**ASSIGNMENT 1 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 5: Security | | |
| **Submission date** | 10th/04/2022 | **Date Received 1st submission** | 31th/03/2022 |
| **Re-submission Date** | 25th/04/2022 | **Date Received 2nd submission** | 19th/04/2022 |
| **Student Name** | Nguyen Huy Hoang | **Student ID** | GCH200739 |
| **Class** | GCH0908 | **Assessor name** | Michael Omar |
| **Student declaration**  I certify that the assignment submission is entirely my work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** | C:\Users\Admin\Downloads\z3311860408145_b93399b9ab41a108a3a600bf0b1b74d1-removebg-preview.png |

**Grading grid**

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

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

Table of Contents

[Table of Contents 3](#_Toc100410498)

[List of Figures 4](#_Toc100410499)

[INTRODUCTION 5](#_Toc100410500)

[TASK 1 - IDENTIFY TYPES OF SECURITY THREATS TO ORGANIZATIONS. GIVE AN EXAMPLE OF A RECENTLY PUBLICIZED SECURITY BREACH AND DISCUSS ITS CONSEQUENCES (P1) 6](#_Toc100410501)

[1. Define threats: Software assaults, loss of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion are all examples of information security threats. 6](#_Toc100410502)

[2. Identify threats agents to organizations 6](#_Toc100410503)

[3. List the type of threats that organizations will face 8](#_Toc100410504)

[4. What are the recent security breaches? List and give examples with dates 12](#_Toc100410505)

[5. Propose a method to assess and treat IT security risks (M1) 18](#_Toc100410506)

[TASK 2 - DESCRIBE AT LEAST 3 ORGANIZATIONAL SECURITY PROCEDURES (P2) 20](#_Toc100410507)

[1. Definition 20](#_Toc100410508)

[2. Discussion on Incidence response policy 20](#_Toc100410509)

[3. Discussion on Acceptable Use Policy 23](#_Toc100410510)

[4. Discussion on Remote Access Policy 24](#_Toc100410511)

[TASK 3 - IDENTIFY THE POTENTIAL IMPACT TO ITS SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS (P3) 25](#_Toc100410512)

[A. Firewall 25](#_Toc100410513)

[1. Firewall Definition 25](#_Toc100410514)

[2. How Does A Firewall Provide Security To A Network? 28](#_Toc100410515)

[B. IDS 29](#_Toc100410516)

[1. IDS Definition 29](#_Toc100410517)

[2. IDS Usage 30](#_Toc100410518)

[3. How Does IDS Work 30](#_Toc100410519)

[C. The Potential Impact (Threat-Risk) Of A Firewall And IDS If They Are Incorrectly Configured In A Network 31](#_Toc100410520)

[TASK 4 - SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY (P4) 32](#_Toc100410521)

[A. DMZ 32](#_Toc100410522)

[1. Definition 32](#_Toc100410523)

[2. How Does DMZ Work 32](#_Toc100410524)

[3. Advantages Of DMZ 33](#_Toc100410525)

[4. Service of DMZ: 34](#_Toc100410526)

[5. The Importance Of Dmz Networks 34](#_Toc100410527)

[B. Static IP 34](#_Toc100410528)

[1. Definition 34](#_Toc100410529)

[2. How static IP addresses work 35](#_Toc100410530)

[3. Advantages of Static IP 36](#_Toc100410531)

[C. NAT 36](#_Toc100410532)

[1. Definition 36](#_Toc100410533)

[2. How Does NAT Work 37](#_Toc100410534)

[3. Types of NAT 37](#_Toc100410535)

[4. NAT security 38](#_Toc100410536)

[D. Discuss Three Benefits To Implement Network Monitoring Systems With Supporting Reasons (M2) 38](#_Toc100410537)

[CONCLUSION 39](#_Toc100410538)

[References 39](#_Toc100410539)

# List of Figures

[Figure 1:Security Threats 6](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806696)

[Figure 2: Data Breaches 12](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806697)

[Figure 3: Security Procedures 20](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806698)

[Figure 4: Firewall 25](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806699)

[Figure 5: Diagram How Firewall work 29](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806700)

[Figure 6: How IDS Work 30](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806701)

[Figure 7: DMZ 32](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806702)

[Figure 8: How DMZ Work 33](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806703)

[Figure 9: Static IP 35](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806704)

[Figure 10: NAT 36](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806705)

[Figure 11: NAT Working 37](file:///C:\Users\Admin\Dropbox\My%20PC%20(DESKTOP-MF8CEC3)\Documents\FGW\IT\Security\1_Lecture%201\1_Unit%205%20-%20Assignment%202%20frontsheet.docx#_Toc99806706)

# INTRODUCTION

Data frequently travels freely between people, organizations, and enterprises in today's data-driven and globally linked society. Data has significant worth, something cybercriminals is well aware of. Hence, the demand for security experts to secure and defend an organization from assault is increasing due to the continual rise in cybercrime. To help me get deeper knowledge in this field, this report will discuss some fundamentally basic theories of security including identifying types of security threats to organizations; organizational security procedures, Firewall policies and IDS, DMZ, static IP and NAT in a network.

# TASK 1 - IDENTIFY TYPES OF SECURITY THREATS TO ORGANIZATIONS. GIVE AN EXAMPLE OF A RECENTLY PUBLICIZED SECURITY BREACH AND DISCUSS ITS CONSEQUENCES (P1)

1. **Define threats:**  Software assaults, loss of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion are all examples of information security threats.

Anything that can exploit a vulnerability to breach security and negatively change, delete, or injure an item or object of interest is considered a threat. In this tutorial series, we'll define a threat as a potential hacker attack that allows someone to obtain unauthorized access to a computer system (garg, 2021).

Figure :Security Threats

1. **Identify threats agents to organizations**

* **Nation States**: Companies in specific industries, such as telecommunications, oil and gas, mining, power generation, national infrastructure, and so on, may become targets for other countries, either to disrupt operations today or to provide that nation with a future grip in times of crisis.
* **Non-target specific** (Ransomware, Worms, Trojans, Logic Bombs, Backdoors and Viruses perpetrated by vandals and the general public):
  + Companies have told me several times, "Oh, we're not going to be a target for hackers because..." However, because the number of random assaults that occur every day is so large (there are no reliable numbers to give here), any organization can become a victim.
  + The WannaCry ransomware assault, which infected over 200,000 machines in 150 countries, is the most well-known example of a non-target specific attack. It caused the NHS in the United Kingdom to be shut down for many days. Of course, there's the bored teenager in a loft someplace who's just looking for a weak link on the internet.
* **Employees and Contractors**
  + Morrisons was penalized because the company did not have the required technological and organizational procedures in place to prevent the ex-employee from committing the crime (note that Morrisons is currently appealing the fine).
  + There are instances when businesses want specialized assistance and hire contractors or external organizations who require access to their systems or data. These third parties are frequently the source of problems since their equipment may not have the same degrees of security as the controller's data.
* **Terrorists and Hacktivists**
  + (political parties, media, enthusiasts, activists, vandals, general public, extremists, religious followers) Similar to the threat posed by nation-states, the amount of harm posed by these agents is dependent on your activity. However, some terrorists choose to target certain sectors or nations, so you may face constant fear of a random assault.
  + The Wikileaks dumps of diplomatic cables and other documents linked to the combat in Iraq and Afghanistan in 2010 are perhaps the most prominent example of this.
* **Organised crime** (local, national, transnational, specialist)
* Criminals are after personal information for a variety of purposes, including credit card fraud, identity theft, and bank account fraud. These crimes are now being carried out on a large basis. The methods employed vary, from phishing attempts to 'Watering Hole' websites, but the ultimate effect is the same: your data and you are being harvested and exploited for evil purposes.
* According to the 2018 Fraudscape report from the Credit Industry Fraud Avoidance Society (Cifas), the number of identity fraud cases grew in 2017, with about 175,000 cases reported. Although this is only a 1% rise from 2016, it is a 125 per cent increase from a decade earlier, with 95 per cent of these cases including the impersonation of an innocent victim.
* **Natural disasters** (fire, flood, earthquake, volcano)
  + Although not a cyber assault, these occurrences can have a similar impact on your capacity to do business.
  + If you can't get into your offices, data centres, or cloud-based information, you're still dealing with a data disaster, which must be considered. The risk of an earthquake in the United Kingdom is quite low, but every year we see images of a town or metropolis submerged in water.
* **Corporates** (competitors, partners)
  + Although the fear of a rival stealing your intellectual property is evident, we are increasingly collaborating with a wide range of partners to address skills and resource gaps, as well as to supply services. Depending on their motivations, these partner firms may steal or expose your intellectual property or personal data, either unintentionally or deliberately.
  + The attack on the US retailer Target in 2013 is perhaps the best example of how partner organizations may be the source of a breach. The hackers targeted (pardon the pun!!) suppliers and discovered a weak link with Fazio Mechanical, an HVAC contractor. The hackers gained access to Target's point-of-sale systems by sending a phishing email to a Fazio employee. This allowed them access to up to 40 million credit and debit cards from customers who visited its stores throughout the holiday season of 2013. Target has spent more than $200 million on this.

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

There are three main sources of threats:

1. **Human errors and mistakes**
   * Accidental problems
   * Poorly written programs
   * Poorly designed procedures
   * Physical accidents
   * User destructing systems, applications, and data
   * User violating security policy
   * Disgruntled employee waging war on the company or causing a sabotage
   * Employee extortion or blackmail.
2. **Malicious human activity**

**APT** (Advanced Persistent Threats)

* + When it comes to hacking a business, cybercriminals who use Advanced Persistent Threats (APTs) aim to play the long game. They penetrate a computer network invisibly and in close synchronization, looking for access and departure points that will allow them to remain unnoticed.

Figure : APT

* + They snoop about, install specialized harmful programs, and acquire essential data and sensitive information once inside an organization (RSI, 2021).
  + Here are commonly five progressions that an Advanced Persistent Threat undergoes to strengthen its damage:

Infiltration of Access: Phishing, trojan horses, and malware are used by APT attackers to gain access to the system.

Grip Strengthening: The ability of an Advanced Persistent Threat to gain a foothold inside a company is its strength.

Invasion of the System: APT attackers will begin attacking the system by getting administrator access and breaking passwords left and right once they have complete freedom of movement.

Lateral Movement: hackers have made the enterprise their playground.

Deep Machinations: The APT attackers have total control of the company during this phase, deleting all evidence of their intrusion and building a solid backdoor for future use.

* + They employ cutting-edge technologies such as malware and computer intrusion tactics to compromise an organization's cybersecurity. These cybercriminals are ruthless, preferring to utilize stealthy methods to obtain access to an organization and inflict havoc (RSI, 2021).

**Distributed Denial of Service** (DDoS)

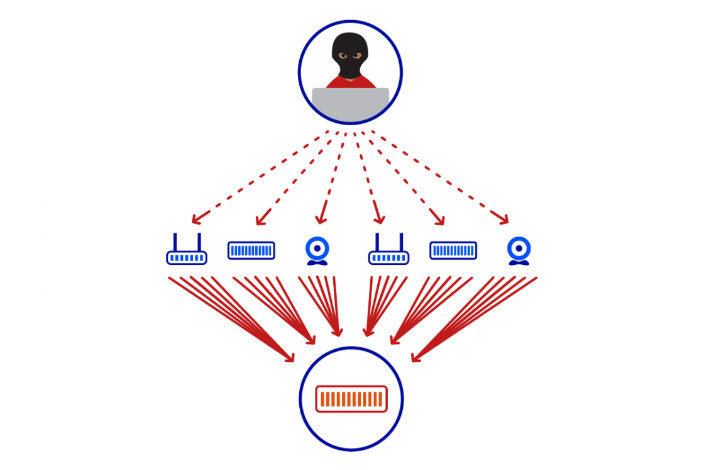
* + When fraudsters use Distributed Denial of Service, or DDOS, their primary purpose is to disrupt a website.
  + In a nutshell, they swarm a target network with fake requests to overburden the system and cause it to fail. Because the website will be offline, legitimate users or clients will be unable to access it. Because of these unneeded interruptions, DDoS can result in significant production losses.

Figure :DDOS attack

* + Because the incoming onslaught does not come from a single source, it is impossible to counter a Distributed Denial-of-Service assault. Consider a restaurant where a rowdy throng gathers at the front door to create a ruckus.

**Ransomware**

* + Once hackers have established a foothold in your network, ransomware is a type of virus from cryptovirology that hackers execute and encrypt to perfection. They take crucial business data or sensitive personal information from clients, then threaten to jeopardize the material unless the target organization pays a ransom.
  + Over time, ransomware has evolved into a popular way of extorting money from businesses.
  + The important information found within an infiltrated network is weaponized by digital attackers. To lure employees into the firm, standard ways include presenting an innocent attachment or link.

**Phishing**

* + Phishing is one of the most common ways for hackers to get access to a system. Other sophisticated security concerns, such as ransomware and Distributed Denial of Service (DDoS), can be accessed through it (DDoS).
  + Phishing is mostly based on deception. Attackers create email blasts that look to come from a reputable source. Clicking on these attachments or URLs without realizing it can infect a machine and its network.
  + Hackers posing as a senior employee or a client organization are common impersonations. They may pose as a business transaction or a bank request, which the victim employee would expect. Phishing's success is determined by how sophisticated it is and how well it can track its targets into communicating realistically.

**Worms**

* + Worms are malware that multiplies itself, especially once it has made contact with a computer network. They seek out weaknesses in a network to expand and extend their presence and effect.

**Botnet**

* + A botnet is a combination of the words "robot" and "network." It is a collective term for private computers suffering infestations from malware, making them vulnerable to remote access by cybercriminals without the organization’s knowledge.
  + The transmission of spam, the execution of DDoS barrages, and data theft all need this level of delicate control and understanding of target networks. Botnets are hackers' force multipliers for disrupting target firms' complicated systems.
  + Botnet architecture has progressed significantly in terms of evading detection. Its applications impersonate clients to connect with existing servers. Cybercriminals can then control these botnets remotely via peer-to-peer networks.

**Cryptojacking**

* Nowadays, cryptocurrency is all the trend. It requires the tactic of mining to generate more currency organically. Phishing tactics have been used by cybercriminals to infect and hijack more slave machines that will be used to mine cryptocurrencies.
* Because targets are unaware that their resources are being used to mine cryptocurrency, cryptojacking can cause slower computers.

1. **Natural Events And Disasters**

* Fires, floods, hurricanes, earthquakes, tsunamis, avalanches, and other acts of nature. This type of threat includes losses resulting from activities taken to recover from the first problem, as well as losses resulting from actions taken to recover from the initial problem.

1. **What are the recent security breaches? List and give examples with dates**
2.  **Security Breaches Definition:** A successful effort by an attacker to obtain unauthorized access to an organization's computer systems is referred to as a security breach. Theft of sensitive data, corruption or sabotage of data or IT systems, or acts meant to deface websites or harm reputation are all examples of breaches (Cassetto, 2019).

Figure : Data Breaches

1. **Recent Security Breaches, List and give examples with dates**
   * + 1. **Sina Weibo (March 2020)**

Sina Weibo is one of China's most popular social media networks, with over 600 million members. The firm started in March 2020 that an attacker had gained access to a portion of its database, affecting 538 million Weibo users and their personal information, including actual names, site usernames, gender, location, and phone numbers. The database was reportedly sold on the dark web for $250 by the attacker.

