CLIENT ALERT

WANNACRY RANSOMWARE CYBER-ATTACK

What you need to know

There has been an overwhelming amount of information circulating in the media at the moment about the recent ransomware attack. Here's what you need to know and what to do if you are affected.

What is "WannaCry?"

On Friday 12th May, the world was hit by a ransomware cyber-attack. The attack, known as "WannaCry" or "WannaCrypt", locks up user's files, and does not release them until a ransom had been paid. The ransom must be paid in Bitcoin, which is a digital currency.

How did this attack originate?

Interestingly, this is a new variant of ransomware that has been attached to a self-proliferating "worm" that looks for unpatched systems and then infects them. Ransomware has traditionally required a human trigger, an individual clicking a link or attachment, which then launches the ransomware. In other words, WannaCry can spread very rapidly across organisations and the Internet without human assistance.

Who is vulnerable to the attack?

All organisations with out-of-date Microsoft Windows software are at risk, regardless of size, industry and country. Microsoft became aware of a vulnerability in their software earlier this year, and released an update to fix the problem in March. They also released a patch for unsupported systems, including Windows XP.

Who has been affected so far?

The attack has hit an estimated 300,000 victims in 150 countries so far. 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. UK hospitals were asking non-critical patients to avoid hospitals until they could access their systems again. The NHS spread of the ransomware was early and severe due to a proliferation of unsupported Windows XP across the organisation.

What's the impact in Australia?

It is estimated that more than 12 Australian businesses have been affected with more anticipated due to the prevalence of organisations with out-of-date software. In addition, another large-scale cyber-attack is underway, that could potentially cause even more damage than WannaCry.

The new attack, called "Adylkuzz" targets the same vulnerabilities as the WannaCry ransomware, but instead of locking up users' files, the virus uses the hundreds of thousands of computers believed to have been infected, to transfer virtual currency to the authors of the virus. There are no reported cases of the attack in Australia just yet, however organisations should remain on high alert.

What should you do if you have been targeted?

- Follow the actions set out in your cyber incident response plan or equivalent crisis plan;
- Patch your Microsoft Windows in order to prevent further attacks;
- Report the event to relevant authorities. We recommend that affected individuals contact the Australian Cybercrime Online Reporting Network (acorn.gov.au), organisations contact the Computer Emergency Response Team (cert.gov.au) and government entities contact Australian Cyber Security Centre (acsc.gov.au)

How can I increase my organisation's cyber resilience?

Organisations need to proactively manage their cyber risk exposures and reduce the impact of future incidents by doing the following:

- Identifying and quantifying their cyber risk exposures
- Formulating a plan to reduce and manage these exposures
- Creating a cyber incident response plan
- Enhance cyber security awareness training in your organisation
- Considering the integration of cyber insurance into your risk mitigation program

How do cyber incident response plans assist organisations?

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: industry leading attorneys, forensics, crisis management, law authority, 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 organization and issues in advance of the incident to facilitate quicker, more accurate, more coordinated and more comprehensive responses
- Adequate and tested back-up systems
- Identification of critical decision points facing affected organizations, 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 that a ransomware attack of this nature, 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 extortion payments 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. Cyber ransom, in this case to address a ransom demand of $300 (to be paid in Bitcoin) for malware called "WannaCry," can also be included in many cyber insurance policies.

Despite the urge to move swiftly in response to this crisis, we recommend policyholders understand and comply with the cooperation clause and notice provisions of their policies to insure they preserve their right to insurance coverage.

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 the cyber risks unique to your organisation.

We also offer cyber insurance, which can cover ransomware incidents. Cyber insurance can include a cyber incident response team who can assist with the first response to a cyber incident and coordinate the actions required. Please contact us if we can assist in preparing for, responding, mitigating and transferring risks of cyber incidents.

aon.com.au/cyber

Contacts:

Fergus Brooks
Cyber Risk Practice Leader
T +61 2 9253 7835
E fergus.brooks@aon.com

Michael Parrant
Cyber Insurance Leader
T +61 3 8613 3485
E michael.parrant@aon.com

Stephen Trickey
Specialties Sales Director
T +61 2 9253 7577
E Stephen.trickey@aon.com

Empower Results®