SECURITY AUDIT / SECURITY MANAGEMENT

Philip Jeremiah Kadiri

Contents

Executive summary

This Report provides insight into the information security measures and policies of Devon Partnership NHS Trust, the report includes an overview of the company, an information security mind map, a risk assessment, and critiques of the information security policy. The report highlights the importance of IT governance in information security and identifies areas for improvement in the company's policies. The recommendations outlined in the report can help Devon Partnership NHS Trust enhance its information security measures and minimize the risk of security breaches and incidents.

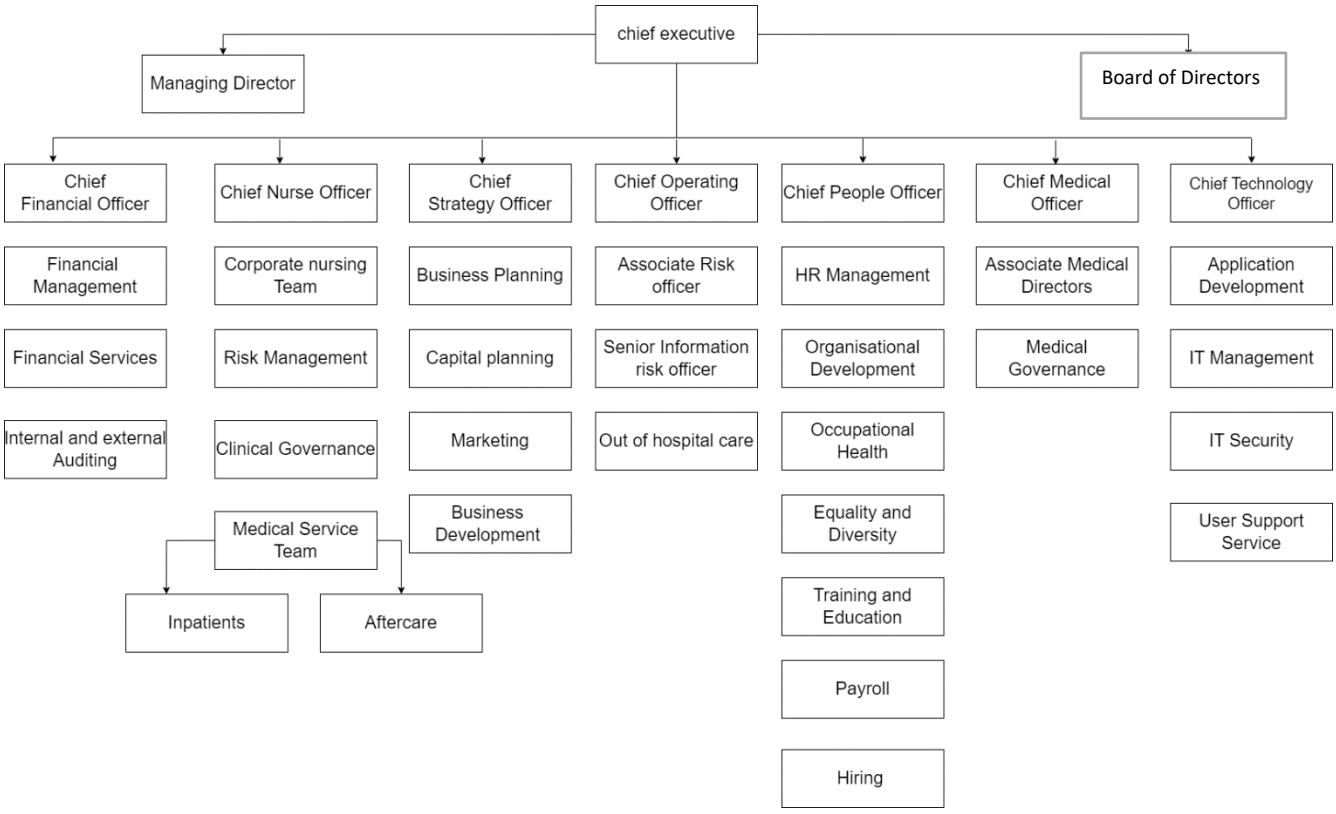
Insight into Company

Devon Partnership NHS Trust is a company that serves the purpose of providing specialist care in mental health, learning disabilities, and neurodiversity services. They are a government agency that works in the healthcare industry. The company was established on 1st April 2011 during the merging of two former NHS trusts which were established separately during the 1990s-2000s.

