<u>UNIT 1</u>

1.1 Cyber security

Cyber security is the most concerning matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organizations, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and are focusing on adopting all possible measures to deal with cyber threats.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

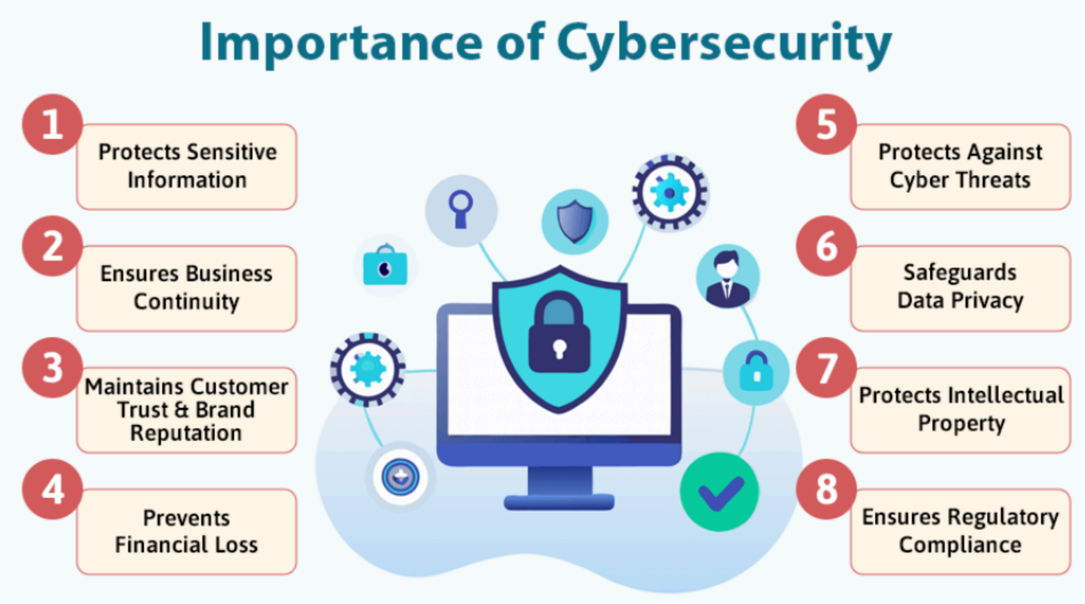
Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

It is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.

It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.

It manages the set of techniques used to save the integrity of networks, programs and data from unauthorized access. It refers to the body of technologies, processes, and it may also be referred to as information technology security.

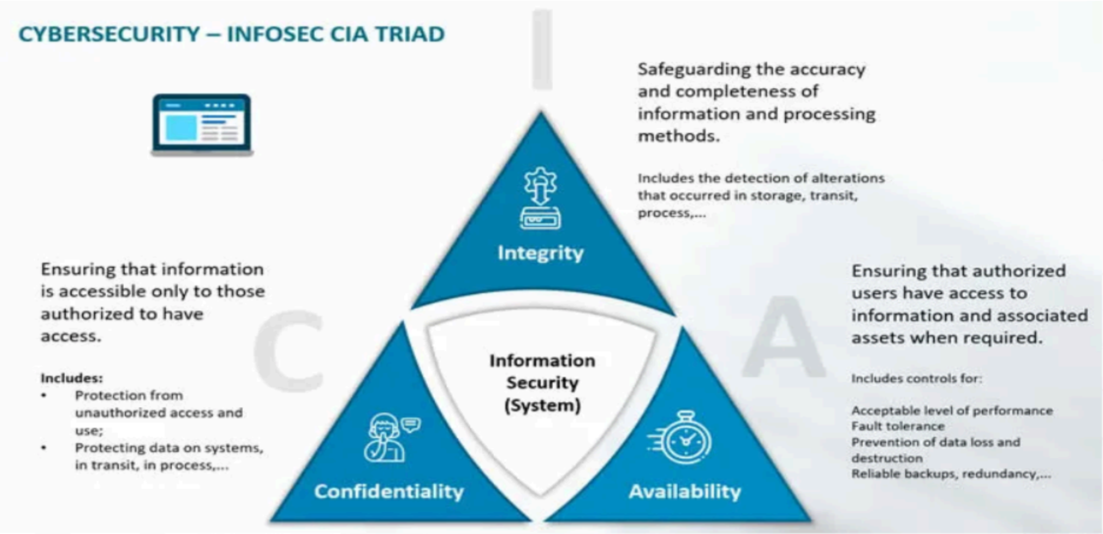
Importance of Cyber Security


Importance of Cybersecurity
1 Protects Sensitive Information
2 Ensures Business Continuity
3 Maintains Customer Trust & Brand Reputation
4 Prevents Financial Loss
5 Protects Against Cyber Threats
6 Safeguards Data Privacy
7 Protects Intellectual Property
8 Ensures Regulatory Compliance

1. **Protects Sensitive Information**: Cybersecurity safeguards personal and corporate data from unauthorized access, ensuring that sensitive information remains secure.

2. **Ensures Business Continuity:** Cybersecurity keeps businesses operational by defending against potential disruptions, even in the face of cyber threats.
3. **Maintains Customer Trust and Brand Reputation:** Proper cybersecurity practices protect customer data, fostering trust and loyalty, which are crucial for a strong brand reputation.
4. **Prevents Financial Loss:** Cybersecurity helps mitigate the financial damages associated with data breaches, fraud, and system outages, which can be costly.
5. **Protects Against Cyber Threats:** It protects against threats such as phishing, ransomware, and malware, which can cause system disruptions and data loss.
6. **Safeguards Data Privacy:** Cybersecurity guarantees the confidentiality of sensitive data, whether personal or business-related, keeping it out of unauthorized hands.
7. **Protects Intellectual Property:** Companies rely on cybersecurity to prevent intellectual property theft, ensuring their competitive advantage remains intact.
8. **Ensures Regulatory Compliance:** Many industries have strict data protection rules, and strong cybersecurity helps meet these standards, preventing penalties and legal problems.

CIA Triad


CYBERSECURITY – INFOSEC CIA TRIAD
I
Integrity
C
A
Information Security (System)
Confidentiality
Availability

Safeguarding the accuracy and completeness of information and processing methods.

Includes the detection of alterations that occurred in storage, transit, process,...

Ensuring that information is accessible only to those authorized to have access.

Includes:
- Protection from unauthorized access and use;
- Protecting data on systems, in transit, in process,...

