerpt from this study showing this level of misconfiguration disconnect:

- **Disaster recovery** – Cybersecurity planning is needed to protect the effects of significant negative breaches. A disaster recovery plan includes policies, procedures, and tools designed to enable the recovery of data and allow an organization to continue operations and business.
- **Insider threats** – A rogue employee is capable of using cloud services to expose an organization to a cybersecurity breach. A recent McAfee Cloud Adoption and Risk Report revealed irregular activity indicative of insider threat in 85% of organizations.

Advantages of Cloud security :

1. **Efficient recovery –**
   Cloud computing conveys quicker and more exact recoveries of applications and information. With less downtime, it is foremost productive recuperation arrange.
2. **Openness –**
   Get to your data wherever, at whatever point. A Web cloud framework increases benefit and commerce capability by ensuring that your application is constantly accessible. This takes under consideration basic participation and sharing between clients in different regions.
3. **No material required –**
   Since everything will be encouraged within cloud, a physical stockpiling community is never once more critical. In any case, it might justify considering a support in case of a calamity that seem moderate down your business' effectiveness.
4. **Preferred position –**
   Straightforward execution – Cloud encouraging grants an organization to keep up comparative applications and trade shapes without managing with specialized parts of back-end. Easily managed over Web, a cloud establishment is viably and quickly accessible to organizations.
5. **Cost per head –**
   Advancement overhead is kept to a base with cloud encouraging organizations, allowing organizations to utilize additional time and resources to make strides trade system. Versatility for improvement. The cloud is successfully versatile with objective that organizations can include or subtract resources as demonstrated by their necessities. As organizations create, their system will development with them.

Disadvantages of Cloud security :

1. **Bandwidth issues –**
   For perfect execution, clients need to arrange in like manner and not pack

expansive sums of servers and capacity gadgets into a little set of information centers.

2. **Without excess –**
   A cloud server is not one or other overabundance nor reinforced. Since development can bomb to a awesome degree, go without from getting seared by buying an overabundance course of action. Whereas this can be an additional cost, much of time it is defended, in spite of all inconvenience.
3. **Data transfer capacity issues –**
   For idealize execution, clients ought to plan moreover and not gather colossal amounts of servers and capacity contraptions in a small course of action of server ranches.
4. **More control –**
   At the point once you move organizations to cloud, you move your data and information. For organizations with insides IT staff, they won't have choice to bargain with issues all alone. Be that because it may, Stratosphere Systems has an all day, each day live helpline that can address any issue right absent.
5. **No Redundancy –**
   A cloud server isn't excess nor is it supported up. As innovation may fall flat here and there, maintain a strategic distance from getting burned by obtaining a excess arrange. In spite of fact that it is an additional taken a toll, in most cases it'll be well worth it.

Security Architecture:

While security architecture has many definitions, ultimately it is a set of security principles, methods and models designed to align to your objectives and help keep your organization safe from cyber threats. Security architecture translates the business requirements to executable security requirements.

A cyber security architecture is the foundation of an organization's defense against cyber threats, and ensures that all components of its IT infrastructure are protected. Environments that are secured by a cyber security architecture include:

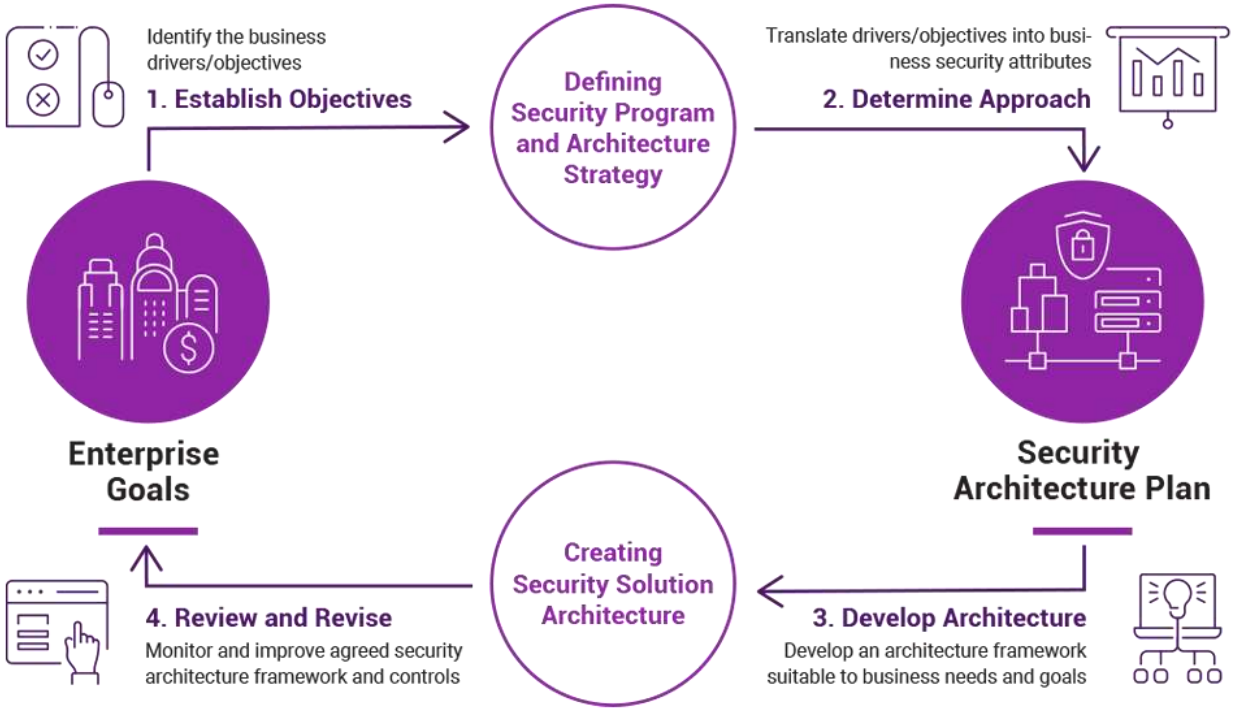
- Cloud
- Networks
- IoT

- Endpoints
- Mobile

When a cyber security architecture adheres to all seven principles of the Zero Trust security model (devices, people, data, networks, workload, automation & orchestration, visibility & analytics) an enterprise can secure data and IT resources wherever they reside.

THE ELEMENTS OF SECURITY ARCHITECTURE:

As we noted, security architecture has a number of definitions. This is because each organization is different, and therefore every security architecture framework has to meet unique needs. That said, there are many similarities between the common methods that architects use.



Frameworks:

Much like property architects have guidelines to work within, so too do security architects. These are commonly referred to as 'frameworks'.

What is a security architecture framework? It can be a few different things, but is generally considered a consistent set of principles and guidelines for implementing security architecture at different levels of the business. There are many international framework standards, each solving a different problem.

Some companies will also devise their own frameworks. For example, at dig8ital we use best-practices based on three of the world's most common security architecture frameworks: SABSA, TOGAF and OSA (see below). By combining standards, we are able to provide a more versatile service that uses the best guidance from each. This enables us to design, implement and measure highly tailored security requirements and solutions.

Examples of common security architecture frameworks

1. **TOGAF:** The Open Group Architecture Framework, or TOGAF, helps determine what problems a business wants to solve with security architecture. It focuses on the preliminary phases of security architecture, an organization's scope and goal, setting out the problems a business intends to solve with this process. However, it does not give specific guidance on how to address security issues.
2. **SABSA:** Sherwood Applied Business Security Architecture, or SABSA, is a quite policy driven framework that helps define key questions that must be answered by security architecture: who, what, when and why. Its aim is to ensure that security services are designed, delivered and supported as an integral part of the enterprise's IT management. However, while often described as a 'security architecture method', it does not go into specifics regarding technical implementation.

3. **OSA:** Open Security Architecture, or OSA, is a framework related to functionality and technical security controls. It offers a comprehensive overview of key security issues, principles, components and concepts underlying architectural decisions that are involved when designing effective security architectures. That said, it can typically only be used once the security architecture is already designed.

Components of Security Architecture

For making the security architecture important, there are certain components that are involved in the design. The components are people, process and the tools. All these components combine helps to protect the organization assets. After defining the components, the next step is to make the policy and the reinforcement technique for the policies. After the other important steps are the method procedural for the implementation of security architecture and how the architecture will get enforced. By this, the overall design and architecture are designed for the organization that will protect them throughout their business operations. For a proper security architecture, some of the components are briefly discussed:

1. Guidance

The policies and procedures that act as the guidance should be design and implement properly. The policies should include the documentation that includes the objectives and goals for designing the architecture, standards, policies, rules and regulations for the organization, identification of scope and function, identification of other security policies.

2. Identity Management

It is the type of system that include the organization processes, technologies and policies that directly help users to gain access to the online applications and other network resources. For the organization, the proper responsibilities and roles need to be clearly stated, and individual tasks need to be designed for the employees.

3. Inclusion & Exclusion

The other components are the inclusion and exclusion that include the security of elements of the organization in which company resources are protected. The company resources include web resources, e-mail servers, private HR data and other reporting system information. The access should be grant to authorized users only so that the privacy and integrity can be maintained in the organization.

4. Access and Border Control

The organization should develop an architecture that is able to control the access to the business resources and can use the layer system for providing access to the company employees. Only authorized users should gain complete access to the system, and the rest should be provided with limited access of the system.

5. Validation of Architecture

As the technology advances, the company need to renew the policies and laws as per the changes, and continuous effort is needed by the organization in this

change. For that, the continuous monitoring is required, and according to that, proper changes can be made in the architecture.

6. Training

As for the organization, to maintain the privacy and integrity, the security architecture system is very important. AS there is a continuous change in the system, it becomes important that the employee should know about the changes and proper training is given to them so that they can use the system and protect the company assets and elements.

7. Technology

To reinforce the security architecture, the software and hardware used for making the architecture become very crucial for the organization. Because of continuous change in technology, there is a requirement of continuous change in the system so that the system can be up to date and help to make the system secure and private.

THE BENEFIT OF SECURITY ARCHITECTURE:

1. STRONG SECURITY ARCHITECTURE LEADS TO FEWER SECURITY BREACHES

Modern businesses need to have a robust security architecture framework for protecting their most important information assets. By strengthening your security architecture to close common weaknesses, you can drastically reduce the risk of an attacker succeeding in breaching your systems.

One of the top benefits of security architecture is its ability to translate each organization's unique requirements into executable strategies to develop a risk-free environment up and down the business, aligned with business needs and the latest security standards.

2. PROACTIVE SECURITY MEASURES SAVE MONEY

Detecting and fixing security vulnerabilities costs real money. It halts production, requires a thorough investigation and can lead to damaging product recalls or embarrassing press conferences.

In this way, the later in the product development cycle an error is detected, the more money it can cost - not to mention the risk of reputational harm.

To put that in figures, detecting an error during the coding phase of development could increase the cost of fixing it up to 500% - detecting the same error later, in the production or post-release phases, can cost up to 3,000% more.

3. IT MAY HELP MITIGATE DISCIPLINARY MEASURES IN THE EVENT OF A BREACH

While legislation differs around the globe as to the consequences for a cyber security breach, one of the common elements is that the more a business tries to reduce its risk and prevent vulnerabilities, the more favorable the outcome may be in the event of an attack. In general, regulators have shown that they respect when organizations do their best and punish businesses that only pretend to try, or do not try at all.

Another important point is that regulations are only getting stricter. Before 2016, nobody had heard of the GDPR and certainly didn't have to adhere to its standards. Now, of course, it guides much of the digital landscape in Europe and the globe. The legislative landscape is working hard to catch up to technology, and for businesses this means that there will likely be more, tighter rules to follow in future.

Malware Protection:

Malware security protection provides that second vital layer of protection for your computer or network. The increased need for malware protection also has to do with the widespread availability today of sophisticated tools originally intended for cyber espionage and cyber warfare.

1. **Access control and password security:** the concept of user name and password has been a key way of protecting our information. This may be one of the first measures regarding cyber security and protection.
2. **Authentication of data:** the documents that we receive must always be authenticated be before downloading that is it should be checked if it has introduced from a trusted and a safe source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus a good anti-virus software is also essential to protect the systems from viruses.
3. **Malware scanners:** this is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and mentioned to as malware.
4. **Firewalls:** a firewall is a software program or piece of hardware that helps mask out hackers, viruses, and worms that try to reach our computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the

specified security criteria. Hence firewalls play an important role in detecting the malware.

5. **Anti-virus software:** antivirus software is a computer program that detects, prevents, and takes action to defeat or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

Attackers always look for quick ways to steal data. Using readily available automated tools and advanced techniques, they can do so with ease, leaving your traditional network defenses ineffective. Malware is designed to spread quickly, create havoc and affect as many machines as possible. To protect your organization against such threats, you need a holistic, enterprise-wide malware protection strategy.

You create the illusion of security if you only rely on perimeter security, such as firewalls, intrusion prevention systems and URL filtering, or focus only on endpoint security, such as antivirus, anti-spam and malware analysis. With the ever-increasing attack surface and the growing prevalence of automated, sophisticated and volumetric attacks, you need a platform approach built for automation. To stay ahead of attackers, you need a malware protection strategy that includes a global threat intelligence community and covers the network, endpoint and cloud.

Threat Intelligence

A successful military operation relies on credible threat intelligence to make executive decisions. Similarly, contextual threat intelligence shared with a global community enables organizations to respond to attacks more quickly. Security analysts can subscribe to premium and free versions of global threat feed to help their teams stay ahead of attackers.

Network

Everything runs on the network. Business transactions, application deployments, access to resources, web browsing and video streaming all depend on the network running smoothly. The network is also a doorway to your most critical business assets, and it needs protection. Firewalls, intrusion prevention systems, URL filtering and sandboxing systems are typically deployed to protect the network by detecting, analyzing and preventing malicious activity.

Endpoint

The main targets for attackers are mostly laptops, desktop computer and servers – wherever there is valuable data. Attackers look for vulnerabilities and target users with credential theft, phishing and social engineering. Organizations can deploy endpoint security products like antivirus, anti-spam and anti-malware in the form of agents that protect against advanced attacks.

These agents can provide effective malware protection by employing static and dynamic malware analysis.

Cloud

More organizations are moving their critical assets to the cloud for its scalability, agility and cost savings. However, there are some security risks organizations must address. Hackers go after your data no matter where it lives, so cloud infrastructure is still open to cyberattacks similar to those that target traditional data centers. To protect against malware, you need to gain complete visibility into your cloud infrastructure, provide strong protections for incoming and outgoing traffic, secure your containers, and run compliance audits to expose data leaks.

The key is to seamlessly integrate cloud, network and endpoint security with global threat intelligence to quickly detect and deliver automated malware protections in near-real time. Tight integration across your network, cloud and endpoint environments, coupled with global threat intelligence, simplifies security so you can secure your users, applications and data everywhere.

XDR: Malware Protection Evolved

Extended detection and response (XDR) is a new category of security solutions that can help you stop malware. XDR combines next-gen antivirus and

endpoint protection with network detection and response, user behavior analytics and more to deliver holistic security across all your digital assets. The industry's first XDR platform, Cortex XDR, gathers and integrates data from any source to block malware and detect and eradicate stealthy threats.

Common Types of Malware

Here are some of the most common types of malware:

Ransomware—malware which is designed to infiltrate computers and encrypt key files. After these files have been encrypted, the individual behind the ransomware demands payment for access to the secret key required to decrypt the encrypted files.

Viruses—malware that functions by infecting different computer programs. For instance, a virus could overwrite the code of an affected program with its own code or make the program import and use a malicious code.

Worms—malware that is created to sprawl out to additional infected systems. This could include malware that spreads by releasing phishing emails or that scans for different vulnerable computers.

Rootkits—malware that is created to be secretive and can watch a computer user. Once it has been installed, the rootkit attempts to hide itself so as to avoid detection by antivirus and other security programs, while exfiltrating and collecting data for the operator.

Cryptomining malware—cryptocurrency mining programs are created to exploit cryptocurrencies awards by solving Proof of Work computational puzzles. Cryptomining malware makes use of the CPU tools of an infected computer to find solutions to these problems. This enables criminals to win award money.

