ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	TRAN QUANG HUY	**Student ID**	GCD18457
Class	GCD0821	**Assessor name**	Dang Quang Hien

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature
HUY

Grading grid

P1	P2	P3	P4	P5	P6	P7	P8	M1	M2	M3	M4	M5	D1	D2	D3

❒ **Summative Feedback:**

❒ **Resubmission Feedback:**

Internal Verifier's Comments:

Signature & Date:

INTRODUCTION

As Internet use is developing, more and more companies are opening their information system to their partners and suppliers. Therefore, it is essential to know which of the company's resources need protecting and to control system access and the user rights of the information system. The same is true when opening company access on the Internet.

Moreover, because of today's increasingly nomadic lifestyle, which allows employees to connect to information systems from virtually anywhere, employees are required to carry a part of the information system outside of the company's secure infrastructure.

When you create systems that store and retrieve data, it is important to protect the data from unauthorized use, disclosure, modification or destruction. Ensuring that users have the proper authority to see the data, load new data, or update existing data is an important aspect of application development. Do all users need the same level of access to the data and to the functions provided by your applications? Are there subsets of users that need access to privileged functions? Are some documents restricted to certain classes of users? The answers to questions like these helps provide the basis for the security requirements for your application.

CONTENT

TABLE OF FIGURES

TABLE OF TABLES

LO1: Assess risks to IT security

P1. Identify types of security risks to organizations.

No system is safe from computer security threats before today's 4.0 technology era. Once your technology is deployed to run your system more advanced, cyber criminals also try to exploit your business more carefully and in more detail. It will be a frightening and overwhelming reality for companies of all sizes and in all types of industries. A single security breach can potentially jeopardize company's important data assets, incur high costs and even make them inactive.

Figure 1 - Security risks to organizations.
(McConnachie, 2019)

- **Identify all security threats in the organization:**
  - **Malware:** Threats come in many different sizes and forms and mostly use malicious code called "malware". It is software application specifically designed to break, corrupt or gain unauthorized access to the most popular computer systems and delivery methods via email and suspicious websites.

- **Hacker:** At the other end of every security breach is an individual with malicious intent. Most often, businesses are targeted by hackers for financial gain. These predators are seeking out opportunities to capitalize on vulnerabilities, and they are the reason why your organization needs to be on high alert to avoid being victimized by hackers, you must stay vigilant and employ a comprehensive security plan, including file sharing and data management solutions that work hard to keep your critical business assets safe. In addition, your employees need continual education and training on ways to recognize threats and thwart attacks. Without this reinforcement, they are highly susceptible to accidentally inviting an intruder who can do irreparable damage to your company.

➢ **Types of malware:**

- **Virus:** Viruses are dangerous, they're costly and they could be happening right now if you don't have the proper protocols in place to ensure prevention. A virus is a piece of software created to damage a computer. The program replicates and executes itself, interfering with the way a computer operates. It can steal data, corrupt your files or delete them altogether, which is a menacing threat to any business. A virus may also leverage other programs on the machine, such as email, to infect additional computers, and it can be transmitted by a user via a network, USB stick or other media.
- **Worm:** Wiggling its way into your network, a worm is deployed to self-replicate from one computer to another computer. What makes it different from a virus, however, is that it requires no user interaction in order to spread. This software is applied to reproduce in large quantities in a very short period, and it can both wreak havoc on your network performance and be used to launch other malicious attacks throughout your system.
- **Trojan horse**: A Trojan horse, as its name suggests, maliciously pretends to be another thing. Often found in unlocking software downloaded from unauthorized sources (BenSanders, 2017).
- **Rootkit**: Software designed to gain administrator rights (or Root) on the computer without being detected. Often these programs can hide their tracks, making them very difficult to detect. After installation, they can be used to access remote computers or steal information (BenSanders, 2017).

- **Spyware:** An application that collects information about a person or organization they don't know.
- **Adware:** When unwanted advertisements start appearing on a computer, it has been victimized by adware. Your employees may accidentally download adware while trying to access free software, and it can be used to retrieve information without permission or knowledge as well as redirect your users' browsers.
- **Ransomware** - one of the most popular malware in recent years, is software designed to exploit known Windows vulnerability and thus bypass traditional and authoritative antivirus protection. administer malware to the victim's computer. From this point, it starts encrypting all user files and after done, it locks the victim out of their computer and asks to pay the ransom before unlocking the computer (BenSanders, 2017).
- **Polymorphic malware** - An advanced type of special malware that changes its own code when copying, making it difficult for anti-malware programs to detect infection.
- **Phishing**: A phishing scam tricks an internal user into providing information such as usernames and passwords that can be used to breach your system. This information is solicited from employees through email and disguised as legitimate requests (e.g., a vendor or financial institution asking for login details in order to fix an account or resolve an issue). Once the recipient hands over the sensitive information, the hacker gains the access they need to lock up, steal or otherwise compromise your company's critical data. Some phishing techniques use key loggers in combination with sophisticated tracking components to target specific information and organizations. There are also spear-phishing emails that result in a small piece of malware being downloaded to the user's computer without their knowledge, unleashing a network breach that may go undetected for long periods of time. Ultimately, a single phishing attack can endanger the business's entire network and leave every file exposed.
- **Dos attack:** In a DOS (Denial-of-Service) attack, your company's website or web service can be rendered unavailable to users. Often, these attacks are used against businesses for ransom or blackmail purposes. Perhaps the most well-known version is DDoS (Distributed Denial of Service), which involves bombarding your server with traffic and requests in order to overwhelm and shut down the system. With the system and its defences down, an intruder has the capability to

confiscate data or hold your operation hostage. Don't allow your organization to be terrorized by these computer security threats. If you don't have one already, formulate a strong plan to safeguard your business's critical data and protect your assets.

- **Botnets:** A botnet can be used for anything from targeting attacks on servers to running spam email campaigns. As botnets typically involve so many computers, many businesses find them difficult to stop. Basically, this computer security threat is deployed by a botmaster, who commands a number of bots, or compromised computers, to run malicious activities over an Internet connection. The collection of infected computers is often referred to as a "zombie army," carrying out the ill intent of the botmaster. If your organization's network of computers is overtaken by a botnet, your system could be subsequently used to assault other networks by the likes of viruses, worms, Trojan horses and DDoS attacks.
- **Rootkits:** Imagine having a cyber-attacker gain complete control over one of your computers or, worse, an entire network of them. That is what a rootkit, or collection of software implemented to procure administrator-level access, is designed to accomplish. A hacker obtains this access through other threats and vulnerabilities, such as phishing scams, spyware or password weaknesses. The rootkit has the ability to go undetected and enables the originator to modify existing software -- even the security applications employed to protect your computers. (Horan, 2017)

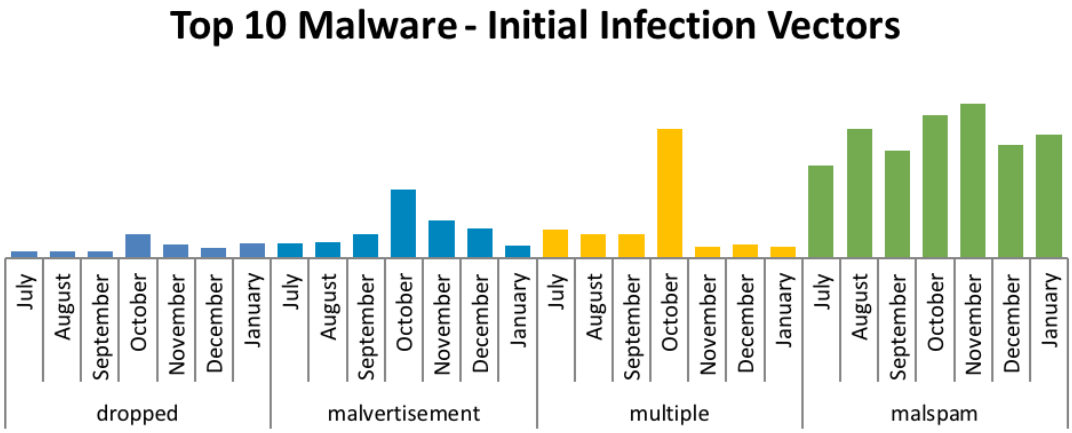


Figure 2 - Top 10 Malware - Initial Infection Vectors

- **How to reduce malware infections?**
  - When there is an attack on any business or organization, it will have a very high level of risk that makes the organization cannot be working immediately and here are some ways to reduce risks for organizations when attacked by malware.
    - Install antivirus software and make sure the software is fully updated.
    - Be extremely cautious about the email attachments you open or the websites you visit. As a rule of thumb, you should not open attachments or click links in emails from people you don't know or even from people you know, but from friends who don't expect attachments or links.
    - Always scan all flash drives with antivirus software before you open any files on them because sometimes there will be some malware found hidden in that drive.
    - Windows firewall must always be turned on.
    - In short, these are just some of the threats to security breaches you need to know, to ensure that your organization is safe and reduces data security risks in the safest way.
  - Security breaches and all types of organizational security risks are again a very important and essential issue in today's system security. Although there are many stories about security leaks and distributed denial of service (DDOS) (Schiff, 2015) attacks and repetitive alerts from security experts that businesses and individuals need to implement. In order to better protect sensitive data, many businesses have not been properly prepared or protected from a variety of security threats.
- **Identify other security threats in the organization:**
  - In addition to the external risks of the organization being attacked into the data system, we also have some cases inside the organization and when attached to the system, it is even more dangerous to be attacked by viruses. outside. We have a few cases:

- **Staff dissatisfied:**

- Employees are the biggest security risk for any organization because they know where the company's valuable data is stored and how to access it. The most common cause of data breach is from an old employee or an unhappy employee, who is not promoted or raises a salary. If a trusted employee is against you, the result may be disastrous if you are not prepared. The best ways to prevent an internal attack are:
  - Be sure to change your password, authenticate and authenticate or disable information when an employee leaves or gets fired, just like you took his or her access card.
  - Monitor and manage access information very closely and ensure privileged account log activity and monitor unusual behaviour.

- **Careless staff:**
  - In addition to malicious attacks, careless employees pose huge network security risks. Too often, workers leave passwords in clear view, posted on their screens or desks or colleagues sharing passwords. Another common problem is that employees open suspicious email attachments or surf malicious websites, which can bring malware into the system.
  - The solution is to train employees with appropriate security procedures. In addition, we must ensure that they absolutely must understand the importance of data security and remind employees to constantly on the risks of malware and suspicious emails. For added security, encrypt the data so it cannot be read even if the system is hacked.
  - Outdated software

- A network security vulnerability is very common in all networks that are outdated software. New viruses and malware are introduced every day and are much more advanced every day. Similarly, operating systems need to be updated periodically with security patches. Obsolete and customized software can also contain serious network security issues, for example: BKAV antivirus software if not updated every day to recognize all new viruses will be attacked right away. Your best strategy now is to ensure that all patches and software definitions are constantly updated, even for business software.

P2. Describe organizational security procedures.

- Security process in the organization are extremely important because of these security procedures help an organization reduce a lot of risks in the organization's data system and help an organization can develop as smoothly as possible. If any organization does not have these security procedures, the organization may have a lot of risks that lead to unwanted.

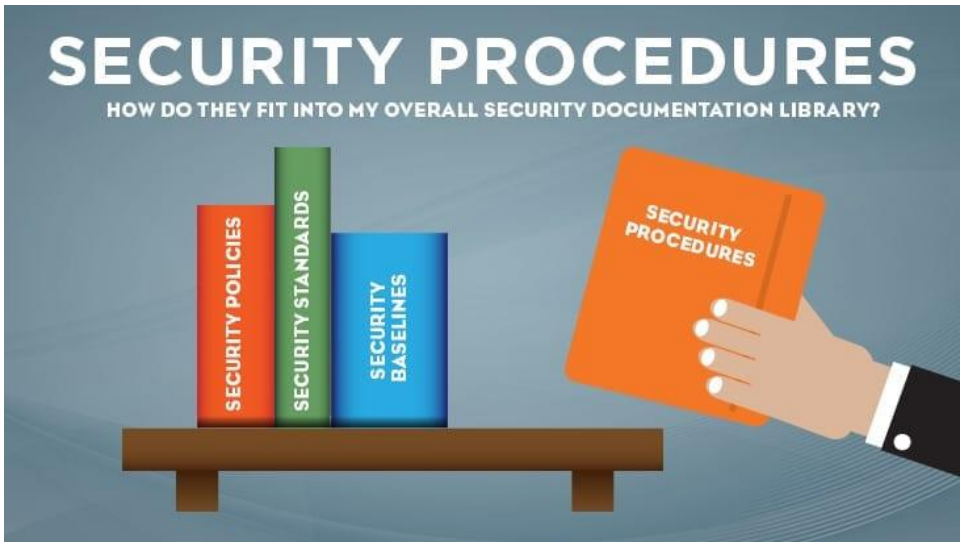


Figure 3 - Security Procedures

(RAY DUNHAM (PARTNER | CISSP, 2018)

- **What is the security procedure?**
  - Security procedures in the organization are all the most detailed instructions about always of implementing all the security controls listed from your organization's security policies and as detailed as possible. All Security procedures will include all hardware and software components required to support all your business processes as well as any security-related business processes.

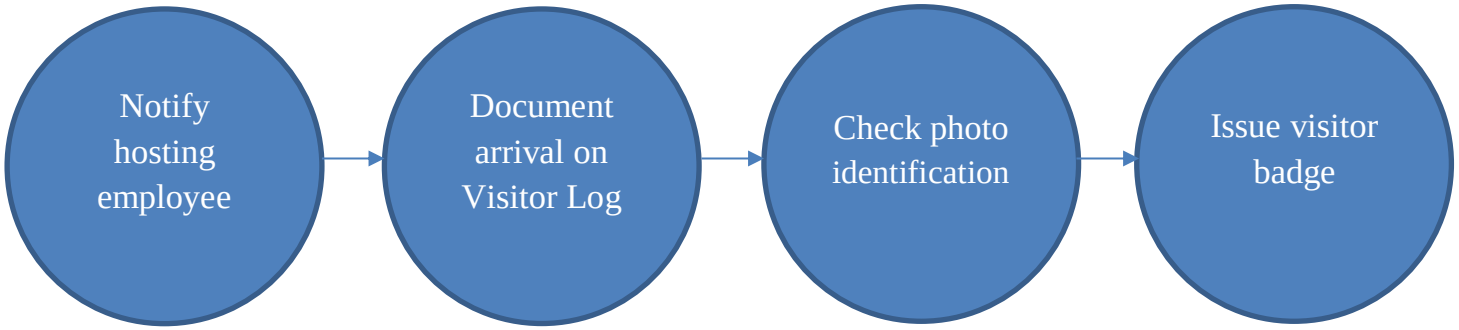


Figure 4 – Example Visitor Entrance (Visitor Controls)

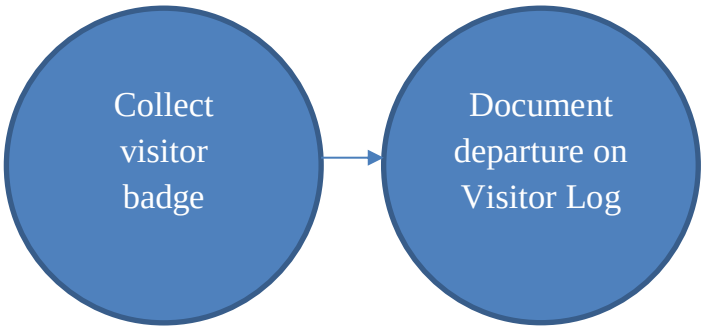


Figure 5 -Example Visitor Exit (Visitor Controls)

- **Why are security processes and purposes necessary in the organization?**

The purpose and process of organization security is to protect and reduce data risks in implementing security controls. They must be enforced every time a security control or business process is followed by all these procedures, such as when you enter a high-security place as the president's meeting must follow. All checklists before meeting the president and you will have to surprise and ask a question "Why do they do this?". Simply, they do it to ensure that you will never assassinate the president. Although security is strict and armed to ensure safety, they still follow the checklist. Follow the checklist to ensure safety and reduce the risk as much as possible. Although they may have made the checklist hundreds of times. In addition, if the process is not tracked in the database, the system administrator can skip a step to the server or unacceptable data and face very dangerous risks in security's organization.

- **What is the relationship between security policy and security procedures?**
  - **A policy** is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.
  - **A standard** is typically a collection or system-specific or procedural-specific requirements that must be meet by everyone. For example, you might have a standard that describes how to harden a Windows 8.1 workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows 8.1 workstation on an external network segment. In addition, a standard can be a technology selection, e.g. Company Name uses Tenable Security enter for continuous monitoring, and supporting policies and procedures define how it is used.
  - **A guideline:** is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

- **A procedure:**
  - A sequence of detailed steps in order to realize the end.
  - Step by step Manual for realization.
  - Example: Standard surgical procedure, Medical procedure.
  - Additional: comes from a “process”; determined way how to do something.

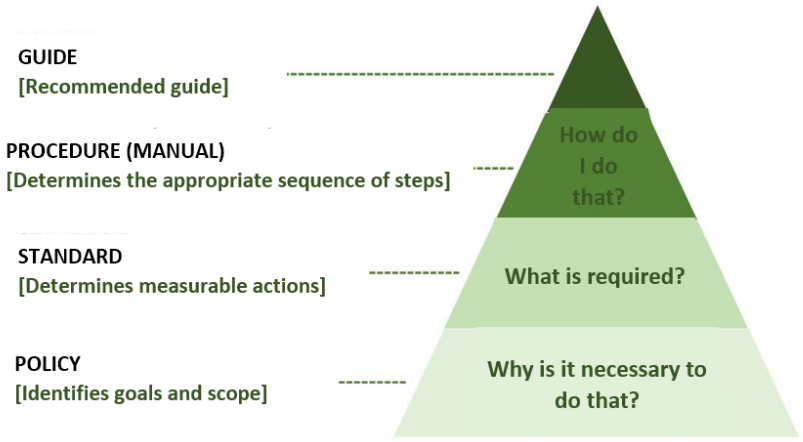


Figure 6 - Schematic representation of the pyramid of policy, standard, procedure (manual) and guide. (zmc, n.d.)

- **Security procedures are built based on the organization's privacy policy.**
  - Organizational security policies are an important platform for an organization's security program. The important principles of all security policies are required to focus on guiding the implementation of all organization's security policies. Like all security policies, all security processes must also be focused on organizational behaviour. In addition, all privacy policies once mentioned who, what and why are required, all security procedures must notify all individuals in the organization at the same time. To help focus on implementing all the security processes in the organization, all the best standards must be enforced and the baseline is also required to be clearly defined. In addition, all standards and baselines should be geared towards technology to implement within an organization, while all policies and procedures must focus on guiding behaviours.

- To better understand the organization's security process, imagine that in your organization, any policies that have been defined and related to creating backups for important information of team users Your position. The organization's security process will be required to support and determine when all backups are made, to the same location and backup media will be recorded as well as all individual steps will be made backup. In summary, keep in mind that all procedural steps will be required to guide all an individual's behaviours to get the clearest and desirable result in an organization.

- **Organization security procedures must have all the details.**
- The organization's security policy must contain all security requirements in a general or advanced way. In addition, all security procedures must provide the most detailed and understandable for an individual who is not familiar with the privacy policy process to achieve the desired results in the organization's privacy policy, because If the privacy policy is too difficult to understand, anyone will not understand and they will cause many risks in the organization's privacy policy.
- **All the organization's security procedures include problems:**
  - Without any organization without an organization's own security policies and procedures in the organization's and post-data systems, one of the most popular organization's security policies includes:
  - **Organization information:**
    - The purpose of this information is to declare all the organization's privacy policies and all of these policies belong to the organization's ownership of your organization.
  - **Apply policy:**
    - The purpose of the application This policy will apply to all information created, received, stored and for the organization's data and applications including: Use, management and storage, information and data. The application of this policy covers all areas, such as: Access control, information security incident management, development and maintenance.
  - **Policy principles:**
    - The principle of an organizational security policy is to identify all the principles to establish all security measures to ensure the integrity of the organization security and reduce all security risks organization, such as: Take all appropriate control measures to protect information from being disclosed to the outside, delete or copy all information of the organization.

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

- **What is a security risk?**
  - **A security risk** is something that could result in the compromise, loss, unavailability or damage to information or assets, or cause harm to people. Security risk is the effect of uncertainty on objectives and is often measured in terms of its likelihood and consequences. The causes are generally people, systems, processes, procedures, crime, attacks or natural events. An:
    - **Effect** is a deviation from the expected and may be positive or negative.
    - **Objective** has different aspects such as financial, health and safety and environmental goals, and can apply at multiple levels such as strategic, organisation-wide, project, product and process levels.
    - **Entities** are encouraged to consider where security risks intersect with other risks including fraud, privacy and business continuity. Entities are encouraged to treat risk holistically across its operations. For example, there may be opportunities to treat multiple risks with one mitigation control.
- **Establishing a risk management framework:**
  - These are the rules governing how you will identify risks; who you assign risk ownership to; how the risks affect the confidentiality, integrity and availability of the information; and the method of calculating the estimated damage of each scenario and the likelihood of it occurring.
  - A formal risk assessment methodology needs to address four issues:
    - Baseline security criteria
    - Risk scale
    - Risk appetite
    - Methodology: scenario- or asset-based risk assessment

- **Security plan – threats, risks and vulnerabilities:**
- Identify the people, information (including ICT) and assets to be safeguarded.
- **Risk identification:** Determine specific risks (including shared risks) to its people, information and assets in Australia and abroad.
- **Criticality assessment:** identify and assess criticality of people, information and assets.
- **Threat assessment:** identify the threats to people, information and assets.
- **Vulnerability** assessment: assess the degree of susceptibility and resilience to hazards.
- **Risk analysis:** assess the likelihood and consequence of each risk occurring.
- **Risk treatments:** Implement protective security measures to mitigate or reduce identified risks to an acceptable level.

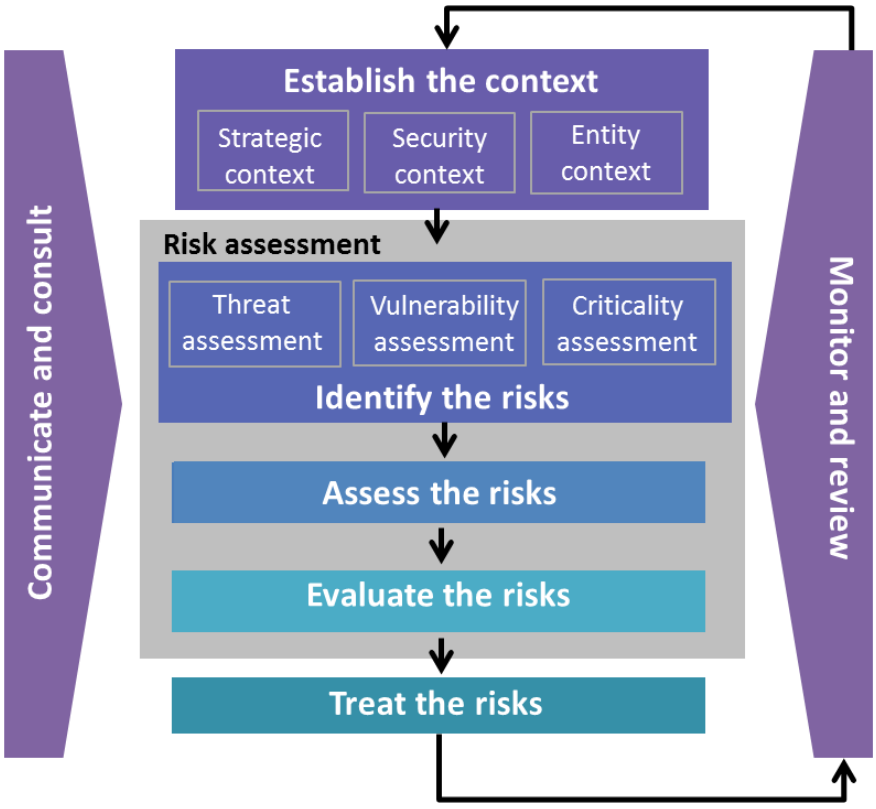


Figure 7 - Security planning. (protectivesecurity, n.d.)

- **Identify risks:**
  - Identifying risks that may affect confidentiality, integrity, and availability of information is the most time-consuming part of the risk assessment process.
  - We recommend following an asset-based approach. Developing a list of information assets is a good place to start, but if you can find an existing list, most of the work will be done for you.
- **Analyze risks:**
  - You must identify the threats and vulnerabilities that apply to each asset. For instance, if the threat is 'theft of mobile device', the vulnerability is 'a lack of formal policy for mobile devices'.
- **Evaluate risks:**
  - You need to weigh each risk against your predetermined levels of acceptable risk (i.e. your risk appetite) and determine which risks you need to address and which ones you can ignore.
- **Select risk treatment options:**
  - There are four ways you can treat a risk:
  - Avoid the risk by eliminating it entirely
  - Modify the risk by applying security controls
  - Share the risk with a third party (through insurance or by outsourcing it)
  - Retain the risk (if the risk falls within established risk acceptance criteria)

Figure 8 - Risk management. (continuingprofessionaldevelopment, n.d.)

- **Calculate Risk Rating**
  - Even though there is a ton of information and work that goes into determining your risk rating, it all comes down to a simple equation:

Impact (if exploited) * Likelihood (of exploit in the assessed control environment) = Risk Rating

  - Some examples of risk ratings are:
    - **Severe** – A significant and urgent threat to the organization exists and risk reduction remediation should be immediate.
    - **Elevated** – A viable threat to the organization exists, and risk reduction remediation should be completed in a reasonable period.
    - **Low** – Threats are normal and generally acceptable but may still have some impact to the organization. Implementing additional security enhancements may provide further defence against potential or currently unforeseen threats. (sagedatasecurity, n.d.)

Identified Threat	Impact	Likelihood	Value	Risk Calculation
Unauthorized Access (Malicious or Accidental)	High [100]	High [1.0]	100*1.0=100	Severe
Misuse of Information by Authorized Users	High [100]	Medium [.5]	100*.5=50	Elevated
Data Leakage / Unintentional Exposure of Customer Information	High [100]	Medium [.5]	100*.5=50	Elevated
Failed Processes	High [100]	Low [.1]	100*.1=10	Low (Normal)
Loss of Data	High [100]	Low [.1]	100*.1=10	Low (Normal)
Disruption of Service or Productivity	High [100]	Low [.1]	100*.1=10	Low (Normal)

Table 1 - Example Calculate risk rating

D1. Investigate how a 'trusted network' may be part of an IT security solution.

- **What is a Trusted Network?**

Someone was hired by a community college to configure a trusted network of computers and mobile devices within the campus. A trusted network is a network of devices that are connected to each other, open only to authorized users, and allows for only secure data to be transmitted.