Weibo has been asked by China's Ministry of Industry and Information Technology (MIIT) to improve its data security procedures to better secure personal data and to alert users and authorities when data security breaches occur. Sina Weibo said in a statement that an attacker obtained publicly available information by utilizing a tool designed to assist users to find their friends' Weibo accounts by providing their phone numbers, but that no passwords were compromised. However, it recognized that if passwords are repeated on other accounts, the leaked data might be used to link accounts to passwords. The corporation stated that it had enhanced its security policy and had informed the proper authorities of the situation (Michael Hill and Dan Swinhoe, 2021).

* + - 1. **Nintendo (April 2020)**

Nintendo stated in April 2020 that 160,000 accounts had been compromised in a suspected credential stuffing attack. Hackers were able to get access to user accounts using previously disclosed user IDs and passwords, allowing them to purchase digital things using stored cards and read private data such as name, email address, date of birth, gender, and nationality.

The gaming behemoth has been investigating the incident and has subsequently disclosed that they believe an additional 140,000 accounts were stolen, increasing the total number of infected accounts to 300,000. All impacted customers' passwords have been changed, and users are advised not to use the same password for numerous accounts and services.

* + - 1. **Zoom (April 2020)**

When staff were settling into their new working from home environment at the beginning of April, it was revealed that virtual conference tool Zoom had suffered a humiliating security breach, exposing the login data of over 500,000 users.

Hackers appear to have gotten access to the accounts by exploiting username and password combinations stolen in prior data breaches in yet another credential stuffing assault. The information was subsequently sold for as low as 1p on dark web hacker forums.

Login credentials, email addresses, personal meeting URLs, and Host Keys were among the information stolen. Criminals were able to log in and attend meetings or use the information for other nefarious reasons, as a result of this.

* + - 1. **LinkedIn (June 2021)**

In June 2021, data linked with 700 million LinkedIn members were released on a dark website, affecting more than 90% of the company's user base. Data scraping techniques were utilized by a hacker known as "God User," who exploited the site's (and others') API before releasing the first data collection of about 500 million consumers. They then boasted that they were selling the whole 700 million-person consumer database.

* + - 1. **Data on 3.3 Million Audi Customers Exposed in Unsecured Database (June 2021)**

Volkswagen said in June 2021 that 3.3 million Audi customers' data, including present and potential purchases, had been left publicly available online. Names, email addresses, and phone numbers, as well as particular vehicle-related data, were included in the data cache, which was obtained between 2014 and 2019.

Around 90,000 people were impacted, and additional sensitive information was taken. This may contain Social Security numbers and dates of birth.

The data was exposed online at some point between August 2019 and May 2021, according to the business. The organization continues to look into the occurrence in order to establish a precise timeframe.

* + - 1. **Kaseya Ransomware Attack (July 2021)**

Kaseya, a supplier of IT solutions, had a significant attack on their unified remote monitoring and network perimeter protection product in July 2021. A supply chain ransomware assault targeted managed service providers and their downstream clients, stealing administrative control of Kaseya services.

The assault, according to ZDNet, disrupted Kaseya's SaaS servers and impacted on-premise VSA solutions used by Kaseya clients in 10 countries. Kaseya was quick to respond to the incident by notifying its customers. The Kaseya VSA detection tool was released by the corporation, allowing business users to assess their VSA services and manage endpoints for symptoms of vulnerabilities.

* + - 1. **Databases and Account Details on Thousands of Microsoft Azure Customers Exposed (August 2021)**

Due to a Cosmos DB vulnerability, Wiz security experts were able to acquire access to Microsoft Azure account credentials and client databases in August 2021. The weaknesses resulted in a loophole, allowing people to access databases that were not their own. The problem impacted a wide spectrum of businesses, including numerous Fortune 500 enterprises.

It's unclear whether anyone other than the security experts had access to the data. Anyone who did get access to the systems, on the other hand, would have had unrestricted ability to download, delete, and modify records.

* + - 1. **Crypto.com (January 2022)**

According to security firm Peckshield, CryptoCrypto.com was hacked for 4,600 ETH valued at roughly $15 million. Users began reporting strange behaviour with their accounts yesterday, and Crypto.com responded quickly to stop withdrawals, but not before the hackers snatched the Ethereum loot. Crypto.com claims that no user funds were stolen, implying that the breach occurred on the company's hot wallets, though this does not explain why users were the first to notice unusual activity in their accounts.

After a few hours, Crypto.com confirmed that certain customers had suffered "unauthorized activity" in their accounts, but added that "all monies are secure," which doesn't explain why some users' accounts had lost ETH.

* + - 1. **Microsoft Breached by Lapsus$ Hacker Group (March 2022)**

The hacker group Lapsus$ shared a screenshot to their Telegram channel on March 20, 2022, claiming that they had hacked Microsoft. The screenshot was obtained in Azure DevOps, a Microsoft collaboration tool, and it revealed that Bing, Cortana, and other Microsoft projects had been hacked.

Microsoft published a statement on March 22 acknowledging that the assaults had taken place. According to Microsoft, only a single account was hijacked, and the company's security staff was able to terminate the assault before Lapsus$ could enter any further into their business.

1. **The Consequences Of Those Breaches**

**Sina Weibo**: affecting 538 million Weibo users and their personal information, including actual names, site usernames, gender, location, and phone numbers.

**Nintendo**: 160,000 accounts had been compromised in a suspected credential stuffing attack, approximately 300,000 accounts had been affected.

**Zoom**: It was revealed that virtual conference tool Zoom had suffered a humiliating security breach, exposing the login data of over 500,000 users. The information was sold on dark web forums.

**Linkedln**: 700 million-person consumer database was sold and released for free on the dark web.

**Audi Database:** 3.3 million Audi customers' data, including present and potential purchases, had been left publicly available online. Around 90,000 people were impacted, and additional sensitive information was taken

**Kaseya:** A supply chain ransomware assault targeted managed service providers and their downstream clients, stealing administrative control of Kaseya services.

**Microsoft Azure:** The problem impacted a wide spectrum of businesses, including numerous Fortune 500 enterprises.

**Crypto.com**: 4,600 ETH valued at roughly $15 million was hacked and moved to ambiguous wallets.

**Microsoft:** Bing, Cortana, and other Microsoft projects had been hacked.

1. **Suggest solutions to organizations:**

* Quickly deploy a highly qualified and experienced cyber security team and our cutting-edge technologies to your organization, whether you've had a breach or want to build an effective response capacity. Work to develop visibility, address concerns, and implement strategies to prevent repeat accidents.
* Define, detect, defend, and prevent, For successful breach management, there are four essential criteria solutions. Define To identify and defend against threats, businesses must create an entire strategy and security lifecycle. Planning, risk assessment, policy formulation, and controls should all be addressed. A strong business and technical architecture may significantly increase the amount of resilience needed to survive a coordinated attack (Zola, 2019).
* **Define**: To identify and defend against threats, businesses must create an entire strategy and security lifecycle. Planning, risk assessment, policy formulation, and controls should all be addressed. A strong business and technical architecture may significantly increase the amount of resilience needed to survive a coordinated attack. By incorporating security into this architecture, businesses can rest certain that they are as secure as possible in the event of a compromise.
* **Detect:** An attack's harm is limited if it is detected early. An organization needs to have the capacity to monitor and detect prospective activity when it has a clear and defined plan. Knowing the sorts of assaults, attack sites, and attack vectors employed requires an understanding of baseline environment volumes, types, and performance. To build a system for acquiring situational awareness and actionable security intelligence that can help you prepare for speedy alerting of assaults, you'll need a combination of people, processes, and technology.
* **Defend:** There are no fail-safe techniques available to avoid attacks; nonetheless, it’s suggested that defining plans to secure the organization’s key services and information. The threat should be removed, the vulnerability should be closed, and the effect should be controlled as part of your defensive plan. A strong strategy is a multilayered defence that enables you to detect a breach sooner, respond faster, lessen the effect of the breach, and decrease continuing exposure. As a consequence, costs are reduced, control is increased, and risk exposure is reduced over time.
* **Deter:** Organizations can identify and defeat a variety of attack tactics and sources by collaborating and sharing security intelligence. There is support for legal action against attackers since there are effective processes in place for recording, reporting, and auditing security breaches.

