Module 4: Risk Assessment Report Assignment

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-7990-101: Capstone

Dr. Rosemarie Pelletier

September 24, 2023

Module 4: Risk Assessment Report Assignment

Assets associated with and threatened by the ransomware attack include, at a minimum, four offshore platforms (Georgetown University, n.d.-a, para. 1). These platforms were infected by the ransomware and are directly impacted by the threat actor. Additionally, the remaining six platforms are technically threatened as the threat actors appear to have maintained persistence in the environment and can retaliate (Georgetown University, n.d.-a, para. 1; Georgetown University, n.d.-b, para. 2). Each "control system application package" at each offshore platform "costs approximately $2.5 million" (Georgetown University, n.d.-a, para. 4). This brings direct costs to $10,000,000 if all four offshore platforms remained encrypted or were lost. Downtime costs can be estimated from some of the metrics we have been given—including the fact that a single offshore platform produces approximately $300,000 of revenue per day (Georgetown University, n.d.-a, para. 9). Thus, a single day of downtime would cost Ackme approximately $300,000 x 4 = $1.2 million. Therefore, in this quantitative assessment, there are significant costs associated with inactivity from Ackme. Ackme must ultimately decide to either pay the ransom or pursue an alternative restoration method as was what was suggested in this course's Module 4—using backups (Georgetown University, n.d.-b, para. 2).

As part of a combined or hybrid risk assessment approach, I will also look at qualitative components of Ackme's ransomware incident. Using backups to restore carries a LOW (x1) chance of failure but with a HIGH (x3) impact of data loss and disruption to operations. Thus, Ackme carries a qualitative risk of 1 x 3 = 3 restoring from backups. Next, Ackme is potentially under the threat of retaliation from the adversary for restoring from backups (Georgetown University, n.d.-b, para. 2). This risk could be represented with a MEDIUM (x2) probability of retaliation from the ransomware threat actor with a potential HIGH (x3) impact. This risk is

approximately 6 (2 x 3) and is added to 3 (from the first qualitative assessment) to equal 9. Additionally, the HIGH impact is justified, as the adversary has already demonstrated successful attack capabilities having encrypted four Ackme platforms and successfully deploying ransomware. They can simply decide to destroy or not give the encryption keys or exploit any kind of remote access they have already obtained to increase the impact against Ackme. Paying the ransom provides a different qualitative assessment. Ackme would have a MEDIUM (x2) probability of failure to restore systems and a HIGH (x3) impact of data loss and disruption to operations. I set the probability of restoration failure at MEDIUM as there is no guarantee that organizations can fully recover all data and systems by paying a ransom after a ransomware attack (Buffington & Webb, 2023, para. 3). This brings out the initial risk total to 6 (2 x 3). Next, the impact is HIGH, as previously mentioned, each platform contributes to approximately $300,000 worth of revenue a day (Georgetown University, n.d.-a, para. 9). However, when discussing retaliation, it must be noted as a key difference with paying the ransom versus restoring from backups. It is unlikely the threat actors would retaliate if a ransom was paid or the payment was in progress. Thus, the probability of retaliation is LOW (x1) and the potential impact is MEDIUM (x2) as the threat actors would not likely want to destroy a company that is trying to pay their ransom. Thus, the total risk from paying the ransom comes out to 2 + 6 = 8. However, additional concerns must be specified and understood during a valid risk assessment. Those include legal and regulatory concerns that potentially govern Ackme. Ackme specifically may be subject to the Office of Foreign Assets Control (OFAC) with their oversights and sanctions (OFAC, 2021, pp. 3-5). Ransom payments per OFAC may be illegal (Gross Mendelsohn, 2021). However, actual enforcement data is sparse, and it is unclear how likely it is for Ackme to be criminally charged or pursued for making a ransom payment. However, looking

at the prosecution of perpetrators of ransomware, it was found that prosecution efforts were, unfortunately, few due to numerous reasons (Freeze, 2023, para. 1). Thus, I determined the probability of legal consequences of paying a ransom to be LOW (x1), but the impact to be HIGH (x3). This brings the legal risks of paying the ransom to be 3 (1 x 3). I determined the impact to be high as if prosecution is successful, Ackme could be forced to pay "millions" in dollar fines for producing a ransom payment (Concord Law School, 2021). If Ackme, however, chooses to respond to the incident by the proposed plan via backups and restoration processes, Ackme effectively accrues zero legal risk due to a zero chance of legal prosecution (as no ransom payment was made). Due to the legal and regulatory risks involved, the risk score of paying the ransom rises to 11 despite the risk of restoring from backups, which stays at 9. Finally, Ackme is an organization licensed by the BSEE (Bureau of Safety and Environmental Enforcement) to provide crude oil and natural gas from ocean-based offshore platforms to domestic American companies nationwide (Georgetown University, 2020, pp. x-1; BSEE, n.d.). Ackme reportedly had their critical "Historians" affected during the cyber incident, which are also involved in their reporting obligations to the BSEE (Georgetown University, n.d., para. 3). Ackme offshore platform operators reportedly must act manually in place of the missing Historians (Georgetown University, n.d.-a, para. 3). The BSEE can conduct random audits, known as "spot checks," against regulated companies, including Ackme (BSEE, 2021, pp. 1-2). Failure to produce necessary records can lead to a "shut-in," where the BSEE essentially closes a facility and penalizes the license holder (BSEE, 2021, p. 2). Therefore, as previously stated, Ackme must act to prevent a forced closure. Furthermore, if paying the ransom and restoring from backups are given equal probabilities of success, the impact is the same, which allows Ackme to quickly produce records for BSEE auditors and adequately respond to inspections.

