**Week 5: Project One (Cybersecurity Policies)**

Author(s)

Affiliation

Institution

Instructor

Date

**Project One Memo Template**

**DATE:** January 28th 2023

**TO**: Company Leadership Team

**FROM:** Information Security Manager

**SUBJECT:** Recommendations to Address Multiple Identified Security Risks

**Introduction:** As the recently hired Information Security Manager for our e-commerce company, I am addressing you through this memo to inform you of a recent third-party consultant evaluation of our information security posture. The assessment revealed several high-level security risks that must be discussed in order to protect our company's important information assets.

It is worth mentioning that addressing these aspects of information security is critical to our company's advancement and success. We can reduce the risks of data breaches by utilizing the recommended measures, which can lead to substantial financial losses, reputational damage, and loss of customer trust (Ramachandran, 2020). We can ensure that industry standards and guidelines are followed, thereby preventing costly fines and penalties.

I have created a set of recommendations to discuss several discovered security risks. These suggestions are intended to be effective, efficient, and in line with our company's general business objectives. I have also included reasons for my decisions to give you a better understanding of why I made each suggestion.

**Laws and Regulations:** Information security risks are often found in an organization’s information management policies and procedures. Information technology has many laws and regulations that must be followed by businesses. One such regulation is the Sarbanes–Oxley Act of 2002 (SOX). This law requires publicly traded companies to maintain strong internal controls designed to help prevent unauthorized access to important data, including electronic files, networks, applications, systems and data (Ramachandran, 2020). In addition, SOX also takes on accounting fraud through enhanced record-keeping and financial reporting standards as well as cybersecurity responsibilities for all federal contractors that use the nation’s critical infrastructure. This Sarbanes laws when followed well it will protect the assets of this company.

To ensure the security of the company's information assets, this company is required to implement information security policies and procedures that include physical, technical and personnel controls (Ramachandran, 2020). If these laws and regulations are not followed, the company may face consequences such as financial fines and legal actions if it suffers from a data breach.

**Technical Controls:** The e-commerce company has several systems that were designed 5 years ago and are no longer reliable. The systems need to be replaced with software that is updated regularly and meets current security requirements (Milov, 2021). The company should logically separate open applications from sensitive data, use appropriate encryption technologies to protect sensitive data. The company also need to limit access to IT tools that are not required for day-to-day operations and change passwords often. Lastly, there is need to install antivirus software as frequently required to protect the company system data.

**Administrative Controls:** The information security risks identified by the consultant include; exposed SMTP service to staff; lack of appropriate permissions for managing user access; configuration issues in VNC and SSH services and uncontrolled configuration options for applications including weak passwords, outdated software and poor configurations (Milov, 2021). These issues must be addressed to ensure that all managed devices are secure. To addressing these risks, I recommend the company to reevaluate employees training and make improvements for new employees with the risk of being stuck with older technology that includes weak passwords and configurations with easy-to-guess credentials such as usernames and passwords (Milov, 2021). The company should not allow new employees to register accounts on the company network until they have received training on how to use IT resources. This will stop hackers from accessing critical information of the company from employees.

**Physical Controls:** The physical controls that I would recommend to address these risks are two-fold: the first being a digital certificate management solution, and the second being implementing identity and access management (IAM). By having digital certificates, users would be able to show their identification when accessing sensitive data. This could be achieved through a single sign on between different apps or websites which utilize the same credential or other means of identification. In addition, by implementing identity and access management, we can ensure that employee IDs are synchronized as well as logon credentials for IT staff so they can be tracked from their identification when accessing company network resources.

**Business Impact:** The proposed recommendations impact current information security policies and practices within this company by identifying and taking appropriate actions as needed to address identified risks (Milevskyi, 2021). In order to resolve these risks, the company will be required to address several areas within their security program to ensure that the systems being monitored effectively, layered protocols are in place with firewalls, data encryption for sensitive information and removable media. Employees training on security issues such as assigning clear responsibilities for creating new accounts, understanding and implementing proper device configurations, as well as strengthening links between internal operations and other external partners will ensure the company overcome security risks and earn more profit.

**Conclusion:** In Summary, the recommendations in this memo are essential for strengthening our company's information security stance. We can reduce the likelihood of data breaches and safeguard our company's important information assets by adhering to industry norms and regulations, such as the Sarbanes-Oxley Act of 2002, and implementing technical, administrative, and physical controls (Goutam, 2021).  This will result in significant financial savings, a better public image, and increased client trust. Moreover, by adopting digital certificates and identity and access management, we can ensure that employee IDs are synchronized and IT staff logon credentials are tracked, adding an additional layer of security.

**References**

Goutam, R. K. (2021). *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals (English Edition)*. BPB Publications.

Milevskyi, S. V. (2021). Fundamentals of construction and protection of microprocessor systems: working program of the discipline for students’ specialty in 125 “Cybersecurity” educational program “Cybersecurity” first (bachelor's) level.

Milov, O. V. (2021). Theoretical fundamentals of cryptography: working program of the discipline for students specialty in 125 “Cybersecurity” educational program “Cybersecurity” first (bachelor's) level.

Ramachandran, R. B. (2020). Introductory & Cybersecurity Fundamentals-Fall 2020.