The cost of cyber security for your small business

Earlier this year, Ticketmaster had the grim task of issuing a memo that no business wants to issue. It was addressed to its customers and it told them numerous things such as the following: reset your passwords; monitor your bank accounts and... sorry.

Josh Jennings

The suspected data breach was yet another in a long string of cyber incidents to malign businesses of all shapes and sizes this year. In July, the Office of the Australian Information Commissioner released its quarterly figures for the Notifiable Data Breaches scheme, finding 242 notifications were received for the most recent quarter.

A 2018 international study of anonymous invoice data from 321 randomly-chosen breaches between 2014 and 2015 also found 90% of organisations that experienced breaches were SMBs. The most

expensive breaches were identified in leisure, retail and hospitality, at an average of $18,000 per incident.

It's one thing for an SMB to acknowledge a cyber security strategy has the potential to protect against costly cyber attacks but specifically how should you invest in cyber security and ultimately what returns should you expect?

Assessing the effectiveness of cyber security

There's no shying away from the reality that adopting, implementing and operating a cybersecurity strategy takes time, money and expertise. It's therefore logical to establish explicitly how much of each you have. It's also often good practice for SMBs to engage the services of specialist advisors and consultants to review cyber security requirements.

Other steps you can take to evaluate the effectiveness of your cybersecurity strategy include technical testing of your networks, systems and operations, comparing your strategy with other organisations, closely monitoring your cybersecurity against industry standards and capturing trends in incidents and costs.

To extend your diligence, you could also consider the merits of undertaking return on investment calculations. Although this is challenging, demonstrating how your investment in security is impacting on your bottom line is a powerful way to consolidate your cyber security orientation.

SMBs awareness of cyber security costs

2017 report Cyber Aware highlights how cybercrime has shifted from an almost-unheard of event in the 1990s to a ubiquitous global

happening today. The survey indicates 40 percent of cybercrime incidents are costing Australian businesses between $1000 and $5000 and about two thirds of businesses are unable to recover these costs. It also finds that more than 40 per cent of SMBs nationally believe they can fortify their business against cyber crime by restricting their online activity – at the expense of the economic benefit of healthy online presence – and more than half continue to unwittingly take cyber security risks through common practices such as emailing and using social media.

Cyber insurance for peace of mind

CERT Australia, a part of the Australian Cyber Security Centre, highlights that some of the common cyber attacks you should be prepared for include ransomware, phishing and social engineering.

As you work towards implementing an informed and effective cybersecurity strategy, it's also a good idea to evaluate the merits of cyber insurance coverage.

You can inform your evaluation by asking yourself questions such as what a serious cyber incident would cost your organisation? Who the beneficiaries of access to your information might be? How cyber aware and hygienic your staff are and how prepared your company is to respond to a cyber security incident?

A specialist cyber insurance provider can offer SMBs assurance that, if they do incur costs from a cyber security incident (cyber crime is costing Australian businesses an estimated $1 billion annually), they'll have coverage. With average premiums for SMBs usually in the range of $2,000 – $3,000 annually, there is research to indicate that the majority of businesses who take out cyber insurance consider their premiums reasonable in light of their risk.

Companies such as Edmund Insurance can also offer your business access to a 24/7 emergency response unit (powered by KMPG), so you can get the immediate support you need in the instance you discover a cyber breach or threat of extortion.

Knowing the true cost of cyber crime is the key to effectively managing the risk.