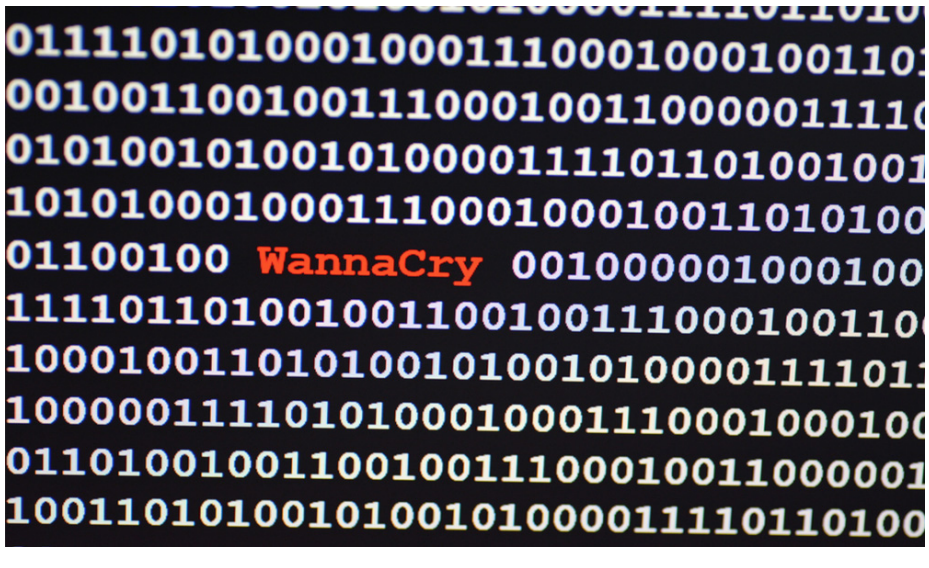
THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES



RISK & INNOVATION

4 Lessons And 7 Questions From The WannaCry Ransomware Attack

OVERVIEW

All around the world, hundreds of thousands of computer users have been confronted with a big red screen demanding in big red letters a payment of up to $600 in bitcoins to unlock it.

They had fallen victim to the ransomware virus WannaCry, which locked up more than 200,000 computers in more than 150 countries on May 12, 2017.

While the initial WannaCry virus was partially stopped in its tracks after a couple of days, the full extent of the damage remains unclear. Plus there are fears that a second wave of ransomware viruses could soon be on its way.

"WannaCry's worm-like behavior and its ability to easily propagate across the organization make this a particularly dangerous strain of ransomware," says Ed Stroz, Co-President at Stroz Friedberg, an Aon Company.

"The malware spreads from the infected computer by scanning other computers and systems on the network, and over the internet, infecting these connected machines by exploiting the same vulnerability, all without any user action.

"Essentially, it only takes one infected user on a network to put the whole organization at risk."

Another factor behind WannaCry's speed and relative success is the intricate and Byzantine nature of modern computer networks.

"One of the challenges of cyber is that it is a very complex environment," says Jim Trainor, Senior Vice President, Aon Risk Solutions and former Assistant Director of the FBI's Cyber Division in Washington, DC.

"Bad actors use and exploit infrastructure both in and out of the United States. A lot of groups who conduct such criminal activity don't reside in the U.S. This makes it increasingly challenging for both government and companies to protect themselves because those attacking them don't actually reside in the locations in which they operate."

With cyber risk on the rise, and business interruption a growing concern, what key lessons can organizations learn from the WannaCry incident?

IN DEPTH

Lesson 1: The Real Threat Of Ransomware Isn't The Ransom

While businesses might have been tempted to pay the $300 to free up their machines, not only might this encourage further attacks, it could also risk voiding their insurance policies. And in any case, financial risks spread much further than the ransom itself.

"Too much focus is being put on the dollar amount of the ransom," says Kevin Kalinich, Global Practice Leader, Network Risk/Cyber Insurance, Aon. "It's more about the larger financial statement business interruption impact and the forensic costs of cleaning it up. Cyber extortion coverage does not necessarily mean business interruption and extra expense coverage – they are separate coverage grants."

West Coast cyber risk modeling firm Cyence estimated the average individual ransom cost from Friday's attacks at $300, but the total economic costs from interruption to business at $4 billion. The U.S. Cyber Consequences Unit, a non-profit research institute that advises governments and businesses on the costs of cyberattacks, estimated more modest total losses of up to $1 billion.

"If you're a hospital that turned away patients, or if you're a global delivery company that can't send a package, or a telecom company in Spain, Russia or China, the financial statement impact from the business interruption is much larger than the $300 ransom," Kalinich told Reuters.

With much more at stake than paying a few hundred dollars, organizations need to take ransomware much more seriously. And with ransomware attacks becoming more common – up 300 percent in 2016 to an average of 4,000 attacks a day in the U.S. alone, according to the U.S. Justice Department – the threat is rising.

Lesson 2: Understand Insurance Policy Coverages

A typical cyber insurance policy will protect companies against extortion including ransomware attacks. But, rather worryingly, most organizations outside the U.S. still don't have cyber cover.

Nearly nine out of 10 cyber insurance policies in the world are in the U.S. – in part due to greater aptitude for litigation in the United States and breach notification laws putting obligations on organizations. The upcoming European Union General Data Protection Regulation (GDPR), due to be implemented in May 2018, is likely to increase cyber insurance penetration in Europe – but EU firms still lag behind.

