|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 5: Security | | |
| **Assignment title** | Security Presentation | | |
| **Academic Year** | 2020 | | |
| **Unit Tutor** | Ho Hai Van | | |
| **Issue date** |  | **Submission date** |  |
| **IV name and date** | Le Luong Minh Man | | |

|  |
| --- |
| **Submission Format** |
| The submission is in the form of two documents/files:   1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy. 2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics.   You are required to make use of the font **Calibri,** **Font size 12,** **Line spacing 1.5, Headings,** P**aragraphs**, S**ubsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.** |

|  |
| --- |
| **Unit Learning Outcomes** |
| **LO1** Assess risks to IT security. **LO2** Describe IT security solutions. |
| **Assignment Brief and Guidance** |
| You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS.  FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of your role, your manager Jonson has asked you to create an engaging presentation to help train junior staff members on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment.  In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation.  Your presentation should:   1. **Identify** the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences 2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. 3. **Propose** a method that FIS can use to prioritize the management of different types of risk 4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons. 5. Investigate network security, **identifying** issues with firewalls and **IDS** incorrect configuration and **show** through examples how different techniques can be implemented to improve network security. 6. **Investigate** a ‘trusted network’ and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS.   Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics. |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO1** Assess risks to IT security | | **LO1 & 2 D1** Investigate how a ‘trusted network’ may be part of an IT security solution. |
| **P1** Identify types of security threat to organisations.  Give an example of a recently publicized security breach and discuss its consequences.  **P2** Describe at least 3 organisational security procedures. | **M1** Propose a method to assess and treat IT security risks. |
| **LO2** Describe IT security solutions | |
| **P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.  **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. |

Table of Contents

[1 P1. Identify types of security threat to organisations. 9](#_Toc54173849)

[1.1 Define threats 9](#_Toc54173850)

[1.2 Identify threats agents to organizations [1] 9](#_Toc54173851)

[1.3 Example of a recently publicized security breach and discuss its consequences. 14](#_Toc54173852)

[1.3.1 Uber[10]: 14](#_Toc54173853)

[1.3.2 Facebook data breache [13] 14](#_Toc54173854)

[1.3.3 Marriot data breach [15] 15](#_Toc54173855)

[1.4 Consequences [16]: 16](#_Toc54173856)

[1.5 Solutions: 16](#_Toc54173857)

[2 P2 Describe at least 3 organizational security procedures. 17](#_Toc54173858)

[2.1 Security procedure definition: 17](#_Toc54173859)

[2.2 Security procedure purpose 17](#_Toc54173860)

[2.3 Some organizational security procedures 18](#_Toc54173861)

[2.3.1 Network Access procedure: 18](#_Toc54173862)

[2.3.2 Advising on personal security procedure: 19](#_Toc54173863)

[2.3.3 Conducting security patrols of company premises [19] 20](#_Toc54173864)

[3 M1 Propose a method to assess and treat IT security risks. 21](#_Toc54173865)

[3.1 Methods required to assess it security threat: Security Risks Assessments 21](#_Toc54173866)

[3.1.1 What is Security Risks Assessments 21](#_Toc54173867)

[3.1.2 How does Security Risk Assessments works? 21](#_Toc54173868)

[3.1.3 The importance of Security Risks assessment 22](#_Toc54173869)

[3.1.4 The following step of Security Risks assessment 22](#_Toc54173870)

[3.2 The current weakness or threat of the organization 24](#_Toc54173871)

[3.2.1 Data is not encrypted 24](#_Toc54173872)

[3.2.2 Unauthorized data change 24](#_Toc54173873)

[3.2.3 Fake technique 24](#_Toc54173874)

[3.3 Tools to propose to treat the IT security risk 25](#_Toc54173875)

[3.3.1 Splunk 25](#_Toc54173876)

[3.3.2 OSSED 25](#_Toc54173877)

[4 D1 Investigate how a ‘trusted network’ may be part of an IT security solution. 25](#_Toc54173878)

[4.1 Discuss and explain what are trusted network 25](#_Toc54173879)

[4.2 Give brief details with an example on how its use. 26](#_Toc54173880)

[4.3 How can it be a solution in IT security 28](#_Toc54173881)

[5 P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS [20]. 30](#_Toc54173882)

[5.1 Firewall 30](#_Toc54173883)

[5.1.1 Definition 30](#_Toc54173884)

[5.1.2 Advantages: 30](#_Toc54173885)

[5.1.3 Usage: 30](#_Toc54173886)

[5.1.4 How does a firewall provides a security to a network 31](#_Toc54173887)

[5.1.5 The potential impact (Threat-Risk) of FIREWALL incorrect configuration to the network 31](#_Toc54173888)

[5.2 IDS: 32](#_Toc54173889)

[5.2.1 Definition: 32](#_Toc54173890)

[5.2.2 Usage of IDS: 32](#_Toc54173891)

[5.3 The potential impact (Threat-Risk) of FIREWALL and IDS incorrect configuration to the network. 33](#_Toc54173892)

[6 P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security 33](#_Toc54173893)

[6.1 DMZ [24] 33](#_Toc54173894)

[6.1.1 Definition 33](#_Toc54173895)

[6.1.2 Usage: 34](#_Toc54173896)

[6.1.3 Purpose of DMZs : 34](#_Toc54173897)

[6.2 NAT: 35](#_Toc54173898)

[6.2.1 Definition: 35](#_Toc54173899)

[6.2.2 Usage 35](#_Toc54173900)

[6.2.3 Purpose Of NAT: 36](#_Toc54173901)

[6.3 Static IP: 36](#_Toc54173902)

[6.3.1 Definition: 36](#_Toc54173903)

[6.3.2 Usage: 36](#_Toc54173904)

[6.3.3 Purpose: 36](#_Toc54173905)

[7 M2 Discuss three benefits to implement network monitoring systems with supporting reasons 37](#_Toc54173906)

[7.1 What is Network Monitoring? 37](#_Toc54173907)

[7.2 Some of the networking monitoring devices 37](#_Toc54173908)

[7.2.1 Router 37](#_Toc54173909)

[7.2.2 Firewall 37](#_Toc54173910)

[7.2.3 Intrusion Detection Systems (IDS): 38](#_Toc54173911)

[7.3 Why do you need to monitor network? 39](#_Toc54173912)

[7.3.1 Cost Savings 39](#_Toc54173913)

[7.3.2 Network Performance 39](#_Toc54173914)

[7.3.3 Security 39](#_Toc54173915)

[7.3.4 Troubleshooting 40](#_Toc54173916)

[7.3.5 Usage Trends 40](#_Toc54173917)

[7.4 Benefits to implement network monitoring systems 40](#_Toc54173918)

[8 References: 42](#_Toc54173919)

List of Figure:

Figure 1 : Threat agents classification.

Figure 2: Country on the World.

Figure 3: Worm, horse.

Figure 4: Theft.

Figure 5: Hacker.

Figure 6: Organized crime.