Ensuring that authorized users have access to information and associated assets when required.

Includes controls for:

Acceptable level of performance
Fault tolerance
Prevention of data loss and destruction
Reliable backups, redundancy,...

Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

Confidentiality

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.
Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

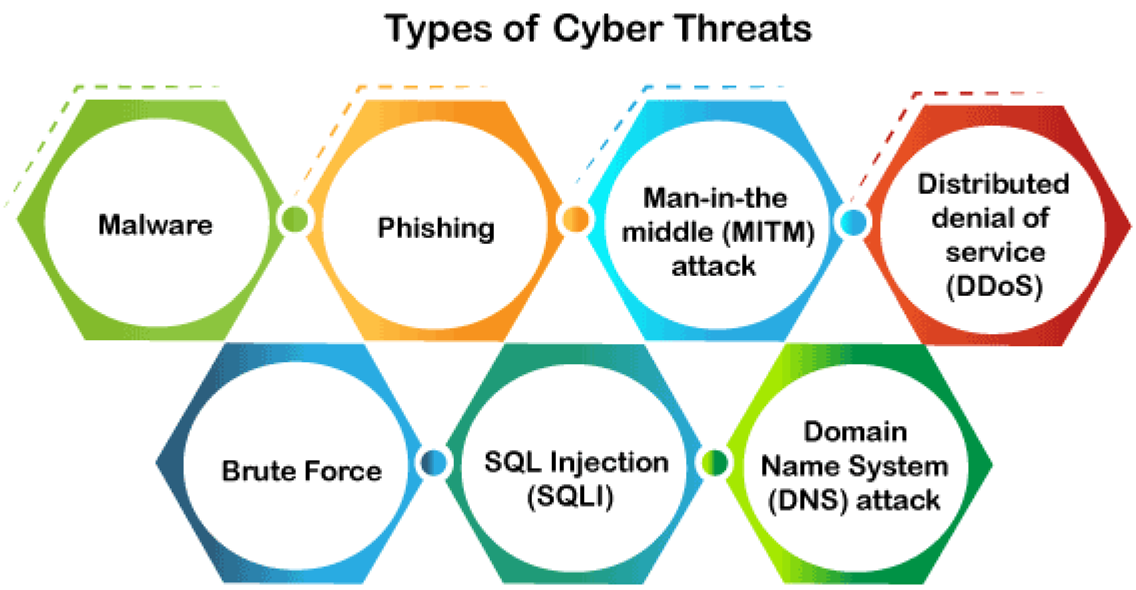
Integrity
Data integrity is what the "I" in CIA Triad stands for.
This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability
This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

1.2 Threats and its types

A threat in cyber security is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupt digital life in general.

The cyber community defines the following threats available today:



Types of Cyber Threats
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

https://www.javatpoint.com/what-is-cyber-security

https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

https://www.baeldung.com/cs/security-interruption-interception-modification-fabrication

Malware

Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The following are the important types of malware created by the hacker:

- **Virus**: It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stealing information, or damaging devices.
- **Spyware**: It is a software that secretly records information about user activities on their system. For example, spyware could capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.
- **Trojans**: It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.
- **Ransomware:** It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.
- **Worms:** It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.
- **Adware:** It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this program is to generate revenue for its developer by showing the ads on their browser.
- **Botnets:** It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Phishing

- When a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details, and passwords.
- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email.
- The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.
- Example: Phishing is a type of cybercrime in which a sender seems to come from a genuine organization like PayPal, eBay, financial institutions, or friends and co-workers. They contact a target or targets via email, phone, or text message with a link to persuade them to click on that link. This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords.

Man-in-the-middle (MITM) attack

- A man-in-the-middle attack is a type of cyber threat (a form of eavesdropping attack) in which a cybercriminal intercepts a conversation or data transfer between two individuals.
- Once the cybercriminal places themselves in the middle of a two-party communication, they seem like genuine participants and can get sensitive information and return different responses. The main objective of this type of attack is to gain access to our business or customer data.
- For example, a cybercriminal could intercept data passing between the target device and the network on an unprotected Wi-Fi network.

Distributed denial of service (DDoS)

It is a type of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses that can make the system unusable, overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital functions.

Brute Force

A brute force attack is a cryptographic hack that uses a trial-and-error method to guess all possible combinations until the correct information is discovered. Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

SQL Injection (SQLI)

SQL injection is a common attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.

Domain Name System (DNS) attack

A DNS attack is a type of cyberattack in which cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It is a severe cybersecurity risk because the DNS system is an essential element of the internet infrastructure.

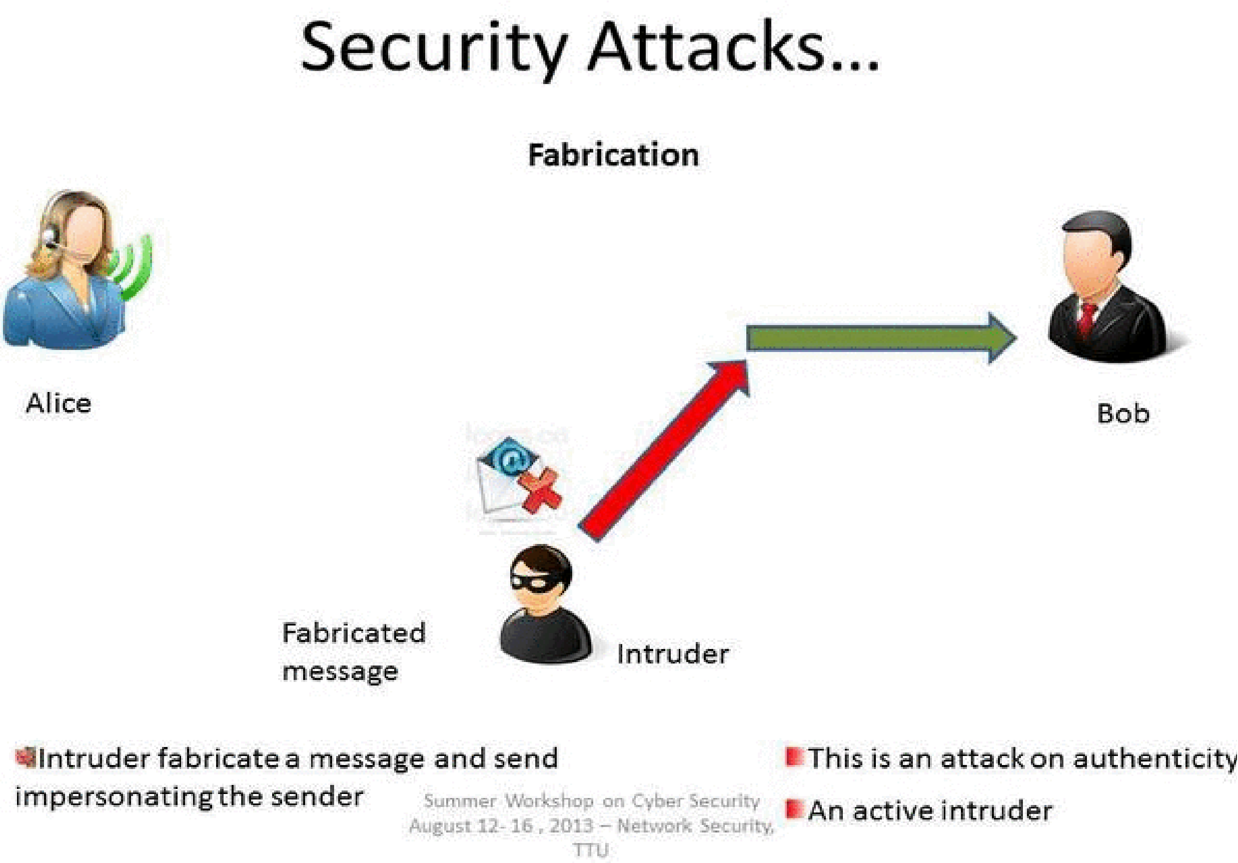
In an Information Security context there are 4 broad based categories of attacks:

1. Fabrication
2. Interception
3. Interruption
4. Modification

1. Fabrication

As stated above, *fabrication* is one of the four broad-based categories used to classify attacks and threats. A fabrication attack creates illegitimate information, processes, communications or other data within a system.

Often, fabricated data is inserted right alongside authentic data. When a known system is compromised, attackers may use fabrication techniques to gain trust, create a false trail, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system.



Security Attacks…

Fabrication

- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

Examples of Fabrication attacks include:

- SQL Injection
- Route Injection
- User / Credential Counterfeiting
- Log / Audit Trail Falsification
- Email Spoofing

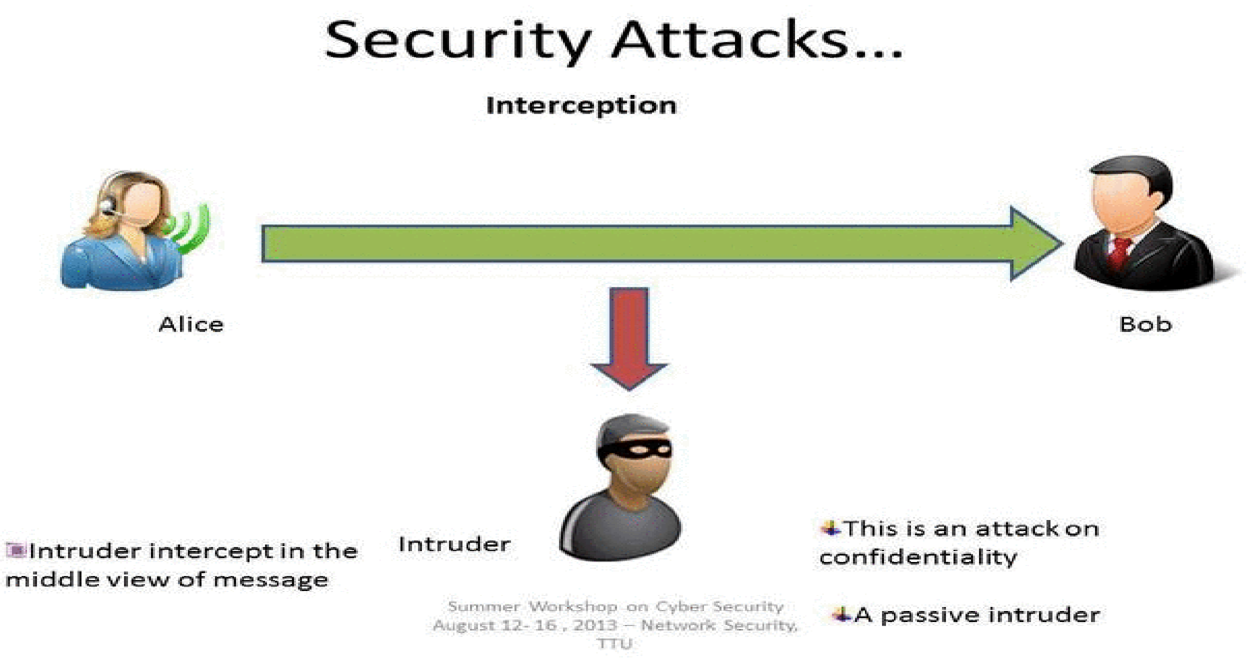
Mitigate the attack :

- Use of Authentication and authorization mechanisms
- Using Firewalls

- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

2. Interception

An interception is where an unauthorized individual gains access to confidential or private information. **Interception attacks** are attacks against the **confidentiality** objective of the CIA Triad.



Security Attacks...

Interception

▣Intruder intercept in the middle view of message

✚This is an attack on confidentiality

✚A passive intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

Examples of Interception attacks:

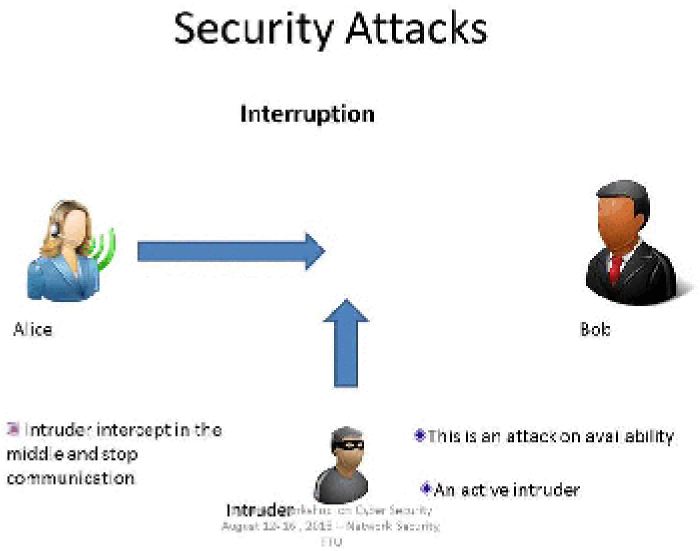
- Eavesdropping on communication.
- Wiretapping telecommunications networks.
- Illicit copying of files or programs.
- Obtaining copies of messages for later replay.
- Packet sniffing and key logging to capture data from a computer system or network.

