



RESEARCH AND CASE SCENARIO IN DATA SECURITY AND COMPLIANCE

Module code: ACCA5034

Abstract

Technologies that will help improve the security of a company's network have been discussed. These technologies include firewalls, VPN's and intrusion detection prevention systems. It is important to understand how these technologies work because then you can understand how they can be implemented into a network. Different options may be more viable so they will all be discussed.

Thomas Reynolds (2305662)

Data Security and Compliance:

Assignment 1

Task 1 - Security technologies, Intrusion Detection and Prevention Systems

For companies to ensure security on their network they need implement security technologies. Important data resides on the network which includes client's data and workers data. If a company suffers data loss, there could be a lot of financial and reputation damage. However, these technologies need to be set up to allow customers and clients to access the network but not enough privileges where an attack could be formed. Some of these technologies include firewalls, access controls, VPN'S, etc. These should be configured with the companies' goals in mind otherwise they may interfere with the work that is being done.

One of the most important of these technologies are firewalls. This is a combination of hardware and software that is used to filter unwanted traffic that flows in and out of the network. There are different firewalls that operate on different levels of the OSI model. However, they all work in the same way where there are rules set in place that will block unwanted and potentially dangerous traffic coming into the network. Without this there would be no restrictions on what could be sent into the network, meaning many attacks could be formed. The firewall could be on a separate computer system, a software service running on an existing router or server and a separate network containing supporting devices.

The different firewalls are MAC firewall, packet-filtering firewall, SPI firewall and application layer proxy firewall. [1] The MAC firewall operates on the physical and data link layer. This firewall filters packets based on their ACL entries which ties into the MAC addresses of the device. Packet filtering operates on the network layer of the OSI model. Predefined rules are given to the firewall, any packets that go against these rules will be blocked. Rules are usually based on IP addresses and port numbers. The SPI firewall operates on the network and transport layer. SPI stands for stateful packet inspection and filters packets but does is different to the previous example. This is because it does not block traffic based on predefined rules, but it looks at the context of the incoming traffic. An example is recognising that one IP address sending an overwhelming number of packets is irregular and probably an attack. The previous firewall wouldn't block those packets because there is nothing inherently dangerous about them, however this firewall can recognise that it's part of a DDOS attack and then close the appropriate ports. [2]

The application layer proxy firewall operates on the session, presentation and application layers. [3] This firewall filters messages at the application layer and can be installed on a networks server but can also be a remote server.



The image above shows how this firewall is used between networks. This firewall can be used to make sure unauthorised users don't have access to all parts of the network. Another use is restricting access to certain sites, organizations may use this to stop employees from going on social media during work hours. Proxy firewall has its own IP address, meaning external packets do not go straight to the network. Without this firewall any user who accesses the network would have no restrictions on what they could do. Meaning many attacks could be formed on the network and data theft can occur.

A hybrid firewall is a combination of multiple firewalls.[4] This will ensure that the environment is very secure, this is because there are firewalls on different levels of the OSI model. You can have more control over your network, for example the SPI firewall can help defend against a denial-of-service attack and the proxy firewall can be used for content filters. Different firewalls can be designated for different type of threats. Hybrid may be the best option for a network but there are disadvantages. One being the configurations will take a long time to implement. Also, the network will become more complex which may create problems when maintaining the security of the network.

When choosing what firewall is best for the scenario there are different factors that need to be considered, one being the price. You need a secure firewall, but you do not want to waste money on a firewall that is too expensive to keep. And are there better alternatives that also cost less. If there are no staff or team members that can set up and configure the firewall, that may be another factor to consider. Also, as time goes on the network may change and adapt. Which means you need a firewall that can do the same.

Access control determines who can access a certain resource and who cannot. There are different types of access controls, mandatory access controls, discretionary access