Figure 7: Natural disaster.

Figure 8: Stolen data.

Figure 9: Uber data breach.

Figure 10: Facebook data breach.

Figure 11: Marriot data breach.

Figure 12: Network access list.

Figure 13: Learning rule from the company.

Figure 14: The “trusted” network.

Figure 15: Diagrams the example of how firewall works.

Figure 16: Diagram of IDS.

Figure 17: Diagram of DMZ.

Introduction:

The report is written by the student for the Assignment 1 of the Security subject in the University of Greenwich. By conducting the information and data from the Internet as well as the knowledge from the school, I hope this can help another student can know clear about this subject. The main value of the report include something such as: Identify types of security threat to organisations; Give an example of a recently publicized security breach and discuss its consequences; Identify types of security threat to organisations; Give an example of a recently publicized security breach and discuss its consequences; Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS; Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security; It just the basic content, moreover, I mention to some advance information such as: Propose a method to assess and treat IT security risks; Propose a method to assess and treat IT security risks.

Body of the report

# P1. Identify types of security threat to organisations.

## Define threats

A security threat is described as a threat that can potentially affect computer systems and organizations. Like someone stealing a device containing vital data, the trigger may be physical. The trigger can also be non-physical, such as an attack by a virus.

## Identify threats agents to organizations [1]

A threat agent also called a threat actor is any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat. Examples of threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states or individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.system entity that performs a threat action, or an event that results in a threat action. Type of threats that organizations will face. Some examples below will help you to know the issue clear

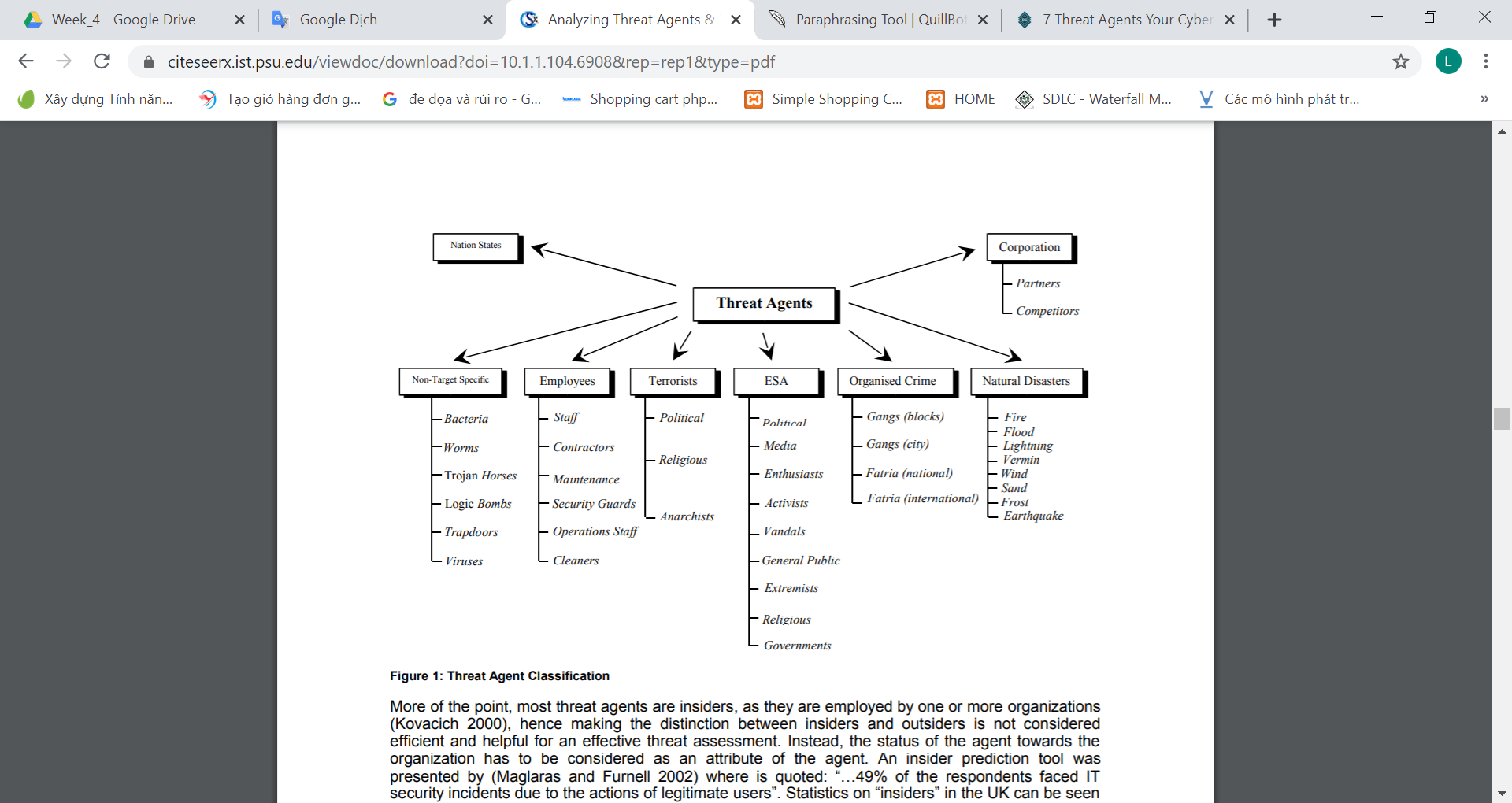


Figure 1 : Threat agents classification [1]

1. States of the Country:

Companies operating in some sectors, such as telecoms, oil & gas, mining, power generation, national infrastructure, etc., may find themselves targeting foreign countries to either disrupt operations now, or to offer a potential hold to that nation in times of adversity.



Figure 2: Country on the World (Lindholm et al., 2020)

2. Non-target specific (vandal-perpetrated ransomware, worms , trojans, logic bombs, backdoors and viruses and the general public).



Figure 3: Worm, hore [4]

The number of random attacks that occur every day is so enormous that every organization can become a victim (there are no reliable statistics on this to share here).

3. Employees and Contractors



Figure 4: Theft [5]

Machines and software programmes are quite good at protecting against malware, unless it is a Zero-day virus. It is humans that are often the weakest link in the security system, either maliciously or accidentally.

4. Terrorists and Hacktivists (political parties, media, enthusiasts, activists, vandals, general public, extremists, religious followers)

Rather like the threat caused by nation states, it does depend on your activities as to the level of threat these agents pose. However some terrorists look to target certain industries or countries so there could be a persistent threat of a random attack against you.



Figure 5: Hacker.

5. Organised crime (local, national, transnational, specialist)



Figure 6: Organized crime [7]

Criminals are targeting personal data for a number of different reasons; credit card fraud, identity theft, bank account fraud and so on. These crimes are now being perpetrated on an industrial scale. Methodologies vary from phishing attacks to ‘Watering Hole’ websites, but the end result is the same; you and your data are being extracted and used for nefarious means.

