**Task 3**

Abow125

John Mammen

July 04, 2023

**Proposal Topic:**

Our company has recently been hacked and we need to update security protocols.

**Significance of problem:**

With our company recently experiencing a breach in data, it’s in our best decision to make a few changes. Keeping sensitive data safe is our responsibility. We’ve already experienced that we are not where we should be. Updating security protocols increases our ability to defend against cyberattacks. There are many things we can do to improve our security. Our primary focus in improving security is to do so in a way that limits vulnerabilities. The best thing we can do is to move forward with a plan.

**Thesis-** The best solution to prevent future data breaches is to implement stronger security protocols because they make it harder for hackers to access sensitive data and they will increase employee awareness of threats.

**Course of Action:**

The first step in our plan is identifying what parts of our business are most vulnerable to cyber attacks. These are the places targeted first and the most often. The most vulnerable would be things like servers, databases, and network devices. We cannot eliminate every risk. Vulnerabilities are prioritized by how our business will be affected if compromised. We can make this decision with the aid of a certification test. “The certification test ascertains the truth about the vulnerabilities to the greatest extent possible” (Mowbray, 2013 p. 140). Investing in our security and implementing better security protocols save us money in the long run. One of the goals of a cyber criminal in an attack is to gain access to customer data. Customer data includes passwords, bank account details, and social security numbers. Private information that we are responsible for. Allowing threat actors to expose and exploit vulnerabilities would cost more than our organization. Not only are our customers at risk of losing their livelihoods from being victims of identity theft, but we risk our reputation with said customers.

The next step in our plan is to implement a strong-password policy. A strong password policy is a set of requirements for password creation that encourage users to create stronger passwords. A strong password policy also includes rules regarding how often to reset passwords. According to (Landsberger, D., 2019), resetting your password on an interval is the easiest and most impactful thing we can do when it comes to IT security, and it shouldn’t cost us anything. The recommendation for how often we reset passwords is every 90 days. Increasing password strength makes it harder for hackers to infiltrate user accounts and access sensitive data.

The third step in our plan is to enable Multi-Factor Authentication. Enabling MFA adds another layer of protection from cyber criminals. In the event a hacker gains access to a user account via password, MFA will send a notification to the account owner. The user will then verify if they are trying to access their account. If the answer is no, the next step is a password reset. The notification usually comes via text or email. There are many ways to authenticate, but these two are the most common.

The final step is employee training. The cybersecurity field is constantly evolving. Keeping up-to-date on the latest cybersecurity practices is in a company’s best interest. The first and most important place to train is on phishing. Phishing is when a cyber criminal sends, usually an email, to a member of an organization in an attempt to gain their account details. According to (Eitel, B. 2023), phishing causes 90% of data breaches. Employees are the cause 9 out of 10 times. Having a properly trained staff cuts down cyber attacks by a large margin.

**Challenges and rebuttal:**

Some might argue that implementing stronger security protocols would be too expensive and out of the budget. Implementing stronger security protocols begins with a shift in company culture. Three of the four steps in the plan cost us next to nothing. Our investment would be in time, but developing a company mindset surrounding strong security makes the shift and future changes easier to implement. Employee training is the only step that could cost us resources. We can source the training from authorities in cybersecurity, like CompTIA. They host free and low-cost company training on their website. The risks of implementing this plan are small and worth taking.

**Conclusion:**

Companies need to be responsive to changing ways; this includes improving how they protect their data. We have already been victims of a data breach. Our best option to limit future hacks is to update our security protocols because they make it harder for cybercriminals to access sensitive data and they will increase employee awareness of threats. Things like identifying our most valuable assets, implementing a strong password policy, and enabling Multi-Factor Authentication prevent future hacks and are cost-effective. While, beginning and maintaining employee training will increase overall awareness of security threats. Anything we can do to make the slightest difference is better than waiting for another attack. Our customers deserve to know they can trust us with their sensitive data. We must be proactive about security; our reputation depends on it.

**References**

Landsberger, D. (2019). Security Awareness Training: Passwords Are a Pain – But They Are Critical to IT Security. https://www.comptia.org/blog/security-awareness-training-passwords

Eitel, B. (2023). 4 Simple Steps to Better Protect Your Company from Cyberattacks. National Cybersecurity Alliance. https://staysafeonline.org/resources/4-simple-steps-to-bet ter-protect-your-company-from-cyberattacks/

Mowbray, T. B. (2013). Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions. http://ci.nii.ac.jp/ncid/BB15795615