**Module 11 Assignment**

Alice Mace

Cybersecurity, Bellevue University

CYBR 615: Cybersecurity Governance & Compliance

Professor Erich Krueger

February 25, 2023

Our nation is affected by so many threats in many different spheres, many that continue to evolve and become more complex as technology improves. Businesses and other organizations commonly face cyberattacks that can be detrimental to their data, operations, and credibility. A cyberattack is a “deliberate exploitation of computer systems, technology-dependent enterprises and networks” that “use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes.” (Techopedia, 2019) Examples of cyberattack methods are phishing, spoofing, denial of service, viruses, worms, malware, and many others, and these are commonly committed by threats such as criminal groups, foreign nation states, hackers, insider threats, or terrorists. (Otero, 2018) This paper will take a look at two cyberattacks that occurred in the United States over the last few years, as well as security audit controls and procedures that would’ve helped to mitigate or reduce the impact of the attacks.

**Attack 1 - Ryuk Attack on Universal Health Services**

In September 2020, Universal Health Services (UHS) had to shut down their systems around the United Statue after it was affected by ransomware, that likely started by a phishing attack (*UHS Hospitals Hit by Ryuk Ransomware, Forced to Shut Down Systems*, 2020), and resulted in about $67 million lost in operating income, labor expenses, and recovery costs. (Dinu, 2022) UHS is one of the largest healthcare services providers that, “through its subsidiaries, the company operates 26 Acute Care hospitals, 328 Behavioral Health inpatient facilities, and 42 outpatient facilities and ambulatory care centers in 37 states in the U.S., Washington, D.C., Puerto Rico and the United Kingdom.” (*UHS Hospitals Hit by Ryuk Ransomware, Forced to Shut Down Systems*, 2020) There was no evidence of access or misuse of patient or employee data, but during the attack, “files were being renamed to include the .ryk extension” which is commonly used by the Ryuk ransomware, and screen displays changing to “display a ransom note reading "Shadow of the Universe," a similar phrase to that appearing at the bottom of Ryuk ransom notes.” (*UHS Hospitals Hit by Ryuk Ransomware, Forced to Shut Down Systems*, 2020)

Three types of information security controls that could’ve assisted in the prevention and handling of this cyberattack are threat management, trust management/encryption, and incident management. “Threat management includes virus protection, spam control, intrusion detection, and security event management.” (Otero, 2018) This may have helped to prevent or detect the malware sooner, in addition to user awareness training when a system is infected. Trust management includes the use of encryption and access controls. If this attack did stem from a phishing email, if the use of email encryption had been mandatory for authorization to open an email, it may have prevented the breach entirely. Lastly, incident management focuses on the how to handle things like security incidents, malfunctions, loss of power or communications servers, installation mistakes, and access violations. While there was no evidence of data spillage or leaks, a quicker reaction and ability to identify, report, prioritize, and analyze the situation may have reduced the amount of downtime servers had to be shut down to address the threat. (Otero, 2018)

**Attack 2 - Marriot Data Breach**

In January 2020, Marriott suffered a breach into their system that provides services to guests at hotels by compromising the user login credentials of two employees. It was not discovered until the end of February 2020 and they believe the compromise consisted of contact information, loyalty account data, personal details, partnerships and affiliations, and stay details of approximately 5.2 million guests. (Zorz, 2020) Marriott is the largest hotel chain in the world with over 8,000 properties in 139 countries and territories, but thankfully it is believed that no account passwords, payment information, or state/national ID numbers were disclosed. (*We Are*, n.d.) One of the investigating organizations believes the data collected would likely be used for various cybercrimes like phishing campaigns targeted on business email accounts or other customer affiliations. (Zorz, 2020)

A few information security controls that could’ve assisted in the prevention and handling of this cyberattack are vulnerability management, threat management, and identity management. Vulnerability management helps to combat risks by identifying, evaluating, and mitigating risks through asset and change management. This can include processes or policies that govern how passwords and username information should be configured and frequency of changes. This may have assisted in the prevention or earlier detection of the data breach. Threat management controls may have been able to detect and alert on possible scripts or abnormal IP addresses accessing and running within the network. Identity management “is the process used to determine who has access to what in an organization” and can encompass how to maintain login credentials for multiple accesses without compromise by writing them down or using simple words. Others assessing the data breach noted that had Marriott incorporated two-factor authentication and user account activity monitoring, it likely would’ve prevented or substantially decreased the data compromised. (Zorz, 2020)

**References**

Dinu, C. (2022, February 12). *Ryuk Ransomware Attack Cost UHS $67M in Lost Revenue*. Heimdal Security Blog. https://heimdalsecurity.com/blog/ryuk-ransomware-attack-cost-uhs-67m/

Otero, A. R. (2018). *Information Technology Control and Audit, Fifth Edition* (5th ed.). Auerbach.

Techopedia. (2019, February 5). *Cyberattack*. Techopedia.com. https://www.techopedia.com/definition/24748/cyberattack

*UHS Hospitals hit by Ryuk ransomware, forced to shut down systems*. (2020, September 29). 2020-09-29 | Security Magazine. https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems

*We Are*. (n.d.). Marriott International. https://www.marriott.com/marriott/aboutmarriott.mi

Zorz, Z. (2020, May 28). *Marriott International 2020 data breach: 5.2 million customers affected*. Help Net Security. https://www.helpnetsecurity.com/2020/04/01/marriott-data-breach-2020/