Mitigate the attack :

- Using Encryption - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Interruption

In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the availability of the network.



Security Attacks

Interruption

- Intruder intercept in the middle and stop communication
- This is an attack on availability
- An active intruder

Workshop on Cyber Security August 12-16 , 2013 – Network Security ETU

Figure

Examples of Interruption attacks :

- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved.

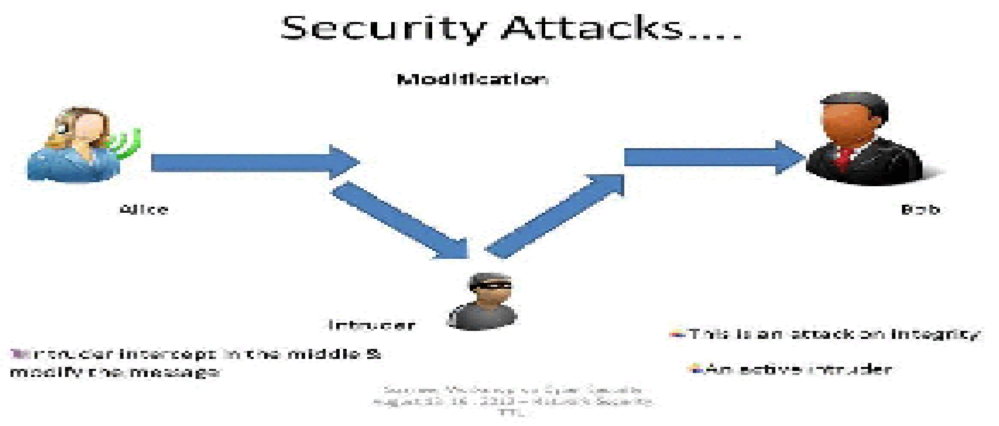
Mitigate the attack:

- Use Firewalls - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from DoS attack traffic.
- Keeping backups of system configuration data properly.
- Replication.

Modification

Modification is an attack against the integrity of the information. Basically there are three types of modifications.

- Change: Change existing information. The information already existed but was incorrect. Change attacks can be targeted at sensitive information or public information.
- Insertion: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.
- Deletion : Removal of existing information.



Security Attacks....

Modification

Intruder intercept in the middle & modify the message

This is an attack on integrity

An active intruder

Examples of Modification attacks include:

- Modifying the contents of messages in the network.
- Changing information stored in data files.
- Altering programs so they perform differently.

- Reconfiguring system hardware or network topologies.

Mitigate the attack :

- Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.
- Using Encryption mechanisms
- Traffic padding
- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

1.3 Digital Asset

Digital assets include photos, manuscripts, documents, data, cryptocurrencies, and much more.

Digital assets are increasingly important because they are becoming more a part of our professional and personal lives while continuing to be essential for businesses and governments.

Digital assets have morphed into more than the words, pictures, videos, audio, and documents we associate with the term. When Bitcoin was introduced in 2009, it brought with it the blockchain—a distributed public ledger secured by a consensus mechanism. The concept was not new because data itself had become a valuable digital asset that required security measures, management, and storage. Distributed ledgers and the information contained in them had been around for some time.

However, it was new to most people who lived and worked outside of data science, data management, data analysis, or any other field requiring large distributed data networks.

Types of Digital Assets

There are many different types of digital assets. Here is a list of many of the familiar ones:

- Photos
- Documents
- Videos
- Books
- Audio/Music
- Animations

- Illustrations
- Manuscripts
- Emails and email accounts
- Logos
- Metadata
- Content
- Social media accounts
- Gaming accounts

Newer digital assets are based on blockchain or similar technologies:

- Nonfungible tokens
- Cryptocurrency
- Tokens
- Crypto Assets
- Tokenized Assets
- Security Tokens
- Central Bank Digital Currencies

Importance of Digital Assets

When you look at a list of the digital items that can be considered assets, it becomes clear that our lives are more digitally based than ever. For example, when we want to learn about something, we turn to digitally hosted information because it is quicker and easier than driving to a library, hoping they have the resources you need.

Our photos, entertainment, and important documents are mostly in digital form. Businesses and governments keep and store data and information, all of which have different values depending on how they can be used.

1.4 Security Incident

A security incident is an event that could indicate that an organization's systems or data have been compromised or that security measures put in place to protect them have failed.

In IT, an event is anything that has significance for system hardware or software and an incident is an event that disrupts normal operations. Security events are usually distinguished by the degree of severity and the associated potential risk to the organization.

Example: If a single user is denied access to a requested service, for example, that can be considered a security event because it might indicate a compromised system. But the access failure could also be caused by many other things. The common theme for most security events, no matter what caused them, is that they don't typically have a severe impact on the organization. However, if large numbers of users are denied access, it likely indicates a more serious problem, such as a distributed denial-of-service (DDoS) attack, so that event can be classified as a security incident because of its disruptive impact on operations.

Examples of security incidents include the following:

- Attempts from unauthorized users and sources to access systems or data.
- Unplanned disruption to a service or denial of service.
- Unauthorized processing or storage of data.
- Unauthorized changes to system hardware, firmware or software.
- Insider breaches of networks, systems or information instigated by employees or contractors, including malicious attacks on systems and networks.
- A malware infection such as ransomware or a virus that compromises networks, systems or workstations or performs unauthorized actions.
- An outside cybersecurity incident that's intended to disrupt, disable, destroy or maliciously control an organization's entire computing environment or infrastructure.
- An attack designed to destroy or steal data.
- Loss or theft of computer equipment.

On the other hand, a security breach pertains to data breaches only -- not network or system access violations or malware invasions where data isn't involved. In this respect, the security breach is a subcategory of a security incident that specifically relates to unauthorized access or theft of data only. This data breach could involve the alteration and outright theft of sensitive company data such as intellectual property or customer lists. It can also involve the unauthorized access, alteration and theft of the personally identifiable information (PII) of customers, clients, patients or others that violates these individuals' privacy rights.

Examples of security breaches include the following:

- Unauthorized access to privileged and personal data.
- Stealing a computer device that contains sensitive data or PII.
- Stealing physical documents that contain sensitive or personal data.