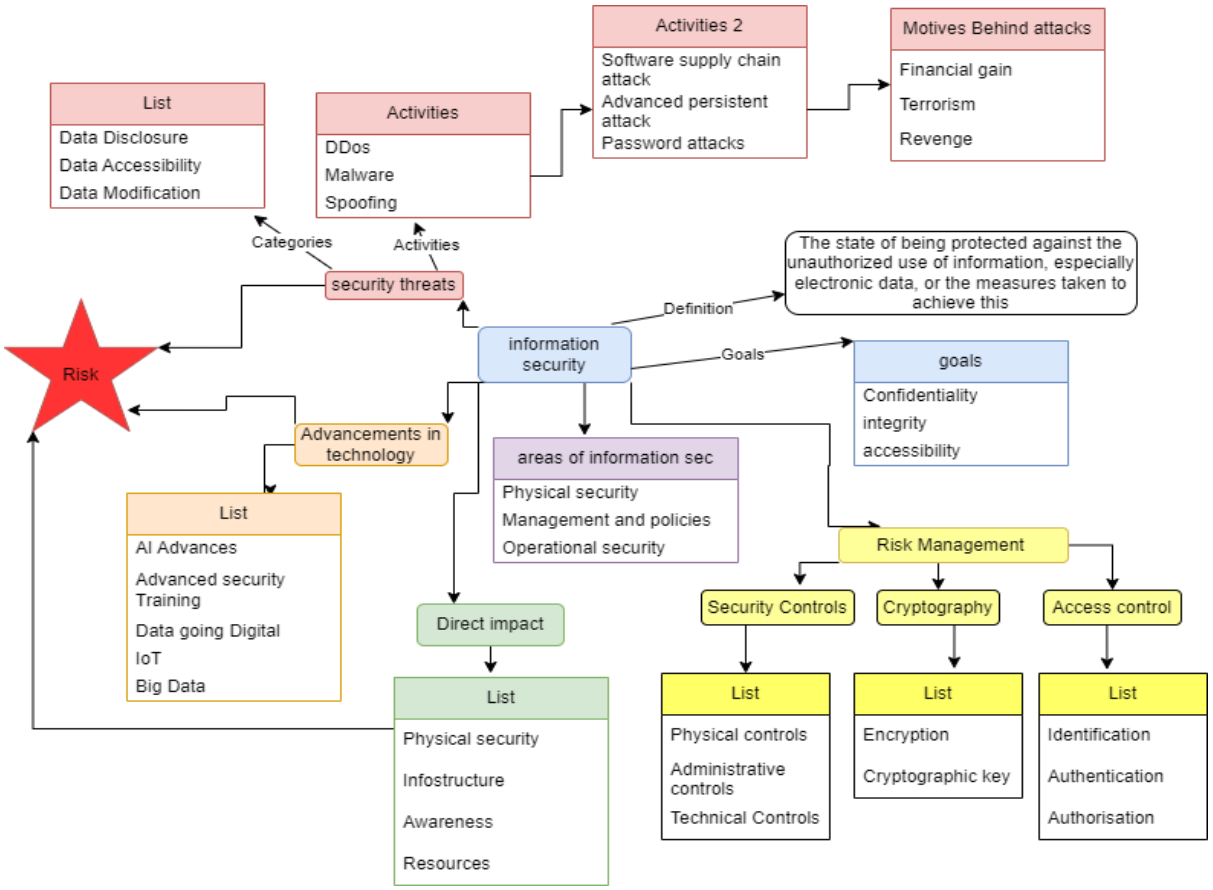
The company would be classed as a medium-sized company due to them only having 3000 employees and a revenue of £169M. according to their LinkedIn 54% work in healthcare services, 8% in administrative, 5% in community and social services, and 5% in Information Technology. The company is ranked 138th in NHS Foundation Trusts expenditure.

