**Name: Akewusola Elizabeth**

**Womentechsters email:** [**akewusola.elizabeth@womentechsters.org**](mailto:akewusola.elizabeth@womentechsters.org)

**Practical Activity 1**

Risk assessment plan is a plan developed to manage a number of risks incase thing don’t go exactly asa planned. Avoiding risk is a goood idea however some risk are important to ensure the growth and survival of any company’s business. Firstly as an Information security officer in MBI Insurance company, I would liike to list out the risks, threat and vulnerabilities MBI insurance company can be faced with.

Rsk likely to be faced with are;

* Operational Risk: this risk is associated with failures in day to day operation that can impede the company’s revenue examples are; I] strategic risk: involves change in business direction, II] Reputation risk: involves perceived incompetence, dishonesty or company’s tarnished image III] Quality risk has to do with failure to meet the quality of the services , IV] structural risk: has to do with where the company be it home, office or commercial properties can suffer damage
* Financial risk: money loss as a result of external forces, this risk has the potential for damaging result in the future examples are I] Currency risk: when the value of foreign exchange affects the company’s transaction, II] Inflation risk: where investment in the business will not be worth as much in the future.
* Governmental risk: this is how political events and outcomes can affect companies to take certain risk like, I] Taxation risk: when new tax law favours company’ competitor than the company, II] Compliance risk: has to do with breaking laws, rules and regulations of the government, III] Country risk: doing business in a country experiencing negative effect associated with political event in its economy

The threat are;

* Social Engineering: with the increase in interaction cybercriminals are using the oppurtunity to launch social engineering attacks
* Patch management: If an insurance company is using outdated software, the company will be at a very high risk of cyberattack because most cyber criminals exploit the loops holes to gain access to the company’s information and this can be highly damaging
* Ransomware threat: here hackers attack your network and prevent you from accessing it until certain amount is paid
* ThIrd party exposure threat: hackers use malware to access personal data and most organizations don’t take necessary precautions. The use of third parties' services is a common practice these and it is necessary to take precaution
* Outdated hardware : with the inccreasing rate of software update some hardware may not be able to keep up with the changes and thise could lead to data vulnerabily to attacks

The vulnerabities are;

* Cloud vulnerability: as cloud access and storage is now a common practice, this has increased the risk of data breach
* Through employees: Social interaction, Customer interaction, Discussing work inpublic locations, Taking data out of the office (paper, mobile phones, laptops),
* Emailing documents and data, Mailing and faxing documents, Installing unauthorized software and apps, Removing or disabling security tools, Letting unauthorized persons into the office
* Opening spam emails, Connecting personal devices to company networks, Writing down passwords and sensitive data
* Losing security devices such as id cards, Lack of information security awareness,

Secondly the likelihood that these risks will occur in my insurance company

|  |  |
| --- | --- |
| Operational risk | It has some chance to occur |
| Financial risk | Has some chance of happening |
| Governmental risk | Very likely to occur |

Some of these risks has little or adverse effect on the company’s businness for example some risk like compliance risk taxation risk, reputation risk , structural risk can cause major disruptions in the company when they happen so necessary precaution should be taken to avoid their occurrence. When this high business risk happen both the assets and the stakeholder will have their share of the negative effect.

The precautions that is needed to be taken to avoid this threat, vulnerabities and

* Keeping the system software up to date
* Ensure end point protection to protect networks that are remotely bridged to device that is devices connected to corporate networks
* Control who has access to systems
* Wifi security
* Coperation with the government rules and regulations
* Making sure the services offered by the company shows high leel of competence for the company’s reputation sake.

Business continuity, recovery plan, rocovery strategy, auditting, logging, creating defensive firewallsare also good precautions to put in place