1. **PROPOSE A METHOD TO ASSESS AND TREAT IT SECURITY RISKS (M1)**

To help FIS prioritize to manage different types of risks(including assessing and treating risk), one of the most effective methods that can be proposed is creating an ISRM(Information Security Risk Management) program with the use of information technology. Using the NIST framework which provides a comprehensive, flexible, repeatable and measurable process for improving how IT systems are designed, secured and monitored is a good selection for creating an ISRM.

Specifically, here are some abilities of an ISRM proving that this will help FIS manage risks:

* It guarantees that unacceptable risks are detected and appropriately managed.
* It guarantees that resources and effort aren't squandered on insignificant risks.
* It gives top management insight into the organization's risk profile and risk treatment priorities, allowing them to make more strategic decisions.

ISRM process:

* Identify – Data Risk Analysis:
* This stage involves identifying your digital assets, which might include a wide range of data.
* Financial data that must be regulated under Sarbanes-OxleyHealthcare records that must be kept secret under the Health Insurance Portability and Accountability Act, or HIPAA
* Product development and trade secrets are examples of company secrets.
* During this stage, you'll assess not just the risk of data loss or theft, but also the procedures to take to reduce or eliminate the risk connected with each type of data.
* This involves classifying data for security risk management based on its level of confidentiality, compliance laws, financial risk, and acceptable risk level (Dobran, 2019).
* Protection – Asset Management:
  + Employees get security awareness training on the correct handling of private information.
  + Implement access controls to ensure that only those who have a legitimate need for information have access.
  + Establish a company "owner" for each identified risk to ensure buy-in for planned controls and risk tolerance.
  + Create a role for an information security officer who will be responsible for assessing and mitigating data security risks.
* Implementation:
  + Examine the security dangers that have been discovered and the measures that are in place.
  + New danger detection and containment mechanisms are being developed.
  + Analyze real and attempted attacks using network security technologies.
  + Install and use technologies for alarms and unwanted access capture.
* Security Control Assessment:
  + Verify that notifications are sent to the appropriate people for timely action.
  + As new or updated apps are introduced, make sure that a continual data risk analysis is performed.
  + The efficiency of network security measures should be checked on a regular basis. Have controls been reviewed and approved if your business has audit functions?
  + Have you questioned data company owners (stakeholders) to confirm that risk management solutions are acceptable? Are they suitable for the underlying vulnerability?
* Information Security System Authorizations:
  + This level of authorization must look at not just who is notified, but also what actions are performed and how promptly they are taken. When your data is at risk, you need to act quickly to prevent data theft or loss.
* Risk Monitoring:
  + In order to provide a safe environment for your technological assets, you must implement an information risk management framework.
  + A sophisticated software-driven system of controls and alert management is an important component of a risk management strategy (Dobran, 2019).

# TASK 2 - DESCRIBE AT LEAST 3 ORGANIZATIONAL SECURITY PROCEDURES (P2)

1. **Definition**

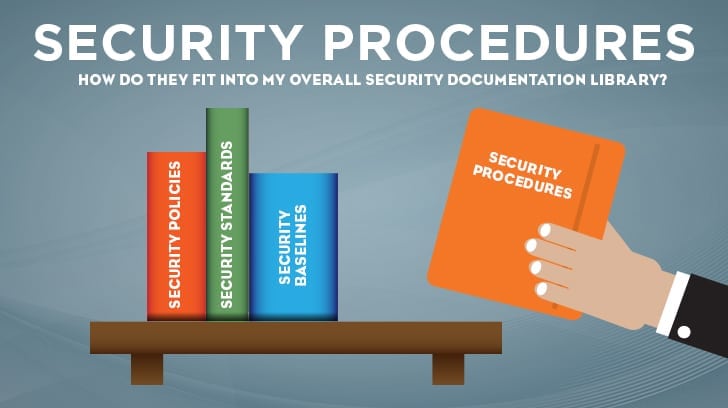
A security process is a collection of steps that must be followed to complete a certain security duty or function. Procedures are often developed as a set of actions to be performed in a consistent and repeatable manner to achieve a certain goal. Security procedures, once developed, give a set of defined steps for performing the organization's security affairs, making training, process auditing, and process improvement easier. Procedures serve as a starting point for establishing the uniformity required to reduce variance in security procedures, hence improving security control inside the business. In the security sector, reducing variance is also an excellent method to reduce waste, enhance quality, and boost performance (Patterson, 2018).

Figure : Security Procedures

1. **Discussion on Incidence response policy**

**Incident Response (IR) Procedure**: Provide the necessary procedures for incident management, reporting, and monitoring, as well as incident response training, testing, and support, to ensure that the is prepared to respond to cyber security incidents, secure State systems and data, and avoid interruption of government services.

This type of policy usually includes information about:

1. the organization's incident response team;
2. Each team member's role;
3. The people in charge of testing the policy;
4. How to put the policy into action;
5. The technological means, tools, and resources that will be used to identify and recover compromised data.

**Incidents Phases:**

* **Preparation phase:** The way users of a system and the IT professionals in charge of it are taught and prepared to respond to security issues is known as the preparation phase. This phase should involve not only the identification of tools and resources that might be used during an incident but also the implementation of preventative actions like conducting periodic risk assessments and raising user awareness.
* **Identification phase:** Identifying and detecting a security incident, as well as establishing the severity and priority level of the discovered problem. This phase entails (i) identifying incidents that use common attack vectors (e.g., attacks via removable media, the Web, and e-mail); (ii) recognizing signs of incidents; (iii) identifying detectable precursors; (iv) performing initial analysis and validation through file integrity checking; (v) running packet sniffers; (vi) filtering data, and (vii) evidence preservation.
* **Containment phase:** Instructions on how to separate systems that have been impacted by the assault to avoid further damage to other systems.
* **Eradication phase:** Determining the cause of the occurrence and removing the impacted systems.
* **Recovery phase:** Returning afflicted systems to their regular operating environment.
* **Post-incident phase:** recording the whole occurrence, performing a comprehensive investigation, determining the reason for the incident, assessing related expenses, and formulating a strategy to prevent future events.

**Elements of an incident response policy:**

* **Identification of an incident response team**
  + There are two types of incident response teams: centralized incident response teams and dispersed incident response teams. Small organizations are more likely to adopt the first type, but large organizations are more likely to use the second because it allows them to successfully coordinate people in culturally, linguistically, and legally varied situations.
  + Occurrence response teams can be made up entirely of company workers or outsourced largely or completely, depending on the sort of incident. Furthermore, the company must verify that the members are not only specified in the agreement but also appropriately taught to carry out their tasks and obligations.
* **Information about the system**: System specifics, such as network and data flow diagrams, hardware inventories, and logging data, should be included in the policy.
* **Incident handling and reporting procedures**: Another important section of the policy should define the methods for dealing with and reporting an event (suspected or occurred). Such processes should identify what occurrences will trigger response measures, in addition to guidance on how to report the incident (e.g., the timing of the incident, a list of corrupted or inaccessible data, and mitigation techniques in place). For example, the rules should address whether the organization would respond to a prospective attack or if the assault must be successful to trigger response measures.
* **“Lessons Learned”:** The "Lessons Learned" part of an incident response policy is an essential feature that is sometimes overlooked. Such a "Lessons Learned" effort, which uses a meeting and a discussion among all stakeholders concerned, might be a useful tool in enhancing security measures in the business and the incident handling process itself.
* **Reporting to outside parties**: Timeframes and procedures for reporting to third parties, such as IT workers, security analysts, data protection or law enforcement agencies, media, impacted external parties, and software providers, may be included in an incident response policy. Incident reporting may be mandated by law in some jurisdictions.