Since the company is a publicly funded organization and a nonprofit charity organization, I wouldn't say the company has competitors in the same way that apple and amazon have competitors, however, there are other organizations in the area that work within a similar industry. Cornwall Partnership NHS Foundation Trust, Somerset NHS Foundation Trust, and Dorset Healthcare University NHS Foundation Trust are examples of organizations that provide similar services in the wider Southwest. Additionally, private healthcare companies that provide similar services such as Priory Group and Cygnet Healthcare could be seen as competition due to them paying their staff more and offering less stressful work.

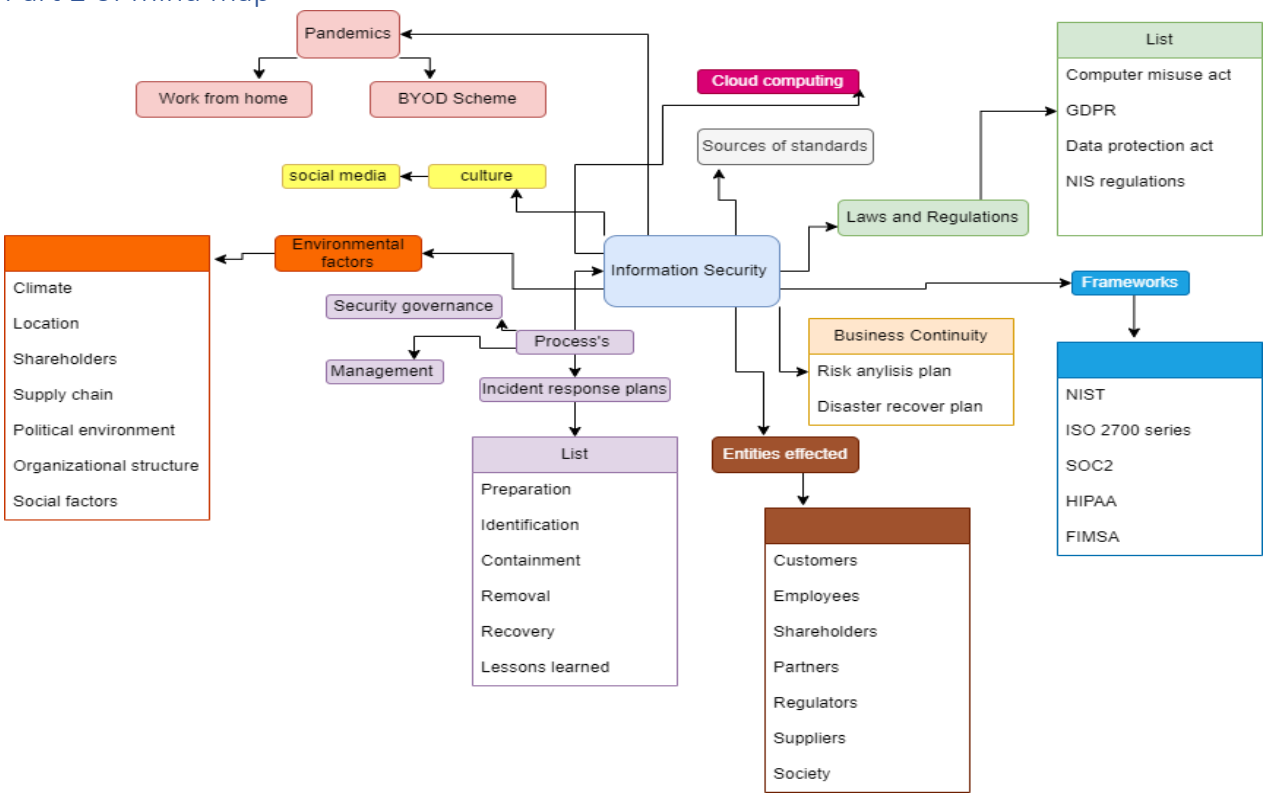
The services they offer include:- Community and urgent care mental health services, Community services for children, young people, and families, Specialist Early Psychosis Teams for 14-65-year-olds, West of England Specialist Gender Identity Clinic, The Haldon eating disorder service, Services for adults with a learning disability, Personality disorder service for mild, moderate or severe personality disorders, and Adult talking therapies and psychology services.



Information Security Mind-Map



Part 2 of mind map



IT Governance

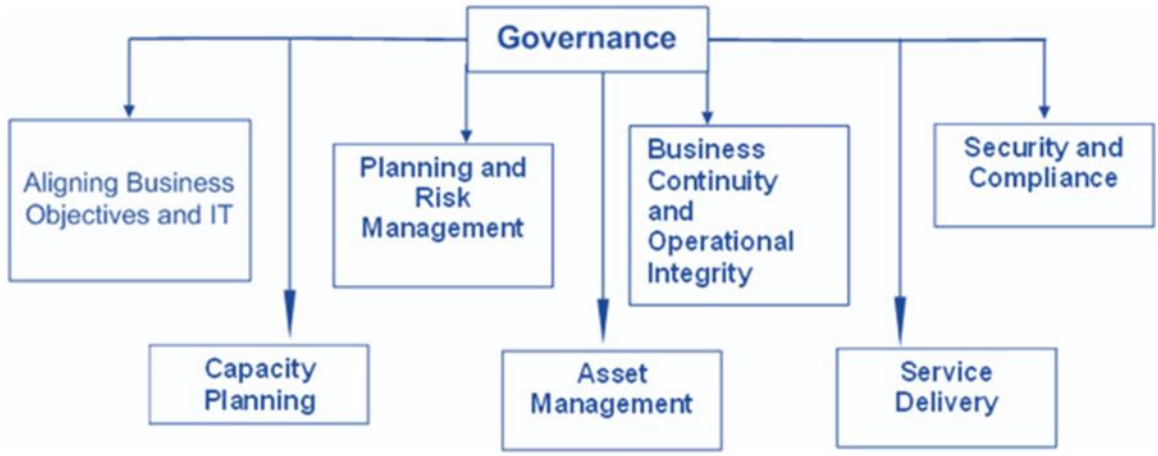


Figure 1: Diagram of what IT Governance is

IT governance is the process by which firms align IT actions with their performance goals and assign accountability for those actions and their outcomes. To be effective, IT governance must be actively designed not the result of isolated mechanisms (Weill & Ross, 2004). Everyone is responsible for IT governance and it's important to hold each other accountable for overall succession.

IT governance is important to Devon Partnership NHS Trust in terms of information security as it will ensure that the company is running in a safe and secure manner. Information security is vital to information governance as it establishes the confidentiality, integrity, and availability of high-risk data.

Since Devon Partnership NHS Trust is a health care provider this means that the type of information assets they hold are extremely sensitive and will need to be protected with great care as unauthorized disclosure of information could affect the individuals and the company drastically, however, IT governance makes sure that data management and IT system policies are designed with information security in mind. Additionally, adhering to IT governance will mean that they are minimizing the risk of legal and financial penalties. Furthermore, IT Governance allows organizations to structure their information security policies with the business's risk tolerance and requirements.

Secondly IT governance is important to the company because as a Health organization they will need to conduct Data protection impact assessments which are tools for identifying, quantifying, and mitigating data privacy risks. These are usually put into place to ensure new processes/systems are being used with high-risk data i.e. health data. It is a legal requirement to conduct these assessments under the General Data Protection Regulations. Furthermore, this use of IT governance in terms of Information security will help to change policies/procedures where needed and to counteract new cyber-attacks data breaches and system failure.

