RISK INSIGHTS Technology

INSURANCE BROKERS Robison Challenging Convention

Data Security through Employee Education

Data security is of the utmost importance in the technology sector. A data breach can expose your company's and your clients' highly confidential information. The results can include violating the Data Protection Act (DPA), professional liability claims, the loss of your customers' trust and negative impact on your reputation and bottom line.

One of the first lines of defence in the fight against data loss is your staff. Implementing a strong data security training programme for employees can help your company retain high standards for data protection across the organisation. Well-trained and managed workers are more effective than technology tools alone.

Emphasise Continuous Caution

After undergoing education and training, employees should understand that data security is a continuous and constant concern for your organisation. Instead of a one-time session, data security education should be an ongoing part of the business process. Organisations can use posters, newsletters and other reminders to keep data security issues top of mind.

Be Aware of Potential Risks

Employees are very susceptible to phishing attacks, where a hacker poses as a legitimate organisation such as a client, bank or your own company. Some phishing attacks ask employees to supply confidential information such as passwords or client information to a source through an e-mail message or Web page. Others try to get employees to download attachments that launch malicious software, invading all parts of their computer and eventually working its way into the company's network. Spear-phishing attacks are targeted at a small group of people, making it easier for the message to be customised and extremely convincing.

Company leaders should be aware of potential risks in order to effectively inform and train employees of their existence and how to prevent them from occurring.

Initiate and Enforce Policies

Even the best-trained employee can make a mistake. Effective policies and procedures need to be in place to act as checks and balances for all data-related actions.

> Data security training for employees who handle sensitive and confidential information will help decrease your company's exposure.

This includes double-checking and recording activities, which will allow users or managers to see if something was done incorrectly before any damage happens.

Following these policies and procedures needs to be part of the continuous security education to ensure their effectiveness.

Worth the Investment

The cost of not taking the time to properly train employees on data security far outweighs the investment. Professional liability claims, a third-party security audit and DPA compliance fines are just some of the potential expenses that your company could expect if a data security incident happens.

Contact Robison & Co Ltd for more information about managing your data security risk.