Botnet—a network of infected computers. Cybercriminals use and control botnets in order to carry out large-scale, automated attacks, such as Distributed Denial of Service (DDoS) and credential stuffing. Botnet malware is intended to infect computers with a place a control and command structure that lets attackers send commands to the malware so that it carries out the attacker’s intention.

Trojans—malware created to impersonate something. Trojans try to steal the credentials of online accounts that may offer access to various streams of income like online bank accounts.

Fileless—a form of malware that avoids detection by traditional antivirus applications, which scan a computer's files for indications of malware. This is achieved by removing custom malicution code and using functionality built into the system being targeted. This makes fileless malware difficult to detect, because it doesn't have the file that matches signatures previously retained by antivirus applications.

Adware—malware that is created to serve malicious ads to computer users. Malware developers gain revenue from the advertisers whose ads the author serves.

How to Prevent Malware Infections in Your Organization

You can prevent malware with a variety of techniques:

- Install anti-malware software on your devices
- Ensure safe user behavior on devices (i.e. avoiding opening attachments from untrusted sources)
- Keep your anti-malware software updated, so you can benefit from the latest patches
- Implement a dual approval process for transactions between different organizations
- Implement second-channel verification processes for transactions with customers
- Apply threat detection and response procedures to identify malware and prevent it from spreading
- Implement robust security policies such as whitelists or allow lists
- Deploy advanced threat protection solutions for email security
- Ensure that files uploaded via collaboration channels and cloud storage are properly scanned
- Implement security at the web browser level

Malware Protection

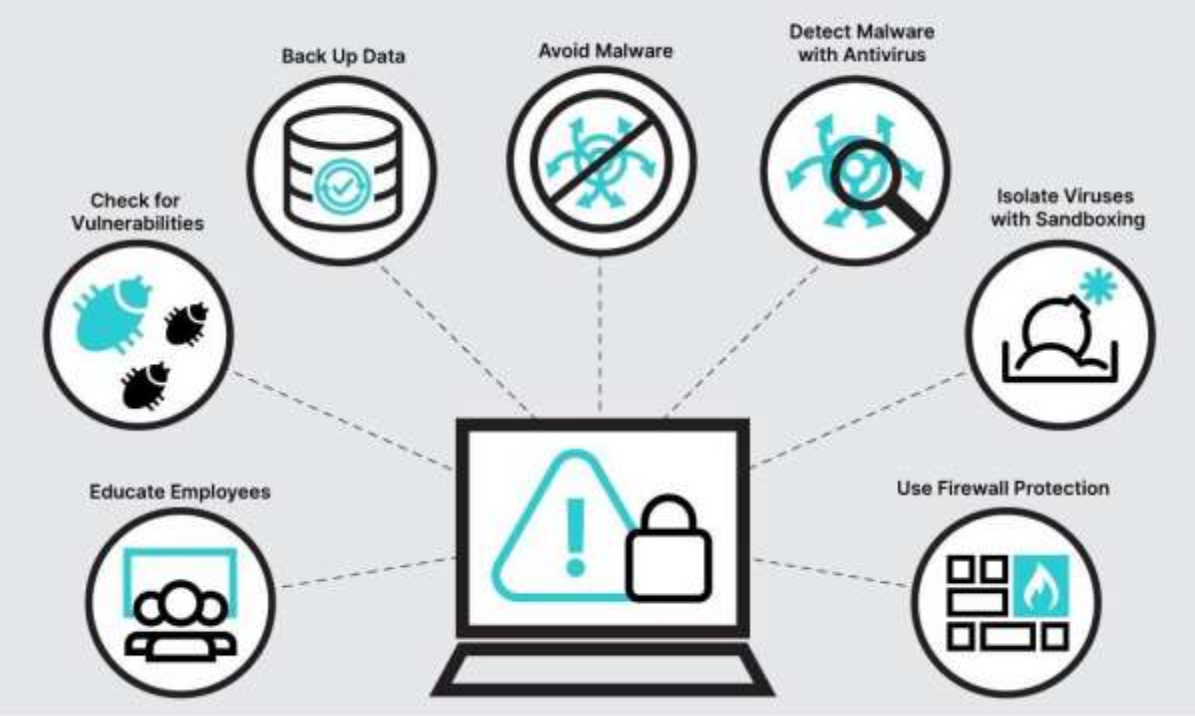
1. **Strong passwords and software updates**—ensure all users create strone, unique passwords, and regularly change passwords. Use a password manager to make it easier for users to use and remember secure passwords. Update your systems as quickly, as security flaws become known and patches are released.
2. **Back up your data and your test restore procedures**—backup is a critical practice that can help to protect against data loss. It can help ensure that normal operations can be maintained even if the

organization is attacked by network-based ransomware worms or other destructive cyber attacks.

3. **Protect against malware**—you should employ a layered approach that employs a combination of endpoint protection tools. For example, you can combine endpoint protection with next-generation firewalls (NGFW), and also implement an intrusion prevention system (IPS). This combination can help you ensure security is covered from endpoints to emails to the DNS layer.
4. **Educate users on malware threats**—train your users on techniques that can help them avoid social engineering schemes, such as phishing attacks, and report suspicious communication or system behavior to the security team.
5. **Partition your network**—you should use network segmentation to isolate important parts of your network from each other. This can significantly reduce the "blast radius" of successful attacks, because attackers will be limited to a specific network segment, and cannot move laterally to other parts of the network.
6. **Deploy advanced email security**—the majority of ransomware infections are spread via malicious downloads or email attachments. You should implement a layered security approach; one that can prevent advanced threats from reaching your end users as well as a company-sanctioned file-sharing solution that is scanned, and endpoint protection on user devices.
7. **Use security analytics**—continuously monitor network traffic, and use real-time threat intelligence feeds to add context to security alerts. This can help you gain extended visibility into threats affecting your network, understand their severity and how to respond effectively.
8. **Create instructions for your IT staff**—develop an incident response plan, which tells security staff and other stakeholders what they should do to detect, contain, and eradicate a cyber attack.
9. **Deploy a zero-trust security framework**—in this security approach, all access requests, whether coming from outside or inside the network, must be verified for trustworthiness before they can gain access to a system. The goal is to secure access by end-user devices, users, APIs, microservices, IoT, and containers, all of which may be compromised by attackers.

How to Protect Against Malware Attacks

It is important to be proactive when trying to avoid having malware infected systems in your organization. This involves a combination of prevention, preemptive mitigation, and education.



1. Avoid Malware

Most malware is relatively easy to spot if you know the signs. The most common places to encounter it are within spam emails, malicious websites, and pop-ups that appear on your device either while using the internet or in the course of normal operation.

Phishing schemes that seek to trick users to disclose sensitive data could also use malware so that even if you do not provide the information the phisher needs, you still end up clicking something that gives them access to your system. Therefore, it is a good idea to never click on anything that appears randomly on your screen or open anything in an email—attachment or otherwise—that seems suspicious.

2. Back Up Data

Backing up data is a form of preemptive mitigation that will be invaluable if a malware attack is successful. All endpoints and servers should have backups that are shielded from malware. If an attack is successful, you can use the backup to restore your infected device after wiping it.

3. Educate Employees

All employees should have a working understanding of what malware is, how it penetrates a system, its harmful effects, and tips for how to best avoid it. This

may include arming them with preventative knowledge such as the value of multi-factor authentication (MFA) and developing strong passwords. Employees should also know to look for red flags in an email or pop-up, as well as who to notify and what to do—or not do—if they suspect their endpoint has been exposed.

4. Check for Vulnerabilities

Have a full cybersecurity system that can help you find the places where malware might enter your network. A proactive security system can closely monitor all endpoints (including mobile devices) as well as a variety of servers—both on-premises and in the cloud.

5. Isolate Viruses with Sandboxing

Sandboxing can block a malware attack by isolating and confining malware—such as a malicious email attachment—to a protected environment. Inside a sandboxed area, the IT team can observe how the malware behaves and how it reacts to security measures taken to neutralize it. All the while, other devices and sections of the network are protected from infection. You can control and isolate malicious software with FortiSandbox.

6. Use Firewall Protection

Firewall technology prevents malware delivery by filtering network traffic. This includes traffic entering and exiting the network. Two-way malware protection is important because malicious programs within your system can be leveraged to affect users, devices, and networks that connect to yours. NGFWs incorporate packet filtering, network monitoring, Internet Protocol (IP) mapping, IP security (IPsec), and secure sockets layer virtual private network (SSL VPN) support. It also uses deeper inspection measures to protect a company from intrusion or from having applications hijacked.

The Fortinet NGFW solution is constantly updated to stay ahead of the latest threats in the cyber universe. Each update provides the NGFW with the data it needs to filter the latest and most dangerous threats. Protect against malware and more with FortiGate.

7. Detect Malware with Antivirus

The FortiGuard Antivirus Secruity Service leverages the power of the FortiGuard Labs Global Threat Intelligence system. In the span of a minute, FortiGuard eliminates, on average, 95,000 malware programs for real-time

protection. FortiGuard does this by incorporating knowledge of the different types of malware within the global threat landscape. Countermeasures are engineered to neutralize each type of threat, and then they are automatically enacted by FortiGuard, thereby protecting the networks under the FortiGuard umbrella.

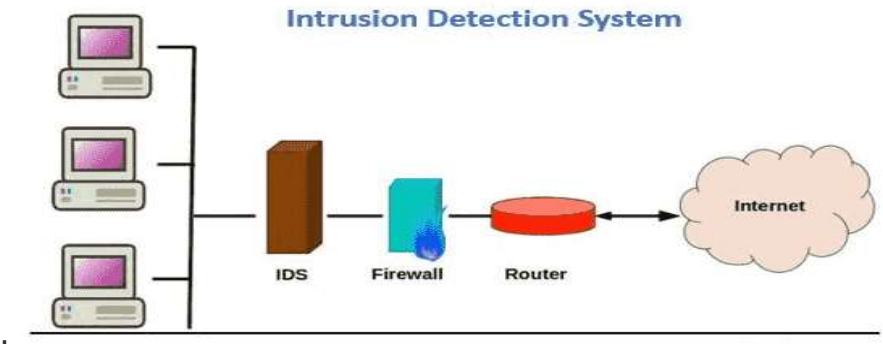
The FortiGuard Antivirus can attach to FortiGate, FortiSandbox, FortiMail, FortiWeb, and FortiClient.

8. Malware Removal

The best way to remove malware from an infected computer or personal device is by running antivirus security software. Using data about each kind of threat, antivirus apps can detect, remove, and quarantine malware on the different devices you use: desktop, laptop, smartphone, or tablet. Antivirus programs use data from its most recent update to locate the widest possible range of threats, so it is best to choose a solution that constantly updates.

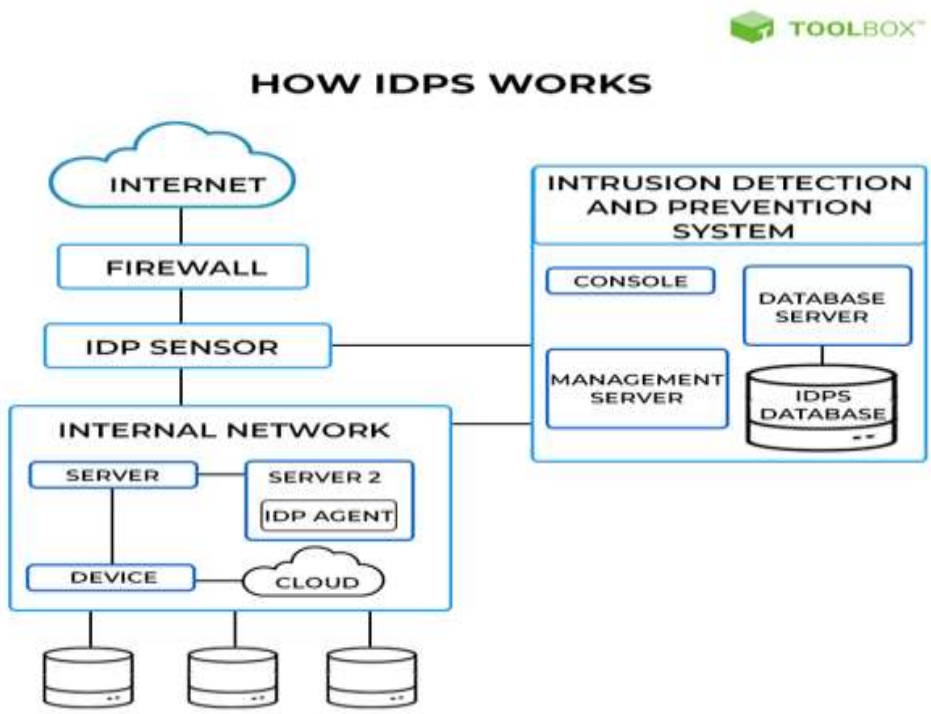
Intrusion Detection:

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'



How does an IDS work

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

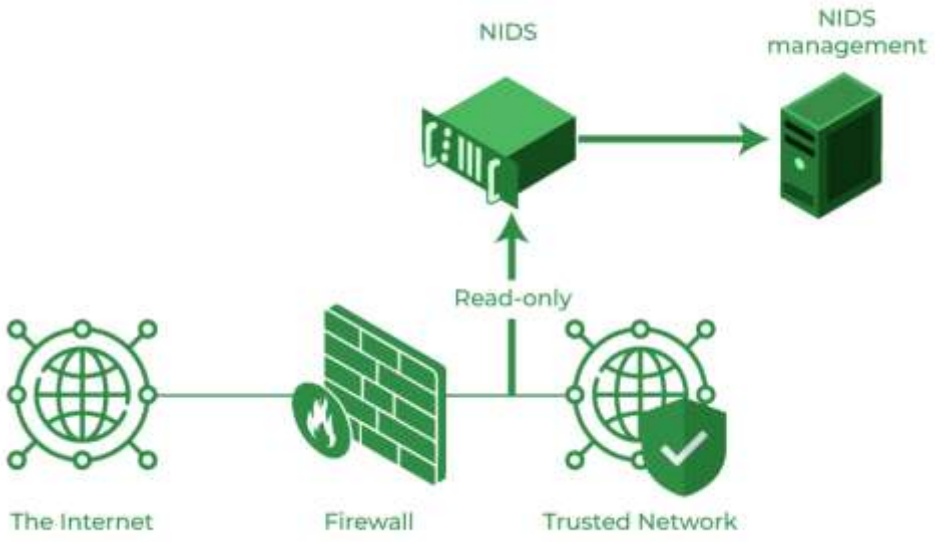


Classification of Intrusion Detection System

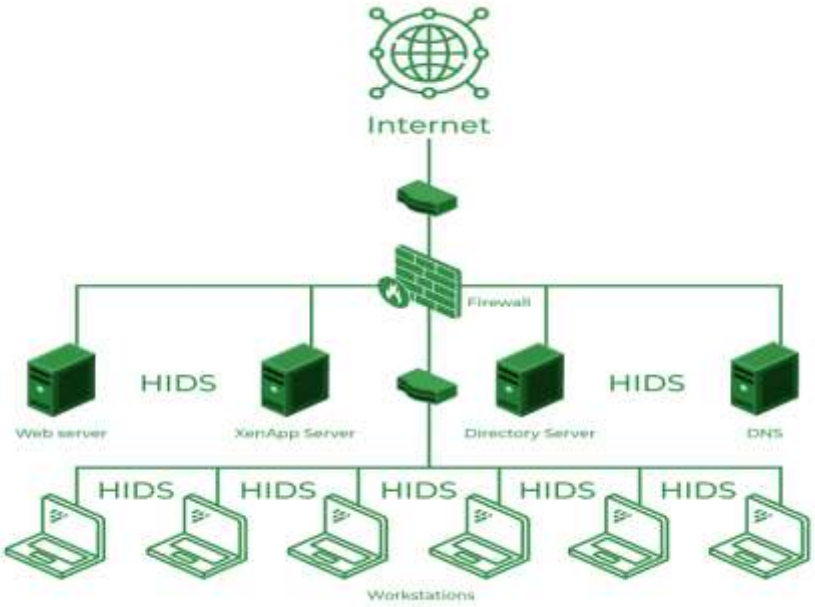
IDS are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet

where firewalls are located in order to see if someone is trying to crack the firewall.



- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Benefits of IDS

- **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

1. **Signature-based Method:** Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method:** Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations
3. **Hybrid Detection:** A hybrid IDS uses both signature-based and anomaly-based detection. This enables it to detect more potential attacks with a lower error rate than using either system in isolation.

Digital Rights Management:

Digital rights management (DRM) is a way to protect copyrights for digital media. This approach includes the use of technologies that limit the copying and use of copyrighted works and proprietary software.

In a way, digital rights management allows publishers or authors to control what paying users can do with their works. For companies, implementing digital rights management or processes can help to prevent users from accessing or using certain assets, allowing the organization to avoid legal

issues that arise from unauthorized use. Today, DRM is playing a growing role in data security.

With the rise of peer-to-peer file exchange services such as torrent sites, online piracy has been the bane of copyrighted material. DRM technologies do not catch those who engage in piracy. Instead, they make it impossible to steal or share the content in the first place.

How Digital Rights Management Works

Most of the time, digital rights management includes codes that prohibit copying, or codes that limit the time or number of devices on which a certain product can be accessed.

Publishers, authors, and other content creators use an application that encrypts media, data, e-book, content, software, or any other copyrighted material. Only those with the decryption keys can access the material. They can also use tools to limit or restrict what users are able to do with their materials.

There are many ways to protect your content, software, or product. DRM allows you to:

- Restrict or prevent users from editing or saving your content.
- Restrict or prevent users from sharing or forwarding your product or content.
- Restrict or prevent users from printing your content. For some, the document or artwork may only be printed up to a limited number of times.
- Disallow users from creating screenshots or screen grabs of your content.
- Set an expiry date on your document or media, after which the user will no longer be able to access it. This could also be done by limiting the number of uses that a user has. For instance, a document may be revoked after the user has listened ten times or opened and printed the PDF 20 times.
- Lock access only to certain IP addresses, locations, or devices. This means that if your media is only available to US residents, then it will not be accessible to people in other countries.
- Watermark artworks and documents in order to establish ownership and identity.

Digital rights management also allows publishers and authors to access a log of people and times when certain media, content, or software was used. For instance, you can see when a particular e-book was downloaded or printed and who accessed it.

The different types of DRM technologies used

The various digital rights management technologies are as follows:

- **Limited Install Activations**
  This tech restricts the number of users in whose systems, the software application/video game can be installed. This is done by requiring an online activation through the vendor's server, after the installation of the product. For example, suppose an anti-virus software is a '3 user only' product. This would mean that every time it is installed on a computer system, the user would have to activate it online. The user can only install the product in only 3 computers at the same time because the server would check the number of computers from where it was activated. This limits the number of users who can use it.

- **Persistent online authentication**
  Persistent online authentication a.k.a always-on-DRM requires to user to remain connected to the online server in order to use the product. This is popular mostly with video games, which require the user to connect to the server to play, even when the user is playing in single-player mode. This, however, has a major disadvantage: the product becomes unusable when there's a problem with the internet connection.

- **Software tampering**
  Many vendors deliberately introduce dormant bugs into their applications and video games which would be activated whenever the product is suspected to be pirated. For example, the game would deliberately start crashing as soon as the computer is connected to the internet and the product covertly establishes a connection with the server. Microsoft Windows too, implemented this feature in Windows XP and Windows 7 that whenever the OS was found to be pirated, the desktop wallpaper would turn black and volume icon would be locked.

- **Product keys**
  This has been, by far, the most common way of authenticating a product. While purchasing the application, the user would be provided with a product key which he/she would have to put while installing the application. It would later be checked by the server to find a match as every copy of the application has a different key. If a match is found, the product is not activated.

- **Enterprise digital rights management**
  It's a combination of identity and access management and encryption. The content is encrypted and coupled with the protection that allows

different access and modification policies for different entities. The protection is independent of the device and access location. It is mainly used to secure documents such as MS Word docs, PDF, Autocad files etc.

- **Content Scrambling System**
  It is an encryption system which is used in commercially produced multimedia discs to secure them from unauthorized copying and distribution. It uses a 40-bit stream cipher algorithm. It is, however, now been replaced with 'Content Protection for Recordable Media' and ' Content Protection for Record-able Media' systems which use 56-bit and 128-bit encryption standard respectively, and are compatible with Blu-ray and HD-DVDs.

- **DRM In Streaming Services:** Streaming services like Netflix, Comcast, Amazon prime etc use products such as Microsoft PlayReady, Xfinity etc, which are media file copy prevention technologies which include the concept of domain(group of devices belonging to the same user which can share the same licenses), embedded license (the licenses embedded with the contents of file0 etc. They're mostly portable and platform independent.

1. **Internet Connectivity Issues**: Many DRM-enabled products require online authentication. However, when there's a problem with the server or the Internet, there are problems with using the product.
2. **Bypass Methods for Audio and Video Content**: The process called 'ripping' extracts audio and video files from DRM protected files, and puts them into DRM-free files. Thereby, the whole thing of protecting copyright fails here.
3. **Short product life for paying users**: Mostly non-transferable to other technologies, platforms, and some are even gone forever after basic operating system updates, therefore leading to the product becoming unusable.
4. **Watermark Removal**: Watermarks can easily be removed through third party software.
5. **Purpose Built Hardware**: Often the protected content requires a specially built hardware to decrypt and show the content to the user, which is done in order to protect the decryption key. However, the system is prone to failure.

Benefits of Digital Rights Management

1. **Provides Privacy**: Businesses may use DRM technology to encrypt critical documents ranging from contracts and strategic plans to secret personnel information. It allows users to restrict access to files and trace who has

accessed them, as well as prohibit them from being changed, saved, duplicated, or printed.

2. **Securing ownership**: DRM is significant for authors and writers who want to safeguard their work. They can utilize technology to keep control of their material and prevent it from being changed or rebranded. This is also beneficial to scientists who wish to safeguard their discoveries and innovations.
3. **Prevent unauthorized, unintended usage.**: DRM technology aids material buyers in adhering to the license information that governs how, when, and even where they can use it and avoids financial penalties.
4. **Ensuring appropriate content access**: DRM limits content to targeted audiences and restricts it to certain audiences. Content aimed at those above the age of 18 will, for example, be restricted to adults who can prove their age.
5. **File privacy**: DRM facilitates companies in securing sensitive files and safeguarding their privacy. Intruders are unable to access or view confidential or sensitive information as a consequence of this.

Digital Rights Management Use Cases

DRM material may be found in a variety of digital media types, from music to photos to movies to eBooks, as well as proprietary company assets, database subscriptions, and software. The creators and legitimate owners of these works can utilize digital rights management software to protect their assets and material from being duplicated, modified, or used in ways they didn't intend. Some use cases of DRM are mentioned below:

- **Media Companies:** DRM technology aids artists, filmmakers, writers, and other content creators in combating unlawful use of their work in the media sector. If individuals are allowed to distribute this sort of content, artists and producers will find it difficult to make a living from their work.
- **Technology Companies:** According to a DataProt survey, 57% of computer users admit to having pirated software in the past. It's critical for technology businesses to secure their valuable software products against piracy in the age of software-as-a-service (SaaS).
- **Enterprise:** Enterprise digital rights management (EDRM) has become its own industry, with Gartner estimating that it will be worth more than $330 million by the end of 2026. DRM material is commonly used by businesses to secure sensitive data, particularly during product design papers and M&A (merger and acquisition) preparations.

Challenges of Digital Rights Management

Digital rights management does not sit well with everyone. Users who pay for music on iTunes, for example, would want to be able to listen to it on any device and use it in whatever way they choose.

Businesses that spend thousands of dollars for a high-value industry study, on the other hand, are ready to utilize DRM to prevent their competitors from obtaining the same information for free. Some DRM detractors argue that this offers an unfair edge for corporations with money to burn because smaller enterprises may be unable to buy the information required to expand their companies.

DRM technology, on the other hand, is not a perfect answer. Even if copyright holders include digital rights management coding in their product, the public may find a way around it. For example, if they only allow their material to be played on one player, some people would undoubtedly try to figure out the decryption keys and then construct another player that can play the protected content. Users then download the updated player in the hopes of getting around the DRM encryption. There are other free programs for removing DRM codes, which, while immoral, are widely available on the internet.

Cryptographic Techniques:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.
The most commonly used techniques in cryptography, are,

- Symmetric Key Cryptography,
- Asymmetric Key Cryptography,
- Hashing,
- Secret Sharing,

- Digital Signatures,
- Elliptic Curve Cryptography,
- Quantum Cryptography,
- Steganography,
- Zero-Knowledge Proofs,
- Homomorphic Encryption.

Features Of Cryptography are as follows:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Applications Of Cryptography:

1. **Computer passwords:** Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.
2. **Digital Currencies:** To safeguard transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
3. **Secure web browsing:** Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.
4. **Electronic signatures:** Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.
5. **Authentication:** Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.
6. **Cryptocurrencies:** Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to safeguard transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
7. **End-to-End Encryption:** End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

Advantages

1. **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.

2. **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.
3. **Protection against attacks:** Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.

Disadvantages

- **Speed:** Encryption can slow down during the data transmission, taking longer than unencrypted messages.
- **Require a large amount of power:** Cryptography is computationally intensive, requiring large amounts of computing power to encrypt and decrypt data.
- **Vulnerable:** It is also susceptible to cryptographic attacks, such as brute-force attacks, that can compromise the security of encrypted data.
- **Requiring a high skill:** Cryptography requires a high degree of skill, knowledge, and resources to implement correctly.

Threat and Incident Management:

Threat:

Threat management framework is often used by cybersecurity professionals to manage a time cycle of a cyberthreat as an attempt to find and respond to it with accuracy and speed. The seamless integration between people and technology tools to stay ahead of unknown cyber threats or vulnerabilities is the foundation that threat management is built upon.

Importance of Cyber Threat Management

With the ever increasing number of threats and complex network and system attacks, organizations are constantly struggling to keep up with mitigation and prevention solutions. According to an article from IBM on the Cost of a Data Breach, businesses and other organizations can save an average of $1.2 million when breaches are detected sooner. Detecting cyber threats is more important to organizations now than ever. Threat management increases the collaboration

between common technology security processes and people, giving businesses the best chance at detecting threats and responding to them sooner.
When a business or organization is successfully able to implement a cyber threat management framework, they can benefit from a variety of helpful solutions including:

- Develop a unified security team through education, skills, and effective threat management solutions
- Improvement through built-in process reporting and measurement throughout the threat management lifecycle
- Lower risk and faster detection of threats, leading to consistent vulnerability investigations and faster solution response

Common Challenges Managing Cyber Threats:

It is often hard to protect against advanced persistent threats and other threats from insider sources. Many security leaders across the cyber security industry often find themselves faced with challenges in a security network or system.

System Visibility is Little to None

Security teams do not always have the available resources to obtain a complete view of their entire threat landscape with relevant context. Teams often need visibility to internal data such as HR users, cloud information, and databases. They also need visibility to external data including threat intelligence, dark web information, and social media sources.
This lack of visibility is often caused by the conflict that exists between the lack of integration between point solutions, information technology security teams, and inconsistent processes throughout the organization. IBM estimated that corporations can use as many as 80 different security products from over 40 different vendors. The convoluted nature of excessive amounts of security products clouds visibility for those who need it most.

Lack of Insights and Necessary Reporting

A security team does not necessarily have insight into specific KPIs that need to be tracking down. Additionally, there is no easy way to develop progress reports that identify maturity standards and compliance due to a lack of integration between the organization's point solutions.
Additionally, it can often become difficult to align security teams on a unified goal for an organization if the teams are measured against different KPIs. Many cyber security experts believe that the complexity of an IT environment ranks among some of the biggest security challenges faced in creating a cybersecurity threat management program.

Burnout and Shortage of Staff and Their Skills

Security leaders are having a tough time hiring qualified talent and keeping the current staff motivated due to a skill shorting in the market, as well as analyst burnout. This has made it difficult to find additional staff budgets, meaning security leaders have to find unique ways to use talent from other cross-functional units including customer support and technical sales. Then these employees are trained to become effective in their new field of work.

Effective Managing Cyber Threats: Best Practices:

An organization needs to unite defenses and response to stop threats faster and more efficiently if they wish to succeed and grow rapidly. When a solid framework is applied, effective threat management is achieved. This framework typically includes one or more practice methods including:

- **Unified Insight.** Awareness of current threat operations can be used to tailor your organization's management plan to meet the unique needs of your organization.
- **Access to Visibility.** Access into the threat landscape with services to test an organization’s system for risks can integrate security and non-security data resources.
- **Risk Detection.** Identifying the most critical threats to an organization through the integration of AI, attack models, and intelligence systems from years of securing well known companies.
- **Use of Investigation Tools.** Investigation with the help of artificial intelligence and advanced analytics across data sources with multiple degrees of capabilities.
- **Effective Response.** Response to automated actions against common threats provide organizations with a business-wide playbook for the orchestration of threat management across people and technological processes.

An organization needs to unite defenses and response to stop threats faster and more efficiently if they wish to succeed and grow rapidly. When a solid framework is applied, effective threat management is achieved. This framework typically includes one or more practice methods including:

- **Unified Insight.** Awareness of current threat operations can be used to tailor your organization's management plan to meet the unique needs of your organization.
- **Access to Visibility.** Access into the threat landscape with services to test an organization’s system for risks can integrate security and non-security data resources.

- **Risk Detection.** Identifying the most critical threats to an organization through the integration of AI, attack models, and intelligence systems from years of securing well known companies.
- **Use of Investigation Tools.** Investigation with the help of artificial intelligence and advanced analytics across data sources with multiple degrees of capabilities.
- **Effective Response.** Response to automated actions against common threats provide organizations with a business-wide playbook for the orchestration of threat management across people and technological processes.

Incident Management:

Incident management is the process used by cybersecurity, DevOps, and IT professionals to identify and respond to incidents in their organization. Cybersecurity incidents can be anything from a server outage to a data breach to something as simple as an employee misconfiguring a firewall.

Cybersecurity incident management aims to minimize the impact of these incidents on business operations and prevent them from happening again. To do this, incident managers must first identify the cause of the incident and take steps to fix it. They also need to ensure that the proper procedures are in place to prevent incidents from recurring

Roles and Responsibilities of an Incident Management Team

An effective incident management team has several key roles and responsibilities (Chai & Lewis, 2020).

- **Identifying incidents.** The first step in resolving an incident is identifying that it has occurred. Incident managers must be able to promptly locate any issue that could impact business operations.
- **Resolving incidents.** Once an incident has been identified, it is up to the incident manager to fix it as quickly as possible. This often includes working with other departments to get things back up and running.
- **Reporting incidents.** Incident managers must provide regular reports on all happenings in their organization. This helps prevent future incidents and keeps everyone up to date on the latest information.
- **Training employees.** One of the critical responsibilities of an incident manager is training staff on how to respond to different types of incidents. This includes teaching them about the procedures that have been put in place and helping them understand the impact that an incident can have on business operations.

Tools Used by Incident Management Teams

Incident management teams use several tools and technologies to help them respond appropriately to incidents. Some of the most common tools include:

- **Intrusion detection systems.** These systems detect and react to security incidents. They often have features such as real-time alerts and reporting.
- **Netflow analyzers.** These tools help incident managers understand the traffic flowing in and out of their network. This information can identify malicious activity and quickly respond to incidents.
- **Vulnerability scanners.** These scanners help identify vulnerabilities in an organization's systems and networks. This information can be used to fix the vulnerabilities and prevent future incidents.
- **Availability monitoring.** This type of monitoring helps incident managers track the availability of critical systems and applications. This information can be used to quickly identify and resolve incidents affecting business operations.
- **Web proxies.** A web proxy is a server positioned between the client and the target server. It intercepts all requests from the client and forwards them to the target server. This can be used to monitor traffic and block access to specific websites.
- **Security information and event management (SIEM) tools.** SIEM tools collect and analyze incident security data across an organization. This can help incident managers quickly identify and mitigate any potential threats.
- **Threat intelligence.** Threat intelligence is information about current or emerging threats that can impact an organization. It can be leveraged to help incident managers stay ahead of any potential attacks and protect their business.

