**ASSIGNMENT 1 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 5: Security | | |
| **Submission date** | 23/04/2023 | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** | Nguyễn Hải Việt | **Student ID** | GCD210136 |
| **Class** | GCD1101 | **Assessor name** | Đặng Quang Hiển |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** |  |

**Grading grid**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| P1 | P2 | P3 | P4 | M1 | M2 | D1 |
|  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Lecturer Signature:** | | |

Contents

[Task 1 - Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences (P1) 3](#_Toc133161196)

[**1.** **Define threats** 3](#_Toc133161197)

[A) It threats define 4](#_Toc133161198)

[B) Some of threats 4](#_Toc133161199)

[**2.** **Identify threats agents to organizations** 8](#_Toc133161200)

[**3.** **List type of threats that organizations will face** 8](#_Toc133161201)

[**4.** **What are the recent security breaches? List and give examples with dates** 9](#_Toc133161202)

[**5.** **Discuss the consequences of this breach** 10](#_Toc133161203)

[**6.** **Suggest solutions to organizations** 12](#_Toc133161204)

[Task 2 - Describe at least 3 organisational security procedures (P2) 13](#_Toc133161205)

[1. Acceptable Use Policy (AUP) 13](#_Toc133161206)

[2. Access Control Policy (ACP) 13](#_Toc133161207)

[3. Change Management Policy 13](#_Toc133161208)

[4. Information Security Policy 13](#_Toc133161209)

[5. Incident Response (IR) Policy 14](#_Toc133161210)

[6. Remote Access Policy 14](#_Toc133161211)

[7. Email/Communication Policy 14](#_Toc133161212)

[8. Disaster Recovery Policy 14](#_Toc133161213)

[9. Business Continuity Plan (BCP) 14](#_Toc133161214)

[Task 2.1 - Propose a method to assess and treat IT security risks (M1) 15](#_Toc133161215)

[1. Discuss methods required to assess security threats? E.g., Monitoring tools 15](#_Toc133161216)

[2. What is the current weakness or threats of an organization? 16](#_Toc133161217)

[3. What tools will you propose to treat IT security risks? 16](#_Toc133161218)

[Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS (P3) 18](#_Toc133161219)

[1. Discuss briefly firewalls and policies, their usage and advantages in a network 18](#_Toc133161220)

[2. How does a firewall provide security to a network? 19](#_Toc133161221)

[3. Show with diagrams the example of how firewall Works 20](#_Toc133161222)

[4. Define IDS, its usage, and show it with diagrams examples 22](#_Toc133161223)

[5. Write down the potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network 23](#_Toc133161224)

[Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4) 23](#_Toc133161225)

[1. Define and discuss with the aid of diagram DMZ. 23](#_Toc133161226)

[2. Define and discuss with the aid of diagram static IP. Focus on its usage and security function as advantage 25](#_Toc133161227)

[3. Define and discuss with the aid of diagram NAT. Focus on its usage and security function as advantage 26](#_Toc133161228)

[Task 4.1 - Discuss three benefits to implement network monitoring systems with supporting reasons (M2) 28](#_Toc133161229)

[1. List some of the networking monitoring devices and discuss each of them. 28](#_Toc133161230)

[2. Why do you need to monitor networks? 29](#_Toc133161231)

[3. What are the benefits of monitoring a network? 30](#_Toc133161232)

[\*REFERENCES: 31](#_Toc133161233)

[Figure 1: Malware 4](#_Toc133143537)

[Figure 2: cyber attack 5](#_Toc133143538)

[Figure 3: social engineer 7](#_Toc133143539)

[Figure 4: data leak 7](#_Toc133143540)

[Figure 5: FireWalls 18](#_Toc133143541)

[Figure 6: diagram of firewalls 21](#_Toc133143542)

[Figure 7: IDS diagram 22](#_Toc133143543)

[Figure 8: DMZ diagram 24](#_Toc133143544)

[Figure 9: static IP diagram 25](#_Toc133143545)

[Figure 10: NAT diagram 28](#_Toc133143546)

# Task 1 - Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences (P1)

1. **Define threats**
2. It threats define

An entity, situation, capacity, action, or event that might be harmful exists when there is a possibility for a security breach. a situation or incident that might lead to the loss of assets and the unfavourable effects that would follow.

1. Some of threats
2. **Malware**:

Malware, short for malware, is a general term for viruses, worms, trojans, and other harmful computer programs that hackers use to destroy and gain access to sensitive information.

In other words, software is identified as malicious software based on its intended use, rather than a specific technique or technology used to build the software.

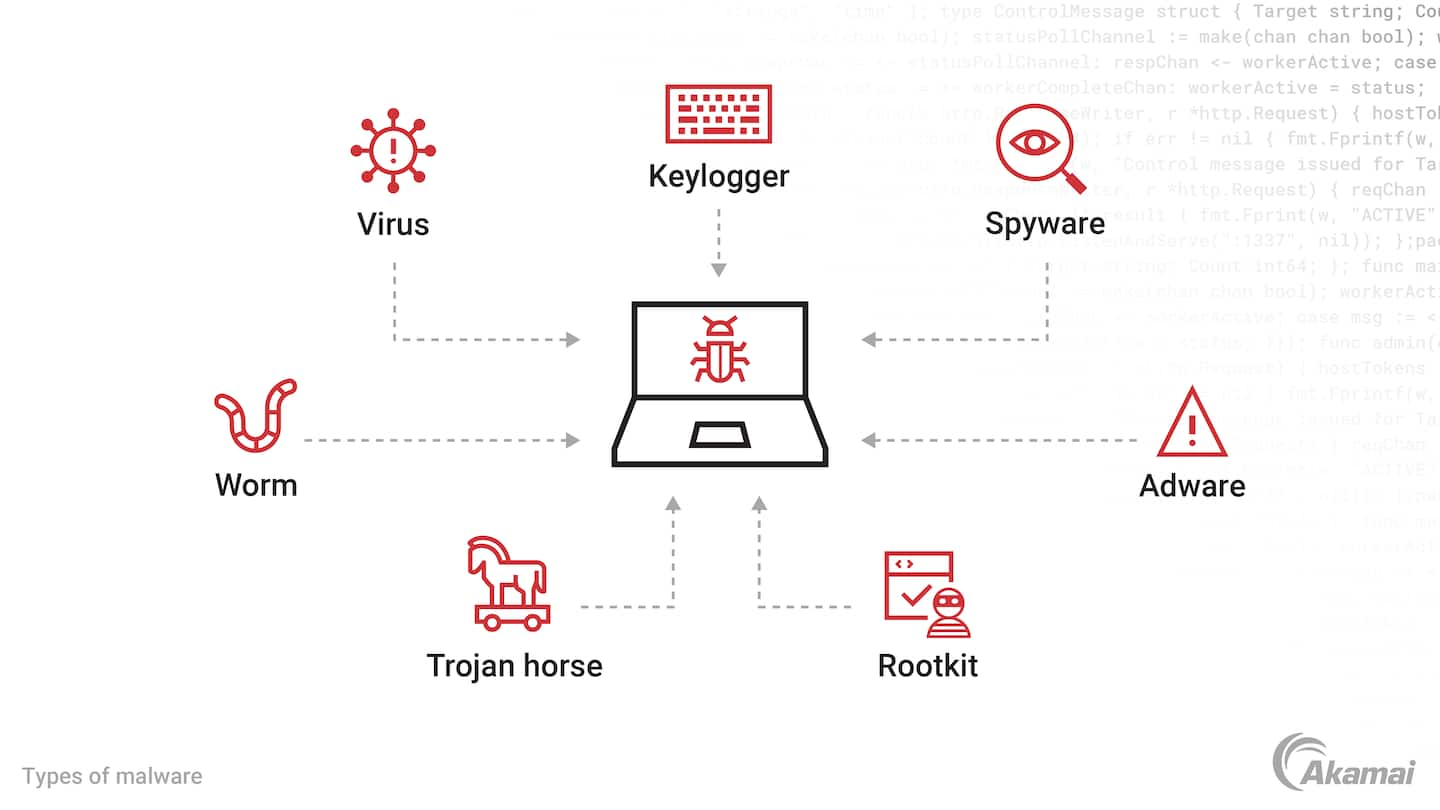


Figure : Malware

* **Virus**: A kind of malware that may replicate itself and spread to other system files or programmes. Viruses are often started when a user accesses or runs a file or programme that has a virus in it.
* **Worm**: A kind of malware that may duplicate itself indefinitely and spread over a network without the involvement of a user. Worms may swiftly propagate over a network, overloading it or infecting neighbouring systems, among other issues.
* **Trojan**: A sort of malware that users are tricked into downloading and running by being disguised as beneficial or innocent software. Trojans are often used to get into users' computers and steal their data, including bank account details and personal information.
* **Ransomware**: is a kind of malware that encrypts user data and demands payment in order to be unlocked. Important files, systems, or an organization's whole network are often targeted by ransomware, which may seriously harm data integrity.
* **Spyware**: is a sort of malware that enables hackers to secretly gather data from victims' computers or internet activity. Without the user's knowledge, spyware may record their online habits, passwords, bank account information, and other actions.