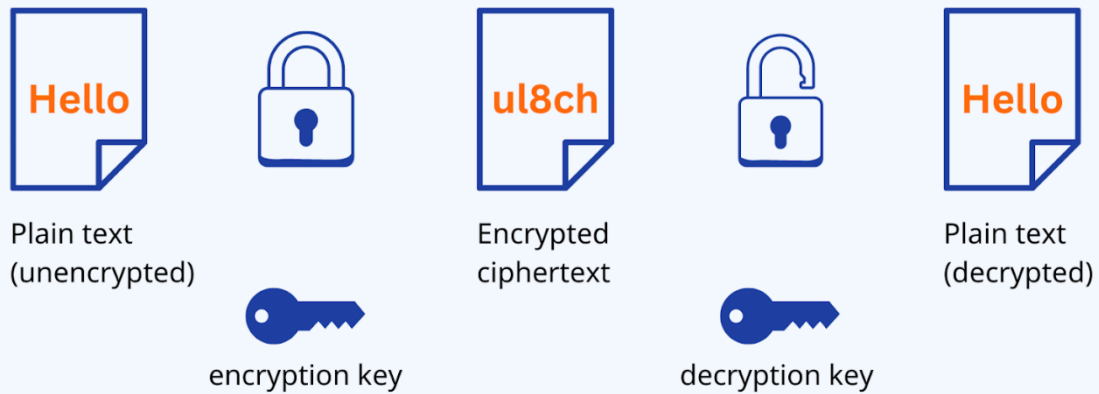
controls and nondiscretionary access controls. Not all users should have complete access to a network or resource, because some people will have ill intent. Access controls ensure only the people that should have access to a certain resource have access by proving they are the user they say they are. With each type of access control there are four functions that show the system you are who you say you are. These functions are identification, authentication, authorization and accountability.

Identification and authentication is when you show the system you are a user and that you can prove you are a user of the system. This usually with a username and password, some other systems require two factor authentication and answering a security question. Authorization is when you are given access to the network with the privileges set by the admin. Accountability is when the system can track and monitor your use of the system.

Mandatory access control is when the operating system gives you access based on data confidentiality and user clearance levels.[5] As previously said you need to enter username and password to get clearance on the system and then depending on your clearance you can then access different parts of the system. The operating system checks the username and password that has just been entered and compared them to the database, then access will be granted. Discretionary access control is when the access controls are made by the owner. For example, someone who makes a word document can choose if only they can read it and modify it, and others can read but not modify it. Another example is smartphone applications, depending on what the app is designed to do it may not have the privileges to do so. It may need the user's location or access to the phone's camera. The app then asks the user for permission to do these actions, and only when permission is granted the app can perform its actions. Some files have more sensitive data than others, meaning not all users should have access to it. This is why MAC (mandatory access control) is secure and makes sure only the ones who are supposed to see data see it. However, there are advantages to discretionary access control those being flexibility and speed. Users can set controls for individual objects quick and easy.

Moving onto VPN's (virtual private networks) which are very important when it comes to secure connections between devices. VPNs create a secure connection by encrypting your data which makes it harder for others to see your online activity.[6] This can be beneficial for individuals and organisations. Especially if you are someone who uses public Wi-Fi a lot, public Wi-Fi is unsecure as there is a lack of protection there. Attackers can make fake networks and do packet sniffing to try and steal data. VPN's can be an extra layer of security to make sure your data is not stolen. Some VPN's can mask your online identity by giving you a new IP address. It is not your actual IP address but what people would see. You can also choose to connect to many different servers around the world, so when a website looks at the IP address the VPN gave you they think you are in a different country. VPN's encrypt and decrypt using keys.

How encryption keys work



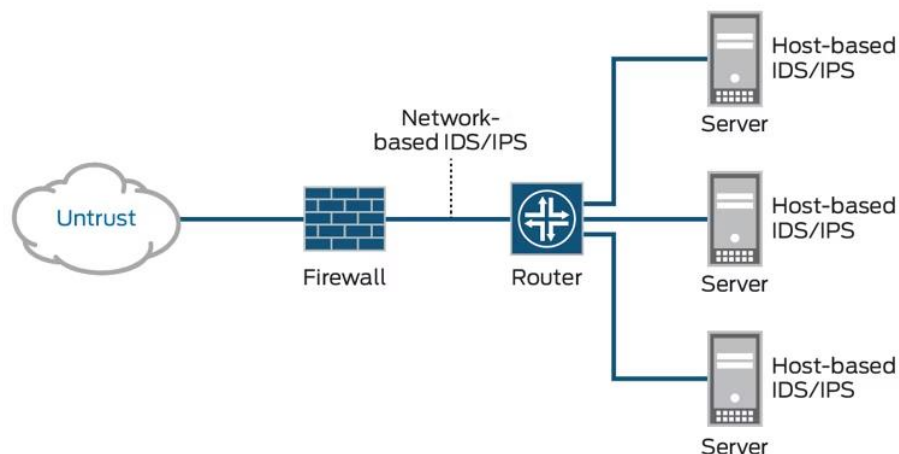
The image above shows how the process works. The encryption key turns the plain text into encrypted ciphertext. Which means if there were important data on the plain text it cannot be stolen from the cipher text. Then the ciphertext is decrypted back to plain text so it can be read. This can be very beneficial for organisations if they will be sending sensitive files over a network. Even if there was a packet sniffer monitoring the network the data would not be able to be stolen when encrypted.

