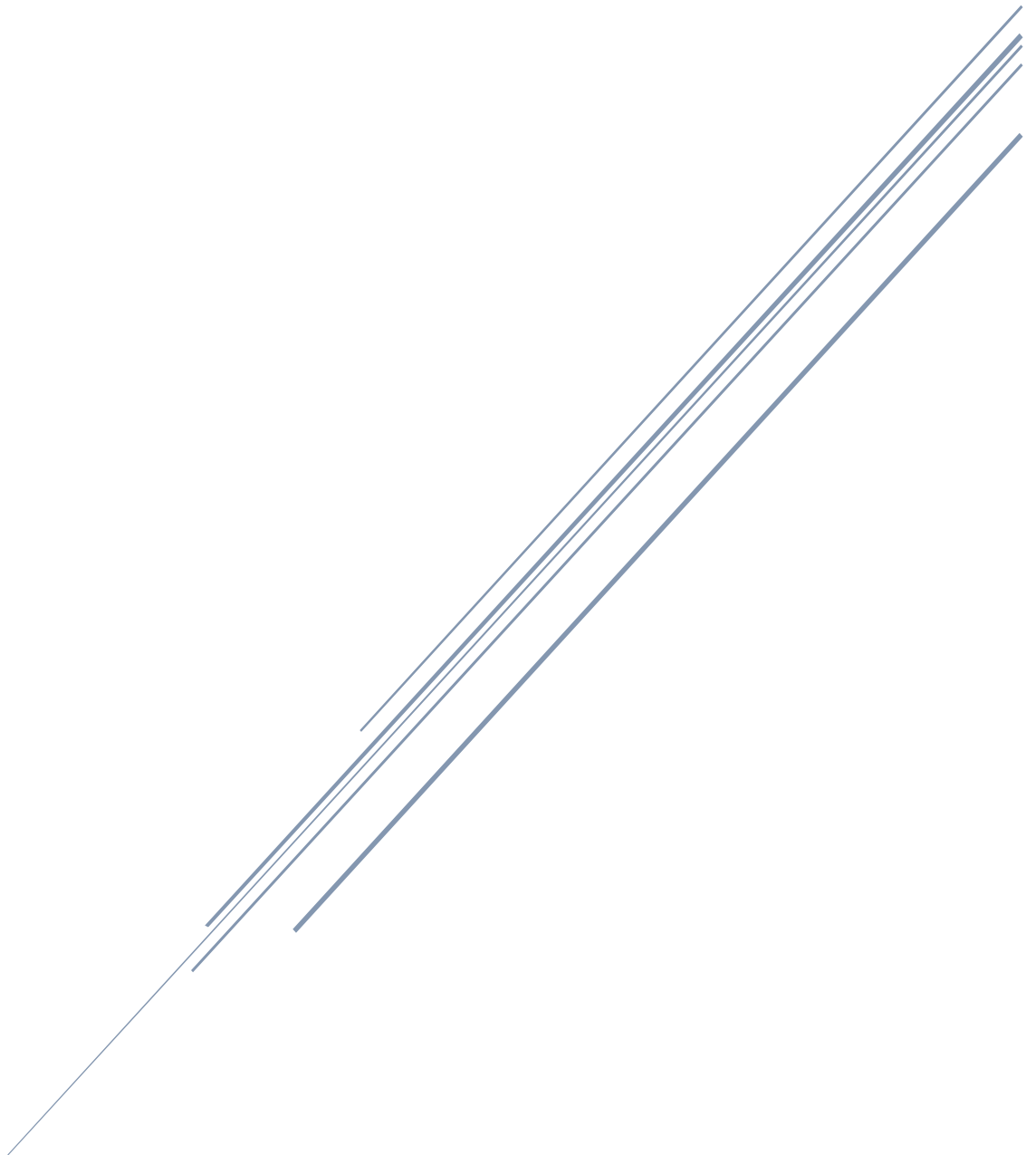


DATA SECURITY & COMPLIANCE

ASSIGNMENT – 14th December 2023



Networks and Cybersecurity
Che Morris - 2203458

Table of Contents

Task 1 – Research in Data Security and Compliance	2
Introduction	2
Security Technologies - Firewalls	2
Security Technologies – VPNs	4
Security Technologies – Access Controls.....	6
Task 2 – Case Scenario (StresSolution).....	8
Introduction	8
Organization Structure / Chart.....	8
Policies and Procedures	9
Access Control & Data Security Policy.....	9
Network Security Policy	9
Physical Security Policy	9
Cloud Storage Policy.....	10
Compliance (Laws and Ethics).....	10
Strategic Planning for Security	11
Risk Assessment	12
Conclusion.....	12

