Protect your workplace: Cyber security measures to prevent a data breach

April 2019

Terrorism is not limited to physical attacks. Terrorists can make use of data security breaches to weaken organisations as well as critical infrastructure. Every organisation connected to the Internet should work on the assumption that they are likely to be a targeted victim of a cyber attack. Doing nothing is no longer an option.

The following recommendations can be considered to strengthen cyber security at your workplace:

1. Minimise vulnerabilities of your IT systems:

- Constantly monitor your IT assets and install necessary software to detect and prevent unauthorised access.
- Update your operating systems and applications as soon as patches become available.
- Perform periodic backups on a secure platform and advise employees to do the same for their data.
- Install an Application Control software with a multi-engine antivirus scanner to keep out malware and phishing attacks.

2. Build a strong cyber security culture at the workplace:

- Impose a password policy that prevents the creation of easily guessed passwords.
- Set systems to lock accounts after a few failed attempts.
- Employees should be made to change their passwords regularly.
- Create avenues for feedback and reporting of suspicious emails.
- Educate employees on the risks of discussing work-related topics on public domains, such as social media.

3. Know how to respond effectively in the event of a cyber attack

When a breach occurs, hackers can compromise your company's data by disabling the network and sabotage business operations. Critical data of stakeholders may be affected and the effectiveness of your company's response can have an impact on its reputation among clients in the industry.

How can you respond in the event of a cyber breach?

Step 1: Investigation and Assessment

- Identify how and where the breach occurred. Was it through phishing or data leakage caused by misplaced devices?
- Evaluate the damage caused to the business and clients.

Step 2: Recovery Measures

- Change the server and database administrator passwords.
- Restrict domain administrator access.
- Monitor database and system logs.
- Block connections to prevent further access.

Step 3: Crisis Communications

- Notify regulators of any breach involving the public or third party data. Be prompt and honest in your disclosure.
- Reassure the general public as well as internal and external stakeholders, and provide ongoing updates to keep them informed.
- Appoint a senior management to be the spokesperson to deliver messages, and to provide assurance to the audience.

Step 4: Post-Crisis Evaluation

- Identify lessons learnt.
- Overhaul systems and processes to ensure that the incident will not repeat.
- Look out for comprehensive cyber insurance plan that covers security or privacy breach.

Our community is now more aware of the terror threat and the role they play in the SGSecure movement.

Click **here** for the report on our Safety and Security Situation in 2018.

SGSecure@Workplaces Bulletin