There are three defined VPN's, trusted, secure and hybrid. Hybrid is a combination of the previous two. Trusted uses a providers' network, secure sends traffic over the public internet but its encrypted. Hybrid implements two of these mechanisms.

Intrusion detection consists of finding system intrusions, prevention systems is what discourage an intrusion. [7] IDPS are ways of detecting an intrusion, this can contain an attack and prevent a mass loss of data or damage. The traffic on the network is constantly being monitored which is how they can identify where attacks came from. The main purpose is to identify the potential attack and notify the administrators of the network before it happens. It can also help with the continuous improvement to the security of the network. Information is logged about the attack or potential attack. That data can be used to improve security systems to improve the overall network. For these reasons IDPS's have become a necessary part of a network for businesses. This is because business networks are always at risk of attacks because of the data they have. There are network-based IDPS's and host-based IDPS's.[8] A network based IDPS has its focus on safeguarding information assets. These can most of the time be implemented into a network with small levels of interference. However, a network-based IDPS can become overwhelmed if there is too much network volume. This means that it will then

struggle to identify attacks. It also cannot analyse encrypted packets. This shows that there are ways around an IDPS, there is not a way to make a network completely secure. With the advancement of technology new attacks will be made or new tools will be introduced to help take down or infiltrate a network. However, this is why the security of a network should always be improving to adapt to new potential threats. And IDPS's are a great tool for this.

Moving onto host-based IDPS, this system occupies a computer or server. It then monitors activity like the NIDPS but only for the host it resides in.



The image above displays where the systems are deployed on a network. The NIDPS sits between the firewall and router, this means it can monitor the traffic coming in and leaving the network. The HIDPS (host-based IDPS) resides on each server in this example. Then the activity on that server will be logged. HIDPS's can be beneficial if there are key system files stored on the system it is monitoring. So, if that file gets deleted or modified it can identify those changes. Unlike NIDPS it can access encrypted information then act on developing risks to the network. However, HIDP's do not give a truthful depiction of the network. This is because it is deployed on a singular system and only monitors the activity on that host. If there is irregular traffic elsewhere on the network the host-based IDPS will not identify it. Which is why network-based IDPS's and host-based IDPS's should both be deployed on a network. This allows for traffic of the network and key system files to be monitored.

IDPS uses different methods to identify potential misuse on the network. One of these ways is signature-based detection which is also known as knowledge-based detection. This is where the system searches the network traffic for well-known signatures. This is a very popular detection method because there are a lot of attacks that have clear signatures. If it is a common attack, it can be identified quickly and dealt with accordingly. This does mean however new patterns will have to be added to the IDPS's database, also if an attack pattern is not in the database the network is vulnerable to it. With IDPS's a lot always goes back the continuous improvement of the security, and this

signature-based detection method is a good example of this. New attack patterns will not be recognised, meaning the system must always adapt. Another disadvantage to signature-based detection method is attacks that have multiple events have the possibility of escaping detection.

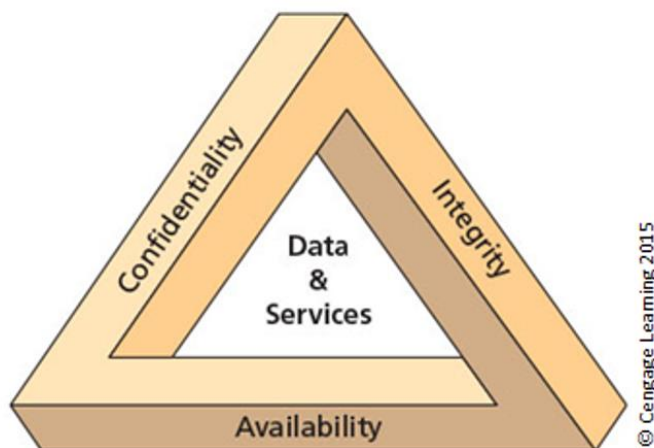
Next method is called anomaly-based detection (or behaviour-based detection.) [9] This method analyses network traffic and collects data to see what normal traffic looks like. It can see what normal traffic flow between devices should be. Then when there is traffic that goes against the normal traffic it has monitored it will send an alert to the administrator of the network. The advantage of this is that it can identify new attack patterns instead of relying on knowledge from a database. If the new attack is irregular when compared to normal traffic flow the admin will get alerted. As it is constantly comparing traffic it does more work than the signature-based method as that only looks for a pattern it has saved in a database. This means that this method needs more processing power which could put more strain on the network. Another negative is that there may be false negatives. This means activity on the network that has no malicious intent may be reported to the admin. If it slightly deviates from what the method deems as normal traffic it will lead to the admin getting reported. Which can waste time and resources if it was a false negative. So, anomaly-based detection can identify a lot more threats on a network than signature. However, a lot of them are not attacks. A lot depends on how accurate the baseline is which means it must also get updated regularly to try and decrease the number of false negatives.

