**SALLY OKETCH - PRACTICAL APPLICATION ACTIVITY.**

**RISK ASSESSMENT PLAN FOR MBI INSURANCE.**

**Purpose.**

The purpose of this assessment was to identify threats and vulnerabilities related to the MBI insurance company because of the working from home policy. The company has just recently embraced the work from home policy due to Covid-19 and some of the staff will work from home using their internet and devices.

Remote employees can be the biggest threat to MBI insurances security. Employees can end up giving hackers and cyber criminals access to the network and the companies sensitive data by unknowingly following some of the worst practices of cyber security.

Listed below are some of the risks and threats our employees may unknowingly experience:

**Phishing.**

Involves an entity or person behaving like a legitimate source over email to trick a victim into providing details like login credentials or sensitive information, which can be used to illegally access accounts, steal more sensitive information, carry out identity fraud, and much worse things breaching the confidentiality and integrity of the data. This might lea to data loss or theft that might bring about legal risks, reputational risks and financial risks.

These types of emails have become more advanced that it is difficult for employees to detect them now especially when phishing emails make it past email filters straight to the employees’ main inbox.

*So, what do we do now?*

Our employees are required to be trained on how to detect and avoid phishing emails so as to reduce the risk that phishing emails pose to the company’s data security. The company also needs to build a comprehensive cybersecurity awareness training program implement it from the first-time new hires arrive.

By educating employees about phishing from the first day and continuing education with newsletters, phishing tests, and periodic trainings, a workplace culture of strong cyber security will be instilled company-wide.

**Passwords**

Hackers know that human error is easier to exploit than trying to get into a very secure software, so the try crack account passwords to access sensitive information. Cyber criminals will use a lot of ways to crack passwords like compiling lists of commonly used passwords that can be used to easily access poorly protected accounts. Hackers will often write code to continuously attempt to crack passwords by trying out different variants and with time crack one’s password unless it is extremely complex. Repeat passwords are also insecure since once hackers crack one password to one account, they will try gaining access to other accounts with that password, therefore employees who repeat passwords are at a higher risk of having their company accounts hacked hence compromising the confidentiality and integrity of data. This might bring about operational risks like failed internal processes.

*So, what do we do now?*

Password policies can help foster a culture of personal responsibility in our organization. Passphrases and bans on using personal information and repeat passwords for account logins are recommended password policy clauses. Passphrases are strings of random group of words anywhere between 4 to 14 or more words including numbers, punctuations and special characters are most preferred since longer passwords are harder to crack. An example is S@l liked t0 h@ck. Employees are requested not to write passwords on sticky notes or note apps in their phones because someone with ill intentions might find it. The organization should consider adding a clause in their password policy that discourages writing own passwords.

**File sharing.**

This entails encryption of data when it is in transit from one location to another. Employees share so much sensitive information from client account information to files that we can not afford to secure this information from hackers. If this information is intercepted it can lead to identity fraud, ransomware attacks, theft among many others compromising the data’s integrity, availability and confidentiality. This might bring about legal risks like when sensitive data is exposed and a customer decides to sue the company.

*So, what to do?*

Sensitive data should be encrypted when it’s sent over email or phone. Email encryption platforms to secure email data. Outlook does a great job at encrypting emails. Voicemail information can be encrypted with the right business phone systems that have features that can encrypt and securely email voicemail data to ensure sensitive data is protected. Data can also be encrypted by using a secure file-sharing platform such as Dropbox and OneDrive.

**Personal devices.**

Employees are now forced to use their personal devices while working from home and most of them do not think to encrypt them so when work is conducted on them the data can potentially be accessed by hackers unless the device is encrypted. This may cause a breach of data confidentiality and integrity. This may bring about reputational risk when there is loss of trust if any of the customers data is leaked.

*So, what now?*

Employees are asked to refrain from using personal devices to conduct business unless they encrypt them.

**Home Wi-Fi.**

Most WI-FI networks that their employees use to work with at home may be posing a risk to the security of company data. For instance updates to home router software’s are often overlooked and many people do not have a firewall to guide their home’s network also while some routers are hybrid router-firewalls, these firewalls are not that secure which can lead to potential network security gaps for remote employees putting the integrity and confidentiality of data at risk. This might about reputational risks.

*So, what to do?*

Periodically updating your router’s software when updates are available ensures that any existing security gaps are quickly patched before a hacker can exploit them.

If the company can budget for it they can consider providing each employee, or at the very least those who work with a lot of sensitive data, with a firewall to better secure their home’s Wi-Fi