Task 1 – Research in Data Security and Compliance

Introduction

The rise of technology throughout the last few decades has practically transformed the way that we communicate with each other, live our lives and work and could be referred to as revolutionary. This rise, whilst mostly good and has improved how we do things, comes with its challenges. Not everyone uses this technology with good intentions, which forces us to more carefully consider how we handle sensitive data and information and find ways to make sure attackers are unable to gain access. This is especially important within organizations it's in their best interest to protect themselves and their employees but more importantly, they're being trusted by others with the information and can potentially face extreme backlash if their data is breached. Companies in the past have faced big fines for data breaches, with some staff even facing jail time for approaching the breach incorrectly. A great example of this is the Uber breach in 2016, where "57 million users and 600,000 driver's license numbers" [1] were compromised. It was handled horribly by the Chief Security Officer at the time, which after an investigation led by new management, he ended up being charged with three years of probation and had to pay a \$50,000 fine [1].

Security Technologies- Firewalls

In terms of data security, there are a multitude of ways a person or organization can approach securing their systems and information. One of these methods would be using a firewall. A firewall is put in place to act as a middleman in between the internal private network and outside networks that are untrusted, such as the internet. There are many types of firewalls, one of these is a packet-filtering firewall. A packet-filtering firewall analyses data packets, the header information to be specific and has both its advantages and disadvantages. A study conducted by Firkhan Ali Bin Hamid Ali [2] found that a packet-filtering firewall has many advantages and disadvantages, it has the advantage of doing basic checking on IP packets and allows or discards packets based on set rules decided by the information from the source address, destination address, protocol and port number. All traffic on the network is also passed through this firewall and is checked between both networks and is usually included in routers as standard so should be something that routers already have preinstalled [2]. Packet-filtering firewalls usually come integrated into routers as standard so therefore it would be a cost effective and easily deployable solution for any individual or organization.

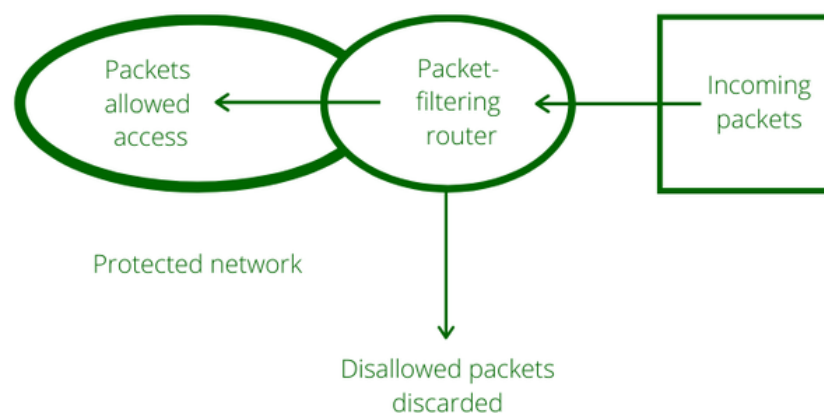


Figure 1 - Diagram of Packet Filtering Firewall [3]

Another type of firewall that could be an option is the application layer proxy firewall, this implementation introduces a whole new layer of control over incoming and outgoing network traffic by changing how traffic is routed between your internal network and outside networks. This type of firewall sets up a proxy server that acts as a middleman between both your network and an outside network, typically the internet, and redirects the connection to whatever you wanted to connect to. You're able to configure this type of firewall so that only correctly configured connections are allowed through and add other rules in place to minimize the risk of unauthorized or unsafe connections being allowed through. As per the study, the advantages of include the amount of applications supported (HTTP, HTTPS/SSL, SMTP, TELNET, FTP and more shown in below diagram) and the fact that it's so easy to configure what outgoing connections are allowed in and out and allows for logging of what goes through the proxy; however, it does have the disadvantage of needing to be configured on a per application basis and it's up to the user to configure applications and some may not support the proxy [2]. This type of firewall is highly regarded by organizations and is offered by a lot of the major cyber security companies including Cisco and Fortinet and is majorly beneficial due to the previously mentioned feature of allowing requests and connections to be logged, allowing the company to keep an eye on what it's employees may be doing.

