12693154

Literature Review

Unit 7

**Topic: Financial Impact of Ransomware and Malware in United Kingdom**

**Introduction**

Cyberattacks have become more prominent and has become a significant threat to businesses and individuals alike. Specifically, the United Kingdom has noticed a rise in cyber incidents over the recent years leading to the breach of sensitive data and severe financial damage on affected entities. One of the most common attacks that is being done is that of ransomware, which involves encrypting the target entities data and demanding a ransom be paid for the decryption key of the encrypted data. This kind of cyber attack is known for how it disrupts operations and adds a financial burden to the targets.

These attacks have significant financial impact on several different sectors in the UK, including the health, financial and public sector. Considering this rise, the United Kingdom has implemented regulations that entities must follow in order to protect the data of its citizens and businesses which includes the GDPR and UK Data Protection Act. The United Kingdom has also released a guide titled the “Financial Sanctions Guidance for Ransomware”. It is clear that with all the attacks that have taken place that the United Kingdom has actively taken steps in order to ensure the protection of data.

However, it can be noted that with the implementation of the Financial Sanctions Guidance for Ransomware and other acts that more financial liabilities do fall on companies should there a breach of these acts. Therefore, considering the financial liability that is being imposed from the ransomware side and the government, the following research question can be asked: what is the financial impact of ransomware on businesses and government in the United Kingdom?

**Methodology**

With this literature review, we need to answer the question of what is the financial impact of ransomware on business and government in the United Kingdom? To assess the financial impact of ransomware attacks on businesses and the government in the United Kingdom, a literature review of peer reviewed papers, articles and journals around this topic can be done. This will consist of an in-depth analysis on the chosen peer reviewed articles and journals around the topic in order to gain a better understanding around the impact of ransomware, how it works and the effects there of on businesses within the United Kingdom. These resources will be gathered mainly from the internet articles found from accredited publishers as well as directories such as Google Scholar, JStor and Research Gate where scholars can find journals on the topic at hand. It is important that peer reviewed content is preferred over other content. By using these sources, we can establish the knowledge that is currently known on the topic and discuss points that could be explored further. (Snyder, 2019)

**Research**

In order to fully understand the research question, we need to define what exactly ransomware is and how it has evolved through the years. Ransomware is a malicious piece of malware that encrypts files and folders on a target device. This can scale vary from a single device being targeted to a whole network of devices being targeted and encrypted. Once the encryption is complete, the devices are held at ransom until a payment is made for the decryption key. (Palmer & Osborne, 2023)  
Between the years from 2016 to 2019, there seemed to be a shift in ransomware attacks moving from attacks focused on quantity to quality. Rather focusing high value targets than attacking multiple low value targets. Cybercriminals also rather shifted from automated ransomware attacks to targeting businesses and organizations to extort them with the goal of hindering and potentially stopping daily operations for the target. This turn for cybercriminals has resulted in much more profitable attacks than previously with the mass attack on computer networks. This has also resulted in sophisticated cybercriminal groups being formed with these groups adapting the new extortion model of targeting high profitable targets.  
The United Kingdom has seen a lot of ransomware cyber attacks affect the country. In 2020, the local government of Redcar and Cleveland suffered an attack that left them with a repair bill totalling 18 million great British pounds, which is more than double the 7.4 million great British pounds allocated to the government. The attack lasted roughly three weeks where government members were instructed not to use any government device during this period. The result of this attack was the Redcar and Cleveland government building a new server. (Pidd & Robinson, 2020)  
A more recent attack in 2024 targeted a high school in the south of London, Charles Darwin School. This left approximately 1300 students without classes for half a week. The school responded to the attack quickly, disabling all relevant accounts linked to students, formatting the devices used by teachers. Students were also asked to be vigilant with their emails and not to respond to any mails that seem suspicious. It was to be noted that the attack was similar to other attacks that the NHS, National Rail, Transport of London and other schools had experienced recently as well. It was also noted that attacks with in the sector of childcare has been on the rise as well. (Martin, 2024b)  
Highlighting the attack on the National Health Service (NHS), the United Kingdom NHS was affected by the “WannaCry” ransomware attack which attacked dozens of facilities leading to the more than 60 NHS trusts which led to patient records being inaccessible. This attack reached to even more countries affecting countries as far as Canada. These countries were not affected by the attack with most of the hospital anti-virus software sandboxing the attack. (Collier, 2017)  
The United Kingdom has responded to the increase in ransomware attacks by introducing financial sanctions against ransomware. This guide released by the government of the United Kingdom outlines the process businesses and individuals should follow should they be attacked. It was stated explicitly that the government does not condone businesses paying for the ransom and that the attack must be reported to the government. The Office of Financial Sanctions will then step in to handle the attack further with the correct authorities. Targets who do not follow the regulations put in the place by the government could face penalties on top of the ransom that would need to be paid. (Martin, 2024a) (Office of Financial Sanctions Implementation, 2024).