1. Cyber attack

Cyber Attack is an attack carried out by cybercriminals (high-tech criminals). They use one or more computers against other networks or machines. An attack can disable computers, stealing data. Or even use that machine as a starting point for other attacks. Cybercriminal uses a variety of methods to deploy Cyber Attack. Among them are malware, Command injection, phishing, ransomware, DDoS... and some other methods.



Figure : cyber attack

* **Denial of Service (DoS) attack**: The sending of a large number of requests to a computer system or network to render the system or service inactive, unresponsive, or overloaded, affecting the activities of official users.
* **Distributed** **Denial** **of Service (DDoS)**: Similar to DoS, but performed by many computers from many different locations, increasing attack potential and complexity.
* **Intrusion**: Intrusion into the system or computer network of another person in order to access data, information or control the system remotely.
* **Phishing**: A phishing technique in which an attacker impersonates the websites or emails of organizations, usually financial institutions or businesses, to trick users into providing personal information. personal, bank account, or other important information.

1. Security hole

A "security hole" is a weak spot or gap in the security system that an attacker may exploit to gain access to the system or carry out unlawful actions. A software, hardware, configuration, or design error that leaves a system vulnerable to infiltration or external assault is known as a security hole.

* **Software vulnerabilities**: These are vulnerabilities that appear in the source code or design of software, allowing attackers to exploit to break into the system. Common vulnerabilities in software include buffer overflow errors, injection errors, improper authentication errors, session management errors, and more.
* **Configuration errors**: These are errors that appear in the configuration of the system, including misconfiguration, weak default configuration, or failure to apply security measures properly. For example, don't disable unnecessary services, don't set a strong password for the admin account, or don't install the latest security patches.
* **Hardware Vulnerabilities**: These are vulnerabilities that appear in the system's hardware, including firmware, BIOS, electronics, and other hardware components. Hardware vulnerabilities can allow attackers to perform intrusion operations, remotely control, or obtain information on a system.

1. Physical penetration

In the context of network security, the phrase "physical penetration" is used to describe actions that physically access a computer system or network without the use of networking infrastructure. This is one of the attack strategies used in cyber assaults, when an attacker attempts to access and breach a system or network without using distant attack techniques and instead makes use of ways to directly access the system's physical location or exploit its physical weaknesses.

* **Impersonated employee**: An attacker posing as an employee or person with access to the physical location of the system to gain access to unauthorized documents or systems.
* **Device theft**: An attacker can get into the physical location of a system and steal devices such as computers, servers, hard drives, or other storage devices to gain access to data or perform other intrusive activities.
* **Use of physical media**: An attacker can use physical means such as fake network cables, rogue devices, or other physical tools to gain access to a system or network without having to use it. remote attack techniques.

1. Social engineering

The term "Social Engineering," which combines the terms "social" and "engineering," captures the heart of this form of attack: the strategies and tactics used to exploit human beings' social character, which cannot be replicated by computers. Non-technical Assault is another name for social engineering attack.

By actively influencing human psychology, creating connections with a purpose, and using information for its own ends (such as blackmail, property theft, threats, and the destruction of people or organisations), social engineering exploits information. Criminals often use social engineering techniques to exploit weaknesses by concealing their actual identities and motivations by presenting a credible front that throws the target off guard. Social engineering may utilise sophisticated techniques to lead to technological assaults even while it may not explicitly use technical means (to hack into systems or damage them).

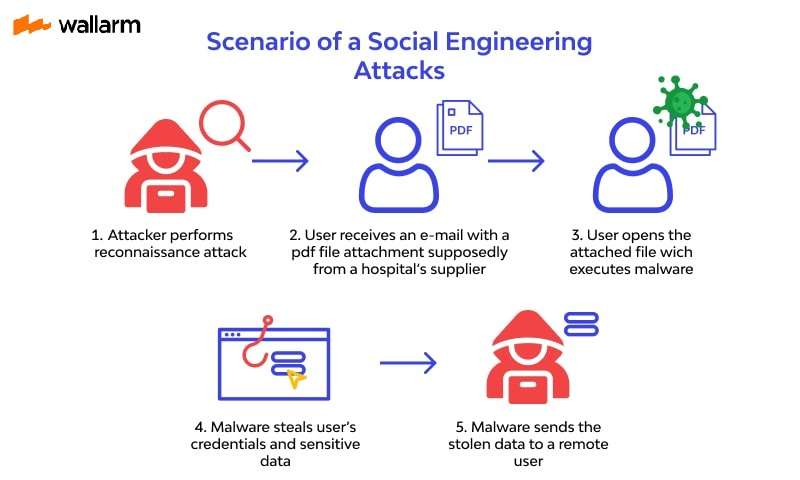


Figure : social engineer

* **Phone Phishing**: Attackers make fake calls or send fake messages to trick users into providing sensitive information such as passwords, PINs, or personal information.
* **Email Phishing**: Attackers send fake emails or fake messages to convince users to provide personal information or access malicious links.
* **Intrusion into the office**: An attacker acts as a fake employee or partner to gain access to the office or networked area to be able to obtain information or perform intrusive activities.
* **Social hacking**: Attackers use social networking sites to impersonate, scam, or deceive users into obtaining personal information or accessing online accounts.

1. Data leak

When confidential data from a system, person, or organisation is accessed without authorization, it is referred to as a data leak (also known as a data breach). access privileges. Technical failures, setup mistakes, network assaults, and unethical employee conduct are just a few causes of data breaches.