6. Natural disasters (fire, flood, earthquake, volcano)



Figure 7: Natural disaster [8]

Whilst not a cyber attack, these events can have the same net effect to your ability to do business. If you cannot access your offices, data centres, or files stored on the cloud, then you are still experiencing a data disaster, and this must be taken into account. In the UK the threat of earthquake is very low, but every year we see pictures of a town or city under water.

7. Corporates (competitors, partners)



Figure 8: Stolen data [9]

The threat from a competitor stealing your intellectual property is obvious, but we are increasingly working with many partner organisations to fill gaps in skills and resources, or simply to provide services. These partner companies may steal, or reveal, your intellectual property, or the personal data you are storing, either unwittingly, or maliciously, depending on their motives.

## Example of a recently publicized security breach and discuss its consequences.

### Uber[10]:



Figure 9: Uber data breach [11]

Nope, 2017 was not Uber’s year. In November, Uber disclosed that hackers previously stole the personal information of approximately 57 million riders and drivers in a mega data breach that occurred in October 2016. Back when it actually happened, Uber paid the criminal $100,000 to keep quiet about the breach and keep the data safe

The stolen data included email addresses, phone numbers, and names belonging to riders and drivers. Some of the drivers also had their drivers license numbers stolen as well. According to Uber’s new CEO, Dara Khosrowshani, the deal Uber struck with the thieves was arranged by the company’s former CSO and CEO.

### Facebook data breache [13]



Figure 10: Facebook data breach[12].

In April 2019, the UpGuard Cyber Risk team revealed two third-party Facebook app datasets had been exposed to the public Internet. One, originating from the Mexico-based media company Cultura Colectiva, weighs in at 146 gigabytes and contains over 540 million records detailing comments, likes, reactions, account names, FB IDs and more. This same type of collection, in similarly concentrated form, has been cause for concern in the recent past, given the potential uses of such data.

### Marriot data breach [15]



Figure 11: Marriot data breach [14]

Marriott says a security breach may have exposed the personal information of 5.2 million guests. This marks Marriott’s second data breach in recent years, following a breach in 2018.

Personal information such as names, birthdates, and phone numbers may have been taken in the breach, along with language preferences and loyalty account numbers, Marriott says. Although an investigation is still in progress, Marriott said there is “no reason” to believe that payment information was leaked.

## Consequences [16]:

Data loss is a major annoyance that interferes with the daily functioning of any information-based organization. In order to fill the holes left by deletion, your company must expend time and money recreating or retrieving certain data when essential data and records are lost. Although you may be able to find hard copies of records, these may not be as up-to - date as the missing digital copies.

Data loss also sets back deadlines for efficiency and if it is accompanied by security breaches, it may cause you to lose clients. Your business must disclose this to consumers when confidential data is stolen or compromised, causing you to lose their trust and respect. You would need to spend time rebuilding consumer relationships even though your business will recover from the data loss.

Perhaps the biggest long-term consequence of a data breach is the loss of customer trust. Customers share their sensitive information with businesses like yours assuming that you’ll have the proper security measures in place to protect their data. A good reputation is often a company’s most prized asset as a business must work constantly to build and maintain the integrity of its brand. However, one compromising episode like a data breach can tarnish even the best of reputations.

## Solutions:

Understanding the consequences of a data breach is an important first step on the road to safeguarding your business. The next step is creating an action plan so you can protect what you’ve worked.

Here are some details can help you to solve some security issues:

1. Using and configure firewall :

The importance of firewall will not in debate. The right firewall gives many benefits such as: Monitors Network Traffic; Stops Virus Attacks; Prevents Hacking; Stops Spyware;Promotes Privacy.. Up to now, it plays an important role to protect the orgainization.

2. Uninstalled unsecured application:

When you download and install some harmful application, the hacker can steal the neccesary information of your organization. So, eliminate downloading unauthorized application to prevent it.

3. Setup the limited permission for the application

By doing the rules, the application can not access to some necessary folder or files that you stored in the devices.

# P2 Describe at least 3 organizational security procedures.

## Security procedure definition:

A security procedure is a set sequence of needed activities performed by a particular task or feature of security. Procedures are typically structured as a sequence of steps to be followed to achieve an end result as a consistent and repeated method or cycle. When introduced, security protocols include a series of steps in place to perform the organization's security affairs that will promote preparation, process auditing and process enhancement. Procedures provide a starting point for the implementation of the continuity required to minimize security process inconsistency, which improves security control within the organization. Decreasing variability is also a good way for the safety department to reduce duplication, improve efficiency , and increase performance.

## Security procedure purpose

The purpose of security procedures is to ensure consistency in the implementation of a security control or execution of a security relevant business process. They are to be followed each time the control needs to be implemented or the security relevant business process followed.

## Some organizational security procedures

### Network Access procedure:

#### Definition:

This is a list of steps that the user must to follow when they want to access the network of the Office or the Organization. And play an important role to protect information of our office or organization.

#### Purpose:

Network Access Control (NAC) helps enterprises implement policies for controlling devices and user access to their networks. NAC can set policies for resource, role, device and location-based access and enforce security compliance with security and patch management policies, among other controls.

#### Network Access procedure in organizational:

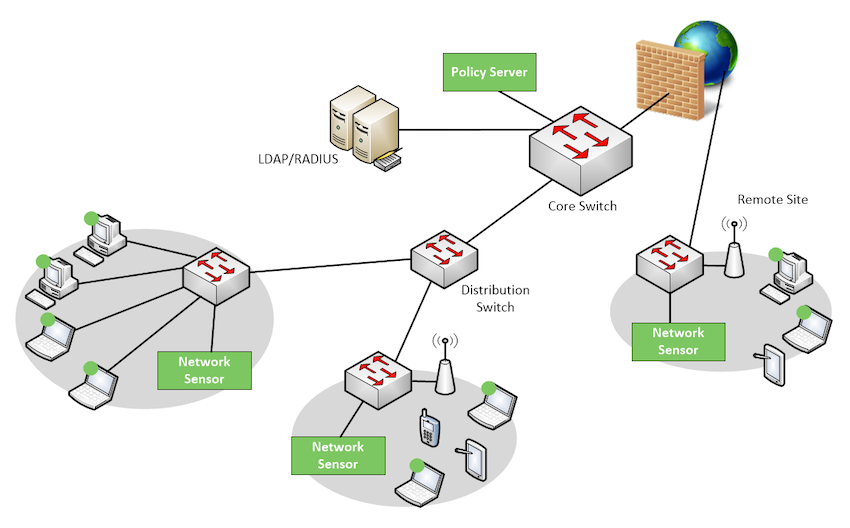


Figure 12: Network access list [17]

Step 1. Each user is allocated an individual user name and password. Logon passwords must not be written down or disclosed to another individual. The owner of a particular user name will be held responsible for all actions performed using this user name.

Step 2. Staff must notify the IT Help Desk when moving to a new position or location within company. This ensures that the necessary setups to provide fast access to the most appropriate mail and file servers can be put in place.