1. **Discussion on Acceptable Use Policy**

**Acceptable Use Policy(AUP):** An AUP outlines the restrictions and procedures that employees who use organizational IT assets must accept in order to have access to the business network or the internet. For new employees, it is a typical onboarding protocol. Before being assigned a network ID, they must read and sign an AUP. It is suggested that the IT, security, legal, and HR departments of a firm consider what is included in this policy (Anon., 2008).

**General Use and Ownership:**

This policy applies to any data produced or stored on the Organization's systems.

* All data including non-public personal information must be encrypted before being electronically transmitted.
* Non-public personal information and other sensitive information shall be encrypted following the Information Sensitivity Procedures in all other circumstances.
* For this policy, all information and data residing on the organization's systems and networks are considered the organization's property.
* For any reason, at any time, with or without notice, the organization may monitor or audit any information, including data files, emails, and information stored on company-issued computers or other electronic devices, for testing and monitoring compliance with these security procedures.

Without sufficient authority, all sensitive material must be kept secret and not distributed or made available to anybody. Sensitive data will be utilized purely and exclusively for the investigation. It is only to be used for the administration of receivership and not for any other purpose.

**Security and Proprietary Information:**

* The official website of the organization should not include any sensitive information.
* Information on the organization's systems, including public and private websites, should be categorised as either public or sensitive, according to the organization's information sensitivity policies.
* Passwords must be kept confidential and not shared with anyone else. The security of their passwords and accounts is the responsibility of authorized users.
* Passwords at the user level must be updated by the organization's systems usage policy, but at the very least every six months. Accounts at the user level include, but are not limited to:
  + Email
  + Web
  + Social
  + Media
  + Access to sensitive information through application accounts
* Authorized users must exercise great caution when opening e-mail attachments, which may include viruses, e-mail bombs, or Trojan horse code, either purposefully or inadvertently. All users must be taught how to recognize possible threats (Anon., 2008).

1. **Discussion on Remote Access Policy**

**Remote Access Policy:**

The remote access policy is a document that discusses and specifies permissible means of connecting to an organization's internal networks from a remote location. I've also seen addendums to this policy including rules for using BYOD assets. This policy is required for enterprises with scattered networks that might extend into unsecured network locations, such as the neighbourhood coffee shop or unmanaged home networks.

**General:**

All employees, contractors, suppliers, and other people who have access to the Organization network must agree to keep all access procedures and codes confidential and not disclose them to anyone else. Employees, contractors, suppliers, and agents having access privileges to Organization's network must guarantee that their access connections are subject to security measures that are essentially comparable to Organization.

**Requirements:**

Secure remote access must be rigorously regulated, and only those personnel approved by the Information Security Officer should have access. One-time password authentication or public/private keys with strong passwords must be used to establish authorized access.

Authorized users must not give their login credentials to anyone else, and they must not write or keep a record of their login credentials (Anon., 2008).

Unless the Information Security Officer approves differently, authorized users may only access the network using equipment provided by Organization.

Authorized users must guarantee that remote connections comply with minimal authentication standards like CHAP or DLCI.

Authorized users are responsible for ensuring that any remote host connected to the organization's internal networks is running antivirus software with the most recent virus definitions.

# TASK 3 - IDENTIFY THE POTENTIAL IMPACT TO ITS SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS (P3)

1. **Firewall**
2. **Firewall Definition**

A firewall is a network security device that monitors and filters incoming and outgoing network traffic according to security regulations set by an organization. A firewall, at its most basic level, is the barrier that separates a private internal network from the public Internet. The primary goal of a firewall is to allow non-threatening traffic in while keeping harmful traffic out.

Figure : Firewall

**Types of Firewalls:**

* **Packet filtering:** A tiny quantity of data is examined and delivered by the filter's requirements.
* **Proxy service:** At the application layer, a network security system protects while filtering communications.
* **Stateful inspection:** Dynamic packet filtering keeps track of current connections to decide which network packets to let through the Firewall.
* **Next-Generation Firewall (NGFW):** Deep packet inspection Firewall with the application-level inspection.

**Firewall Policies:**

Firewalls are available as both software and hardware appliances. Many hardware-based firewalls also provide additional services to the internal network they protect, such as operating as a DHCP server. To guard against attacks from the public Internet, several personal computer operating systems feature software-based firewalls. Many routers that transmit data across networks include firewall components, and many firewalls may perform basic routine duties as well.

**Firewall Usage:**

* **Prevents the Passage of Unwanted Content**

On the internet, there is no such thing as poor or undesirable content. Unless a robust firewall is in place, such undesirable content can readily get into the system. The majority of operating systems will have a firewall that will successfully protect users from unwanted and harmful internet information (Pedamkar, 2020).

* **Prevents Unauthorized Remote Access**

There are several unethical hackers in the world today that are always attempting to get access to weak systems. The uninformed user has no idea who has access to his machine.

A powerful firewall is required to safeguard your data, transactions, and other sensitive information; for businesses, private data and information leakage can result in significant loss and failure.

* **Prevents Indecent Content**

The vast network of the internet has exposed individuals, particularly adolescents and youngsters, to immoral information. This content's malicious nexus has been rapidly growing.

Exposure to obscene information of any kind can be damaging to young minds, leading to unusual behaviours and immoral behaviour.

* **Guarantees Security Based on Protocol and IP Address**

Hardware firewalls are effective for inspecting traffic patterns based on a certain protocol. When a connection is created, a record of activity is retained from start to finish, which helps to keep the system secure.

Network Address Translation (NAT) is a form of firewall that efficiently protects computers against attacks from outside their network. As a consequence, the IP address of these computers is only accessible within their network, keeping them independent and protected (Pedamkar, 2020).

* **Protects Seamless Operations in Enterprises**

Enterprise software and systems have grown increasingly important in today's business world. Authorized stakeholders can utilize and work on the data for effective company operations thanks to decentralized distribution mechanisms and data access throughout the whole geographical presence.

A user can log in to his system using credentials from any system on the network. Given such a large network system and large amounts of data.

* **Protects Conversations and Coordination Contents**

Organizations in the service industry must continually communicate with third-party clients. They continuously share relevant material with the customer and internal teams as part of various initiatives.

Almost all of the content generated by these coordinating operations is secret and must be well safeguarded; no organization can afford the expense of such essential information being leaked.

* **Prevents Destructive Content from Online Videos and Games**

Users may watch movies on a variety of websites, and some even enable them to download games or videos. Similarly, a slew of websites allows you to play and download games. Except for a few well-known sites, hardly all websites guarantee access security. And there's frequently a constant stream of harmful stuff in the shape of malware and viruses attempting to infiltrate the user's machine. A firewall is required in the system because it protects the user's machine against virus assaults via online games or films.

**Advantages of Firewall:**

* Hackers and remote access are prevented by a firewall.
* It safeguards information.
* Enhanced security and network monitoring capabilities
* It gives you more privacy and security.
* Assist the VOIP phone's dependability.
* It guards against trojans (Bradley, 2021).
* Allow for more advanced network capabilities to be implemented.
* An OS-based firewall can only protect single PCs, but a network-based firewall, such as a router, can protect many systems.

