Cyber Security Evaluation

Student's Name

Institutional Affiliation

Date

Cyber Security Evaluation

Various Concepts of Cyber-Security

There are three concepts of cyber-security, which include confidentiality, integrity, and availability. A reliable network should be confidential and not vulnerable to hackers. Hackers breach confidentiality for malicious or financial gain. On the other hand, cyber-security enhances the integrity of all stakeholders, systems, and users. Integrity helps in maintaining a focus for efficient policy implementation without hampering organizational productivity. Integrity helps in identifying the information of related assets, examining the possible potential threats, impacts, and vulnerabilities, deciding on models of addressing threats and risks while mitigating the share and accepting the nature of risks (Talib et al., 2018). Lastly, a system should be available uptime often based on the enterprise security paradigm. Availability guarantees that systems are efficient, where it is possible to respond to the users' information, and being in a position to safeguard resources.

Implementation Plan

Cyber-security implementation requires policies that guide in developing new security thresholds that help in protecting the organization as a unit while ensuring that the organization is developed to incorporate detailed opportunities and responsibilities.

Communication Plan

As an executive approach, it is important to notify team leaders on the suggested cybersecurity initiative. The cybersecurity initiative helps in developing logistics that would oversee the reduction of challenges that play a critical role in solving the challenges affecting the organization.

Setting Priorities

Priorities help in drafting a responsive plan of action. This further includes the integration of research for the consulted organization while ensuring explicit goals of cybersecurity are met. In drawing a reliable communications plan, the approach further includes risks management, contract management, and audit tracking and reporting (Craig et al., 2016). The approach further includes actionable ways of formatting communication goals.

Implementation

As a center of the communication plan, the approach includes mechanisms of measuring success. This includes the goals of creating a cyber-security plan, which would help in measuring the strengths and weaknesses of the established security metrics.

Types of Cyber-Security Threats

Cyber-security threats have been on the rise, and they keep changing with the changes in enterprise resource structure. Common cyber-security threats include malware, phishing, ransomware, spamming, botnets, SQL injection attacks, eavesdropping attack, hacking, and distributed denial of service (DDoS). These cyber-security threats constantly threaten the welfare of the organization. While there is no ranking of risks in each of the above named, it is clear that a network remains vulnerable when attackers combine one or more threats. Cyber attacks lead to the loss or damage of electronic data, leads to extra expenses, leads to the loss of income, increases the rates of network security and privacy lawsuits, and system vulnerabilities (Rizov, 2018). Other formats of cyberattacks lead to the possible extortion losses, which might lead to the destruction of an electronic key and might lead to the destruction of encrypted files. Destruction of information can heighten the company's reputation, and as such, customers might avoid doing business with the organization.

Principles of Underlying Development

An enterprise cyber-security policy framework requires specific principles of development, which helps in risks mitigation. Enterprise cyber-security policy framework includes standards, best practices, and guidelines that prioritize handling the rising challenges. Cyber-security is often a framework prioritized to be flexible, and the following principles are therefore considered. According to Kamenov (2018), the principles include keeping cybersecurity policies updated, insuring the Enterprise Architecture, training of security staff, prevention as the foundation, developing data storage patterns, and improving how data is accessible.

Alternative View Points

Cyber-security will remain a key threat, considering that attackers' keep strengthening their models of attacks. Worse still, there is a full underground internet, known as the Dark Web. Protocols of Dark Web and their specific browser, Tor, are more deadly and cannot be detected on the mainstream web. Although organizations are heavily investing in security measures, the degree of attacks is often crucial. Application developers such as Oracle have improved their security system, generally allowing growth and development of viewpoints.

Potential Implication

With the parallel growth of technologies and the possible introduction of collective big data analytics quantum physics on cybersecurity, one will notice that security will become extremely better (Kamenov, 2018). Operating systems such as Android have heavily improved resource framework, especially data management hence there will be better and more practical alternatives towards handling security threats. Meanwhile, the regulations channel has improved how resources are shared.

Assumptions

Cyber-security technologies and regulatory procedures have often remained efficient in controlling the nature of attacks. As the industry continues requesting deeper spending, it is possible to draw upon alternative mechanisms of enhancing security. Sponsored organizations will continue developing the cyberspace messages while developing skills for motive and continuous contribution for attacker ecosystems for highlighting abilities (Lehto, 2013). In the near future, organizations will continue working with institutions and nations to ensure that technical skills are improved, while still, users will become more wary of attacks.

References

Craig, A., Valeriano, B., & Bren, D. (2016). Reacting to Cyber Threats: Protection and Security in the Digital Age. *Global Security And Intelligence Studies*, *1*(2). doi: 10.18278/gsis.1.2.3

Kamenov, D. (2018). Intelligent Methods for Big Data Analytics and Cyber Security. *Information & Security: An International Journal*, *39*(3), 255-262. doi: 10.11610/isij.3921

Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. *International Journal Of Cyber Warfare And Terrorism*, *3*(3), 1-18. doi: 10.4018/ijcwt.2013070101

Rizov, V. (2018). Information Sharing for Cyber Threats. *Information & Security: An International Journal*, *39*(1), 43-50. doi: 10.11610/isij.3904

Talib, A., Alomary, F., Alwadi, H., & Albusayli, R. (2018). Ontology-Based Cyber Security Policy Implementation in Saudi Arabia. *Journal Of Information Security*, *09*(04), 315-333. doi: 10.4236/jis.2018.94021