"Ransomware" - cyber security and practical tips

WannaCry is the computer malware "worm" that has been infecting computer business systems around the world in the last few days. It reportedly attacks a vulnerability in Microsoft Windows operating systems and locks users out of their own computer systems, demanding a ransom of about $300. Hence the name -"ransomware."

But the $300 ransom is the least of the troubles caused by the attack. The scope for business interruption is huge - with businesses unable to access their data, unable to order stock or send packages, unable to provide services and having to turn customers away.

High profile victims thus far include Britain's National Health Service, French car manufacturer, Renault, and Spanish telecommunications company, Telefónica.

New Zealand businesses have not featured widely in media accounts. But computer experts are expecting a second wave.

The purpose of this update is to alert clients to these events and to suggest steps to protect their businesses in relation to this and future ransomware events.

Drawing on suggestions from computer commentators, you may want to consider actioning the following practical steps:

- If you use Microsoft Windows, check for, install and enable their latest security updates/patches.
- Check on other software that is integral to your business - have you been ignoring "pop-ups" and the like, advising you to install the latest update?
- Alert your staff to what has been happening with the "WannaCry" ransomware - not all staff keep up with current affairs.
- Instruct staff to be extra careful with opening emails as these are often the conduit for ransomware. Staff should be told not to open emails (and in particular any links or attachments) from unknown senders. Stress to staff that if they do open emails, attachments or links accidently, they must tell someone immediately - IT or management.
- Regularly back up your business data to a secondary source.
- If you are using pirated software, invest in non-pirated software - that way you will get the benefit of security updates.
- Consider whether you have any other vulnerabilities in your computer systems. Not addressing them could compromise your position, including potentially with any insurance you have in place for cyber attacks.
- Think wider - do you need to get your house in order by consulting an external cyber security expert? Can you afford not to, given the disruption to your business if you didn't have access to your systems? Taking these steps may also have a positive effect on your insurance premiums for cyber attack cover.

- If you don't already have one, consider taking out a cyber insurance policy. Many small to medium sized businesses who to date have considered cyber insurance a "want, not a need" are precisely those who may have older systems which are more vulnerable to ransomware. Consider carefully what business interruption cover is on offer under the various cyber attack policies offered by the insurance market.
- Consider amending contractual supply terms so that "force majeure" events expressly include cyber attack.

If your business has already been infected with ransomware and you have cyber insurance, notify your broker and insurer immediately. Talk with your broker and insurer *before* paying any demand for a ransom. If you don't have cyber insurance, consider consulting with a computer expert immediately. Also consider the likely effect on your customers if their data has been compromised.

In New Zealand, there is currently no law requiring that businesses notify customers of security breaches. In addition, with WannaCry, it would seem that the hackers are not particularly interested in exposing or exploiting the data themselves - they simply withhold access to it, in return for the ransom. However, it is conceivable that this or other ransomware in future may put customers' safety, reputation or finances at risk. You may be liable to them for having failed to take steps to safeguard their information or data. It may therefore be wise to inform affected individuals so that they can take steps to protect themselves. This could reduce the amount of any later legal claim against you. Again, if there is a cyber insurance policy in place, any steps (including notifying affected customers) should be taken in consultation with your insurer, including so as not to jeopardise policy coverage.

For further information please contact:

Jonathan Scragg
Partner, Wellington

d +64 4 471 9422
m +64 21 878 972
jonathan.scragg@duncancotterill.com

Julie Maslin-Caradus
Associate, Nelson

d +64 3 539 5406
m +64 21 905 595
julie.maslin-caradus@duncancotterill.com