Moving onto log file monitors which are like network-based IDPS. This looks at files created by servers, network devices and other IDPS's for patterns and signatures. So, it monitors the entire network for patterns that may indicate an attack. It is a demanding method as it views the network. All methods require updates to make sure they keep up with new attacks and continue to have a secure network.

Task 2: CyStresSoloution (CSS)

CyStresSoloution is a company that helps businesses defend against potential threats using methods that were previously discussed and more. It sells its services online to help combat cyber-attacks. CSS is setting up a new information security unit, there are factors that are needed for this unit to work effectively.

The C.I.A. triad (2 of 2)



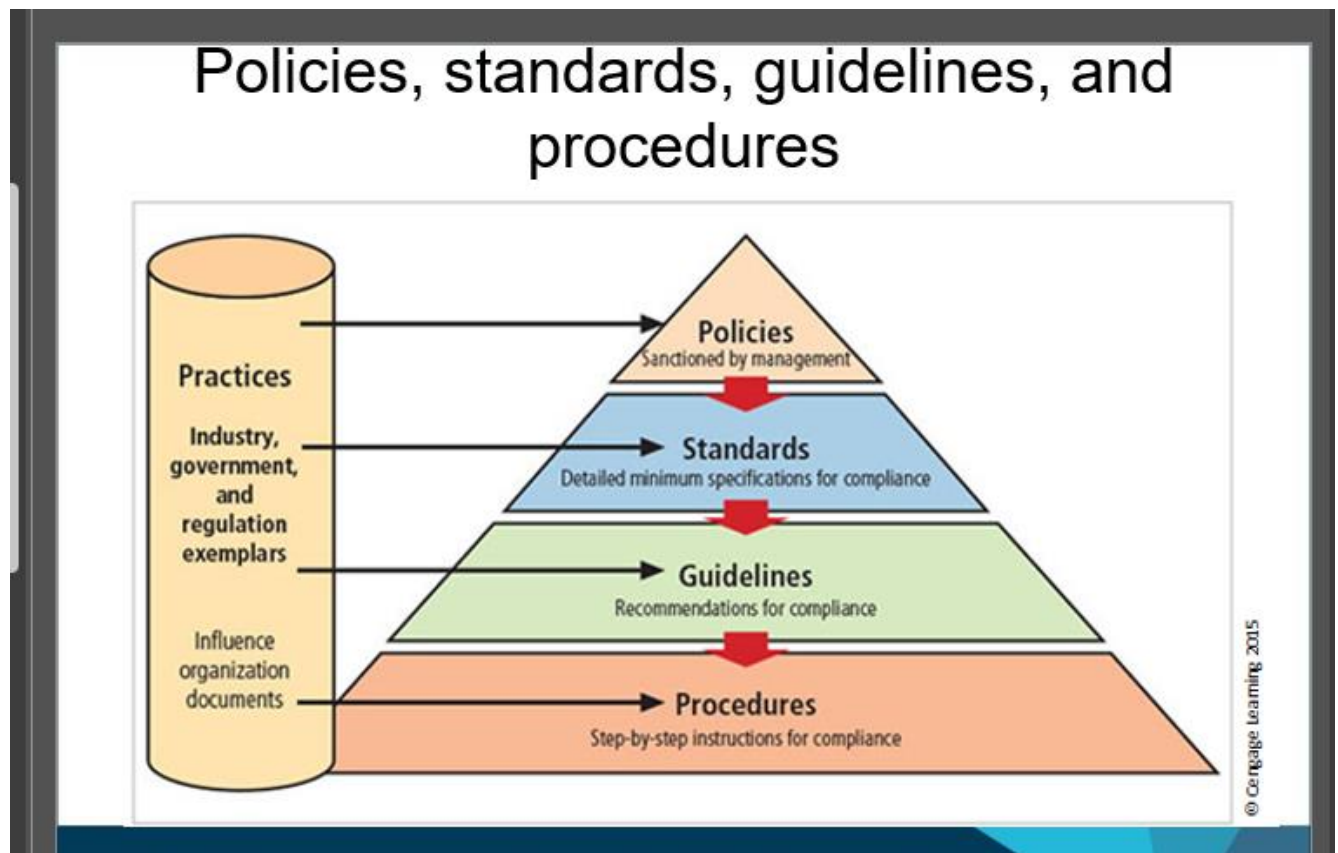
The CIA triad has three components that are integral for information security. These being confidentiality, integrity and availability. [10] This allows for assets to remain safe so they can be safely given to clients. One way to ensure this is the organisation structure. When implementing information security, a lot of thought must go into management. Things must be considered like who has access to what data and what team is responsible for identifying potential problems and reporting them.