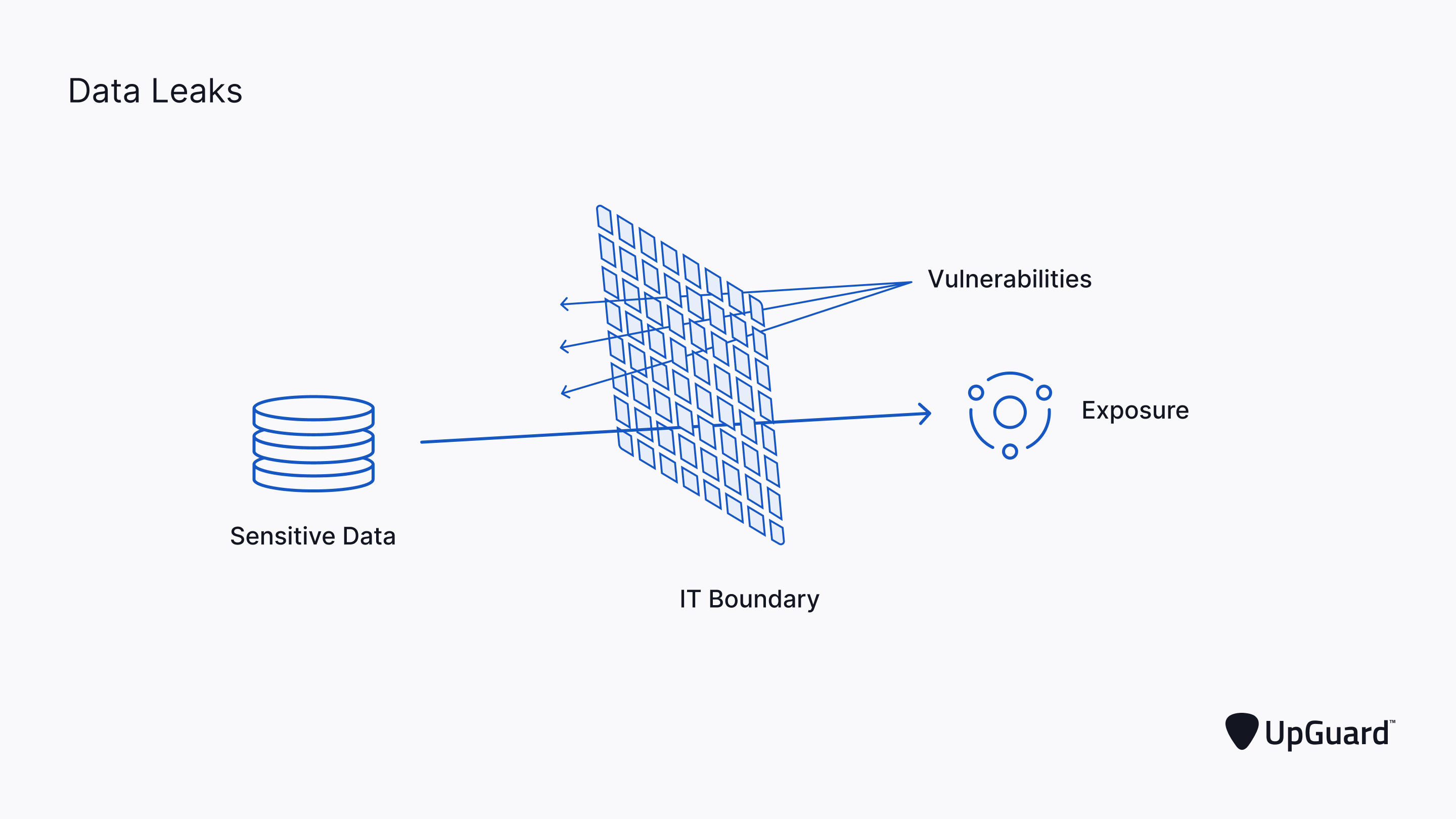


Figure : data leak

* **Disruption or intrusion into the system**: An attacker can find and exploit vulnerabilities in a system or application to infiltrate an organization's network or system, thereby accessing, copying or taking away. sensitive data.
* **Phishing, social engineering**: An attacker can use social techniques to trick an organization's employees, such as fraud, phone scams, email scams, or other types of attacks to fool employees. reveal sensitive information or improperly provide access to an attacker.
* **Malicious code, malware**: An attacker can deploy malicious code, malware to an organization's system to monitor, collect data or gain unauthorized access to sensitive information.
* **External Attacks**: An attacker can carry out attacks from outside the organization's systems, including cyberattacks (such as DDoS attacks), remote attacks, or the use of malicious tools. tools, malware to gain unauthorized access to the system.

1. **Identify threats agents to organizations**

* **External attackers**: These are outside attackers who may be persons, companies, or groups with the intent to damage, steal information, or access the organization's computer systems.
* **Insider Attackers**: They are people—either workers or internal objects from inside the company—who may have access to its computer systems and data but misuse that power. could violate the business's privacy.
* **Service providers or partners**: These are businesses, groups, or people that the organisation collaborates with, partners with, or exchanges information with. However, if they disregard security regulations or are the target of an external assault, service providers or partners might likewise endanger the company.
* **Careless users**: If employees or users inside an organisation violate security policies, use weak passwords, divulge sensitive information, or fall for social engineering, the organisation might be placed at danger.
* **Technical flaws or vulnerabilities**: Systems, applications, or infrastructure vulnerabilities or defects that might be used by threat actors to access, harm, or steal information from an organisation.
* **Natural or Disaster**: Natural catastrophes or occurrences like earthquakes, floods, fires, explosions, or other natural activity may potentially endanger the organization's security, result in data loss, or interfere with business operations. commercial activity.

1. **List type of threats that organizations will face**

* **Information technology**: Cyber attacks, viruses, malware, denial of service (DDoS) attacks, system intrusions, data theft, information disclosure and intrusion activities or harm an organization's systems, applications, and data.
* **Social**: Social engineering, email scams (phishing), phone scams (vishing), social media phishing, spoofing, and other intrusive or fraudulent activities aimed at obtain logins, passwords, or important personal information of an organization's employees or customers.
* **Physical**: Physical entry into the office, unauthorized access to infrastructure, theft or destruction of physical equipment, or activities that physically infiltrate or harm the organization.
* **Employee**: Acts of disloyal employee, employee knowingly or unintentionally disclosing information, improperly using privacy policy or procedures, committing a mistake or abusing his or her authority, or disobeying compliance with the organization's security policies and procedures.
* **Outside Activity**: Attacks from outside, such as cyber-attackers, hackers, illegal financial or business activities, political or dissident activities, and reputation-threatening activities, the organization's reputation or business.
* **Natural**: Threats related to nature, including natural disasters (earthquakes, floods, wildfires), climate change, disease outbreaks, environmental crises, or environmental problems institution, infrastructure, or natural resources.

1. **What are the recent security breaches? List and give examples with dates**
2. Yum Brands (KFC, Taco Bell, & Pizza Hut): April 2023

Yum Brands, the parent company of well-known fast food chains KFC, Taco Bell, and Pizza Hut, confirmed a cyberattack that took place in January 2023 and was made public in April of the same year. The organisation first thought that just corporate data was affected, but they have recently realised that customer personal information may possibly have been stolen. Yum Brands has responded by taking steps including shutting over 300 stores in the UK, boosting security, alerting impacted customers, and managing brand reputation. This event cost the organisation money and serves as a reminder in 2023 of how seriously huge companies may be financially impacted by data breaches.

1. ChatGPT: March 2023

The parent firm of ChatGPT, OpenAI, disclosed a data breach at the end of March. Before ChatGPT was shut down, certain users had access to another user's first and last name, email address, payment address, last four credit card numbers, and credit card expiry date. Full credit card numbers weren't revealed, however. Affected users will be notified, emails will be verified, and extra security measures will be put in place by OpenAI. Some users, especially those in the United States, may become less trusting of ChatGPT and AI technologies as a result of this data incident.

1. Chick-fil-A: March 2023

Chick-fil-A, a popular fast-food chain, confirmed a data breach in their mobile app in the first few months of 2023. Unusual login activity was detected, and the company determined that a cyber attack had taken place. The hacker used email addresses and passwords from a third-party source to access the system and obtain customer information, including membership numbers, names, emails, and addresses. Although less than 2% of customer data was breached, Chick-fil-A has taken steps to increase online security and monitoring, as well as reimburse any affected accounts. Customers are advised to secure their accounts and report any unauthorized transactions to receive reimbursement.

1. Activision: February 2023

Activision, the video game publisher known for the Call of Duty franchise, confirmed a data breach that occurred in December and was discovered on February 19th. The hacker used an SMS phishing attack on an HR employee to gain access to employee data, including emails, cell phone numbers, salaries, and work locations. Although Activision claimed that the breach was swiftly addressed and did not warrant immediate alerting of employees, a security research group found that the hacker also accessed the company's 2023 release schedule, in addition to sensitive employee information. California law requires companies to alert their employees if 500 or more individuals' data is breached. The hesitation to notify employees may result in legal and financial consequences for Activision.

1. Google Fi: February 2023

Google Fi, a mobile virtual network operator (MVNO), experienced a data breach as a result of the earlier T-Mobile data breach that occurred in 2023. Google Fi relies on T-Mobile's network infrastructure, and thus their customers' phone numbers were compromised in the T-Mobile breach. While phone numbers may seem like relatively benign information, cybercriminals can potentially use them for phishing attacks, luring users into clicking on links that could provide access to further sensitive information. Google Fi users are advised to exercise caution and be vigilant against suspicious messages in 2023.

1. **Discuss the consequences of this breach**
2. Financial Loss

Organisations might suffer rapid financial losses from data breaches. Costs may include consumer compensation, incident response, breach investigation, additional security measures, and legal costs. Non-compliance with data privacy rules like the GDPR may result in fines of up to 4% of worldwide revenue or 20 Million Euros.

Data breaches may affect the company's share price and worth. Yahoo's 2013 hack was exposed in 2016 amid Verizon's takeover. Verizon bought Yahoo for $4.48 billion, $350 million less than the initial asking price, demonstrating the financial damage a data theft can cause.