How to Create an Effective Incident Management Plan

An effective incident management plan is key to ensuring that your organization can adequately respond to any incidents that occur. Here are some tips for creating effective incident response strategies (Griffin, 2021).

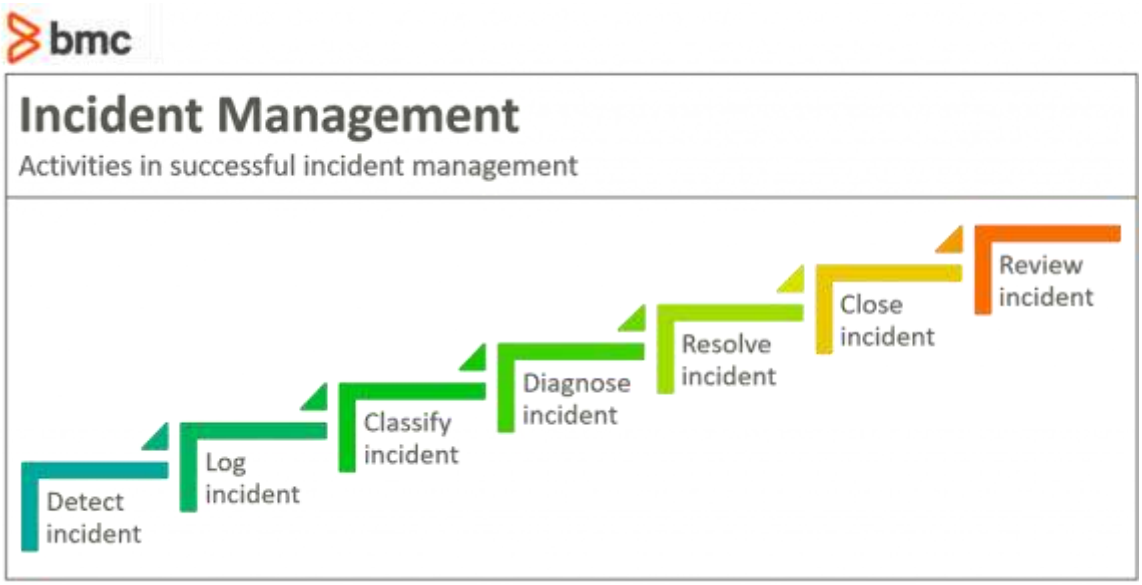
- **Define the roles and responsibilities of the team.** Ensure everyone on the team knows their role and what they need to do to resolve an incident.
- **Establish procedures.** Make sure that you have clear procedures for responding to different types of security incidents. This will help ensure that everyone is on the same page when resolving an incident.
- **Train employees.** Train security and other staff to recognize and respond to various incidents. This will help get the business back up and running with as little downtime as possible.

- **Create a communication plan.** Make sure you have a communication plan and incident response policy in place for sharing information about incidents with employees, customers, and partners.
- **Test your plan.** Testing your plan regularly ensures that it runs smoothly, functions effectively, and is updated to account for new developments in business operations and cybersecurity.

Incident management workflow & activities:

You can see from these examples that any number of activities might help—or hurt—your attempt to address an incident.

In order to handle incidents in a way that meets the needs of customers and relevant stakeholders, your IT team will perform a variety of activities, generally in this order:



1. Detect the incident

Incident detection usually happens in one of two ways:

- A user reports a service issue and the service provider validates it as an incident.
- The service provider identifies an incident from alerts or trends from the components used to provide the service.

2. Log the incident

The service provider logs the incident. This should register it in a system for purposes of proper management, including:

- Assigning the right handler to the incident
- Tracking the handling progress, particularly the timelines

3. Classify the incident

In the incident classification phase, the service provider categorizes the incident in terms of:

- Type
- Impact, as in who and what is affected
- Urgency, or the speed required for resolution
- Priority, with regard to business and customer perspectives

Classification is useful for accelerating the process of identifying:

- Who should handle the incident
- What model, if any, is best suited
- Whether existing workarounds can be used

4. Diagnose the incident

During incident diagnosis, the service provider investigates in order:

- Identify what has gone wrong
- Determine the fastest way to recover normal service

Diagnosis can be done by one person (handler) where the symptoms relate to a previously known and documented incident. But, for more complex and/or relatively new incidents, a team of cross-functional representatives, known as a swarm, may conduct a joint investigation.
Diagnosis may result in an update to the classification of the incident.

5. Resolve the incident

Incident resolution refers to when the solution is applied—be it a workaround or a permanent fix. Resolution can take one or several forms:

- Implemented automatically
- Documented for the end user to apply it by themselves
- Handled by the support team
- Forwarded to a more skilled unit or even the vendor

Depending on the length of time the incident is taking and its classification, communication with affected users and stakeholders must be carried out in parallel, informing them of status and timelines.

If your resolution efforts are not bearing fruit at the required speed, you may need to backstep to diagnosis or trigger the disaster recovery plans.

6. Close the incident

Once the incident is resolved, formal incident closure of the record takes place. Closure might require:

- Communicating and confirming from users that the service experience is normalized
- Billing of handling activities
- Updating configuration information where required

7. Review the incident

During the incident review, sometimes known as an incident postmortem, the process owners or management may review how the incident was handled to determine what was done right and what went wrong. Both are useful in future incidents by illustrating what activities might need to be changed or reinforced. Review can usher in process activities from other ITM practices such as:

- Information security management
- Change management
- Others as needed

The Pros of an Incident Management System

The advantages of an incident management system are as follows:

All Tickets are Answered

One advantage to using a system is the ability to take action on each ticket.

The system ensures that each ticket is answered when a new ticket is created by the customer.

If a customer ticket remains unanswered for a long period, the system sends an alert to the team about it.

The ticket is then reassigned to another technician.

Increased Employee Productivity

In order to improve employee performance, the company has a system that provides numbers and analytics for each employee.

The data allows for faster resolution of incidents by security team personnel.

In addition, managers can assist staff members by letting them know where they are spending more time or how they can improve.

When this is done, customer concerns are resolved more quickly, and customer satisfaction levels increase.

Organizational productivity also increases.

Quick Resolution

Sports facilities, arenas, or conference centers can identify Incident Types that are slower to respond to, and improvements can be made.

Every time a new incident is created, the command center is alerted about it, and then it is assigned to a specific department for resolution.

To improve incident management, an efficient software system should be utilized.

Accurate Data

Due to the system being automated, accurate data is provided.

This reduces errors, which makes the data more helpful in making improvements.

The data you have collected helps you set goals for the future and achieve them.

In short, the data can assist you in knowing your current position and how to improve your efficiency by taking proper actions.

The Cons of An Incident Management System

The cons of an incident management system are as follows:

Access to New Updates

Whenever a new update is released or if there is a change in the platform, the support team needs to be informed of these changes to resolve all of the issues.

These incidents can be serious and repetitive, and there are some incidents whose causes are unknown.

Incidents with no known cause can be lethal since there may be no proper solution for them.

For some solutions, however, they may require a long period of them to handle, which may cause upset.

It's important to choose an IMS system that informs you of new updates, whether by platform notification, knowledgebase, or email, so you can keep your team informed.

Access to Sensitive Information

In the information age, employees have access to sensitive data.

For example, command post employees may have access to season ticket holder data.

If any such employee is not reliable, then a huge loss can occur in the business.

Therefore, only certain, reliable employees should have access to certain information.

Data must be restricted from certain individuals.

Data Hacking

Technology is one of the key elements to development.

Without technology, progress is impossible.

Technology can be both a blessing and a curse.

Data hackers use technology to steal or manipulate data.

This can be lethal for businesses as it threatens their profitability and reputation.

That's why it's important to choose an Incident Management System that runs on cloud technology on a protected server, such as AWS.

Vulnerability management:

Vulnerability management is the ongoing process of discovering, assessing, prioritizing and remediating software vulnerabilities. Vulnerability management seeks to continually identify vulnerabilities and prioritize remediation efforts to quickly patch security flaws and improve the organization's security posture. With cybercriminals looking to take advantage of open vulnerabilities, vulnerability management is a proactive process that helps close security gaps in your network before they are utilized for a cyberattack.

To understand the vulnerability management process better, let's look at a relatable analogy. To ensure that we remain in top health, we go for periodic health check-ups. Such check-ups include various health specific scans such as blood tests, treadmill tests, complete metabolic tests, CT scans etc. Post this step, we consult a general physician doctor who assesses the reports and helps us prioritize what we should focus on first. This leads to the discovery of the current and potentially the future health issues. After we consume prescribed medication, we gradually begin to improve our health.

Think of a vulnerability management process quite akin to the health check-up but for your network and assets. A typical cyber security vulnerability management process has the following stages- Discovery, Prioritization and Response.

Let's take a deep dive into each of these stages.

Vulnerability Management Process

Stages of vulnerability management Process

Discovery

The first step towards vulnerability management is knowing “what” to scan which starts by gaining enterprise-wide visibility into all the assets of your organization. Comprehensive and accurate asset inventory is a core capability that is required to discover all potential vulnerabilities. If your vulnerability management system only “sees” a few types of assets, your coverage is insufficient. Consider an automated asset discovery and inventory solution that identifies all types of assets and inventories them, empowering you to manage risk across the entire attack surface.

An automated system powered by specialized AI/ML can solve the problem of unifying asset and vulnerability information across your entire enterprise—regardless of the number of tools or repositories that you might have. Automation allows your team to collect, de-duplicate, correlate and analyze asset data from multiple repositories in real-time—greatly reducing the time to inventory. Using automation, data can be continuously ingested from your various security tools to provide a more accurate, real-time view of your assets and vulnerabilities. Armed with this information, your security team is better equipped to tackle your organization’s vulnerabilities in the most efficient manner and increase the effectiveness of your vulnerability management efforts.

Prioritization

With hundreds or thousands of vulnerabilities, it’s important to effectively prioritize remediation to ensure your security team isn’t racing to address issues that pose little or no real risk to your business-critical assets. Since not every vulnerability presents the same security risk to operating systems, it’s critical to get context around each vulnerability and the enterprise asset that it affects.

To effectively prioritize the remediation of vulnerabilities, organizations need to adopt a risk-based prioritization approach, which requires a vulnerability management platform that understands and learns your business context, considers the value of each asset to your business and takes into account vulnerabilities, active threats, exposure due to software usage and any mitigating controls already implemented in your enterprise to calculated risk. With this approach, your organization can first focus on actions that are critical and make smarter decisions to reduce your risk, both strategically and tactically.

Response

After you've identified the vulnerabilities that exist across your systems, it's important to evaluate the risks they pose and determine how to effectively manage them. There are several ways to treat vulnerabilities: remediation (fully fixing or patching a vulnerability), mitigation (lessening the likelihood of a vulnerability being exploited), or taking no action (accepting the risk posed by that vulnerability). A risk-based vulnerability management tool will analyze different remediation scenarios and the related risk reduction results to recommend the best remediation option for your security team, such as highly tuned patch instructions. It can also help align remediation efforts to business priorities by identifying the owners of risk issues and assigning them remediation tasks. With this approach, security leaders have processes that enable prioritization and can build an effective strategy so they can quickly address security issues and protect their organization.

5 Main Stages Of The Vulnerability Management Process:

As opposed to vulnerability assessment, which is a one-time event, vulnerability management is a continuous, ongoing process. Follow these five main steps of the vulnerability management process to strengthen your cybersecurity.

As a process, vulnerability management entails identifying, assessing, and prioritizing security vulnerabilities across systems, workloads, and endpoints. After the vulnerabilities have been classified, the process typically delves into remediation, reporting, and resolving the uncovered threats satisfactorily.

Step 1: Identifying Vulnerabilities:

This step revolves around identifying and classifying vulnerabilities. Vulnerabilities are typically ranked using the Common Vulnerability Scoring System (CVSS).

The role of the CVSS is more prominent in stage two; however, what takes center stage at this point is vulnerability scanning. Vulnerability scanning is often done as part of a penetration testing exercise by a pentester or a security team of penetration testers.

In this process, a vulnerability scanner is an automated tool used to search, identify, and report the known vulnerabilities present in a company's IT infrastructure.

It creates an inventory of all the IT assets available in the system, especially those actively connected to the organization's network. These typically include

firewalls, servers, operating systems, containers, virtual machines, routers, printers, laptops, desktops, and switches.

Step 2: Evaluating Vulnerabilities:

After the vulnerabilities have been discovered, the next step is to evaluate the identified vulnerabilities for their degree of risk. In step 1, I briefly mentioned CVSS and how it is used as a ranking system for cybersecurity vulnerabilities.

CVSS is a free and open standard used to communicate the severity of vulnerabilities. It provides a score ranging from 0.0 to 10.0. To augment the vulnerability assessment, the National Vulnerability Database (NVD) includes a severity rating for the CVSS scores, as indicated in the table below.

CVSS Score	Severity Rating
0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

These scores communicate to organizations the risk posed to their infrastructure by each vulnerability. Hence, organizations are able to prioritize the vulnerabilities and threats to focus on. This evaluation also informs the organization's risk management strategy and remediation efforts.

Step 3: Remediating Vulnerabilities:

This step focuses on treating and mitigating the discovered vulnerabilities. Several strategies are put in place to prioritize and eliminate vulnerabilities based on the level of risk they pose to the business.

Patching

Patching is often the low-hanging fruit that remediates a large portion of the vulnerabilities found in software. In fact, most cybersecurity breaches are a

result of unpatched software. Therefore, a patch management system that ensures operating systems and third-party software are up-to-date is vital.

However, there might be occasions when a vendor hasn't yet released a patch for a particular vulnerability. In this instance, the organizations should switch to mitigation measures to lessen the impact of the vulnerability's possible exploitation.

These measures might include limiting user permissions for those activities, or—depending on their severity—truncating or blacklisting the impacted devices from the network.

Acceptance

Acceptance is also a counterintuitive vulnerability management strategy. This involves taking no action with discovered vulnerabilities. This strategy makes sense with low-risk vulnerabilities that pose minimal threats to the business. More so when the cost of fixing the vulnerability exceeds the possible cost incurred by its exploitation.

Even when there are only benign vulnerabilities to be fixed, organizations should still strive to optimize their reported vulnerability metrics. Hence, the more the vulnerability management system is geared to improving those metrics, the more it reduces the organization's attack surface.

Step 4: Verify Vulnerabilities:

This step ensures that the threats in the system have been eliminated through follow-up audits. Penetration testing should also be used to verify the efficacy of the remediation measures taken. In addition, it also makes sure new vulnerabilities weren't inadvertently created during the process.

Step 5: Report Vulnerabilities:

It is important to document not only the discovered vulnerabilities but a security plan on how to describe known vulnerabilities and monitor suspicious activity. These reports are vital because they leave records that help businesses improve their security responses in the future.

These reports are also important to share with top management and for compliance audits. This is because demonstrating and recording fixed vulnerabilities and issues displays accountability. And this accountability is often required to maintain compliance standards.

Benefits Of Vulnerability Management:

1. Is Cost Effective

Certainly, one of the top benefits to any organization is cost effectiveness, and a vulnerability management possesses multiple cost saving advantages.

It eliminates ad hoc patching which can lead to missed patches and compound costs. It also reduces technical debt by helping the organization set focus and prioritization around assets that present the highest risk if exploited.

Plain and simple, vulnerability management helps to bring structure and precision to an organization's security posture, bolstering its justification to stakeholders who will then be more likely support vulnerability initiatives.

2. Matures Your Security Program

Growth is an important component of any organization, but especially in and around its cyber security program.

Vulnerability management enhances the overall security posture of your organization by recognizing key assets and where to prioritize efforts in order to reduce risk.

Working together with other security teams, it helps prevent access and data exploitation by threat actors.

But not all risks are due to outward attacks. Vulnerability management also achieves specific goals for security frameworks or compliance requirements.

3. Gain Operational Efficiencies

Keeping teams and systems aligned to project goals and outcomes is important – especially when involving highly sensitive security for an organization.

