**Discussion**

Student’s Name

Instructor’s Name

Course

Date

**Week Three**

Vulnerability assessment and risk assessment are two important aspects of cybersecurity. According to Bisht (2020), Vulnerability assessment mainly focuses on identifying vulnerabilities and areas of weakness used in the information systems, networks and overall infrastructure used in a given organization. A detailed outline of all the vulnerabilities is the main goal of a vulnerability assessment after which the threats are grouped and prioritized for fixing. On the other hand, risk assessment refers to a broader evaluation of the potential impacts of identified threats to the organization’s operations and assets. Its broader and delves into the impact of identified vulnerabilities to the organization as a whole. This includes financial effects as well.

The National Infrastructure Protection Plan abbreviated as NIPP refers to the critical components developed by the United States for the sole purpose of enhancing security of its most crucial systems. According to the Department of Homeland Security, (2018), it provides a five-part guideline on how critical infrastructure should be protected. These include how to handle risk management, the benefits of public – private collaborations, provides sector specific plans, how to handle incident response and finally provides guidelines on recovery and resilience.

**Week Four**

In today’s digital landscape, safety and security is of great concern. To achieve this, a robust information security system needs to be established. To achieve this the following key elements, have to be integrated. It should have access control mechanism. This is implemented through user authentication. According to Alsharif et al, (2017), user authentication and authorization is a crucial part of establishing a robust information security system. The other elements include, data encryption, vulnerability management, security monitoring as well as physical monitoring. The plan should also include employee training and incidence report structure where all information is reported to help with vulnerability analysis.

BYOD – Bring Your Own Device, has both positive and negative aspects in regards to its implementation on the mobile security plan of any organization. It enhances employee productivity as well as enhancing their job satisfaction (Liu et al., 2018). This is crucial in promoting a great work experience. On the other side, it exposes the organization to security risks as more devices translate to more avenues hence increased surface area for attack. Such an implementation will have to strike a balance between employee satisfaction and security of the computer infrastructure used in the organization.

**Week Five**

Maintaining an emergency response plan is beneficial to an organization as it helps to effectively respond and mitigate disasters on systems. It helps establish a rapid response as all the procedures are outlined and clearly stated (Smith et al., 2019). Other benefits include minimizing losses, allowing for effective resource allocation, establishes good communication channels and finally provides outline for both legal and regulatory compliance (Smith et al., 2019).

The following complications may arise from not maintaining an emergency response plan. The fist is disorganization and confusion, as there will not be a clear cause of action to take. Ineffective resource management, increased risk to security breaches, a negative public perception and the organization may face legal issues which can end up costing a lot of money.

Risk assessment plays a huge role in emergency planning, according to Kapucu and Khosa, (2019), it helps assess potential vulnerabilities and hazards specific to an organization. The information is crucial in establishing an effective emergency response plan. Risk assessment also helps with resource allocation. The other roles, it plays include; scenario planning and continuous improvement (Kapucu and Khosa, 2019).

**Week Six**

Coordinating agencies in crisis involves the use of internal teams to mitigate and prevent the crisis from becoming a disaster. It often deals with issues such as reputation management which aims to saving the image of the organization from negative public perception (Britt & Gallus, 2019). They also handle internal communication as well as response to critical incidents. Disaster on the other hand is more widespread and significant. The coordinating agencies for such include collaboration between multiple organizations and the government. They manage the impact of the disaster. Emergencies, on the other hand require more rapid response. The coordinating agencies include local and international emergency service providers. They ensure public safety and prevent further impact (Britt & Gallus, 2019).

To determine who is in charge in each occurrence, the following are considered. Jurisdiction, the person in charge is usually a government official who is in charge of the area. It might be a state, country, or county (Kapucu & Khosa, 2019). The nature of the event can also be used, some events need an international organization to take charge based on the complexities of its solution. The emergency response plan, also outlines the levels of authority during a disaster. Based on this, it can also be used to determine who is in charge. Finally, incidence command system may also be used as well as mutual aid agreements between the responsible agencies or parties (Kapucu & Khosa, 2019).

**Reference**

Alsharif, M. H., et al. (2017). The Importance of Information Security Policies: A Critical Literature Review. International Journal of Information Management, 37(5), 561-571.

Bisht, D. (2020). Vulnerability Assessment vs. Risk Assessment. International Journal of Computer Applications, 175(28), 13-15.

Britt, T. W., & Gallus, J. A. (2019). The Psychology of Crisis and Emergency Coordination. Oxford Research Encyclopedia of Psychology.

Department of Homeland Security. (2018). National Infrastructure Protection Plan. <https://www.dhs.gov/sites/default/files/publications/NIPP%202018-508.pdf>

Liu, C., et al. (2018). A Comprehensive Review of BYOD Security Risks and Defense Mechanisms. IEEE Access, 6, 7225-7237.

Kapucu, N., & Khosa, D. (2019). Disaster and emergency management: A policy analysis. Routledge.

Smith, K., et al. (2019). Effective disaster risk reduction strategies and pathways for building resilience to multiple hazards. International Journal of Disaster Risk Reduction, 38, 101225.