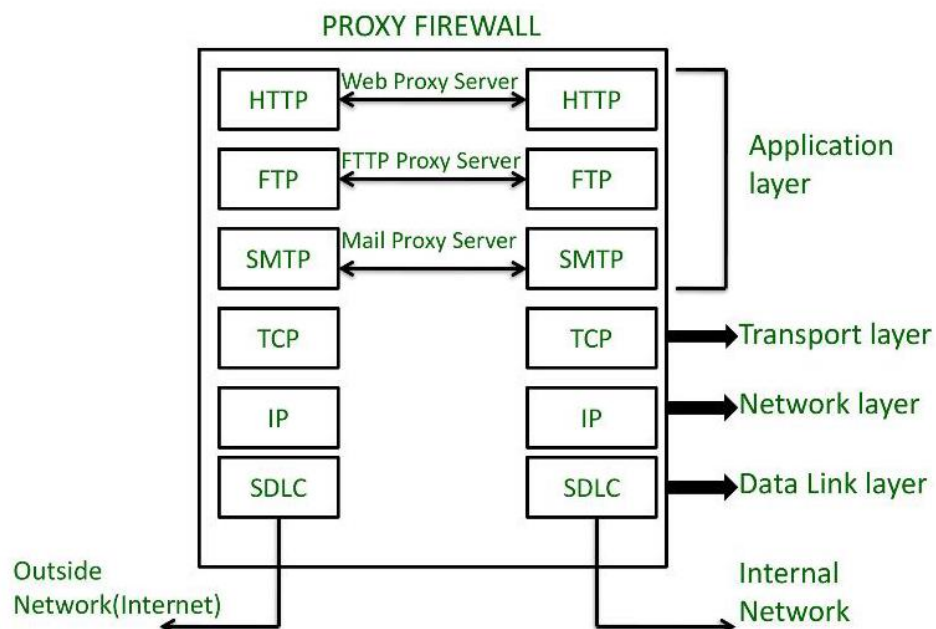


Figure 2 Diagram of Application Layer Proxy Firewall [4]

Security Technologies – VPNs

Another security technology that is commonly used is the use of VPNs (virtual private networks). VPNs are used as a secure and encrypted method to create 'end-to-end' private network connections, this can be between an end user and another network or just between two private networks. The encryption offered by a VPN can ensure that the information being shared can remain confidential even while on the internet which can be classed as an untrusted and insecure network. They don't just serve this purpose though, VPNs have multiple uses such as providing remote access client connections, LAN-to-LAN internetworking and controlled access within an intranet [5].

Remote access VPNs can be used to provide remote access to another location, such as a workplace, and can provide a secure way to temporarily access a remote network while having the benefit of the user having to follow the policies present on that network [5]. As these are typically used to a workplace, or at least something that should require high security, it does require some maintenance from the user as to take advantage of a remote access VPN, a user must install a VPN client which then lets them access the organization's internal network.

Remote access VPNs do come with their risks though, in comparison with accessing the network from an office or the actual building where the network is, they usually have a full set of security solutions in place to prevent attacks which is something that employees connecting remotely will not have on their computers and won't be covered by this security. The company is also responsible for making sure that all security holes are patched and are keeping on top of updating their systems as if a vulnerability becomes present, this could lead to someone with malicious intentions connecting to the network and causing problems [6]. They still do have their benefits though, it can be more convenient for people working remotely as they can have access to company files and as it's encrypted, people working remotely won't have to worry about their data being intercepted and they can work as usual no matter where they are [6].