To maintain alignment, vulnerability management aims to define the process for identifying vulnerabilities and remediating them.

It also has the potential to reduce manual workflows and provide automation with continuous monitoring, alerting, and remediation solutions.

This not only adds to operational efficiency but has very much become a standard security practice.

4. Enhances Visibility And Reporting

As mentioned previously, when deploying a vulnerability assessment, vulnerability management helps to build a system of tracking and reporting.

Having visibility into a project explains the return on investment in security to stakeholders and can help to support other projects.

Vulnerability reporting also helps to uplift the team by providing actionable dashboards and trend reports to quickly measure performance and state of the program.

In turn, these contextualized reports provide key metrics and indicators for senior management to make informed decisions on key initiatives.

5. Maintains Compliance Requirements

Effective vulnerability management will help to achieve regulatory requirements.

This can be done by reviewing and implementing compliances from various frameworks, such as the Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPPA).

PCI has a list of compliances that range from the more general, as in, “provide a patch audit report”, to the more specific, such as, “deploy patches on systems

for both internal and external applications only after testing them in separate test environments".

A robust set of patch management policies and procedures are required for a healthcare organization to meet HIPAA compliance. This includes proper inventory management, testing, documentation and configurations around automatic software updates, unmanaged hosts, firmware, and more.

Security Event Management:

Security event management (SEM) is the process of identifying, gathering, monitoring and reporting security-related events in a software, system or IT environment. SEM enables the recording and evaluation of events, and helps security or system administrators to analyze, adjust and manage the information security architecture, policies and procedures.

SEM stands for Security Event Management. As the name implies, SEM is the process of managing the security events happening across the network of an organization. This process is automated by SEM systems (tools).

Security events

Security events are activities of systems or software running on a computer network of the organization. These events are recorded in files one after the other as they occur. Those files are called event logs.

Since event logs are generated on each system of the network, they are then transported into a centralized location with the help of protocols such as Syslog and SNMP.

Event logs:

Many systems and applications which run on a computer network generate events which are kept in event logs. These logs are essentially lists of activities that occurred, with records of new events being appended to the end of the logs as they occur. Protocols, such as syslog and SNMP, can be used to transport these events, as they occur, to logging software that is not on the same host on which the events are generated. The better SEMs provide a flexible array of supported communication protocols to allow for the broadest range of event collection.

It is beneficial to send all events to a centralized SEM system for the following reasons:

- Access to all logs can be provided through a consistent central interface.
- The SEM can provide secure, forensically sound storage and archival of event logs (this is also a classic log management function).
- Powerful reporting tools can be run on the SEM to mine the logs for useful information.
- Events can be parsed as they hit the SEM for significance, and alerts and notifications can be immediately sent out to interested parties as warranted.
- Related events which occur on multiple systems can be detected which would be very difficult to detect if each system had a separate log.
- Events which are sent from a system to a SEM remain on the SEM even if the sending system fails or the logs on it are accidentally or intentionally erased.

Security event manager (SEM) is the solution that allows organizations to manage and analyze their security events through an intuitive web interface. Once these security events are analyzed, the results can be shared with other teams and with the providers of cyber security services.
SEM can be used to gather both structured and unstructured data, such as logs, traces, errors, and system messages, along with all proprietary data such as configuration files or network traffic.

Working of SEM tools :

SEM tools identify, gather, organize the log events in a centralized location and represent them in visual formats such as graphs and charts for the security team of an organization to easily understand what is happening and what happened in their organization's systems connected in a common network.
By analyzing the log events in real-time, SEM tools do the following.

- Detects threats/vulnerabilities and bad actors like ransomware in the network.
- Automatically responds to incidents in real-time. Such as log off users, block an IP address on firewalls, killing an ongoing process, etc.
- Reports compliance in the network.

Need of SEM tool :

In the modern era; with the advancement of technology, numerous innovations solve significant problems and make things more convenient and comfortable than ever.
Along with that, some people exploit the technology maliciously for their own good or someone's downfall. So keeping crucial data within the organizations securely and confidentially has become a challenge.

Hence, organizations need to protect their data and resources proactively before someone sneaks in digitally. Without accessing the systems connected in a network within an organization, it's almost impossible for invaders to sneak in and get their hands on crucial data and resources.

That is one of the most important reasons for organizations to monitor and keep track of the activities going on all the systems of their organizations connected in a common network.

And manually keeping track of the ongoing activities across the network of numerous systems is impossible. Even if it's done manually by increasing the workforce, what happens next is the inefficient use of resources, wasting a huge amount of time and money on the additional workforce. So the pitch-perfect solution for such a significant scenario is Automation.

Benefits of SEM :

1. **Confidentiality –**
   SEM ensures that no unauthorized person gets access to the data and resources of an organization through the network. If someone sneaks in and gets unauthorized access, then the SEM tool will notify the security team and also take the necessary action to prevent the access instantly.
2. **Integrity –**
   Data and resources remain the same as left by the authorized person. No unauthorized person can modify any data and use resources while the SEM tool is in charge.
3. **Availability –**
   Access to certain data and resources for authorized users are available for a specified time only. So that no users can get access to them in runtime. i.e They are available to users only when they should be.
4. **Non-Repudiation –**
   Whoever gets access, makes modifications and/or just being in the

network are known and noted by SEM tools. This ensures that the information is passed between the authorized sender and receiver appropriately.

These benefits appease the organizations that use SEM tools by total security.

The combination of SEM and SIM(Security Information Management) tools is known as SIEM tools which are used widely these days to deliver unified solutions of Security Information and Event Management.

Cons of being an security event management:

While there are many advantages of being an event manager, there are some disadvantages, including:

1. Unconventional work hours

Event managers often work nights and weekends to complete their responsibilities, sometimes in addition to normal office hours during the weekdays. Event planners may also work during holidays to coordinate seasonal parties and celebrations. While many jobs have a limit to the number of hours for employees to work each day or week, event planners might spend an unlimited amount of time completing their responsibilities. They might work shifts up to 15 hours compared to the traditional nine-hour shift for many professions.

2. Time away from family and friends

Event planners might travel often to manage their tasks. This can result in time spent away from friends and family members. It might be challenging to maintain relationships when you travel frequently. This profession may also require an event planner to balance their work responsibilities with their responsibilities at home.

3. Experience requirements

Event management positions often require applicants to have extensive experience in their field. When starting your career as an event manager, you might seek unpaid internships to gain this experience before advancing to paid positions. While establishing your career and earning experience, you might find little job stability. The experience requirements of a job in event management might cause professionals to begin their careers with unpaid opportunities.

4. Job instability

Event managers that provide their services through freelance opportunities instead of working through an event management company may encounter unstable job conditions. The level of stability for this profession often changes throughout the year. For example, an event manager might plan multiple parties during the holiday season but have fewer clients during the summer months. Consider growing your list of clients throughout your career and searching for new event management opportunities to help with this issue.

5. Multiple events at the same time

As an event manager, you might find yourself planning several events at the same time. You may also handle multiple clients with different needs and desires at once. It's important for event managers to keep an efficient schedule and manage communication with all their customers when planning multiple events. This can help them provide the same level of care and attention to each client and organize the details of each event.

Forensic Investigations:

Forensic investigations can be triggered from many different types of events generated by a variety of security controls. Whether they originate as a result of human watchfulness, rule matching in an intrusion prevention system, or modification of data alerted on file integrity monitoring (FIM), organizations must demonstrate an acceptable level of due diligence by ensuring they review each event as they are generated.
While reviewing events, security analysts need to quickly assess the level of risk to the organization and make a decision of whether a full forensic investigation needs to be initiated. The criteria for deciding when an event becomes an investigation should not be simply left to the judgment of the security analyst, a series of policies and procedures must be established to clearly define when this escalation is performed. At the point an investigation is initiated, governance documentation should already be in place and include detailed information for how to proceed and whom to involve.

Investigation services

Should something go wrong, any suggestion of impropriety can quickly destroy a business, its finances and its reputation.

If the worst does happen, the first priority is to stop any further loss or reputational damage.

Our dedicated global teams of investigators, forensic accountants, compliance specialists and technology professionals help companies respond rapidly to instances of alleged fraud, bribery and other misconduct, as well as provide support throughout any subsequent regulatory, civil or criminal proceedings.

Using advanced forensic technologies and data visualization tools, we gather facts and evidence quickly to assess the extent of the issue and to help organizations manage the concerns of all relevant stakeholders.

We support legal counsel by analyzing varying data sources to uncover links, patterns and anomalies, and by presenting findings in legal proceedings.

- Rapidly investigate allegations of wrongdoing in your business
- Efficiently satisfy regulators' demands for information
- Prepare to litigate in response to issues identified
- Demonstrate to stakeholders that actions have been taken to mitigate future risks of improper conduct

Tasks and responsibilities

The specific tasks of a digital forensic investigator will vary depending on the company or agency and industry. These are some of the tasks you might expect to perform (based on actual job listings):

- Retrieve data from virtual and physical devices
- Collect and analyze network intrusion artifacts and evidence of malicious network activity
- Reconstruct the series of events leading to a compromise or breach
- Collect, process, analyze, and preserve digital evidence in criminal cases.
- Extract and analyze metadata
- Collaborate with law enforcement, as well as legal, compliance, and HR teams
- Ensure chain of custody of digital evidence
- Write technical reports to document case findings.
- Identify potential threats and provide recommendations for better security.
- Provide testimony in depositions, trials, and other legal proceedings

Key Components of Forensic Investigation:

- Crime Scene
- Preservation of the Crime Scene
- Recording of the Crime Scene

Crime Scene

A scene of occurrence of a crime is the place where a particular crime has been committed or where physical evidence of such crime is found when it is first brought to the notice of the police. It is a starting point for the investigator, which provides him with the information on the victim and the suspect, and to reconstruct the crime.

The scene of occurrence cannot be limited to one place only. It may extend to one or more places. It may also not be limited to immediate surroundings, but may In a wider area depending upon the nature of the crime committed. In a compact scene of crime, such burglary, the scene may be divided into five parts, namely:

- Line of approach
- Point of entry;
- Actual scene;
- Point of exit; and
- Line of retreat.

The scene of crime may be classified as outdo or indoor scene. A crime committed on a road or a field is an outdoor crime. Whereas a crime committed in a house, a car, etc., is an indoor crime. There may be certain types of crime, which have no 'scene' at all. The crime of this nature are forgery, embezzlement etc.

The crime of indoor and outdoor nature like theft, house breaking, robbery, dacoit, homicide, rape, traffic accident, etc., have invariably physical evidence at their scenes because of intense physical activities involved in their commission. Physical evidence found at the crime scene can be the key to the solution of a crime.

Preservation of The Crime Scene

Preservation of the crime scene is most important task of the police. The first person arriving at the scene should. Be able to protect the scene from curious onlookers and family members. He should isolate the scene the crime by cordoning it off. Nothing on the scene should be touched, changed or altered until the investigating officer takes its proper note. Once any material object of dead body is moved from its place, it can never be restored to its original position That scene, once touched or altered, will make the task of an investigator, in reconstructing the crime and identifying the criminal by physical evidence, very difficult, it not impossible.

Recording of Crime Scene

After taking an immediate action to protect the crime scene Investigator should then proceed to record the evidence. But before doing so, he should seek the help of two independent reliable witnesses, preferably from the neighbourhood of the crime scene, as their presence will strengthen the case of prosecution at the time of trial. No evidence should be picked up, or touched or even disturbed till it has been minutely described in notebook, its location shown in a sketch and photography taken.

(a) Recording of notes:

The investigator has to begin his investigation by recording pertinent Facts and details observed by him at the crime scene. The discovery of every significant item of evidence, when and where it was found, should be accurately described. These factual reports are important to overcome defence claims

regarding the theory of the crime and its reconstruction. The notes should cover the following aspects of the crime scene:-

The date and time of the FIR

The nature of crime.

Location of crime scene and a brief description of the area.

Brief facts of the crime

The names of all officers, witnesses, investigators and special Personnel at the crime scene.

The names of personnel, who took the photography, fingerprints, Sketches, etc.

The weather and lighting condition at the time of recording the scene

A description of the interior and exterior of the crime scene, number of room, door, windows, etc.

The location and collection of evidence.

The date & time of completion of recording and examination of the crime scene.

(b) Sketching the crime scene:

The investigator must make a rough sketch of the crime scene. The sketches in combination with the photography provide an ideal presentation of the scene. The sketch of the scene of occurrence should be prepared at the site and not at any other place. The distance should be measured exactly and not by approximation. The directions should be indicated with the help of the compass. The sketch should show and locate important objects at the scene. Unimportant objects should be omitted

(c) Photography of the crime scene:

The scene of occurrence should be photographed as a matter of routine. It is a supplement to the above methods of recording and often the best way to record and illustrate the details of a crime scene and its evidence.
In order to tell the story of scene graphically and coherently, an orderly progression of shots will be required. The subject matter of crime scene photography should move from the general to the specific.

Advantages

There are various advantages of forensics. It has a broad spectrum of applications which are very useful to us. Some of the advantages of this science are discussed below.

☛ With the help of certain computer tools, it is possible to control cyber crime. This is done through packet sniffing (sensing critical information in the data packets), IP address tracing (to get the address from where the criminal was accessing), email address tracing (to get the details of the email server and in cases of email bombs). This is called computer forensics.
☛ It helps in determining the cause of death by examining the postmortem changes, blunt injuries, burns and scalds on the body, and the scene of death. If it's sudden natural death, the case is investigated by the coroner or a medical examiner.
☛ Forensic analysis is used to investigate accident cases and to determine its cause by analyzing the vehicle condition, tire and other marks, eye witnesses, calculating the vehicle's speed etc

☛ The alcohol content in a human being can be determined by analyzing the blood and other body fluids like saliva, urine etc.
☛ It also includes anthropology and helps in sex determination.
☛ Clinical forensic medicine is useful in finding out child abuse, defensive wounds on a victim, gunshot wounds, injury patterns in domestic violence victims, self-inflicted injuries, sexual assault, and semen persistence.

☛ Biometrics technology is combined with forensics, which helps to identify the fingerprint of the criminal, on the objects present in the crime scene.
☛ Phonetics, which is also a part of forensics, that is used to tap the voice signals and identify the speaker. Speech enhancement, speech coding and tape authentication are other techniques used in phonetics.
☛ Other useful aspects of forensic analysis includes fire investigation, forgery and fraud in payment cards, lie detection, footprint marks, voice analysis, digital imaging and photography etc.

Disadvantages

Despite numerous advantages of this science, there are some ethical, legal, and knowledge constraints involved in forensic analysis.

☛ DNA analysis of a person is believed to be against human ethics, as it reveals private information about an individual.
☛ Equipment used in forensics is expensive.
☛ Scientific analysis consumes lot of time because of which the verdict is

delayed.
☛ It requires precise and accurate analysis. Even if a minor error occurs in the analysis, it may result in the wrong figure.
☛ The evidence cannot be accessible at all times.

☛ Evidence is prone to manipulation, which may end up in an unrighteous verdict.
☛ Interpretation of the analysis differs from one forensic scientist to another.
☛ Forensic analysis can be prevented by strong influences (political or financial factors).
☛ There is no particular standard to verify the result of the experiment. It requires wide knowledge and intensive study.
☛ Innovation is hindered as the approach is mostly the same.
☛ Misconceptions and ignorance can mislead the experimental analysis.
☛ Maintaining privacy and secrecy of the information gathered through forensic analysis is quite difficult.

Local Environment Management:

An Environmental Management System (EMS) is a set of processes and practices that enable an organization to reduce its environmental impacts and increase its operating efficiency. This site provides information and resources related to an EMS for small businesses and private industry, as well as local, state and federal agencies.