- Data penetration that results in data corruption or destruction.
- A ransomware attack that steals data and then demands a ransom for its return.
- Access to company customer data through a third-party data broker without company or customer consent.

Security incidents cover a wide spectrum of security threats and breaches that businesses can face.

Common security incidents include the following:

- **Unauthorized access attacks**. These cybersecurity incidents involve unauthorized attempts by cybercriminals to access systems or data using authorized user accounts. These attempts can be made through brute-force attacks, phishing attacks or other password exploits to steal sensitive information.
- **Malware infections**. Malware refers to malicious software that can infect systems and jeopardize their security. Malware incidents involve the infiltration of systems by viruses, worms, ransomware or other types of malicious software.
- **Privilege escalation**. Privilege escalation attacks occur when an attacker seeks unauthorized access to an organization's network and aims to acquire additional privileges through a privilege escalation exploit. A successful exploit grants the attacker privileges beyond those of normal users. Typically, this attack occurs after the hacker has already compromised the organization's endpoint network security by gaining unauthorized access to a lower-level user account.
- **Denial-of-service attacks**. DoS attacks are designed to flood a system or network with an excessive amount of traffic so that it becomes unusable for authorized users.
- **Phishing attacks**. This is a type of social engineering attack in which the perpetrator impersonates a trusted entity via email to share malicious code or links, aiming to extract login credentials or account details from victims. More sophisticated variations, known as spear phishing attacks, involve the attacker investing additional time in researching the victim for a targeted and refined approach to information theft.
- **Insider threats**. These are various types of compromises arising from individuals within an organization, either intentionally or unintentionally, posing a security risk.

For example, a disgruntled employee seeking retribution could carry out an insider attack.

- **Security misconfigurations**. Misconfigurations in systems, networks or applications can lead to security problems because they can produce vulnerabilities that hackers can take advantage of.
- **Advanced persistent threats**. An APT is a sophisticated and prolonged attack that involves discrete infiltration, persistent presence and targeted exploitation of systems or networks.
- **Web application attacks**. This event happens when a web application is used in an attack. Web application attacks involve exploiting code-level vulnerabilities and bypassing authentication mechanisms. A specific instance is a cross-site scripting attack, where an attacker injects data, such as a malicious script, into content from typically trusted websites.

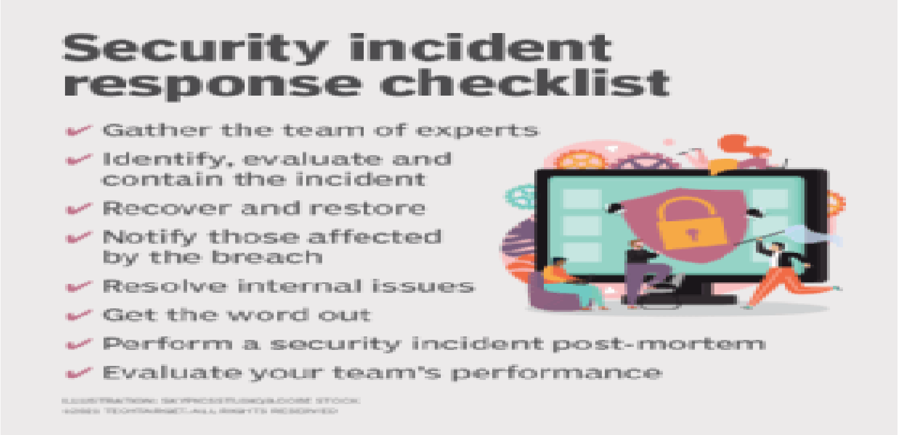
How Can I Detect Security Incidents?

There are different ways to detect if your company is under threat of a critical security incident. Different types of information security incidents will have markers for discovery.

Some methods for finding indicators of a current or future incident include:

- Look for traffic anomalies, attempts to access accounts without permission, excessive use, and access of suspicious files — this can be indicative of malicious activity.
- Servers tend to have a relatively stable and consistent volume of traffic, subject to business calendar needs and resultant fluctuations. If a company experiences an unusual traffic increase, it should look into the cause and look out for an attack.
- Unusual traffic or outages on an organization’s network, especially when it’s unexpected, can be a sign of unauthorized access.
- Employees are a main entry point for an InfoSec compromise, so restrict access appropriately and install endpoint security on company assets.
- Implement tested security tools and solutions to provide your information security program with enhanced detection and response capabilities.
- Take threats seriously — initiate your incident response protocol if your organization is being blackmailed, threatened with a cyberattack, or held for ransom.

How to respond to a security incident

- Because security breaches are actually a subset of security incidents, the tools and techniques used to address them are similar. In all cases, the goal is to subdue or resolve the incident as quickly as possible.
- 

Security incident response checklist

- ✓ Gather the team of experts
- ✓ Identify, evaluate and contain the incident
- ✓ Recover and restore
- ✓ Notify those affected by the breach
- ✓ Resolve internal issues
- ✓ Get the word out
- ✓ Perform a security incident post-mortem
- ✓ Evaluate your team's performance

- A checklist detailing the steps for responding to a security incident.
- Organizations can use the following tools and techniques to respond to security incidents:
- Gather the team. Coordinate the team of security experts who will assess the severity of the incident, communicate with management and perform mitigation.
- Identify, evaluate and contain the incident. Identify what has been compromised. If a particular network is infected but other networks aren't, immediately isolate the affected systems and network to prevent the infection from spreading. At the same time, preserve all data in the infected network for later analysis.
- Recover and restore. If systems or networks are so severely affected that they can't be operated confidently, perform a full disaster recovery and failover.
- Notify those affected by the breach. If customer, client or patient data was compromised during the incident, notify persons affected of the breach and offer to pay for the mitigation services they might require.
- Resolve internal issues. If a malicious activity was perpetrated by a company employee, notify human resources so appropriate actions can be taken.
- Get the word out. Coordinate with corporate marketing and public relations for any messaging that needs to be made to the press or the public.

- Perform a security incident post-mortem. Once the security incident is resolved, review what happened, how it happened and what steps can be taken to avoid similar incidents in the future. Revise policies and practices to reflect any changes.
- Evaluate your team's performance. Security teams should determine how long it took to detect the incident, how long it took them to resolve the issue and provide remediation, and if there was anything they could have done better.