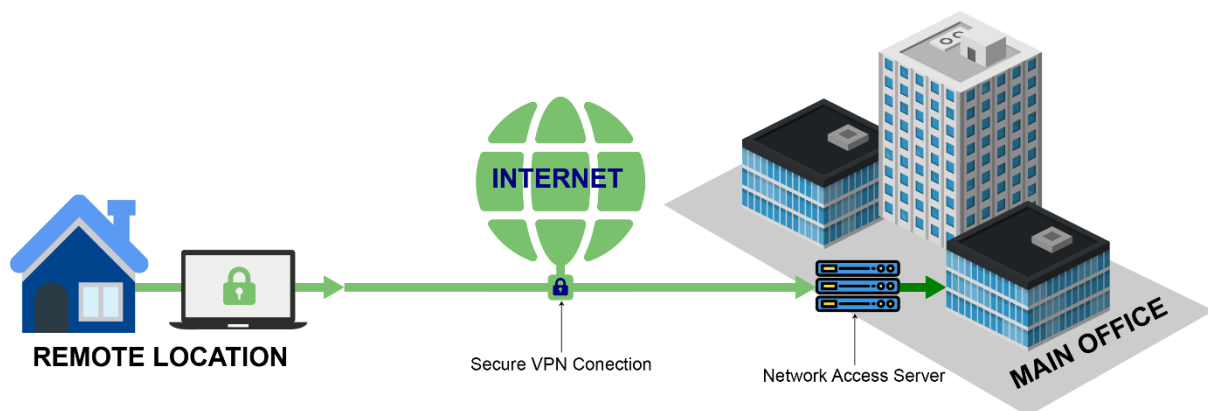


Figure 3 Network Access VPN Diagram [7]

Another type of VPN is the site-to-site VPN, this is something that links different locations or workplaces through using the internet. This is done using a device like a router or firewall at each location which starts and ends connections which enables people in each location to share resources in a secure manner [8]. These are typically used more than remote access VPNs nowadays as with the rise of cloud computing, a lot of businesses are moving their software to online portals (like the Office suite & the Adobe suite) and it can be a lot cheaper than remote access. It's still encrypted just like the other implementations and is decrypted on the other end when the data is received.

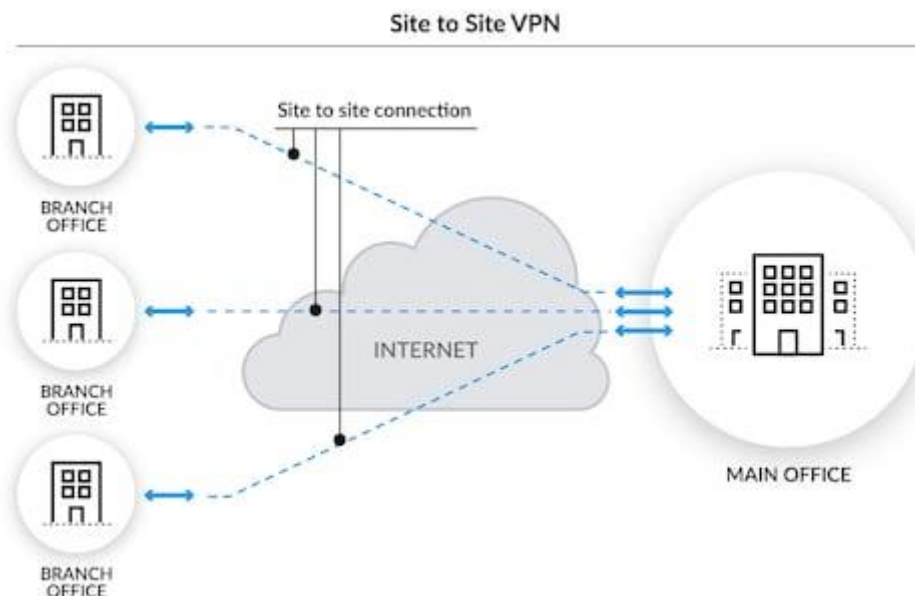


Figure 4 Diagram of Site to Site VPN [9]

There are a multitude of different security protocols used with VPN technology, while more are popular than others, the main ones that have been used across the last few decades are PPTP, IPSec and SOCKS. They all incorporate authentication and encryption as standard which allows the correct person's identity to be established and allows data to be hidden and secure.

PPTP is a protocol developed by the 'PPTP forum' which was created by Microsoft, 3Com, ECI Telematics and US Robotics and is designed to "query the status of Comm servers, provide in-band management, allocate channels, place outgoing calls, notify the server on incoming calls, transmit and receive user data with flow control in both directions and notify the server on disconnected calls" [5]. It was typically used for remote access VPNs but has fallen out of use over recent years due to it having many known vulnerabilities and is much less secure when compared with other protocols.

