Safeguard your business from fraud and theft

02 July 2019
by David Goodall

Fraudulent business activities are on the rise

The New Zealand Crime and Victims Survey (May 2019) highlighted almost 400,000 people have experienced one or more incidents of fraud or cybercrime over the last 12 months. It's becoming common place to find at least one fraudulent email a week in your inbox and a quick search on the internet reveals a startling amount of corporate fraud cases in Taranaki alone. To understand more about how this can affect your business, let's first look at the five most common types of corporate fraud.

Data breaches - Cybercriminals are skilled hackers who know how to find weak links within your payment processing system. This is often the most harmful to a business because it puts their customers at risk, which not only has a financial implication but can also lead to a lack of trust.

Identity Fraud - When fraudsters obtain sensitive business information to enable them to set up false accounts in your company's name.

Occupational Fraud - Many small and large businesses have lost hundreds of thousands of dollars, most commonly through the illegal actions of trusted employees, often in an administrative role. They take advantage of their position by altering timesheets or paying a fake monthly service fee into their own account.

Phishing - An email or text that tries to trick you into providing your personal details.

Computer Virus Scams - This usually appears as a pop up on your screen but it is also common to receive a phone call saying your computer has been infected with a virus, which the caller can fix, as long as you give them your credit card details and remote access to your computer.

Awareness of corporate fraud is increasing, and the government continues to invest heavily in strategies to help prevent attacks on the internet. However, the risk remains very real and businesses must be implementing their own strategies to stay safe both online and offline.

How to protect your business from cyber crime

To safeguard your business from fraudulent activity or theft you must have a fraud prevention and detection strategy. This includes reviewing your current system for weaknesses and creating a backup procedure and disaster recovery plan.

Having an IT security review provides your customers with confidence in your business and peace of mind that their information is being kept safe. It also assists management within your business with identifying and prioritising areas which require focus. Having high level IT security protocols in place, for example password control, two factor authentication and back-ups will reduce the likelihood of an attack.

The Audit and Business Computing Services (BCS) teams at Baker Tilly Staples Rodway can provide your business with an 'Internal Systems Review'. Following an initial scoping meeting, our Audit and BCS teams can conduct a review of your IT security procedures and controls in place within your organisation.

Upon completion you will receive a detailed report summarising issues identified, associated risks and corresponding recommendations.

Businesses, no matter their size, should be doing more to secure themselves, not only for their continued success but for the safety of their customers and employees. Being aware of your business' weaknesses will enable you to be proactive rather than reactive in the fight against fraud.

Contact david.goodall@bakertillysr.nz to start the conversation.