He had recently graduated with a degree in Network Systems and Security, so he was excited to be able to put his newly acquired knowledge to good use and met with his new co-workers and team members to discuss more about this project. They decided that the trusted network should have the following features:

- **Authentication:** the network should require users to login so that only authenticated users can use the network.
- **Encryption:** the data should be encrypted so that secure data cannot be intercepted and transmitted to unauthorized users.
- **Firewall:** the computers and servers on the trusted network should include hardware like a firewall, which is a software program or piece of hardware that helps screen for security.
- **Private Network:** the computers and servers on the trusted network should be equipped with software like virtual private network (VPN), which allows for remote work with secure data transmission. (study, n.d.)

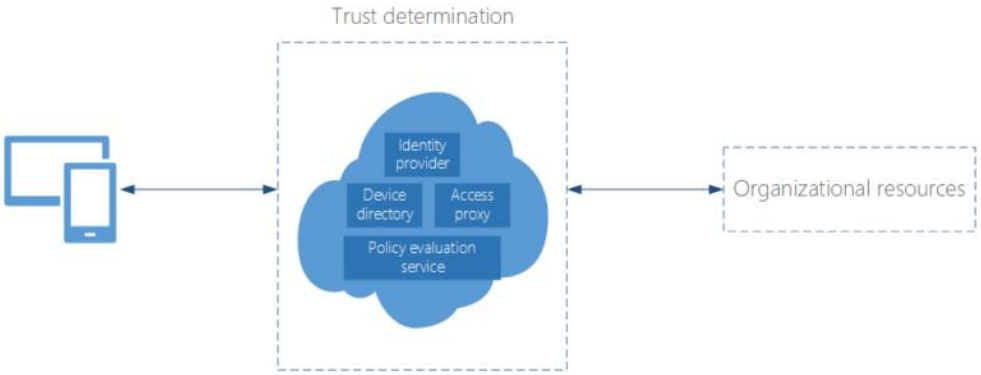


Figure 9 - Basic components of a general Zero Trust network model. (microsoft, n.d.)

- A common security policy we make every time we connect a device to a network is the "Trusted or Untrusted Network." For example, every time you take your laptop into a coffee shop and use their open Wi-Fi connection, you're prompted to define the network zone to which you are connected: home, work or public. Depending on what's selected, the appropriate security settings are enabled.
- In the context of VoIP and IP networking, trusted and untrusted zones are defined by where the security control devices are located. Firewalls are typically used as an IP network control point and SBCs are used as VoIP control points.
- It is important to place an SBC between trusted and untrusted IP networks to provide security policies and ensure that each network does not have a direct connection. The Internet is the most untrusted IP network, and carrier private WAN IP networks are also outside the security of the enterprise trusted LAN network.

➢ **On-premises web applications:**

- Employees today want to be productive anywhere, any time, and from any device. They want to work on their own devices, whether they be tablets, phones, or laptops. And they expect to be able to access their corporate on-premises applications. Azure AD Application Proxy allows remote access to external applications as a service, enabling conditional access from managed or unmanaged devices.
- Surely Money has built their own version of a code-signing application, which is a legacy tenant application. It turns out that the user of the compromised device belongs to the code-signing team. The requests to the on-premises legacy application are routed through the Azure AD Application Proxy. The attacker tries to make use of the compromised user credentials to access this application, but conditional access foils this attempt.
- Without conditional access, the attacker would be able to create any malicious application he wants, code-sign it, and deploy it through Intune. These apps would then be pushed to every device enrolled in Intune, and the hacker would be able to gain an unprecedented amount of sensitive information. Attacks like these have been observed before, and it is in an enterprise's best interests to prevent this from happening.

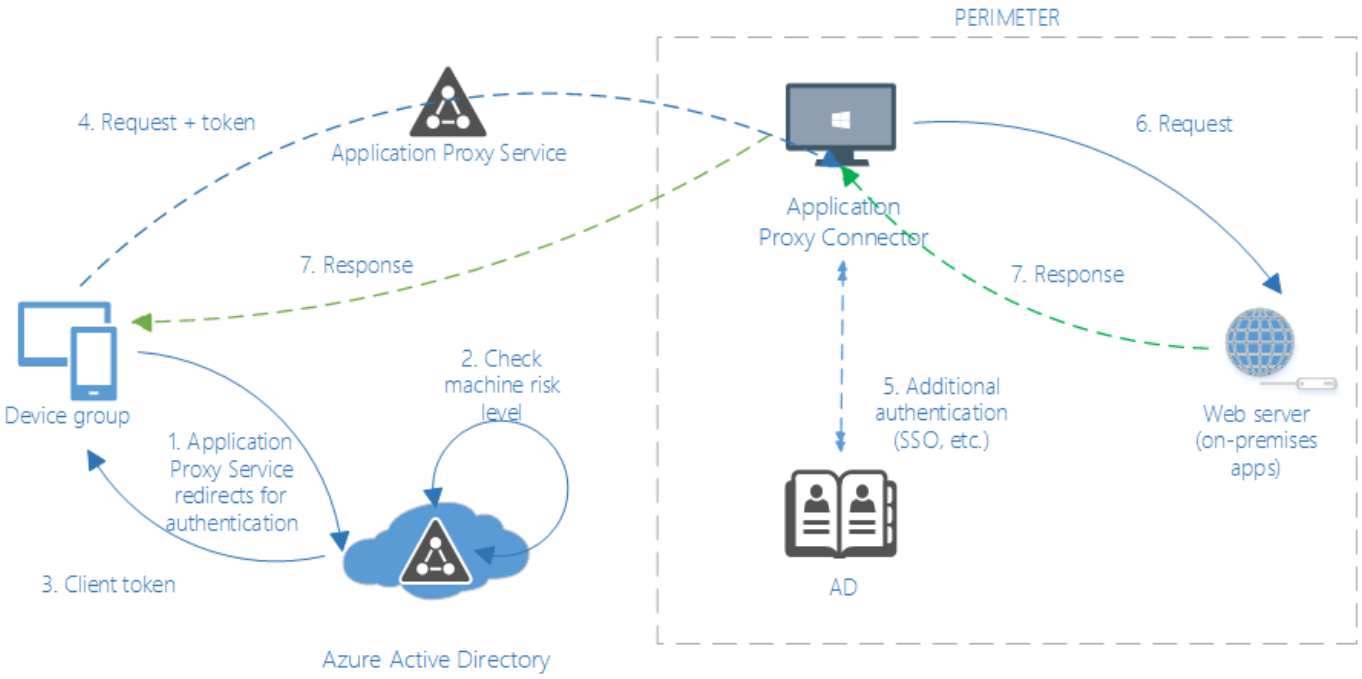


Figure 10 - Zero Trust network model for on-premises web applications. (Sumesh Kumar, n.d.)

- **Trusted Network connect (TNC):**
  - The name of a subgroup of the trusted computing group (TCG).
  - An open network access control architecture.
  - An open network access control standard.
  - Ensures interoperability.
  - From the Trusted Computing Group (TCG).

- **Firewall:**
  - Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both.

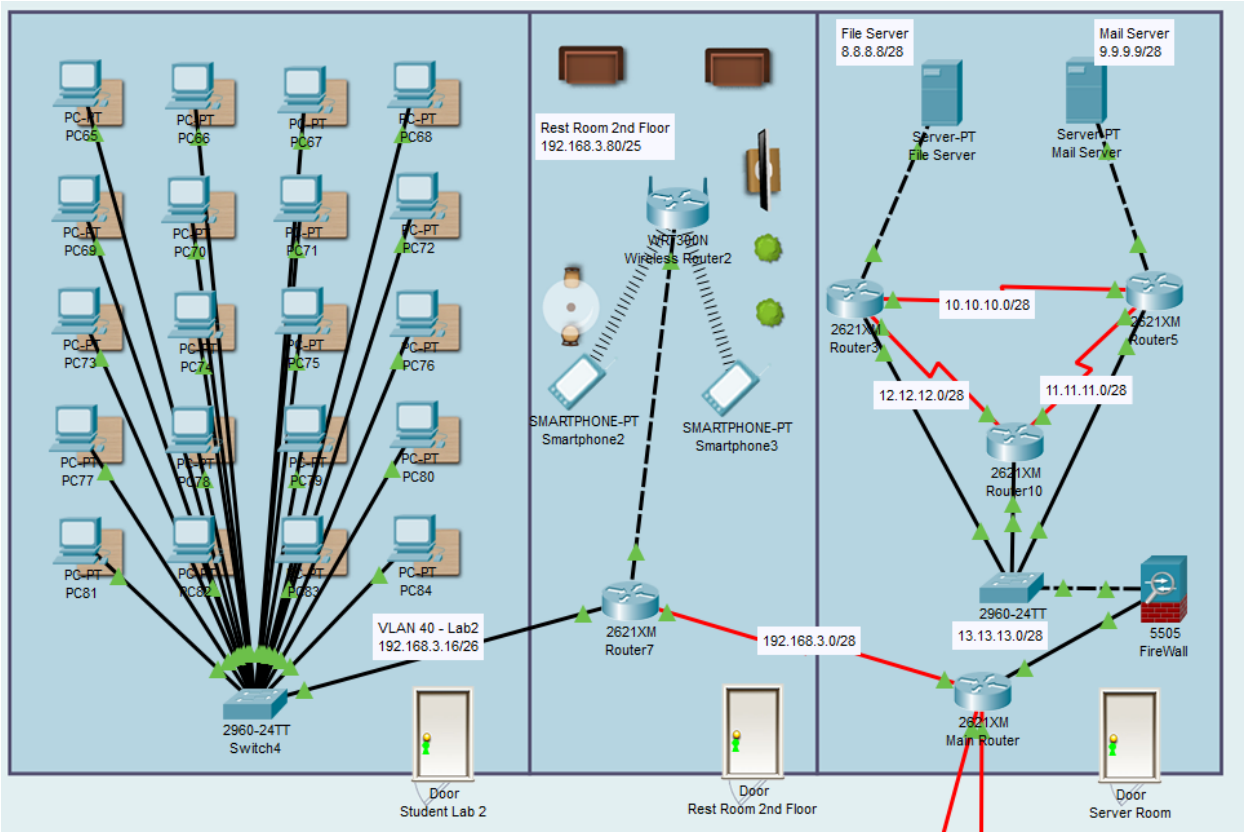


Figure 11 - Using firewall to protect DMZ

- **IP Unreachable, Redirects, and Mask Replies:**
  - The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages under a wide variety of conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: 'Host unreachable', 'Redirect', and 'Mask Reply'. Automatic generation of these messages it is important to be disabled on all interfaces, especially interfaces that are connected to untrusted networks.

- **Using NAT:**
  - A router can hide the structure of the trusted network, by transparently translating all IP addresses and coalescing distinct IP addresses into one. (researchgate, n.d.)

```
ip nat pool net-208 172.31.233.208 172.31.233.233 netmask 255.255.255.240
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool net-208 overload
interface gigabitethernet 1/1/1
 ip address 192.168.201.1 255.255.255.240
 ip nat inside
!
interface gigabitethernet 0/0/0
 ip address 192.168.201.29 255.255.255.240
 ip nat outside
!
```

Figure 12 - Example using NAT to Allow Internal Users Access to the Internet

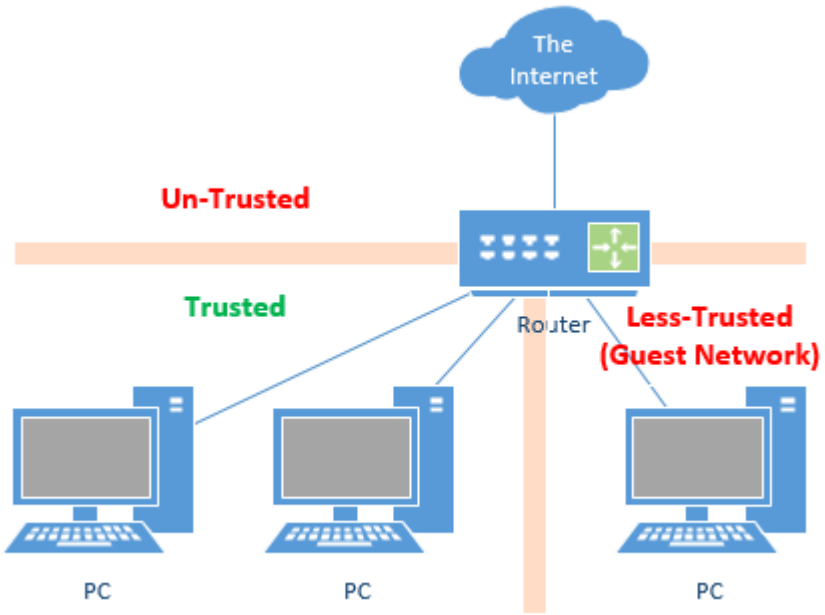


Figure 13 - Example model of Trusted – Un-Trusted network

LO2. Describe IT security solutions

P3. Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs.

- **What is VPN?**
  - A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g. a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common though not an inherent part of a VPN connection. (wikipedia, n.d.)

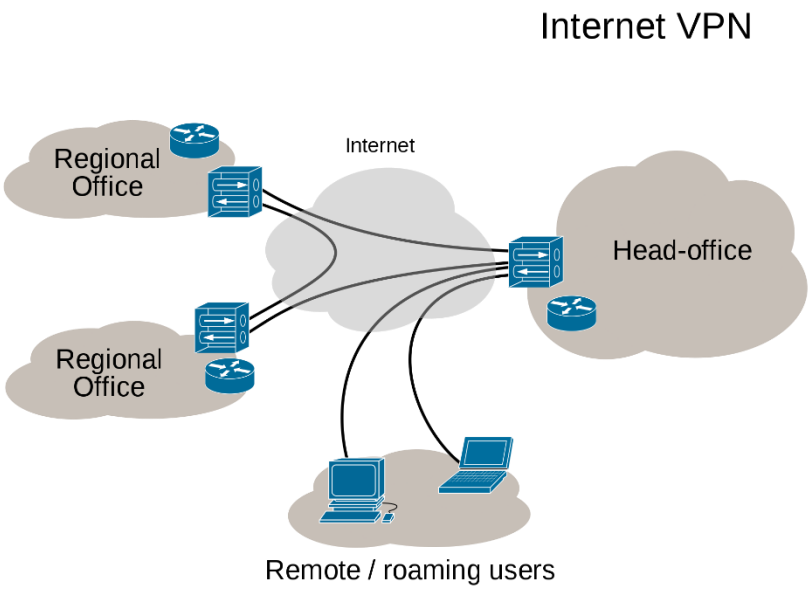


Figure 14 - VPN connectivity overview

- When you use a VPN service, your data is encrypted (because you're using their app), goes in encrypted form to your ISP then to the VPN server. The VPN server is the third party that connects to the web on your behalf. This solves the privacy and security problem for us in a couple of ways:
  - The destination site sees the VPN server as the traffic origin, not you.
  - No one can (easily) identify you or your computer as the source of the data, nor what you're doing (what websites you're visiting, what data you're transferring, etc.).
  - Your data is encrypted, so even if someone does look at what you're sending, they only see encrypted information and not raw data.
- **How Secure is a VPN?**
  - VPN security causes debate among IT pros and others in the industry, and no two services are identical in their offerings or security. There are two main factors:
    - The limitations of the type of VPN technology used by a provider.
    - Legal and policy limitations affecting what can be done with that technology. The laws of the country where the server and the company providing the VPN are located and the company's own policies affect how the company implements this technology in their service.
- **How to configure VPN?**
  - Download the openvpn server package and install

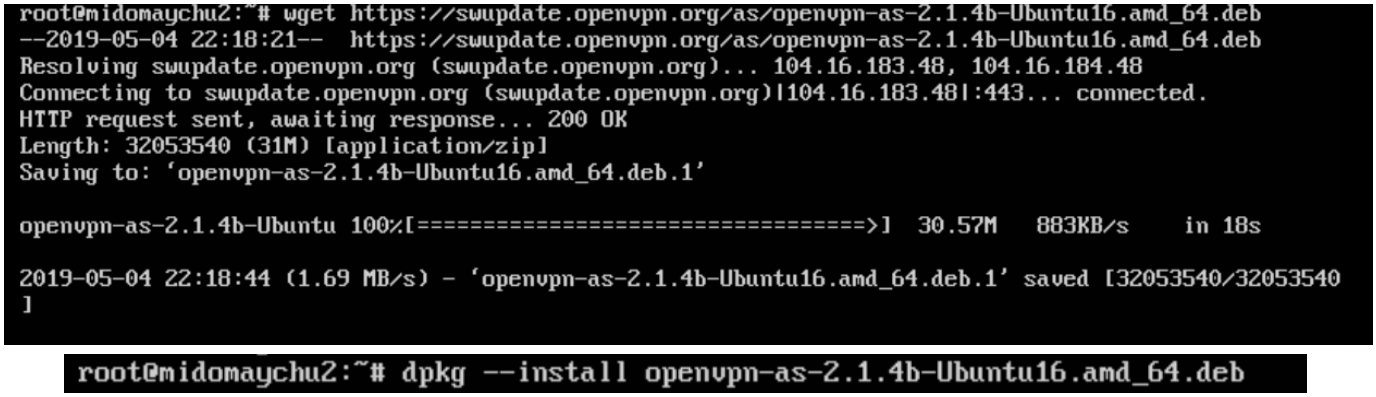


Figure 15 - Download and install VPN

- **Configuration VPN**
  - Server Network Settings: If we change the Hostname, Protocol or Port Number after VPN clients are deployed will cause the existing clients to be unusable (until a new client configuration or VPN installer is downloaded from the Client Web Server). If we "listen on all interfaces" that will make danger to our Server because the attacker is easy to connect to VPN.

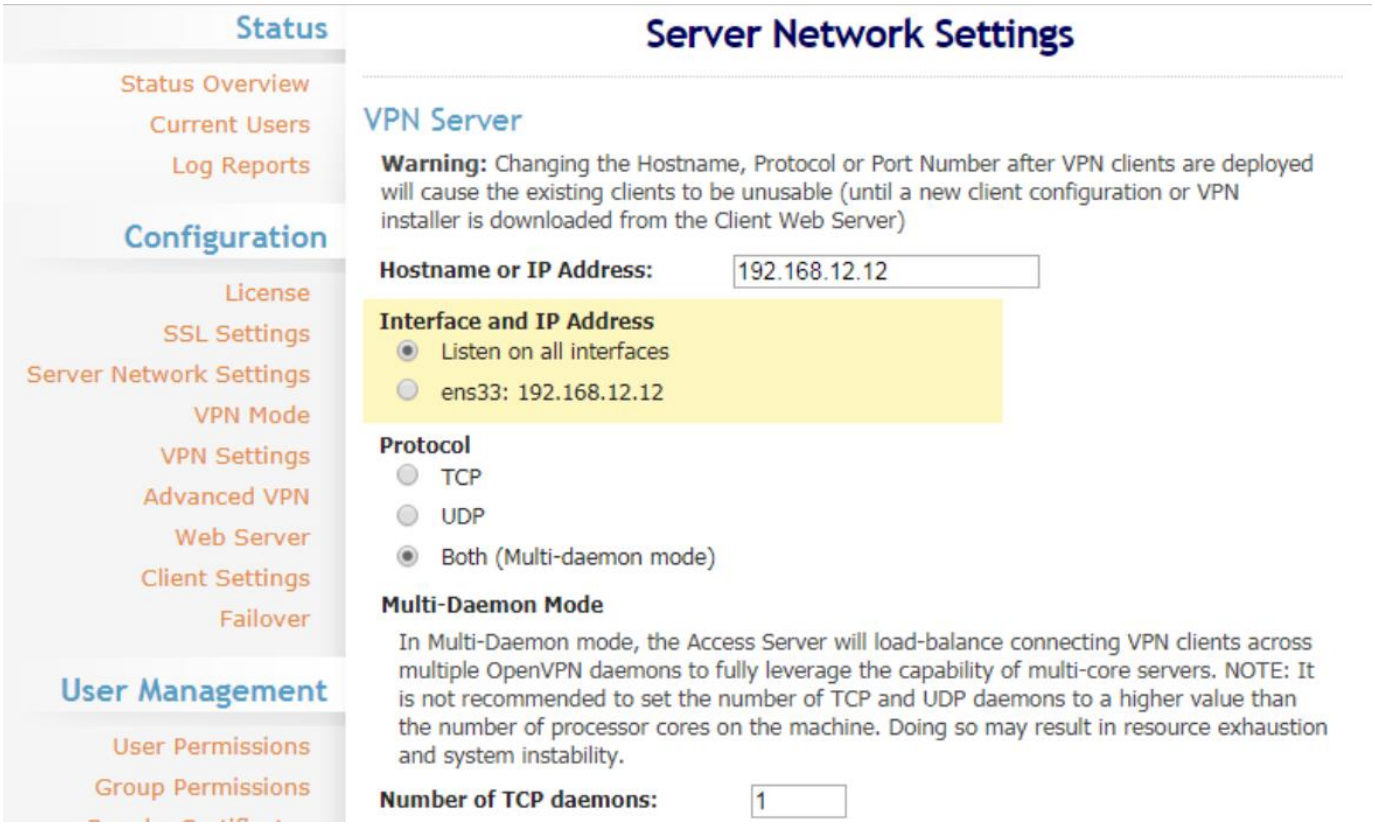


Figure 16 - Server Network Settings

- Routing: NAT is preferred for client access to private networks. Routing may be useful for applications that do not traverse NAT. When we use NAT on VPN, it will make the system more security.

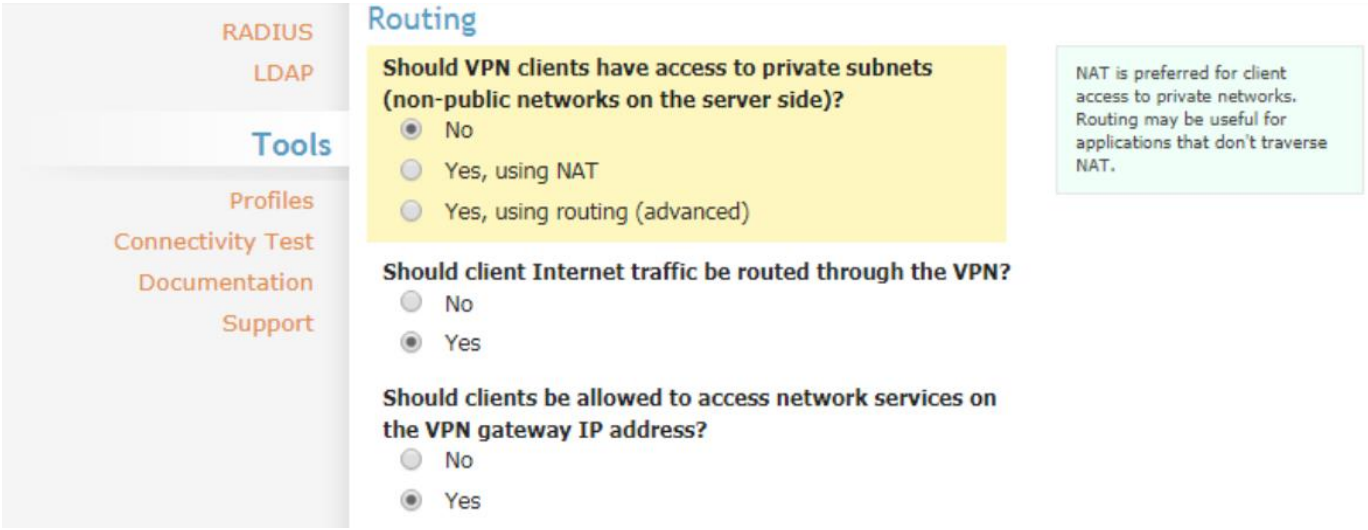


Figure 17 - Routing VPN

- Customize Client Web Server UI: We can control the visibility of link provided to Client Web Server users. When we configure this will make sure that users can connect to VPN through specific operating system.

Figure 18 - Customize Client Web Server UI

- Inter-Client Communication: This feature allows or prevents packet routing between clients on the VPN IP Network. If someone connect to VPN allow/not allow to communicate another device, so this will make the system more security or easy attacked.

➢ **Incorrect configuration:**

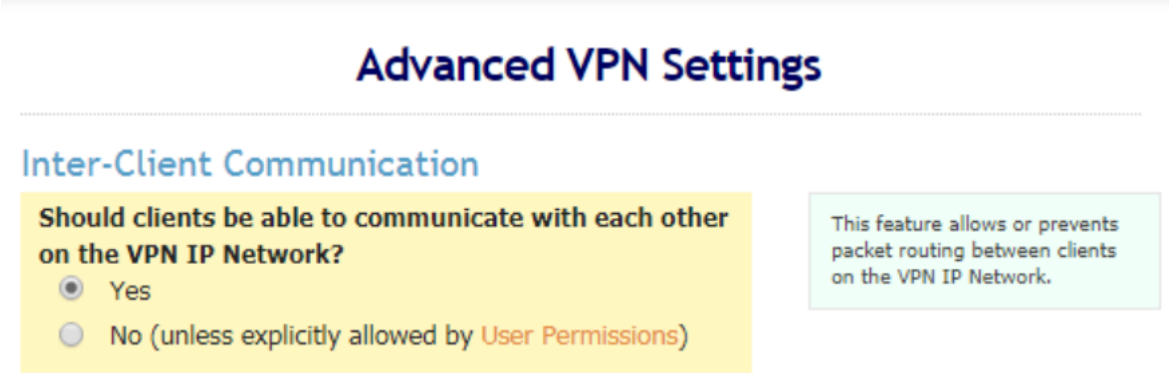


Figure 19 - Inter-Client Communication

Firewall policies:

- Non-standard authentication mechanisms will be got the impact of failure firewall. Remote Control Gone Wrong so Traffic doesn't reach it's intended destination; it will likely be noticed fairy quickly when process don't work as expected.
- Configuration mistakes:
  - It was blocked.
  - Get wrong rare limiting, too much or too little network traffic passed the firewall.
  - Broad policy configurations.
  - It was routed to the wrong destination.
  - It could not be routed at all.
- Undesirable traffic reaches a destination it should not. Get Risky rogue services, management services and false sense of security it could generate, making it more troubleshooting other part of system with more difficult. On bad standards/ instructions/ policy.

- Dangerous with ports open (Get error possible this could cause some negative consequence by accident), it's also a possible good attack vector for individuals with malicious intent (The cyber threat).