Step 3. Management must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential client information and moves to another role where this access is not required.

Step 4. All user accounts have the following password settings on the lists: Minimum password length of 8 characters; A combination of alpha, numeric and punctuation should be used; Users are forced to change their passwords every (insert number) days; Users cannot repeat passwords; Accounts are locked after (insert number) incorrect login attempts; Passwords must not be easily guessed (i.e. names, months of the year, days of the week, usernames, etc. must not be used as passwords).

### Advising on personal security procedure:

#### Definition:

Advising on personal security procedure is the set list follow can help the staff in the Office or Organization. They must to study and learn to apply it on the Organization environment.



Figure 13: Learning rule from the company [18]

#### Purpose

It plays an important role that help the fresher can follow the rules of the organization, by thatm can help the security of us can work more productivity and no mistake while operating and working.

#### Advising on personal security procedure:

Step 1: Develop Personal Security Guidelines and make them available to members of the University community.

Step 2: Provide training and/or information sessions on personal security as required, e.g.: preventing violence in the workplace, dealing with conflict and aggression in the workplace, domestic/family/relationships violence, personal and/or asset protection.

Step 3: On having a threat to personal security reported, develop in consultation with the individual affected and relevant stakeholders a Violence Prevention Plan to eliminate or minimise risks

Step 4: Report circumstances to Safer Campuses Initiative Team, with approval of person concerned

Step 5: Assist the individual(s) and School/Directorate concerned obtain and implement any risk control measure required (e.g. response protocols, alarms, etc.)

Step 6: Monitor the continued  implementation of the risk control measures.

### Conducting security patrols of company premises [19]

#### Definition

In some large companies, protecting the security patrols is very importance. The security guard must to do the step by step to ensure the safety zone.

#### Purpose

Ensuring the working-zone, create the environment avoid some thefts or terrorisms.

#### Conducting security patrols of company premises procedure

Step 1: Conduct routine and ad hoc patrols of Company premises in accordance with Standard Operating Procedures (SOPs) to Help your organization can follow the rule before establish the following step.

Step 2: Establish a visible and competent security presence that provides direct assistance to the Company community.

Step 3: Secure premises after hours and, if required, assist authorised persons to gain access to Company premises.

Step 4: Monitor the presence after-hours of members of the University community on Company premises, in accordance with the After-Hours Work/Study Procedure.

Step 5: Deter and detect security threats and defend the Company community and property from these threats, whilst protecting own safety.

Step 6: Respond to incidents and emergencies in accordance with the Incident and Emergency Management Procedure and SOPs.

Step 7: Provide first aid to any injured person.

Step 8: Record and report all security incidents, activities and interactions with the Company community.

Step 9: Report instances of unserviceable security infrastructure

Step 10: Identify and report workplace hazards, damage to property.

# M1 Propose a method to assess and treat IT security risks.

## Methods required to assess it security threat: Security Risks Assessments

### What is Security Risks Assessments

Security Risk Assessments are deep dive evaluations of your company, or maybe even a specific IT project or even a company department. During the assessment, the goal is to find problems and security holes before the bad guys do. The assessment process should review and test systems and people, looking for weaknesses. As they are found, they are ranked based on how big of a risk they are to the company. The resulting report will identify systems that are working well and properly secured, and those that have issues. A Security Risk Assessment will typically have very specific technical results, such as network scanning results or firewall configuration results.

### How does Security Risk Assessments works?

An information security risk assessment will give you an accurate snapshot of the security risks that might compromise the confidentiality, integrity and availability of your organization’s information assets. It can be used to help an organization select the appropriate security controls based on business needs and a cost-benefit analysis. ISO/IEC 27001:2013 (ISO 27001) defines best practices for building and managing an information security management system (ISMS), a risk-based approach to securing corporate information assets that addresses people, processes and technology.

### The importance of Security Risks assessment

Security risk assessments help an organization strengthen its security. They can help a company identify security vulnerabilities, create new security requirements, spend cybersecurity budgets more intelligently, conduct due diligence and improve communication and decision-making. A security risk assessment can improve an organization’s security posture, which is essential in today’s increasingly insecure world.

### The following step of Security Risks assessment

The steps below will help an organization build an effective risk assessment:

**- Define the requirements**

The first step is to identify the business, regulatory and contractual requirements that must be met related to information security. For example, the requirements of the European Union’s General Data Protection Regulation (GDPR) apply to organizations that process or control personal information. The second step is to establish the risk scale, a combination of the likelihood and impact of security incidents. Risk assessments may be qualitative or quantitative

- Identify risks:

Risk identification is a time-consuming activity that involves validating the risks for each of the following:

• The asset (the value to be protected)

• The threat (which can affect the asset)

• The vulnerability (the weakness that allows the threat to affect the asset).

Threats and vulnerabilities vary. Be sure to identify the risks that compromise the confidentiality, integrity and availability of data impacting the organization. Check the existing controls to avoid unnecessary duplications of measures.

- Analyze risks:

Risk analysis typically involves understanding how a threat might occur, which requires you to identify a vulnerability in your assets and a threat that could exploit the vulnerability.

For each security event you identify, you should be able to assess the likelihood of a threat exploiting the vulnerability and assign it a score or value. Referring back to the risk scale, the factors influencing the impact of the threat can include human, financial, legal, regulatory, reputational and operational issues, and the likelihood factors can include frequency of occurrence, previous occurrence, current levels of security control, size of attack group and knowledge of vulnerability.

- Evaluate risks:

Your company’s risk assessment software should automatically collect the results of your risk analysis, calculate where each risk sits on the risk scale and identify whether the risk falls within your predetermined level of acceptable risk. You should quickly be able to identify your highest risks and, therefore, prioritize which risks to address first.

- List risk treatment options:

After evaluating and prioritizing risks, companies should respond to them based on the existing controls. Treatment options include:

* + Accept the risk: This is normally done by implementing security controls that will reduce the risk’s likelihood or impact.
  + Mitigate the risk: You can accept that the risk falls within your established risk acceptance criteria, or decide that it requires extraordinary decisions.
  + Transfer the risk: This generally happens through insuring or outsourcing. Although your company will typically still suffer the effects of a breach, it can share the risk with someone better able to mitigate it.
  + Terminate the risk: Your company can take steps to end the activity or circumstance causing the risk.

- Conduct regular visits:

Risk assessment is a cycle that follows the plan-do-check-act (PDCA) approach. Risks will continue to emerge, change or recede. Companies should consider all the factors documented in the first step in a risk management plan when revisiting the risk assessment on a regular basis. The results should be discussed with a company management security forum.

## The current weakness or threat of the organization

### Data is not encrypted

According to VSEC expert analysis, data encryption is a very basic but extremely important part of effective network security measures. All data stored online or on the organization's computers must be encrypted. Because if the data is not encrypted, hackers can easily steal and use it immediately.