**Discussion**

It is clear that ransomware is a threat that can cripple any target today. We can also see that not only the United Kingdom has been affected by these kinds of attacks. The United Kingdom, however, has been a prime target for these attacks which clearly has had severe financial implications on the government sector, school sector and health sector. The ransomware attack against Redcar and Cleveland left damage of 18 million great British pounds which the government in the end could not afford to pay as it was above the yearly quota given to the Redcar and Cleveland government. The government of the United Kingdom has responded effectively to the rise in ransomware attacks with the Office of Financial Sanctions issuing guidelines for those affected by ransomware attacks. The question that must be brought forward however, are these guidelines in the interest of protecting the government or protecting the targets? It is clearly stated in the Office of Financial Sanctions Implementation that if an entity targeted with a ransomware does not report the attack or pays the group responsible for the cyber-attack, additional cost will be placed on the company targeted by the attack. This implies the targets could have their businesses crippled just by fines issued by the government. Considering this, the question has to be asked, what is the financial impact of ransomware on business and government in the United Kingdom? As it would appear in the United Kingdom, the government is protecting itself more than it protects the targets of ransomware attacks.

**Conclusion**

Ransomware attacks has evolved over the years into a very serious threat for any entity, business or government. Ransomware has over the years progressed from being used on the masses to being used on high profile entities with cybercrime groups being formed to target these entities. Businesses and governments have started to respond to the on-going threats and have implemented safeguards and protocols to try and minimize the amount of damage such an attack can due to an entity. Specifically focusing on the United Kingdom, after having various critical systems compromised, have implemented safe guards and financial sanctions to try and circumvent ransomware attacks. However, after considering the sanctions put in place, one has to ask the question, is the United Kingdom government trying to protect itself or the targets of ransomware with the potential fines that can be imposed on ransomware victims? What truly is the financial impact of ransomware on business and government in the United Kingdom?

**References**

Collier, R. (2017) ‘NHS ransomware attack spreads worldwide’, *Canadian Medical Association Journal*, 189(22). doi:10.1503/cmaj.1095434.

Gecsoyler, S. (2023) *UK at high risk of ‘catastrophic ransomware attack’, report says*, *The Guardian*. Available at: https://www.theguardian.com/technology/2023/dec/13/uk-at-high-risk-of-catastrophic-ransomware-attack-report-says (Accessed: 14 September 2024).

Hernandez-Castro, J., Cartwright, A. and Cartwright, E. (2020) ‘An economic analysis of ransomware and its welfare consequences’, *Royal Society Open Science*, 7(3), p. 190023. doi:10.1098/rsos.190023.

MacColl, J., Husch, P. and Nurse, J.R.C. (2022) *Beyond the bottom line: The societal impact of ransomware*, *Royal United Services Institute*. Available at: https://rusi.org/explore-our-research/publications/commentary/beyond-bottom-line-societal-impact-ransomware (Accessed: 15 September 2024).

Martin, A. (2024a) *Exclusive: UK to propose mandatory reporting for ransomware attacks and licensing regime for all payments*, *Cyber Security News | The Record*. Available at: https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks (Accessed: 16 September 2024).

Martin, A. (2024b) *Ransomware attack forces high school in London to close and send students home*, *Cyber Security News | The Record*. Available at: https://therecord.media/ransomware-attack-forces-london-high-school-to-close (Accessed: 14 September 2024).

Office of Financial Sanctions Implementation, 2024, Financial sanctions guidance for ransomware, https://www.gov.uk/government/publications/financial-sanctions-guidance-for-ransomware/financial-sanctions-guidance-for-ransomware#sectoral-sanctions-risk

Palmer, D. and Osborne, C. (2023) *What is ransomware? everything you need to know and how to reduce your risk*, *ZDNET*. Available at: https://www.zdnet.com/article/what-is-ransomware-everything-you-need-to-know-and-how-to-reduce-your-risk/ (Accessed: 14 September 2024).

Pidd, H. and Robinson, G. (2020) *Ransomware attack leaves council facing huge bill to restore services*, *The Guardian*. Available at: https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack (Accessed: 15 September 2024).

Sakellariadis, John. 2022. "Behind the Rise of Ransomware." Atlantic Council. Accessed September 16, 2024. [https://www.jstor.org/stable/resrep42765]

Snyder, H. (2019) ‘Literature review as a research methodology: An overview and guidelines’, *Journal of Business Research*, 104, pp. 333–339. doi:10.1016/j.jbusres.2019.07.039.