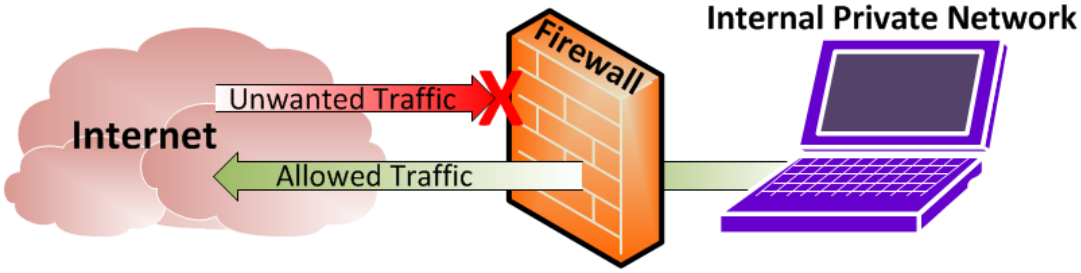


Figure 20 - Firewall policies

Problems of misconfiguration VPN:

- Learning how to set up VPNs correctly in an organization will avoid complications later. Here are some VPN issues and related technical problems:
  - VPN client software must work on all user devices, such as PCs, laptops, tablets and smartphones; this will help your company avoid a VPN security breach.
  - VPN protocols must work end-to-end through firewalls, routers and switches.
  - Must pick VPN devices that are compatible and interoperable with concentrators, appliances and servers.
  - Balance security and protection against ease and convenience of using your chosen VPN to avoid technical VPN issues.
  - They Compromise about your Security, privacy No. more encryption. They Track Your Online Activity, They Limit the Amount of Data You Can Use
  - Slow Down your Internet, They Bombard You with Ads, They Sell Your Bandwidth
  - Using your computer for their options you don't know.

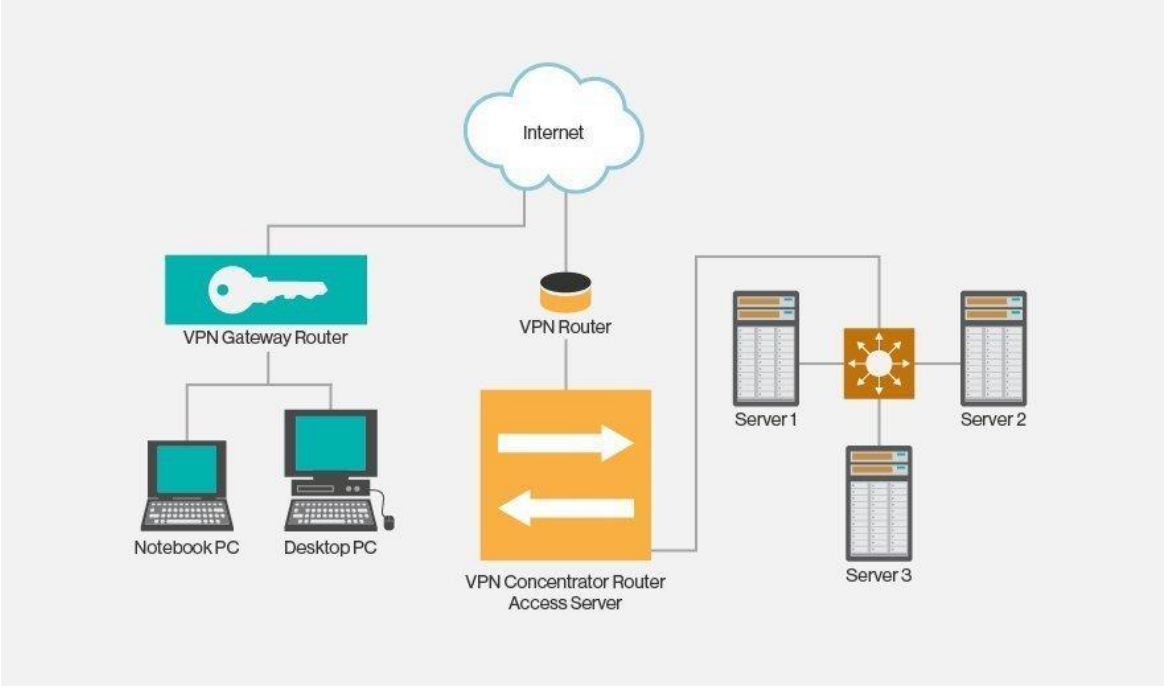


Figure 21 - Configuration VPN

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

- **Implement DMZ:**
  - The simplest way to implement a DMZ is to have a single firewall server with three NIC cards, each connected to the internal, external and DMZ networks. This is the cheapest option but has limited fault tolerance with a single point of failure. It can also be difficult to ensure that no traffic can bypass the DMZ.

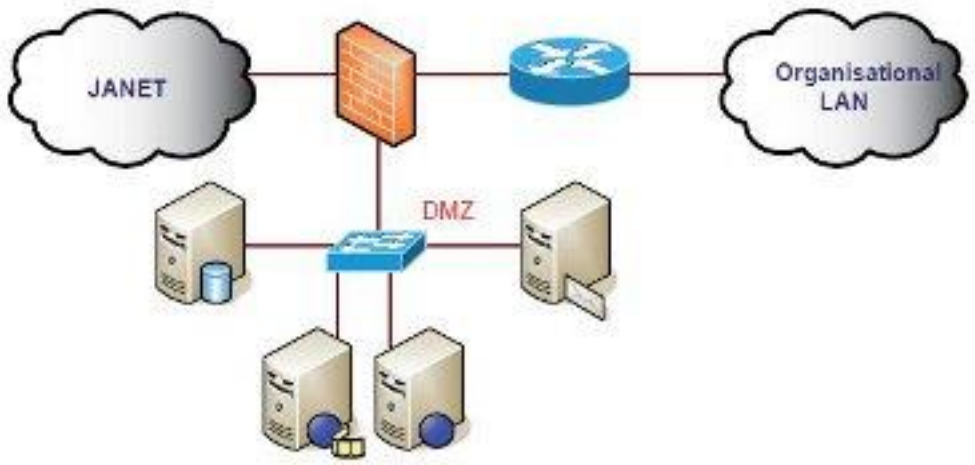


Figure 23 - Implement DMZ

  - In this configuration the DMZ sit between the internal and external networks. The two firewalls can use screening router to force all traffic to flow through the DMZ and thus prevent direct flow between the internal and external networks. It will be more expensive to implement but provides much better levels of security.
  - DMZ stands for demilitarized zone as a network segment that is part of a local network and separate from another secure network segment. Devices included in the DMZ can be mail servers, web servers or databases. It applies to the office network or corporate network to ensure that the entire won network has been affected by any external threats or any dangers.
  - Assume that we have the network below that has servers and workstations connected to the same router.

- Any external malicious requests going through the security layer of the intranet will invade the server and the database. Because all devices connect to the same network, harmful packets can go through all devices causing services and the entire office to stop working.

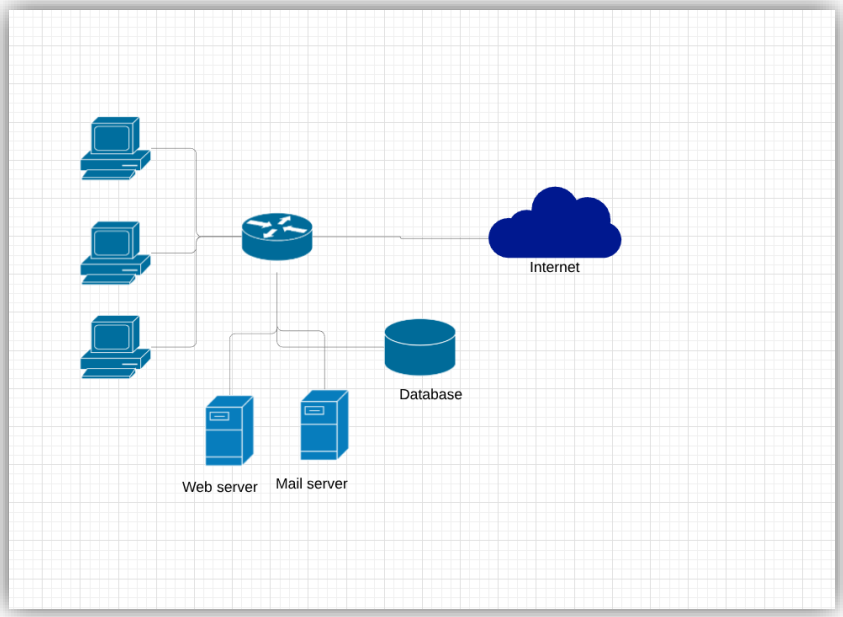


Figure 25 - A network not implement DMZ security 1

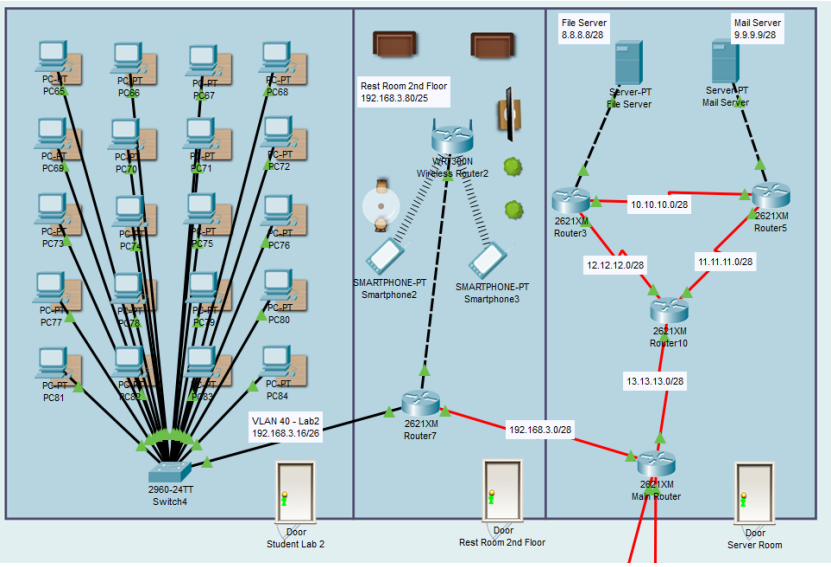


Figure 24 - A Network not implement DMZ security 2

- Therefore, we need to put the servers and office computers on the different network segments which helps to reduce the harms from the outside.

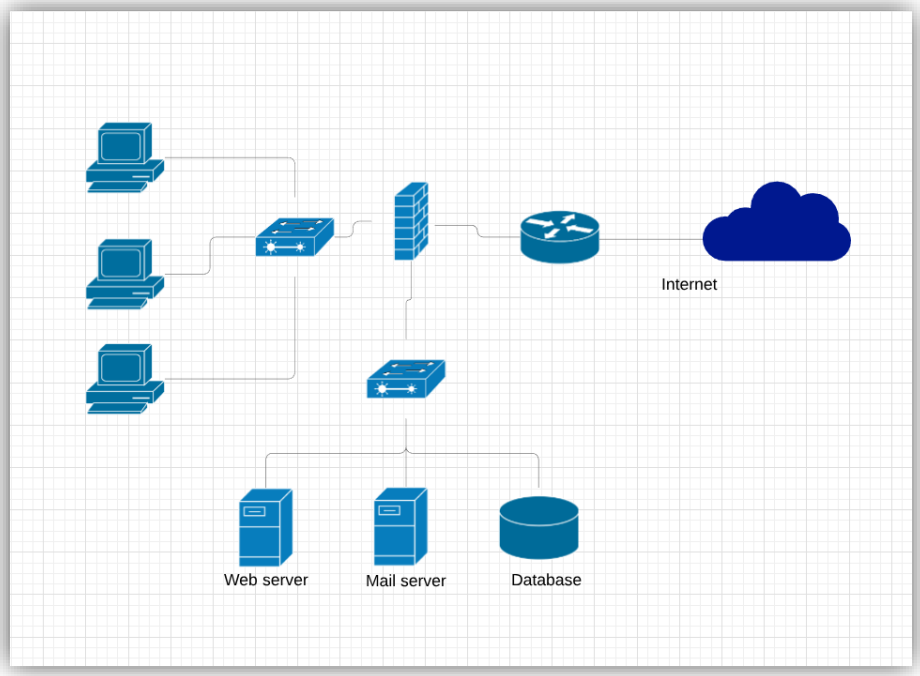


Figure 26 - A network has implemented DMZ security

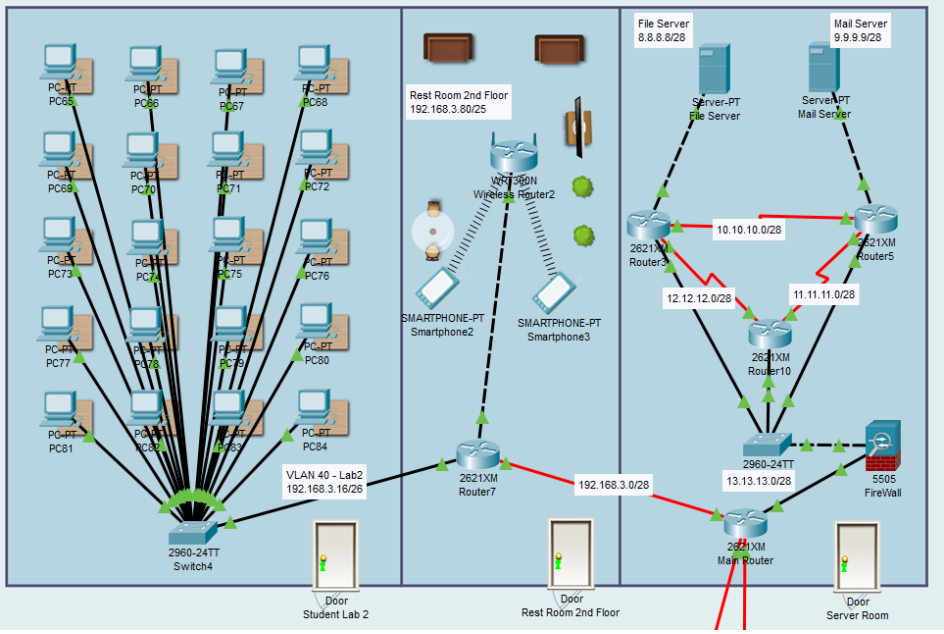


Figure 27 - A network has implemented DMZ security 2

- Now all the traffic from the outside of the network will only reach the servers in that internal network. We also put the firewall as an intersection of the network traffic to filter all the unnecessary or unauthorized requests that might be harmful to the network. When it comes with public access, many companies may need to open their servers to the internet in order to provide the services needed by the public but also make sure that other parts of the networks are secure and inaccessible from outside requests. Therefore, the area in the figure above that contains Web server, mail server and database are called the demilitarized zone.
- There is also an additional approach to increase the security for the network by using double firewalls which have the DMZ put between them.

➢ **The NAT which stands for Network address translation and static IP configuration can help to improve network security.**

- NAT (Network Address Translation) is a process of changing the source and destination IP addresses and ports. Address translation reduces the need for IPv4 public addresses and hides private network address ranges. The process is usually done by routers or firewalls. There are three types of address translation:
    - **Static NAT** – translates one private IP address to a public one. The public IP address is always the same.
    - **Dynamic NAT** – private IP addresses are mapped to the pool of public IP addresses.
    - **Port Address Translation (PAT)** – one public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.

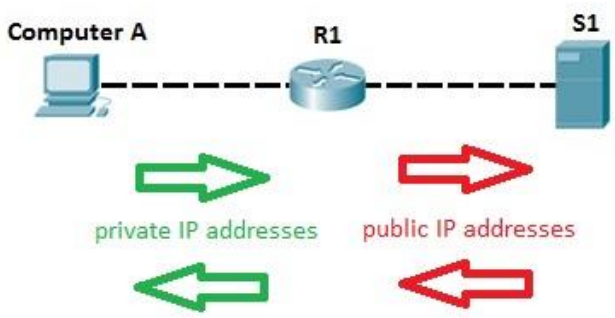


Figure 26 - Example NAT concept

- **Configure NAT on Router**: Computer A requests a web resource from S1. Computer A uses its private IP address when sending the request to router R1. Router R1 receives the request, changes the private IP address to the public one and sends the request to S1. S1 responds to R1. R1 receives the response, looks up in its NAT table and changes the destination IP address to the private IP address of Computer A.

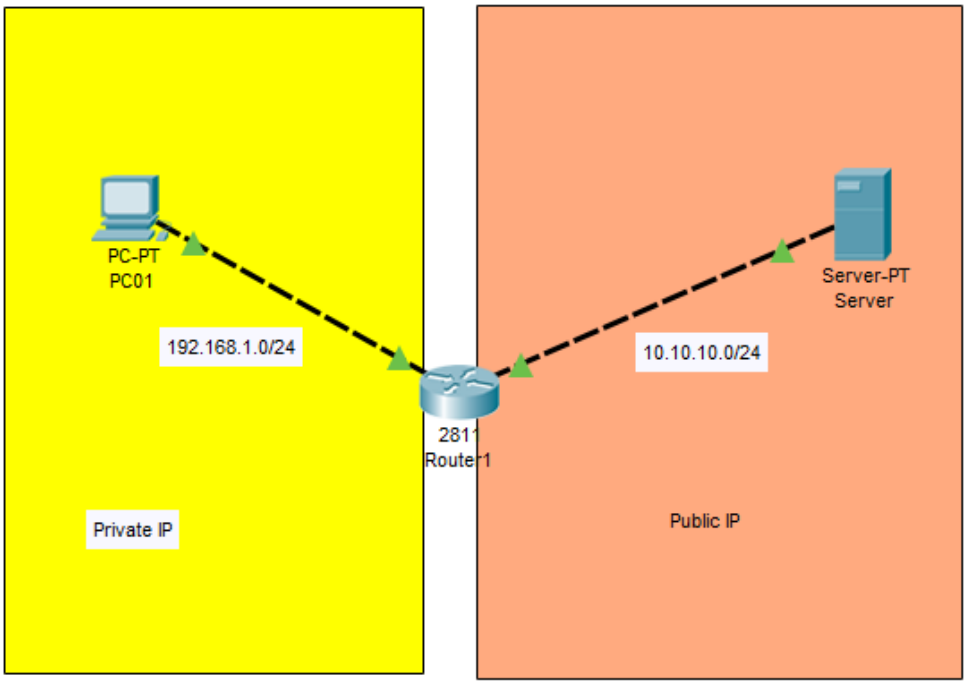


Figure 27 - Example to configure Nat on Router

- Configure static NAT:

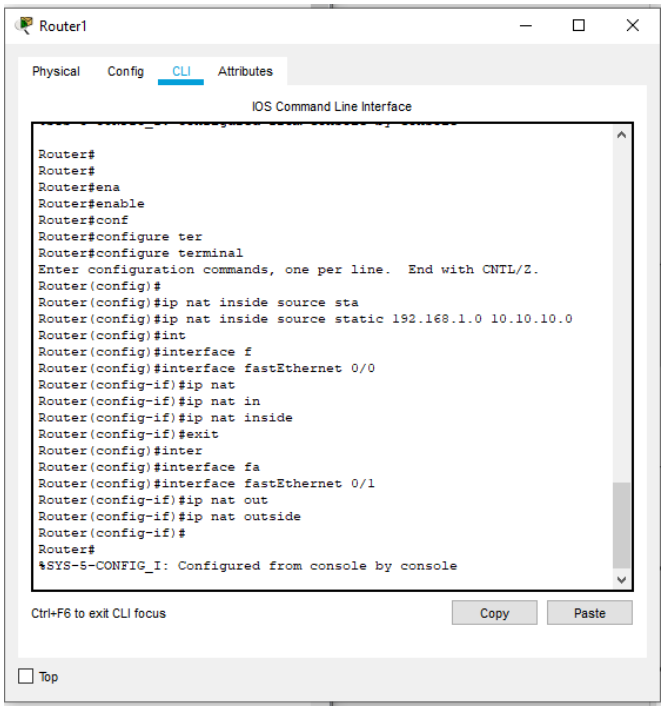


Figure 28 - Configure static NAT

- Check NAT:

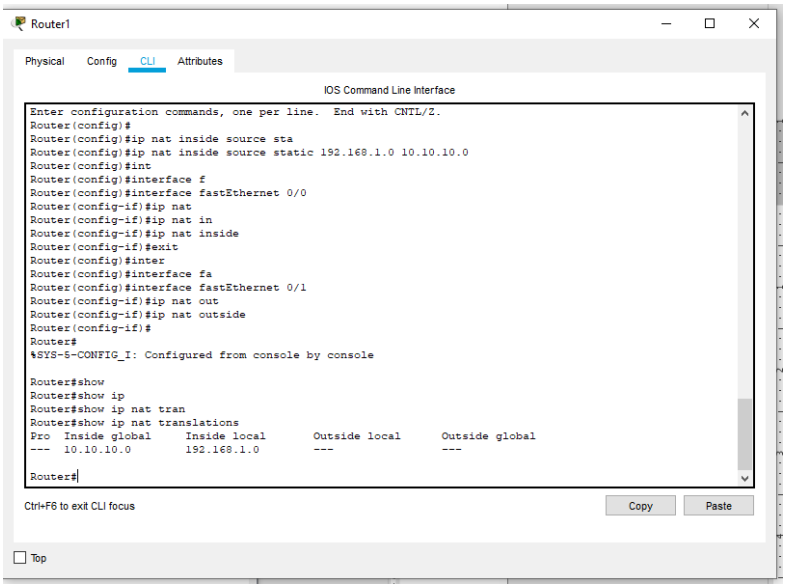


Figure 29 - Check NAT

- The NAT which is a method of converting a public IP address to the private or local IP address. The main purpose of using NAT is due to its reusable feature that help to avoid the lack of IP addresses so that whenever a device connects to the network, it gets a unique IP address. Even though all the devices in that network have different IP addresses and they just need a public IP address to access the Internet.

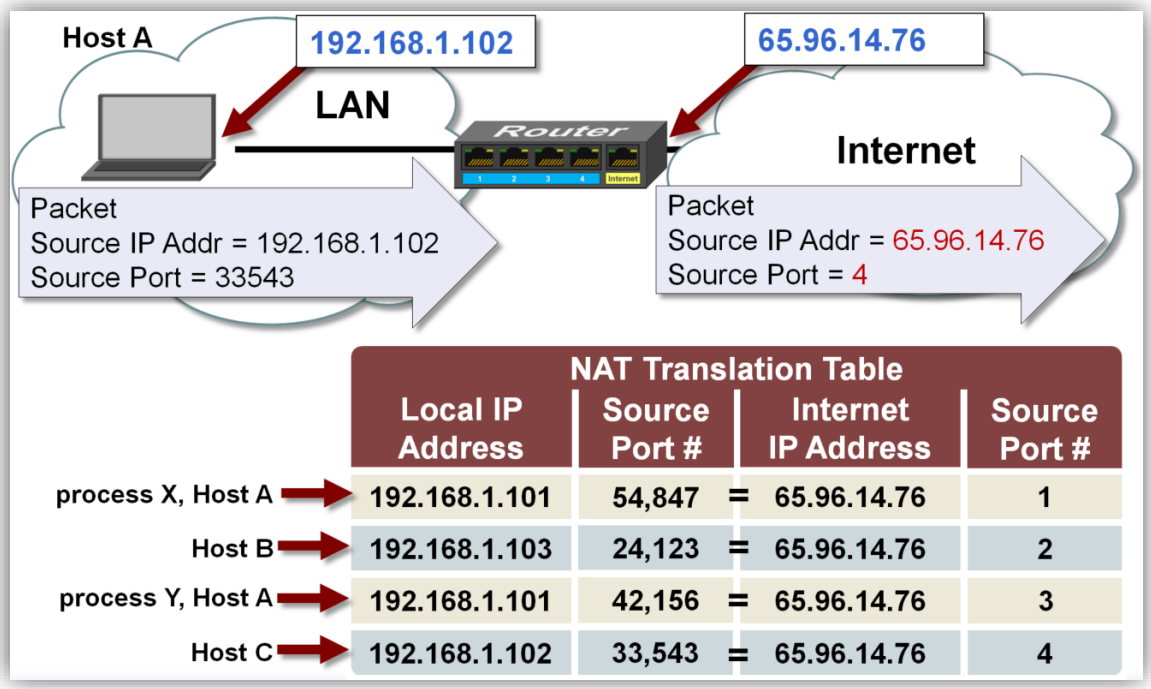


Figure 30 - Use NAT to help improve network security

- All the local IP address will use a single IP address to get out of the internal network. By using NAT, all packets going through the router will have their IP address converted to the same IP. If any of the device in the internal network try to connect to a remote network or device, it cannot detect the actual IP address of that device which is the sender because all the devices in the LAN use the same public IP address. Therefore, someone with malicious intents like hackers will have a hard time to get which device the packet come from because all hacker can see is the public IP provided by the Internet Service Provider not the private IP address provided by the DHCP server.

