Willis Towers Watson

WannaCry ransomware attack exposes organizations' vulnerabilities

What happened?

Over the last few days, a large-scale cyberattack utilizing a powerful strain of malware known as "WannaCry" took advantage of a flaw in the operating system of Windows-based computers. WannaCry was first brought to light during a recent WikiLeaks release of information (known as Vault 7) on the activities and capabilities of the U.S. government. WannaCry is ransomware that causes end-user frustration by encrypting any infected machine and making it unusable until the owner pays a ransom using the untraceable digital currency Bitcoin.

The attack first came to light midafternoon in the U.K. on May 12 and then spread across the globe, affecting computers in China, France, Germany, Japan, Russia, Spain and the U.S.[1] The attack also impacted many industries, including health care providers (mainly hospitals), manufacturing, telecommunications, utilities, logistics, transportation and educational facilities.

The spread of the ransomware was slowed when a U.K. security research team found a kill switch within the ransomware and turned it on.[1] While this action limited further spread of the malware, it did not resolve the issues for any computers that were already infected. In addition, it's been reported that variants of this ransomware have been reprogrammed without the kill-switch function.
Although the flaw was discovered earlier this year and Microsoft released a patch to fix the vulnerability shortly thereafter, Friday's widespread attack highlights the fact that many businesses (or individuals) either did not heed the warnings or delayed installation of the patch. As a result, more than 200,000 computers in 150 countries[2] have been affected by the first wave of the attack.[3]

1. Source: https://www.ft.com/content/05a79c02-37ee-11e7-821a-6027b8a20f23
2. Source: http://www.bbc.co.uk/news/world-39919249
3. Source: http://uk.reuters.com/article/us-cyber-attack-idUKKCN18B0AC

People

WannaCry was likely enabled through phishing emails (i.e., employees had to click on an infected link, likely a malicious Microsoft Word file, to enable the ransomware). This is another reminder that employees are the weakest link in any organization's cybersecurity strategy and are also the strongest defense. As such, to effectively manage the people risk, organizations should consider the following:

- Increase the level and regularity of employee awareness training in your organization. It is important that employees are trained to review emails closely to ensure they are from trusted and known senders before clicking on links. A cyber-savvy workforce holds the key to your enterprise resiliency.
- Assess whether your organization's IT department has the right or sufficient talent and skills needed in today's environment to effectively be prepared to handle these emerging threats. In this case, organizations that have been impacted should ask themselves why the patch that Microsoft made available was not installed in a timely manner. Was the lag in installation a talent or employee engagement issue?
- Evaluate whether your organization's culture is supportive of cyber awareness and action-oriented behaviors. For example, do leaders model positive behaviors that encourage employees to do the same, and do employees truly know what actions to take to report a cyber incident?

Technology

Several technology providers, including BAE Applied Intelligence, recommend the following steps to mitigate exposure to your organization's network systems:

- Ensure security updates are current for Microsoft and other operating systems.
- Ensure your antivirus and anti-spam filters are current. Most of the credible antivirus/anti-spam providers have already updated their systems to detect and prevent this malware, but because variations are emerging, it is difficult for providers to stay current with real-time fixes (i.e., zero-hour protection).
- If your networks have already been impacted, consider the following:
    - Restore your data from backup.
    - Consult with law enforcement and legal counsel on whether you should pay the ransom.
    - Focus on patch and antivirus updates.

Capital

Cyberinsurance continues to play a central role in managing cyber risk and protecting your organization's balance sheet. In addition to cyberliability insurance policies, there may be some coverage under kidnap and ransom or property policies. Coverage may be available for the cost of legal counsel, computer forensics, data restoration, business interruption and the ransom itself. Most policies require notification to the insurer as soon as practicable or within a set period of time, and also require consent before engaging outside vendors or incurring expense. It is therefore imperative to address this step immediately upon discovery of an attack. Click here for an earlier blog on ransomware.

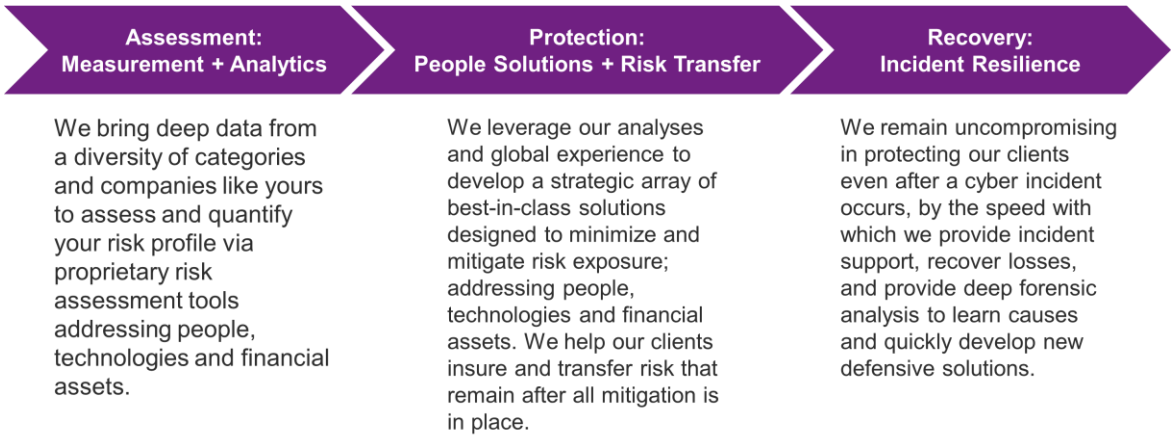
Willis Towers Watson is closely monitoring this incident. This type of attack, if not addressed quickly and effectively, could have far-ranging consequences to an organization's net income, network functionality and critical data. Please contact a member of your Client Service Team with any questions relating to this incident or to report a claim.

Willis Towers Watson

How Willis Towers Watson can help

Using proprietary tools, we'll assess, protect and help you recover from a cyber incident by evaluating the vulnerabilities within your people, capital and technology. Those assessments are then merged with deep data from companies like yours to produce a detailed risk profile and, ultimately, a more cyber-savvy workforce and resilient organization.

An integrated process that brings critical insights, best-in-class protections and uncompromising recovery resources to a businesses' cyber risk profile



Find out more: www.willistowerswatson.com/en/campaigns/cyber/assessment