Organisations must recognise the financial ramifications of a data breach and take preventative actions to comply with data protection rules. To reduce financial risks from data breaches, this may involve investing in strong cybersecurity, developing effective incident response strategies, and prioritising data privacy and security across the organisation.

1. Reputational Damage

Data breaches may ruin a company's image. A third of retail, banking, and healthcare clients will discontinue doing business with data breached companies, according to surveys. 85% and 33.5% will also share their experience.

Data breaches may become worldwide news within hours. Negative news and customer distrust may ruin a compromised firm.

Consumers respect their personal data, and if an organisation cannot prove it has taken all required steps to secure it, they may switch to a rival that does. network security. When sensitive data is leaked, identity theft might occur. Hackers may use this data to impersonate users and make unauthorised transactions or account openings.

Reputation damage lasts and impacts the company's capacity to attract new customers, invest, and hire.

1. Operational Downtime

Cyber attacks damage company operations. Data breaches and system access inquiries must be controlled by the company.

Operations may need to stop until investigators get adequate answers. Depending on the breach severity, identifying vulnerabilities might take days or weeks. This may hurt a company's revenue and resiliency.

Gartner estimates network outage costs $5,600 per minute, or $300,000 per hour. This figure might fluctuate based on the organization's size and sector, but it can definitely have a severe influence on corporate productivity.

1. Legal Action

The legal implications of a data breach are significant, as organisations are required to demonstrate compliance with data protection regulations and individuals can take legal action for compensation. Class action lawsuits have increased, with notable cases such as the Equifax data breach resulting in substantial compensation payouts. As breaches become more frequent and severe, it is likely that more group cases will be brought to court.

1. Loss of Sensitive Data

Data breaches that leak sensitive personal data may be harmful. Personal data is anything that may identify a person. Name, passwords, IP address, and credentials. Biometric and genetic data may also be used to identify an individual.

A data breach deleting a crucial patient's medical information might seriously impact their treatment and perhaps their life. Cybercriminals value biometric data more than credit card and email addresses. Data breaches may cause irreparable harm beyond financial and reputational loss.

In today's cyber security scenario, complacency is dangerous. A unified security plan preserves data privacy, lowers risks, and defends your brand.

MetaCompliance offers the finest cybersecurity awareness training. Our tools simplify cyber security and compliance to solve cyber risks and corporate governance issues. Contact us to see how we can help your company change cyber security training.

1. **Suggest solutions to organizations**
2. Limit access to your most valuable data.

In the past, employees had unrestricted access to all files on their computers. However, companies are now realizing the importance of limiting access to critical data. This reduces the risk of accidental clicks on harmful links. In the future, it is expected that companies will partition off records so that only those who need access will have it, which is a common-sense solution that should have been implemented earlier.

1. Third-party vendors must comply.

Companies should be vigilant in knowing who their third-party vendors are and taking appropriate precautions. This includes conducting background checks on vendors who have access to their premises and limiting the types of documents vendors can view. Demand transparency from vendors and ensure they are complying with privacy laws. CEOs need to prioritize security and take proactive measures to prevent data breaches, even if it may be a hassle for the IT department. Taking these steps can help prevent costly data breaches and instigate positive change in cybersecurity practices.

1. Conduct employee security awareness training.

Employees are often the weakest link in data security, despite training efforts. One-time cybersecurity training is not enough, and regular, ongoing training is necessary. Employees may still make mistakes, such as opening suspicious emails, even after training. Studies show that repeated reinforcement of cybersecurity messages is needed to change behavior effectively.

1. Update software regularly.

Professionals recommend regularly updating all application software and operating systems, and installing patches as soon as they are available. Network vulnerabilities can arise from outdated software. Microsoft's Baseline Security Analyzer is a useful tool to regularly check and ensure that all programs are patched and up to date, providing a cost-effective way to strengthen network security and prevent attacks.

1. Develop a cyber breach response plan.

Many companies lack a proper breach response plan in the event of a data breach. In the past, companies have been slow to disclose breaches and have downplayed their severity. This lack of transparency is unacceptable to consumers who expect to know the truth about breaches and their scope. Developing a comprehensive breach preparedness plan is crucial to limit damages, restore trust, and prevent negative publicity. The plan should include evaluating what was lost, identifying responsible parties, and taking swift action. Transparency with employees and the public is essential in managing the aftermath of a data breach.

# Task 2 - Describe at least 3 organisational security procedures (P2)

1. Acceptable Use Policy (AUP)

Employees utilising IT assets to access the business network or internet must agree to an AUP. New hires are onboarded. They read and sign an AUP before getting a network ID. IT, security, legal, and HR should debate this policy.

1. Access Control Policy (ACP)

The ACP specifies employee data and information system access. NIST's Access Control and Implementation Guides are often included in policies. This policy also covers user access, network access, operating system software, and corporate password complexity. Additional features include ways for monitoring corporate system access and usage, securing unattended workstations, and removing access when an employee departs.

1. Change Management Policy

Change management policies formalise IT, software development, and security services/operations changes. A change management programme raises awareness and knowledge of planned changes throughout an organisation and ensures that all changes are implemented systematically to minimise service and customer impact.

1. Information Security Policy

An organization's information security policies are high-level policies that encompass various security controls. The primary information security policy is issued by the company to ensure that all employees using IT assets within the organization comply with the stated rules and guidelines. Employees may be asked to sign this policy to acknowledge that they have read it, similar to an Acceptable Use Policy (AUP). This policy serves to make employees aware of the rules and guidelines related to the sensitivity of corporate information and IT assets, and emphasizes their accountability in adhering to these rules.

1. Incident Response (IR) Policy

The incident response policy organises how the organisation handles incidents and restores operations. The policy CISOs hope to never employ. This policy describes how to handle an event to minimise harm to company operations, customers, and recovery time and cost.

1. Remote Access Policy

Remote access policies define allowed means of connecting to an organization's internal networks. It may incorporate BYOD asset usage addendums. Organisations with distributed networks that may reach unsecured networks like coffee shop Wi-Fi or unmanaged home networks need this strategy. To safeguard the organization's data and remote connections, the policy specifies secure remote access techniques.

1. Email/Communication Policy

An email policy formalises how workers may use the company's electronic communication medium. This policy includes email, blogs, social media, and chat. This policy instructs workers on proper and improper use of business communication technologies.

1. Disaster Recovery Policy

Disaster recovery plans are usually part of company continuity plans and include cyber security and IT departments. The incident response policy guides the CISO and teams. The Business Continuity Plan will be initiated if the occurrence is business-critical.

1. Business Continuity Plan (BCP)

The BCP will coordinate activities throughout the organisation and utilise the disaster recovery plan to restore business-critical infrastructure, apps, and data. BCPs explain each company's emergency response.

# Task 2.1 - Propose a method to assess and treat IT security risks (M1)

1. Discuss methods required to assess security threats? E.g., Monitoring tools
2. Define IT Risk Assessment

IT security risk assessments focus on identifying the threats facing your information systems, networks and data, and assessing the potential consequences you’d face should these adverse events occur. Risk assessments should be conducted on a regular basis (e.g. annually) and whenever major changes occur within your organization (e.g., acquisition, merger, re-organization, when a leader decides to implement new technology to handle a key business process, when employees suddenly move from working in an office to working remotely).

Not only is IT risk assessment important for protecting your organization and right-sizing your security investment, but it may also be mandatory. Some information security frameworks, such as ISO 27001 and CMMC, actually require risk assessments to be conducted in specific ways and documented on paper in order for your organization to be considered “compliant”.

IT risk assessments are a crucial part of any successful security program. Risk assessments allow you to see how your organization’s risks and vulnerabilities are changing over time, so decision-makers can put appropriate measures and safeguards in place to respond to risks appropriately.