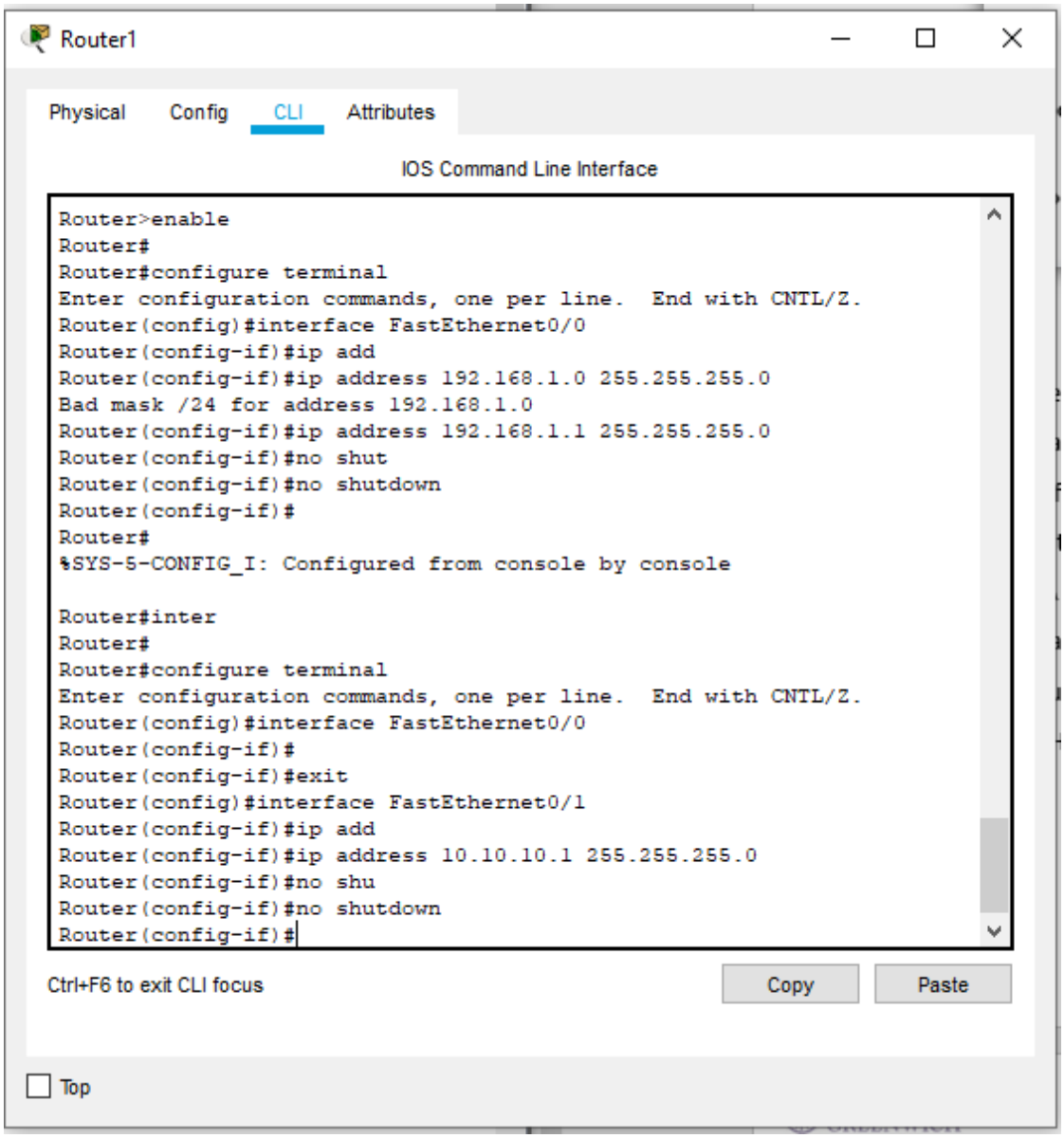
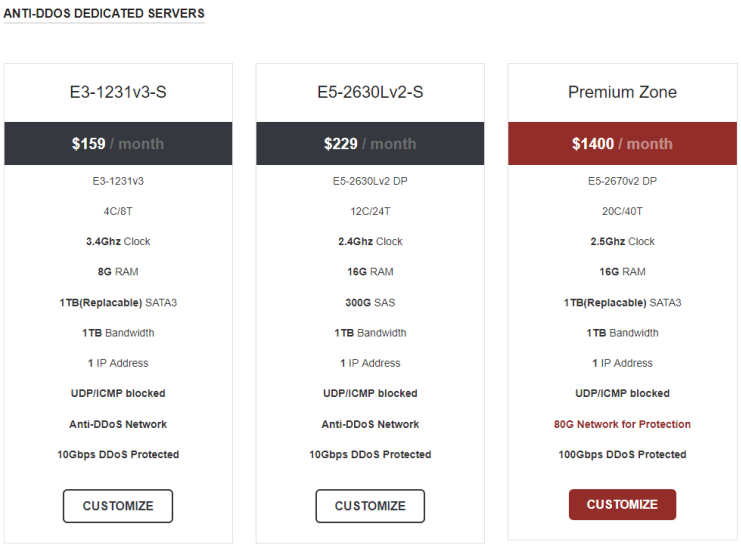
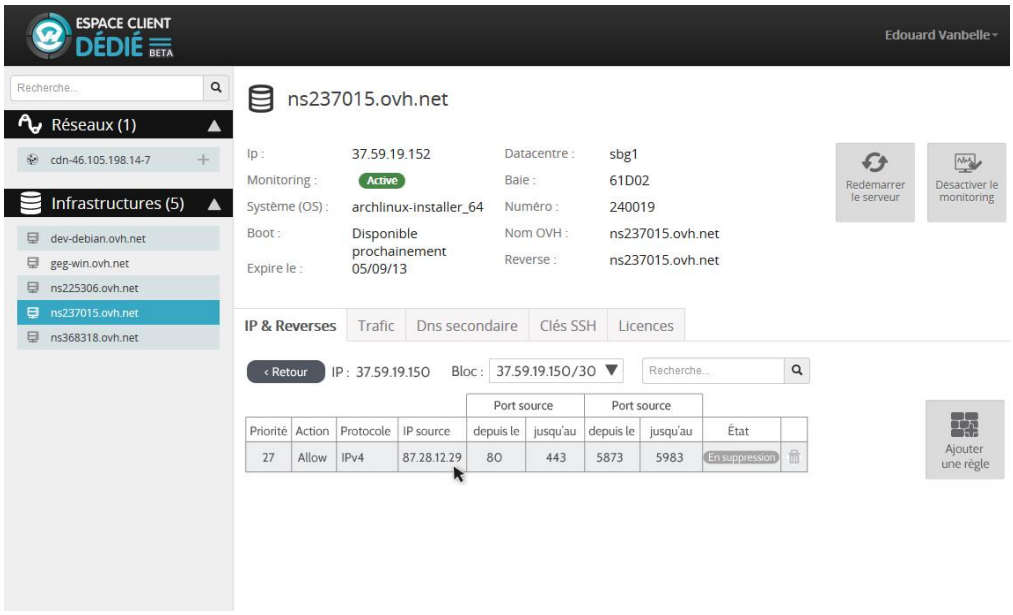


Figure 31 - Static IP to help improve network security

➢ **Use anti-DDos dedicated servers:**

- Your servers are placed in a redundant DoS/DDoS Protected network with multiple 10GE carriers providing the best connectivity with East Asia.
- A DoS/DDoS Attack is mitigated nearly instantly, avoiding downtimes and side effects related with it.
- Quality is an important factor; our engineering team is always available for you.
- All kinds of DDoS attacks are mitigated into our systems and only the good traffic can pass.
- We aren't resellers like the competition, we develop our mitigation technology daily, improving it day-by-day to become the most up to date and quality DDoS Protection available.
- You will be protected against any kind of DDoS Attack, being TCP, UDP, CC Attack and so on.





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

- **What is network monitoring?**
  - Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble. Network monitoring is part of network management. (wikipedia, n.d.)
- **How can Network Monitor help you?**
  - What is going on in your network.
  - What device or type of flow is the cause of the delay?
  - Why an application failed.
- **Benefits of network monitoring:**
  - Identify security threat:
    - The prevention of Cybercrime is a major challenge for any organization. As attacks become increasingly more sophisticated and difficult to trace, detecting and mitigating any form of network threat before it escalates is critical.
    - A network monitoring tool can provide that first level of security. The biggest benefit you get is make it easy to spot anything out of the ordinary or a strange device connected to your network. You can know what the most stranger device intrusion into your network and who is that device.
  - Fix issues faster:
    - In a bad situation, time is money. Network monitoring makes problem-solving easier and faster for time-strapped network professionals.
    - If you have a lot problem, network monitoring software helps you get to the bottom of issues once and for all. Monitoring software will help you know the source of problems and handle it.

- Stay ahead of outages:
  - Implementing network monitoring is one of the most basic and simple ways to prevent these outages from happening in the first place.
  - Network monitoring will help you know potential issues by showing live network performance data in easy-to-read interface, network monitoring software helps you identify outages that could cause bottlenecks.

➢ **Some Network Monitoring Tools & Software:**

- **Solarwinds Network Performance Monitor:**

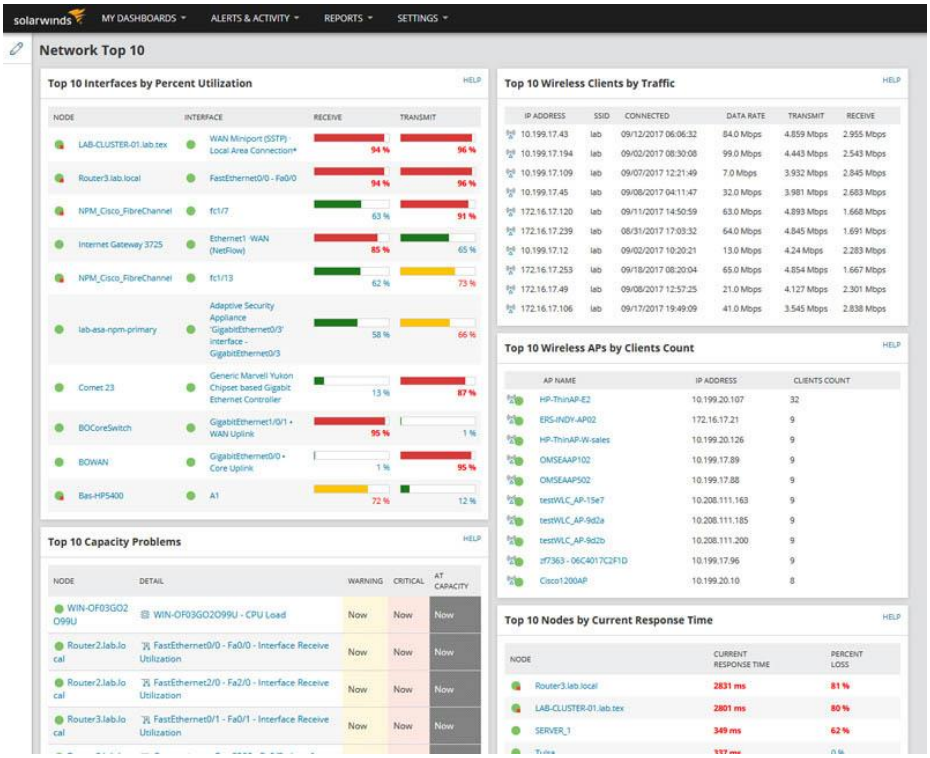


Figure 32 - Example of Solarwinds

- SolarWinds Network Performance Monitor is easy to setup and can be ready in no time. The tool automatically discovers network devices and deploys within an hour. Its simple approach to oversee an entire network makes it one of the easiest to use and most intuitive user interfaces.

- The product is highly customizable and the interface is easy to manage and change very quickly. You can customize the web-based performance dashboards, charts, and views. You can design a tailored topology for your entire network infrastructure. You can also create customized dependency-aware intelligent alerts and much more.

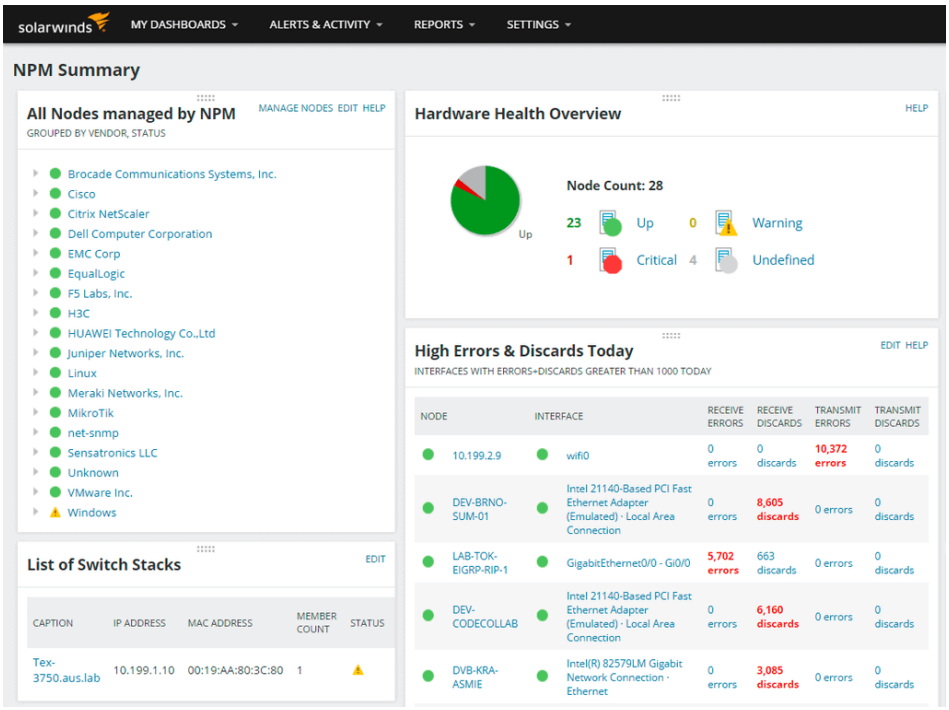


Figure 33 - Solarwinds summary

- Solarwinds NPM has an Extensive Feature:
  - Automatically Network Discovery and Scanning for Wired and Wifi Computers and Devices
  - Support for Wide Array of OEM Vendors
  - Forecast and Capacity Planning
  - Quickly Pinpoint Issues with Network Performance with NetPath™ Critical Path visualization feature
  - Easy to Use Performance Dashboard to Analyze Critical Data points and paths across your network
  - Robust Alerting System with options for Simple/Complex Triggers
  - Monitor CISCO ASA networks with their New Network Insight™ for CISCO ASA.

- Monitor ACL's, VPN, Interface and Monitor on your Cisco ASA
- Monitor Firewall rules through Firewall Rules Browser
- Hop by Hop Analysis of Critical Network Paths and Components
- Automatically Discover Networks and Map them along with Topology Views
- Manage, Monitor and Analyze Wi-Fi Networks within the Dashboard
- Create HeatMaps of Wi-Fi Networks to pin-point Wi-Fi Dead Spots
- Monitor Hardware Health of all Servers, Firewalls, Routers, Switches, Desktops, laptops and more.
- Real-Time Network and Netflow Monitoring for Critical Network Components and Devices.

- **Microsoft network monitor:**
  - Microsoft Network Monitor is a deprecated packet analyzer. It enables capturing, viewing, and analyzing network data and deciphering network protocols. It can be used to troubleshoot network problems and applications on the network. Microsoft Network Monitor 1.0 (codenamed Bloodhound) was originally designed and developed by Raymond Patch, a transport protocol and network adapter device driver engineer on the Microsoft LAN Manager development team.
  - Network Monitor has been replaced by **Microsoft Message Analyzer**. (wikipedia, n.d.)

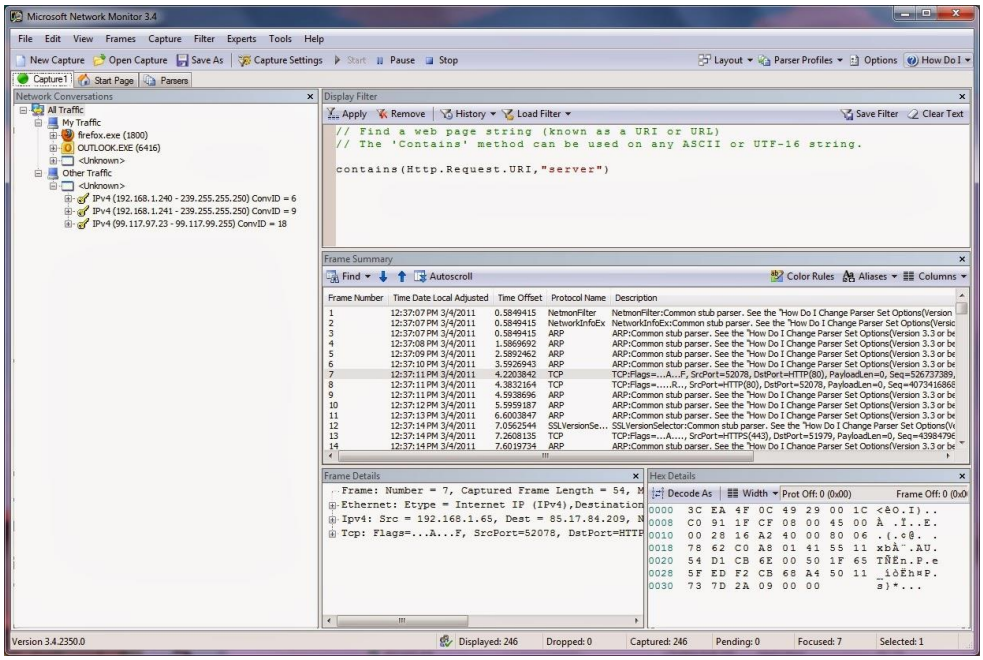


Figure 34 - Example Microsoft network monitor

LO3. Review mechanisms to control organizational IT security

P5. Discuss risk assessment procedures.

- **What is risk assessment procedures?**
  - Obtain an understanding of the client, including internal control.
  - Identify and assess risks of material misstatement of the financial statements.
  - Evaluate both overall risks and risks that affect only specific assertions.
- **Planning and Risk Assessment procedures:**

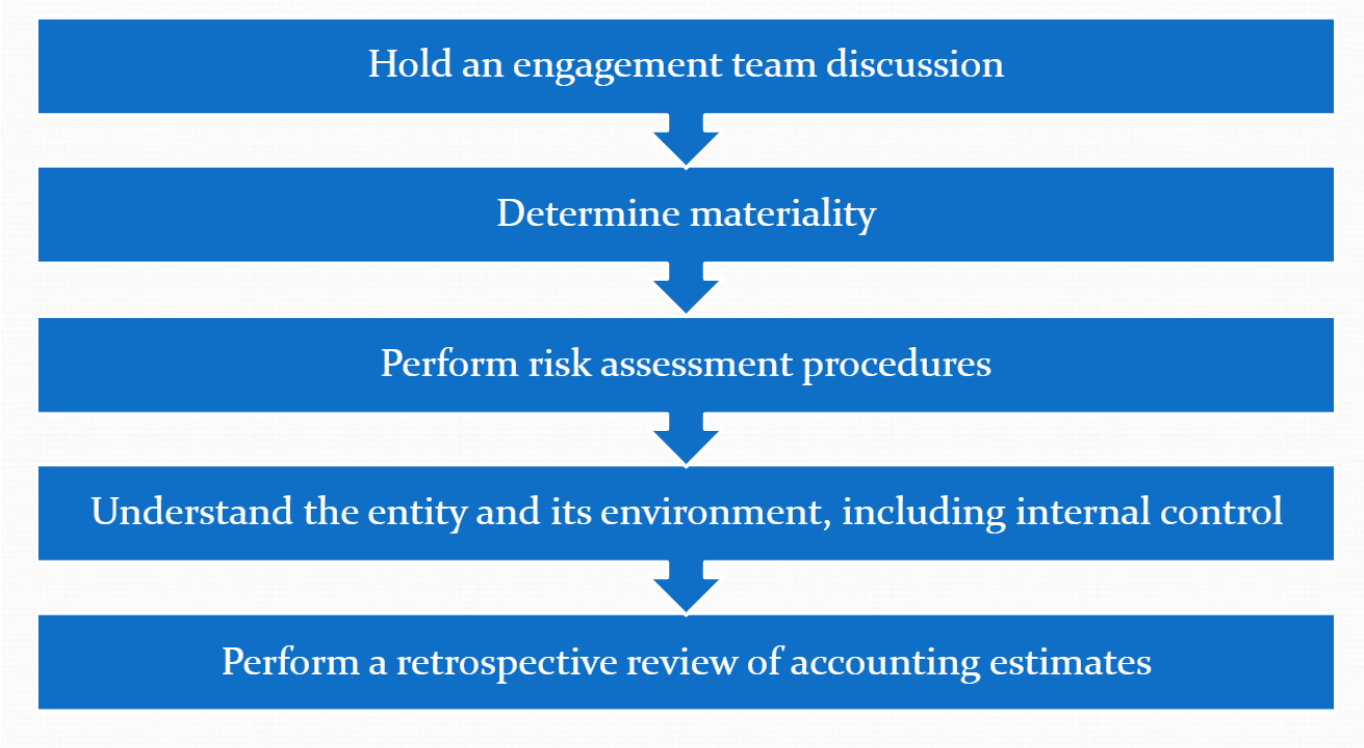


Figure 35 - Planning and Risk Assessment procedures

- Engagement team discussion:
  - Discuss the susceptibility of the financial statements to material misstatement.
  - Consider fraud risks and risks of error.
  - Include:
    - Critical issues and areas of significant audit risk
    - Unusual accounting practices
    - Important control systems
    - Materiality considerations
    - Business risks
    - Fraud considerations
- Materiality:
  - Materiality for the financial statements as a whole.
  - Materiality for items of lesser amounts.
  - Performance materiality.
  - Consider decisions that users make
  - Use appropriate benchmarks, such as percent of assets or revenue.
- Risk assessment procedures
  - Two categories of audit procedures:
    - Risk assessment procedures.
    - Further audit procedures.

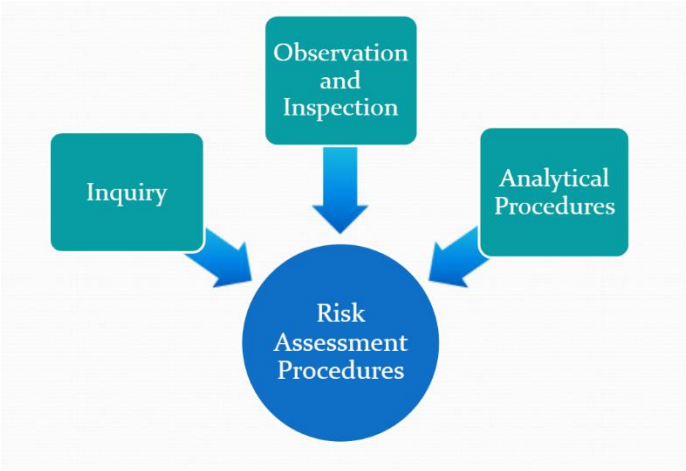


Figure 36 - Risk assessment procedures

- Performed to obtain an understanding of the entity and its environment, including internal control, for the purpose of assessing risks.
- All the procedures should be performed.
- Inquiry alone is not enough to understand internal control.

➢ **The Security Policy Cycle**

- First part of the cycle is risk identification.
- Risk identification seeks to determine the risks that an organization faces against its information assets.
- That information becomes the basis of developing a security policy.
- A security policy is a document or series of documents that clearly defines the defence mechanisms an organization will employ to keep information secure.

➢ **Risk analysis**

- Involves the four steps:
  - Inventory the assets.
  - Determine what threats exist against the assets and by which threat agents.
  - Investigate whether vulnerabilities exist that can be exploited.
  - Decide what to do about the risks.

➢ **Asset Identification**

- An asset is any item with a positive economic value.
- Many types of assets, classified as follows:
  - Physical assets – Data
  - Software – Hardware
  - Personnel
- Along with the assets, attributes of the assets need to be compiled.
- After an inventory of assets has been created and their attributes identified, the next step is to determine each item's relative value.
- Factors to be considered in determining the relative value are listed on pages 386 and 387 of the text.

- **Threat Identification**
  - A threat is not limited to those from attackers, but also includes acts of God, such as fire or severe weather.
  - Threat modelling constructs scenarios of the types of threats that assets can face.
  - The goal of threat modelling is to better understand who the attackers are, why they attack, and what types of attacks may occur.
  - A valuable tool used in threat modelling is the construction of an attack tree.
  - An attack tree provides a visual image of the attacks that may occur against an asset.
- **Vulnerability Appraisal**
  - After assets have been inventoried and prioritized and the threats have been explored, the next question becomes, what current security weaknesses may expose the assets to these threats?
  - Vulnerability appraisal takes a current snapshot of the security of the organization as it now stands.
  - To assist with determining vulnerabilities of hardware and software assets, use vulnerability scanners.
  - These tools, available as free Internet downloads and as commercial products, compare the asset against a database of known vulnerabilities and produce a discovery report that exposes the vulnerability and assesses its severity.
- **Risk Assessment**
  - Final step in identifying risks is to perform a risk assessment.
  - Risk assessment involves determining the likelihood that the vulnerability is a risk to the organization.
  - Each vulnerability can be ranked by the scale.
  - Sometimes calculating anticipated losses can be helpful in determining the impact of a vulnerability.

- Formulas commonly used to calculate expected losses are:
  - Single Loss Expectancy
  - Annualized Loss Expectancy
  - An organization has three options when confronted with a risk:
  - Accept the risk
  - Diminish the risk
  - Transfer the risk

Risk Identification Action	Steps
A. Asset identification	1. Inventory the assets.
	2. Record asset attributes.
	3. Determine the asset's relative value.
B. Threat identification	1. Classify threats by category.
	2. Design attack tree.
C. Vulnerability appraisal	1. Determine current weakness in assets.
	2. Use vulnerability scanners on hardware and software
D. Risk assessment	1. Estimate impact of vulnerability on organization.
	2. Calculate loss expectancy.
	3. Estimate probability the vulnerability will occur.
	4. Decide what to do with the risk.

Table 2 - Risk Identification Action

P6. Explain data protection processes and regulations as applicable to an organization.

Exploring some key security controls that need to be in place to ensure your organization is ready for General Data Protection Regulation (GDPR):

- **Identity and Access Management (IDAM)**
  - Having the proper IDAM controls in place will help limit access to personal data for authorized employees. The two key principles in IDAM, separation of duties and least privilege, help ensure that employees have access only to information or systems applicable to their job function.
  - What does this mean in terms of GDPR? Only those who need access to personal information to perform their job have access. In this situation, privacy training should be available to those individuals to ensure that the intended purpose for collection of personal data is maintained.

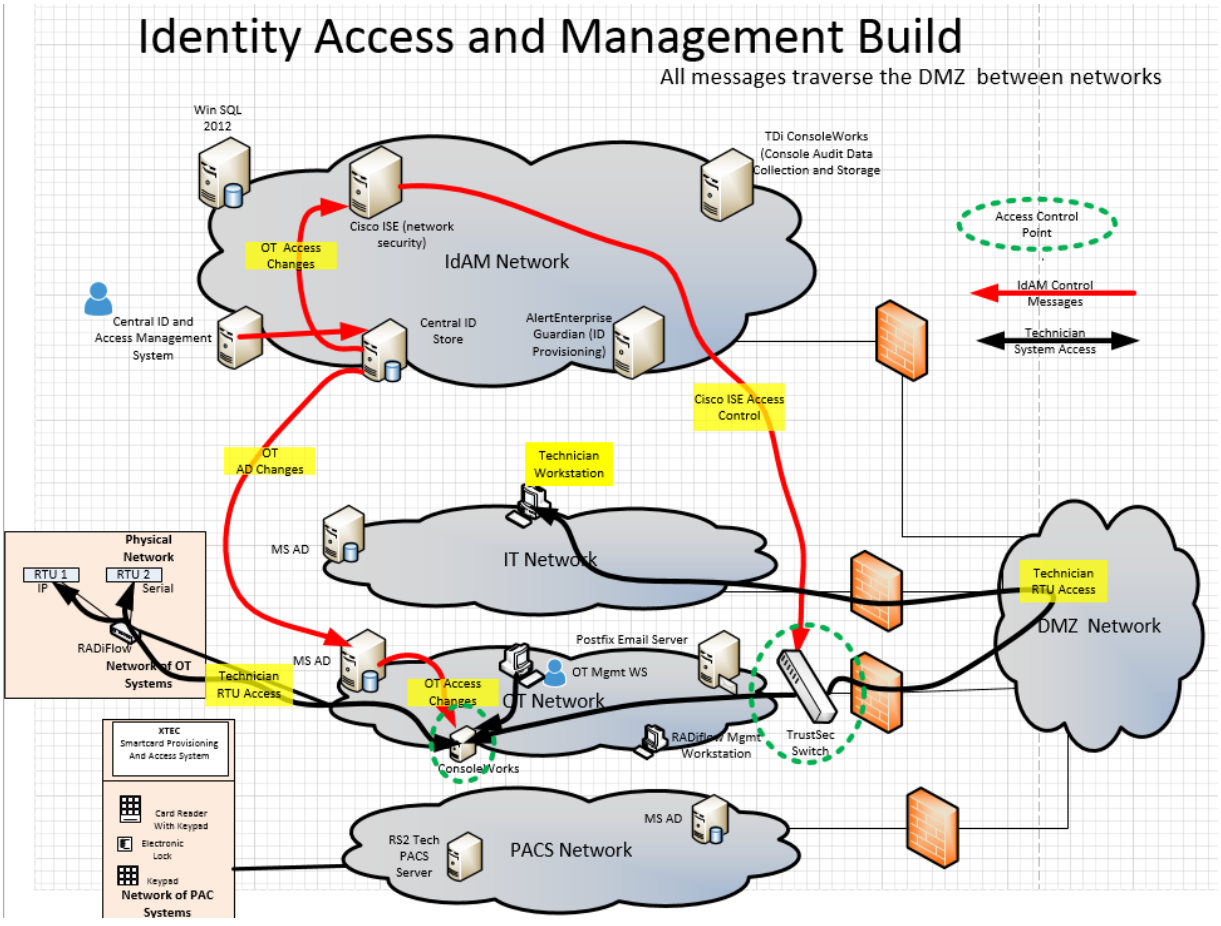


Figure 37 - Identity Access and Management Build. (nccoe, n.d.)