### Unauthorized data change

According to the VSEC expert, sometimes hackers do not enter to steal data, they simply want to change data. This type of attack is difficult to detect and can cost financial institutions heavy losses, since the original data format and after the attack are not very different, so determining what was changed if Being hacked in this way is no small challenge.

Hackers try to impersonate the organization's URL with a website that looks and behaves exactly the same way, when a user logs in immediately, information will be stolen. What's more, the latest spoofing techniques use only a similar URL - it is possible not to be identical to target users who visited the exact URL.

### Fake technique

As a bank or financial institution, it is imperative to find ways to mitigate information security threats while still being able to offer customers advanced, convenient technology options.

Banks and financial institutions must invest heavily in training, both to improve the professional skills of the internal security engineering team, and to promptly and continuously update threats and issues. data protection. Another highly recommended security management model today is CsaaS (Cyber ​​Security as a Service), which allows an organization to use a team of experienced and skilled professionals to come up with the appropriate network security strategy well suited.

## Tools to propose to treat the IT security risk

### Splunk

Designed for both real-time analysis and historical data searches. Splunk is a fast and versatile network monitoring tool.

One of the more user-friendly programs with a unified interface. Splunk’s strong search function makes application monitoring easy. Splunk is a paid app with free versions available. The free version is limited. This is an excellent tool to put on the list for those who have a budget to work with. Independent contractors tend to be careful about the premium tools they buy. Splunk is well worth the cost. Any information security professional with a strong enough client base should invest in Splunk.

### OSSED

OSSEC open-source intrusion detection service provides real-time analytics of system security events. It can be configured to be constantly monitoring all possible sources of entry and access, including files, rootkits, logs, registries, and processes. It is also available for a variety of platforms, such as Linux, Windows, Mac, BSD, and VMWare ESX. The OSSEC user community is also good at sharing strategies, modifications, support, and other useful information. Other available tools include “Atomicorp,” which provides ‘self-healing’ to automatically fix detected vulnerabilities, and Wazuh, which offers training and support.

# D1 Investigate how a ‘trusted network’ may be part of an IT security solution.

## Discuss and explain what are trusted network

it is not easy to define what a trusted network consists of, or what comprises a trusted network even within a single corporation or entity, since the concept of “trust” doesn’t apply equally even within a single company—you’ll still want to control access to sensitive information such as payroll or HR information. The old concept of firewalls and networking dictated that we have an Internet connection coming into a firewall from a single point, and this firewall would protect our inside networks from all attackers. Today, the idea of the network perimeter is expanding and shifting; many technologies make this previous definition outdated. Today we are remotely accessing our network via mobile phones, VPN clients from a personal DSL connection in our homes; we are also providing access to our network for our employees, and often for our suppliers and customers. The idea of perimeter security is disappearing because of the prevalence of wireless and home-based high-speed Internet connections in such a way that old concepts are no longer valid. Attackers are not always coming from outside your network; insiders may become the most dangerous attackers, as they have access to the intranet and may get proprietary information. Therefore, it should be mandatory to restrict the accesses and privileges in a “Need to Know” or “Need to Access” policy, giving access and privileges just when necessary and not by default to all your users. You have to update your mental schemas to protect your networks from today’s threats.

As always, identify the data that is going through each network segment to be able to apply the appropriate security measures. This is a crucial step because, in a typical environment, an Engineering department’s requirements would differ from Human Resources’, and the network running the fileservers would be different from the network supporting the Web server. And what about your financial departments, or the differences between the procurement and the sales departments? Each group of users needs different accesses and privileges, and you will have to provide them all in a way that is easy and productive.

## Give brief details with an example on how its use.

A “trusted network” is required for each organization to clearly distinguish between functional network zones and to establish separate information security policies for each network area according to actual requirements.

First, we need to learn about the components in the secure network model, the components in the “trusted” network include:

1. Local area network: Also known as LAN (Local area network), is the place where network devices, workstations and servers belong to the internal network of the unit.

2. DMZ Area: The DMZ area is a neutral network area between the internal network and the Internet, which contains information allowing users from the Internet to access and accept risks from Internet attacks. Services commonly deployed in the DMZ are: Web server, Mail server, DNS server, FTP server, ...

3. Server Network Area (Server Farm): Server or Server Farm network area, is the place where servers do not directly provide services to the Internet. Servers deployed in this area are usually Database Server, LDAP Server, ...

4. Internet area: Also known as external network, connects to the global Internet.

The security network model organization to ensure security has a great impact on the safety of network systems and electronic information portals. This is the first basis for the construction of defense and protection systems. In addition, the organization of a secure network model can effectively limit internal and external attacks.

Example:

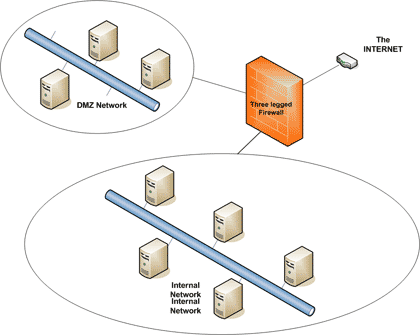


Figure 14: Trusted network.

In the case of network security zones, a firewall enforces the access control policy, determining which traffic is allowed to pass between the configured zones. With this common three-zone implementation (Internal network, DMZ network, and the external network- the Internet ), there are several recommended zone filtering policies that should be in place:

- Inside-to-Outside and Inside-to-DMZ: As it passes towards either the outside or the DMZ, traffic originating from the inside is inspected. Examples involve an employee requesting a web page from a public web server or accessing inside the DMZ some resource. With very few constraints, if any, this type of traffic is permitted.

- Outside-to-Inside: Traffic coming from outside and heading into the inside is completely blocked, unless the traffic is in response to an internal resource request. For example, if a website is requested from a public web server by an internal user, this outside-to-inside traffic is enabled. Connections that are not a response to a request from a public network will be refused.

- DMZ to Inside: Traffic originating from the DMZ and moving inside is also completely blocked, unless the traffic is a response from inside to a valid request.

- Outside to DMZ: The firewall inspects and selectively permits or refuses traffic originating from the outside and heading into the DMZ. Unique traffic types, such as email, HTTP , HTTPS, or DNS traffic, can be passed through. Note also that DMZ responses back to the outside will be dynamically enabled. In other words , in order to allow the necessary traffic from the DMZ to the outside as needed, the firewall will dynamically open a port.

- DMZ to Outside: On the basis of service specifications and firewall regulations, traffic originating from the DMZ and heading towards the outside is selectively permitted. For example, if there is an email server in the DMZ that needs to be replicated to another location with an email server, this form of traffic should be allowed by the firewall policy.

## How can it be a solution in IT security

In the IT security, the big importance in advantages aspect of the “trusted” network bring can be use very popular in the organization, company and no one can rejected the mission such as:

- Filter and manage Denial-of-Service attacks: Today, A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle. So, the mission of protect this kind of attack can be treated in the “trusted” network.