Critique Information Security Policy

https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v4.0.pdf

The objectives of an IT security policy is the preservation of confidentiality, integrity, and availability of systems and information used by an organization's members (Paloalto, n.d). The principles named make up the CIA triad which makes sure data is confidential and cannot be accessed by unauthorized people, Integrity ensures data isn't modified and is accurate, and availability assures systems are delivered and available to the right people.

The information security policy is suitable for the current business operating environment because covers all the major aspects of information security like access control, incident management and data protection which is big as the company collects a lot of data. However, the policy was last updated in 2018 so it might not be up to date on newer threats from then.

The policy doesn't address measures that could be taken for future environments, for example, the policy doesn't mention cloud computing and IoT devices. Also, the policy gets updated every 2 years so it is outdated and may not be suitable

- positive aspects of the policy

One of the positive aspects of the policy is that it outlines the specific responsibilities for information security to the appropriate employees. Furthermore, This shows who is Responsible for what when it comes to security. Additionally, this allows for structure and for accountability within the organization as the roles are clear and concise.

Secondly, the policy clearly states that the company should conduct risk assessments to find and mitigate security threats.

Thirdly, the policy clearly outlines the importance of employee security training as it states that employees must take part in regular information security training to help raise awareness of risks. I believe every company should have security training because according to Proofpoints human factor Report, Twenty-six percent clicked an email link that led to a suspicious website, 17% accidentally compromised their credentials and only half were able to correctly identify the term phishing (Bernard et al., 2022).

Additionally, The policy is aligned with the correct legal and regulatory requirements, which are the Data Protection Act 2018 and GDPR, this will allow the company to avoid legal penalties by ensuring compliance.

- negative aspects of the policy

The first negative that was easily picked on was that the company are using a security policy that was made in 2018 this means that they are not up to date on recent risk, regulations, and policies. Additionally, it doesn't clearly state how frequently their policies should be updated or reviewed.

Secondly, the policy doesn't address the risks associated with the use of smartphones and laptops for personal and work purposes. This is a risk as BYOD comes with major threats that employees are not aware of for example connecting to unsecured wifi connections with work devices and bringing in devices that are jailbroken which can put the device at more risk of being hacked. BYOD plays a big part in security risks within SME's this is shown by more than 500 SMEs polled in the UK, 61% said they had experienced a cyber security incident since introducing a BYOD policy (Ashford, 2018).

Thirdly the policy doesn't state how users can report a security risk or incident I.e. whom to report to. Furthermore, this can be drastic for the company as they might have security risks that they may not be aware of and cause them to be late to response and management.

- Standard used to make a judgment

A benchmark that we could use to make a judgment on the policy could be the ISO/IEC 27001 or NIST SP 800-53 standard, ISO/IEC 27001 is the international standard for information security. It sets out the specification for an effective ISMS, it helps organizations manage their information security by addressing people, processes, and technology (ITGovernance, n.d). the categories inspected when critiquing are regulatory compliance, risk assessment and management, and overall clarity. I have inspected the following policy to make a judgment on whether it includes the specifications any company policy should address:

1. Objectives

2. Scope

3. Specific goals

4. Responsibilities for compliance and actions to be taken in the event of non-compliance (Paloalto, n.d).

Risk Assessment

A security risk assessment identifies, assesses, and implements key security controls in applications. It focuses on preventing application security defects and vulnerabilities. Additionally, it allows an organization to view the application portfolio holistically—from an attacker's perspective (Synopsys n.d.) we will be using NIST framework to conduct our risk assessment