- **Data Loss Prevention (DLP)**
  - Relevant to GDPR, DLP helps prevent the loss of personal data.
  - Technical safeguards, such as a DLP tool, are critical in preventing a breach and becoming the next headline. According to GDPR, organizations, whether they are the controller or processor of personal information, are held liable for the loss of any personal data they collect. Incorporating DLP controls adds a layer of protection by restricting the transmission of personal data outside the network.

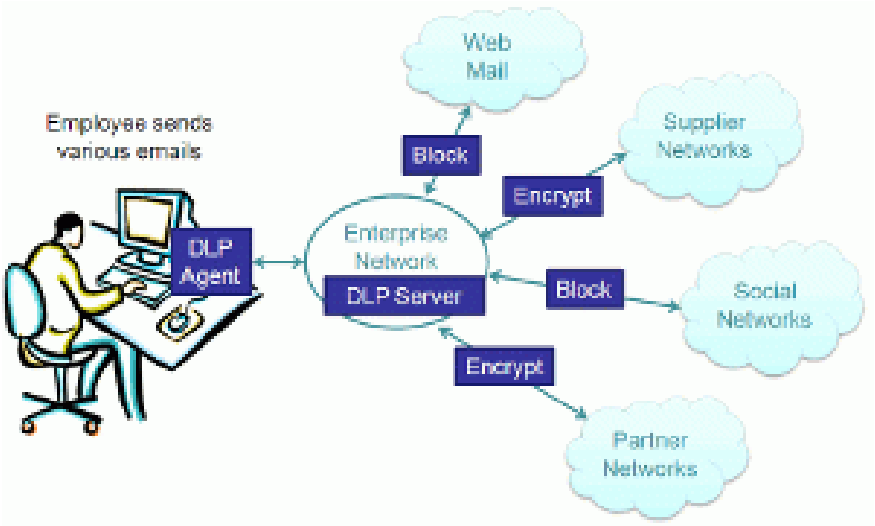


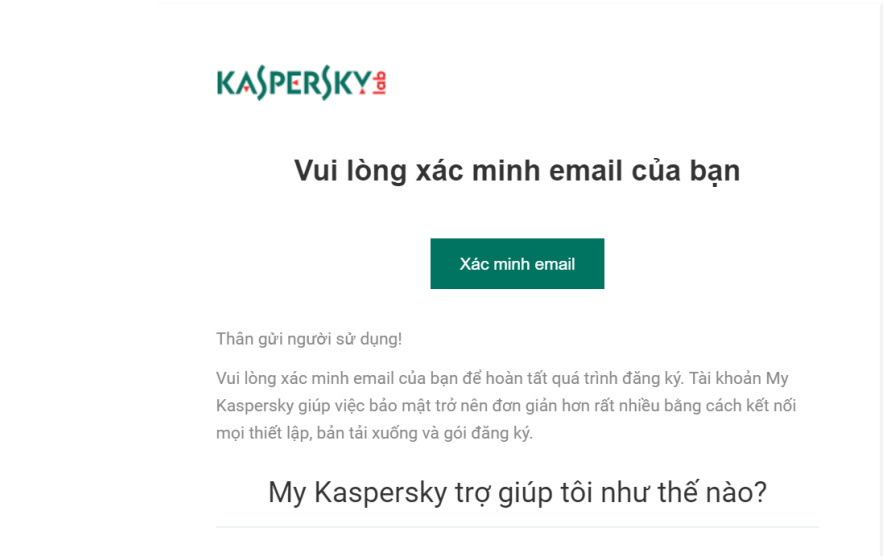
Figure 38 - Example Data loss Prevention (DLP). (veracode, n.d.)

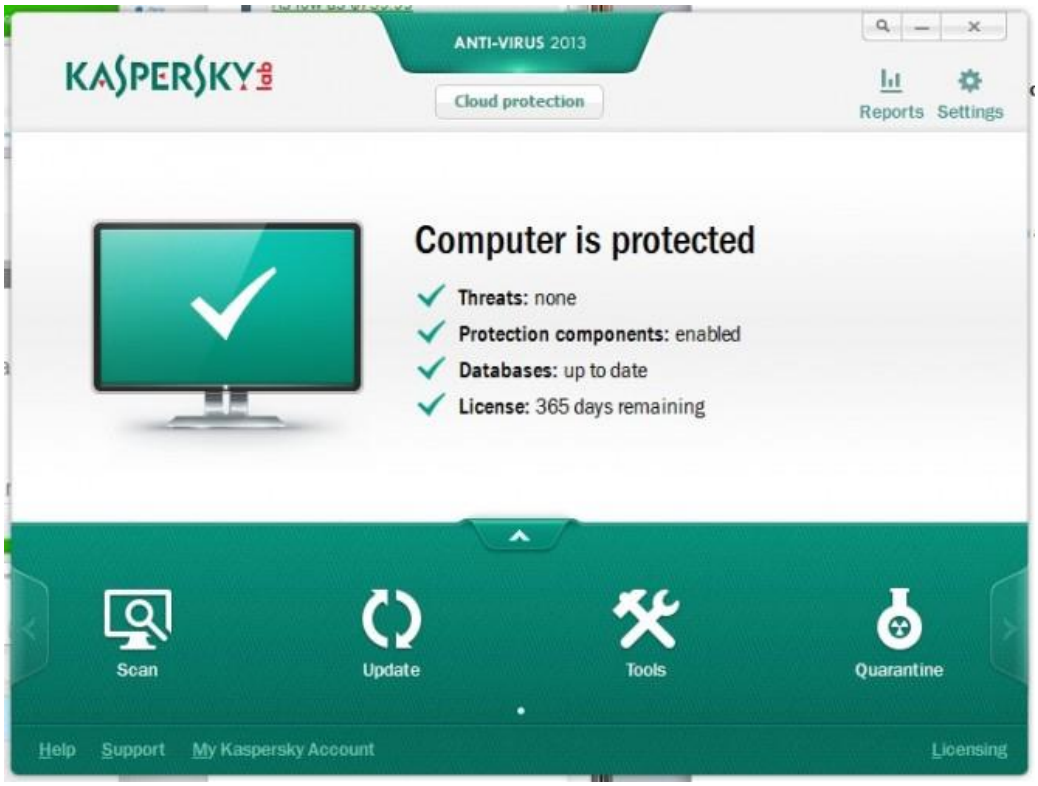
- **Encryption & Pseudonymization**
  - Pseudonymization is difficult word to spell and an even more difficult one to pronounce, pseudonymization is “the processing of personal data in such a way that the data can no longer be attributed to specific data subject without the use of additional information” (GDPREU.org). This fancy, hard-to-say word, may include field level encryption in databases, encryption of entire data stores at rest, as well as encryption for data in use and in transit.
  - Pseudonymization is something the GDPR “advises” but doesn’t require. However, if an incident leading to security breach occurs, investigators will consider if the organization responsible for the breach has implemented these types of technical controls and technologies.

- **Incident Response Plan (IRP):**
  - Mature IRP should address phases such as preparation, identification, containment, eradication, recovery and lessons learned. But what if an incident occurs and it was identified that personal data may have been breached?
  - Well, GDPR has requirements for your organization's incident response. Breach notification requirements are among the most notable in legislation. Under GDPR, "In the event of potential data breach that involves personal information, an organization must notify the Data Protection Authority without undue delay, within 72 hours if feasible, after becoming aware of the breach; and Communicate high-risk breaches to affected data subjects without undue delay" (GDPREU.org).
- **Third-Party Risk Management**
  - Third-party management is the process whereby companies monitor and manage interactions with all external parties with which it has a relationship. This may include both contractual and non-contractual parties. Third-party management is conducted primarily for the purpose of assessing the ongoing behaviour, performance and risk that each third-party relationship represents to a company. Areas of monitoring include supplier and vendor information management, corporate and social responsibility compliance, Supplier Risk Management, IT vendor risk, anti-bribery/anti-corruption (ABAC) compliance, information security (infosec) compliance, performance measurement, and contract risk management.]The importance of third-party management was elevated in 2013 when the US Office of the Comptroller of the Currency stipulated that all regulated banks must manage the risk of all their third parties. (wikipedia, n.d.)
  - If an organization entrusts the processing of personal data to processor or sub-processor, and a breach occurs, who is liable?

- **Policy Management**
  - While this is the last concept covered in this post, it's my personal favorite.
  - Policy is the teeth, the hammer and "accountability partner" for the previously discussed security controls.
  - To be effective, policy must receive enterprise-wide buy-in in order to manage and update security controls in an always changing cyber security environment. For best practices, organizational policy acknowledgement, training ensures policies are properly communicated and understood.
  - Put it all together and, if managed and followed accordingly, policy management will be foundation for compliance toward GDPR readiness.

- **Use KaperSky Anti-Virus**
  - Our security invention helps protect you from viruses, encrypted viruses, spyware, phishing, dangerous websites, spam, banner ads and more.
  - Whenever you go online, we will help protect your personal data, contact information and identity - plus we prevent followers from seeing what you do online and we prevent Your webcam is used to track you.





M3. Summarize the ISO 31000 risk management methodology and its application in IT security.

- **What is ISO 31000?**
  - The International Standards Organisation (ISO) have developed a voluntary standard to assist organisations in risk management and managing risk. Risk management being the architecture we develop and managing risk how we apply it. This architecture consists of setting out clear principles, a sound framework for which foundations can be built and processes for effectively managing risks. The building of a detailed framework within any organisation should consist of four key commissions, the design, implementation, monitor & review and continual improvement. As security risk management specialists, it is important to understand all four elements to the framework, in this discussion however we will delve into implementation and look at the risk management process itself.
  - ISO 31000 is applicable to all organizations, regardless of type, size, activities and location, and covers all types of risk. It was developed by a range of stakeholders and is intended for use by anyone who manages risks, not just professional risk managers.
- **Application ISO 31000 risk management in IT security can help us:**
  - Enhancing ability to achieve planned objectives;
  - More active in management;
  - Raising awareness about the need to identify and handle risks in the organization;
  - Improve the identification of opportunities and threats;
  - Help to comply with legal requirements, international regulations and standards;
  - Improving financial statements;
  - Improve governance;
  - Improve the trust of interested parties;
  - Establishing a reliable basis for decision making and planning;
  - Improve management methods more effectively;
  - Allocate and effectively use resources to handle risks;
  - Improve the effectiveness of activities and implementation results;
  - Enhance health, safety, as well as protect the environment;

- Improving prevention of loss and incident management;
- Improve the learning environment in the organization;
- Improve organizational coping capacity.

➢ **Implementing the Risk management process**

- The organization's risk management process should involve the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk

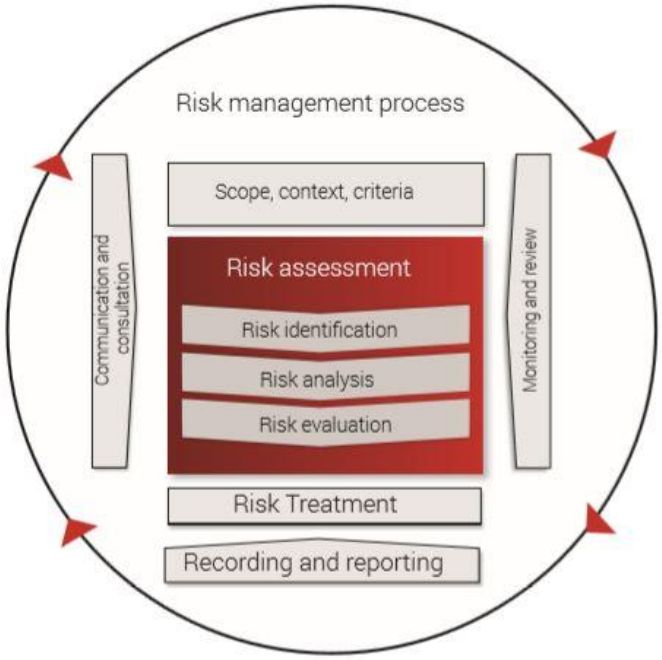


Figure 39 - The ISO 31000 risk management

- The main purpose of the risk management process is to enable the organization to assess the existing or potential risks that may be faced, evaluate the risks by comparing the risk analysis results with the established risk criteria, and treat such risks using the risk treatment options. The organization should use such process in the decision-making process

- The fundamental processes that needs to be developed which make up the full risk management process are:
  - **Establishing the context**: When establishing the context, the organization needs to consider the organization's external environment (political, social, etc.) and internal environment (objectives, strategies, structures, ethics, discipline, etc.). The organization's context must be understood before the full range of risks can be identified. While establishing the context, the organization should define the purpose and scope of its risk management activities and determine the objectives of the risk management process and the specific objectives of risk assessment. Furthermore, the organization should define the scope and boundaries related to the risk management process and identify all the constraints that affect the scope. After identifying the constraints, the organization should define the risk criteria which will be used during the whole process. This is the key consideration that most security risk management practitioners fail to understand. We need to fully appreciate the internal organisational makeup and the business objectives to be achieved or maintained if we are to build an effective plan. The external environment where the organisation operates is just as important to understand to. Having a fully informed picture of all upstream and downstream stakeholders will provide a richer contextual foundation upon which to build a strong treatment plan and define the risk criteria that reflects the organisations values and objectives.
  - **Risk identification**: The identification of risks should be a formal, structured process that includes risk sources, events, their causes and their potential consequences. Simply said, risk identification is about the creation of a comprehensive list of risks (both internal and external) that the organization faces and can involve input from sources such as historical data, theoretical analysis, expert options, and stakeholder's needs. The risk identification process enables the organization to identify its assets, risk sources, risk events, existing measures and consequences. By identifying such elements, the organization will be ready to begin the risk analysis process.
  - **Analysis risk**: The organization should analyse each risk that was identified in the previous step. Based on the level of risk that is determined after the risk analysis, the organization

can define whether the risk is acceptable or not. As so, if the risk turns out to be unacceptable, the organization can take actions to modify the risk to correspond to the acceptable level of risk. The organization should use a formal technique to consider the consequence and likelihood of each risk, and these techniques can be qualitative, semi-quantitative, quantitative, or a combination thereof, based on the circumstances and the intended use.

- **Assess the risk**: We need to consider the risks we have identified and the fallout should they occur. It is again important that we apply a systematic and strong objective analysis of risk at this stage which take into consideration expert advice and divergence. If we fail to apply accurate analysis, then we will either over or understate the impact of risk on the organisation's objectives and the likelihood for this occurring.
- **Risk treatment**: Proper risk management requires rational and informed decisions about risk treatment. Typically, such treatments include avoidance of the activity from which the risk originates, risk sharing, managing the risk by the application of controls, risk acceptance and taking no further action, or risk taking and risk increasing in order to pursue an opportunity. Remember that organizations do not always find themselves in trouble because of their excessive and reckless behaviour. Sometimes organizations fall behind their competitors as a result of their reluctance to take risks and pursue opportunities.
- **Communication and consultation**: Proper risk management requires structured and ongoing communication and consultation with those affected by the organization's operations. The communication seeks to promote awareness and understanding of risk and the means to respond to it, whereas consultation involves obtaining feedback and information to support decision-making.
- **Recording and reporting**: Another step of the risk management process based on ISO 31000 is the recording and reporting, i.e. the outcomes of the risk management process are to be documented and reported through appropriate mechanisms. Recording and reporting is important for reasons such as communication of the risk management

activities and outcomes pertaining to those activities throughout the organization and providing the necessary basis and information for making informed decisions.

- **Monitor and review**: Considering that both the external and internal environments are subject to constant change, the purpose of this step is to help organizations assure and improve the quality and effectiveness of the risk management process. Monitoring includes actions such as examining the progress of treatment plans, monitoring the established controls and their effectiveness, ensuring that activities which are proscribed are being avoided, and checking that the environment has not changed in a way that affects the risks.

- There are two elements of the process that can be considered as continually acting. These are:
  - Communication and consultation with internal and external stakeholders, where practicable, to gain their input to the process and their ownership of the outputs. It is also important to understand stakeholders' objectives, so that their involvement can be planned and their views can be taken into account in setting risk criteria.
  - Monitoring and review, so that appropriate action occurs as new risks emerge and existing risks change as a result of changes in either the organisation's objectives or the internal and external environment in which they are pursued. This involves environmental scanning by risk owners, control assurance, taking on board new information that becomes available, and learning lessons about risks and controls from the analysis of successes and failures.

M4. Discuss possible impacts to organizational security resulting from an IT security audit.

- **What is IT security audit?**
  - An IT security audit involves an IT specialist examining an organisation's existing IT infrastructure to identify the strength of its current security arrangements and pinpoint any potential vulnerabilities.
  - Using specialist tools to gather data from the various systems that a business uses to carry out their digital day-to-day tasks, whomever is carrying out the audit will conclude by putting together an in-depth report that covers the aspects where the infrastructure is strong and where it is perhaps more vulnerable.
  - This is followed up with a number of recommendations to bolster the business' network security arrangements, with tasks identified to be carried out in the short, medium and long term. (cheekymunkey, n.d.)
- **Why does organizational need an IT security audit?**
  - Principally, an IT security audit is needed to ensure that your cyber-defences are as up to date as they can be, in order to effectively respond to the threats posed by hackers and other such criminals who manipulate IT systems for their own ends.
  - Should an IT system's defences be found wanting when compared to the cutting-edge approaches used by hackers, then everything your business has worked for could be at risk. Just a single vulnerability can lead to not only your bank details and subsequently your cash being stolen, but also your personal data that you wouldn't want to be made public knowledge.
  - Small businesses in particular are tempting target for cyber-criminals, as the thinking is that whilst they have significant cash reserves due to be a commercial entity, they are unlikely to have a sizable team or level of resources solely dedicated to IT protection. Due to their attention being diverted elsewhere, an infiltrator can go about their business without being detected, whereas larger company with greater manpower would be able to quickly detect that something is amiss.

- **Types of audits conducted:**
  - ISO/IEC 27001 Internal audits: part of certification process.
  - Information Security Assessments: Complete or Partial to know security posture of the organization.
  - In house security audits:
    - Target: Ministries and Departments with IT infrastructure of basic to medium complexity.
    - Scope: Key components of the IT infrastructure (Servers, Network devices).
    - Approach: Conducted by IT security Unit staff and use of an Industry Standard Vulnerability Assessment Toolset.
    - Outcome: Report on Vulnerabilities identified and recommendations. This will recommend implemented by Ministries/Departments.
  - Outsourced security audits:
    - Target: Highly complex and critical Information Systems of the Government, IT security Unit manages the project.
    - Scope: Include all components of the Information System: Application, software, middleware, database, operating system, hardware and network infrastructure. And all interfaces to/from remote applications.

- **Standard Techniques:**

IT security auditing requires below standard techniques to know the security level of systems and networks in organizations.

- **Network Scanning:** Network scanning tool scans port to verify the connectivity between the host and organization's network. Thereby it provides complete list of all active hosts, printers, switches and routers. By network scanning, organization can verify the unauthorized network connectivity, vulnerable service, and collect forensic evidence.
- **Vulnerability Scanning:** Vulnerability scanning distinguishes open ports and the data of associated vulnerability. It also guides on mitigation of detected vulnerabilities. Vulnerability scanner also provides active tools that help to find vulnerabilities before the attackers find it. In addition, organization can easily gauge about the level of its security and chances of being exposed to external vulnerabilities. Moreover, vulnerability scanning identifies applications and

banner grabbing, OS, misconfigured settings, active hosts on networks, outdated software versions.

- **Password Cracking:** Password cracking software used to find weak passwords, and grab password hashes. Once the hashes are found, password cracker generates hashes until a right password is matched.
- **Log Review:** Log reviews give idea about the difference in system logs compared to prescribed organization's security policy. The logs include firewall logs, IDS logs, server logs, these logs provide a real image of ongoing activities that can be matched with defined security policy. After reviewing log reviews, organization can change firewall policy to minimize the access to susceptible system.
- **Virus Detection:** Organizations are prone to virus, worms, malware, which result into deletion of files, pop up screen message or destruction of sensitive information. Virus Detection program identifies current virus in systems and can be installed on network infrastructure and mail servers in organization. Virus detection detects virus before it enters the network besides, it detects virus in emails, USB drive, hard disk, documents and local host, websites. To get rid of virus and other malwares, organization should have antivirus software and the virus definition should be updated regularly.
- **Penetration Testing:** Penetration testing refers to circumvention of system's security features based on the system implementation and structure. Such testing identifies the method of gaining the system access using tools and techniques. It needs expertise to run penetration testing. It may happen that while running penetration testing, the network response time may be slow. While carrying testing few details like IP addresses, restricted hosts, testing techniques, testing time, points of contact should be considered. (clickssl, n.d.)

- **Possible impacts to organizational security:**
  - IT security auditing ensures that your cyber defence measures are updated as quickly as possible.
  - To effectively deal with threats posed by hackers and other criminals who manipulate IT systems.
  - Security audit helps you to save money by finding more effective ways to protect your information system and minimize resource wastage for outdated or inefficient operations.
  - Security audit can use the standards needed to mature your position and provide practical utility. We can help you make the most of your involuntary investment.

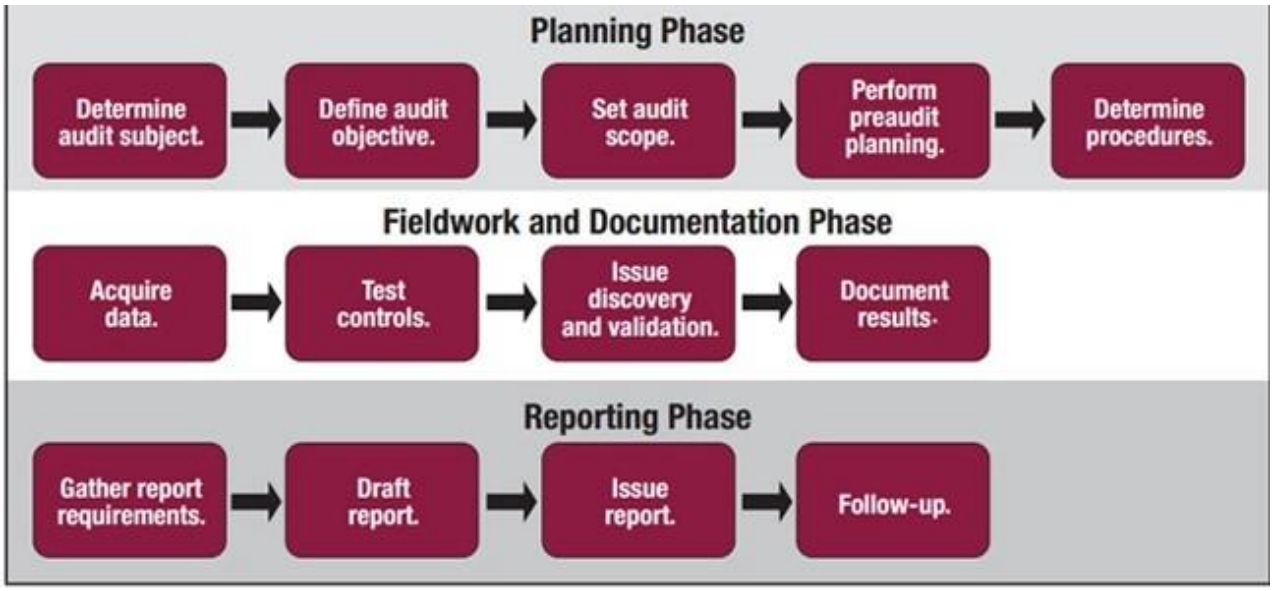


Figure 40 - The Auditing Process and Cybersecurity. (isaca, n.d.)

D2. Consider how IT security can be aligned with organizational policy, detailing the security impact of any misalignment.

- **What is Organizational Policy?**
  - A security policy is expected to do many things. Primarily it should protect people and information, as well as set the rules for expected behaviour by users, system administrators, management and security personnel. It should also authorise relevant personnel to monitor, probe, investigate, define and authorise the consequences of violations, in addition to defining the company's baseline stance on security. This can help minimise risk and help track compliance with appropriate regulations.
  - This is fine in theory, but as recent high-profile cases have demonstrated, having written policies does not always mean that people follow them. (armstrongadams, n.d.)
- **IT security has 7 related domain names that may be linked to the organization's policy:**
  - **Culture:** Develop an organizational culture in which users, managers and IT professionals all make good decisions about information risk.
  - **Planning:** The strategic and tactical planning activities of the information security organization provide ample opportunity for aligning the resultant projects and actions to actual business requirements. For example, a key strategy is to leverage enterprise architecture principles in security planning practices.
  - **Processes:** Adopting a strategic process approach, such as the ISMS prescribed by ISO 27001, to the security management program. It establishes the ability to assess, develop and implement security solutions as and when required by the business, rather than enforcing a "one size fits all" control baseline.
  - **Communications:** A primary objective should be to develop security-related service-level metrics that can be included in formal service-level agreements (SLAs) between IT, service providers and user constituencies.
  - **Competencies:** Business alignment often requires skills not normally associated with information security specialists such as architecture practice, personal communications, business knowledge and marketing skills.

- **Technology:** The way security technology is utilized can have a major impact on how security is perceived by technology users. The success of an integrated IT service delivery strategy, such as that prescribed by ITIL v3, will depend on how security controls are technically integrated with IT services.
- **Relationships:** The importance of establishing and maintaining effective relationships with other roles and individuals within the organization. Alignment depends on the cooperation and support of key influencers, decision makers and other stakeholders.

➢ **Detailing the security impact of any misalignment.**

- **External Misalignment:**
  - **Customer Requirements:** The data analysis reveals the extent to which customer requirements drive the software development process. For the BA, the important subject is ensuring customer satisfaction, however, still maintaining the quality and credibility of the software. Both the BAs and the developers indicated the need to focus on customer needs and preferences when adding security features. However, it is clear from the data analysis that customer preferences can result in security vulnerabilities. In the study, one example which can be used to illustrate this aspect relates to a customer requesting the introduction of web banners inside the mobile banking application to advertise the other products offered by the customer.
  - **Standards and guidelines:** External misalignment can also occur in terms of variability in security guidelines and standards. It is important to note that security in mobile apps can be achieved by an additional tool provided by a third-party company that specialises in security, by building security components in-house such as authentication or by implementing both security mechanisms.
  - **Regulatory requirements:** The data analysis indicated complexities around the understanding of government regulations that relate to security of information. In addition, one may need to consider regulations from different countries as software development is global. A company may be providing software to customers in different countries, with different laws and regulations. According to one developer, several

regulations are in place which makes following and aligning them the to the development process difficult.