1. Method require to Access security threats

* **Vulnerability scanning**: Automated tools scan systems, networks, and applications for known vulnerabilities. Vulnerability scanners find software, configuration, and system vulnerabilities that attackers might exploit. Vulnerability scanning may reveal security risks.
* **Penetration testing,** often known as ethical hacking, includes authorized people or teams exploiting system or network vulnerabilities in a controlled and supervised setting. Penetration testing replicates real-world assaults to evaluate security safeguards and uncover vulnerabilities.
* **Risk assessments**: An organization's systems, networks, and data are assessed for security threats. This strategy comprises recognizing threats, analyzing their probability and effect, and calculating their risk. Risk assessments help firms prioritize security and allocate resources.
* **Security audits**: Comprehensive reviews of an organization's security posture, policies, and processes. This technique examines an organization's security controls, procedures, and practices for vulnerabilities. Security audits check configuration settings, access restrictions, user permissions, and other security measures against best practices and industry standards.
* **Security information and event management (SIEM):** SIEM products gather, correlate, and analyze log data from systems, networks, and applications to detect security risks. Advanced analytics and machine learning algorithms discover abnormalities, trends, and signs of compromise that may signal a security concern. SIEM systems help enterprises to react quickly to security threats with real-time monitoring and alerts.
* **Security awareness training**: Employees might pose security hazards, thus security assessments must include them. Security awareness training teaches workers on typical security risks, safe computing practices, and how to detect and report security problems. Regular security awareness training may help staff become security first responders.

1. What is the current weakness or threats of an organization?

* **Cybersecurity risks**: Cybercriminals who try to obtain unauthorized access to systems, networks, or data for nefarious goals, such as stealing sensitive data, upsetting operations, or committing financial fraud, constitute a hazard to organizations.
* **Insider threats**: Threats that come from inside a company, either knowingly or unknowingly, are referred to as insider threats. Employees, subcontractors, or other insiders who abuse their access rights or unintentionally undermine security due to carelessness or human mistake are included in this category.
* **Risks to physical security**: Organizations may experience physical security risks including theft, damage, or illegal access to vital infrastructure, data centers, or physical locations.
* **Attacks using social engineering**: Social engineering attacks include tricking employees of a company into disclosing confidential information, such as passwords or other credentials, using techniques like phishing, pretexting, or impersonation.
* **Risks from other parties**: Businesses may also be at risk from third-party partners, suppliers, or vendors who may have access to their networks, systems, or data. These hazards may include holes or flaws in third-party products or services, as well as poor security procedures used by third-party organizations.
* **Regulatory and compliance risks**: Organizations may be at risk for failing to adhere to relevant laws, rules, or industry standards. Fines, penalties, legal repercussions, or reputational harm are a few examples of this.

1. What tools will you propose to treat IT security risks?
2. Automated questionnaires

Cyber risk evaluations include third-party risk questionnaires. Sending and evaluating surveys requires resources. SecurityScorecard's Atlas platform creates vendor-specific surveys that can be issued and monitored at scale to solve these issues. You can follow vendor replies in real time, simplifying questionnaire administration.

1. Security ratings

Security ratings give a data-driven, objective perspective of an organization's cybersecurity posture, making them crucial cyber risk assessment tools. Many companies now employ security ratings to monitor their internal security efforts. These are particularly helpful for attack surface control and threat detection. Security ratings systems can evaluate vendor questionnaire replies, enabling comprehensive vendor risk management.

1. Third and fourth-party vendor-provided tools

Third- and fourth-party network solution suppliers often give tools to check their products for faults. Ask third-party providers for free tools. Google's free security tools evaluate internet-connected devices' security. These and security assessment solutions help establish your risk profile.

1. Vulnerability assessment platforms

Vulnerability assessments catalog and evaluate security mechanisms to discover IT infrastructure weaknesses. The assessment report helps companies prioritize threats by assessing the risk of each network vulnerability. An impartial vulnerability assessment lets you review vendor performance, strengthening third-party business ties.

1. NIST Framework

The NIST Cybersecurity Framework, based on standards and practices, helps enterprises manage and decrease cybersecurity risk. The NIST approach improves internal-external cyber risk management communication while helping firms detect and react to cyber threats. Enterprise security teams may create cross-departmental cyber risk management plans by developing a uniform language.

Five risk management functions comprise the framework. Five functions are:

* Identify
* Protect
* Detect
* Respond
* Recover

Each function is then broken into 23 categories that give assistance based on risk management results. This information helps firms manage cyber risk and detect threats.

1. Penetration testing

A penetration test evaluates security measures while complying with PCI DSS, HIPAA, FINRA, SOC 2, and FFIEC. It reveals real-world compromising threats and provides a remedy plan. Penetration testing may reveal weaknesses like:

* High-risk vulnerabilities
* Magnitude of potential business impacts after an attack
* Feasibility of a customized set of attack vectors
* Your network’s ability to detect and respond to an attack
* Forensic analysis post security incidents

1. Employee assessments

Cyberattack protection and mitigation depend on your personnel. Without training, workers may click on phishing emails, download malware, or improperly authorize access to security data. That's why it's crucial to provide cybersecurity training and check employees' cybersecurity knowledge and incident response plans. These evaluations assure compliance and the best data breach response strategy for your company. Proper training reduces employee risk.

# Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS (P3)

1. Discuss briefly firewalls and policies, their usage and advantages in a network
2. Define firewall

Firewalls are network security systems that prevent unauthorized access to a network by examining and blocking incoming and outgoing traffic based on a set of rules. They can be hardware or software units used in enterprise and personal settings. Firewalls are essential for securing computer networks and preventing cyberattacks. Most operating systems have basic built-in firewalls, but using a third-party firewall application can provide better protection.

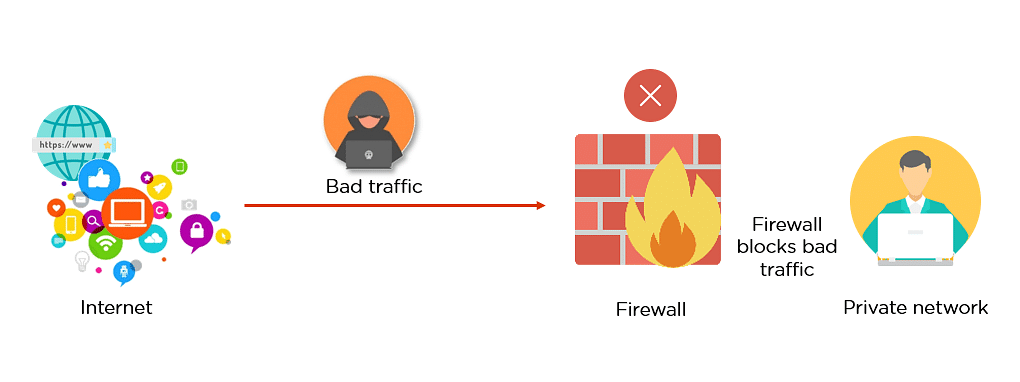


Figure : FireWalls

1. Why are FireWalls important

Modern security methods are employed in a variety of applications, and they are included into the design of firewalls. under particular, under the client-server paradigm, which is the core architecture of contemporary computing, networks in the early days of the internet needed to be constructed using novel security mechanisms. Firewalls have begun to do that, constructing the security for networks of different complexity. It is well knowledge that firewalls examine traffic and reduce dangers to the hardware.

1. Firewalls policy

Firewall policies are a set of rules that define what types of network traffic are allowed or denied based on specific criteria, such as IP addresses, port numbers, protocols, or applications. These policies are configured on the firewall to determine how traffic is filtered and controlled.

1. Advantages of Using Firewalls

* In order to handle security, firewalls are crucial in businesses. Here are a few significant benefits of employing firewalls.
* It offers improved privacy protection and security against unsecured services. It stops unauthorised individuals from connecting to an internet-connected private network.
* Firewalls provide quicker reaction times and have greater traffic load capacity.
* With the aid of a firewall, you can manage and update the security protocols with ease from a single authorised device.
* It defends your network against phishing attempts

1. How do firewalls work

Firewalls safeguard computer networks against unauthorised access. They monitor private network traffic and decide whether to allow or reject data packets depending on criteria.

The firewall analyses network traffic based on IP addresses, ports, protocols, and content. This study compares firewall security rules. The private network allows traffic that meets the requirements. Traffic that fits any of the banned rules is prevented from accessing the network.

Firewalls block questionable or harmful communications to prevent cyberattacks. They can also detect and stop DDoS, incursion, and malware threats.

1. How does a firewall provide security to a network?

**Access Control:** Firewalls examine incoming and outgoing traffic based on predefined rules that specify which traffic is allowed and which is denied. These rules can be configured to allow or block traffic based on various aspects such as source and destination IP addresses, ports, protocols, and content. By controlling access to the network, firewalls prevent unauthorized access and help protect against cyberattacks.