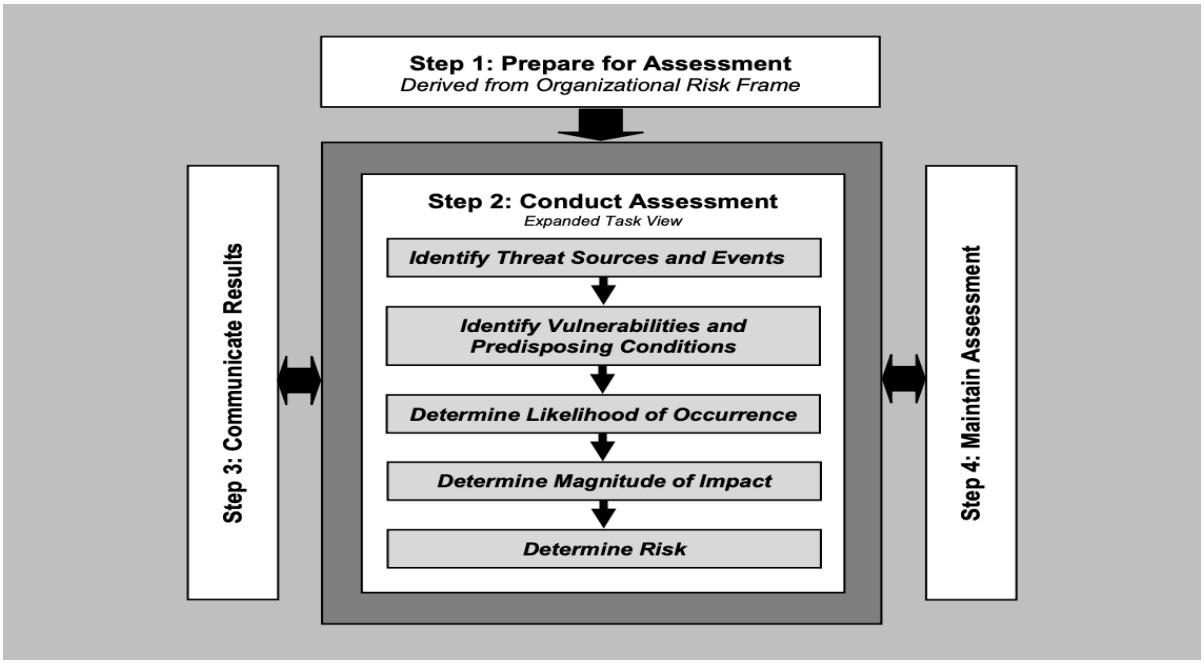


Figure 2: Diagram of how to conduct a risk assessment (Dijk, 2023)

Approach of a risk assessment is as follows:

identify the scope-this entails reviewing what assets need to be protected i.e servers, customer data, system software and network infostructure.

Threat detection- companies should identify possible threats that can affect assets. This can be done by keeping a track record of previous or known attacks i.e. sabotage, natural disaster and malicious cyber-attacks.

Vulnerability assessment- companies should identify vulnerabilities in their company and determine the likelihood of these threats being exploited.

Impact assessment- companies should assess the impact of the attacks based on financial loss and disruption time.

Risk calculation: companies should determine the severity of each risk and prioritize the risks with the greatest impact.

Control recommendations- the company should identify countermeasures to combat the risks.

Monitoring and documentation- the risk assessment should be done regularly to stay up to date against new risks and to make sure their controls are working. All results from these assessments should be documented too.

Threat	Likelihood	Severity
Phishing attacks	high	High

sub-security policies affected by threat
Email and Messaging Policy: phishing attacks make use of emails primarily
Incident Response Policy: a successful attack will need an incident response policy plan to reduce the impact
User Awareness Training Policy: policies should educate users before the attack on how to spot them.
Access control: if user credentials are stolen they can be used to gain unauthorized access

Key controls to implement security training and security awareness testing should be mandatory and those who fail the simulated test should be monitored and re-educated to spot the risk of further attacks.

Email and web filters should be added to stop access to and prevent malicious emails from reaching their target.

Threat	Likelihood	Severity
DDos attack	Medium	medium

sub-security policies affected by threat
Incident Response Policy: a successful attack will need an incident response policy plan to reduce the impact
Backup and Recovery Policy
Network Security Policy
Disaster recovery

Key controls to implement: intrusion prevention systems should be installed to identify and filter out unusual traffic before it gets to the network and causes damage.

