PRACTICAL APPLICATION ACTIVITY 1

BABALWA MPUNYUKA

babalwampunyuka@womentechsters.org

Cybersecurity problems are becoming a lot more alarming as organisations and businesses strive to have normal operations within their daily activities or tasks. Cybercrime surged up due to the COVID-19 pandemic. To enhance the security of the organization the chances of building a mightier defence system as the attackers are attracted by the vulnerabilities.

In order to fight off malicious attacks, it is of imperative importance to have an effective risk management plan for your organization in order to prioritize cybersecurity measures with regards to possible consequences of vulnerabilities in the process.

**STEP 1**: Identify the hazards (threats, vulnerabilities)

**System failure**- The organizations most critical systems running on high- quality equipment and available to all parties within the organization.

**Human Error**- Does the organization have a proper education around malware, phishing and social engineering? Anyone can accidentally click a malware link or enter their credentials into a phishing scam, exposing the organization data. The organization needs to implement a strong IT security controls including regular data backups and password managers.

**Misuse of information**- This is typically an insider threat where data is altered, deleted or used without approval.

**Data Leaks**- Personally identifiable information (CII) and other sensitive data by attackers via poor configuration of cloud services.

**Loss of data**- The organization might lose data or accidentally delete data as a result of backup or replication.

**Unauthorised access**: Access from attackers and employees.

**Lack of productivity**:

**STEP2:** Decide who might be harmed and how (assets, stakeholders)

**Stakeholders:** Stakeholders can be affected or harmed by the malicious attacks of anorganization.

**Connectivity:** Connectivity when working away from the office might be a struggle.

**STEP3:** Evaluate the Risks and decide on precautions

**Train and upskill employees:** The implementation of an organization’s cybersecurity plan will not come to life without having experienced staff. An employee without knowledge can become a liability to a company, instead of being an asset. The organization may need to train staff with risk management to encourage a security aware workspace.

**Assign responsibilities:** Every employee in the organization must be aware of the possible risks and know the suitable actions to prevent breaches. Duties and responsibilities should be given accordingly to other employees in order to guard the organization against human-related intrusions.

**Create a team**: Creating a cybersecurity teamto address emerging security threats ca be quite a challenge. Because it requires a committed full-time team, it is likely that highly experienced staff should be deployed.

**STEP4:** Record findings

**Health outcome:** Pain, self-reported health, stress levels, depression, fatigue, strain and happiness are reported as the affected health outcomes.

**Lack of organizational support:** To support employees, colleague support and social connectedness.

**The level of family conflict**