IPSec is a protocol which uses a sort of 'hybrid' system using both encryption and tunnelling mechanism. It is the most secure protocol and the most widely used protocol that can be used for a VPN and specifically protects against "man in the middle" attacks by masking IP addresses that otherwise could be easily intercepted [5]. It is most used for site-to-site VPNs and can sometimes be difficult to configure, but the effort of configuring it makes it worth it as it offers great flexibility in exploring other security options.

SOCKS works at a higher level compared to the other protocols at layer 5 in the OSI but this brings it's own set of advantages and disadvantages. It does allow for network administrators to choose which applications are allowed to use VPN traffic; however, it must also be installed both on the network and on the users end so can be a bit trickier to set up [5]. SOCKS doesn't include its own security features but is used in combination with other security protocols to ensure security as it doesn't provide its own encryption.

Security Technologies – Access Controls

Access controls are a method that allows systems to put permissions in place to which individuals can access what resources or information and what they may do to that information. They are crucial as it helps prevent unauthorised access to information held by the organisation by restricting access to certain users or user groups and can also prevent them from modifying or deleting certain pieces of information if needed. They can also ensure that information is kept confidential as due to it being limited to certain users or user groups, it can also be tracked as to who may have downloaded or modified that file in the result of a data breach and then that individual can be punished accordingly. They also play an important role in protecting networks by putting access policies in place, organisations can prevent unauthorised individuals or devices from accessing information in this way which in the long run will reduce the risk of cyber attacks or unauthorized access taking place.

Access control has come way over the last few decades and has evolved spectacularly and quite rapidly from what it used to be. Information has gone from being strictly paper based and being basically accessible by anyone who could get their hands on the documents to then as computers became more widely available all digitalised and been password based where users had to verify themselves with a simple username and password. It was then recognised that this was quite insecure as anyone who could obtain a username and password could then access the information so now these days also have other policies in place related to access control in terms of authorization, in most organisations you are now required to have an extra layer of authorization through the use of something you possess like a fob, something unique to you such as biometric or fingerprint verification or through a 2FA mobile app (such as Authy or Google Authenticator) on your smartphone [10]. Once the user has been authorised though, their identify is verified and they will be granted access to the information they were attempting to access.

Access control is not just present in terms of computers though, it is also used elsewhere such as gaining access to buildings or locations, almost like a key. A few examples are, accessing rooms on a university campus, using your ticket to gain access to a train, signing into your phone with a fingerprint or facial scan or scanning IDs to ensure that people are not using a fake ID and are of age.

In terms of computers though, there are multiple types of access control that can be implemented, these include Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-based Access Control (RBAC). Mandatory access control is a method of access control that places strict policies on specific users and the data and system they want to access, these policies are managed by the system administrator at the organisation and users are not able to change or set these policies, they must be done through the administrator [10].

Discretionary access control is another model of access control that allows the owner of the information to decide who should have access to it and allows them to assign access and rules to users that they specify. The only downside of this is that when a user is granted access to information or a system, they can then allow access to other users making that information quite vulnerable to a breach as if someone with bad intentions gets access, they can then grant access to whoever they please and change basically whatever they want.

Role-based access control is something we've briefly touched upon previously but this type of access control sorts users into groups by their role so for instance Sales Assistant, Management, Administration etc. It is then decided what permissions and information these roles have access to and then anyone within that role holds those permissions and can access whatever data that role has access to and can do anything that the role can do; however, they cannot change their group or permissions [10].

Task 2 – Case Scenario (StresSolution)

Introduction

StresSolution (SS) is an intelligence and consultancy company that wish to establish an Information Security Unit to assist businesses in safeguarding against cyberattacks. They also want to use their consultancy services to provide their customers with the correct tools and frameworks to suit their state of compliance, business continuity, data recovery and risk management which also includes their cloud storage and services. This case scenario will outline the steps that SS can take to establish their Information Security Unit.

Organization Structure / Chart

SS will need to have a clear and effective structure within the new information security unit so will need to start splitting their employees into specialized teams with leaders for each team. I believe that going with a hierarchical structure would be best suited here as it would allow for one person (the chief of the unit) to oversee everything while allowing for the other departments to focus on what they're assigned to. Each group would have a specialist or multiple specialists within the group that are quite knowledgeable.

