**Risk assessment plan**

Phishing Schemes

Your remote employees can be the biggest threat to your network’s security. By unknowingly following cyber security worst practices, employees can end up giving hackers and cyber criminals access to your network and your company’s sensitive data.

When business operations suddenly or temporarily transition to remote work, employees can become confused as to how to continue to work securely

**Prevention**

Training employees on how to detect and avoid phishing emails can greatly reduce the risk that phishing emails pose to company data security.

By educating employees about phishing and cyber security best practices

Unencrypted File Sharing

While companies may think to encrypt data that’s stored on their network, they may not consider encrypting data when it’s in transit from location to another.

Employees share so much sensitive information on a daily basis, from client account information to files and more, that your company cannot afford to not secure this information from being intercepted by a hacker

**Prevention**

Sensitive data should be encrypted when it’s sent over email or phone. When it comes to email encryption, Outlook, a popular email platform, has features that can convert plain text emails to scrambled cipher text so that only the recipient with the key can decrypt the message.

You can also use email encryption platforms to secure email data, attachments, and contact lists

**Insecure Home Wi-Fi**

While companies usually think to secure their remote employees’ work laptops, many do not consider how the Wi-Fi networks that their employees work off of at home may be posing a risk to the security of company data.

For instance, while many people know to update their smartphone or antivirus software, updates to home router software are often overlooked. Similar to when updates aren’t completed on other devices such as your smartphone, routers that aren’t updated won’t have security gaps patched, which can lead to data breach risks over time

Working from Personal Devices

**Prevention**

**APPLICATION ACTIVITY 1**

1. Imagine that you are the Information Security officer of MBI Insurance Company. The company has just embraced the work from home policy due to Covid-19 Where some of the staff members will be working from their homes, using their internet and devices.

Using the knowledge, you have learned and researched, develop a risk assessment plan for the organization stating any assumptions made.

Assess security risks, threats and vulnerabilities to the company and implement appropriate information security protection mechanisms by analyzing requirements following the CIA triad measures.

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

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

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

**STEP4:** Record finding

* + **Start collecting and researching information**
  + **Think creatively.**
  + **Develop the report in Microsoft Word format**
  + **Not more than 2pages**

Answer:

-assuming the company consisting of 10 employees