- Scan e-mail messages for virus, content, and Most viruses, Trojan horses, and worms are activated when you open an attachment or click a link contained in an email message. If your email client allows scripting, then it is possible to get a virus by simply opening a message. It's best to limit what HTML is available in your email messages. The safest way to view email messages is in plain text.Prevent application-layer attack but, when the employee forget this, the trusted network can prevent.

- Provide port scans: A port scan is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system’s firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer. By the function of trusted network, it’s under the control of the system.

- Limit access to the trusted network via a single protocol: organizational network likely has a connection to the Internet. You also likely have partners, vendors, or contractors who attach devices that are not owned by your organization to your network. Because you do not manage those devices, you cannot trust them to be free of malicious software, maintained with the latest security updates, or in any way in compliance with your organization's security policies. These untrustworthy devices both on and outside of your physical network must not be permitted to access your organization's devices except where it is truly required. By using the trusted network, you can mitigate this risk, you must be able to isolate the devices you trust, and restrict their ability to receive unsolicited network traffic from untrusted devices. By using connection security and firewall rules.

# P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS [20].

## Firewall

### Definition

A firewall is software or firmware that prevents access to a network from being unauthorized. Using a set of rules to recognize and block threats, it inspects incoming and outgoing traffic.

In both private and business environments, firewalls are used, and several machines come with one built-in, including Mac, Windows , and Linux computers. They are commonly considered an important component of the security of the network.

### Advantages:

They have had an immense effect on modern safety practices and are still commonly used. In the early days of the internet, they first appeared, when networks needed fresh security methods that could manage growing complexity. In the client-server model, the core architecture of modern computing, firewalls have since become the cornerstone of network security. Firewalls or closely related mechanisms are used by most devices to inspect traffic and mitigate threats.

### Usage:

In both corporate and customer environments, firewalls are used. Modern companies integrate them together with other cybersecurity devices into a security information and event management (SIEM) strategy. They can be built to protect against external threats at the network perimeter of an enterprise, or inside the network to establish segmentation and protect against insider threats.

In addition to immediate threat defense, firewalls perform important logging and audit functions. They keep a record of events, which can be used by administrators to identify patterns and improve rule sets. Rules should be updated regularly to keep up with ever-evolving cybersecurity threats. Vendors discover new threats and develop patches to cover them as soon as possible.

### How does a firewall provides a security to a network

A firewall creates a boundary between the network it guards and an external network. Via a network link, it is inserted inline and inspects all packets that reach and exit the guarded network. It uses a set of pre-configured rules to differentiate between benign and malicious packets when inspecting them.

Rule sets can be based on several things indicated by packet data, including:

* Their source.
* Their destination.
* Their content.

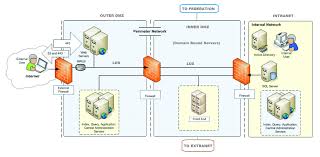


Figure 15: Diagrams the example of how firewall works [21]

### The potential impact (Threat-Risk) of FIREWALL incorrect configuration to the network

A firewall error either creates security holes that will allow malicious traffic to sneak into a private network or blocks legitimate traffic and disrupts normal business processes, which in turn could lead to irreparable, if not tragic, consequences. It can destroy all the data and neccesary information of your organization. The hacker or the cracker will steal the necessary for them. Moreover, the physical consequences include harmfull the information technology system. Make the organization delay or cancel the activities of us.

Moreover, while using the incorrect firewall, your network will face with some big problems such as: Virus attack by the hacke,… some spywares as well as malware which wants to steal information and data of the network.

## IDS:

### Definition:

(Intrusion Detection System) Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack. Intrusion detection is very tricky. Too much analysis can add excessive overhead and also trigger false alarms. Insufficient analysis can overlook a valid attack.

### Usage of IDS:

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.

Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and domain name system (DNS) poisonings.

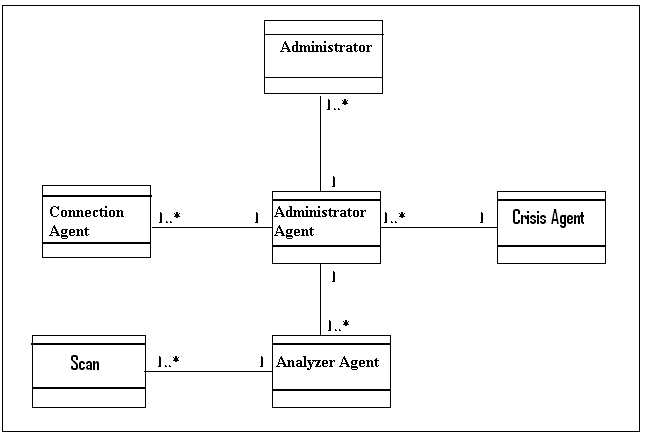


Figure 16: Diagram of IDS. [22]

## The potential impact (Threat-Risk) of FIREWALL and IDS incorrect configuration to the network.

An incorrect IDS can impact very much to the security of the network such as it can not monitor and evaluate threats, catch catch intruders and take action in real time to thwart such instances that firewall or antivirus software may miss. Do not prevent DoS/DDoS attacks or maintain the privacy of users as IPS records the network activity only when it finds an activity that matches the list of known malicious activities.

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

## DMZ [24]

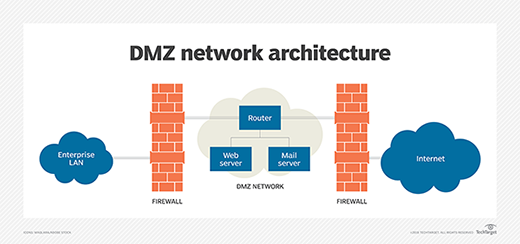


Figure 17: Diagram of DMZ [23].

### Definition

A DMZ (demilitarized zone) in computer networks, also often referred to as a perimeter network or a screened subnetwork, is a physical or logical subnet separating an internal local area network ( LAN) from other non-trusted networks, typically the public Internet. In the DMZ, external servers, tools and services are located. They are therefore available from the internet, but the remainder of the internal LAN remains inaccessible. This provides the LAN with an extra layer of security as it limits the ability of a hacker to access internal servers and data directly through the internet.

The DMZ network can be used for any service offered to users on the public Internet. Web servers and proxy servers, as well as email, domain name system ( DNS), file transfer protocol ( FTP) and voice over IP ( VoIP) servers, are some of the most popular of these services.

### Usage:

DMZs are intended to operate between the public internet and the private network as a sort of buffer zone. Deploying the DMZ between two firewalls ensures that all inbound network packets are screened before they hit the servers hosted by the company in the DMZ using a firewall or other security appliance.

If a better-prepared threat actor goes through the first firewall, before they can do any harm, they must then gain unauthorized access to those services and those networks are likely to be hardened against such attacks.

Finally, assuming that a well-resourced threat actor can penetrate the external firewall and take over a system hosted in the DMZ, before they can access critical enterprise resources, they must also break through the internal firewall. Although even the best-secured DMZ architecture can be compromised by a determined intruder, a DMZ under attack can set alarms, giving security professionals ample warning to avoid a complete breach of their org.