I believe that based on the approach that SS wish to go for, the following departments would need to be created and positions filled:

- Chief of Information Security Unit
- Cryptography
- Physical Security
- Security Technologies
- Compliance and Risk Management
- Cloud Storage
- Security and HR

The Chief of the Information Security Unit would provide leadership and direction for the whole team and would also communicate with the customers and keep them informed. The Cryptography team would focus on securing communication and data using encryption techniques and would collaborate with the other teams to add these into the systems they work on. The Physical Security team would work on securing the facilities of the customers. The Security Technologies team would be more focused on preventing cyber-attacks using firewalls, VPNs and more. Compliance and Risk Management would carry out risk assessments and ensure compliance with industry standards. The Cloud Storage team would allow SS to provide customers with their cloud storage and this team would build upon that. The Security and HR team would build the policies for the customers and make sure that they are followed. An organization chart is below displaying this structure.

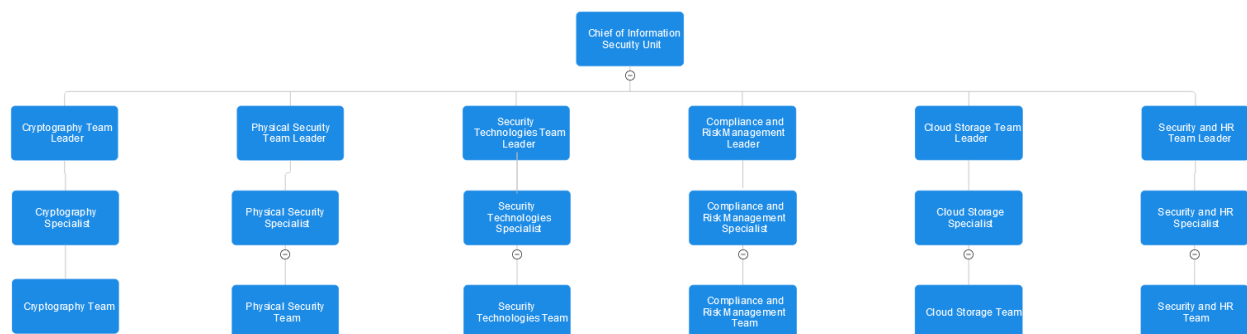


Figure 5 Company Organisation Structure

Policies and Procedures

As the Information Security Unit is developed, policies and procedures will need to be implemented so that employees of SS have some sort of guide on their behavior, their decisions and their actions within the organization. Throughout the development of the Information Security Unit, they will play a big role in making sure everyone plays nice with each other and that the customers get the best experience possible. Based on the case scenario, I believe that SS will need to put a few policies in place which I'll begin to list and explain below.

Access Control & Data Security Policy

The Access Control policy will be in place to outline the rules and procedures about which users should have access to which systems and information. This should be standard practice within companies, hence why it has been implemented here. This will be set up by the Chief of the Information Security Unit and the rules will be outlined by him. SS will also be taking data security very seriously since that's almost entirely what they stand for in the eyes of the customers they work with so it's imperative that how data is handled is looked at closely. This will be quite like the Systems-Specific Security Policy (SysSP) as that's pretty much what this policy would cover.

Network Security Policy

As SS focuses on facing cyber security threats, we need a network security policy, this policy will outline the guidelines for securing SS's networking setup which will include firewall configurations, intrusion detection and prevention systems and the configurations on end devices.

Physical Security Policy

SS will also be helping customers work on their physical security as outlined by the organization structure, so we'll also need a physical security policy. This policy will outline the measures taken for physical security which will include access controls put in place to enter the building which

employees will have to follow, CCTV surveillance put in place both inside and outside of the building and other methods of authorization that will have to be followed by employees.

Cloud Storage Policy

As SS appears to host its own cloud storage and services, there must be a policy in place to ensure uptime for this service is taken very seriously. It will also address the concerns that can come with hosting a cloud service such as the security risks, so we'll have to make sure data protection and encryption is taken very seriously.