EMS under ISO 14001

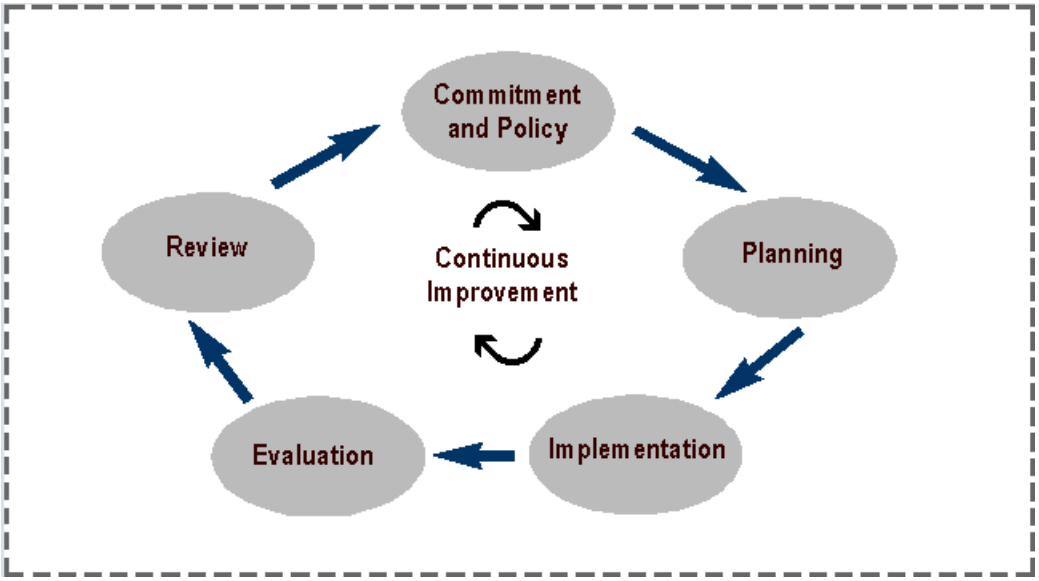


Figure 1: The continuous improvement cycle.

An EMS encourages an organization to continuously improve its environmental performance. The system follows a repeating cycle (see figure 1). The organization first commits to an environmental policy, then uses its policy as a basis for establishing a plan, which sets objectives and targets for improving environmental performance. The next step is implementation. After that, the organization evaluates its environmental performance to see whether the objectives and targets are being met. If targets are not being met, corrective action is taken. The results of this evaluation are then reviewed by top management to see if the EMS is working. Management revisits the environmental policy and sets new targets in a revised plan. The company then implements the revised plan. The cycle repeats, and continuous improvement occurs.

The most commonly used framework for an EMS is the one developed by the International Organization for Standardization (ISO) for the ISO 14001 standard . Established in 1996, this framework is the official international standard for an EMS which is based on the Plan-Do-Check-Act methodology. The five main stages of an EMS, as defined by the ISO 14001 standard , are described below:

1. Commitment and Policy - Top management commits to environmental improvement and establishes the organization's environmental policy. The policy is the foundation of the EMS.

2. Planning - An organization first identifies environmental aspects of its operations. Environmental aspects are those items, such as air pollutants or hazardous waste, that can have negative impacts on people and/or the environment. An organization then determines which aspects are significant by choosing criteria considered most important by the organization. For example, an organization may choose worker health and safety, environmental compliance, and cost as its criteria. Once significant environmental aspects are determined, an organization sets objectives and targets. An objective is an overall environmental goal (e.g., minimize use of chemical X). A target is a detailed, quantified requirement that arises from the objectives (e.g., reduce use of chemical X by 25% by September 2030). The final part of the planning stage is devising an action plan for meeting the targets. This includes designating responsibilities, establishing a schedule, and outlining clearly defined steps to meet the targets.

3. Implementation - A organization follows through with the action plan using the necessary resources (human, financial, etc.). An important component is employee training and awareness for all employees (including interns, contractors, etc.). Other steps in the implementation stage include documentation, following operating procedures, and setting up internal and external communication lines.

4. Evaluation - A company monitors its operations to evaluate whether objectives and targets are being met. If not, the company takes corrective action.

5. Review - Top management reviews the results of the evaluation to see if the EMS is working. Management determines whether the original environmental policy is consistent with the organization's values. The plan is then revised to optimize the effectiveness of the EMS. The review stage creates a loop of continuous improvement for a company.

The development of an environmental management system provides a cohesive and comprehensive framework for a city or local government to identify significant aspects and manage its environment - both opportunities and risks - and to document, evaluate and communicate its environmental plans and programmes to local stakeholders.

There are five key principles for the management of the local environment. They are (a) development of strong local government commitment to environmental management, (b) proper planning and compliance, (c) creation of enabling systems, (d) appropriate performance and accountability, and (e) the continual measurement and improvement of policies and programmes. Each of these five principles are analyzed below in terms of the way in which it facilitates participation of the community.

1. **Local government commitment**

   Commitment from the local government to improve environment performance and establish policies for the purpose is very important for obtaining political support, developing policy, integrating into operational system, and showing environmental leadership.

   How does this facilitate community participation? A strong commitment from the local government to be inclusive, develop political support, or show leadership will necessitate the involvement of the community. A prudent local government will involve the community in order to ensure broad commitment from all residents of the city. This will also ensure acceptance and ownership of its policies and programmes with the community.

2. **Planning and compliance**

   The local government plans and implements proactive programmes to identify and address environmental problems and corrects deficiencies in the local environment. These programmes also broadly aim to, for example, comply with environmental laws/regulations, prepare for

natural and man-made emergencies, and prevent pollution and conserve resources.

How does this facilitate community participation? The planning of environmental management systems needs to include views of the community and residents in order to ensure its success and become effective. It will essentially be through participation (meetings, seminars, hearings etc.) that views of the community can be incorporated.

3. **Enabling systems**

   The local government develops and implements the necessary measures to enable various urban stakeholders to perform their tasks and implement their programmes/projects on the environment . These measures provide opportunities for learning, and support with standards, systems, and programmes. Information management, communication and documentation policies also create the necessary enabling environment.

   How does this facilitate community participation? One of the key criteria that will enable urban stakeholders to perform their tasks for environmental management is an effective system of community participation. Participation becomes easier if it is built into the management system and process.

4. **Performance and Accountability**

   The local government develops measures that addresses environmental performance of all urban stakeholders, and ensure full accountability of their functions that help in instilling responsibility, authority and accountability. These include the development of performance standards in consultation with all local actors. Accountability is ensured by keeping actions and processes transparent.

   How does this facilitate community participation? It is essentially through effective community participation that good performance and accountability can be built. A decentralized approach where all actors play their role to achieve overall goals and objectives, works best when effective participation is linked to effective performance and accountability.

5. **Measurement and Improvement**

   The local government develops and implements programmes to assess progress towards meeting it environmental goals and uses it to improve its environmental performance. This is done through the development of

an evaluation programme or gathering and analyzing relevant data. It could also compare its performance with other local governments, or incorporates continuous improvement of its policies, programmes and their impacts.

How does this facilitate community participation? Measurement and improvement of environmental management processes can be done to established indicators and parameters. But it is third party views, particularly coming from the community and its representatives that will lead to better performance and improvement. This can be generated through good community participation and involvement.

Business continuity:

Business continuity is the advance planning and preparation undertaken to ensure that an organization will have the capability to operate its critical business functions during emergency events. Events can include natural disasters, a business crisis, pandemic, workplace violence, or any event that results in a disruption of your business operation. It is important to remember that you should plan and prepare not only for events that will stop functions completely but for those that also have the potential to adversely impact services or functions.

What Does Business Continuity Include?

BC covers the planning and preparation needed to ensure an organization will have the capability to perform its critical business functions during emergency events. It identifies, plans for, and/or creates:

- How to communicate with customers, vendors and other third parties to ensure you are providing good information and support.
- How to ensure services or products can still be provided to customers.
- The order and timing required to restore business processes.
- How to support employees during an emergency event.
- The required technology to support the business functions (disaster recovery – or DR – will implement recovery solutions for technology).
- Workaround processes to use when technology is not available.
- Where and how to relocate people and processes in the event business locations are impacted or not available.
- The teams and organization that will be necessary to manage emergency events.

- Business process dependencies (what, or who does each business process rely upon in order to do their work).
- Regular exercises to validate that plans and actions meet requirements and will be functional in an actual event.
- Ensure staffing levels will be adequate during an event for both external and internal needs.
- Documentation of the steps and actions to take during an event to accomplish the items above.

The Anatomy of a BCM Program

At MHA, we divide up the Business Continuity Management (BCM) program into four key dimensions:

1. **Program Administration**
2. **Crisis Management**
3. **Business Recovery**
4. **IT Disaster Recovery**

We believe that when these four dimensions are operating optimally, individually and in an integrated fashion, the BCM program will have an elevated level of sophistication, maturity, and capability.

Organizations may not be able to work on the four dimensions in parallel and effectively implement the components, but without implementing all areas, an organization will not truly be prepared. Many unexpected issues arise during a crisis event, too many to address ad hoc. If your organization tries

to address the unexpected and perform critical actions on the fly during a crisis event, it will not be able to effectively and efficiently perform the tasks required for a successful recovery.

The BCM Team

A good BC program starts with a Business Continuity Management (BCM) team. The following individuals are the core members of the BCM team. They are responsible for implementing the policies and directing BCM efforts across the organization**.**

- **Sponsor:** The senior management individual with overall responsibility and accountability for the BCM program.
- **The Business Continuity Manager:** The individual with direct responsibility for the BCM program.
- **Assistant Business Continuity Manager:** The backup to the Business Continuity Manager. This could be a titled position or an assigned position.
- **Administrative Assistant:** The individual responsible for supporting the BCM team. This is often an administrative assistant working in the Business Continuity office, if it exists, or another individual from the administrative assistant team.

The BCM Process

To get started, consider performing the following steps. We have provided links to relevant MHA blog posts on these topics.

- **Assessment:** The first step to a successful planning process is to make sure that you have a thorough understanding of what is, and is not, critical to your organization. You can (and should) perform a Business Impact Analysis (BIA) and a Threat & Risk Assessment to guide you. Without understanding your organization's processes, how critical those processes are, and the threats and risks inherent in your operations, you cannot effectively develop appropriate plans and strategies.
- **Business Recovery:** The purpose of business recovery planning is to ensure that your critical business processes can be recovered in the event of an emergency. Your plan will document the actions, including temporary workarounds, that will be necessary to keep critical

functions operational until IT applications, systems, facilities, or personnel are again available.

- **IT Recovery:** IT recovery planning refers to the development of plans and strategies for the recovery of your technology, including actions that will be necessary to restore critical IT applications and systems.
- **Crisis Management:** Crisis Management refers to a specific plan that details how your organization will manage a crisis event, as well as to an internal organizational unit (the Crisis Management Team) that will manage that event.

What type of events does business continuity planning guard against?

A variety of events cause digital business disruptions. Just because you're not at risk of one particular cataclysmic disaster doesn't mean many other incidents can't take you offline:

- **Disasters: Natural and Local**
  Data loss and system failure can obviously be caused by natural disasters such as floods, earthquakes and fires, but even a simple electronic malfunction could destroy valuable information. When it comes to data, putting all your eggs in one basket is a perilous risk.

- **Network Disruptions**
  Third party internet networks can fail. Fiber can get cut. Your in-house local area network can be disabled. If your business needs continuous connectivity, make sure network availability is a top priority.

- **Cybersecurity**
  The prevalence of cybersecurity threats are a global phenomenon that no business, large or small, can ignore. New threats such as Ransomware are predicted to be on the rise. Backing up your data with high frequency is crucial to ensuring such attacks don't bring your business down plan against data breach is paramount.

- **Human error**
  Vulnerability points are often located right in the cubicle next to you. Employees or vendors can cause outages simply out of ignorance, due to innocent mistakes, or even as a result of ill intent.

Steps for Building and Executing Your Business Continuity Plan

If your business is behind in disaster planning, you don't have to catch up alone.

Whether taking on business continuity planning alone or with a third party, follow these three steps to start protecting your company from unplanned downtime:

Step 1: Perform a Business Impact Analysis

A business impact analysis defines what data your company cannot live without and the amount of downtime acceptable in a given period of time. Finding a hosting provider that promises 100% uptime will help with this, but you'll also need to determine two important numbers key to disaster recovery: **Recovery Time Objective and Recovery Point Objective.**

Step 2: Perform a Risk Assessment

This step is critical if you manage your own infrastructure. Risk assessments are all about identifying potential points of failure. For example, if you have your data stored in only one location and the location dies, you will lose your data. If a hosting provider is in charge of your servers and data within a data center, ideally you will have everything stored and replicated in more than one location. A service provider with a well-defined SLA will give additional confidence that your risk of downtime will be at a minimum.

Step 3: Manage Your Risks

Once you've assessed the risks, you must manage them—whether your data and infrastructure lives in house, with a hosting provider, or a combination of both. Regularly backup your data offsite as specified by your business continuity plan and go a step beyond by adding redundant, offsite infrastructure to your network to ensure 100 percent uptime.

Advantages

I. During planning the potential of the business booming up is established plus the possible weaknesses and challenges the company might face are outlined and effective solution are established in advance.

II. The main advantage that any financial institution stands to gain from the use of an incident command system is the ability to identify potential threats and plan in advance hence avoiding suspension of critical financial operations.

The threats might range from natural epidemics, cyber-attacks or just computer failures as a result of hardware or software issues.

III. The financial organization has increased abilities to maintain effective coordination and to maintain the response directions. Besides, the organization can gain insights on the importance of coordination of resources and the ability to identify the incident priorities.

IV. The financial institution has a good platform for testing and reviewing the most likely threat hence allowing for coordination of BCP with external stakeholders.

V. The long-term use of incident command systems is an advantage in itself as it leads to gaining of experience hence I the long run will lead to higher efficiency in restoration and fast recoveries. However, the full implementation becomes a disadvantage as it is time-consuming.

Disadvantages

Failure to do business continuity planning one is at a significant risk of either:

I. The implementation process is often considered as tedious hence requiring professionals to handle it. Besides the organization has to employ qualified personnel to handle that. No business intends to invest heavily in preparing for unknown threats as they rather wait for it to happen then defend (Systems, 2012).

II. The process of using incident command systems as a business continuity planning tool is both costly and time-consuming. This may lead to over investment of funds that could have otherwise been dedicated to other business operations.

III. Business collapsing or failure that is as a result of poor management skills, techniques, and evaluation techniques. Hence, one is not in a position to establish the coming danger and ends up regretting the already outcome.

IV. The death of individuals could occur after the fire, building collapsing where the insurance covers have been ignored, have not been implemented by professionals or due to lack of adequate testing of the possible scenarios.

UNIT-5:-

Security Monitoring and Improvement:

Security monitoring, sometimes referred to as "security information monitoring (SIM)" or "security event monitoring (SEM)," involves collecting and analyzing information to detect suspicious behavior or unauthorized system changes on your network, defining which types of behavior should trigger alerts, and taking action on alerts as needed.

From hackers and malware, to disgruntled or careless employees, to outdated or otherwise vulnerable devices and operating systems, to mobile and public cloud computing, to third-party service providers, most companies are routinely exposed to security threats of varying severity in the normal course of conducting business. Given the ubiquitous, unavoidable nature of security risks, quick response time is essential to maintaining system security, and automated, continuous security monitoring is key to quick threat detection and response.

Staying ahead of threats allows you to respond to them before they occur. Detecting and managing potential threats in good time helps you to protect your business applications, users' data, and overall network. The process of keeping up to date with security vulnerabilities typically involves:

- Collecting and analyzing data to identify changes to your network or unusual behavior
- Drawing on threat intelligence to pick out the latest risks
- Deciding the specific types of behavior that require attention
- Taking action before threats become a security incident
- Generating detailed network security reports for compliance purposes

THE IMPORTANCE OF CYBERSECURITY MONITORING

The cybersecurity landscape has changed remarkably in recent years. Today, simply using cybersecurity tools to prevent attacks from happening is not enough. You need to adopt a proactive approach that will enable you to be prepared for attacks. Here are a few reasons why cybersecurity monitoring is important for your business.

1. MINIMIZE DATA BREACHES

In 2020 alone, the total number of data breaches in the United States was 1001. This is a clear indication that businesses are constantly exposed to cyber threats. Continuous monitoring of your network will help you to detect

threats ahead of time and combat them before they wreak havoc. Detecting unusual activity will allow you to limit the damage that cyber-attacks can cause by preventing the threats from spreading to other areas. This way, you can protect your valuable information and your reputation.