### Purpose of DMZs :

The primary purpose of a DMZ is that it provides users with access to some protected resources from the public Internet while also retaining a gap between those users and the internal private network. The protection advantages of this buffer are manifested in many ways, including:

Access Control for Organizations

Organizations may provide users with access through the public Internet to services located beyond their network perimeters. A DMZ network offers access to these required resources while also adding a level of network segmentation that increases the number of barriers that must be bypassed by an unauthorized user before they can access the private network of an entity.

Prevent attackers from performing network reconnaissance

A DMZ prevents an attacker from being able to search out possible targets within the network, since it serves as a buffer. Even if a device inside the DMZ is breached, the internal firewall separating it from the DMZ still protects the private network. For the same cause, it also makes external reconnaissance harder. Since the servers in the DMZ are publicly exposed, another layer of security supports them. The public face of the DMZ prevents the contents of the internal private network from being seen by attackers.

Protection against IP spoofing

By spoofing an approved IP address to impersonate another computer on the network, attackers bypass access control restrictions. A DMZ may stall potential IP spoofers while another network service verifies the legality of the IP address by checking whether it is reachable.

In each case, the DMZ offers a degree of segmentation of the network that creates a space where it is possible to organize traffic and to access public services at a safe distance from the private network.

## NAT:

### Definition:

Stands for “Network Address Translation.” NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

### Usage

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

### Purpose Of NAT:

Some puropse of NAT include

+ Reuse of private IP addresses

+ Enhancing security for private networks by keeping internal addressing private from the external network

+ Connecting a large number of hosts to the global Internet using a smaller number of public (external) IP address, thereby conserving IP address space

## Static IP:

### Definition:

A static IP address is simply an address that doesn’t change. Once your device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes. Static IP addresses generally are used by servers or other important equipment.

### Usage:

Static IP addresses are necessary for devices that need constant access.

Alternatively, if the server were assigned a dynamic IP address, it would change occasionally which would prevent your router from knowing which computer on the network is the server.

### Purpose:

A static IP is useful for consumers and many small businesses that have minor needs such as:

* Host a web, mail or FTP server
* Access a corporate network remotely
* Host a webcam for video streaming
* Use video conference applications

# M2 Discuss three benefits to implement network monitoring systems with supporting reasons

## What is Network Monitoring device ?

In today’s world, the term network monitoring is widespread throughout the IT industry. Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.

Important aspects of network monitoring:

* Monitoring the essentials.
* Optimizing the monitoring interval.
* Selecting the right protocol.
* Setting thresholds.

## Some of the networking monitoring devices

### Router

Routers connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel. It connects your business to the world, protects information from security threats, and can even decide which computers get priority over others.

Nowaday, the Router help the user manage the network, or in the Router, they can configure the Access-list, to control the access to the under-control network.

### Firewall

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you’re setting up your network with specific policies to allow or block incoming and outgoing traffic.

### Intrusion Detection Systems (IDS):

Available as devices or as software applications, Intrusion Detection Systems (IDS) allow you to monitor a network for malicious activity or policy violations. Typically, these breaches and activities are centrally reported or collected by a security information and event management system. Some IDS systems are able to intervene as soon as an intrusion is detected. They will then be called intrusion prevention systems (IPS).

Placed at a strategic point or at different points within a network in order to monitor the traffic to and from all the devices on a network, an IDS system will analyze the passing traffic before matching it to the traffic. Transmitted over subnets, to the library of known attacks. Once an attack has been identified or abnormal behavior detected, the administrator will be alerted.

By sticking to the facts of the available techniques that cybercriminals rely on to breach a secure network, IT teams will be able to understand how IDS systems can be configured so they don’t miss out. No threat. Here are some of these techniques:

* Fragmentation: by sending fragmented packets, attackers are able to go completely unnoticed, thus bypassing the detection of the signature attack performed by the system.
* Avoid default locations: The port that the protocol uses does not always indicate details of the protocol being transported. If the attacker has reconfigured the protocol so that it uses a different port, the IDS system may not be able to detect the presence of a Trojan horse.
* Coordinate low bandwidth attacks: Cybercriminals, by organizing a scan between multiple attackers or by assigning different ports or hosts to different attackers complicate the task of the IDS system, making it possible to link the captured packets and understand that a scan current network is much more complex.
* Generate a proxy or spoofing attack: Cybercriminals are able to hide the source of the attack by taking advantage of insecure or poorly configured proxy servers to return an attack. A spoofed source returned by a server makes detection of the attack extremely difficult.
* Modify an attack pattern: IDS systems rely on pattern matching to detect attacks. By changing the architecture of an attack, cybercriminals are able to avoid detection.

## Why do you need to monitor network?

### Cost Savings

Network monitoring can provide significant cost-saving opportunities for your business.

Network monitoring software will also help you to understand which network elements are being used (or overused) and which are underused. It may also help you to discover unnecessary costs that can be eliminated, or identify a network component that requires upgrading to maintain future performance.

Finally, network monitoring provides cost-savings in the form of reduced manpower from your IT team. Reliable monitoring software can reduce the time required to troubleshoot network issues and allow your team to focus on other tasks.

### Network Performance

Monitoring is the best way to keep a pulse on the performance of your business’s network. Active monitoring can assist you in catching problems early, before they impact your daily operation.

Network monitoring software will provide you with real-time data on a wide range of metrics, including bandwidth usage, packet loss, jitter, latency, and much more. This detailed overview of your system will enable your IT team to easily identify the source of any problems.

### Security

Although it should not be your only security solution, network monitoring can help you provide enhanced cyber security for your business and prevent intrusions like ransomware attacks.

There are many ways to detect a security risk on your network. Unusual traffic spikes or unfamiliar devices connected to the network may be early signs of a cyber attack, and network monitoring can spot these red flags.

Proper network management can also prevent your users accidentally accessing harmful websites that could affect your network. Your network can be configured to block access to harmful sites and strengthen security protocols, with the assistance of monitoring. These tactics will help improve the overall security of your network.

### Troubleshooting

The time required to troubleshoot network problems is greatly reduced with proper monitoring. Network monitoring software should provide you with clear benchmark data on your network’s normal performance, which will show you where abnormalities are appearing and effectively trace them back to their root cause.

Active monitoring will also help you to troubleshoot proactively, rather than reactively. This approach will help your business avoid the financial losses that may come with a network outage.

### Usage Trends

Monitoring will help you see usage trends for different time slots and geographies. By identifying usage patterns, you will be able to identify peaks in demand and allocate resources to deliver a better experience for your users.

You can also track the usage of specific applications to understand what’s popular with a specific group or location. This information can help improve your systems for both internal usage and client-facing applications.