How to prevent a security incident

Methods and tools used to prevent security incidents include the following:

- Regularly train employees to ensure they're familiar with corporate security standards and practices.
- Using internal and outside IT auditors, regularly review IT security policies and practices to ensure they're current, including penetration and vulnerability testing of networks and systems.
- Ensure that security patches to hardware and software are promptly deployed.
- Monitor physical facilities, including secured access to data centers and to closets, file cabinets and other storage areas that might contain sensitive hardcopy documents.
- Monitor and log user and data activity at networks, system workstations and internet of things (IoT) devices. Use automated real-time alerts to detect potential threats and security violations.
- Vet vendors for conformance to corporate security and governance standards.
- Form agreements with business partners that restrict the sharing of confidential information with third parties without your company's express permission.
- Enforce strong access controls by limiting access to sensitive data and critical information to only authorized users.
- Promote the use of multifactor authentication among employees, as it requires users to provide an extra form of identification besides their username and password.
- Encrypt laptops and mobile devices and lock down any equipment that's lost or has been stolen in the field.

- Stay actively connected with security communities and attend conferences to stay up to date on the most recent security risks, trends and best practices.
- Processes and tools designed to help with security incident management
- A variety of commercial incident response tools and service providers are available to assist in the handling of security incidents. Examples of these tools include the following:
- Endpoint detection and response tools. EDR software analyzes endpoint devices such as laptops, desktops and mobile phones to detect security incidents at the periphery of the enterprise, which is helpful for securing IoT environments. CrowdStrike Falcon and Symantec Endpoint Detection and Response are examples of EDR tools.
- Security information and event management tools. SIEM tools gather and analyze log data from multiple sources, including network devices, servers and applications. They create warnings for possible security incidents, correlate events and identify patterns. IBM Security QRadar, McAfee SIEM and SolarWinds Security Event Manager are examples.
- Incident response software. Incident response planning templates assist in developing and mapping an enterprisewide security incident response plan. Providers of incident response planning templates include BlueVoyant and Exabeam.
- Security orchestration, automation and response tools. SOAR tools automate incident response by integrating with security tools, orchestrating workflows and handling repetitive tasks, leading to a faster and more efficient response. Examples include Palo Alto Networks Cortex XSOAR, Splunk Phantom and Swimlane.
- Unified threat management tools. UTM products offer a full set of security features, such as a firewall, antivirus, intrusion detection and prevention, virtual private network support and threat intelligence. They help businesses manage different security functions from a single platform. Examples of UTM tools include Check Point Next Generation Firewall, Cisco Meraki and WatchGuard Network Security.
- Security training software. Security training software helps employees learn the basics of effective security practices. However, it doesn't replace the in-house security training that should be part of every new employee orientation and annual security refresher courses for current employees. Examples of security awareness training providers and platforms

include Infosec IQ from Infosec Institute, Proofpoint Security Awareness Training and SANS Institute.

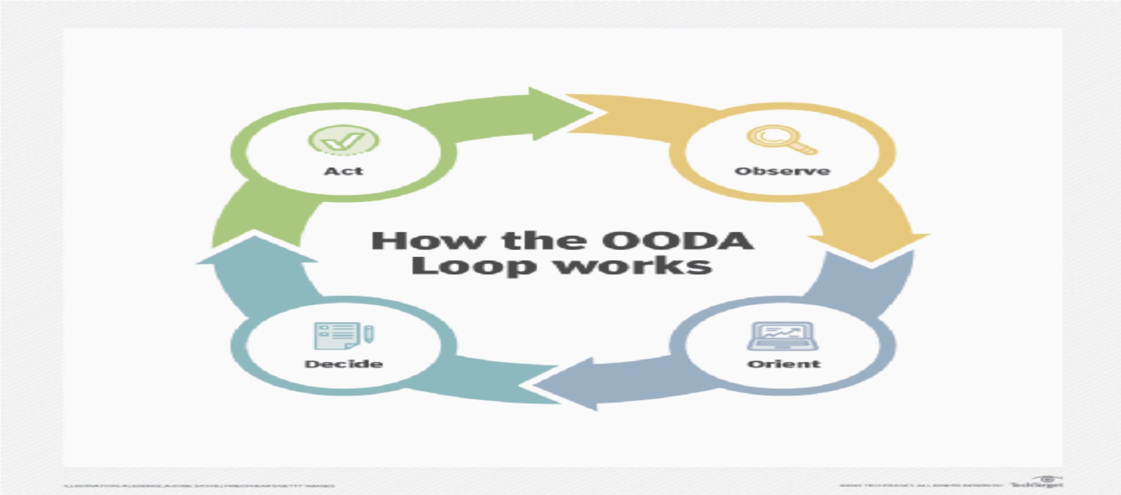
Examples of security incidents

- Here are several examples of well-known security incidents:
- Cybersecurity researchers first detected the Stuxnet worm, used to attack Iran's nuclear program, in 2010. It is still considered one of the most sophisticated pieces of malware ever detected. The malware targeted SCADA systems and spread through infected USB devices. Both the U.S. and Israel have been linked to the development of Stuxnet, and while neither nation has officially acknowledged its role in developing it, there have been unofficial confirmations that they were responsible for it.
- In October 2016, another major security incident occurred when cybercriminals launched a DDoS attack on domain name system provider Dyn, which disrupted online services worldwide. The attack hit a number of websites, including Netflix, Twitter, PayPal, Pinterest and PlayStation Network.
- In July 2017, a massive breach was discovered involving 14 million Verizon Communications Inc. customer records, including phone numbers and account PINs, which were reportedly exposed to the internet, although Verizon claimed no data was stolen. A month earlier, a researcher from security firm UpGuard found the data on a cloud server maintained by data analytics firm Nice Systems. The data wasn't password-protected, and as such, cybercriminals could have easily downloaded and exploited it, according to the security firm.
- In 2023, casino giant Caesars Entertainment fell victim to a social engineering campaign that led to the exposure of sensitive customer data, including Social Security numbers. Threat actors reportedly called the IT service desk and tricked personnel into resetting MFA factors for Okta super administrator accounts. MGM suffered a similar incident the same month, resulting in an estimated $100 million in losses.

Real-Life Examples of Information Security Incidents

- There have been many high-profile information security incidents involving major corporations that end up having a significant effect on regular folks; and an uncountable number of regular folks who have found themselves the victim of cybercrime.. In addition to the Colonial Pipeline ransomware exploitation, both Alibaba and LinkedIn have experienced large data breaches in recent years. In 2019,Alibaba experienced a leak of more than 1 billion units of user data when a developer scraped customer info, including user names and cellphone numbers from their Chinese shopping site, Taobao. The information did not end up on the black market, but after the eight-month-long theft was discovered, the culprits were caught and ultimately fined and sent to prison. It was in June 2021 that the theft of LinkedIn information for 700 million users — representing approximately 93% of their user base — was exposed when a hacker bundled data for sale on the black market. The hacker scraped data using the site's API and captured information, which included email addresses, phone numbers, geolocation information, and other social media details that could lead to follow-up social engineering attacks.