2. IMPROVE YOUR TIME TO RESPOND TO ATTACKS

Cyberattacks can happen when you least expect them. Considering what is at stake, you have to contain and remediate threats as soon as they are detected. Continuous cybersecurity monitoring lets you detect threats and data breaches way before they escalate into serious security issues. By identifying events that require your attention and receiving alerts, you will be in a great position to respond to attacks before they cause widespread damage.

3. ADDRESS SECURITY VULNERABILITIES

Cybersecurity involves many moving parts. Part of protecting yourself from cyber crimes entails locating weaknesses within your IT infrastructure. To keep attackers at bay, you need to control access by updating your firewalls with the latest security patches. This should be done in time so that attackers do not get an opportunity to exploit weaknesses in the firewall code. One of the ways of doing this is to stay on top of your network security. Monitoring your network around the clock helps to ensure continuous data protection.

4. COMPLIANCE WITH STANDARDS AND REGULATIONS

When it comes to cybersecurity, organizations are required to meet certain controls to protect the integrity, confidentiality, and availability of the data in their possession.

Failure to meet these requirements can increase your vulnerabilities, put your reputation at risk, increase your exposure to legal liability and lead to hefty fines. Constant cybersecurity monitoring will help you achieve and maintain the set standards, effectively ensuring compliance.

5. REDUCE DOWNTIME

Cyberattacks that result in data breaches and data loss can have far-reaching effects on your organization. Round-the-clock preventative cybersecurity monitoring will help you make improvements to your network and ensure it is fully functioning so that it supports your day-to-day operations. Minimizing data breaches, responding to threats quickly, and addressing your

vulnerabilities will go a long way in reducing the chances of disruptions. This will assist in avoiding IT downtime that could lead to financial costs for your organization.

6. THE NATURE OF THREATS HAS CHANGED

Cyber criminals are getting smarter and are finding ways to get around the defenses that people have put in place. The nature of threats has also changed; new threats are emerging all the time. Without enhancing your cybersecurity, you run the risk of being a victim of cybercrimes. One of the best ways to ensure you are ready to combat the evolving cyber threats is to constantly monitor your network.

7. THE RISE IN REMOTE WORKING

The outbreak of the coronavirus pandemic and the use of cloud-based services have accelerated the remote working trend. Today, staff can work on any device and from any location. However, remote working has made it more difficult for businesses to control access to their computer networks. In effect, this has given cyber criminals an opportunity to gain unauthorized entry. Continuous cybersecurity monitoring will enable you to detect changes to your system and unusual behavior, so you can take the necessary action.

8. INCREASE THE PRODUCTIVITY OF EMPLOYEES

Keeping an eye on your IT infrastructure can contribute to increased employee productivity. Being vigilant will go a long way in ensuring your entire computer network is in tip-top condition. Improved network performance will enable employees to not only work efficiently but also complete tasks faster. Also, having an expert to handle the technical duties will allow your staff to concentrate on their core tasks. This will help to boost the productivity levels of your workers.

What Are the Benefits Of Cyber Security Monitoring?

Cyber security monitoring is critical to ensuring that your system is constantly online and functioning properly. However, many small firms do not have the time or finances to engage extra IT personnel to constantly monitor a network. Failure to monitor a network exposes your company to severe security risks and raises the likelihood of several technical faults in the workplace. A managed security services provider may assist you in avoiding many of these

issues by providing round-the-clock network monitoring services for a monthly set charge. Cyber security monitoring benefits include

Reduced Downtime:
One of the primary benefits of cyber security monitoring services is that they are an effective method to prevent downtime for your business. A fully functional network is critical for day-to-day corporate activities. And a managed security services provider will guarantee that everything is operating at peak performance by testing it on a regular basis. These preventative monitoring services will also repair and upgrade your network to reduce the possibility of downtime, which may result in major financial consequences for your firm.
You might wish to read: How to implement continuous cyber security monitoring?

Increased Employee Productivity:
Another advantage of cyber security monitoring services is that it is an excellent technique to boost each employee's productivity levels. A managed security service provider, for example, will handle all technical chores regarding a network, allowing staff to focus on their primary job activities. Improving network speed is a primary objective for an IT service provider since it allows employees to execute their job obligations more quickly and efficiently.

Reduced Cyber Attack
Cyber attacks may create massive data leaks and destroy the business's brand. Many of these cyber attacks are aimed at breaking into networks to steal vital information and wreak havoc on the entire operating system. However, you can mitigate the impact of cyber assaults by collaborating with a managed service provider that provides cyber security monitoring services. It will identify any strange activity within your network and prevent a cyber attack from spreading to other regions and creating significant damage.

Improvement:

5 Steps Towards Improved Security Monitoring

The challenges to cybersecurity grow more every day. One way to stay on top is to use security monitoring as part of your arsenal of weapons. Here are 5 ways security monitoring can help.

1. Standardizes your risk

The best way to effectively communicate threats iis to have a common language. Create what is called an "apples-to-apples" framework for threat

assessment. The easiest way to open your network to threats is to talk at cross-purposes. To avoid that, create a table of risk priorities and ranks. In other words, create a uniform method of grading vulnerabilities across your organization and employ that method with institutional discipline for more meaningful comparisons.

2. Understand your endpoint security

Malicious users access your IT infrastructure and apps through doors, windows, vents, and tunnels. You need to know every single entrance to and exit from your network to the larger world outside. Make use of endpoint security to detect intrusion attempts on the host by looking for hidden processes, files, ports and known rootkits. Endpoint security looks for signs of an intrusion, inconsistent behavior and activity so that if you have a zero day or custom developed malware, you can see the results of the malware on the system.

3. Add knowledge to know-how

Proper security protocols, combined with the right security software and services, get you most of the way in terms of your network security. What will take you over the top, and give you the high ground, is intelligence. You need to continuously educate yourself on all threats - new and old. You will never receive a degree in threat assessment and graduate—your learning has to be as constant as your vigilance. Who, how, why, where, and what are constant questions. Who's hacking? What's their motivation? How are they gaining targets? Where are they breaching networks? What are they after? Staying current may necessitate getting help especially for companies with small IT teams..

4. Measure the right thing

When it comes to security, what do you measure? Well, if you measure the number of scans, the number of updates you install, the number of times you've patched a program, the number of virus definitions you've added, you'll have a number alright. You'll probably have a large number. But then, given how these things work, you'll be expected to make that number higher.

The problem is that this number does not measure success—it measures actions. Actions that do not result in success are useless to your understanding of how well you're dealing with your security needs. Instead, measure the number of threats you've eliminated and the problems you've remediated. After all, the ideal number here is zero. If your network security is perfect, you won't see any breaches or malware; you will see nothing. Ofcourse,

we don't live in a perfect world; however, you can edge yours a little closer to the ideal by measuring the number of successful measures you take.

5. Implement continuous security monitoring

Collecting security events across your IT infrastructure, network, and applications and reporting on threats on a constant basis, is integral to your network safety. Continuous monitoring requires combining log management and SIEM technology with machine learning to proactively eliminate threats and meet compliance objectives. But, you need to spend time digging through the noise of thousands of events, or analyzing raw log files, to determine what is happening in the network. Unfortunately, small IT teams do not always have the resource to spend on continuous security monitoring. Using a security monitoring service can help. It provides the technology, people and process to triage and investigate potential security incidents to give you rapid actionable recommendations.

Security Audit:

A security audit is a comprehensive assessment of your organization's information system; typically, this assessment measures your information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations. A comprehensive security audit will assess an organization's security controls relating to the following:

- Physical components of your information system and the environment in which the information system is housed.
- Applications and software, including security patches your systems administrators have already implemented.
- Network vulnerabilities, including evaluations of information as it travels between different points within, and external of, your organization's network
- The human dimension, including how employees collect, share, and store highly sensitive information.

How Does a Security Audit Work?

A security audit works by testing whether your organization's information system is adhering to a set of internal or external criteria regulating data security. Internal criteria includes your company's IT policies and procedures and security controls. External criteria include federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX), and standards set by the International Organization for

Standardization (ISO) or the National Institute for Standards in Technology (NIST). A security audit compares your organization's actual IT practices with the standards relevant to your enterprise, and will identify areas for remediation and growth.

What Is the Main Purpose of a Security Audit? Why Is It Important?

A security audit will provide a roadmap of your organization's main information security weaknesses and identify where it is meeting the criteria the organization has set out to follow and where it isn't. Security audits are crucial to developing risk assessment plans and mitigation strategies for organizations that deal with individuals' sensitive and confidential data.

What Is Security Auditing in Cybersecurity?

A security audit in cybersecurity will ensure that there is adequate protection for your organization's networks, devices, and data from leaks, data breaches, and criminal interference. Security audits are one of three primary types of cybersecurity assessment strategies — the other two are penetration testing and vulnerability assessment, both of which involve running real-time tests on the strength of firewalls, malware, passwords, and data protection measures.

What Does a Security Audit Consist of?

So, what is a security audit and are there any common steps? A security audit consists of a complete assessment of all components of your IT infrastructure — this includes operating systems, servers, digital communication and sharing tools, applications, data storage and collection processes, and more. The steps are often determined by the compliance strategy your organization needs to take, but there are a few common components:

1. Select Security Audit Criteria

Determine which external criteria you want or need to meet, and use these to develop your list of security features to analyze and test. Also keep a record of your organization's internal policies, if your IT team anticipates cybersecurity concerns that external criteria may not cover.

2. Assess Staff Training

The more people who have access to highly sensitive data, the greater the chance for human error. Make sure there is a record of which staff members have access to sensitive information and which employees have been trained in

cybersecurity risk management or compliance practices. Plan to train those who still require training.

3. Monitor Network Logs

Monitor network activity and event logs. Keeping close track of logs will help to ensure only employees with the proper permissions are accessing restricted data, and that those employees are following the proper security measures.

4. Identify Vulnerabilities

Before conducting a penetration test or vulnerability assessment, your security audit should uncover some of your most glaring vulnerabilities, like whether a security patch is outdated or employee passwords haven't been changed in over a year. Regular security audits make penetration tests and vulnerability assessments more efficient and effective.

5. Implement Protections

Once you have reviewed the organization's vulnerabilities and ensured that staff is trained and following the proper protocol, make sure the organization is employing internal controls to prevent fraud, like limiting users' access to sensitive data. Check that wireless networks are secure, encryption tools are up-to-date, and that the proper anti-virus software has been installed and updated across the entire network.

Why Do Companies Need Security Audits?

Companies need regular security audits to make sure they are properly protecting their clients' private information, complying with federal regulations, and avoiding liability and costly fines. To avoid penalties, companies need to keep up with ever-changing federal regulations like HIPAA and SOX. Periodic security audits are necessary to make sure your organization is up to speed with any new requirements.

How Do You Perform a Security Audit?

How you perform a security audit depends upon the criteria being used to evaluate your organization's information systems. A full security audit often involves auditors both internal or external to the organization, and the steps depend on the external security compliance measures your organization must meet.

There are a number of computer-assisted audit techniques (CAATs) on the market designed to automate your audit process. CAATs regularly run through the steps of an audit, seeking out vulnerabilities and automatically preparing audit reports. However, always have a trained IT manager or professional auditor reviewing these reports.

Pros

- **Expertise**

Outsourcing your cybersecurity audit to a specialist firm can ensure that your business receives the most comprehensive and up-to-date service.

To ensure that your security audit is performed by qualified professionals who are well-versed in the latest industry trends and standards, hire a company dedicated to developing and providing cutting-edge cybersecurity solutions.

- **Cost Savings**

Outsourcing a cybersecurity audit can save costs for an organization in several ways. First, many organizations don't have the resources, expertise, or time to conduct a thorough and comprehensive audit of their security systems.

By outsourcing the audit to a third-party security firm, the organization can leverage the expertise of experienced professionals to ensure that their systems are secure and up-to-date.

- **Increased Security**

Outsourcing your cybersecurity audit can increase security by allowing a team of experts to assess your system and identify any vulnerabilities. They can also advise how to improve your security posture and help you implement the necessary changes.

For example, they can help you develop a comprehensive security policy, audit your existing security protocols, and ensure that you have the right tools, processes, and personnel to protect your organization's data.

- **Flexibility**

Outsourcing your cybersecurity audit increases flexibility because it allows you to access specialized expertise and resources that may not be available in-house. It also allows you to quickly adjust to changing requirements and needs by providing access to a larger pool of experts and resources.

Additionally, outsourcing can help you save on costs by paying only for the services you need. Lastly, outsourcing can help you focus on growing your business functions by relieving you of the burden of managing complex cybersecurity audits.

Cons

- **Loss Of Control**

Since the company needs direct oversight of the audit, outsourcing a cybersecurity audit can lead to little or no control over the audit processes and results.

Consequently, companies must rely on a third-party vendor to complete the audit accurately and objectively. It means that the company may need more direct insight into the audit process, including the scope of the audit, the methods used, and the results.

- **Risk Of Data Breach**

Outsourcing your cybersecurity audit increases the risks of a data breach because the third-party auditor may have different expertise or access to the same resources as an in-house auditor.

The auditor may be unable to identify as many security vulnerabilities or be as thorough in their analysis as an in-house auditor.

- **Hard To Determine The Quality Of the Audit**

When you outsource your cybersecurity audit, you're relying on an outside party to evaluate the safety of your network, which can make it difficult to gauge the audit's quality. You have to have trust that the external service provider is giving you an honest assessment of your system's security flaws.

Additionally, it can be hard to verify the accuracy of the audit results since an external party conducted the audit. It's also essential to consider the

qualifications and experience of the auditor, as this can significantly impact the quality of the audit.

Security Performance:

Cybersecurity performance management is the process of evaluating and overseeing the effectiveness of your security program. It can be a challenge to manage, as the usual performance management indicators — cost and revenue — don't apply. Additionally, the field is always changing; new technologies evolve and threats are advancing quickly. It's easy to be taken by surprise, and in light of this constantly-changing threat landscape, it may be hard to know how your cybersecurity program is performing. Cybersecurity performance management is possible, however.

If you're going to manage your cybersecurity program's performance you have to be able to measure it. Fortunately, there are metrics that will help you manage your cybersecurity performance. You just have to choose the ones that are relevant to your organization.

Why is cybersecurity performance management important?

Good cybersecurity performance management tells you where your security program is succeeding, where your weak spots are, and helps your security team and leadership understand what steps you need to take to make your cybersecurity program stronger.

This is done by measuring your information security program against key performance indicators (KPIs), such as:

- The time it takes to detect security-related incidents
- The time it takes to respond to security incidents
- Number of reported incidents
- The number and frequency of unreported incidents discovered after the fact
- Awareness of possible threats
- Level of preparedness
- Security training results
- The absence of unexpected security incidents
- Your organization's security rating

These aren't necessarily the only metrics to track — your security team and leadership should work together to choose the benchmarks that matter most to your organization based on your business goals, best practices, and your company's specific risk. (You may also choose to use competitors' best practices and security budget as a KPI, for example.)

These KPIs should be easy to obtain, easily measurable, and easy to understand.

What are the challenges of cybersecurity performance management?

Although metrics are key, they can also be a distraction. If you're tracking too many metrics, or if your KPIs are subjective or irrelevant, the story you're trying to tell about your cybersecurity program can get distorted.

McKinsey's James Kaplan and Jim Boehm offer the example of reports sent by the security team to senior management. Those reports feature references to "the millions of attacks the organization faces per week or per day." While "millions of attacks" sounds impressive, those incidents are likely not from skilled cybercriminals, and are probably pretty easy to repel.

Focusing on just the number of deflected incidents can provide management with a false sense of security. Executives might think they've got a robust cybersecurity program — after all, they're catching and resolving millions of attacks a week — when in fact the real threats are flying under the radar.

Another pitfall in cybersecurity management is static reporting. Organizations may be relying on metrics that are only issued periodically, such as point-in-time assessments. Those reports are snapshots capturing just one moment. A vendor that's in compliance when a questionnaire is filled out may be out of compliance the next day.