- **Third-party software:** The use of third-party applications brings several alignment challenges in the software development lifecycle. In this case study, the involved organisation integrated a third-party security application as one of the means of ensuring the security of the mobile banking application. Challenges manifested during the processes of integrating a third-party security application to the mobile banking application. One problem as mentioned by one of the developers was the misalignment that resulted due to the conflicting internal security policies and regulations with those of the security vendor.

- **Role Misalignment:** Role misalignment occurs between different specific roles. The roles found in an agile team are easily distinguishable yet connected. Typically, in a scrum environment, because of the augmented team collaboration, there is needed to understand tasks performed by other roles. This will enable one to identify where they fit in on the team and what each team member needs to do to be able to complement the other roles.
- **Skills Misalignment:** Skills misalignment occurs when the expected competency level of a specific role does not align with their ability to perform the role. Skills misalignment can result in inappropriateness of responsibilities, idle time and errors. In the current study, one task that was simple resulted in several errors. One developer indicated that as a result of lack of knowledge on configuring the third-party security application to work with the mobile application, more time was taken to complete the task than what was initially anticipated. The lack of skills required to implement security requirements is mainly because security education is not usually a part of a software developer curriculum. Most developers learn how to write code. Security skills are an additional proficiency often acquired through experience.

- **Requirements Misalignment:** Requirements misalignment occurs when there are conflicting issues between security requirements and the general system requirements. Requirements can either be functional or non-functional requirements with security requirements categorised as non-functional. Regardless, functional and non-functional requirements are equally important and must be taken into consideration during software development. Fragmentation in requirements classification is important but can result in alienating the different types of requirements, with non-functional requirements having less priority and considered after the design stage (Mouratidis et al., 2005).

Category	Definition
External Misalignment	External misalignment occurs when the software development processes conflict with any other elements that are eternal and out of the control of the development team such as the customers, regulations and third-party applications
Role Misalignment	Role misalignment occurs between specific roles such as developer and tester misalignment
Skills Misalignment	Skills misalignment occurs when the current skills do not match the required workload leading to mismatch in responsibilities and incorrect implementation
Requirements Misalignment	Requirements misalignment occurs when there are conflicting issues between the security requirements and the general system requirements

Table 3 - Example of misalignment Categories

LO4. Manage organizational security

P7. Design and implement a security policy for an organization.

- **Network Security Policy**
  - Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.
  - There is no definitive mechanism for protecting a network because any security system can be subverted or compromised, if not from the outside then certainly from the inside. Ultimately to secure a network is to implement different layers of security so that an attacker must compromise two or more systems to gain access to critical assets. The first step in enforcing policies is to define the policies that will be enforced. Security measures often restrict personnel in their operating practices and make some activities less convenient which results in a temptation to boost security regulations. Network policies are, therefore, govern how a network should be implemented and configured to streamline employee's operation in ordinary conditions as well as guides how to react during the occurrence of abnormalities. In this context, the following section explains the imposition of policies measures of each term or principle of network security to protect information and systems.
- **Implementation of security policies security as follows:**
  - Operating systems, databases, applications:
    - Through the strengthening of security implemented especially in operating systems and databases.
    - Audit of security implementation for applications associated with OS and database.
  - Implementation of security, which has pursued policies related to:
    - Privacy.
    - Password.
    - Risk management.
    - Storage and archiving of the data in terms and policies of company.

- Use of e-mail as a way of communication and use of program management to identify problems reported and the time resolution of reported problems.
- Classification of documents and data in groups of "classified" or "not classified".
- Business continuity by eliminating the Single Point of Failures for processes and systems.
- Management of security incidents, reporting, archiving and improve procedures if it will be necessary.

- Network security:
  - Access control.
  - Remote access.
  - Internet and e-mail access security.
  - VoIP communications.
  - Management of Emergencies through back up that should be available and throw changing of access security policies if needed.
- Physical security through management and control for:
  - Entries in the data center with different access levels and for different areas physically separated.
  - Access control, for the use of equipment like server, router, PC etc.
  - Real time monitoring of data center environments with the possibility of registration logs and relevant events, regardless of their nature.
- Hardware and software used for security purposes:
  - Antivirus implemented in the server with CAL for each user.
  - Encryption of data and management of security keys.
  - IDS / IPS, Intrusion Detection System / Intrusion Prevention System.
  - SIEM, Security information and event managements.
  - Firewalls

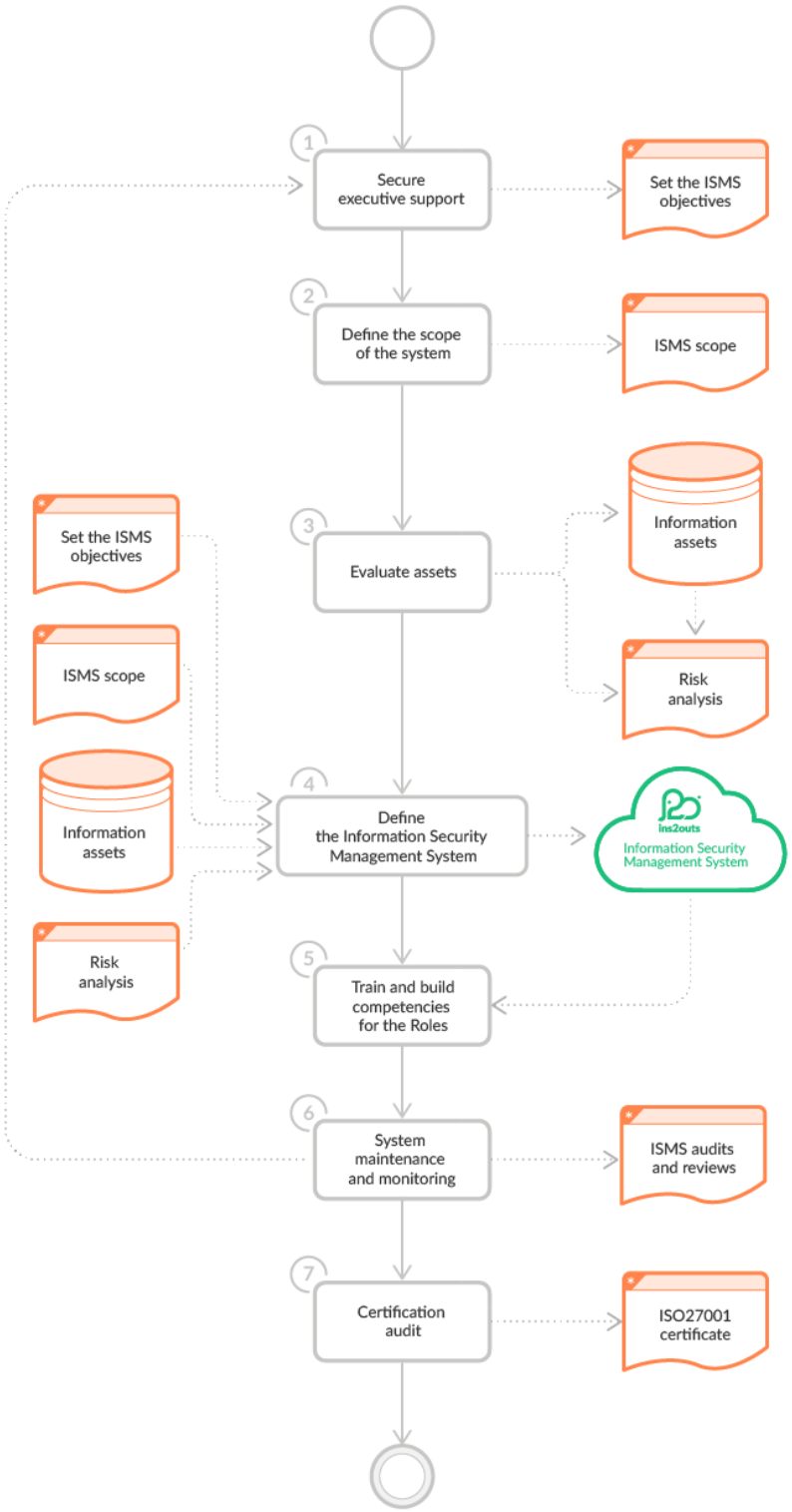


Figure 41 - Implementing an Information Security Management System. (ins2outs, n.d.)

- **Step1: Secure executive support and set the objectives.**
  - Deciding to implement an ISMS compliant with ISO/IEC 27001 should always start with getting the involvement / confirmation of the organisation's top management. This group decides the allocation of resources and budget for defining and maintaining the management system, sets its objectives, and communicates and supervises it in the organisation. Setting the objectives is an iterative process and hence requires annual updates. The information security system objectives should be determined by the top management and reflect the business and regulatory needs of the organisation.
- **Step 2: Define the scope of the system.**
  - Contrary to the public opinion, which dates back to experiences with the ISO 9001 standards, ISO/IEC 27001 is well-grounded in the reality and technical requirements of information security. This is why the organisation should, in the first place, choose those security measures and requirements set out in the standard that directly affect it. The standard defines the processes that should make up the Management System of the organisation as well as the security measures that the organisation should implement to ensure information security. The results of these actions provide a basis for the subsequent steps of the implementation.
- **Step 3: Evaluate assets and analyse the risk.**
  - The next step is to evaluate information processing assets and carry out a risk analysis for them. What is asset evaluation? It is a systematic review, which results in a description of the information processing assets in the organisation. Some of asset categories include:
    - Hardware – computers, phones, physical data storage media,
    - Servers – both physical and virtual serves comprising the company's ICT infrastructure,
    - Network infrastructure – elements of the company's network infrastructure,
    - (Cloud) services – e.g. 365, Amazon Web Services, JIRA, Confluence, Dropbox, banking services, etc.,
    - Customer information – information provided by customers; usually involves the greatest business risk,
    - Other – this category includes paper data media.

- **Step 4: Define the Information Security Management System.**
  - At this stage of implementation, the executive support has been secured, objectives have been set, assets have been evaluated, the risk analysis results are already available, and the risk management plan is in place. As a result, the remaining elements of the Information Security Management System can be defined and security measures can be implemented in the organisation. Usually this is an iterative process where the following ISMS components are defined:
    - Policies
    - Procedures
      Instructions
    - Inputs/Outputs
    - Training
    - Guides
    - Sources of knowledge
    - Roles
    - Normative sources
  - This scope of activities is usually carried out by a consultant or acquired by purchasing ready-made know-how for ISO/IEC 27001. In any case, the management system should reflect the actual processes within the organisation on the one hand, while also introducing the required know-how where necessary. Know-how definitions can specify the persons in the organisation who will be responsible for the specific know-how. Together with the working group, they will be responsible for the maintenance and updating of information and passing it to other people within the organisation during the system maintenance and continuous improvement phase.
- **Step 5. Train and build competencies for the Roles**
  - At this stage, the organization needs to specify the capabilities and skills of those / roles related to the Information Security Management System. The first step after identifying the ISMS is to explain it and inform the organization of the scope and how it operates, as well as how each employee affects information security. This factor needs to be incorporated into the organizational management system by defining the roles and capacities needed for the role

and how to convey this knowledge to new employees and renew it in trained people. At this point, it is worth determining the training, guidance and capacity profiles for each role.

- Some of the information security roles that can be found in most implementations include:
  - Employee – role representing any person employed at the organisation,
  - Internal auditor – role responsible for conducting management system audits,
  - IT administrator – role representing people responsible for managing the IT infrastructure of the organisation.
  - Top management – role representing the group responsible for setting directions and controlling the organisation at the top level,
  - The Personal Data Protection Regulation

➢ **Step 6. System maintenance and monitoring**

- Before commencing the certification of the information security management system it should already work in the organisation. Ideally, a fully defined system will have been implemented and maintained in the organisation for at least a month or two prior to the start of the certification audit, providing the time for conducting the necessary training, carrying out a management system review, implementing the required security measures, and adjusting the risk analysis and risk management plan. During this period, the first actions set out in the infrastructure maintenance and security management plan should be carried out as well.
- This way when the certification audit starts off, the organisation will have the documentation and execution records to prove that the Information Security Management System is deployed and safe. Note that the basic requirement for any management system is its ability to ensure continuous improvement through monitoring, internal audits, reporting corrective actions and systematic reviews of the management system.

➢ **Step 7. Certification audit.**

- The implementation of an information security management system in a company is confirmed by a certificate of compliance with the ISO/IEC 27001 standard. The certification requires completing a certification audit conducted by a body certifying management system. The certification audit has two phases. Phase I usually involves a check of the scope and completeness of the ISMS, i.e. a formal assessment of the required elements of a management

system, and in phase II the system is verified in terms of whether it has been implemented in the company and corresponds to its operations.

- After successfully completing the certification process audit, the company is issued ISO/IEC 27001 certification. In order to maintain it, the information security management system must be maintained and improved, as confirmed by follow-up audits. After about 3 years, a full re-certification involving a certification audit is required.

- **Device Security**
  - You will most likely identify different network segments with different security requirements while designing security for your network. For instance, some servers will need to be accessible by the employees. Some of on the other hand will be openly accessible. Hence, to implement security for different divisions or subdivision, you will erect perimeters that can only be crossed by certain types of traffic in the form of Public network, Private network, and semi-private network. The limitations of such network segments are founded by devices such as router, gateway, bridge, and switch which can regulate and controlling the flow of packets into and out of the segment. Communication and monitoring devices are typically deployed in the network for various purpose, must be configured properly according to requirement and accessed on the ground of given privilege and profile of users as well as, their inbuilt software most up to dated. Apart from that following measure should be taken in the context of device security as
  - The company must sign NDA to each employee about not disclosing the details of deployed devices inside the perimeter.
  - Regularly applied patches and security updates released by vendors.
  - ACL should be maintained to permit or deny TCP and UDP traffic.

```
!
access-list 1 deny 192.168.3.0 0.0.0.255
access-list 1 permit any
!
```

Figure 42 - Configure ACL on Router

  - Services must be disabled if they are not in use.

- **Internet Access**
  - Internet access policies include automatically blocking of all websites identified as inappropriate (especially social media related sites) for company user. Moreover, internet access should be based on the work nature of the employee. The Internet constructs a network topology and connects various crucial assets of the company for example server and account sections, etc. therefore, must be filtered, and monitored properly before wielding.
- **VPN Policy**
  - VPN provides a means to protect data while it travels over an untrusted network. VPN is intended for employee use of organization-owned computer system only. All kind of remote access to corporate network should be routed via VPN with a valid corporate-approval, standard operating system along with appropriate security patches. Access to company computer from home via the internet should not be allowed. To protect the network when VPN are used for remote user access, the security administrator should ensure that adequate protection is implemented over endpoints by applying L2TP with IPSec. Moreover, VPN vendors include firewalling functionality in their client to filter traffic.
- **Port Communication Policy**
  - Communication ports either inbound or outbound at the workstation for unnecessary services must strictly be in the blocked state apart from essential service such as HTTP or HTTPS, etc. as it being mostly noticed that ports open for several services opened needlessly, that typically induces the hacker to breach the system with ease. Such security measures could be applied by the system administrator at Firewall end as the first line of defence. Hence, workstation that does directly communicate to the internet must be limited to use only authorized communication services or ports in inbound connection.

- **Wireless LAN Policy**
  - To stop the possible abuse of wireless network, there should be proper user authentication ensured along with the appropriate replacement of WEP and anomaly tracking mechanism on wireless LAN. Moreover, 802.11i security measures such as TKIP, CCMP should be employed for encryption. At the same time, there is the following list of suspicious events on wireless LAN which should always consider for intrusion detection as:
    - Beacon frames from unsolicited access point
    - Flood of unauthenticated frames (MITM attack)
    - Multiple incorrect SSID on closed network
    - Frames with duplicated MAC address.
    - Randomly changing MAC address
- **Remote Connection Policy**
  - Data security is becoming a vital issue as more organizations establish network links between their employees to share information, increase productivity. As personnel more often prefer to work from home, security begins with a terminal session between an authorized user and remote host on a network and user can perform all functions as if he were on the remote host. At the same, mismanagement of user credentials can lead to exploitation too. Hence, direct access to critical server or system of an organization should be strictly in restricted mode via remote login or SSH utility in exception to authorized user. However, encrypted access could be permissible.
- **Firewall Rules Policy**
  - When a user connects to an insecure, open network, such as the Internet, he opens a large doorway for potential attacks. One of the best ways to defence against exploitation from the insecure network is to employ firewalls at the connection point end, as it is a necessity to safeguard their private networks and communication facilities. There should be rules enforcement policy varies to the type of firewall and resource deployment on the network as:
    - In the case of dedicated server access, application proxy firewall must be placed between the remote user and dedicated server to hide the identity of the server.

- Secondly, if the requirement of traffic filtering based on source and destination IP/Port address, packet-filtering firewall placement is quite useful which augment speed of transmission too.
- On the other hand, when speed is not a concern, state table (stately inspection firewall) filters configuration at the network is an appropriate choice which dynamically validates the connection and forwards the packet.
- Moreover, NAT should also be employed as it complements the use of firewalls in providing an extra measure of security for an organization's internal network, especially preventing DDOS or many SYN flooding attacks.
- If you need higher level of control than is available by preventing an IP address from communicating with your server, IP packet filtering can be used.

➢ **Intrusion Policy**

- IDS should be housed for anomaly detection and monitoring unauthorized access, as for the extreme line of defence, firewall or antivirus are not enough. Security administrator must constantly check system and security log files for something suspicious. Moreover, use Advance Antivirus which has inbuilt IDS/IPS capability, for inappropriate auditing rights, elevated privileges, incorrect groups, altered permission, registry change, inactive users and much more. Most importantly, IDS software is configured on the top of an OS, but network intercepting IDSs are increasingly being deployed as hardware application because of performance perspective.

➢ **Proxy Server Policy**

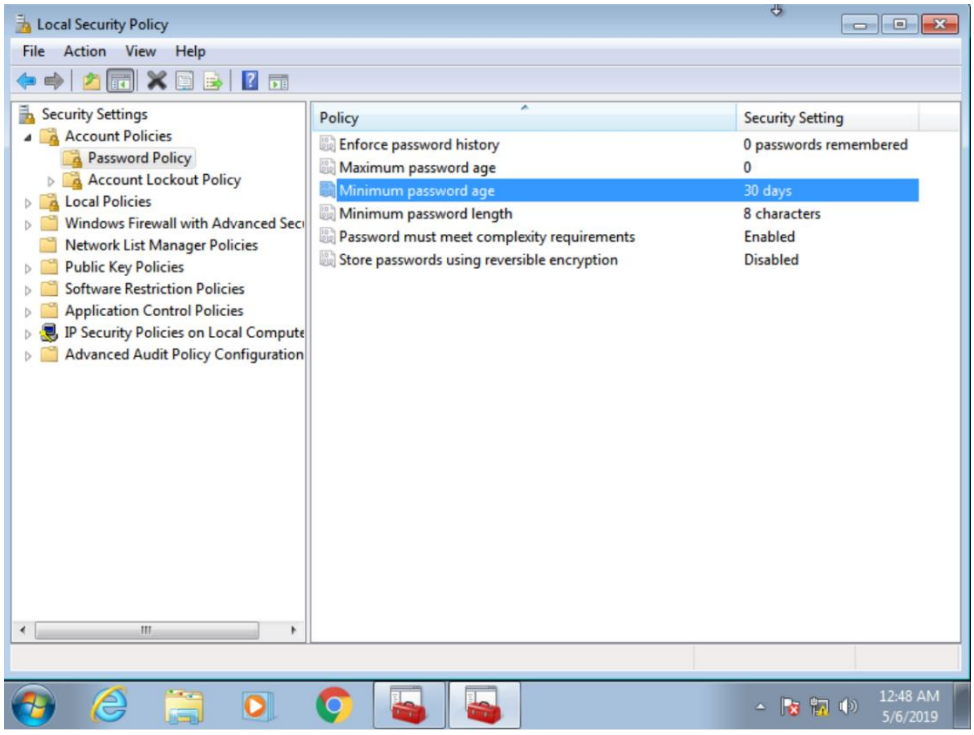
- A proxy server typically resides between server and user, for both offensive and defensive purpose. When deploying a proxy server, the following checklist must make sure as:
- Logging facility should be enabled for all services
- Never allow proxy to accept outside connection.
- The proxy must be running with most up-to-date patches and software.

- **Secure Communication Policy**
  - Data that passes through many channels including a switch, routers on the network in unencrypted form, is vulnerable to many attacks such as spoofing, SYN flooding, sniffing, Data alteration, and session hijacking. Although, you are not in control to of the devices that your data might pass over, but you can secure the sensitive data or may be secure the communication channel from being data accessible to some extent. Hence, employment of numerous ciphering tactics such as SSL, TLS or, IP-Sec, PGP, SSH can encrypt all kind of communication such as POP, HTTP, POP3 or IMAP, and FTP because SSL packets can be passed through firewalls, NAT servers, and other network devices without any special considerations other than making sure the proper ports are open on the device. If we have some data need to transmit data over a network securely, then there are some security initiatives one need to take to mitigate the risk of an attack:
  - Authenticate the identity of people (and/or computers) who will send packets
  - Make sure that the data will not be tampered with (no MITM attack encountered)
  - Ensure that the data will not be read by any unauthorized individual between user and the source.
- **DMZ Policy**
  - Certain system or server for instance e-mail, web server, database etc.…that need to access the public internet, must be deployed on a dedicated subnet which separates from the internal system from outside, because publicly accessible system comes directly under attack by hackers. A potential attack against critical system can be undermined or even negligible by placing them in the segregated network along with the firewall.
- **Create and manage Account:**
  - Account must be protected with a complex password (password length, password complexity).
  - Account holders are only allowed to access necessary information and services.
  - Disable unused temporary accounts, delete unused accounts.
  - Locking the account after a number of times the user log-on failed the system.
  - Accounts on the system will receive 2 main rights:

- User rights: A type of privilege that a User is allowed by the system to perform special actions (e.g. Right to Backup Files and Folders, change system time, system shutdown ...).
- Permissions: Controlled by the system's DACLs (Discretionary access control lists), allowed to access files / folders or Active Directory objects (in Domain) (e.g. User A is entitled to Read / Modify for with Folder C:\Data, User B is Full Control for Business OU ...).

➢ **Password**

- The minimum password length is 8 characters or more including normal letters or flowers (A to Z – a to z), numbers (0 to 9), special characters: !@ # $% ^ & * (). The longer the password, the safer it is.
- Password must meet the complex requirements: not only the length but also the complexity of the password set to ensure account security (example: password and P@ssW0rd).
- Account lockout: Account will be locked for certain period if after some time log-on fails on the system. The purpose of this policy is to prevent brute force attacks on accounts to detect passwords.



Name of Security Policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments and investigate incidents to ensure conformance to security policies or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel

Table 4 - Examples of security policies

P8. List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.

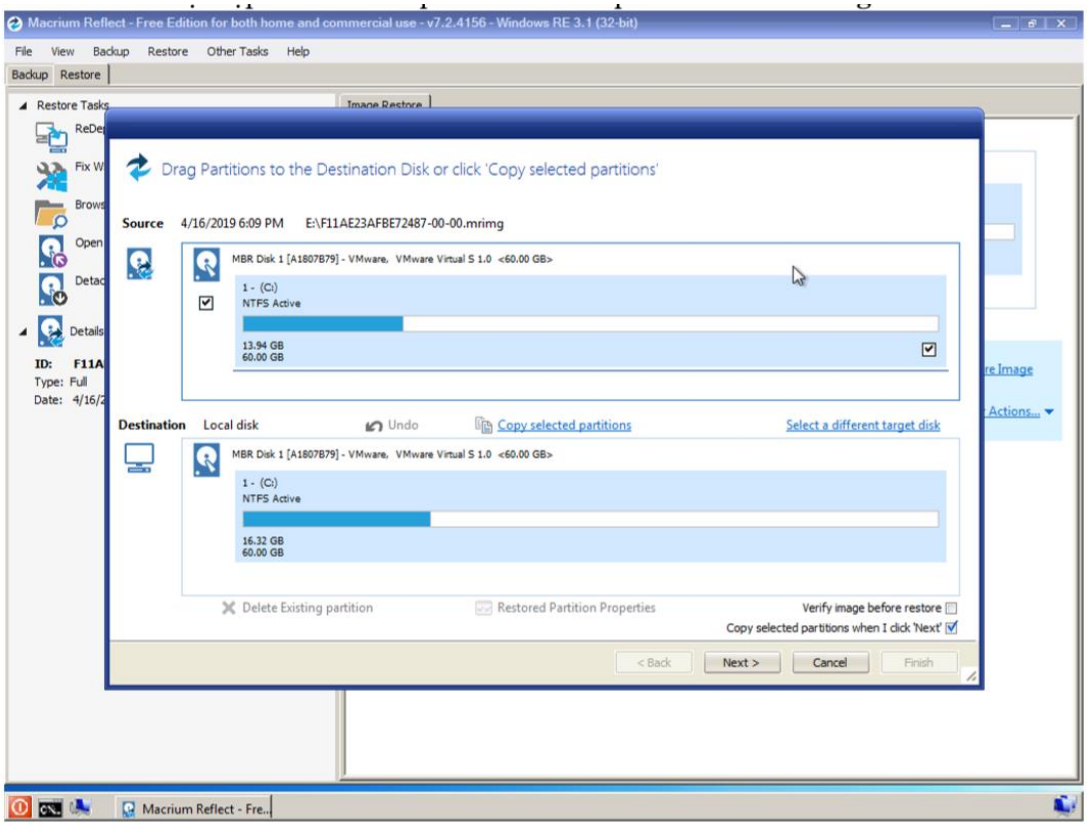
Here are some key elements of a business disaster recovery plan.

- **Communication plan and role assignments.**
  - When it comes to disaster, communication is of the essence. A plan is essential because it puts all employees on the same page and ensures clearly outlines all communication. Documents should have all updated employee contact information and employees should understand exactly what their role is in the days following the disaster. Assignments like setting up workstations, assessing damage, redirecting phones and other tasks will need assignments if you don't have some sort of technical resource to help you sort through everything.
- **Plan for your equipment**
  - It's important you have a plan for how to protect your equipment when a major storm is approaching. You'll need to get all equipment off the floor, moved into a room with no windows and wrapped securely in plastic so ensure that no water can get to the equipment. It's obviously best to completely seal equipment to keep it safe from flooding, but sometimes in cases of extreme flooding this isn't an option.
- **Data continuity system.**
  - As you create your disaster recovery plan, you'll want to explore exactly what your business requires in order to run. You need to understand exactly what your organization needs operationally, financially, regarding supplies, and with communications. Whether you're a large consumer business that needs to fulfill shipments and communicate with their customers about those shipments or a small business to business organization with multiple employees – you should document what your needs are so that you can make the plans for backup, business continuity and have a full understanding of the needs and logistics surrounding those plans.
- **Backup check.**
  - Make sure that your backup is running and include running an additional full local backup on all servers and data in your disaster preparation plan. Run them as far in advance as possible and make sure that they're backed up to a location that will not be impacted by the disaster. It is

also prudent to place that backup on an external hard drive that you can take with you offsite, just as an additional measure should anything happen.

