CYBER SECURITY

Name:

ID:

Module Title and Code:

Semester/Year:

**Cyber Security**

I selected the topic since cyber security is an issue that affects all community members in one way or another. Cyber security is important since it can protect an organization and its customers from cyber threats that can have a devastating effect if they happen. Cyber security has been on social media for a long time as stakeholders try to establish whether the measures currently in use are adequate to protect organizations from malicious parties. It is also an issue I have experienced first-hand, and since it affects people around me and me directly, this influenced me to select the topic to discuss. Cyber security can enable organizations to protect their important data. Computer viruses can spread very fast in a computer system if adequate measures are not put in place to control them. Viruses are other malicious software that can damage systems and important corrupt files that may compromise the operation of an organization. Apart from that, the increase in the rate of cybercrime also influenced my decision to select the topic. If it is leveraged well, it can minimize an organization's exposure to some of these risks.

**Issues, policies and problems that need to be addressed in cyber security**

Cyber security is a combination of an issue and problem that, if not addressed adequately, can affect the ability of an organization to be productive. Research has shown that cyber security is one of the main priorities for many business owners today, and it needs to be addressed to ensure an organization achieves its goals (Cavelty, 2010). A study conducted by CBC money revealed that more than 80% of business enterprises in the United States had been hacked successfully. Since many hackers know the main vulnerability of businesses, it is relatively easy for them to exploit the vulnerabilities for personal gain. Some of the issues and problems that companies face in the industry include:

Unprecedented cyber attacks

There has been a significant increase in the amount of data organizations hold in their computer systems compared to the information contained in the olden days. Due to the drastic increase in the amount of data stored, the vulnerability of exploited organizations has also increased significantly (Conteh and Schmick, 2021). Confidential data is stored in various devices in different physical locations, making it challenging for an organization to monitor all the data. Business leaders are expected to create comprehensive plans to ensure their organizations are successful in the market.

Data theft

Contrary to why many people believe that small businesses are not targets of cybercrime, researchers have argued that they have become the principal target of cyber-attacks. Most of the cyber-attacks that are currently being done are targeted at small and medium-sized businesses. Many malicious parties target this enterprise as gateways into larger organizations since the larger organizations are usually better prepared to counter these issues. Although small organizations face similar cyber security threats as large organizations, they confront these issues with lesser resources. Most of them do not have adequate personnel to help them counter such problems (Ferreira and Cruz-Correia, 2021). While most small businesses handle cyber security risks on their own, most of these organizations do not know what measures they need to take to address such threats. Threats are only likely to grow further in this digital age of technology since, every day, hackers come up with innovative ways to breach security systems for their gain. Organizations can avoid many losses and ensure business continuity even in a cyber-attack if they take adequate measures to counter cyber-security threats.

Ransomware

Ransomware attacks have become more common. Research has shown that Ransomware attacks have hit more than 70% of organizations in the United States of America. A Ransomware attack is a cyber security attack whereby a hacker accesses user data and prevents the user from accessing the data until a ransom amount is paid. Ransomware attacks can be costly to individual users and even more costly for a business organization that may need the data for day-to-day operation (Conteh and Schmick, 2021). Organizations may also use the data to inform their decision-making processes. Without data, an organization may be unable to run its day-to-day task, which may significantly compromise its productivity. In many cases, the attackers do not release data even after the ransom is paid, and instead, they try to extort the individuals or organizations involved more money.

Software vulnerabilities

Even the most recently released software has a vulnerability that may be a significant challenge for cyber security. Since there has been a tremendous adoption of digital devices compared to what it was ten years ago, most people do not update the software on the devices. Some people ignore the updates because they think they are irrelevant. However, this is not the case. Using devices with older software versions is risky since malicious users can leverage these shortcomings to devastating effect. Newer versions of software have patches for security vulnerabilities that have been newly fixed (Alhayani et al., 2021). Most of these security features are not in the previous versions. Research has shown that attacks on unpatched software are one of the greatest challenges to cyber security. Most of these attacks are made by a large number of individuals working together as a team.

**Recommended Changes that can enhance the cyber security of an organization**

1. Build a company culture

TO adequately manage cyber security in an organization, the organizational culture is an important element. Owing to the ever-increasing cyber security risk, establishing a cyber-security-focused culture in all the levels of the organization, starting from part-time employees to the executives, will mitigate cyber security risk.