The image above is from the Corporate Governance Task Force report which came out April 2004. In this image we can see the responsibilities which are needed for implementing information security. It then takes these roles and splits them into roles that could be used by an organisation. The roles in this example have been split into chief executive officer who oversees the overall security. On the next level you have chief security officer, chief information officer, chief risk officer and department head. This level would be responsible for setting security policies and procedures, responding to breaches and responsible for independent annual audit coordination. Then there is the mid-level manager who communicates policies and runs the program training. Then at the bottom the staff who report security vulnerabilities and breaches. So, all levels of this hierarchy have a part to play in ensuring the security of assets. Some organisations will do it differently but having a management structure is very important. You need to know who will help against ongoing threats because then you can report it as quickly as possible. You also need to know who will deal with client's issues with the system. If none of these roles are given, when an attack does occur there will be coordination between members. This allows the attacker to successfully infiltrate the system and perform a data breach.[11]

Another important component for creating a successful information security unit is policies and procedures. Policies show members how they address issues and how

technologies should be used within the organisation. These policies cannot go against the law which means they must hold up in court. If an organisation wants a policy to be effective it must be understood and agreed by all members of an organization.



This image shows how policies, standards, guidelines and procedures are used within an organisation. Policies are set by management, standards are specifications for compliance, guidelines use recommendations for compliance and procedures are step-by-set instructions for compliance. An example of the relationship between these is how organisations treat passwords. The policy may be to use strong passwords and change them frequently. Then the standard would describe what characters to use, some organisations require a minimum of 10 characters with at least one of them being a special character. Guidelines provide help by giving recommendations, which in this example may be to not use a password you have used in the past. Then the procedures give instructions on how to change your password. [12]

Policies are changed frequently meaning there must be measures to make sure they are managed correctly. One important measure is having a responsible manager. It is important to have someone that makes sure the policies are being implemented efficiently, and the intended impact is taking place. Without a responsible manager these policies may become redundant, and the organization can suffer because of this. Reviews are very important to make sure policies remain viable. Getting opinions from all members of the organisation can help see if a positive impact is taking place. If not, actions can be done to ensure the policies are improved for the benefit of all members.

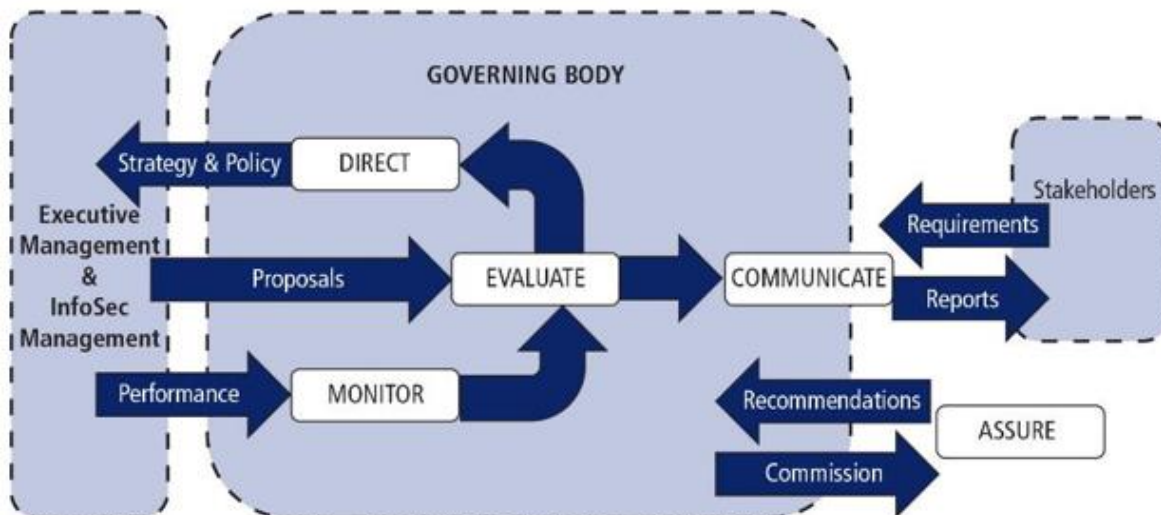
An organisation that implements effective policies and procedures can help improve the security of their system.

