The impact of cyber-attacks on small business

As the world becomes increasingly enabled through technology and continual connection, businesses — both large and small — must take precautions against being compromised through online platforms.

This is a critical business risk, and research from the Australian Small Business and Family Enterprise Ombudsman paints a grim picture. The recent report, *The Small Business Cyber Security Best Practice Guide* indicated small businesses represented 43 per cent of all cyber-attacks last year. In the spate of ransomware attacks that occurred in 2017, 22 percent of affected businesses could not continue operating.

Global fund manager Schroders in its recent market report found that cyber-crime costs global companies around 60 per cent more than it did only five years ago, while in the US, that number has risen by over 80 per cent.

In this piece we're going to look at some of the main points of entry for criminals using online platforms and services.

Email phishing attacks are hoax emails, designed and worded to appear from a trustworthy source, such as a bank or other financial institution. They aim to entice you to click on a malicious link that can lead to a viral infection of your systems, or ask you to input data — such as your login credentials for your bank — which is then taken and used illegally. Australian banks regularly send out updates via email or posted on their website warning of any fraudulent emails that may be in circulating at any given time. According to a recent report in the *Australian Financial Review*, compromise via email cost Australian businesses more than $22 million in 2017. It also said that more than 80 per cent of data breaches came through weak passwords.

Malware is a piece of software sent to you that, if opened or run, infects your machine or network with software. This can then be used to skim info from keyboards as keys are pressed, or provide external access to an unauthorised user in a remote location.

Ransomware is delivered as above, but then locks your system or network down until a ransom is paid to restore access.

A **denial of service** attack bombards your network with requests and locks up your system from functioning normally. This is often used by groups such as the hacker group Anonymous to shut down targeted websites.

According to the Australian Small Business and Family Enterprise Ombudsman data, fewer than one in three business with less than 100 employees take active preventative measures against cyber security breaches, and 87 percent of small businesses believe antivirus software alone is enough to protect them from the above. This is often not the case.

What precautions can you take ?

The first thing to examine is the potential entry points for attacks into your system and this can include point of sale systems, mobile devices used by staff, or allowing people to dial into your systems using a virtual private network (VPN). Once you are aware of where your business may be exposed, you can take appropriate action to protect systems.

The goal for most cyber-attacks is the collection of data, so make sure you have offsite copies of all your critical records. Running data backups daily, or throughout the day, will allow you to restore your system should it become compromised.

If your employees are using mobile devices provided by the company, you can set up network restrictions that don't allow them to access services like online banking, or your network. This will prevent accidental loss of a device potentially opening a route to your information.

Provide employee training to increase awareness on the types of cyber attacks and the need to implement strong system password controls. Consider implementing two-step security on your devices or network, meaning that both a password and a code, sent via email or SMS, will be required to access the network.

Impacts beyond data loss

There is an incorrect assumption that a cyber-attacks will cause potential damage to systems, and only technology will be affected, but the impacts can be far greater.

There are insurance policies that cover some aspects of a cyber-attack, but once an attack occurs and the damage is analysed, there will almost certainly be areas that are not covered. A potential attack could compromise your data, your premises, your clients' data, your ability to operate, or your reputation within your business network, or with the regulator. Depending on the collateral damage, some will be covered, while some will almost certainly not be. It is important to speak to a broker in detail about the risks that your business faces, so that appropriate cover can be discussed. For further information, please contact us.