Network Infrastructure Report

Assessment 2

1 Introduction

This report will consist of seven sections that explore the current college cyber security network and methods to improve upon it. DDoS attacks have resulted in grades being delayed to students, additionally, ransomware attacks have been performed to other educational facilities. This report is an investigation into what occurred and how it can be prevented in the future.

2 Failings in Network Infrastructure

The current security infrastructure is likely not adequate enough to counter another cyber-attack. It is likely that there are some gaps in the college's security. The first case is where not enough money and resources are invested into cyber security. The CEOVIEWS website (n.d.) wrote a list of the top 6 reasons for Cybersecurity failures. They suggest that if there already is some investment in IT security, then this could create a false sense of security. Speculatively, this would lead to serious vulnerabilities in their system and could be a leading cause to many other gaps in the college's coverage.

A lack of management around cybersecurity risk could be another factor for the breach. CEOVIEWS state that around 30% respondents reported challenges prioritising possible threats throughout their organisations. Given the number of vulnerabilities that can be found in a system, this is not surprising. Additionally, CEOVIEWS state that "the rise in officially-designated vulnerabilities correlates with reduced awareness of them and the security environment in general" (n.d.). If this is the case it shows the sheer magnitude of vulnerabilities in the college system given there is not enough time and resources to cover them all. If there are enough resources, then it shows that the college system is under poor management. In either case, the current system is vulnerable to future attacks unless these issues are addressed.

According to Sutton (2019) one mistake he identifies is the “failure to change user access rights when changing role or leaving the organisation”. Users who change roles or leave the company/organisation they are working for may still have access to resources they are no longer entitled to. This can lead to an unintentional case of unauthorised access from former employees, who can leverage permissions to bring attacks to the network or leak details. To mitigate this, the business or organisation need to ensure that former employees lose their privileges, so this event cannot occur.

3 Suitable Technology to Augment Current System

Aaron Kuhn writes in ‘ONSOLVE’, about what technology and methods can help combat cyber-attacks (2020). One suggestion to build up the current system is to use progressive tools for threat identification. This can come in the form of detection and protection tools. Defensive detection techniques can be used. These identify attacks early and transfer vital data before it can be accessed or damaged. Another way progressive tools help protect data is the use of decoys, deception solutions and web application firewalls. Typically used by companies, progressive tools can also be used for academic institutions to protect their data from harm.

Another method Kuhn suggests is building a blockchain: an online ledger that accounts for all data in a program. Typically used for cryptocurrencies, blockchain is also used by companies to tackle cyber-crime. Since blockchains cannot be altered or deleted it prevents the information from being manipulated from third parties. A blockchain is created through a series of sequential hashing coupled with cryptography and as such can be used by parties to share information securely. Since blockchain is used by corporations, there is also potential for usage by colleges since various forms of data need to be shared in confidence. Grades and personal details are some examples of data that would need to stay intact and safe.

Since the colleges and universities have been subjected to ransomware attacks, action must be taken to mitigate this. Ransomware is typically disguised as software or documents that really contain viruses. Witts (2021) states that ransomware can be very damaging to business due to financial and productivity loss as well as damaged and lost data. Methods to help reduce the likelihood of ransomware attacks include updating outdated software and hardware to more modern systems with better security and improved security defences. One suitable technology to improve the system defences would be a dependable and strong anti-virus software. Placed on the endpoint devices, they block malware from entering the system. Universities and colleges can use these to effect as they have another advantage as well. This is that they can alert users of risky websites. Another suitable technology Witts identifies to improve the system is web filtering and isolation technologies. These will stop users from visiting dangerous websites and downloading malicious files. This can help aid at distinguishing between legitimate business software and trojan horses.

4 Impact of Cyber Attacks on People and Technology

DDoS attacks can heavily affect the employees of a business since they are unable to access resources (Kaspersky, n.d.). Additionally, Kaspersky reports that consumers that use eCommerce sites are unable to purchase products or receive support. The site also reports that companies can lose $20,000 per hour after an attack, causing serious consequences to the business and its employees. Evidently, an entire business could be potentially put out of action from cyber-attacks.

Kaspersky also state of the impact for ‘bot’ computers during the act. Sometimes thought as willing culprits, they are actually bystanders caught in the crossfire due to susceptibilities in their systems. Sometimes, security vulnerabilities may let trojan viruses into the network and infect systems. Kaspersky go on to state that during a DDoS attack, secondary victim devices may run slowly and in the end crash. The crash will occur due to the drain on the system resources. Furthermore, even if they remain operational, legitimate requests for service may not be fulfilled by the system.