**Traffic Filtering**: Firewalls filter network traffic, allowing only authorized and legitimate traffic to pass through. They can block traffic from suspicious sources or with malicious intent, such as known malware, viruses, or other types of attacks. Firewalls can also be configured to detect and block specific types of attacks, such as DDoS attacks or intrusion attempts, by analyzing the traffic patterns and behaviors.

**Logging and Monitoring**: Firewalls can log and monitor network traffic, providing valuable insights into potential security threats. They can generate logs of allowed and blocked traffic, which can be reviewed for suspicious activity or anomalies. This helps in identifying and responding to security incidents in a timely manner, allowing for proactive security measures.

**Network Segmentation**: Firewalls can be used to segment the network into different security zones, allowing for better control and isolation of traffic between different parts of the network. This helps in limiting the potential impact of security breaches, as it restricts the lateral movement of attackers within the network.

**Application Control**: Some firewalls also provide application-level filtering, allowing administrators to control and restrict access to specific applications or services based on their policies. This helps in preventing unauthorized access to sensitive applications or services, reducing the attack surface of the network.

**VPN and Remote Access Security**: Firewalls can also provide security for remote access connections, such as Virtual Private Network (VPN) connections, by authenticating and encrypting the traffic between remote users and the internal network. This helps in securing remote access to the network and protecting against unauthorized access.

1. Show with diagrams the example of how firewall Works

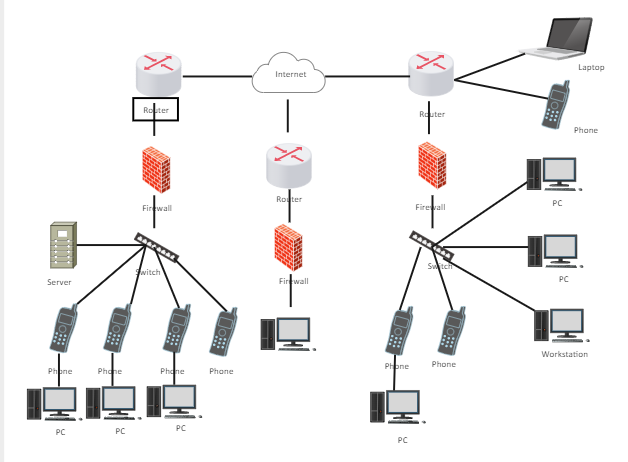


Figure : diagram of firewalls

* How it work:
  + The PC sends data packets to the switch, requesting data transmission to the Internet.
  + The switch receives the packet from the PC and based on the MAC address (Media Access Control) of the PC to determine the destination of the packet is the Firewall.
  + The packet is forwarded from the switch to the Firewall.
  + The firewall receives the packet from the switch and checks the previously configured security rules. If the packet is allowed according to those rules, it is forwarded to the router. Otherwise, it will be rejected and not forwarded.
  + The packet is forwarded from the Firewall to the router.
  + The router receives the packet from the Firewall and checks the routing table to determine the best route to send the packet to the Internet.
  + The packet is forwarded from the router to the Internet through the specified path.
  + The packet travels through the Internet and reaches its final destination.
  + The response packets from the final destination will go back and forth through the devices on the network before reaching the PC.

1. Define IDS, its usage, and show it with diagrams examples
2. Define IDS

IDS (Intrusion Detection System) is a network activity monitoring system to detect suspicious or intrusive activities. Its main function is to detect and report on unwanted or unusual activities on the network. Some IDS systems are also capable of performing actions such as blocking network traffic from suspicious IP addresses. IDS is distinct from intrusion prevention system (IPS), although both monitor and detect malicious activities, IPS mainly focuses on preventing threats after detection, while IDS is mainly focused on detecting and recording threats.

1. How do it work

Intrusion detection systems (IDS) are used to detect unusual activities to stop hackers before causing damage to the network. IDS can be deployed as a network-based system or based on the target computer. The target computer-based IDS system is installed on the client computer, while the network-based IDS system is located on the network.

The IDS system works by looking for signatures of known attacks or anomalies from normal operation. These anomalies are pushed to the protocol and application layer for inspection. IDS can effectively detect events such as Christmas tree scans or Domain Name System (DNS) scams.

IDS can be deployed as a software application that runs on customer hardware or as a network security appliance. Cloud-based IDS systems are also available to protect data and systems in cloud environments.

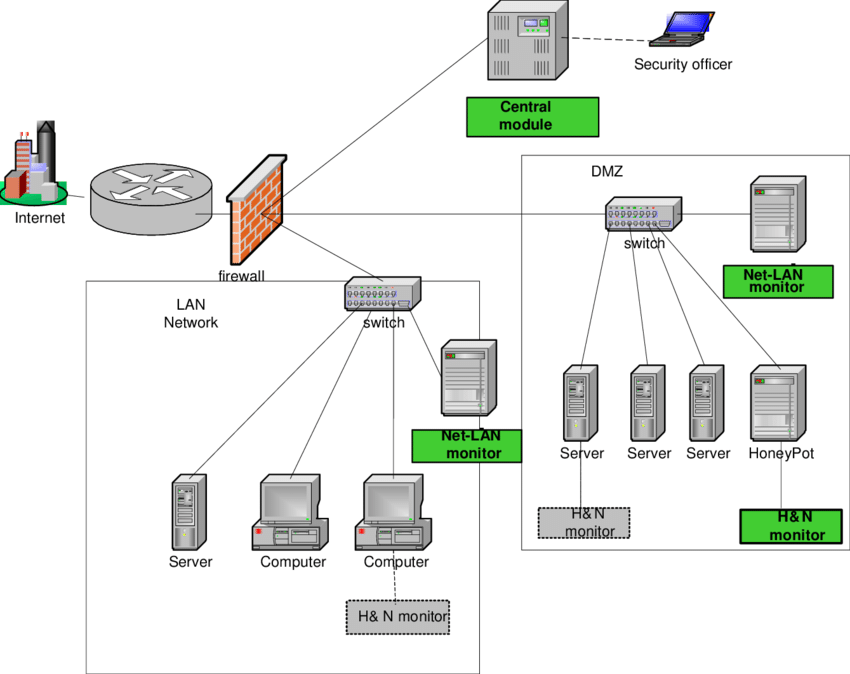


Figure : IDS diagram

1. Write down the potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network

**Unauthorised Access**: If the firewall and IDS are configured incorrectly, hostile attackers may obtain access to the network and endanger important systems or data. Data breaches, unauthorised use of network resources, and potential financial or reputational harm may result from this.

**False positive/false negative**: A firewall and IDS configured incorrectly may provide a false positive or false negative. When legitimate traffic is intercepted, a false positive results, disrupting the network's regular functioning. False negatives happen when harmful traffic is overlooked, enabling prospective threats to get by and perhaps harm the network.

**Inadequate defence**: Misconfigured firewalls and IDS might expose sensitive system or network parts to attack. Due to vulnerabilities created by this, attackers may be able to get around network security measures and access vital assets without authorization.

**Lack of visibility**: into network traffic due to improper IDS settings might make it challenging to identify and adequately react to possible attacks. As a result, security issues may be handled slowly or ineffectively, giving attackers the opportunity to do damage.

# Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4)

1. Define and discuss with the aid of diagram DMZ.
2. Define DMZ

An offshore military air zone (DMZ) protects an organization's internal network against untrusted traffic. The DMZ's ultimate purpose is to enable an organisation to access untrusted networks like the internet while protecting its private network or LAN. DMZ servers host DNS, FTP, email, proxy, VoIP, and web servers.

These servers and resources are segregated and given restricted LAN access to allow internet access without LAN connection. Thus, the DMZ prevents hackers from immediately accessing an organization's data and servers through the internet. The organisation can secure its LAN, protect personnel, and enable secure communication and file sharing.

