TECHNOLOGY Snapshot

gardiner. knobloch.
ACCOUNTANCY + ADVICE

August 2016

IT Risk

Ransomware

We've become aware of an increase in the instances of ransomware in New Zealand and around the world.

What is Ransomware?

It is malicious software that literally holds your computer to ransom by preventing you from accessing some or all of the information on your computer unless you pay a ransom by a certain time.

How does Ransomware get onto my computer or server?

The main ways you can get Ransomware are emails containing attachments or malicious links. The emails can appear to be genuine emails from large corporates e.g. NZ Post, NZ Police, FedEx, Inland Revenue, etc.

How do I know I have it?

It may not appear immediately, but at some point you will get a window on your PC containing instructions and a countdown timer. It's important to understand that this is a genuine threat to you and your business data (even your personal data on your home computers and devices).

Prevention

Our IT consultants, Spark Digital Hawkes Bay, have let us know what you can do to protect yourself from Ransomware.

- **Educate your Team** to know about what to look for with emails. Do not open attachments or click on links in emails that appear suspicious or from unknown senders, including any from Fedex, UPS or other well-known organisations. Rule of thumb is if you are unsure don't open or click.
- Make sure you have **anti-spam software** installed on your computers, servers and mobile devices. They recommend cloud based versions like SMX which may stop the threat before it gets inside your mail systems.
- Think about using **Office 365** if you are a small business as it has anti-spam and anti-virus protection with its email service.
- **Backup everything** and regularly test these backups to ensure they are successful.
- **Update, update, update.** Ensure your computers, servers, anti-virus software is all up to date with the latest versions. Consider having a service agreement with your IT support to ensure this is happening.
- **Get it checked.** Get your IT Support, or ours, to do a Health Assessment of your computer systems and recommend any actions required.

Backups

If Ransomware gets through:

We've been told to be prepared to wipe our system and restore from our latest backup. So with that in mind here are some things to think about:

- Do you have a routine backup of your computer servers, computers and devices?
- Are your backups to the cloud or to a device that is removed from site regularly and stored securely.
- How often do you backup?
- Does your backup capture data on all computers?
- What about your home computer of devices, are they backed up?

CHARTERED ACCOUNTANTS
AUSTRALIA • NEW ZEALAND

August 2016

Ransomware in New Zealand

We know of a few recent cases of Ransomware in the Hawkes Bay region. This is a real threat for you and your business.

Spark Digital have reported that in the last year cyber-crime cost our economy $257 million and affected more than 856,000 New Zealanders.

With 60% of all targetted cyberattacks hitting small-to-medium businesses it means we all need to take note.

In New Zealand

Insurance

You can take out insurance cover to protect your business against the costs of ransomware and other cyber-crimes. This is generally an additional insurance to your standard business insurance so you will have to talk to your insurance company about it.

The policy should cover things like business interruption, reimbursement of costs related to the crime (data restoration, forensic costs, public relation costs, legal expenses, etc) and third party costs related to failure to keep data secure (including compensation, investigations, fines, penalties, etc).

‘A good plan today is better than a perfect plan tomorrow’ - old proverb

Actions

What do I do if I’m attacked?

If the Ransomware screen appears telling you to make payment you need to limit the impact, particularly if you are on a network.

- Disconnect your computer from the internet immediately (remove the network cable or turn off your wireless connections).
- Disconnect any USB storage devices.
- **Contact your IT support immediately** and have them attempt to remove the Ransomware or restore your system from backup. If you are unable to get your data back through these ways you may have to pay the ransom.

Disclaimer: This publication has been carefully prepared, but it has been written in general terms only. The publication should note be relied upon to provide specific information without obtaining appropriate advice after detailed examination of your particular situation.