INVEST
+ PROTECT

AON

The Rapid Rise of Ransomware

In early May, the world was hit by a ransomware cyber-attack known as 'WannaCry' which locked users' files, not releasing them until a ransom had been paid in Bitcoin (digital currency). This new variant of ransomware was attached to a self-proliferating 'worm' that looks for unpatched systems and then infects them. Ransomware traditionally required a human trigger however WannaCry spread very rapidly through organisations and the internet without human assistance.

This virus exploited out of date Microsoft Windows software regardless of size, industry and country.

Who was affected?
The attack hit an estimated 300,000 victims in 150 countries. Some of the most high profile impacts have been on hospitals in the UK, including the National Health Service (NHS) and international shipper Fed-Ex. The NHS spread of the ransomware was early and severe due to unsupported Windows XP across the organisation.

Further threats
Even if businesses had not been affected, there was a further threat from phone scammers pretending to be from Microsoft and using the WannaCry concerns as a means to gain access to computers.

In addition, another large-scale cyber-attack followed called 'Adylkuzz' which targeted the same vulnerabilities as WannaCry. Instead of locking up users' files, this virus used the hundreds of thousands of computers believed to have been infected to transfer virtual currency to the authors of the virus.

How can I increase my organisation's cyber resilience?
Organisations can proactively manage their cyber risk exposures and reduce the impact of future incidents by doing the following:

- Identify and quantify your cyber risk exposures;
- Formulate a plan to reduce and manage these exposures;
- Create a cyber incident response plan;
- Enhance cyber security awareness training in your organisation; and
- Consider the integration of cyber insurance into your risk mitigation program.

How do cyber incident response plans assist?
Building an incident response plan in advance of a cyber incident is directly correlated with a lower total cost of risk:

- Identification of an internal response team including forensics, crisis management, legal, internal and external crisis management/external communications, and insurance professionals. (This pre-identified and engaged response team allows the team members to benefit from knowing the organisation and issues in advance of the incident facilitating quicker, more accurate, more coordinated and more comprehensive responses);
- Preparation of adequate and tested back-up systems; and
- Identification of critical decision points facing affected organisations and ensuring that the stakeholders in these decisions are aware of their role and that there are backup contacts in the case of unavailability.

How can cyber insurance assist with ransomware incidents?
A cyber insurance policy tailored to your organisation's needs can protect against the financial damage caused by a ransomware attack, while also connecting you with a network of cybersecurity, legal and crisis communications experts in the event of a serious system breach.

Investigation expenses, legal expenses and costs to end the ransom attack can all be covered under a robust cyber insurance policy. There is further cover available, where a system compromise leads to a data breach or a system disruption.

What should you do in the event of similar attacks?

- Follow the actions set out in your cyber incident response plan or equivalent crisis plan;
- Patch your systems in order to prevent further attacks;
- Report the event to relevant authorities. Aon recommends that affected organisations contact the Computer Emergency Response Team (cert.govt.nz).

How Aon can help
Aon are leaders in cyber risk consulting and insurance solutions. We offer a range of cyber risk management solutions, including risk profiling, that helps you understand and manage the cyber risks unique to your organisation.

We also arrange cyber insurance, as described above.

Aon.co.nz/cyberrisk

Visit: aon.com.au/canz

No use crying over spilt data . . .

Do you or your firm understand the financial implications and brand damage following a cyber event?

Businesses are entrusted with vast amounts of client and employee sensitive data which is the target of criminals.

Managing the risks of external attacks including hackers and malware or internal risks such as human error and malicious employees is a relentless task.

No matter if your business is large or small or if you manage your own dada and systems or it's outsourced, your business is vulnerable to a cyber attack.

Speak with one of our specialists to learn more about cyber risk and find out how you can reduce the exposure within your business.

0800 266 276
charteredaccountantsanz.com/aonnz

aon.co.nz/cyberrisk

AON
Empower Results®

Aon is the approved insurance broker for the Chartered Accountants Australia and New Zealand Affinity Members Programme.

Affinity MEMBERS PROGRAMME