Compliance (Laws and Ethics)

Running a business, especially one of the types that SS is, comes with a lot of laws that must be followed and ethics that must be considered. I'm assuming that SS operates within the UK so that's the laws and ethics that I'll be following. Someone within the company (should be the Chief of the Information Security Unit) should be keeping up to date with these laws and ethics and how they may change as not only is it legally required of the business, it's also important for building trust with their employees and customers. It also can help build a good reputation for SS with its business partners.

SS will need to keep up to date with the GDPR Regulations (General Data Protection Regulation) which is important and legally required for the processing of personal data to ensure that individuals are protected. If these regulations are not followed SS can face legal action, fines and lose the trust of its customers and partners.

NIS (Network and Information Systems) regulations will also have to be followed by SS, they are designed to help enhance the security of network infrastructure and compliance of this regulation helps safeguard essential services, protect against cyber threats and contribute to national security.

PECR (Privacy and Electronic Communications Regulations) will also have to be followed and closely monitored by SS, they regulate electronic communications and will also monitor SS's marketing practices. Compliance of these regulations will ensure that SS remains both ethical and in good standing legally with their customers.

FCA (Financial Conduct Authority) regulations are extremely important to be followed as they will help maintain both the integrity and the security of financial information that SS takes on board, this can include any purchases they make or sales they make to potential customers. This will also help SS avoid any legal or financial consequences.

As SS will be taking on quite a few employees, they must make sure that they're following employment and human rights laws as this will help make SS a positive place to work and will also ensure the protection of employee information and privacy. This will also ensure that ethical standards are followed within employee management.

This one isn't exactly one that MUST be followed but SS should ideally be reporting any cyber incidents that they face to the NCA (National Crime Agency) as this will aid law enforcement with their cybersecurity efforts and will help protect SS and its clients from any unauthorized activities.

Strategic Planning for Security

In SS, strategic planning for security would be extremely important for them as it's basically the whole point of them creating this Information Security Unit in the first place. To start with a strategic plan, SS would have to ensure that they're in compliance with the previously mentioned regulations and standards and would have to ensure that processes are created by upper management to run regular audits to make sure that they're remaining compliant. They could appoint a compliance officer to run through these things, but they would have to have a pretty good understanding of what procedures the SS already have in place. The audits for some things could be run on an annual basis, things such as, employee training sessions, security audits and assessments and policy reviews but somethings would have to be done more regularly like there would have to be continuous monitoring to try and detect compliance issues in real time and making sure documents are kept up to date.

As SS already offer cloud services, it would have to be made sure that this has future proofing including making sure that it's up to date with current standards and is audited regularly to ensure that all software for this is up to date and isn't vulnerable to any attacks. Multi-factor authentication could be introduced here including things that are unique to the person such as a retina or facial scan combined with something a bit simpler like simple 2FA on someone's phone before they can sign in, this would prevent someone from obtaining a username and password and just being able to sign into the service.

I would also recommend having a SIEM (Security Information and Event Management) system in place, this is a system that allows for organizations to discover and address any potential security threats or vulnerabilities before they take place which will prevent business by SS being disrupted [11]. This would be beneficial to SS as while they help businesses stay clear of cyber-attacks, they can't do that if they're a victim of a potentially crippling cyber-attack themselves.

A process for ensuring continuous improvement is always happening at SS should be put in place, the security procedure should be reviewed regularly by either the chief of the unit or the potential compliance officer and based on any emerging threats or any changes in technology, penetration testing could also be used here to ensure that SS isn't vulnerable to any type of attack. This could also be aided by investing in emerging technologies which nowadays is seen a lot within bigger companies. Emerging technology such as artificial intelligence or machine learning could be considered as it could potentially be helpful in identifying threats and coming up with new responses to them.

Some sort of 'security awareness' program could be introduced for all the employees to help reduce the 'human error' that could potentially happen if an attacker does decide to go that route. This could be used to keep employees up to speed with the latest phishing or social engineering tactics, possibly could also run phishing simulations through the company email to keep the employees on their feet when it comes to recognizing such emails.

A strong network infrastructure should also be setup within SS, firewalls such as a packet-filtering or application layer firewall should be put in place. Regularly scheduled security assessments should also be utilized as this can help detect if anything does go wrong with the system and it can be fixed as soon as possible. VPNs could also be beneficial here as not only would it allow employees to work from home, if necessary, it would allow for connections to be encrypted and to prevent 'man in the middle' attacks. It could also help SS expand in the future if they desired.

