MARSH

May 2017

CLIENT ALERT

WANNACRY RANSOMWARE CRISIS – LESSONS FOLLOWING THE TEARS

On Friday, May 12, 2017, a ransomware dubbed "WannaCry" claimed hundreds of thousands of victims in at least 150 countries. It demanded a payment of at least US$300 to release files and data, or to recover computer access.

The ransomware exploited a vulnerability in machines running older, unpatched versions of the Windows operating system.

Reported victims of the ransomware include commercial entities, telecommunication providers, government agencies, and even emergency service providers.

WHAT IS RANSOMWARE?

As its name suggests, ransomware holds data ransom by encrypting it and demanding a payment for the decryption.

The computer systems and/or data become inaccessible until the ransomware can be removed, either by IT security experts (no known solution has been found so far), or after payment of the ransom (assuming the group behind the attacks honour their end of the bargain).

The WannaCry virus is distinct, as it does not rely on victims to click on an infected link or attachment. It is a worm which, once inside an organisation, searches for vulnerable machines, and infects a large number of these machines quickly even without any user involvement.

HOW SHOULD YOU RESPOND IF YOU HAVE BEEN AFFECTED?

Marsh, like many other experts, generally advises against paying the ransom. While paying the ransom does sometimes result in the release of your data, there is no guarantee, and there is no recourse should the attackers renege on their promise. Furthermore, even after the data has been released, the cybercriminals continue to have unauthorised access to your systems, and are likely to target you in future, as you are known to be a ransom-payer.

Do also note that in some countries, the payment of ransoms is illegal. You may be subject to criminal proceedings should you make a payment.

For more information on immediate actions you should take if subjected to such an attack, please read our earlier piece on Claims and Cleanup Information for WannaCry Ransomware Cyber-Attack.

LESSONS

One clear lesson as we look to deal with the next cyber crisis is that technological infrastructure is more fragile than previously thought. That means firms need to consider the growing risk of business interruptions resulting from cyber incidents.

Greater connectivity and complexity among IT networks increases the risk that such disruptions will cascade. Such effects may be felt even when your firm is spared a direct hit, but suppliers or other business partners fall victim. In today's world, many businesses consider IT and communications outages the leading cause of supply chain disruptions, and these can lead to significant losses.

Beyond addressing technical measures, businesses should consider taking these measures to prepare for future attacks:

1. Build resilience through cyber response exercises. WannaCry was a novel piece of malware whose speed and impact were hard to anticipate. Firms should build flexibility, speed, and adaptability into their event-response capabilities. Regularly test those plans across your organisation, on various event scenarios, and identify and adapt specialised resources and expertise as you do so.

2. Update your risk modelling. Re-think the potential scenarios that could affect your operations, then work to consider the potential operational and financial impacts. That can help you evaluate second- and third-order consequences, like supply chain disruptions and associated financial costs, and determine which risks demand the most focus.
3. Review and update your cyber insurance programme. Networks will continue to become more connected and businesses more dependent on data-sharing. Every business that relies on technology – and most do – should take a fresh look at their cyber insurance programme. You should update policies as needed to provide coverage for business interruption and cyber extortion, and re-evaluate programme limits in the face of catastrophic scenarios.

WHAT CYBER POLICIES DO FOR YOU

Coverages can be customised to include any or all of the following in the event of a cyber breach:

- Network and security liability.
- Information asset.
- Business interruption.
- Cyber crime.
- Cyber extortion.
- Crisis management.
- Reputational damages.
- Legal proceedings.

ADDITIONAL TAKEAWAYS

1. Cyber is not merely an IT department issue. It is a risk issue for everyone in the organisation to deal with. To insist it is only an IT department issue is akin to insisting the government security and military agencies are the only parties responsible for fighting terrorism.
2. Just like terrorism, even the best security measures are unable to totally prevent cyber incidents. It is important to work on resiliency and crisis plans to supplement the security measures.
3. Nobody is ever 100% safe from cyber-attacks. A case in point: The WannaCry crisis originated from a breach in the network of the National Security Agency, a military intelligence organisation within the US Department of Defense. It should be safe to assume that they had some of the best IT engineers working on their systems which were ultimately breached.
4. The most common source of cyber breaches: human error/carelessness. When the system is breached, it is not necessarily the fault of the IT department.
5. Outsourcing IT functions does not outsource your liabilities to your clients, business partners, employees, and regulators.
6. Studies have shown that many individuals around the world believe their lives can fall apart if they lose their mobile devices. The loss of data or functionality of their networks can also have a similar devastating effect on businesses. There have been cases of otherwise-profitable businesses which have collapsed because of cyber incidents.
7. It is not just the loss of data that is at stake in a cyber-attack. The reputational loss from having customers' personal data exposed can sink a business overnight, especially when trust or goodwill is critical to the relationship between the business and its customers. The loss of data, therefore, is not necessarily proportionate to the reputational and business loss. For example, a bank may lose 10 customers' data, resulting in their personal information being compromised.
   The direct financial impact from this may be manageable to a bank – simply compensating these 10 customers for their losses. However, once this piece of news is reported in the media, the bank's reputation takes a hit, and thousands of other customers may decide to take their business elsewhere. As a result, the financial fallout from that reputational loss will be much greater.

Ransomware and other evolving threats will increase in frequency and sophistication. Firms need a comprehensive cyber risk management strategy — including economic risk modelling, optimised cybersecurity and cyber insurance programs, and resilient cyber response capabilities, to ensure a quick, effective response and a timely return to normal operations.

For more information about cyber risk management contact your Marsh representative or:

Kelly Butler
Cyber Leader
+61 3 9603 2194
Kelly.Butler@marsh.com

marsh.com.au