Next factor to discuss is compliance, which goes over laws and ethics. Companies must keep their systems secure, but they must do them in legal ways. To reduce the risk of liabilities the company must understand the current legal environment, continue to follow laws that are very present in their scenario and identify new issues that are frequently emerging. If a company has many liabilities due to poor management, then credibility and money can be lost. There are important computer laws that all companies must follow to ensure the safety of user's data. One being computer fraud and abuse act of 1986. This prosecutes users who commit cyber based crimes which are constantly evolving. These crimes consist of people using computers to steal data, gain access to a network which they are not allowed to and cause damage to systems. The National Information Infrastructure Protection Act of 1996 took many parts of the previous act and modified them. Also, the penalties were increased for certain crimes which shows computer attacks were becoming more dangerous. The change between the two acts is evidence that laws involving computers will change with time. So, if a company does not adapt with these acts they may be at risk to liabilities. An example of an organization breaking the law for financial gain is illegally selling your data.

If an organization uses payments from cards there are additional standards, they must comply to which are set by the PCI Security Standards Council. This is because holding users bank details are incredibly important and if they get stolen your company can lose a lot of credibility. As no one wishes to use a company that does not keep sensitive data safe. The standards that were addressed are as follows:

- Build and maintain secure networks.
- Protect cardholder data.
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain information security policy.

Strategic planning and governance are the next factors to consider. [13] Starting with governance, which is how the executive management run their practises and set their responsibilities. The end goal is to help supply a strategic direction for the company and its employees to follow. As well as objectives and measurements to see the progress towards those objectives. The governance's five goals are strategic alignment, risk management, resource management, performance measurement and value delivery.



This image shows how changes are communicated with different parts of the organization including stakeholders. The executive management can then monitor the performance and any changes that need to be made will be taken back to the executive management. Strategies and policies should always be monitored to see what can be updated as computers and technologies are always evolving. Meaning a company's strategies and policies from a decade ago may not hold up today as everything is always changing. Such as attacks, laws and technologies themselves. This is why the governance process is important as without a successful one no updates to the system will be made. And no one will manage resources and value delivery.

When discussing the organization structure, we looked at an example of how the governance responsibilities could be split into roles. The structure allowed for new policies to be communicated to all members. At the top of the structure, we have a chief executive officer who oversees corporate security, who can measure the performance and make changes accordingly. The next layer down is responsible for implementing new policies made by the board. Policies come up a lot when looking at an organizations structure. This is because they act as organizational laws which all members follow. Poor policies that are not updated will take the executive management further away from good value delivery.

Part of the strategic planning involves security education and training. Having strong policies is good, but having employees trained to identify potential attacks is one way to improve security.

Comparative Framework of SETA

	Education	Training	Awareness
Attribute	Why	How	What
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or False • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