Effective Security Performance Measurement

Our solutions are designed to be non-intrusive, quick to implement, with an actionable output adapted to your business context.

Combining standardized frameworks (NIST CSF, ISO27001, etc..), privacy and industry specific regulations (GDPR, CCPA, etc..) with technical control frameworks (CIS) we measure your control performance relative to your business context and key IT assets.

We also propose a security scoring platform to manage your 'external' rating and help you identify remediation activates to optimize your score.

Our Cyber Security Budget Benchmarking solution maps your investments to the NIST CSF model and provides a benchmark against industry peers.

Information Risk Reporting:

Infromation Risk:

The term “information security risk” refers to the damage that attacks against IT systems can cause. IT risk encompasses a wide range of potential events, including data breaches, regulatory enforcement actions, financial costs, reputational damage, and more.

Although “risk” is often conflated with “threat,” the two are subtly different. “Risk” is a more conceptual term: something that may or may not happen. A threat is a specific, actual danger.

The Steps for an Information Security Risk Assessment?

A successful cybersecurity strategy (one that can feed into larger enterprise risk management efforts) starts with a risk assessment. While all risk assessments will differ depending on your individual needs, there are certain common elements that you can use as a framework.

Identify

Start by identifying every security risk your company is currently facing or could reasonably face in the near future. Including future risks in this step is crucial, as IT risk changes frequently when new technologies develop.

Analyze

In this step, examine each risk and determine both its likelihood of occurring and the potential impact. Not every risk will require the same amount of attention, and risk analysis can help you prioritize the risks that have the largest potential for harm.

Prevent

Once you understand what risks are faced by your company, you'll need to develop controls and procedures to either minimize the damage or prevent it altogether. Your incident response strategy will also be developed during this step. The four most common types of risk response (discussed below) will help you create a risk management program that is tailored to your company and your goals.

Document

Clear documentation of your policies and risk mitigation efforts will serve you well long term. Creating a risk register with your risks, assignments, and controls will keep everyone on the same page and minimize confusion and miscommunication. Documentation will also help you revisit your policies and revise them if change is needed in the future.

Monitor and Reassess

Your security risks will change as your business operations evolve, or as new technologies emerge, or as attackers find new ways to penetrate IT defenses. So monitor the success of your security efforts, reassess your risks periodically (usually once a year), and adjust your policies, procedures, and controls as necessary.

Risk Reporting

Risk reporting is a method of identifying risks tied to or potentially impacting an organization's business processes. The identified risks are usually compiled into a formal risk report, which is then delivered to an organization's senior management or to various management teams throughout the organization.

Types of risk reporting

A fundamental truth of risk management is that risks vary from one another in scope. Some risks are relatively minor in scope. For example, a minor risk might delay a project's completion by a day or two. Conversely, businesses might occasionally face major risks that jeopardize the wellbeing of the entire organization.

Not only do risks vary by severity, but they can also vary in terms of their impact. Some risks affect a whole organization or even an entire industry. Other risks might only impact a single department or a particular account.

Because risks can vary so widely from one another, there are several different types of risk reporting. Some of the more common risk reporting types include:

- **Project risk reporting.** As the lowest level of risk reporting, this pertains to risks that may affect a particular project, such as a supply chain disruption or a change in the price of raw materials.
- **Program risk reporting.** In business, programs are generally made up of multiple projects. A program risk report generally covers any project-level risks or other risks that are significant enough to adversely impact the entire program.
- **Portfolio risk reporting.** This is generally an aggregate summary of program-level risks across an organization's entire portfolio or collection of programs.
- **Business risk reporting.** This is used for significant risks that have the potential to impact the entire organization.

What should a risk report include?

A risk report's structure can vary based on the report's intended purpose. For example, a risk report that outlines risks to employee safety would likely be

structured differently from a report meant to convey financial risks. Even so, several elements commonly included in a risk report include:

- **Executive summary:** A synopsis for senior management to identify the biggest risks.
- **Risk profile:** A description that uses numerical values to help quantify a risk. Although these risk profiles can be created in various ways, they are often based on a risk's seriousness combined with the odds of the risk actually occurring.
- **Risk capacity:** A metric reflecting how much risk an organization can afford to take. For example, a risk capacity might be a worst-case statement of how much money an organization could lose without going out of business.
- **Tolerance levels:** A measurement of how much risk an organization is willing to take on. Whereas risk capacity reflects how much an organization could lose before going bankrupt, risk tolerance measures how much an organization is willing to lose. A risk tolerance value is normally much lower than its risk capacity value and is sometimes categorized as conservative, moderate or aggressive.
- **Key risk indicators (KRI):** Metrics that are tied to a risk that has been identified. If one of these metrics reaches a threshold value, it may indicate that the identified risk is beginning to happen. As such, KRIs act as an early warning system that can give management teams time to act before an identified risk can fully occur.
- **Effective risk management:** A section of the report that explains how the organization will attempt to proactively reduce or eliminate risks that have been identified.
- **Environmental risks:** Identifies risks that the organization's activities pose to the environment due to factors such as pollution. This section is not always required, depending on the type of risk report.

Best practices for building an effective risk report

Some common best practices for creating an effective risk report include:

- Include charts or other graphical elements in the report whenever possible. These can make the report easier to digest.
- When possible, include a sunrise and sunset for each risk. The sunrise is the point at which a risk comes into play. The sunset is when an identified risk is no longer considered to be a risk. For example, in the case of making a large financial investment, the sunrise might be the time at which the contract is signed, and the sunset might be the point at which the organization has hit the break-even point for the investment.
- Each identified risk should include a clearly written risk statement explaining the threat. If necessary, a corresponding context statement can add additional clarity. For example, this section might include KRIs explaining the significance of each indicator and what the organization plans to do if certain conditions are met.
- Each risk should also include a closure criteria statement explaining what the organization is doing in terms of risk mitigation.

What a Risk Report Should Address

Every risk in the report should include a discussion of its potential *impact.* That's what senior executives and board directors want to understand as they decide how the risk should be addressed.

We can define "impact" along several lines:

- **Financial:** monetary penalties as part of regulatory enforcement action; related manpower or equipment costs for that investigation (outside counsel, new technology, and so forth); lost revenue or profits
- **Operational**: whether a risk might lead to inventory that can't be sold, factories that can't be used, business processes that might not work when necessary, and so forth
- **Strategic:** whether a risk could thwart certain long-range options, such as leaving the company with too little cash to acquire merger targets or develop new products

- **Reputational**: could a risk damage the corporate reputation among customers, consumers, or business partners

Advantages of Business Reports:

The main characteristic of a business report is that it is used as a tool for communication, analysis and decision-making. There are a number of benefits of business reports. They are:

1) Helps in making crucial business decisions: Good report writing is a key ingredient in making important decisions and taking steps towards the development of a company. The information provided in a business communication report is used to formulate strategies, take action and analyze complex problems.

2) Business reports act as a tool for managers: Business reports are a great managerial tool. They make it easy for the managers and executives in a company to oversee how the business is running. Managers use the components in business reports to achieve the following functions:

- Coordinate
- Control
- Plan
- Organize
- Analyze
- Motivate

3) Represent important facts and business data: The purpose of a business report is to communicate factual data and accurate information. Business reports rely on information collected through researching and consulting credible sources. For example, the stats about a company's monetary standing are recorded in a financial report.

4) Overcoming business challenges: Any kind of business sees its highs and lows. Over the lifespan of a business, challenges and problems of various kinds may arise. Reports help in recording and analyzing problems. These reports can be referenced in the future to solve these issues from recurring.

5) Recourse for investigation: Reports are crucial for documenting research, accidents, field studies, etc. The researchers conduct their studies and the key findings of their investigation are written in the form of reports. Along with this, they may offer solutions and recommendations for solving the issues that arise.

Disadvantages of Business Reports:

In the above section, we discussed the advantages of a business report. The importance of business reports in the effective functioning of a company is crucial. They are a vital part of any business. However, there are a few drawbacks and limitations to business reports come. They are:

1) Business reports are not interactive: One major limitation of a report is that they are not interactive. Once a report is drafted and submitted, it takes some time for the manager to review it and offer feedback. This could cause delays in communication and lead to a waste of time.

2) Business reports can be biased: Report writing must always contain factual and accurate information for effective decision-making. A writer may slip personal bias and opinions into the report. This could change the nature of a report which is supposed to be unbiased and objective.
3) Extensive use of technical jargon: Business reports should be easy to understand and skim through for busy managers. However, sometimes a writer may include extensive technical language and “insider terms” in the report making its readability suffer.
4) Outlining is time-consuming: A report usually must follow a set format and guidelines. Before writing it, a writer must collect factual information from different sources and prepare an outline for the report. This information is then written accordingly in an introduction, body and conclusion format.
This process can be time-consuming. Even in the case of informal business reports, a format and outline have to be prepared.
5) Limited Time Span: As a company carries operations, the need for reports increases. A report is prepared for a specific time and purpose. After this purpose is achieved, the report becomes redundant. This makes the usefulness of a report valid only for a limited amount of time.

Information Security Compliance Monitoring:

Information security

- **Confidentialit**y, ensuring that only those who are authorized and genuinely need the information for their job ("need-to-know" principle) can access the relevant data, therefore avoiding problems of unintended leaks or deletions of sensitive information.
- **Integrity**, ensuring that the information and its processing methods are accurate and complete, therefore preventing possible unauthorized alterations.
- **Availability,** ensuring that authorized users can access the information and its associated assets when they need to, guaranteeing access to the company's critical systems at all times through the preparation of business continuity plans.

Information Security is an essential part of Indra's business strategy due to the impact it has on its own business and its customers' business. The company has therefore developed an Information Security Management System, certified under standard ISO 27001, to define, implement and improve the most effective controls and procedures to minimize and manage risks in its internal processes, daily operations, the development and execution of programs and services from the commercial phase to the operation, and in its customer management processes.

What is InfoSec compliance?

Infosec compliance is the process of following industry-specific laws, regulations, and standards related to information security. It involves implementing policies and procedures to ensure that an organization's data is secure from unauthorized access or modification. Compliance also includes regularly testing systems for vulnerabilities and responding quickly to any threats that are identified. The correlation between information security and compliance is strong. Information security measures are essential for organizations to ensure that they meet their regulatory and legal obligations regarding data protection, privacy, and other areas of compliance. By implementing appropriate controls, organizations can reduce the risk of a breach or data loss while also ensuring they remain compliant with applicable laws and regulations.

Identifying and monitoring infosec cyber security risks is an essential part of compliance. It allows organizations to identify potential threats, assess their likelihood, and take steps to reduce or eliminate them. This helps ensure that the organization's data and systems are secure from unauthorized access or disruption. Additionally, it provides the necessary information for creating effective countermeasures against cyber-attacks. By identifying risks early on, organizations can more quickly respond to any incidents they may experience while also reducing their financial losses.

What is an information security assessment?

An information security assessment is an analysis of the potential risks and vulnerabilities associated with a company's IT systems, networks, applications, and data. It provides organizations with insight into their current security posture and helps them identify any gaps or weaknesses in their security policies and procedures that need to be addressed. The assessment may also include recommendations on how to improve the overall security of the organization's infrastructure.

What are the infosec compliance requirements?

Develop a comprehensive information security policy that outlines appropriate usage of hardware and software, data protection, access control, incident response, and more.

Ensure that all personnel is trained on proper security measures when handling sensitive data or systems.

Implement technical controls such as firewalls, antivirus/anti-malware software, encryption for data in transit or at rest, network segmentation, and patch management processes to prevent unauthorized access to your organization's networks or systems.

Utilize strong authentication methods such as multi-factor authentication (MFA) for user accounts with elevated privileges or system access rights to protect against malicious actors attempting to gain unauthorized entry into your environment through stolen credentials or other means.

Establish and maintain an incident response plan to quickly identify, contain, remediate, and report security incidents as they occur.

Regularly monitor logs and network traffic for suspicious activity or malicious behavior that could indicate a potential breach of your organization's networks or systems.

Ensure compliance with applicable industry data protection regulations such as HIPAA, PCI-DSS, GDPR, etc., depending on the type of data being processed by your organization and its geographical location(s).

Perform regular risk assessments to identify potential threats and vulnerabilities in your environment, and develop appropriate mitigation measures.

The importance of a compliance InfoSec cover letter

A compliance infosec cover letter is important for any organization that needs to ensure its security measures meet the required standards. It provides a detailed overview of the company's security policies and procedures, as well as how they are monitored and implemented. This type of letter can help protect an organization from potential legal issues related to data protection, privacy regulations, or other security-related matters.

The benefits of implementing an effective compliance program

1. Increased efficiency

Implementing an effective compliance program can help streamline processes and procedures, making it easier for staff to identify and address potential regulatory issues quickly and efficiently. This increased efficiency can reduce costs associated with non-compliance, saving time and money in the long run.

2. Improved risk management

Compliance programs provide organizations with a framework to manage risks related to regulations and laws. By monitoring compliance activities on a regular basis, organizations can identify areas of risk before they become major problems, enabling them to take proactive steps to mitigate those risks as necessary.

3. Enhanced reputation

An effective compliance program helps demonstrate an organization's commitment to ethical business practices, which increases customer confidence in the company. This can help to boost the company's reputation, leading to increased sales and revenue.

4. Improved governance

Compliance programs provide organizations with a structure for establishing and enforcing internal policies and procedures related to ethical business practices. This helps ensure that all employees are held accountable when it comes to following regulations, providing better governance of the organization as a whole.

5. Increased transparency

With an effective compliance program in place, organizations have greater transparency into their operations and activities, allowing them to identify potential areas of risk before they become major issues. This increased visibility also helps build trust between customers and the organization by demonstrating its commitment to responsible business practices.

Security Monitoring and Improvement Best Practices:

1. Conduct a Thorough Network Audit

It is crucial to perform a thorough network audit to identify the loopholes and weaknesses of any system or network. With this thorough network audit, you will identify the weakness in the network design and posture. Through this network audit, your organization will identify and assess,

- Security Vulnerabilities, if any
- Unneeded and Unwanted applications

- Any anti-virus, anti-malware, or suspicious activity/software
- Third-party application/vendor assessment
- Identifying any other security gaps

So, with this detailed and thorough network audit, you will identify the weaknesses and start converting them into strengths with an incredible network security monitoring system.

2. Use Effective Tools that offer exceptional network visibility.

In today's digital world, where everything has become interconnected, it is essential to be aware of your network environment and the traffic that traverses it. Without monitoring your network and its traffic, you won't be able to identify threats, vulnerabilities, and mistakes, which can compromise your network's security and your data's security. So, integrating a professional, affordable, impactful network monitoring tool will constantly add more value to your network security.

3. Deploy Enhanced Security for Routers

Any attacker can efficiently perform a security breach by hitting the reset button on the router. Though it sounds a little strange, it's true. Hackers can gain access to your network and home network by resetting the router. This is how they do it. Hackers look for open Wi-Fi networks and try to get into them by resetting the router. When reset, the router would ask for a username and a password. Hackers then enter the default username and password in the router's manual. A hacker would then access the router and change the admin username and password, giving them access to your network.

So, ensure that you always keep your routers in a secured or locked location for enhanced security.

4. Use a Private IP Address

If you're setting up a server, you'll likely use a public IP address. But what is a public IP address? An IP address is a set of numbers that is used to identify your server on the internet. An IP address is all fine and dandy until you need to keep the server behind a firewall. But how can you do that

if the server's IP address is public? The answer is to use a private IP address.

A private IP address is an IP address that is not visible on the internet. It is only visible within your LAN (local area network) or VPN (a virtual private network). Therefore, if you have a server that needs to stay behind a firewall, make sure you use a private IP address!

5. Stop Using File-Sharing Features

File sharing is a great way to quickly and easily transfer files from one computer to another – but it is also an excellent way for attackers to take over your computer! Almost all files shared over a network are in plain text format, which means that any hacker who wants to get a hold of your files can snoop around for files that look interesting. As a result, it is essential to disable file-sharing features on your devices.

Plenty of secure, encrypted file-sharing services are available if you are interested in transferring large files from one computer to another. These services allow you to send large files without the risk of them being stolen by hackers.

****