THE TEXAS LAWBOOK

SERVING BUSINESS LAWYERS IN TEXAS

WannaCry Attack Prompts Focus on Cyber Insurance

By Amy Elizabeth Stewart of Amy Stewart Law – (June 5, 2017) – Although it didn't wreak the havoc cybersecurity analysts feared it might, the global WannaCry malware attack earlier this month provides a timely reminder that hackers are endlessly inventive and have a lot of time on their hands – time they spend devising new ways to profit by creating chaos and exploiting the world's interconnectedness.

Amy Stewart

Because the ransom demands associated with WannaCry were well below insurance deductibles, the attack is not expected to trigger significant insurance payouts. But imagine a similar scenario with prohibitively high ransom demands, or one in which the hacker insists the corporation take an undesirable action. Consider the risk to a company's bottom line if business-critical data is locked down and operations grind to a halt as a result.

Effective cyber risk management involves assessing the company's potential exposures, ensuring that appropriate security protocols are implemented and understanding the options for transferring cyber risks through insurance.

Driven by headlines, cyber insurance discussions often focus on data breaches and coverage for notification, public relations and breach coach expenses, investigation costs, and defense and indemnification against third-party claims for damages.

As WannaCry illustrates, however, cybersecurity risks reach well beyond data breaches – extending to information system failures, the loss or destruction of data, cyber ransom demands and even cyber theft.

Understand the risks insured by cyber policies. Data breach risks are at the forefront of most cyber insurance discussions, but cyber policies can provide coverage for other cyber risks. WannaCry was cyber extortion – the malware locked computers and held data hostage until the user paid a ransom. The cyber version of kidnap and ransom insurance would likely respond to an attack like WannaCry if the demand amount exceeded the policy's deductible. In addition to data breach and cyber extortion coverage, cyber policies may cover data recovery costs, investigations, lost income or profits due to a system interruption, liability to others for system failures, and damages to others arising from the company's online activities.

Prepare to negotiate. Cyber policies are not standardized. The terms vary widely – from insurer to insurer and from policy to policy. Here's the bad news: Buyer, beware. The good news is that there's room for negotiation, especially for large insureds. Compare the policy forms carefully. Look at the policy's language specifically, not just the marketing hype.

Beware of exclusions. Policy exclusions effectively shift the risk back to the insured. Many, if not most, cyber exposures are tied to human error or to carelessness. In the WannaCry malware attack, an out-of-date Windows security patch allowed malfeasors to install malware to the user's computer and subsequently infect the network. Users who had not accepted recent updates were at risk. Most cyber insurers require information about the company's cybersecurity protocols as part of the underwriting process before the policy is issued. Some policies then seek to exclude coverage if the insured fails to follow its own protocols. These exclusions should be avoided, particularly if they eliminate coverage when the cyber loss is caused by a negligent failure to follow policies and procedures or some other mistake. ›

Negotiate for specific vendors on the front end. Dealing with a breach or other cyber event requires a lot of help from third-party vendors. One benefit of cyber insurance is access to approved vendors that have been carefully vetted by the insurance industry. If you want to use a particular breach coach or notification company, ask the insurer for approval when you buy the policy and make sure the policy is endorsed to make it clear that the vendor is approved. Otherwise, expect to be limited to the vendors the insurance company has preselected.

Negotiate broad coverage for ransom payments. The WannaCry hackers sought ransom in the form of bitcoin, a form of digital currency. Other hackers have made demands for some sort of action. Recall the Sony Pictures cyberattack in 2014, when hackers stole personal and confidential data from Sony's computer systems, then made vague demands that Sony not release The Interview, a film based on a fictional assassination plot against North Korean leader Kim Jong Un. Cyber extortion coverage should cover demands for money, as well as demands for property or other consideration.

Inquire about system interruption coverage. Traditional business interruption insurance covers certain business losses that result from disaster-related damages like hurricanes, fires and floods. A manufacturing facility severely damaged in a fire may be unable to resume operations for months while repairs are made. Certain business losses suffered as a result would be covered under a business interruption policy. Consider the impact if a WannaCry-type virus infects the reservation system for a large hotel chain. Depending on the length of the downtime, countless reservations may be lost as travelers book their stays at competing hotels. Many cyber insurers offer system interruption coverage, which would protect the insured from certain losses caused by a system failure. System failure or system interruption coverage is often subject to a waiting period – meaning that the insurance kicks in only after the system has been down for a specified period of time. Sublimits may also apply.

Comply with notice and consent requirements. In the wake of an attack, companies are understandably focused on assessing and controlling the damage and getting back to business. Given the losses associated with production and operational delays, decisionmakers may seek to make a ransom payment quickly, before notifying the cyber insurer. Cyber policies likely require notice and may require insurer consent. Understand the policy requirements in advance and comply with any notice or consent provisions to avoid jeopardizing coverage.

No business is entirely immune to a cyberattack, and the potential consequences can be devastating. The WannaCry attack may not have unleashed a global "cyber-tastrophe," but it was a clear shot across the bow to businesses. Prepare now for the next one.

Because there will be a next one.

Amy Elizabeth Stewart is the managing principal of Amy Stewart Law, an insurance coverage boutique in Dallas. Amy advises corporate policyholders on insurance issues, negotiates corporate insurance disputes prior to litigation and, when necessary, litigates commercial insurance recovery and bad faith claims. Amy is the author of Texas Insurance Coverage Litigation: The Litigator's Practice Guide, published by Texas Lawyer Books and American Lawyer Media. She also speaks regularly on insurance issues and writes for legal publications, including the American Bar Association's Coverage periodical. For more information on cyber insurance, see Tips for Buying Corporate Cyber Insurance and 6 Quick Tips for Law Firms in the Market for Cyber Insurance on the firm's blog, www.insurancesidebar.com. Amy can be reached at amy@amystewartlaw.com.

Please visit www.texaslawbook.net for more articles on business law in Texas.