5 Why Ransomware is Used for Attacks

Ransomware has been growing at a fast pace, becoming a threat to business and organisations worldwide (Kochovski, 2021). 2019 saw a large increase in cyber attacks and ransomware incidents and in 2020 there was a rise in Covid19 related phishing emails. Koshovski also reports that a Sophos white paper (2020) found that paying the ransom will double the cost to fix the issues caused by ransomware. This is in spite of the expectation that paying the ransom will save the victim’s money. For companies that pay the ransom, the average cost to recover was $1,450,000, whereas companies that did not pay the ransom paid on average $730,000 to recover. This shows that ransomware attacks are very effective at forcing companies to lose a lot of money no matter what financial strategy they employ. As a result, cyber criminals can leverage this method to cause financial havoc on companies they conflict with. This can be more impactful than simply slowing down their system and/or stealing their data since there is a much larger financial cost to it as well.

Matthews (2021) writes in MarketWatch about how cryptocurrency has enabled a massive surge in ransomware attacks. He reports the incident of the Colonial Pipeline attack where the company received a cyber-attack and had to suspend its gas delivery system. They paid the hacking group approximately $5 million to recover the stolen data. According to MarketWatch, experts told them, “the payment was likely paid directly to a digital wallet owned by the criminal enterprise”. As a result, authorities who wish to track the culprits would face difficulty. The article also state that cryptocurrencies add difficulty to tracking cybercriminals because of the “borderless” nature of the type of currency. Due to this information it is clear why ransomware can be so effective as an attack. This is because cyber criminals can make a lot of money and obtain access to private information.

Also, criminals can leverage cryptocurrency to financially drain the company they are targeting whilst easily covering their tracks.

6 Analysis of Ethical and Professional Issues

Gunarto writes in a study about the ethical issues in Cyberspace and IT society (n.d.). He states that IT has problematic implications and a negative impact on society. He states there are three ethical issues: personal privacy, access right and harmful actions. In the case of personal privacy, IT engages in data exchange of information on a world-wide scale. Therefore, there is an increase risk of privacy violations. Individual’s personal details are at risk, especially in the events of cyber-attacks. Details such as their address, financial details, name, and identity can be potentially accessed without consent. To curb this, precautions need to be taken. This includes protection from unauthorised access and ensuring the accuracy of the data.

Access right is another ethical issue Gunarto explores. The subject of IT security and access right has moved to a high priority for corporations and government organisations because of the popularity of online international commerce. Multiple attempts of breaking into US organisations such as NASA and Los Alamos National Laboratories have been reported. A lack of proper computer security policies and strategies leads to vulnerabilities and thus becomes a professional issue.

A professional issue that has not been considered yet is government involvement in cyber-attacks. Estonia over a period of two weeks in 2007 suffered attacks. The Netherlands and the US also were hit from botnet attacks. It was reported that foreign governments may be involved in this activity to cripple another nation’s infrastructure and economy. Issues arise because of this. Estonia suspects which government they think performed the attacks but are unable to prove it or know why it was done (Brenner, 2009). Brenner suggests the following: ‘Real-world warfare is overt and destructive; cyberwarfare will be subtle and erosive’.

7 Legal Implications

Cyberterrorism has been simplistically defined as an attack on electronic communication networks, which defines cyberterrorism as the intentional use or threat of use, with the absence of legally recognised authority, of violence, disruption, or interference against cyber systems. In this scenario it is likely that the use of such actions would result in death or injury of people, property damage, economic sabotage, or civil disorder. There is a great importance to providing a clarity and specificity to the legal framework to cyber-attacks and cyber-terrorism. This is especially the case in a globalised world where there are no legally binding instruments to regulate interstate relations in cyberspace. It is difficult to achieve this due to different states having differing economic interests. If stakeholders took a stronger approach to creating a compromise to stop unlawful exploits then significant threats to cyber security could be reduced (Klenka, 2021). As a result of this, there is a gridlock when it comes to finding international agreement on the laws and regulations of cyber security. This is due to a conflict between different states and nations on what the ideal cyber security laws should be with the minimal cost to economic output. Because of this, cyber criminals will likely have an upper hand when it comes to this, cyber criminals can perform their operations internationally and take advantage of other nation's weaker cyber security laws. This shows that cyber attacks are not going to slow down any time soon.

The Data Protection Act 2018 sets out a list of requirements for people to follow. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. This includes the guarantee that the information is used fairly, lawfully, and transparently, accurate and up to data, kept no longer than necessary, and appropriately protected from loss, damage, or unauthorised access (GOV, 2018). Failure to comply can result in fines, enforcement notices, or an investigation from the data protection regulator, the Information Commissioner's Office. Regulatory fines for non-compliance can be up to either 4% of annual global turnover or €20 million (Law Society of Scotland, n.d.). Not only is it illegal to commit cyber-attacks but a lack of security around people's private information could result in legal action. Therefore, the colleges who were under attack must ensure that the data they hold must be protected strongly to reduce the risk of legal issues.

8 Guidance to Prevent Future Attacks

WaterISAC (2016) state several cyber security measures to combat attacks. One option is to implement network segmentation. Network segmentation involves identifying and categorising IT assets, data, and personnel into different groups, and then restricting access to these groups. In the event of an attack where one device or sector is compromised, the rest of the network cannot be exploited. Without this, cyber attackers are able to find the "weakest chain in the link" to gain entry and then move laterally throughout the network, gaining access to data. This is a crucial step to preventing future attacks especially in the "Internet of Things" age. This is because there is now an abundance of technology that is now connected to the web and internal systems, meaning an attack could cripple many more devices then it would in the past. Therefore, it is of the utmost importance for colleges and universities to implement network segmentation to mitigate future attacks.