Risk Assessment

To complete a risk assessment for the new Information Security Unit, SS would need to appoint someone to carry out this risk assessment, likely the chief and there would be a few steps that would need to be followed.

- All assets related to the unit would have to be identified and listed, this should include all physical assets (hardware, servers, any other devices), software and anything else that's crucial for the unit's operation.
- All threats that could potentially compromise the security of the unit should also be identified, these could include things like cyber threats, physical threats, human error or generic system failure.
- All potential vulnerabilities must also be identified and assessed. This could range from weaknesses in processes or human factors that could be exploited by potential threats (phishing, social engineering or espionage). This could also include things such as outdated software (although this should be checked regularly) or the lack of correct employee training.
- The likelihood of all these threats and vulnerabilities should be evaluated and the potential impact that if they happened, they would have on the new unit.
- The impact and likelihood assessments should be combined and used to evaluate the risks that they would have and should be classified as high risk, medium risk or low risk based on their severity.
- With the help of the rest of the team, mitigation strategies should be created to address the identified risks, whether this be updating policies or procedures, completing additional employee training or perhaps investing in new technology. These should be aligned with the goals of SS.
- This whole assessment should be documented and checked regularly and should include everything discussed (identified risks, vulnerabilities, threats and new mitigation strategies) and can then be used for future assessments and audits (assuming they are implemented and performed regularly). Future changes in technology should also be accounted for during the regular checks though.

Conclusion

The creation of the new Information Security Unit will be a great benefit to StresSolution and sets them up well for a new strategic commitment to cyber security, both for themselves and their customers. I believe that with the new plan SS will be a huge help in both cyber security and consultancy for their customers and if followed correctly the new unit will succeed well.

The new hierarchical structure should be quite effective as it allows for clear lines of communication through all tiers of the hierarchy with the Chief of the Information Security Unit overseeing the whole thing, they should be quite in touch with almost everything going on which will be a huge help to them when working on compliance with laws and ethics and when completing a risk assessment. If everyone within SS communicates well, there shouldn't really be much to worry about.

In summary though, if the plan is followed, I think the information security unit is in a good place to face the challenges of the cyber security world. It's following standard and sometimes more advanced security practices and if it stays in lines with the suggestion made in the plan, it should not only be in line to be secure in it's own right, it should make it's customers happy too.

References

- [1] J. Green. "Ex-Uber chief security officer sentenced to probation for covering up 2016 data breach." The Mercury News. <https://www.mercurynews.com/2023/05/05/ex-uber-chief-security-officer-sentenced-to-probation-for-covering-up-2016-data-breach/> (accessed Dec 04,).
- [2] F. A. Bin Hamid Ali, "A study of technology in firewall system," 2011. doi: 10.1109/ISBEIA.2011.6088813.
- [3] "Packet Filter Firewall and Application Level Gateway." GeeksforGeeks. <https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/> (accessed Dec 04,).
- [4] "What is a Proxy Firewall?" GeeksforGeeks. <https://www.geeksforgeeks.org/what-is-a-proxy-firewall/> (accessed Dec 04,).
- [5] Z. Zhang, et al., "An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN," *Photon.Network Commun.*, vol. 7, no. 3, pp.213-225, 2004. doi: 10.1023/B:PNET.0000026887.35638.ce.
- [6] "What Is a Remote Access VPN?" Fortinet. /resources/cyberglossary/remote-access-vpn (accessed Dec 05,).
- [7] "Remote Access VPN Guide | Greyson Technologies | Florida." Greyson Technologies. <https://www.greyson.com/remote-access-vpn-guide/> (accessed Dec 05,).
- [8] Z. Kerravala, "What is a VPN? A secure network over the internet: VPNs can create secure remote-access and site-to-site connections inexpensively, are a stepping stone to software-defined WANs, and are proving useful in IoT," *Network World (Online)*, 2022.
- [9] "What Is a Site-to-Site VPN?" Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn> (accessed Dec 05,).
- [10] "What Is Access Control? - Network Cybersecurity Systems." Fortinet. /resources/cyberglossary/access-control (accessed Dec 06,).
- [11] "What is Security Information and Event Management (SIEM)? | IBM." <https://www.ibm.com/topics/siem> (accessed Dec 06,).