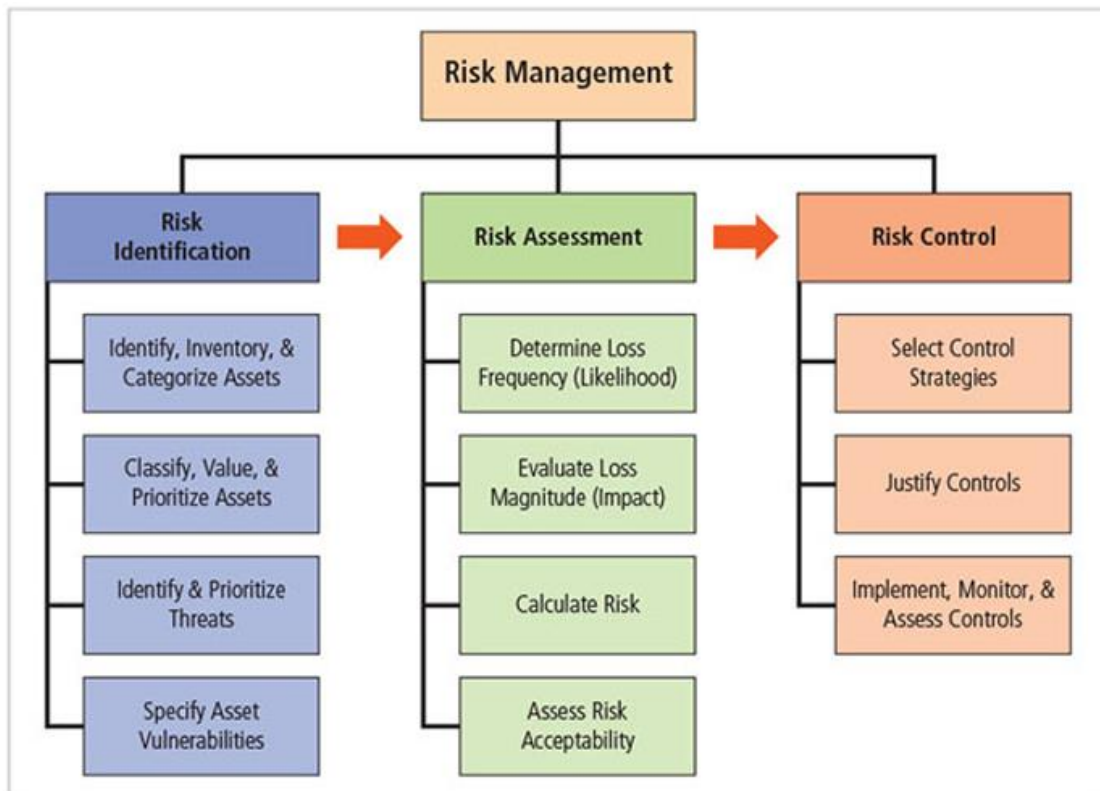
Source: NIST SP 800-12

This framework was made to help guide organizations on educating their employees. There are three different ways you can help give each member a better in-depth knowledge on security [14]. That being education, training and awareness. Awareness is easier to implement as you are only telling them what to look out for. This can be implemented using videos and newsletters then tested with true or false quizzes. Training takes a bit longer as you are developing skills, which can be developed with lectures and workshops. Then to test this you can make problem solving activities. Educating them takes the longest as they need discussion seminars, background reading and hands on practise. To test their knowledge, ask each member to provide an essay on what they have been taught. If only the executive management are educated on such threats, it is more work for them to keep the entire system safe. However, if everyone can play a part then the security is improved massively.

Another aspect of strategic planning is contingency planning. Even after trying to improve the security of your systems there may be vulnerabilities that can be exploited. This is where contingency plans come in, what do you do if a successful attack is pulled off. The concerns should be in disaster recovery and business continuity. How can the company take back what has been lost and how much downtime will there be until the systems are back and running. If this is something that is not planned for there will be a lot more damage done as the company does not know how to respond. Part of this is continuity strategies which is what is done after a successful attack has taken place. Within in this strategy is incident response plans, disaster recovery plans and business continuity plans. Incident response plan needs to be taken place as quickly as possible to avoid escalation. If it does escalate then the plan changes to disaster recovery plan and business continuity plan. Disaster recovery plan is how the organization will restore

systems after the incident has occurred. There will be downtime as systems are restored which can have effects on the business. This is why disaster recovery plans are closely linked to the business continuity plan. The business continuity plan will run at the same time as the disaster recovery plan and goes over the actions to help the business continue to run. This is very important as damage may have also been done to clients in the form of data theft. How will the business make sure this will not happen again and how can they help their clients during this time. It can take businesses a long time to recover from such incidents. However, if there are no contingency plans they may not recover at all.

The next factor is risk management. As previously stated, an organization should have plans in place for potential threats and attacks. There are three steps in how an organization can check for these risks and mitigate their potential damage. Those steps being risk identification, risk assessment. Risk identification is documentation of risks to an organization. Risk control is the act of finding ways to reduce the amount of risks and the damage caused if one of these happened. It is unlikely all risks will have been controlled by an organization, there is always something that can lead to information assets being lost. However, finding ways to reduce the damage can allow the organization to bounce back and make their systems stronger. Risk assessment is when a team checks what information assets are at risk. These risks can vary from environmental damage to hackers forming an attack on the network. Risk management is the three steps put together. It is identifying new risks and analysing the severity of their nature. To make sure that an organization successfully identifies all new risks, all staff should be trained to understand what potential risks look like. This goes back to the strategic planning where all staff should either be educated or trained to identify such risks.



This image shows how the three stages flow into the next one. By following these steps, the security of the company's systems will be improved. As you can see in the risk identification you must identify threats and specify asset vulnerabilities. In the risk assessment you must calculate the risk and evaluate loss magnitude. Then finally risk control you implement and monitor controls. [15]

An organization needs to decide how much security and accessibility they want. If they make their systems more accessible the risks are increased. This is where risk appetite is introduced, which is risks that organizations are willing to accept to allow accessibility to flow. Residual risk is how much risk there is to information assets even after current controls have been applied. The organizations should find a balance between risk appetite and residual risk for the most fully functional systems that are also secure.