What tools does an organization need?

- 

- It depends. Certain organizations follow the OODA loop, which can provide guidance on what tools are needed and when. A military-derived approach to incident response, the OODA loop is a methodology that involves following these four steps when confronting a threat:
- **Observe.** This is the visibility into network traffic, OSes, applications and more, which can help establish a baseline for the environment and provide real-time information into what's happening before, during and after a security event.

- **Orient**. This is the detailed contextual information and intelligence on the threats that exist and what attacks they're carrying out.
- **Decide**. This refers to real-time (proactive, happening now) and forensic (reactive, after-the-fact) information on threats and anomalous behaviors that can help security teams make informed decisions on how to respond.
- **Act.** These are the steps or actions to take to address the threats, minimize their risk to and effect on the business, and bring things back to normal.
- The OODA loop isn't a set of incident response requirements, but an approach security teams can integrate with their existing incident procedures to minimize the effect security incidents could have on their organization.
- Organizations can use the OODA loop within their incident response procedures to understand which steps to take when a security incident occurs.
- Incident response sets expectations, details how things are done and uses the appropriate technologies to ensure procedures are properly addressed and enforced. This gives guidance on incident response tools and how they can help throughout the incident response process. The security team can use this information when selecting incident response software or services and provide insight into how the organization's overall security program can be improved.

Incident response tools and the OODA loop

- Organizations need technologies that provide visibility and control in an automated and repeatable fashion to ensure the network remains resilient and preserves security. This goes for preventative measures, such as multifactor authentication and granular access controls, as well as reactive measures, such as monitoring, alerting and system quarantining.
- Multiple tools can assist with response efforts across the OODA loop. Most tools fall into one of the following categories; certain tools can be used in multiple OODA loop phases:
- NetFlow and traffic analysis.
- Vulnerability management.
- SIEM.

- Endpoint detection and response (EDR).
- Security orchestration, automation and response (SOAR).
- Firewall, intrusion prevention systems (IPSes) and DoS mitigation.
- Forensics analysis.
- Awareness and training.
- Let's look at each step in the OODA loop and which technologies fit into them.

- **Observe**
- This part of the OODA loop requires tools to create a baseline, establish what normal behavior looks like and discover anomalies. Given what's involved, this category encompasses the greatest number of tools:
- Data classification.
- Data loss prevention.
- Cloud access security brokers.
- EDR.
- Antimalware and antivirus.
- IPS.
- NetFlow software.
- Network traffic analysis tools.
- SIEM.
- Vulnerability analysis and management tools.
- The more information you have, the better, which is why these types of tools are critical. They help security teams become familiar with their networks and determine what might be at risk before an incident occurs.

- **Orient**

- Tools used in this step in the OODA loop provide information and context regarding the severity of security events that have occurred. This helps with the scope and effect, which can lead to better decision-making in the next step. Consider the following tools:
- Threat research.
- Threat intelligence.
- Investigation tools.
- Response tools.
- **Decide**
- Incident response tools help security teams reach this step. But this phase of the OODA loop involves people, including security committee or incident response team members, as well as executive management, legal and other stakeholders.
- During this step, critical business decisions are made, including what to do or not do in terms of response efforts. The most important piece goes back to the two previous steps -- observing and orienting -- to ensure teams have all the necessary information to make better decisions.
- In the decide phase, teams might reference security policies, standards, contracts and compliance requirements to ensure they are doing what they said they were going to. The outcome of this step is coming up with a clear plan for remediation efforts. While there are no specific tools for this step, teams might have to go back and interact with incident response and related security tools, depending on the situation.
- **Act**
- This step is where things get done and when teams act on decisions made during the decide phase using incident response and security tools.
- Tools used here include the following:
- Antimalware.
- Backup and recovery.
- Forensics evidence gathering and preservation.
- SOAR tools.
- Information and access systems.

- Patch management.
- Security awareness training.
- SIEM and vulnerability management tools also might be used to ensure security threats have been eliminated and vulnerabilities addressed. Organizations using a change management system might need to use it to follow internal requirements and document what has been done.
- How to choose the right tool for your company's needs
- Each organization's incident response needs are unique. But just because an incident response tool seems to fit the bill now doesn't mean it will over the long haul. Many considerations must be made, and questions must be asked before investing time, money and effort into these products. Be sure to understand the challenges and risks the business is trying to address.
- Rather than simply procuring incident response tools that may or may not be what the organization needs, the security team must determine what's best for the business. This involves asking questions, such as the following:
- What is the organization trying to accomplish? What requirements need to be met to reach these goals?
- What is the organization required to protect? What is it protecting it from?
- Does the organization need to protect the entire network or just a subset of critical systems?
- What challenges does the business currently have in terms of visibility, control and expertise that could be mitigated by the right tools?
- What type of reporting does the organization need for executive management, audit and so on? Will these tools help the security team meet these requirements?
- How will tools affect the business's current network complexity and security posture? Does the organization have the internal resources necessary to properly implement and administer these tools?
- How will security policies, standards and plans need to be adjusted? How will IT and security workflows and processes need to be adjusted?

- How will the organization measure success? Will the tools themselves help in that regard?
- How will incident response tools complement or hinder vulnerability and penetration testing efforts?
- What is the budget? Will it meet both the upfront and ongoing costs of these tools?
- Whether a security team takes the OODA loop approach or not, over time, it will be necessary to tweak incident response tools and overall methodologies. As the security team discovers the patterns and nuances of network traffic and system behaviors, for example, it will need to fine-tune the tools in use to ensure they provide the information needed.
- Teams will also need to determine if the data collected helps or hinders incident response decision-making. Teams might need to establish new security standards or adjust security policies and procedures accordingly, as well as update the organization's formal incident response plan as processes and tools evolve.
- Top incident response tools to consider
- Security teams can help ensure a successful incident response process by asking potential vendors the following questions:
- How will your product or service better protect the organization's network?
- How can your product save the organization time, effort and money?
- What are your product's components? What does each one do?
- Beyond security oversight and incident response, what compliance regulations does your product address?
- Can you provide use cases or specific case studies of how your tool has helped other organizations handle similar cybersecurity incidents?
- What versions of your product are available? Are they on premises or cloud-based?
- How does your company differentiate itself from its competitors?
- Teams should ask for reference accounts in the organization's industry and talk to those people directly. They should also seek out trial versions or do an in-depth proof of concept with certain vendors to see how their incident response tool will work in their team's unique environment. Teams should also discuss ongoing support and training with

prospective vendors and ask what key partnerships they have in terms of integrating with other security tools. Integrations are beneficial because they can take advantage of the organization's existing security technologies.