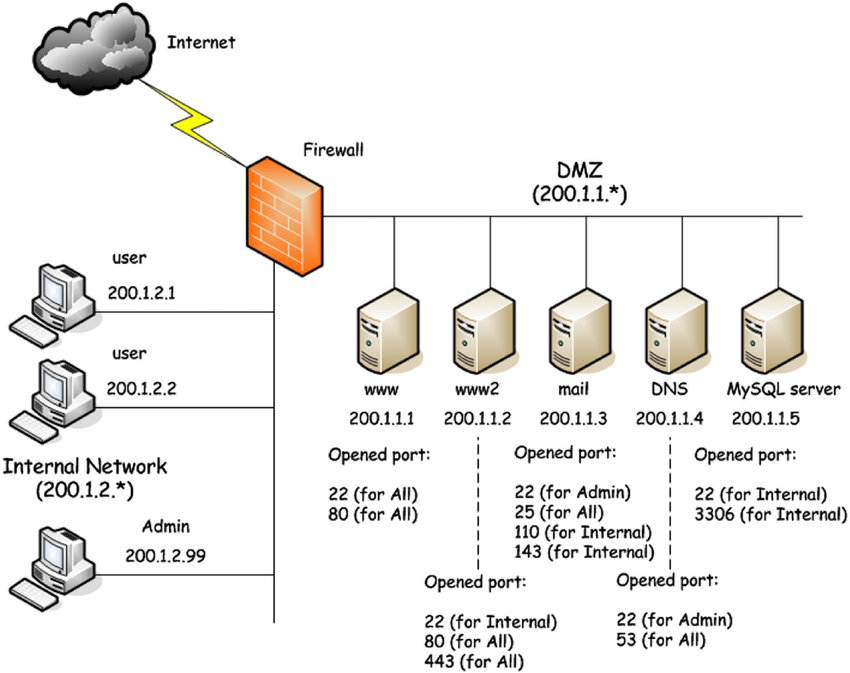


Figure : DMZ diagram

1. How Does a DMZ Network Work?

* Businesses with public websites need to place their web servers on the internet, which means putting the organization's internal network at high risk.
* To prevent this, one option is to hire a hosting company to put the server publicly on a firewall, but this can affect performance.
* Instead, public servers can be located in a separate and isolated network called a DMZ.
* The DMZ provides a buffer between the internet and the organization's private network, protected by firewalls or other security tools.
* The DMZ helps prevent attackers from directly accessing an organization's internal network after breaking through an external firewall.
* If an attacker is able to break into the DMZ, they must also bypass the internal firewall before accessing sensitive organization data.
* Another option is to install a proxy server in the DMZ to help monitor and control user activity, and comply with regulations related to information security.

1. Benefits of Using a DMZ

* The DMZ provides an enhanced layer of security for an organization's internal network by restricting access to sensitive data and servers.
* The DMZ allows website visitors to access specific services while simultaneously creating a buffer zone between them and the organization's private network.
* The DMZ provides additional security benefits such as access control, preventing attackers' targeting activities, preventing IP address spoofing, and providing network segmentation.
* Installing a proxy server in the DMZ can also help monitor and record user activity, and simplify the internal data flow, enhancing the security of the system.

1. Define and discuss with the aid of diagram static IP. Focus on its usage and security function as advantage
2. Define static IP

In contrast to a dynamic IP address, which is issued by a DHCP (Dynamic Host Configuration Protocol) server automatically, a static IP address is a fixed IP address that is explicitly allocated to a device on a network and stays constant throughout time. You may host servers, operate network services, enable remote access, and do other network-related operations with a static IP address.

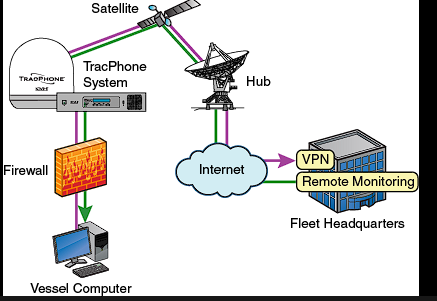


Figure : static IP diagram

1. How Does a static IP Work?

* **Hosting servers**: For hosting web servers, email servers, FTP servers, and other kinds of servers that need a constant IP address for customers to connect to, static IP addresses are crucial.
* **Static IP addresses** are used for remote access to systems or networks, such as for virtual private network (VPN) connections, remote desktop connections, and network device management.
* **Network services:** Devices that provide network services, such as DNS (Domain Name System) servers, DHCP servers, and routers, often utilise static IP addresses.
* **Security equipment**: To enable remote administration and monitoring, static IP addresses may be used for security equipment including firewalls, intrusion detection/prevention systems, and surveillance cameras.

1. Benefits of Using a static IP

* Static IP addresses may be used to set access control rules and restrict access to certain services or devices to only specified IP addresses or ranges. This aids in protecting important materials and limiting access by unauthorised parties.
* Firewall rules: To accept or prohibit traffic based on IP addresses, firewall rules may employ static IP addresses. This gives administrators more granular control and a higher degree of network traffic management.
* Logging and auditing: Because a device's IP address doesn't change over time, static IP addresses make it simpler to monitor and record network activities. This may be helpful for keeping an eye on the network and seeing any strange or malicious activities.
* For secure remote access to devices or networks, including remote desktop connections or VPN connections, static IP addresses are often utilised. This lowers the possibility of unauthorised access by enabling secure and restricted remote access.
* A method used by attackers to spoof network packets' originating IP addresses in order to obtain unauthorised access or get around security measures, IP spoofing must be prevented. By permitting only authorised IP addresses to access the network, the usage of static IP addresses may aid in the prevention of IP spoofing.

1. Define and discuss with the aid of diagram NAT. Focus on its usage and security function as advantage
2. Define NAT

Network Address Translation (NAT) is a computer networking technology that converts IP addresses from one format to another. In order to facilitate communication between private IP addresses and public IP addresses used on the Internet, NAT is often employed in private networks, such as local area networks (LANs). As will be covered below, NAT may offer a number of benefits in terms of use and security features.

1. How Does a NAT Work?

* **IP address conservation**: NAT enables a private network's devices to share a single public IP address among themselves. Since private IP addresses may be reused inside the private network, this helps save the scarce public IP address space.
* **Private network devices** may now connect to the Internet using a single public IP address thanks to NAT technology. Devices in the private network may connect to the Internet because private IP addresses are converted to public IP addresses when talking with the Internet.
* **IP address assignment**: Devices within a private network may be given private IP addresses through NAT that are not routable over the Internet. As a result, IP address management inside the private network is made simple and effective.

1. Benefits of Using a NAT

* **Internal IP addresses are hidden**: NAT blocks public Internet access to the internal IP addresses of devices connected to a private network. Devices' private IP addresses are converted to the public IP address used by the NAT device when they connect with the Internet. This adds an extra degree of protection by restricting direct Internet access to internal IP addresses, which helps to conceal the internal network architecture and IP addressing system.
* **Firewall functionality**: NAT devices often come with a built-in firewall that may provide security capabilities including port forwarding, port blocking, and packet filtering. These firewall characteristics may aid in guarding against malicious traffic and unauthorised access to the private network.
* **Access control:** NAT may be used to construct access control rules that are based on IP addresses, ports, or protocols, allowing for the acceptance or rejection of just certain traffic. By limiting incoming and outgoing traffic and obstructing unauthorised access, this aids in protecting the private network.
* **Denial of service (DoS)** assaults are one sort of network intrusion that may be detected and prevented by NAT devices by scanning and filtering incoming traffic. This lowers the possibility of network breaches and shields the private network from prospective threats.

Network Address Translation (NAT) - GeeksforGeeks

Figure : NAT diagram

# Task 4.1 - Discuss three benefits to implement network monitoring systems with supporting reasons (M2)

1. List some of the networking monitoring devices and discuss each of them.
2. SolarWinds Network Performance Monitor

It is a popular, all-encompassing network monitoring tool that uses SNMP to keep an eye on the devices. Network devices that are linked to the network are automatically detected. On a network topology map, users may see all identified devices, services, and applications and see how the network infrastructure is connected to one another. It provides the NetPath function, which tracks packet transfers hop-by-hop and is useful for more effectively identifying the cause of network problems. It offers a personalized alert system that enables users to define alert trigger situations. Network problems are reported by issue tickets, emails, SMS, Slack channels, and other means.

1. Datadog Network Monitoring Tool

It is a well-known SaaS network monitoring solution for cloud infrastructure that can monitor any networks and topologies. As it is cloud-based, server maintenance is not required. Statistics from network monitoring may also be stored there. It can keep an eye on WANs, single-site LANs, cloud resources, and other things. For real-time statistics, it use SNMP. It offers a variety of tools for network troubleshooting, including Ping, Proxy Ping, Traceroute, SNMP Ping, WMI Query Tool, and CLI Query Tool.

