Risk Assessment Plan

For MBI Insurance Company

|  |  |  |  |
| --- | --- | --- | --- |
| Treads and Vulnerabilities | Asset | Evaluation and Precaution | Solutions |
| Data breaches | Organisation | 1. Check how much is the damage  2. Establish which data is breached  3. Notify appropriate personnel  4. Security audit  5. Enforce strong passwords | If an attacker can unlock our organisation credentials, this escalates their ability to move literally throughout enterprise.  That is why it is important to have strong user credentials, multiple method for authentication, password management and a strong cybersecurity program.  Identify governance solutions help organisations inventory, analyse and understand access privileges granted to employees , partners |
| Phishing schemes | Organisation and employees | 1. Education on phishing attacks.  2. Utilize Anti-spam software.  3. Verify http on address bar.  4. Install and maintain reliable firewall.  5. Never enter sensitive information on a pop-up windows. | Train employees on how to spot and handle phishing attack and other form of social engineering involving remote devices and remote access to company information system. Employees should be warned to be suspicious of emails from people they don’t know – especially if asked to click on a link or open a file, even from people they know. Ask them to double check by phone call when I doubt |
| Data Security and Productivity | Costumers and business | 1. Backup the data  2. Anti-malware protection is a must.  3. encrypt the data  4. Install operating system update.  5. automate the software update | Data security drives our organisation structure, business priorities and its ongoing process  When handle customer data we need to have this priorities at the forefront of the business.  Key considerations include  - Providing employees company monitored equipment  - Protected remote connections network access  - Management oversight and open communication to direct report to teams. |
| Unencrypted file sharing | Organisation and Customers | 1. Evaluate the best file sharing tools  2. Train the employees  3. use Cloud  3.Sort files  5. Define file naming format | When employees need to communicate sensitive information to fellow workers, up-to-date encryption tools should be installed on their devices. We can use mainstream massaging services that come with an end-to-end encryption as a default or as an option. |
| Internet connection | Employees | 1. Authority  2. Accuracy  3. objectivity  4. currency  5. coverage | Wi-Fi systems at home are somewhat secure. Employees should be aware of unsecure public Wi-Fi networks when working away from home, for those are the prime spots for malicious parties to spy on internet traffic and collect confidential information.  Change home router password so that it won’t be vulnerable. It important for employees to take simple steps to protect their home network in order to prevent malicious parties from having access to connected devices  Employees working remotely should use a VPN (virtual private networks). Using a VPN will bypass geographic restrictions on streaming site and other location-specific content. |

Compiled by: Fikile Goodness Mathobela

fikile.goodness@womentechsters.org