PiperAlderman

Article Information

Author: Craig Subocz
Service: Cyber Security, Privacy & Data Protection
Sector: IT

Top Tips for Dealing with Data Breaches

The growing prevalence of and increasing public awareness about cyber incidents focuses attention on data breaches and how companies deal with them. Taking steps to prevent and deal with data breaches may reduce the adverse effect of a data breach and mitigate the potential lost reputation that a data breach can cause.

So, here are five tips to consider when looking to minimise data breach risks and their effects.

1. Imbue a culture of respect for privacy and cyber resilience

Protecting your company against the risks of data breach will improve if the company embeds a culture of respect for privacy and cyber resilience. This should start at board level, where compliance with directors' duties involves directors assuming oversight for cyber resilience. This could include the board approving the company's data breach response plans and cyber resilience strategies.

2. Prepare and implement data breach response plans and cyber resilience strategies

A data breach response plan should outline how the company will respond to and contain a data breach. Having a clear data breach response plan that explains how staff members should respond if a data breach is discovered will help the company in the crucial few hours after the breach.

3. Staff training

Human error remains a significant source of data breaches. Often, a data breach is caused when an email containing personal information is sent to the wrong recipient. Alternatively, an employee might lose a device that contains personal information. Training staff on minimising the risk of inadvertently emailing the wrong recipient will help, but the training should also cover what happens if a mistake is made, including the internal escalation path. Similarly, staff should be trained on dealing with devices issued by the company, including the report structure should the employee lose the device (or the device is stolen).

Staff are often targeted by malicious emails that purport to come from legitimate contacts and which ask for sensitive and/or confidential information or which exposes the company's IT environment to possible malicious software by having the staff member inadvertently downloading the software to attack the IT environment.

Training staff on how to recognise these phishing emails will assist the company protect the personal information it holds. New employees should be inducted on the procedures and processes deployed to protect the integrity of the company's IT environments.

4. Technology

While technological measures should never be treated as the 'be all and end all' of cyber resilience, having a strong and robust technological environment will certainly assist. For example, if an employee loses a device that contains personal information, the company should be able to remotely wipe the device. Enabling multi-factor authentication will minimise the risk of an unauthorised individual gaining access to the company's vital IT environments.

Where the company deals with sensitive information to which access should be restricted, steps should be taken to ensure

to limit access to only those employees with the requisite authorisation to access the sensitive information.

Ensuring that the company's IT environment is protected against vulnerabilities is essential to maximising cyber resilience. This includes ensuring that the IT environment is kept up-to-date with relevant vulnerability patches.

5. Critically review the cyber resilience of your suppliers and vendors

If your suppliers and vendors have access to your data, or are engaged to host or process your data, then don't be afraid to ask tough questions about their cyber resilience and then ensure that the supply contract imposes information security obligations on the supplier.

Companies face an increasingly sophisticated risk environment and cyber resilience requires an increasingly sophisticated and whole-of-company approach to managing that risk.