- Security buyers looking for more information on incident response software and service providers should read our coverage on the following vendors, service providers and tools:
- AT&T Managed Threat Detection and Response.
- AT&T USM Anywhere.
- BAE Systems Incident Response.
- CrowdStrike Falcon Insight XDR.
- Cyderes Enterprise Managed Detection & Response.
- Cynet 360 AutoXDR Platform.
- Cynet CyOps.
- Datadog Cloud SIEM.
- Exabeam Fusion.
- IBM Security QRadar.
- KnowBe4 PhishER.
- LogRhythm SIEM.
- Mandiant Incident Response Services.
- NTT Managed Detection and Response.
- Secureworks Emergency Incident Response.
- Splunk Enterprise Security.
- Sygnia Incident Response.
- Trustwave Managed Detection and Response.
- Verizon Incident Response & Investigation.
- XMatters.

1.5 Difference between Information and Data security

Since data breaches and cyber threats are on the rise, a comprehensive understanding of information security and privacy is essential. Although the two terms are often used interchangeably, they encompass different aspects of protecting sensitive information.

Information Security

- Information security refers to the practices, policies, and measures used to protect information assets from unauthorized access, disclosure, modification, or destruction.
- It is a holistic approach to protecting data, systems, networks and applications from a variety of internal and external threats. And external threats include not only hackers, but also environmental disasters (e.g., fires, floods, natural disasters in general), as well as unexpected external circumstances that you don't even think about at first.
- Information security therefore involves the implementation of technical, administrative and physical controls to mitigate risks and ensure the confidentiality, integrity and availability of information.
- Therefore, information security includes the implementation of technical, administrative and physical controls to mitigate risk and ensure the confidentiality, integrity and availability of information using an internationally recognized standard such as ISO 27001.

Data Protection

- Data protection, on the other hand, is a subarea of information security that focuses specifically on protecting personal or sensitive data from unauthorized access, use, disclosure, or loss.
- This involves compliance with legal and regulatory requirements relating to the collection, storage, processing and disposal of data.
- Data protection measures are aimed at ensuring the protection of the privacy and rights of individuals and mitigating the potential harm that can result from data breaches or misuse.
- Data protection measures aim to protect the privacy and rights of individuals and to minimize the potential damage that can result from data breaches or data misuse. The GDPR addresses this protection through regulations.

Key Differences between Information Security and Data Protection

Scope:

- Information security encompasses a broader spectrum of practices, including technical, administrative, and physical controls, to protect all types of information assets within an organization.
- Data protection, however, narrows down its focus to safeguarding personal or sensitive data, typically governed by privacy laws and regulations.

Objectives:

- Information security aims to ensure the confidentiality, integrity, and availability of all information assets, not limited to personal data. It encompasses measures such as network security, access controls, encryption, incident response, and disaster recovery.
- Data protection primarily emphasizes the privacy and lawful processing of personal data, focusing on aspects like consent, purpose limitation, data minimization, data retention, and individual rights.

Legal and Regulatory Framework:

- Information security is driven by industry best practices, standards, and frameworks, such as ISO 27001, NIST Cybersecurity Framework, and CIS Controls. Compliance with these standards helps organizations establish a robust security posture.
- Data protection, in contrast, is heavily influenced by privacy laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. Compliance with these regulations is essential to protect individuals' privacy rights.

Focus on Individuals:

- Information security is concerned with protecting the overall information ecosystem, including organizational data, intellectual property, and trade secrets, without necessarily focusing on individual data subjects.

- Data protection places a strong emphasis on the rights and privacy of individuals, aiming to ensure that personal data is collected, processed, and stored in a manner that respects individuals' rights and freedoms.
- While information security and data protection share a common goal of protecting data, they operate at different levels and serve distinct purposes.
- Information security is a comprehensive approach to safeguarding all types of information assets, while data protection is a subset that specifically focuses on personal or sensitive data.
- Organizations must prioritize both information security and data protection to establish a robust and compliant data protection framework, ensuring the confidentiality, integrity, and availability of data while respecting individuals' rights and privacy.
- By understanding the differences between these two concepts, businesses can effectively tailor their strategies and allocate resources to mitigate risks and address the evolving landscape of cybersecurity and data privacy.

Difference Between Cyber Security and Information Security

● **Cyber Security**	● **Information Security**
● It is the practice of protecting the data from outside the resource on the internet.	● It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
● It is about the ability to protect the use of cyberspace from cyber attacks.	● It deals with the protection of data from any form of threat.

● Cybersecurity to protect anything in the cyber realm.	● Information security is for information irrespective of the realm.
● Cybersecurity deals with the danger in cyberspace.	● Information security deals with the protection of data from any form of threat.
● Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	● Information security strikes against unauthorized access, disclosure modification, and disruption.
● Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	● Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
● It deals with threats that may or may not exist in the cyber realm such as protecting your social	● It deals with information Assets and integrity, confidentiality, and availability.

media account, personal information, etc.	
● Acts as the first line of defence.	● Comes into play when security is breached.
● Primarily deals with digital threats, such as hacking, malware, and phishing	● Addresses a wider range of threats, including physical theft, espionage, and human error
● Protects against unauthorized access, use, disclosure, disruption, modification, or destruction of digital information	● Protects the confidentiality, integrity, and availability of all types of information, regardless of the medium in which it is stored
● Relies on a variety of technologies, such as firewalls, antivirus software, and intrusion detection systems	● Uses a range of technologies, including encryption, access controls, and data loss prevention tools
● Requires specialized knowledge of computer systems and networks, as well as programming and	● Requires knowledge of risk management, compliance, legal and regulatory issues, as well as technical knowledge

software development skills	
● Emphasizes protecting the data itself, regardless of where it is stored or how it is transmitted	● Emphasizes the protection of information assets, which includes data but also other information such as intellectual property, trade secrets, and confidential customer information
● Deals with constantly evolving threats, such as new forms of malware and emerging cybercrime techniques	● Deals with a wide range of threats, including physical security breaches, insider threats, and social engineering attacks