**Project Three:**

**Technical Brief**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

April 21, 2024

1. **Introduction**
   1. The scenario I chose to analyze for this project is scenario three. The threat actor in this scenario are social engineering attacks such as shoulder surfers, who are known to “look over the shoulder of a person” (Kim & Solomon, 2023) to gain access to sensitive information. What would motivate this threat actor to steal sensitive information is gaining access to other student accounts and committing identity theft. From there the threat actor can use identity theft to commit fraud for financial gain or make changes to student grades using another person’s account to avoid being caught. Another threat actor in this scenario is scammers. Scammers can steal all the students’ emails posted on the door by the professor and send them phishing attacks. In a phishing attack, scammers will send emails or send a link to a webpage to trick people into thinking it’s real to get people to share sensitive information so they can use for financial gain.
2. **Analysis**
   1. A best practice for detecting these threat actors is to regularly monitor to help detect and unauthorized access or activity with student accounts. Another best practice for detecting these threat actors is to implement the principle of least privilege to help restrict access to sensitive information only to those who need it for their roles or responsibilities (Tjaden, 2015). This will help minimize others from having access to everyone students’ sensitive information.
   2. A legal and ethical factor that should be considered is people’s right to privacy when it comes to sensitive and personal information. Laws such as Family Education Rights and Privacy Act (FERPA) “applies to all schools where schools must have written permission from a parent before releasing any information contained in a student’s education record” (Kim & Solomon, 2023, pg. 128). The professor posting personal student information can go against this law and cause legal action to be taken by parents if their students are harmed or attacked.
   3. One tactic or method that is important in responding to and countering this threat actor is immediate notification and communication. The school must notify the affected individuals and guardians, school leaders, and any others as required by law or school policy. Provide clear and timely communication about the incident, including the attack used, the steps being taken to address it, and any potential risks or implications for the affected individuals.
   4. One tactic or method that would be employed to reduce the likelihood of the same situation happening again is to implement the design principle of least privilege. This will help keep the professor from posting student personal information for everyone to have access to. Another is to implement security awareness training for the students. This will help students be aware of situations like this and act before their personal data is leaked. This will also help students understand what to look out for when an incident has happened such as phishing emails or monitoring their personal accounts.
3. **Conclusion**
   1. A potential ramification to the tactic of implementing security awareness training, there is no guarantee that all employees and students will fully complete, absorb, and apply the knowledge gained from the training. According to Steve Buege (2021) “It’s always difficult to achieve 100% employee participation.” Most companies struggle to achieve 100% completion rates whereas students would most likely have even lower completion rates. This would make the training ineffective and cost more time and resources to constantly remind students.

**References**

Buege, S. (2021, November 22).Security awareness training: Top challenges and what to do about them. *Security Magazine*. https://www.securitymagazine.com/articles/96565 security-awareness-training-top-challenges-and-what-to-do-about-them

Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. https://openpage ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST3209 3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1

Tjaden, B. C. (2015). Appendix 1: Cybersecurity first principles. Retrieved from https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf