PracticalActivity **1-Obi Chioma**

**Obi.chioma@womentechsters.com**

**Blessing**

* **Step 1:** the MBI insurance company experience is the following threats and vulnerabilities.

1. **Social engineering:** With the increase of online and social media introductions, cybercriminals are exploiting such opportunities to launch social engineering attacks.; By using trickery and manipulative approaches to lure individuals into taking various actions.
2. **Cloud vulnerabilities:** cloud data access and storage has become a common practice for many BMI insurance company since they have embraced the work-from-home policy to covid-19. This practice can increase the risk of a data breach, they can be susceptible to denial-of-service(DOS) and account hijacking attacks.
3. **Third-party exposure:** They have increased the use of third-party services especially for payment processing. BMI insurance do not take the necessary precautions when engaging in third-party transactions. Even when the party you are transacting which does not handle personal data directly, it can put the organisation at risk of attack. Hackers are using malware to access personal data, such as credit card numbers and social security numbers through third-party companies.

* **step 2**

1. **Damage to brand reputation:** A security breach can impact more than just BMI's short-term revenue. the long-term reputation of her brand is at stake as well.
2. Loss **of intellectual property:** Loss of revenue and damaged reputation can be catastrophic. However in some cases, hackers will also target design strategies and blueprints. Losing intellectual property can impact the competitiveness of your business. Some rivals would not hesitate to take advantage of stolen information.
3. **Online vandalism:** Some hackers fancy themselves as pranksters. In this cases, a security breach might only lead a few words changes to BMI's website. while this seems relatively harmless, it can actually cause a lot of damage. Simple changes are harder to notice. for example, a hacker might change a few letters or numbers on the company's contact page.They may also add vulgar content to some of their web pages.

* **step 3**

BMI insurance company should protect their people and enhance their resilience while seeking potential responses to ongoing financial losses in their insurance policies. the current situation remains fluid, with scientific understanding of the covid-19 virus, medical response, and actions by governments and organisations evolving rapidly.

It’s important for policyholders to note that insurer's form their views on the coverage for a claim based on specific policy language and the specific facts and circumstances of loss.

* **Step 4**

From the examination, the BMI insurance company could be susceptible to data breach and therefore should create an awareness among employees to avoid emails that can cause harm to the organisation and also deploy adequate security in the cloud.