- **Detailed asset inventory.**
  - In your disaster preparation plan, you should have a detailed inventory of workstations, their components, servers, printers, scanners, phones, tablets and other technologies that you and your employees use daily. This will give you a quick reference for insurance claims after a major disaster by providing your adjuster with a simple list (with photos) of any inventory you have.
- **Disaster Recovery Team:**
  - The team will be contacted and assembled by the ERT. The team's responsibilities include:
    - Establish facilities for an emergency level of service within 2.0 business hours;
    - Restore key services within 4.0 business hours of the incident;
    - Recover to business as usual within 8.0 to 24.0 hours after the incident;
    - Coordinate activities with disaster recovery team, first responders, etc.
    - Report to the emergency response team
- **Plan Documentation Storage:**
  - Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose
- **Backup Strategy:**
  - Key business processes and the agreed backup strategy for each are listed below.
  - The strategy chosen is for a fully mirrored recovery site at the company's offices. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

- Backup data with “Macrium reflect”:



KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Purchasing	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
Web Site	Fully mirrored recovery site

Table 5 - Example Backup strategy

- **Risk Management:**
  - There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency has been examined. The focus here is on the level of business disruption which could arise from each type of disaster. Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power Failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

Table 6 - Example Potential disasters

- **Backup Staff:**
  - If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

M5. Discuss the roles of stakeholders in the organization to implement security audit recommendation.

- Security audit is systematic assessment of the security of the company's information system by measuring its relevance with an established set of criteria. A thorough audit often assesses the security of the system's configuration and physical environment, software, information processing processes and user practices. Security audits are often used to determine regulatory compliance, by law (such as HIPAA, Sarbanes-Oxley Act and California Security Infringement Information Act) that specify how organizations must handle information. believe.
- In order to accomplish the purpose of collecting information of businesses, it may need support from third parties to analyse data, market and support customer service and/or provide better services to customers. In the information security process of the business and the following stakeholders will support the process:

STAKEHOLDERS	ROLE
Server manager	A person who constantly monitors and controls the data of the business (meeting requirements, incidents, repairs, ...).
Branches	Affiliates will support each other for security audits to increase security for businesses.
Business Partners	As a second party that cooperates with businesses and helps businesses audit security, two units will work together to comply with security policies.
Customers	Are people who interact with businesses through VPN, and who make requests, report incidents to overcome the system.

Table 7 - Roles of Stakeholders

Recommendation:

- **<u>Server manager, Branches:</u> Server managers need to follow security measures such as:**
  - APPLICATION SECURITY SOLUTION
    - Solution for Web application firewall (Web application firewall - WAF) (**Benefits** - allows to prevent attacks on Web applications, continuously monitoring Web application system and providing warnings if appear vulnerabilities in the application.)
    - Solution against counterfeiting transactions (Fraud detection) (**Benefits** - Preventing acts of forging users, appropriating and using payment accounts on electronic payment environment, e-banking.)
  - DATA SECURITY SOLUTION
    - Database system security monitoring solution
    - Data encryption solution (**Benefits** - Protecting sensitive data in encrypted forms: encrypting folders, files, hard drives, ...)
  - NETWORK SECURITY SOLUTION
    - UTM multi-purpose firewall solution (**Benefits** - Protecting system ports (gateways), preventing risks from the Internet environment.)
    - Solution of anti-intrusion and anti-denial of service (DDoS) attacks (Benefits - Specialized devices to prevent DDoS attacks.)
    - Solution to detect security vulnerabilities (**Benefits** - Identify, monitor and offer solutions to address security vulnerabilities across the network, servers, operating systems, databases and applications.)
    - Gateway spam / virus prevention solution (**Benefits** - Dedicated solutions to prevent email spam forms, prevent viruses.)
    - Network encryption and security solutions (**Benefits** - Dedicated solutions to protect connections between sites in the same system, especially suitable for businesses with many branches and high security requirements on the road transmission.)
    - Solution to monitor and analyse malicious code (**Benefits** - Identify the types of malicious code that are present on the system, integrated with the system malicious gateway level solutions.

- SECURITY SERVICES:

In addition to the above set of security solutions, HPT also provides network security services with the following contents:

- **Black-box:** Assume that an attacker (hacker) does not know the information about the enterprise's system and proceeds to attack components of the system.
- **White-box test:** Assume that hackers are provided with complete system information such as system diagrams, list of operating applications and operating systems.
- **Gray-box verification:** Suppose a hacker is provided an account as a regular user and attacks the system as an employee of an enterprise.

➢ **Business Partners:**

- SECURITY CONSULTING SERVICES
  - Total security advice (Total security consultant): HPT will conduct a comprehensive system survey, detailed analysis of risks and information security risks, so that overall advice on security as well as security investment roadmap suitable to the system of customer.
  - On-demand security advice (On-demand security consultant): Depending on the specific needs of the customer (for example: needing advice on terminal security, application security or system gate level protection, ...) HPT will examine and analyse system components in detail. related, thereby consulting in detail the security solutions / services to be deployed to help meet the security needs of customers.

➢ **Customers:**

- Customers who use the services include surveys and assess the following information:
  - System connection model.
  - Basic network equipment (Router, Switch, ...)
  - Network security software and devices (Firewalls, attack detection and prevention systems, VPN systems, etc.)
  - Data backup and recovery system

- **Example stakeholders in ISP development.**
  - **User Community:** The User Community for any organisation consists of individuals (and groups of individuals) who carry out a variety of diverse functions. ISP literature tends to group the User Community under a few banners, the most popular being "end users". Other terms used in the security literature include Computer Users, User Community, Data Entry Staff, Data Processors and Information Collectors (Szuba 1998).
  - **ICT Specialists:** The ICT Specialist is usually one of the driving forces of the ISP development process. As a result, the ICT Specialist role is highly represented in the ISP development literature. In practice the ICT Specialist may come from several varying roles dealing with the management of an organisation's computing infrastructure. These roles include (but are not limited to) Technical Computer Specialists, the System Designer, IT Specialists, the System Administrator (Swanson 1998), IS Professionals (Anderson Consulting 1999), IT Department personnel (Woodward 2000).
  - **Security Specialists:** The Security Specialist role within an organisation has often been played by someone in IT as an adjunct to their main organisational role. More frequently, however, medium to large organisations are employing people in roles focusing on protecting the organisation's information, and on the development of security policies. The use of people in these roles in the ISP development process ranges from the management of the complete process, through to consulting them for ideas and advice regarding security initiatives. This stakeholder role should be intimately familiar with security matters but may not know about the full inner workings of the computer systems and communications within the organisation. Often this stakeholder will be placed in charge of the ISP development process (Diver 2007).
  - **Human Resources:** In an ISP development lifecycle Human Resource involvement is paramount to ensure that the policy meets standard organisational practices. The focus of Human Resources will be on the consistency of the ISP with the organisational standards, equity of the policy and on training. They will ensure that the process includes a duty of care to ensure that all employees are aware of the ISP and understand how the policy may affect them. Anderson Consulting (1999) suggests that Human Resources will be involved in the development process to ensure that adequate communication channels throughout the organisation are formed to

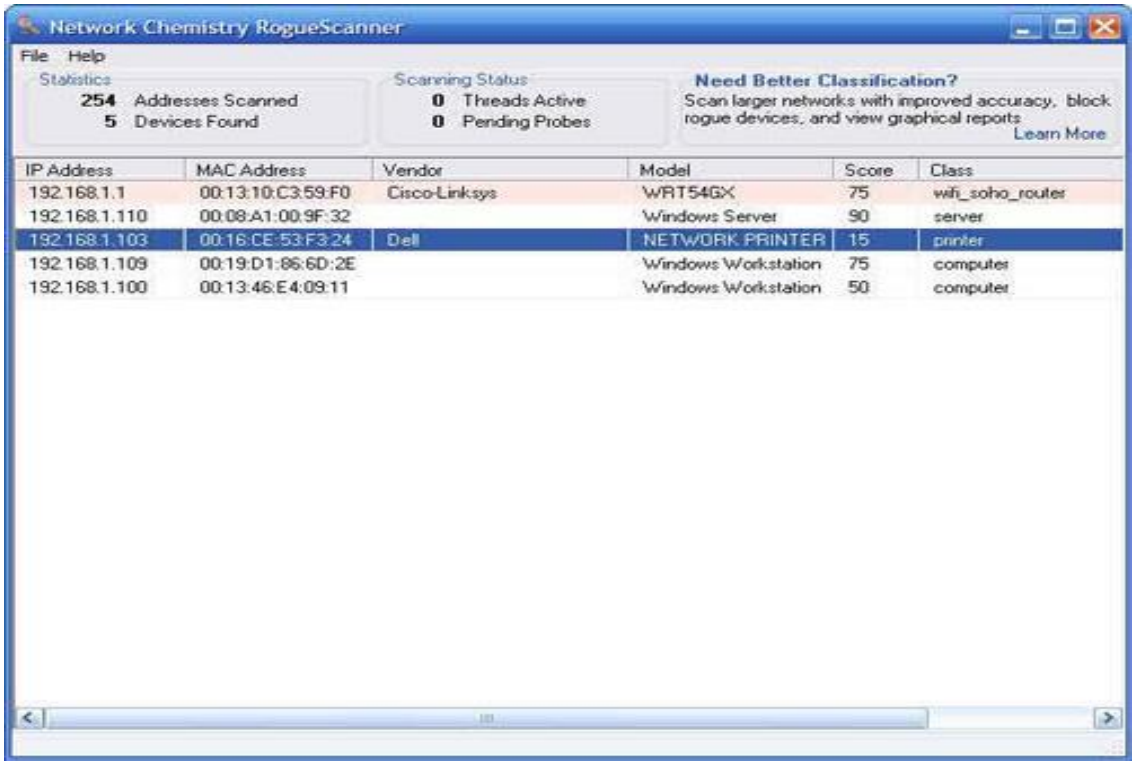
communicate the ISP and to ensure that employees can "comment" on the policies if necessary. Also, issues such as changes to job descriptions, motivation, training and policy enforcement, or policing, will be important roles for Human Resource representatives to be involved with throughout the lifecycle of the ISP.

- **Executive Management:** As with any initiative at the strategic level it is important to involve senior management in that initiative for it to succeed. In ISP development the involvement of senior management is a key success factor in the development and implementation of policy. This is also echoed by many other researchers who state that corporate management must be involved in policy development. This is further emphasized in terms of the success of development: "Successful implementation of a meaningful information security program rests with the support of top management" (State of Oregon 1998).
- **External Representatives:** In many cases for organisations it may be necessary on occasion to involve other people not mentioned previously. For instance, for some organisations it may be necessary to involve customers, suppliers and other external entities. Baskerville (1988) suggests that outside clients who are dependent on organisations systems should be involved in ISP development. Also, where there are strong strategic links between organisations the second organisation may need to be consulted in ISP development. For instance, a major retailer might develop a policy which may impact all their suppliers who are directly linked to the retailer 's computer systems for order procurement, warehousing and distribution. Failure to consult with their suppliers may cause problems in ongoing strategic relationships between the organisations (Bowersox et al. 2002).
- **Public Relations:** An interesting stakeholder role that organisations are beginning to involve in the ISP development process is the Public Relations group within the organisation (Anderson Consulting 1999). As security becomes more of an issue for an organisation the Public Relations stakeholders need to show the public that the organisation is committed to security. This is extremely important if the organisation has a security incident. It is expected that this stakeholder role will only be present within large organisations.

D3. Evaluate the suitability of the tools used in an organizational policy.

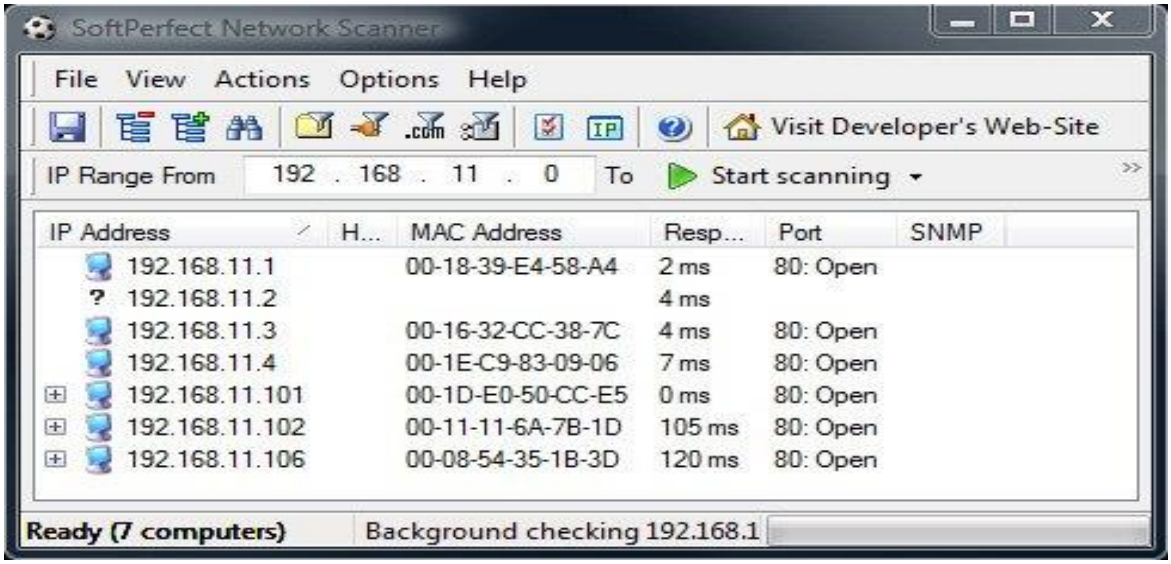
The tools used in organizational policy meet the requirements of organizational policy and do not conflict with any other policies. The tools ensure the functions suitable for the security and operation of the organization. In addition, tools can find security holes, thereby improving policies in the organization.

➢ **RogueScanner:**

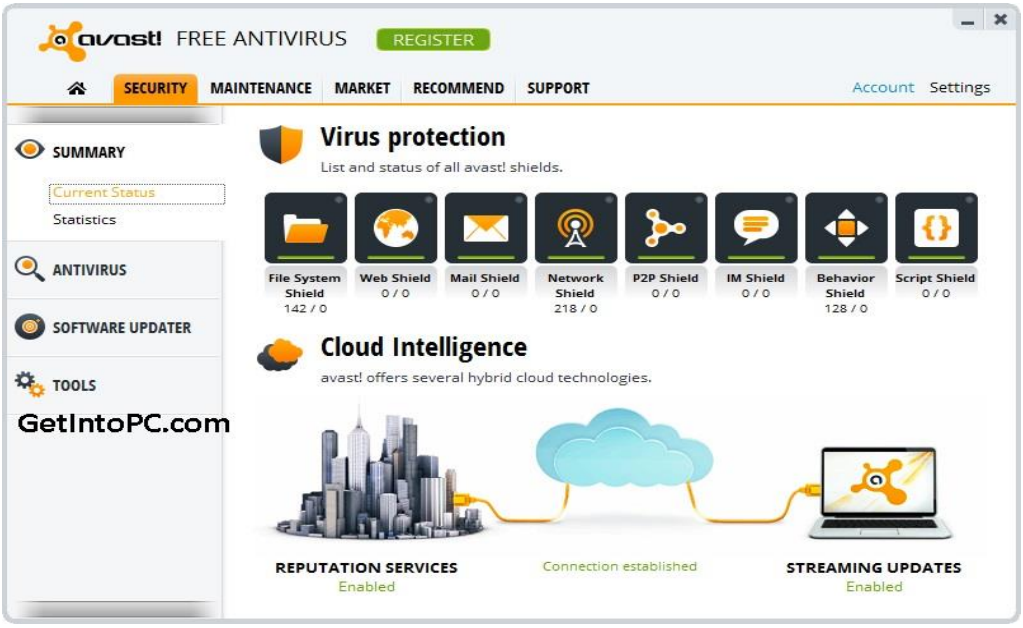


- Allows you to be able to turn on and check, track whether someone is accessing your Wi-Fi, network, computer.
- When using this tool, you will see list of IP addresses and devices connected to your network.

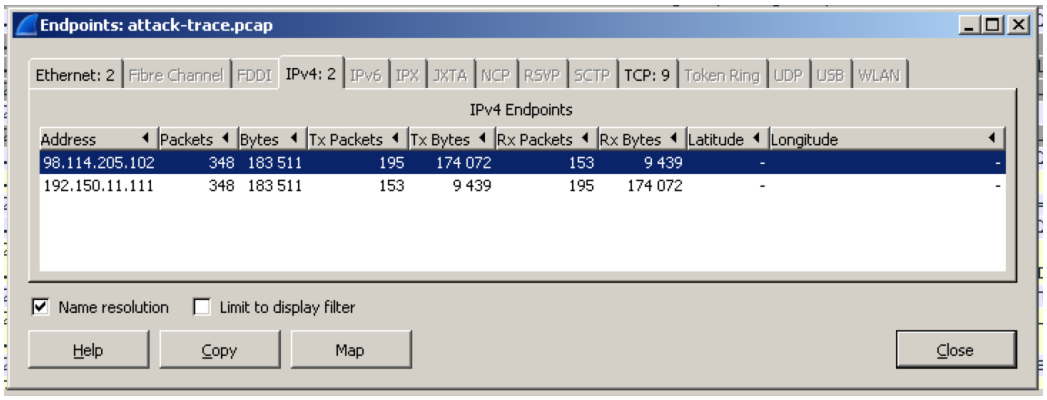
- **SoftPerfect Network Scanner:**
  - This tool allows us to control and ensure network security. check which server is safe.



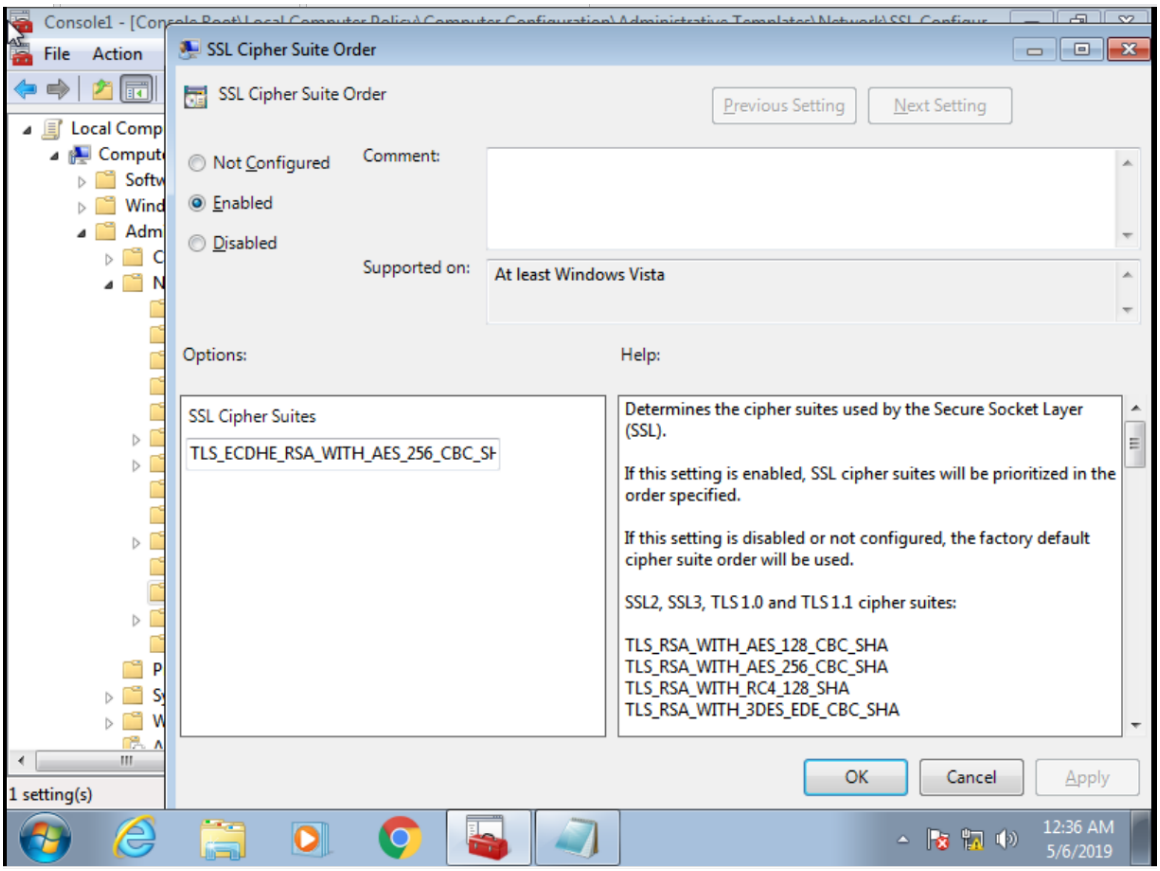
- **Avast Home Edition:**
  - Avast Home Edition is anti-virus software to ensure computer safety, avoid virus intrusion from files, links that are stuck through connecting to the network.
  - Avast Home Edition to kill viruses for PC. With the ability to scan the entire system, files, data in the computer and detect, eradicate hidden viruses in the laptop professionally



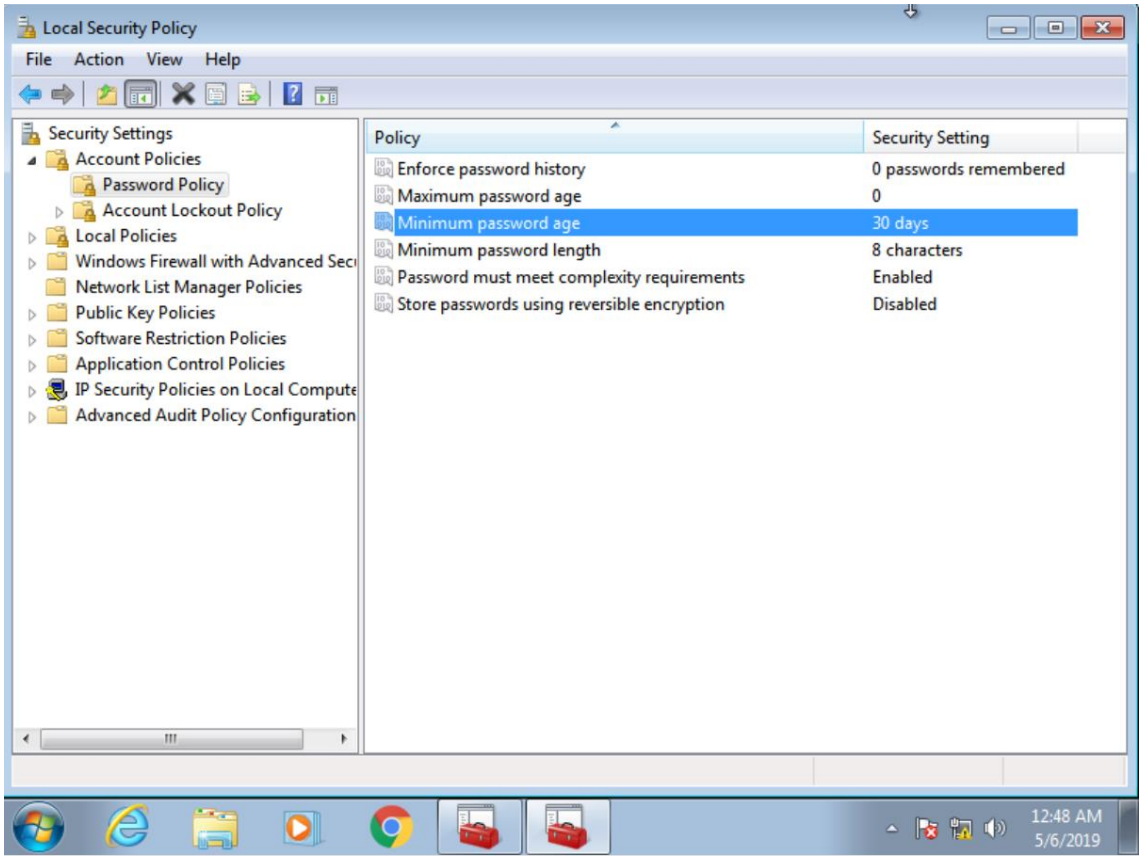
- **Attack Trace:**
  - The tool supports us to avoid those who want to invade our system and insert many malicious codes into the system
  - This tool will be very suitable for our system.

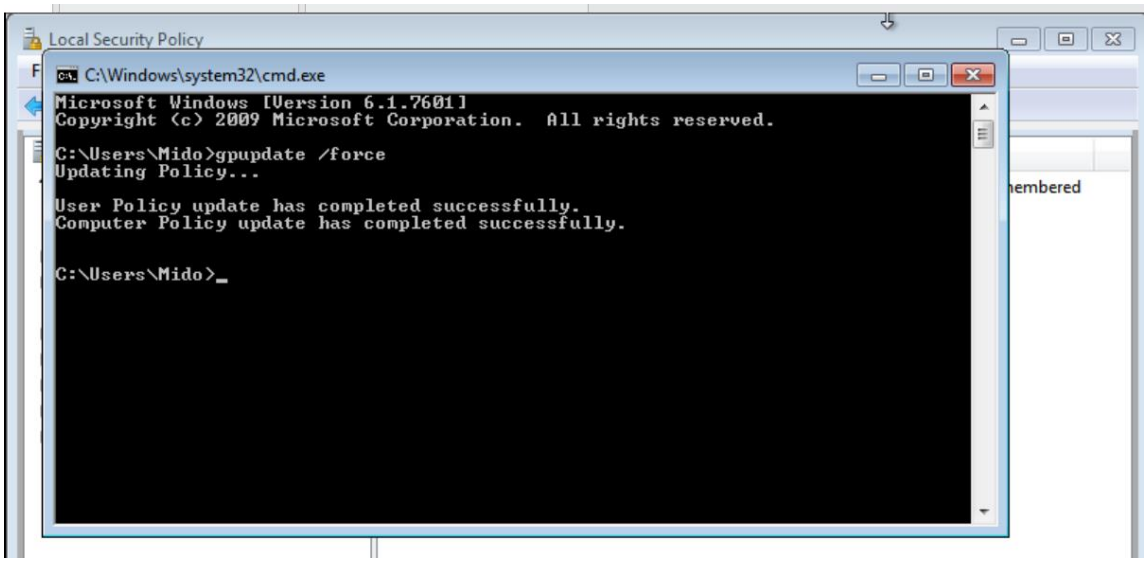


- **Windows LGP (Local Group Policy):**
  - The Local Group Policy Editor is a Microsoft Management Console (MMC) snap-in that provides a single user interface through which all the Computer Configuration and User Configuration settings of Local Group Policy objects can be managed.
    - Computer Configuration Administrators can use Computer Configuration to set policies that are applied to computer, regardless of who logs on to the computers. Computer Configuration typically contains sub-items for software settings, Windows settings, and administrative templates.
    - User Configuration Administrators can use User Configuration to set policies that apply to users, regardless of which computer they log on to. User Configuration typically contains sub-items for software settings, Windows settings, and administrative templates.
  - By default, policies set in the Local Group Policy Editor are applied to all users unless you apply user policy settings for administrators, specific user, or all users except administrators.