## Benefits to implement network monitoring systems

* Keep ahead of the issue: The network management system offers the visibility needed to remain one step ahead of each other of prospective problems. Network monitoring, by viewing live network output data. The device helps to detect outages that can cause bottlenecks.
* Repair problems quicker: As in the network management system, the network monitoring system solves the problems easily and efficiently, live network maps lead to issues and the status window offers metrics for the problems. Over time, results. Not only does network monitoring detect issues, it can resolve them automatically, without having to engage individuals with tools for network automation.
* Allocating capital most efficiently: Efficient network monitoring, the need to dig into output manually or to simply respond. It is possible to eliminate disastrous network events, freeing up resources for other operations.

Evaluation:

The report provide very detail informatiom about the security aspect – one of the issue are carry out from country which approach with digital 4.0. So, we can see the importance of the aspects and the report is the main focus on the hot issue. About the research, this report bring a lot high research (for the object is student) can apply immediately in the real life.

Conclusion:

The report is the individual report, doesn’t copy from another, the information in the report can trusted about the science and study aspects. I hope the research can help the students can understand about the issue that has been increase very fast. But, because this just the student’s research so it can not avoid the verbose and mistake. About 40% information of the report is from the Internet. It maybe out of the control of the science, so I hope the audience can approach and ignore this error.

# References:

1. The Data Guardians. 2020. *7 Threat Agents Your Cyber Security Team Should Be Aware Of | The Data Guardians*. [online] Available at: <https://www.thedataguardians.co.uk/2019/02/27/7-threat-agents-your-cyber-security-team-should-be-aware-of/> [Accessed 15 October 2020].
2. Vidalis, S., 2020. *Analyzing Threat Agents & Their Attributes*. [ebook] Rhondda Cynon Taf: Stilianos Vidalis , Andrew Jones, p.15. Available at: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.6908&rep=rep1&type=pdf> [Accessed 14 October 2020].
3. Lindholm, J., Bodette, M., Lindholm, J., Bodette, M., Lindholm, J., Bodette, M., Lindholm, J. and Bodette, M., 2020. *Why Is The World Split Into Countries?*. [online] Vpr.org. Available at: <https://www.vpr.org/post/why-world-split-countries> [Accessed 15 October 2020].
4. ZOO Repairs. 2020. *Differences Of Virus, Worm And Trojan Horse*. [online] Available at: <https://www.zoorepairs.com.au/computer-tips/differences-of-virus-worm-and-trojan-horse/> [Accessed 15 October 2020].
5. Plushr.com. 2020. *HR Consulting FAQ: The Difference Between An Employee And Contractor*. [online] Available at: <https://www.plushr.com/blog/legal-compliance/hr-consulting-faq-the-difference-between-an-employee-and-contractor> [Accessed 15 October 2020].
6. James, H., 2020. *Does Hacktivism Really Equal Terrorism?*. [online] HackRead. Available at: <https://www.hackread.com/does-hacktivism-really-equal-terrorism/> [Accessed 15 October 2020].
7. New Europe. 2020. *The Fight Against Organized Crime*. [online] Available at: <https://www.neweurope.eu/article/fight-against-organized-crime/> [Accessed 15 October 2020].
8. ArcGIS StoryMaps. 2020. *When Debt Takes The Wheel*. [online] Available at: <https://storymaps.arcgis.com/stories/8c48ba140a7a496b98fa916c08467f24> [Accessed 15 October 2020].
9. Law Technology Today. 2020. *Law Technology Today*. [online] Available at: <https://www.lawtechnologytoday.org/> [Accessed 15 October 2020].
10. Checkmarx. 2020. *Recap: The Biggest Data Breaches Of 2017 | Checkmarx Application Security*. [online] Available at: <https://www.checkmarx.com/2017/12/31/recap-biggest-data-breaches-2017/> [Accessed 15 October 2020].
11. https://www.wtok.com. 2020. *Settlement Reached In Uber Data Breach*. [online] Available at: <https://www.wtok.com/content/news/Settlement-reached-in-Uber-data-breach-494395071.html> [Accessed 15 October 2020].
12. Upguard.com. 2020. *The 36 Biggest Data Breaches [Updated For 2020] | Upguard*. [online] Available at: <https://www.upguard.com/blog/biggest-data-breaches> [Accessed 15 October 2020].
13. Bellemare, J., 2020. *Learnings And Fallout From The Facebook Data Breach | Identityforce®*. [online] We Aren't Just Protecting You From Identity Theft. We Protect Who You Are. Available at: <https://www.identityforce.com/blog/facebook-data-breach> [Accessed 15 October 2020].
14. Fruhlinger, J., 2020. *Marriott Data Breach FAQ: How Did It Happen And What Was The Impact?*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html> [Accessed 15 October 2020].
15. Kedrosky, E., Kedrosky, E. and Marketing, S., 2020. *5 Biggest Data Breaches Of 2020 (So Far) - Security Boulevard*. [online] Security Boulevard. Available at: <https://securityboulevard.com/2020/08/5-biggest-data-breaches-of-2020-so-far/> [Accessed 15 October 2020].
16. Consolidated Technologies, Inc. 2020. *Managed IT Services & Ucaas Provider - NYC | Consolidated Technologies, Inc.*. [online] Available at: <https://consoltech.com/> [Accessed 15 October 2020].
17. Hamill, B., 2020. *Key Considerations For Network Access Control In The Iot Era*. [online] Genians. Available at: <https://www.genians.com/learn-more/insights/key-considerations-for-network-access-control-nac-architecture-in-the-iot-era/> [Accessed 15 October 2020].
18. G2 Esports. 2020. *Welcome | G2 Esports*. [online] Available at: <https://g2esports.com/> [Accessed 15 October 2020].
19. Policy.federation.edu.au. 2020. *Risk Management Procedure*. [online] Available at: <https://policy.federation.edu.au/corporate\_governance/risk\_health\_and\_safety/risk/ch02.php> [Accessed 15 October 2020].
20. SearchSecurity. 2020. *What Is A Firewall And Why Do I Need One?*. [online] Available at: <https://searchsecurity.techtarget.com/definition/firewall> [Accessed 15 October 2020].
21. 2020. *How Do Firewalls Work? Firewall Technology Explained*. [online] Available at: <https://cybersecurity.att.com/blogs/security-essentials/explain-how-firewalls-work-to-me> [Accessed 15 October 2020].
22. SearchSecurity. 2020. *What Is An Intrusion Detection System (IDS) And How Does It Work?*. [online] Available at: <https://searchsecurity.techtarget.com/definition/intrusion-detection-system> [Accessed 15 October 2020].
23. 2020. [online] Available at: <https://www.researchgate.net/publication/328534800\_Evidence\_of\_human-like\_Ca\_2\_Channels\_and\_Effects\_of\_Ca\_2\_Channel\_blockers\_in\_Acanthamoeba\_castellanii> [Accessed 15 October 2020].
24. Siêu thị thiết bị số 24h. 2020. *DMZ Được Hiểu Là Gì?*. [online] Available at: <https://thietbiso24h.com/dmz-duoc-hieu-la-gi> [Accessed 15 October 2020].