Kagai Sally Mukami

[Sally.mukami@womentechsters.org](mailto:Sally.mukami@womentechsters.org)

Practical Activity 1

MBI Company being an insurance company there is sensitive data relating to financial claims, stakeholder's data, investment plans, corporate data, patents among others that if leaked would prove fatal for the company. During my analysis I am going to assume the following:

* Staff are using personal gadgets to access office documents and other office services remotely.
* Each staff is using home fiber or public Wi-Fi at cafés due to maybe a power loss or a fiber cut at their premise.
* The is no secure network allocated like VPN to securely access office data.
* The has been no awareness training for the non-technical staff relating to cyber security.

Working away from the official office setup exposes the company's data to cybercrime because:

1. The home network unlike the office network is not a virtual private network (VPN), lacks firewalls and antivirus software.
2. At work there are security measures put in places to control the Bring Your Own Device practice however at home, an employee may use several tech devices that may not have strong passwords or an authentic antivirus software.
3. Spam and phishing emails targeting the weak employee that has malicious code like worms or trojan horse, bots that an attacker will use to penetrate the office infrastructure.
4. Covid-19 has brought out fears of job security due to tough economic times, in preparation for the worst, some employees are willing to sell corporate data to the highest bidder.
5. Ignoring physical security practices in public areas, example talking loudly on the phone about company sensitive data or exposing laptop screen that is displaying data to third parties.

Threats and vulnerabilities

* Data leakage
* Loss of data
* Misuse of information
* Unauthorized access to company’s resources.

Who will be harmed?

1. Employee personal data, this includes identification numbers or social numbers, passport numbers, pay slips and passwords.
2. Customer information the names of the customers, their occupations and the properties insured.
3. Corporate data- financial plans, and business plans for the company
4. Key infrastructure like the servers, databases and computers
5. Intellectual properties
6. Shareholders and stakeholder's information, that is personal data and bank details.

Precautions

1. Check that the security solutions including cloud solutions deployed are effective and updated.
2. Educate the employee on data security and remind them of company's code of conduct and data policy.
3. Encourage the staff to use strong passwords on all their devices.
4. Use home network services from internet providers that provide VPNs.
5. Implement multi-factor authentication to protect the infrastructure.
6. Use of trusted Wi-Fi instead of public Wi-Fi that is free and more susceptible to attacks.
7. Installation of antivirus software for protection against worms, virus, trojan horse or any other malware.