1. **How Does A Firewall Provide Security To A Network?**

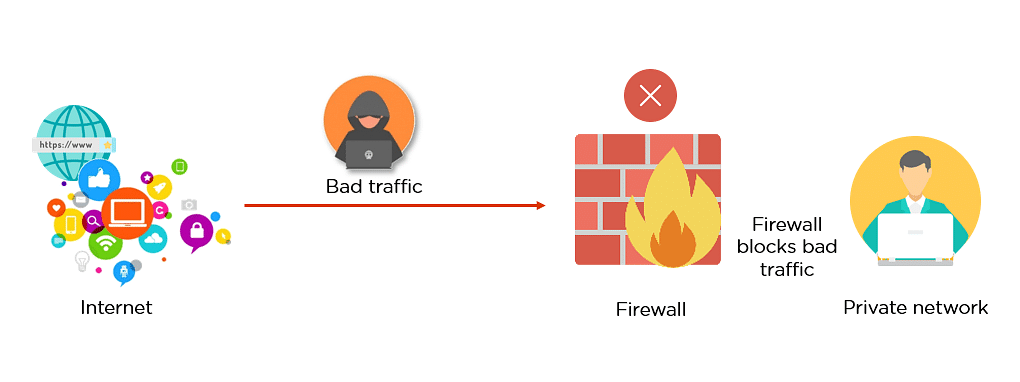
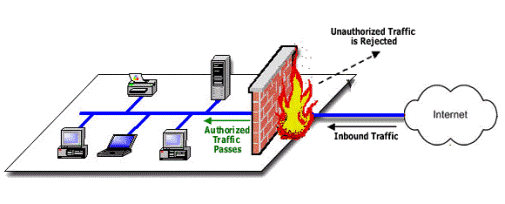
* Within a private network, firewalls filter network traffic. It determines which types of traffic should be permitted or prohibited based on a set of regulations. Consider the firewall as a gatekeeper at the computer's entrance point, allowing only trustworthy sources, or IP addresses, to gain access to the network.
* Only the incoming traffic that has been set to accept is accepted by a firewall. It detects legitimate and malicious traffic and permits or disallows particular data packets based on pre-defined security criteria.
* These criteria are based on numerous factors of the packet data, such as the source, destination, and content, among other things. To avoid cyberattacks, they restrict traffic from suspected sources.
* The graphic below, for example, depicts how a firewall permits excellent traffic to flow through to a user's private network.
* The firewall in the example below, on the other hand, prevents harmful traffic from accessing the private network, safeguarding the user's network from a cyberattack (Bradley, 2021).
* A firewall can do fast evaluations to detect malware and other suspicious activity in this manner.
* At different network levels, several types of firewalls are used to read data packets.

Figure : Diagram How Firewall work

1. **IDS**
2. **IDS Definition**

An intrusion detection **s**ystem (IDS) is a network traffic monitoring system that detects suspicious behaviour and sends out notifications when it is found (Lutkevich, 2021).

While the basic duties of an IDS are anomaly detection and reporting, certain intrusion detection systems may also take action when malicious behaviour or abnormal traffic is discovered, such as blocking traffic received from questionable IP addresses.

An intrusion detection system (IDS) differs from an intrusion prevention system (IPS), which, like an IDS, analyzes network packets for potentially harmful network activity, but focuses on preventing attacks rather than detecting and documenting them.

1. **IDS Usage**

* Other security controls intended at detecting, stopping, or recovering from assaults; monitoring the functionality of routers, firewalls, key management servers, and files that are required by other security controls;
* Allowing administrators to tweak, manage, and comprehend relevant OS audit trails and other logs that might otherwise be impossible to follow or interpret;
* Including a large attack signature database against which information from the system may be compared; offering a user-friendly interface so that non-expert staff members can help with system security management;
* When the IDS detects that data files have been changed, it generates an alarm and notifies the user that security has been broken; attackers are blocked or the server is blocked.

1. **How Does IDS Work**

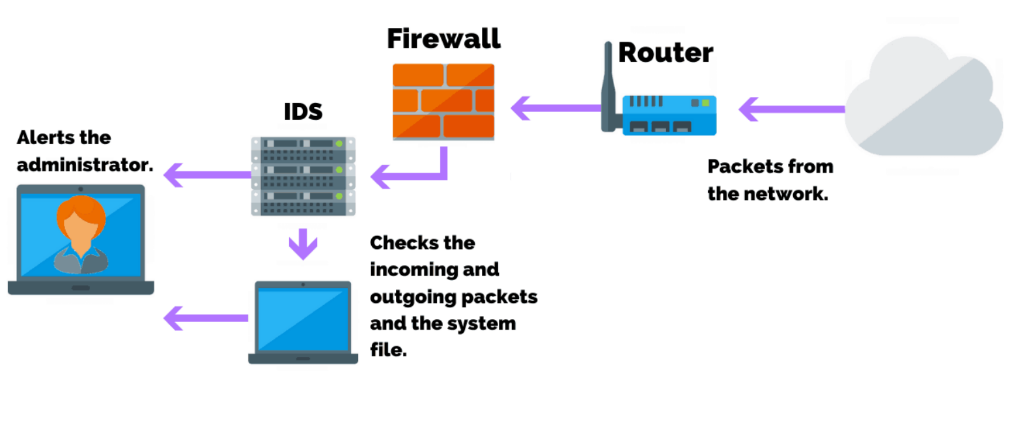
Intrusion detection systems are used to identify irregularities in the network to capture hackers before they do serious damage. Network-based IDSes and host-based IDSes are both possible. The client computer has a host-based intrusion detection system, whereas the network has a network-based intrusion detection system.

Figure : How IDS Work

Intrusion detection systems detect assaults by looking for signs of previous attacks or deviations from regular behaviour. These abnormalities are moved up the stack and investigated at the protocol and application layers. They are capable of detecting occurrences such as Christmas tree scans and DNS poisonings.

An IDS can be deployed as a client-side software program or as a network security device. To safeguard data and systems in cloud deployments, cloud-based intrusion detection solutions are now available (Lutkevich, 2021).

1. **The Potential Impact (Threat-Risk) Of A Firewall And IDS If They Are Incorrectly Configured In A Network**
   * Unencrypted HTTP connections can be abused by an outsider on the same network segment, such as an open/unencrypted wireless network, allowing anybody on the Internet to access the firewall. On the external interface, anti-spoofing restrictions are not enabled, which can permit denial of service and associated attacks. Without logging, rules exist, which may be troublesome for key systems and services.
   * Internal network segments can be connected by any protocol/service, which can lead to internal breaches and compliance violations, especially in PCI DSS cardholder data settings.
   * Unencrypted telnet connections allow anyone on the internal network to connect to the firewall. If ARP poisoning is enabled by a tool like the free password recovery application Cain & Abel, these connections can be abused by an inside user (or malware).
   * Any sort of TCP or UDP service can leave the network, allowing malware and spam to proliferate and resulting in permissible use and policy breaches.
   * There is no documentation for the rules, which might lead to security management concerns, especially when firewall administrators leave the company unexpectedly.
   * The default password(s) are used, resulting in every security risk imaginable, including responsibility concerns when network events occur.
   * Firewall OS software is ancient and no longer supported, making it vulnerable to known weaknesses such as remote code execution and denial of service attacks. It also may not look good in the eyes of third parties if a breach happens and the system's age is revealed.
   * Anyone on the Internet may access internal Microsoft SQL Server databases, which can lead to internal database access, especially if SQL Server is configured using the default credentials (sa/password) or an otherwise weak password.