Insurance can also address other costs incurred following a cyberattack, including the cost of notifying those whose data has been breached, hiring a PR agency to address reputational damage and arranging credit monitoring for those affected, as well as potential legal action. "Business interruption, forensics costs, lost productivity and potential third-party liability can also all be covered by cyber insurance policies," says Kalinich.

For now, however, most non-U.S. firms lack protection – which can be a powerful way to minimize the impact and cost of a breach, as well as a source of support and expertise as insurers work with their clients to assess and mitigate cyber risk.

Lesson 3: Think Holistically About Cyber Insurance Coverage

However, insurance is not a catch-all solution, and it is important for policyholders to understand the limitations of their insurance programs. Many policies have a deductible greater than $300, so the WannaCry ransom payment itself would not be covered.

And even if there are appropriate coverage grants, it's important policyholders understand how they work.

"If the cyber ransom payment is covered by the cyber policy, then the insurer must be notified prior to the cyber ransom payment or the ransom would likely be excluded from coverage. Some cyber policies also require the insured to contact law enforcement to obtain approval to pay the cyber ransom," says Kalinich.

"Even if the ransomware payment is below your deductible, if the "Notice" or "Cooperation" clause requires you to work with the insurance company, then your coverage is void if you trigger the clause by paying."

Many insurers also have "failure to patch" exclusions, such as Chubb. This means that if a gap in a system's cyber-defenses has been identified and a "patch" piece of software issued to cover that vulnerability and an organization *hasn't* installed it, any and all coverage for any and all damages would be excluded.

The vulnerability that let in the WannaCry attack was identified and a Microsoft patch deployed in March 2017. Organizations that failed to update their systems with that patch could find their insurance policies void in this case. Furthermore, organizations that are using pirated software, which is more common in Russia and Asia, will also likely have their insurance claim denied.

Understanding the extent of your coverage means thinking about insurance holistically, rather than as an item-by-item solution. "Analyze your insurance in aggregate rather in a silo," Kalinich recommends. "Looking at all of your vulnerabilities and risk transfer options together is the best way to ensure that you're covered."

Lesson 4: Prepare For Best-In-Class Breach Responses

In addition to financial implications and insurance considerations, the WannaCry attacks forced organizations to make a number of critical decisions. These included: whether to pay the ransom, how to assess comprehensively and remediate any damage done, which other parties to include in this process, and what actions may need to be taken to comply with applicable local laws.

However, it's important to remember that actions companies take in response to such ransomware attacks may have lasting– financial, legal and reputational — consequences.

Despite the urge to move swiftly in response to crises like WannaCry, it is advisable for policyholders to understand and comply with their insurer's cooperation clause (which mandates the policyholder to work with the insurance provider) and notice provisions (which outline how communications between the insurer and the policyholder will proceed in the event of a loss) of their policies to insure they preserve their right to insurance coverage.

"Even if the cyber ransom payment is below threshold to be covered by insurance, the cooperation clause requires the insured to engage the insurer in decisions that could impact insurance coverage," Kalinich warns.

In addition to knowing how to proceed with insurers, it's important for organizations to build processes that help them deal with incidents in real time.

Having an in-house incident response plan in advance of a cyber-incident is directly correlated with a lower total cost of risk.

Adequate back-up systems allow organizations to continue functioning despite the malware.

"As it relates to protecting your business, you can always get better and reduce your risk profile," Trainor explains. "While you're never fully eliminating your risk, instead you're trying to become more of a challenging target for malicious actors."

Regularly performing top-level security exercises like red-teaming – where an independent team is set up to challenge how an organization is run – can also help improve executive decision-making, communication, and broader corporate awareness and accountability without exposure to a real breach.

Building this kind of resilience into organizations is essential as attacks like WannaCry become more widespread.

7 Questions To Ask In Light Of WannaCry

Experts at Aon's cyber risk consultancy, Stroz Friedberg, have outlined a number of questions that organizations should ask themselves so that they can assess their vulnerabilities and prepare for cyberattacks:

- When was the last time you reviewed your company's patch management program? What about your disaster recovery and business continuity plans?
- Can you identify where all of your mission critical data resides and whether regular backups are being made?
- Does your cyber insurance policy provide adequate coverage? Have you taken the necessary steps to ensure you will be eligible to make a claim if your company is impacted?
- Have you communicated with employees about the latest phishing and social engineering techniques?
- Do you have an incident response plan and has it recently been tested so everyone knows what to do in the event of an attack?
- Are all necessary technical and procedural controls in place and operating properly?
- Has your security posture recently been assessed and tested and have you acted on the results?

TALKING POINTS

"As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems. Otherwise they're literally fighting the problems of the present with tools from the past. This attack is a powerful reminder that information technology basics like keeping computers current and patched are a high responsibility for everyone, and it's something every top executive should support." – Brad Smith, President and Chief Legal Officer, Microsoft

"The global reach [of WannaCry] is unprecedented. The latest count is over 200,000 victims in at least 150 countries, and those victims, many of those will be businesses, including large corporations ... We're in the face of an escalating threat, the numbers are going up. We are running around 200 global operations against cybercrime each year but we've never seen anything like this." – Rob Wainright, Director, Europol

FURTHER READING

- Preparing For A Black Swan Cyber Event – Financier Worldwide, January 2017
- European, Asian Companies Short On Insurance Before Ransomware Attack – Reuters, May 15, 2017
- The WannaCry Hackers Made Some Amateur Mistakes – Wired, May 15, 2017
- Path To Cyber Resilience: Sense, Resist, React – SCMP, April 25, 2017
- Global Alert To Prepare For Fresh Cyber Attacks – Financial Times, May 14, 2017

Empower Results®