Cybersecurity
Beware the breach

A Google search for ‘cybersecurity’ delivers 234,000,000 results (and growing daily). A lot of the information can seem very doom and gloom; businesses get hacked, monies and reputation are lost, security breaches cause trading chaos, and it appears to happen daily.

STORY
Greg Taylor
Business Computing Services
Baker Tilly Staples Rodway Taranaki

In our Business Computing Services team, we see the consequences of cyber crime first-hand. Often we are the ambulance at the bottom of the cliff.

Unfortunately putting your head in the sand and ignoring potential threats to your business doesn't make the problems go away. Quite simply, if you don't invest in your IT systems, including a fraud and detection strategy, then it's probably only a matter of time before you are affected.

There are a few easy steps you can take that will start you on the path to a more secure IT infrastructure, and some of them are very simple and a great starting point to being more proactive about protecting your business assets.

Protect USB drives

Most people use USB drives, but few protect the information on them. Would you be fine with someone finding one of yours and accessing sensitive information? An easy way to encrypt the data and add a password to your USB drive is to use BitLocker, a free product available to anyone using Windows 10. It takes a couple of minutes to set up, but it will mean that any info you have saved on it is considerably safer. Should you lose the USB drive, it would be useless to anyone that finds it.

Think before you click

One of the biggest causes of security breaches is not your system being directly hacked, but from the people in your organisation making mistakes. Opening emails or attachments from unknown senders are just some of the way people can allow cybercriminals access to your most important data. There are phishing simulation tools that you can run, which will test your team's ability to identify fraudulent emails. You can see who opens risky emails, opens attachments within the email or click on any links. Once the test is completed, people are given information about what to look out for when opening emails. You can then re-run the test a few weeks or months later and hopefully see an improvement.

A password is not enough

Implementing multi-factor authentication (MFA) is moving from a 'nice to have' to a mandatory for most businesses, regardless of size. This means that employees must use at a minimum 2-step verification when logging in to applications used in the organisation. These include Office 365, banking and accounting services, as well as social media accounts. These only add a few seconds when logging into the applications but could save you thousands of dollars, hundreds of hours and most importantly, your business reputation. Government website CERTNZ (Cyber Security NZ) recommends businesses consider using systems that support MFA. Once you have introduced it to the business, make sure your people know that it is a mandatory requirement, not optional.

Find the weak links

A Cyber Security and Fraud protection audit is a good way to have an open and honest look across your IT and business network and systems to identify any weaknesses. These audits can identify unused user credentials, weak passwords and user work habits, as well as many other indicators. It may be required of your industry or board compliance to have a regular independent audit, or you may want to know that you or your IT support provider is applying best-practice standards across the network.

greg.taylor@bakertillysr.nz