Thus, for this qualitative analysis, both compared options are viewed equivalently and no further numerical additions are needed. Thus, restoring from backups (total risk score of 9) becomes the preferred option after both a comprehensive quantitative and qualitative risk analysis.

Restoring from backups is not always easy, especially after a serious ransomware incident that has already crippled systems and necessitated such a move. Thus, as CISO, I recommend we perform risk mitigation against the backup plan or proposal. A risk mitigation approach would be for Ackme to restore systems individually to confirm they have the capability for restoration with the alleged method. If Ackme takes all systems offline and the adversary cannot beacon the victim hosts, they may suspect Ackme is attempting data recovery without paying the ransom and may seek retaliation, such as exploitation of remaining hosts or sabotage to achieve the MITRE tactic of "impact" (MITRE, 2019). Thus, taking only one host offline to attempt a successful data recovery would be their best option to determine if both their method is effective and to avoid alerting the attacker to their course of action. If the adversary asks why that host is offline, we can say there is a local Internet outage at that site and we intend on paying the ransom for all platforms as soon as the CFO (Chief Financial Officer) approves the payment. This will buy Ackme the most time with the adversary and will also allow us to fully attempt the data recovery method without prematurely interrupting it. Furthermore, if data restoration attempts fail and Ackme must resort to paying the ransom, we will have legal proof that we exhausted our only available alternative. We could potentially use this to our defense and help mitigate any criminal charges or adverse regulatory actions pursued against us.

As CISO (Chief Information Security Officer), I highly recommend we pursue the data recovery option for each host individually. This is based on a hybrid risk assessment and mitigation strategy. As CISO, I am also tasked with being the guardian of Ackme's CIA triad

(Confidentiality, Integrity, and Availability). Because of this incident, we have seen a degradation of all three components of this critical cybersecurity concept. A backup recovery process done per the mitigation strategy will align our organization towards recovering from this degradation and return to a highly available and secure enterprise. This is our best course of action to mitigate potential retaliation from our adversary as well as confirm our recovery abilities. I do not recommend we rush into any solution. Rather, we ease into it with available resources and foresight to enable us to utilize the best options present. Thus, if our data recovery methods were to fail, we could easily "failover" into paying the ransom payment, still individually, to recover our data and restore hosts that way. The costs of doing nothing are too high, therefore, we must not stand idly by, but must swiftly act with strategic precision and prudence. I strongly believe Ackme can overcome this incident after following this restoration plan.

References

BSEE. (n.d.). *Oil & gas*. Bureau of Safety and Environmental Enforcement. Retrieved September 16, 2023, from https://www.bsee.gov/oil-gas

BSEE. (2021). Inspections Fact Sheet. In *bsee.gov*. Bureau of Safety and Environmental Enforcement. Retrieved September 16, 2023, from https://www.bsee.gov/sites/bsee.gov/files/fact-sheet//fnl-fact-sheet-bsee-inspections-5621.pdf

Buffington, J., & Webb, J. (2023). Should I pay the ransom after a ransomware attack? *Veeam Software Official Blog*. https://www.veeam.com/blog/ransomware-attack-paying-or-recovering-2023.html#:~:text=Unfortunately%2C%20even%20paying%20ransom%20doesn,2023%20Data%20Protection%20Trends%20Report

Concord Law School. (2021, February 5). Ransomware victims who pay the ransom could face millions in fines. *Concord Law School*. Retrieved September 21, 2023, from https://www.concordlawschool.edu/blog/news/ransomware-victims-face-fines/

Freeze, D. (2023, July 10). *Global Ransomware Damage Costs Predicted To Exceed >65 Billion By 2031*. Cybercrime Magazine. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Georgetown University. (n.d.-a). *Module 3: In the Thick of a Ransomware Attack* [Slide show; Canvas]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-3-in-the-thick-of-a-ransomware-attack?module_item_id=3283361

Georgetown University. (n.d.-b). *Module 4: Do or Do Not* [Slide show]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-4-do-or-do-not?module_item_id=3283367

Georgetown University. (2020). H. Ackme Oil & Gas Background Material. In *Google Drive*. Retrieved September 7, 2023, from https://drive.google.com/file/d/1TDoFQQWPZTgWTncVxTrKOfP2rMGkz_Re/view

Gross Mendelsohn. (2021, August 26). *Paying Ransom On a Ransomware Attack Is Illegal*. gma-cpa.com. Retrieved September 21, 2023, from https://www.gma-cpa.com/technology-blog/paying-ransom-on-a-ransomware-attack-is-illegal

MITRE. (2019, July 25). *Impact, Tactic TA0040 - Enterprise*. MITRE ATT&CK. Retrieved September 23, 2023, from https://attack.mitre.org/tactics/TA0040/#:~:text=The%20adversary%20is%20trying%20to,manipulating%20business%20and%20operational%20processes.

OFAC. (2021). Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. In *Office of Foreign Assets Control*. Department of Treasury. Retrieved September 23, 2023, from https://ofac.treasury.gov/media/912981/download?inline