1. Distribute responsibility

The burden of maintaining cyber security is the responsibility of all the members of an organization, not just the IT personnel. There are many risks associated with cyber security, and without adequate knowledge, it is very hard to manage the risks and ensure the organization meets its goals (Radu and Smaili, 2021). Every employee should understand the role they play in the organization in preventing cyber-attacks. According to research conducted by Verizon, most of the data breaches experienced in organizations are caused by data phishing. Employees should be offered adequate training and be equipped with adequate tools that can enable them to identify risks and manage the effects of the risks in an organization. This will allow the employees to understand the potential risk and be accountable for all their actions in an organization.

1. Train employees.

Most of the time, employees are the weak link to cyber security in organizations. Therefore, organizations need to come up with continuous employee cyber security training to employees at all the levels of the organizations to enable them to be able to mitigate those risks. Employee training is one of the most effective ways to ensure that all the employees in an organization know how to use the information technology systems and devices to protect them from cyber security attacks (O’Connell, 2012). A suitable security awareness program should educate employees in an organization about the appropriate procedures to be followed when handling sensitive corporate data and other information technology assets. Employees should be equipped with knowledge concerning the kind of data they are allowed to share via various channels such as email and the steps they can take if they run across a security incidence. Other important topics that employees in an organization can be taught include clean desk policies, rules governing bring your own devices, and data management procedures.

1. Leverage a cyber security framework in the organization

An appropriate cyber security framework can be vital in mitigating cyber security threats in an organization (Shaw, 2021). Since no standard is suitable for all organizations, the business should identify a framework that best suits its needs. The cyber security framework to be adopted in an organization will also be influenced by the standards that have been dictated to be implemented in a certain industry. Commonly used standards include Center for Internet Security (CIS) Controls and Payment Card Industry Data Security Standard (PCI DSS).

1. Emphasize speed

Although an organization can implement various measures to prevent cyber security attacks, there is no guarantee that the implemented mitigations will be adequate to stop all the attacks. In the event of the occurrence of a cyber security attack, an immediate response should be made to mitigate the effect that the incident will cause. In many cases, the longer it takes for an organization to react to a cyber security attack, the greater the effect of the attack will be in an organization. While various studies have shown that most network administrators take 1 hour to detect a cyber security attack, this is a lot considering the amount of harm that can be done in 1 hour. A speedy reaction is an integral part of a security forward culture in an organization. An organization should identify the potential risks early and have a mechanism for rapid response to any reported incidents. Speed is of the essence when risk containment is concerned.

Implementing the proposed changes can result in numerous benefits for an organization. The world has become more reliant on technology. Technology has allowed human beings to conduct their activities with ease. An organization that implements the recommended cyber security mechanisms can save a lot of money (Geers, 2011). Due to an increase in cyber security incidents such as information breaches, he recommended that solutions enable an organization to remain competitive in the market. It can also allow an organization to prevent the occurrence of cybercrimes that may affect its day-to-day operations. The fast development of technology has led to an increase in the number of interconnected devices. This has led to a rise in cybercrime. The proposed measures can minimize an organization's exposure to cybercrime. Apart from that, it can increase an organization's credibility by protecting the organization's platform from associated risks. It can also protect an organization's customers from malicious parties.

Reference

Geers K. (2011*). Strategic Cyber Security*, Kenneth Geers

O’Connell M.E. (2012). *Cyber Security without Cyber War*, Journal of Conflict and Security Law

Cavelty M.D. (2010). *Cyber Security,* The Routledge Handbook of New Security Studies

Conteh N.Y., Schmick P.J. (2021). *Cyber Security Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks,* Ethical Hacking Techniques, and Countermeasures for Cybercrime Prevention

Ferreira A., Cruz-Correia C. (2021). *COVID 19 and Cyber Security: Finally and Opportunity to Disrupt*, Jmirx Med

Alhayani B., Mohammend J.H., Chaloob Z., Ahmed J.S. (2021). *Effectiveness of Artificial Intelligence Techniques against Cyber Security Risks Apply of IT Industry,* Materials Today: Proceedings

Shaw T.W. (2021). *Cyber Security for SCADA Systems*, Pennell Books, LLC

Radu C., Smaili N. (2021). *Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cyber Security Related Disclosure*, Journal of Business Ethics