# 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. **DMZ**
2. **Definition**

A DMZ Network is a perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks (Ohri, 2021).

Figure : DMZ

The purpose of a DMZ is to allow an organization to connect to untrusted networks, such as the internet while maintaining the security of its private network or LAN. External-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, are often stored in the DMZ.

1. **How Does DMZ Work**

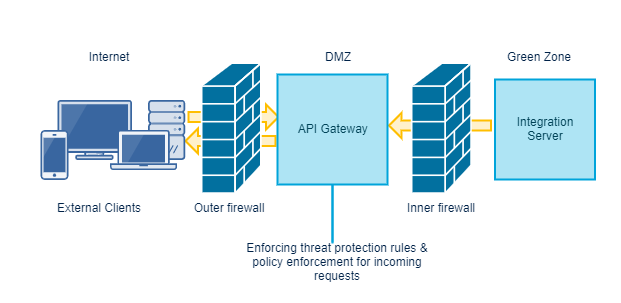
Any gadget that is connected to the internet bears the brunt of most attacks and hence bears the most danger. Companies that have public servers that must be accessible by persons outside the company are more vulnerable to assaults. DMZs serve as a barrier between an external and an internal network. When a DMZ is created between two firewalls, all incoming traffic is filtered by a firewall or security appliance before reaching the organization's server.

Figure : How DMZ Work

If a trained bad guy breaks through the company's firewall and obtains unauthorized access to those systems before they can perform any harmful activity or access the company's sensitive data, those systems will alert the host that a breach has occurred (Ohri, 2021).

1. **Advantages Of DMZ**

Enabling access control: Businesses can utilize the public internet to give consumers access to services outside of their network's perimeters. The DMZ allows access to these services while also enabling network segmentation, making it more difficult for an unauthorized user to get access to the private network. A proxy server, which centralizes internal traffic flow and simplifies monitoring and recording of that traffic, may be included in a DMZ.

Network reconnaissance is prevented by a DMZ, which acts as a barrier between the internet and a private network, preventing attackers from conducting reconnaissance in search of suitable targets. Servers in the DMZ are accessible to the public, but a firewall prevents an attacker from seeing inside the internal network, adding another layer of security.

Even if a DMZ system is compromised, the internal firewall protects the private network by separating it from the DMZ, preventing external reconnaissance.

Blocking IP spoofing: Attackers try to obtain access to systems by spoofing an IP address and impersonating a trusted device that has signed in to the network. While another service validates the validity of the IP address, a DMZ can detect and halt such spoofing efforts. The DMZ also serves as a network segmentation zone, allowing traffic to be structured and public services to be accessible outside of the private network.

1. **Service of DMZ:**
   * Web servers
   * Mail servers
   * FTP servers
   * DNS servers
   * Proxy servers
   * VoIP servers
2. **The Importance Of Dmz Networks**

* The primary benefit of employing a DMZ is that it adds an extra layer of protection to an organization's private network by restricting access to servers and critical data.
* In the DMZ, we may set up a reverse proxy server. Clients on the internet will connect to a reverse proxy server that holds no sensitive information.
* The DMZ not only isolates and keeps possible target systems away from inside networks, but it also limits and controls access to them (Ohri, 2021).
* Users within an enterprise may still exchange and access material on the internet, while unauthorized users outside of a network can still get crucial data from the network, thanks to DMZ.
* Because a DMZ manages both external and internal traffic flow to and from a private network, hackers are less likely to get direct access to the system.
* The DMZ can also be used to respond to security concerns posed by IoT devices, OT systems, and other similar systems.

1. **Static IP**
2. **Definition**

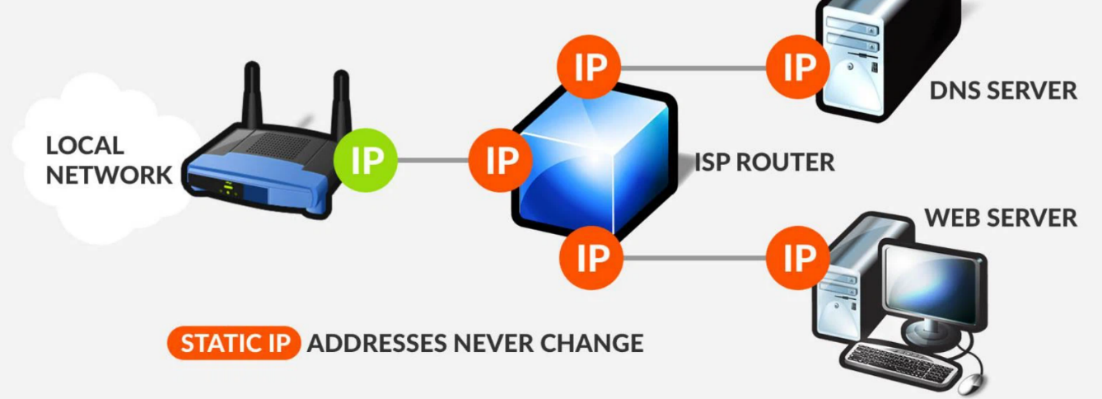
A static IP address is a 32-bit number that is issued to a computer to use as an internet address. An internet service provider will usually supply this number in the form of a dotted quad (ISP).

Figure : Static IP

A device's IP address (internet protocol address) serves as a unique identity when it connects to the internet. IP addresses are used by computers to locate and communicate with one another over the internet, just like phone numbers are used by individuals to locate and communicate with one another over the phone. An IP address can reveal details about the hosting provider as well as geographic location data (Gillis, 2020).

1. **How static IP addresses work**

Because most ISP providers do not supply static IP addresses by default, if an individual or organization wants one, they must first contact their ISP and request that their device — such as a router — be assigned a static IP address. They will need to restart their device after the device has been set up with a new and permanent IP address. The same IP address will be used by computers and other devices behind the router. Because the IP address does not change, there are no further measures required to maintain it.

However, because the quantity of static IP addresses accessible is limited, obtaining one will frequently cost money. IPv6 is a solution to this problem. IPv6 extends IP addresses from 32 bits to 128 bits (16 bytes), resulting in a large increase in the number of accessible IP addresses, making static IP addresses easier to obtain and retain. Today, IPv4 is still used by a major amount of internet traffic, but IPv6 is becoming more popular, thus both are currently in use.

Up to 340 undecillion unique IP addresses are possible using IPv6. To put it another way, it's 340 followed by 36 zeros, or 340 trillion, trillion, trillion unique IP addresses that may now be issued. This increase in the total number of IP addresses enables significant future internet expansion and alleviates concerns about a future shortage of network addresses.

1. **Advantages of Static IP**

* Businesses that use IP addresses for mail, FTP, and web servers might have a single address that never changes.
* For hosting voice over IP, VPNs, and gaming, static IP addresses are preferable.
* They can be more reliable in the event of a connectivity outage, ensuring that packet exchanges are not missed.
* They enable speedier file uploads and downloads on file servers.
* Any geolocation services will have an easier time determining where a device is with a static IP.
* For remote access to a computer, static IPs are preferable.
* A device with a static IP address does not need to make renewal requests.
* When it comes to maintaining servers, network administrators may find it easier to keep static IP addresses.
* It's also easy for administrators to keep track of internet traffic and grant access to users depending on their IP addresses.

1. **NAT**
2. **Definition**

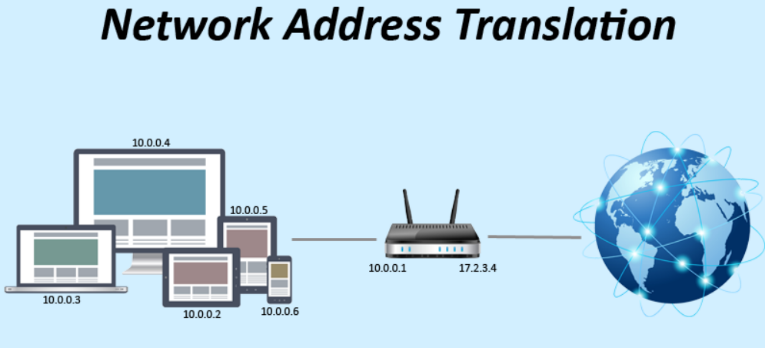
In order to give Internet connectivity to local hosts, Network Address Translation (NAT) is a procedure in which one or more local IP addresses are translated into one or more global IP addresses and vice versa. It also does port number translation, i.e. masks the host's port number with another port number in the packet that will be forwarded to the destination. The NAT table is then updated with the relevant IP address and port number entries. A router or firewall is usually used for NAT (Vaughan-Nichols, 2019).

Figure : NAT

1. **How Does NAT Work**

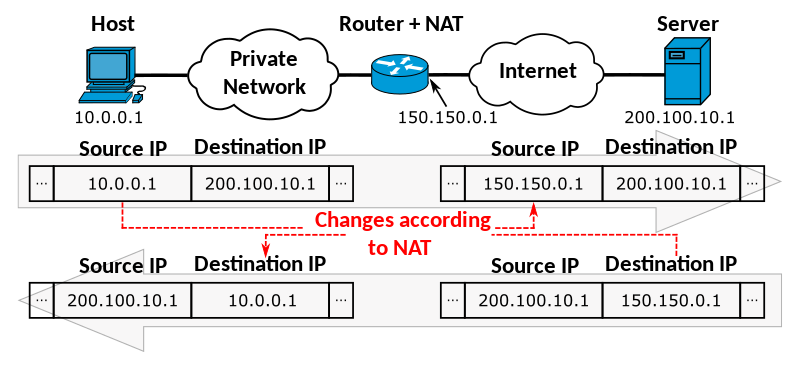
Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

Figure : NAT Working

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

1. **Types of NAT**

* **Static NAT**

This NAT chooses the same local address when it is transformed into a public one. This indicates that the router or NAT device will have a constant public IP address.

* **Dynamic NAT**

This NAT uses a pool of public IP addresses rather than using the same IP address every time. As a result, each time the router translates a local address to a public address, the router or NAT device receives a different address (Vaughan-Nichols, 2019).

* **PAT**

Port address translation is abbreviated as PAT. It's a sort of dynamic NAT, but it binds a group of local IP addresses to a single public IP address. PATs are used by organizations that want all of their employees' activities to be routed through a single IP address, usually under the oversight of a network administrator.

1. **NAT security**

NAT may also help with security and privacy. NAT prevents anything else from accessing the private device by transferring data packets from public to private addresses. The router organizes the data to ensure that it is sent to the correct location, making it more difficult for undesirable data to pass through. It isn't perfect, but it is frequently the first line of protection for your device. If a company wishes to secure its data, it will require more than simply a NAT firewall; it will need to engage a cybersecurity expert.

1. **DISCUSS THREE BENEFITS TO IMPLEMENT NETWORK MONITORING SYSTEMS WITH SUPPORTING REASONS (M2)**

Top three benefits of implementing network monitoring systems:

* + 1. **Identify security threats:**

Cybercrime prevention is a big concern for every organization. Detecting and mitigating any type of network danger before it escalates is crucial as attacks grow more complex and difficult to trace.

Addressing persistent security threats on a daily basis without network insights may be exceedingly time-consuming for an IT staff. Maintaining IT network security necessitates the following:

* Security fixes are updated on a regular basis.
* On all individual workloads, standardized security settings are maintained.

As a result, network monitoring will help an IT staff defend a company's data and systems more effectively.

* + 1. **Manage Client Network Usage with Confidence:**

This is due to the fact that many firms permit office workers and other staff to use the internet as part of their daily tasks. Unfortunately, without network monitoring of client networks, it will be difficult to identify employees who are misusing the system or utilizing confidential information for personal gain. Furthermore, if our clients rely on us for data backup and integrity, few techniques provide the type of smooth interface that network monitoring provides. While IT specialists may be able to develop various ways to monitor the network, everyone will be much more effective if network monitoring systems are implemented.

* + 1. **Benchmark standard performance:**

IT outages can result from a variety of factors.

* Errors made by humans
* Changes to the network that are incompatible
* Technology's ever-increasing complexity

More often than we'd like, organizations are only aware of network performance when it noticeably deviates from the norm, and they only respond when it starts to affect business output (Luminet, 2016).

This is because network monitoring systems offer us the insight to measure daily performance and the foresight to detect any deviations from the norm, allowing us to spot abnormalities ahead of time. Effective network monitoring allows IT workers to spot possible problems early and fix them before they become severe problems that cause system downtime.

# CONCLUSION

This paper covers the risks and remedies, as well as a variety of tools that can help individuals and organizations get better to protect their data when online. List security breaches to help users understand what has happened in the past and how to avoid danger and safeguard data if one has occurred. There are risks, but there are also benefits to consider for the consumer. As a result, the analysis shows that the benefits of such apps have been and continue to be positively evaluated, allowing consumers to select the best software for their needs.

# References

Anon., 2008. *[Organization] Information Security Procedures ,* s.l.: s.n.

Bradley, T., 2021. *What Is a Firewall and How Does a Firewall Work?.* [Online]   
Available at: https://www.lifewire.com/what-is-a-firewall-2487290

Cassetto, O., 2019. *Security Breaches: What You Need to Know.* [Online]   
Available at: https://www.exabeam.com/dlp/security-breach/

Contributor, S., 2020. *What is a Data Breach? Ultimate Guide to Cyber Security Breaches.* [Online]   
Available at: https://www.dnsstuff.com/data-breach-101

Dobran, B., 2019. *Information Security Risk Management: Build a Strong Program.* [Online]   
Available at: https://phoenixnap.com/blog/information-security-risk-management

garg, r., 2021. *Threats to Information Security.* [Online]   
Available at: https://www.geeksforgeeks.org/threats-to-information-security/

Gillis, A. S., 2020. *static IP address.* [Online]   
Available at: https://whatis.techtarget.com/definition/static-IP-address

Luminet, 2016. *Network Monitoring.* [Online]   
Available at: https://luminet.co.uk/top-5-benefits-network-monitoring/

Lutkevich, B., 2021. *intrusion detection system (IDS).* [Online]   
Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Lutkevich, B., n.d. *intrusion detection system (IDS).* [Online]   
Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Michael Hill and Dan Swinhoe, 2021. *The 15 biggest data breaches of the 21st century,* s.l.: s.n.

Ohri, A., 2021. *What Is DMZ Network.* [Online]   
Available at: https://www.jigsawacademy.com/blogs/cyber-security/what-is-dmz

Patterson, D., 2018. *The Importance of Policies and Procedures,* s.l.: s.n.

Pedamkar, P., 2020. *Firewall Uses.* [Online]   
Available at: https://www.educba.com/firewall-uses/

RSI, 2021. *TYPES OF SECURITY THREATS TO ORGANIZATIONS.* [Online]   
Available at: https://blog.rsisecurity.com/types-of-security-threats-to-organizations/

Vaughan-Nichols, S. J., 2019. *Static vs. Dynamic IP Addresses.* [Online]   
Available at: https://www.avast.com/c-static-vs-dynamic-ip-addresses

Zola, A., 2019. *A Guide to Data Breach Best Practices.* [Online]   
Available at: https://www.business2community.com/cybersecurity/how-to-protect-a-small-business-from-a-data-breach-a-guide-to-data-breach-best-practices-02244829