Run vulnerability assessments and Pen Tests to find weaknesses in the network this will allow you to patch them before a hacker gets the chance to exploit them.

host servers at data centers and colocation facilities in different regions to ensure you do not have any network bottlenecks or single points of failure (Velimirovic, 2021).

Threat	Likelihood	Severity
Damage caused by natural disasters	Low	High

sub-security policies affected by threat
Disaster recovery
Backup and Recovery Policy
Physical Security Policy

Key controls to implement: Store backups in a remote location to ensure their safety from a natural disaster, backups can be stored on either the cloud or in another physical location.

Develop a business continuity plan that shows how the business will run after an incident.

Create the capability for employees to be able to work from home.

2 security threats that could occur.

Insider attack

If a company believes an insider attack has taken place, the company will try to contain the threat by disabling access to the company's systems and networks from the user. Next, the company's rapid response team (legal, HR, IT personnel) will investigate the incident and find if anyone else was involved in the attack and the severity of the damage. Additionally, repairs to the company system and security will be done to bring the company back to its feet. Lastly, legal action will be taken against the attacker.

The company can resume business when they deem it is safe to do so, they need to consider the well-being of the customers, employees, and the organization. Additionally, they need to consider whether they are legally compliant to do so.

Ransomware/malware

If a successful ransomware attack takes place the company should first identify the devices affected and the severity of the files/systems compromised, then quarantine the affected devices to stop malware from spreading. Next, the IT team should identify if decryption is possible if not evaluate if the ransom is feasible to pay. The authorities should be notified and data from backups should be uploaded.

The company can resume back to business when all remanence of the malware is gone, and all systems are working correctly. Additionally, they will need to develop a continuity plan that shows the steps needed to be taken to prevent future cyberattacks i.e., data backups and system restoration.

Conclusion

In conclusion, I have shown how critical good security management is to a company especially one like the Devon partnership which holds sensitive data. I have shown how companies need to be able to create better information security policies through a policy review and how critical it is for a company to adjust to new cyber threats and technologies as they arise. Through a risk assessment, I was able to show the severity and likelihood of risks accruing to the organization and the necessary controls to implement.

References

Weill, P., & Ross, J. W. (2004). *IT governance on one page*. Available at SSRN 664612.

Ashford, W. (2018, May 18). *BYOD in UK smes linked to security incidents: Computer Weekly*. ComputerWeekly.com. Retrieved March 24, 2023, from https://www.computerweekly.com/news/252441392/BYOD-in-UK-SMEs-linked-to-security-incidents

Bernard, A., Staff, T. R., Azhar, A., Branscombe, M., Hughes, O., Miles, B., & Greenberg, K. (2022, September 28). *Humans still weakest link in Cybersecurity*. TechRepublic. Retrieved March 24, 2023, from https://www.techrepublic.com/article/humans-weakest-link-cybersecurity/

ITGovernance. (n.d.). *ISO 27001*. IT Governance. Retrieved March 24, 2023, from https://www.itgovernance.co.uk/iso27001

Synopsys. (n.d.). What is security risk assessment and how does it work? Synopsys. Retrieved March 26, 2023, from https://www.synopsys.com/glossary/what-is-security-risk-assessment.html

Velimirovic, A. (2023, March 20). *How to prevent ddos attacks: 7 tried-and-tested methods*. phoenixNAP Blog. Retrieved April 4, 2023, from https://phoenixnap.com/blog/prevent-ddos-attacks

paloalto. (n.d.). *What is an IT security policy?* Palo Alto Networks. Retrieved April 4, 2023, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy#:~:text=The%20objectives%20of%20an%20IT,used%20by%20an%20organization's%20members.

Dijk, V. van. (2023, March 13). *Guide to NIST risk assessments*. Security Scientist. Retrieved April 4, 2023, from https://www.securityscientist.net/blog/guide-to-nist-risk-assessments/

Appendix

The website URL for the Devon partnership NHS Trust: https://www.dpt.nhs.uk/about/research-development-innovation

The information security policy for the Devon partnership NHS Trust: https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v4.0.pdf