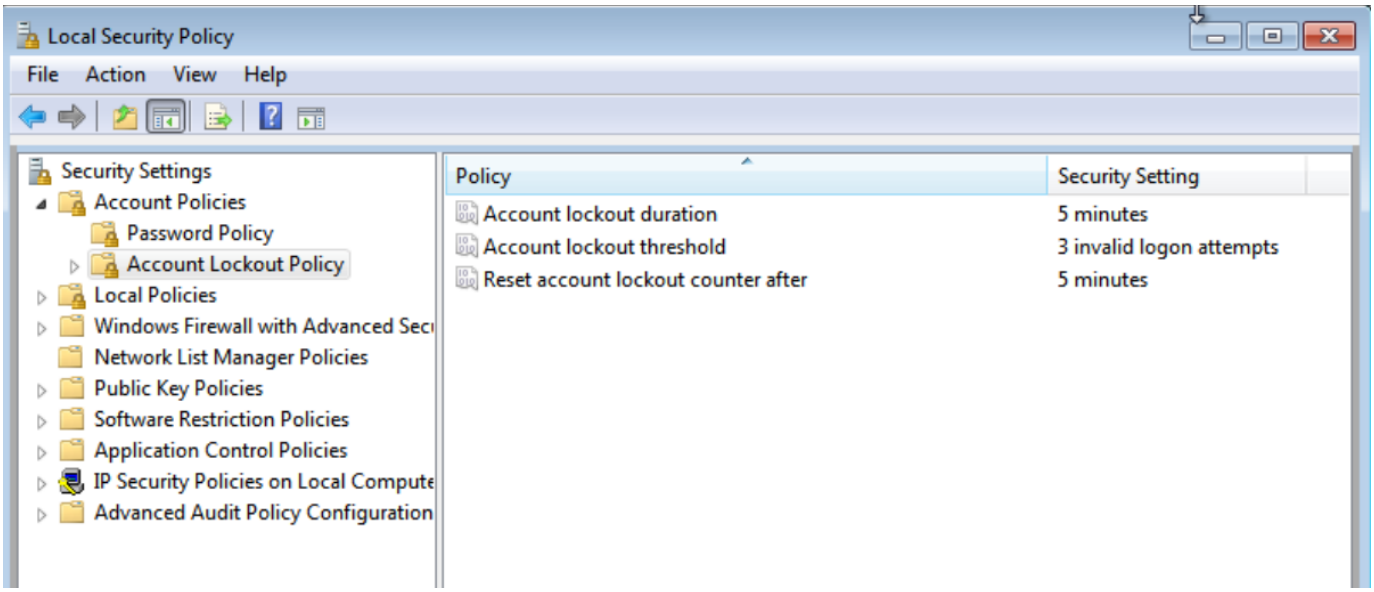


- **Use "Local Security Policies":**
  - Set up complex password policies:
    - Password length: 8 characters
    - Password age: 30 days.

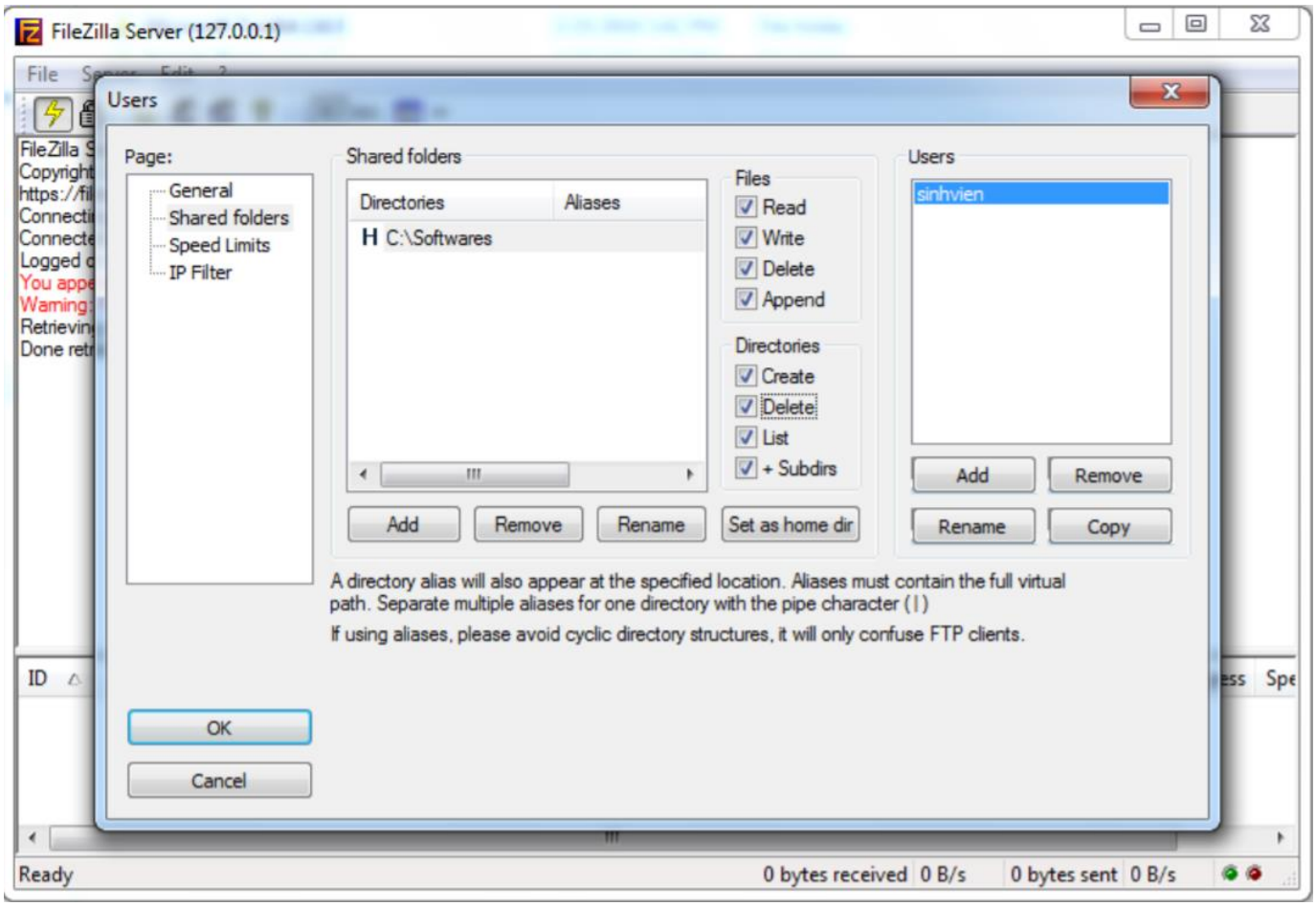




- Set up a computer lock policy after 3 incorrect entries of the login password:

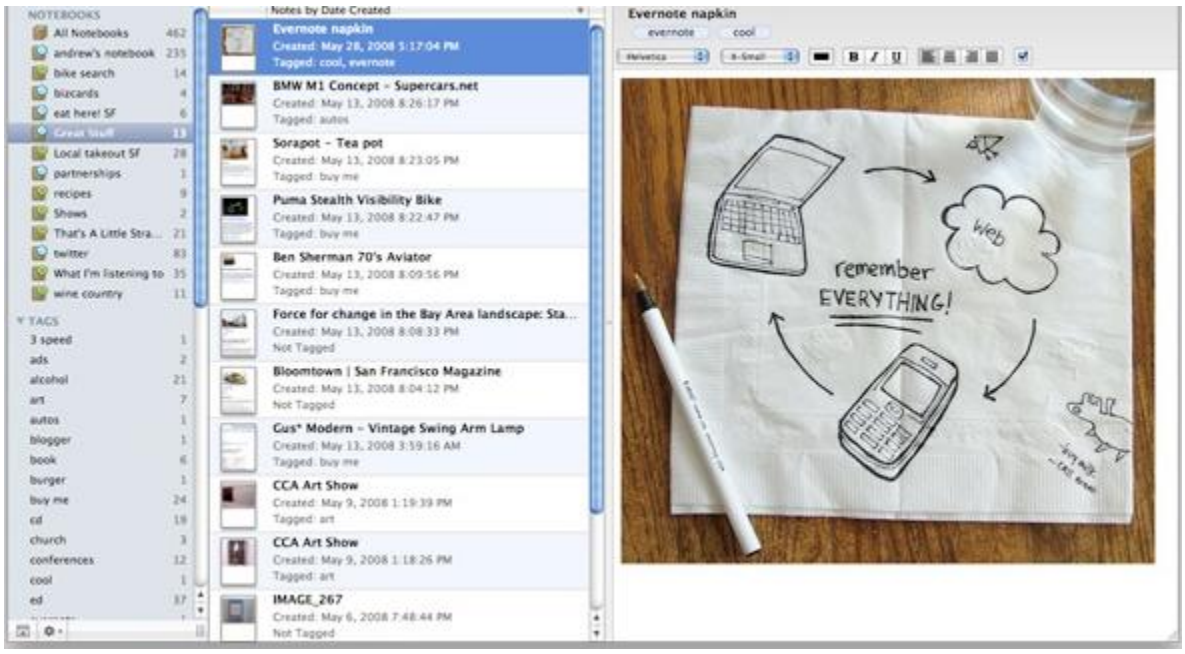


- **Secure FTP server with SSL / TLS with FileZilla Server:**
  - FileZilla FTP Server is a free and open source application for Windows operating systems, supporting secure FTP and FTP connection protocols via SSL / TLS to the server. When using the SSL protocol, we can encrypt the connections between hosts to ensure the amount of data is transmitted securely, while the application also allows users to choose multiple addresses and different server ports.

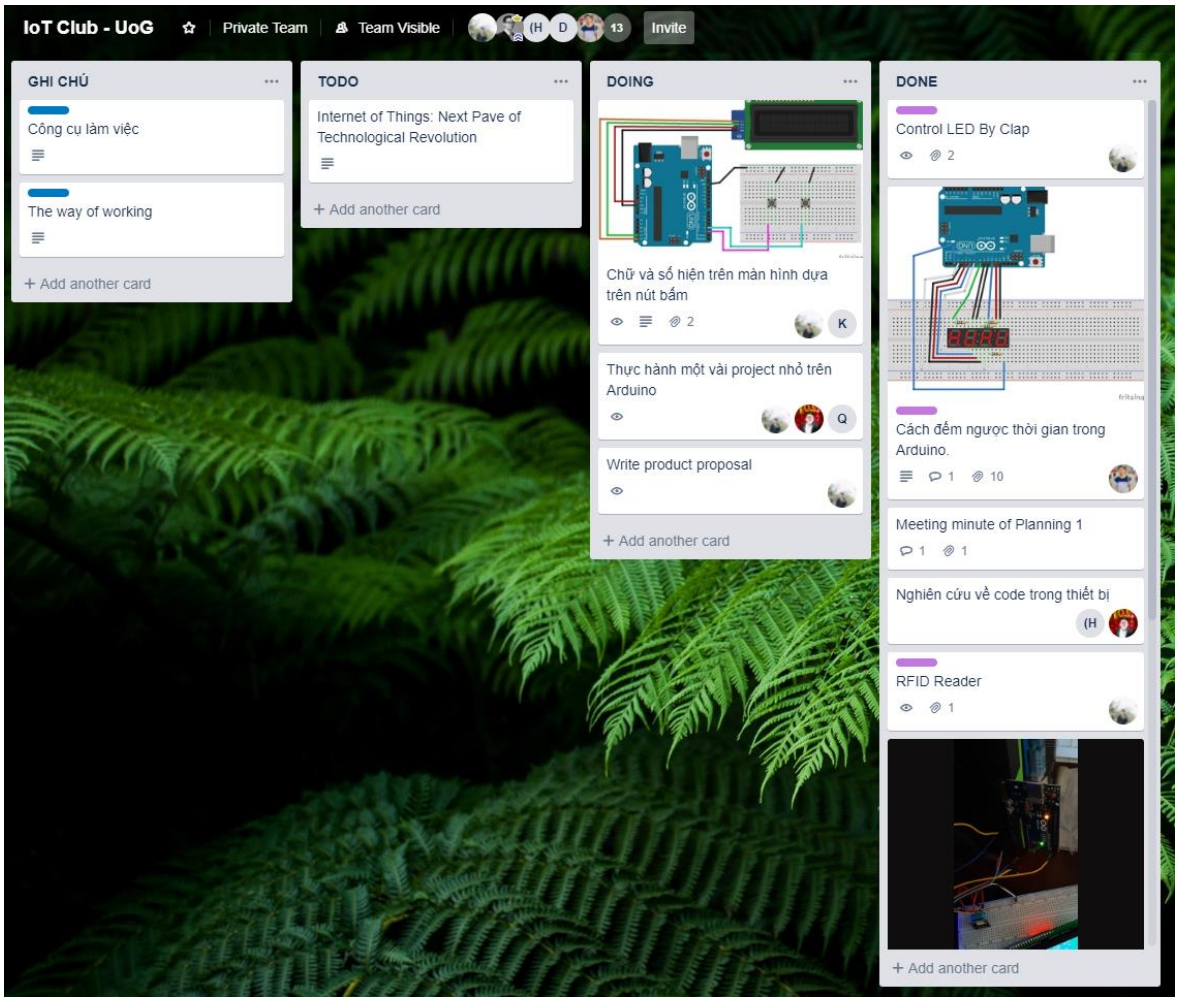


Some Tools can be used in the organization and meet security policies:

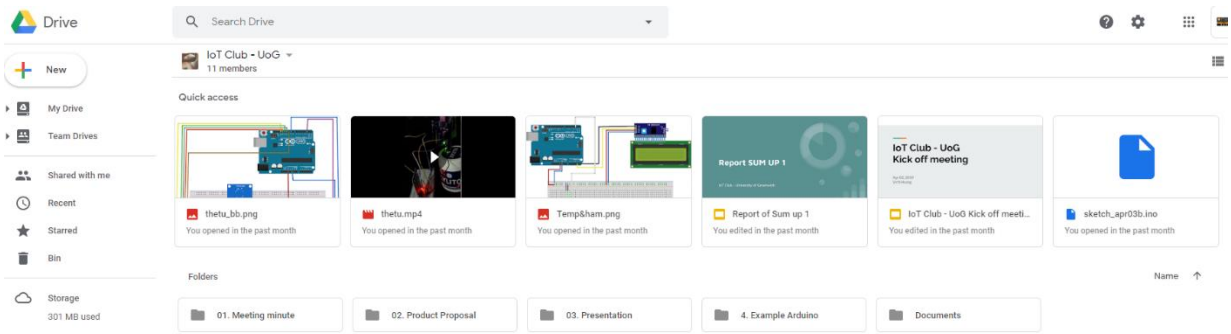
- **Evernote:**
  - Evernote is one of the better-known apps for note-taking and organizing information. I most often use it for organizing research and interview notes, drafting blog posts and eBooks, saving articles to read later, and storing important information - like my favorite code snippets - for easy access.
  - The best part about it is that it syncs across all your devices. So if you think of your next big campaign idea when you're out with friends, all you have to do is whip out your smartphone, open Evernote, and either jot down your idea, record your idea with its audio recording feature, or even take a picture.



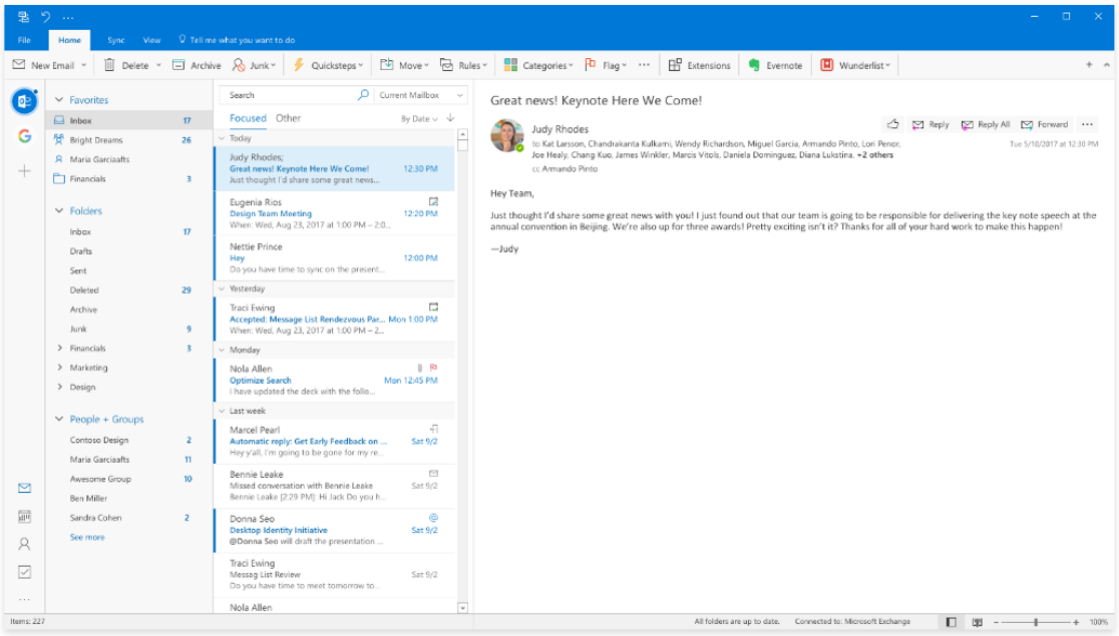
- **Trello:**
  - Trello is a well-known app that's especially good for tracking and visualizing the progress of your ideas. Using their card-based layout, you can create a card for every idea and then jot notes in there, organize these ideas into categories or lists, create task lists and checklists within cards, color-code them, attach files, and so on. To track the progress of that idea, simply drag and drop the card into a new location.
  - For example, I used to drag and drop blog post ideas among columns, which I named "Idea Backlog," "In Queue," "Research/Interview Stage," "Draft in Progress," "In Editorial," "Scheduled," and "Published." Okay fine, the last one was called "DUNZO." To each her own.



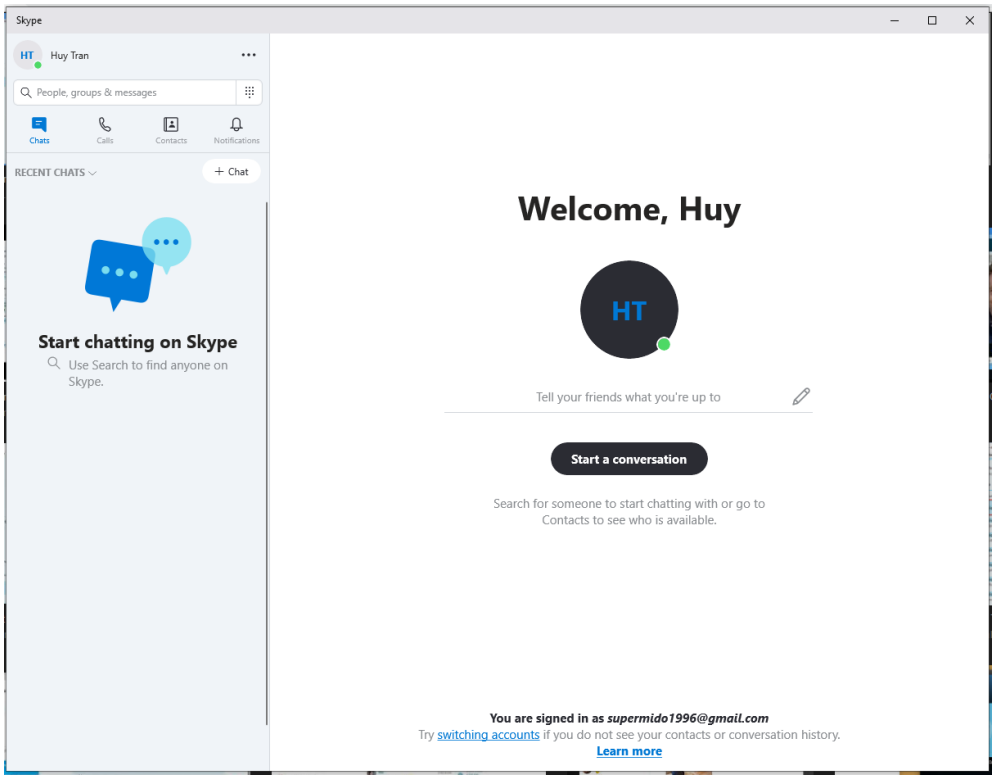
- **Google Docs:**
  - While Google Docs can be a great note-taking tool thanks to its familiar, document-style layout, its best features are the ones related to collaborating with others. It's super easy to share files, and multiple people can edit the same file -- even at the same time and in real time.
  - There are a few, lesser-known features in Google Docs related to collaboration. For example, if you want to ask questions about, make notes in, or highlight changes you've made in a Google Doc you're working on, you can leave comments directly in the document. The comments can act as a conversation thread, as people can reply to them and carry on a conversation.



- **Microsoft outlook:**
  - All email, calendar, contacts are all in the same place: Work effectively with email, calendar, contacts, tasks and more — in one place. Office integration lets you share attachments right from OneDrive, access contacts and view LinkedIn profiles.
  - Security you can trust: Rest assured with enterprise-class security trusted by the largest organizations in the world. Outlook works all the time to protect your confidential information without hindering you.
  - Information suitable for you: Outlook predicts your needs. Payment of bills and travel has been added automatically to your calendar, with smart reminder to help you track progress. The Search feature helps you quickly find information.



- **Skype:**
  - Skype is a peer-to-peer Internet telephone network founded by Niklas Zennström and Janus Friis, who also founded the Kazaa file sharing application and Joost's peer-to-peer TV application. It competes with existing open VoIP protocols such as SIP, IAX, and H.323. Skype Group, which was acquired for $ 2.6 billion by eBay in September 2005, is based in Luxembourg, with representative offices in London, Tallinn, Prague and San Jose, California.
  - Skype has grown rapidly in both the number of users and software development since its launch, both free and paid services. The Skype communication system stands out thanks to features in many areas, including free video and voice conferencing, the ability to use peer-to-peer technology to overcome firewall and NAT issues. Use strong and transparent encryption technology and powerful capability against software or protocol decomplication.



CONCLUSION

Internet connectivity, email and the web, now vital for small business, pose many risks to computer systems and the privacy of the company's data. The onslaught of viruses, worms, and Trojan horses, compounded with the increasing problem of spyware, adware, and blended threats continue to attack an organization's network through multiple methods.

Network security is an important concern that must be seriously deliberated. The number of attacks rises day by day as the use of the Internet becomes increasingly popular and more people become aware of some of the vulnerabilities at hand. Network administrators need to watch out continuously for new attacks on the Internet and take the appropriate actions and precautions.

Without effective network-defense and disaster-recovery practices a business is constantly at risk. Defense requires continually updated products such as AntiVirus or Firewall, and a well-defined outbreak-response plan to identify and deal with this ever-expanding problem. AntiVirus and Firewall provide an effective barrier against security risks and threats, facilitating their identification and removal, and protect sensitive and private company data. Without this protection, companies might find themselves faced with an administrative nightmare, including time consuming and costly full system reloads to recover lost data.

Bibliography

ACADEMY, B. L.-2. (2009, 7 2). *QUẢN TRỊ RỦI RO IT TRONG DOANH NGHIỆP HIỆN ĐẠI*. Retrieved 7 2, 2009, from https://infochief.com.vn: https://infochief.com.vn/blog/quan-tri-rui-ro-trong-doanh-nghiep-hien-dai.html

armstrongadams. (n.d.). Retrieved from armstrongadams: http://www.armstrongadams.com/solutions/?c=organisational-policy

BenSanders. (2017, June 16). *Information Security Awareness: Identifying Security Threats and Vulnerabilities*. Retrieved June 16, 2017, from https://www.digitalcraftsmen.com: https://www.digitalcraftsmen.com/information-security-awareness-identifying-security-threats-vulnerabilities/

cheekymunkey. (n.d.). Retrieved from cheekymunkey: https://cheekymunkey.co.uk/what-is-an-it-security-audit/

clickssl. (n.d.). Retrieved from clickssl: https://www.clickssl.net/blog/it-security-audit-best-practice-to-perform-security-inspection

continuingprofessionaldevelopment. (n.d.). Retrieved from continuingprofessionaldevelopment: https://continuingprofessionaldevelopment.org/risk-management-steps-in-risk-management-process/

Horan, M. (2017, 03 15). Retrieved from https://www.ftptoday.com/blog/main-types-of-computer-security-threats-that-harm-your-company Martin Horan

ins2outs. (n.d.). Retrieved from ins2outs: https://ins2outs.com/implement-information-security-management-system/

isaca. (n.d.). Retrieved from isaca: https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=698

McConnachie, L. (2019, Mar 19). *10 Cyber Security Threats In 2017 That You Can't Just Ignore... [How Vulnerable Are You?]*. Retrieved Mar 19, 2019, from https://purplegriffon.com: https://purplegriffon.com/blog/10-cyber-security-threats-in-2017

microsoft. (n.d.). Retrieved from microsoft: https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/

nccoe. (n.d.). Retrieved from nccoe: https://www.nccoe.nist.gov/forum/energy-sector-identity-and-access-management-es-idam-build-architecture

protectivesecurity. (n.d.). Retrieved from protectivesecurity: https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx

RAY DUNHAM (PARTNER | CISSP, G. G. (2018, March 14). *Security Procedures – How Do They Fit Into My Overall Security Documentation Library?* Retrieved March 14, 2018, from https://linfordco.com: https://linfordco.com/blog/security-procedures/

researchgate. (n.d.). Retrieved from researchgate: https://www.researchgate.net/publication/50367393_Design_and_Implementation_of_a_Network_Security_Model_for_Cooperative_Network

sagedatasecurity. (n.d.). Retrieved from sagedatasecurity: https://www.sagedatasecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment

Schiff, J. L. (2015, JANUARY 20). *6 biggest business security risks and how you can fight back*. Retrieved JANUARY 20, 2015, from https://www.cio.com: https://www.cio.com/article/2872517/6-biggest-business-security-risks-and-how-you-can-fight-back.html

study. (n.d.). Retrieved from study: https://study.com/academy/lesson/trusted-network-solutions-environment-technologies.html

Sumesh Kumar, A. B. (n.d.). *microsoft*. Retrieved from https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/

veracode. (n.d.). Retrieved from veracode: https://www.veracode.com/security/guide-data-loss-prevention

wikipedia. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Virtual_private_network

wikipedia. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Network_monitoring

wikipedia. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Microsoft_Network_Monitor

wikipedia. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Third-party_management

zmc. (n.d.). Retrieved from zmc: http://zmc.mk/en/about-us/guidelines-instructions-standards-and-policies/