PARKER | SMITH | FEEK

COMMERCIAL INSURANCE

EMPLOYEE BENEFITS

PERSONAL INSURANCE

RISK MANAGEMENT

SURETY

PRACTICE GROUP:
TECHNOLOGY

MAY 17, 2017

WANNACRY ON A FRIDAY? –
MITIGATE YOUR CYBER LIABILITY WITH CYBER INSURANCE

Michael Edmonds | Account Executive

The technology, information, and security officers of today certainly have no shortage of job security, with the seemingly endless supply of attacks on company networks. On Friday, May 12, 2017, cybercrime achieved a new record. In a widespread ransomware attack, the WannaCry2 malware attacks crippled critical infrastructure, including hospitals, telecommunications, and distribution/supply chain services in more than 100 countries across the globe within the span of 48 hours.[1]

Some estimates suggest that 300,000 computers were affected by a ransom payment of up to $300 per device demanded by the attackers (that's $90 million for anyone doing the math).[2] WannaCry2 exploited a Windows vulnerability purportedly identified by the NSA and leaked to the internet. Although Microsoft released fixes in March, the attackers took advantage of users that did not apply the software fix and the vulnerability spread with great speed from one workstation to a network of users.[3]

This attack spared no industry. Whether or not your company fell victim to this broad reaching scheme, this should be a wake-up call and serve as a reminder to prepare for the unexpected. While the attack appears disabled now, experts recommend preparing for copycat attacks with new twists. For example, while ransomware (i.e. the criminal practice of stealing data and not returning it to its owner until a ransom payment is made) was the WannaCry2 tactic of choice, criminals could shift to new tactics such as stealing personally identifiable information or embedding Remote Access Trojans.

IBM Security Services[4] recommended the following protective actions for all enterprises:

1. Patch systems immediately to prevent attacks.
2. Deploy security intelligence systems to detect attacks.
3. Develop a response playbook with your team.
4. Ensure your employees, suppliers, and others that work with your company receive regular training.
5. If the WannaCry2 attacks have impacted you, contact a cyber security vendor to determine next steps to mitigate exposure.

[1] https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

[2] http://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC

[3] http://www.bizjournals.com/seattle/news/2017/05/15/microsoft-slams-nsa-windows-ransomeware-attack.html

[4] IBM's Perspective on Security Attacks

continued >

MITIGATE YOUR CYBER LIABILITY WITH CYBER INSURANCE

One thing is for certain; this is not the last and unfortunately will not be the largest scheme of this kind. Cyber insurance is strongly encouraged to protect your organization from damages due to a cyber event. Cyber insurance protects you from both first and third-party costs associated with a breach or suspected breach.

Most important is how the insurance contract is drafted. Many new carriers have released cyber insurance products, and it is vital the contract is specifically tailored to insure your particular needs. Correctly written cyber insurance should cover the majority of the costs associated with this most recent attack. As a reminder, preparedness is the best risk management tactic when planning for a potential breach. Here are a few more things to consider along with the points suggested by IBM above.

1. Third Party System Evaluation of Networks and Servers (Vulnerability Scan and Penetrating Testing). Inventory your data to understand where critical assets are stored. Consider who may be targeting your organization.
2. Develop Cyber/Data Breach Response Plan. Define roles and responsibilities, vendor selection, and who will speak on behalf of the company.
3. Consider Cyber Insurance. Experienced "breach coaches" are a valuable resource, as are pre-negotiated rates for analytics and legal counsel, and pre and post vendor services.
4. Vendor Contract Review. Understand your vendor contracts and your provider's responsibilities in the event of a breach. What are the indemnification, notification, and cooperation requirements?
5. Employee Training. Written social media and network access policies, phishing training, HIPAA training.

> Regardless of industry, every organization must now prepare for the threat of cyber-attacks. Call Parker, Smith & Feek today, and we can help you craft a cyber insurance policy that protects your organization from a potential event.