1. ManageEngine OpManager

It is a network monitoring system that continuously assesses the functionality of virtual computers, routers, servers, and switches. More than 200 widgets are available on its customizable dashboards, which provide a unique monitoring experience.

You can check the reliability of devices on your network using SNMP. It offers a network mapping feature that automatically locates and maps new devices for better visibility. The user may schedule network discovery to detect new devices once they have been added to the network.

You can react rapidly to changes in results thanks to the alert system. False positives are eliminated via ManageEngine OpManager's comparison of network events and the consumer's receipt of only relevant alerts.

1. Nagios Core

With a web interface for network monitoring, it is an open-source network monitoring application. The color-coding of the GUI makes it simple to identify aspects that are unavailable or damaged. Through the alerts system, which delivers email and SMS notifications, it keeps track of performance events. Users may go through the Alerts History area to discover what alerts were produced and when. Additionally, the color-coded alert list makes it simpler to prioritize critical alerts. Users may interface with other network services through APIs.

1. Nmap

One of the most popular network monitoring tools, Nmap provides both network discovery and security audits. Various networking-based tasks including network inventory, service maintenance updates, etc., may be performed by the user. It provides a wide range of cutting-edge methods for mapping networks that use routers, IP filters, firewalls, etc.

1. Why do you need to monitor networks?

* **Troubleshooting and Problem Detection**: Real-time network monitoring lets IT staff find and fix problems. Network administrators can discover and remedy network performance problems by monitoring bandwidth use, latency, and packet loss. This reduces downtime, optimizes resources, and ensures network stability.
* **Performance Optimization**: Network monitoring helps IT teams find areas for improvement. Administrators may manage network resources, alleviate bottlenecks, and efficiently employ bandwidth by monitoring network performance data. This improves network performance and user experience.
* **Security Monitoring**: Network monitoring detects and mitigates security threats and vulnerabilities. Administrators can detect or minimize security issues like unauthorized access attempts, malware infections, and data breaches by monitoring network traffic.
* **Capacity Planning**: IT teams may plan network capacity via network monitoring. Administrators may spot capacity concerns and plan network improvements or expansions to meet rising network needs by monitoring network use and performance patterns.
* **Compliance and Reporting**: Network monitoring aids compliance and audit reporting. PCI DSS, HIPAA, and GDPR demand network monitoring for security and performance. Network monitoring technologies give data and reporting for compliance.
* **Proactive Maintenance**: Network monitoring lets IT teams see and fix possible network problems before they affect performance or availability. Administrators may minimize network downtime and optimize performance by setting up alerts and notifications based on predetermined thresholds or situations.

1. What are the benefits of monitoring a network?
2. Stay ahead of outages

Why do IT disruptions occur? Environmental variables, setup problems, and human mistake are all possible causes. One of the most fundamental and straightforward methods to initially stop these disruptions from occurring is to implement network monitoring.

You have the visibility you need to keep ahead of any problems thanks to network monitoring. Network monitoring software assists you in locating failures that can result in bottlenecks by displaying real-time network performance statistics in an intuitive interface.

1. Fix issues faster

When things are bad, time is money. For time-pressed network workers, network monitoring makes problem-solving simpler and quicker.

Network monitoring software enables you to solve problems once and for all, whether you're dealing with a setup mistake or an unusual traffic fluctuation. Status windows provide performance measurements over time, while live network maps help you locate the source of issues.

Network automation technologies also enable you to advance. Through network monitoring, you may not only spot issues but also automatically resolve them without involving a human.

1. Gain immediate ROI

IT teams often lack the optimum time, manpower, or funding required to execute their projects because of their enormous workloads and projects' rising complexity. A good network monitoring tool may provide a quick return on investment. The team has more time in their day to focus on more important tasks because they no longer need to manually investigate network performance. Troubleshooting takes less time when you can identify the problem's root cause. Additionally, preventing IT breakdowns in advance lowers the expenses of outages for your company.

1. Manage growing, changing networks

The scale of today's IT environments is expanding due to technological advancement and the increase in linked devices. According to a Statista analysis, the estimated number of IoT-connected devices will expand significantly from the 13.8 billion predicted for 2021 to 30.9 billion by 2025. All of this equipment, whether it be internet-enabled sensors, wireless gadgets, or cloud technologies, has to be regularly checked for significant changes and shady activities.

Network complexity is also increasing. Things are changing even more quickly than normal as hybrid office arrangements and remote work become the norm. In order to manage all of your IP assets and guarantee seamless performance—even in the face of change—you need adaptable, trustworthy solutions, whether you're dealing with cloud migrations, IPv6 transitions, or assuring remote access.

1. Identify security threats

Network monitoring may assist safeguard your vital company data if you don't have the funds for intrusion detection software but still want a tier 1 solution to help prevent data breaches.

That first degree of protection may be provided by a network monitoring tool. The main advantage is a picture of what "normal" performance for your business looks like, which makes it simple to identify anything out of the ordinary, such as an increase in traffic volume or a strange device connected to your network. You may take a preventative approach to network security by digging deeper to determine when and on what device an incident happened.

1. Justify equipment upgrades

You may use network monitoring tools to get historical perspective on equipment performance over time to support network improvements. Trends research enables you to decide if you should invest in new technology or scale up your existing technology to match your company's demands.

# \*REFERENCES:

Hell, M. (2022) What is a security threat?, *Debricked*, [online] Available at: https://debricked.com/blog/what-is-security-threat/#:~:text=Defining%20a%20security%20threat&text=A%20potential%20for%20violation%20of,event%20that%20could%20cause%20harm.&text=An%20event%20or%20condition%20that,or%20impact%20from%20such%20loss. (Accessed April 23, 2023).

Anon (n.d.) Malware LÀ GÌ?, *Bitdefender*, [online] Available at: https://www.bitdefender.vn/post/malware/ (Accessed April 23, 2023).

Cystack.net (n.d.) Social Engineering LÀ GÌ? Những điều Bạn Cần Biết VỀ "Tấn công phi kỹ thuật": Cystack security, *CyStack*, [online] Available at: https://cystack.net/vi/blog/social-engineering (Accessed April 23, 2023).

Farrelly, J. (2023) High-profile company data breaches 2023, *Electric*, [online] Available at: https://www.electric.ai/blog/recent-big-company-data-breaches (Accessed April 23, 2023).

Hell, M. (2022) What is a security threat?, *Debricked*, [online] Available at: https://debricked.com/blog/what-is-security-threat/#:~:text=Defining%20a%20security%20threat&text=A%20potential%20for%20violation%20of,event%20that%20could%20cause%20harm.&text=An%20event%20or%20condition%20that,or%20impact%20from%20such%20loss. (Accessed April 23, 2023).

TSMNadmin (2018) 6 ways to prevent cybersecurity breaches, *Tech Support of Minnesota*, Tech Support of Minnesota, [online] Available at: https://techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches (Accessed April 23, 2023).

Privacy Ninja (2022) 9 policies for security procedures examples, *Privacy Ninja*, [online] Available at: https://www.privacy.com.sg/resources/9-rules-security-procedures-examples/ (Accessed April 23, 2023).

Deshpande, C. (2022) What is firewall: Types, how does it work & advantages: Simplilearn, *Simplilearn.com*, Simplilearn, [online] Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall#:~:text=A%20firewall%20is%20a%20security,networks%20and%20untrusted%20external%20networks. (Accessed April 23, 2023).

Lutkevich, B. (2021) What is an intrusion detection system (IDS)? definition from searchsecurity, *Security*, TechTarget, [online] Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system (Accessed April 23, 2023).

Anon (2023) 7 Essential Cybersecurity Risk Assessment Tools, *SecurityScorecard*, [online] Available at: https://securityscorecard.com/blog/essential-cybersecurity-risk-assessment-tools/ (Accessed April 23, 2023).

Anon (2023) Network Monitoring Tools: List of Networking Monitoring Tools, *EDUCBA*, [online] Available at: https://www.educba.com/network-monitoring-tools/ (Accessed April 23, 2023).

Anon (n.d.) Top 7 benefits of network monitoring, *Fortra*, [online] Available at: https://www.fortra.com/blog/top-benefits-network-monitoring (Accessed April 23, 2023).