Finally, the last important factor to consider is protection mechanisms. These can be implemented into the network to help better the security. Many of these mechanisms were discussed in task 1 which included intrusion detection prevention systems, vpn's and firewalls. Intrusion detection prevention systems are used to identify intrusions and attacks. There are different types of intrusion detection prevention systems, those being network based, host-based and log file monitor. Network based monitors the entire network and checks for threats. It checks the activity on the network and compares it to a database that has known attacks stored on there. If it matches the known attack, it

can alert members of the organization. The host-based is stored on a specific device and monitors the activity specifically on that device.

Firewalls filter traffic on a network, depending on how it has been configured it will block certain packets from being sent to devices on the network. It can also manage ports which can block entrance to a network entirely. If there were no firewalls, then there would be no restrictions to who can access the network including those who wish to form an attack. Firewalls can also block content from being accessed if on that network. So for example, an organisation blocking social media so workers cannot access it during work hours. The firewalls need to be configured to allow for good security, but accessibility otherwise the business may suffer. VPN's can allow for secure remote connection, so workers can access materials and resources in a secure way. VPN'S do this by encrypting your data to help defend against attackers who may be spying on your data.

Conclusion:

For an organisation to manage information security it is important to consider these factors which have been discussed. Without considering the organisation structure and how as a business you should defend against attacks then there will be vulnerabilities that will be exploited.

References:

[1] What is a firewall? Definition, Types & Business Uses, hasedout, October 13, 2020

<https://www.thesslstore.com/blog/what-is-a-firewall-definition-types-uses/#:~:text=The%20MAC%20layer%20firewall%2C%20or,layers%20of%20the%20OS%20model>

[2] Aliza Vigderman, What is an SPI-Firewall, security.org, May 30th 2024,

<https://www.security.org/antivirus/spi-firewall/>

[3] Tech Target contributor, Proxy Firewall, TechTarget, June 2021,

<https://www.techtarget.com/searchsecurity/definition/proxy-firewall#:~:text=A%20proxy%20firewall%20is%20a,proxy%20servers%20are%20proxy%20firewalls.>

[4] Frederick Avolio, Firewalls and Internet Security, the Second Hundred (Internet) Years, Avolio Consulting, Inc,

<https://avolio.com/fw2hundred/>

[5] Matunda Nyanchama & Sylvia Osborn, Modeling Mandatory Access Control in Role-Based Security Systems, Springer Nature Link,

https://link.springer.com/chapter/10.1007/978-0-387-34932-9_9

[6] Jeff Tyson, How Virtual Private Networks work,

https://www.communicat.com.au/wp-content/uploads/2013/04/how_vpn_work.pdf

[7] Uzair Bashir; Manzoor Chachoo, Intrusion detection and prevention system: Challenges & opportunities, IEEE Xplore, 12 June 2014

<https://ieeexplore.ieee.org/abstract/document/6828073>

[8] Amrit Pal Singh, Analysis of Host-Based and Network-Based Intrusion Detection System, I.J. Computer Network and Information Security, 2014,

<https://www.mecs-press.org/ijcnis/ijcnis-v6-n8/IJCNIS-V6-N8-6.pdf>

[9] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, A Review of Anomaly based Intrusion Detection Systems, International Journal of Computer Applications, August 2021

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f4179593b4b47d8be8cd97e0caced755e16fefbb>

[10] Mana Saleh Al Reshan, IoT-based Application of Information Security Triad, College of Computer Science and Information Systems,

<https://pdfs.semanticscholar.org/e7ce/6453cabb2526b7793a65dd939bb81d163447.pdf>

[11] Arthur W. Coviello, INFORMATION SECURITY GOVERNANCE: A CALL TO ACTION, Corporate Governance Task Force Report, April 2004

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fcd427ea43ec6635b5ade3b017b8c5724798b9f3>

[12] Thomas R. Peltier, Information Security, Policies, procedures and standards,

https://books.google.co.uk/books?hl=en&lr=&id=mM_LsS-W4f4C&oi=fnd&pg=PP1&dq=policies+standards+guidelines+and+procedures&ots=WiS_u_isfm&sig=sUUwFJIou1o1P7SKcNI8uwGvBc4&redir_esc=y#v=onepage&q=policies%20standards%20guidelines%20and%20procedures&f=false

[13] Linda Parker Gates, Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework, Software Engineering Institute, November 2010,

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4131dff15664678456174778801e0f4a54a94ede>

[14] Carmel Marock, SETA Review, February 12 2009

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1341630

[15] Risk & Compliance Management, softwareAG,

https://www.softwareag.com/en_corporate/resources/process-management/ds/risk-compliance-management.html