Since the colleges and universities were hit with ransomware, an employee cybersecurity training program would be recommended. According to WaterISAC, employees who are not involved in cyber security may leave threats and vulnerabilities unnoticed and "become conduits through which attacks are executed". Social engineering practiced by cyber criminals can affect employees in the form of phishing. Emails, phone calls and messages can entice untrained employees into providing sensitive data. This leaves a great vulnerability in the case of ransomware since untrained staff could be clicking on links, downloading infected attachments, and replying to messages they are not supposed to, thus putting the organisation they work for at risk. The Engine Room (2020) reported that there were two significant spear-phishing incidents in Ukraine in 2019. The first case in November was identified and reported. The second case occurred the following month where activists were sent targeted emails. The attack was on-going by February with the total messages increasing to fifteen. All of them were specifically targeted which indicated there was one group behind the attack. Making sure anything suspicious gets reported is paramount for organisations. The faster it is identified as a threat, the quicker it can be dealt with, in turn this will lead to minimal damage to the company or public body. Crucially staff must be trained to identify anything that could put the company in danger and must be trained to deal with the issue when the time comes.

9 References

Bourne, V., 2020. THE STATE OF RANSOMWARE 2020. [online] 1(1). Available at: <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf> [Accessed 15 May 2021].

Brenner, S., 2009. *Cyber Threats the Emerging Fault Lines of the Nation State*. 1st ed. Oxford: Oxford University Press.

GOV.UK., 2018. *Data Protection Act 2018*. [online] Available at: <https://www.gov.uk/government/collections/data-protection-act-2018> [Accessed 18 May 2021].

Gunarto, H., n.d. *Ethical Issues in Cyberspace and IT Society*. [online] Kyoto, p.2. Available at: <https://www.apu.ac.jp/~gunarto/it1.pdf> [Accessed 16 May 2021].

Klenka, M., 2021. Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, [online] p.3. Available at: <https://link-springer-com.proxy.library.lincoln.ac.uk/content/pdf/10.1007/s12198-021-00232-8.pdf> [Accessed 17 May 2021].

Kochovski, A., n.d. *Ransomware Statistics, Trends and Facts for 2020 and Beyond*. [online] Pentestmag. Available at: <https://pentestmag.com/ransomware-statistics-trends-and-facts-for-2020-and-beyond/#:~:text=In%202019%2C%20the%20average%20ransom,more%20sophisticated%20methods%20of%20attack.> [Accessed 14 May 2021].

Kuhn, A., 2020. *How (And What) Technology Can Help Combat Cyber Attacks - OnSolve*. [online] OnSolve. Available at: <https://www.onsolve.com/blog/technology-combat-cyber-attacks/#:~:text=Organizations%20can%20use%20blockchain%20to,Chase%2C%20Walmart%2C%20and%20UPS.> [Accessed 13 May 2021].

Matthews, C., 2021. *Bitcoin extortion: How cryptocurrency has enabled a massive surge in ransomware attacks*. [online] MarketWatch. Available at: <https://www.marketwatch.com/story/bitcoin-extortion-how-cryptocurrency-has-enabled-a-massive-surge-in-ransomware-attacks-11621022496> [Accessed 15 May 2021].

s.n., n.d. *Cybersecurity Failures: Top 6 Reasons | The CEO Views*. [online] The CEO Views. Available at: <https://theceoviews.com/top-6-reasons-for-cybersecurity-failures/#> [Accessed 12 May 2021].

s.n., n.d. *Distributed Denial of Service: Anatomy and Impact of DDoS Attacks*. [online] usa.kaspersky.com. Available at: <https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work> [Accessed 14 May 2021].

s.n., n.d. *The consequences of a cybersecurity breach | Law Society of Scotland*. [online] Law Society of Scotland. Available at: <https://www.lawscot.org.uk/members/business-support/technology/cybersecurity-guide/the-consequences-of-a-cybersecurity-breach/> [Accessed 18 May 2021].

Sutton, D., 2019. *Cyber Security: A Practitioner's Guide*. 8th ed. Swindon, UK: BCS, The Chartered Institute for IT, p.51.

The Engine Room, 2020. *Case study: Spear-phishing attacks*. [online] p.4. Available at: <https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-Spearphishing-attacks-June-2020.pdf> [Accessed 19 May 2021].

WaterISAC, 2016. *10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks*. [online] pp.2, 5. Available at: <https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf> [Accessed 19 May 2021].

Witts, J., 2021. *How To Stop Ransomware Attacks | The Best Ways To Stop Ransomware*. [online] Expert Insights. Available at: <https://expertinsights.com/insights/how-to-stop-ransomware-attacks/> [Accessed 13 May 2021].