KING & SPALDING

Client Alert

Insurance Coverage & Recovery Practice Group

June 6, 2017

WannaCry, Adylkuzz, and Cyber Breach: How to Maximize Insurance Coverage in the Event of Cyber Attack

The worldwide hack that surfaced on May 12—known as "WannaCry"—wreaked havoc on hundreds of thousands of computers across the globe and is one of the biggest ransomware hacks the world has ever experienced.[i] The U.K.'s National Health Service was forced to reschedule surgeries and appointments, and Fortune 500 companies, along with other businesses, universities, government institutions, and hospitals throughout Asia and Europe also fell victim to the attack.[ii]

The WannaCry malware infects computers running an older version of Windows and then encrypts (or "seizes") the data.[iii] After locking a victim out, WannaCry displays a message demanding a bitcoin payment within 7 days and threatens deletion of the data if no payment is received.[iv] Late on May 12, Microsoft issued a security patch that acted as a kill switch, protecting computers with the patch installed.[v] This kill switch is believed to be the reason that companies in the United States remained relatively unscathed.[vi]

WannaCry's ransom demand was relatively modest (with a first request for $300 and a second request for $600). But its ability to spread quickly throughout several types of public and private institutions, and its effectiveness at seizing data and interrupting business operations, has already inspired multiple imitations, some of which may be developed to elude the security patch.[vii] Some experts are theorizing that WannaCry was (i) merely a test to see how institutions would respond to the problem and how long it would take, or (ii) used as a way to gather intelligence on the types and number of computers and networks that could be infected.[viii] And it is predicted that the next hack will be worse.[ix] Recent reports suggest that a larger attack, known as Adylkuzz, has been released and is lurking in the background of hundreds of thousands of computers mining a virtual currency known as Monero.[x] Other data security experts are warning

For more information, contact:

Meghan H. Magruder
+1 404 572 2615
mmagruder@kslaw.com

Anthony P. Tatum
+1 404 572 3519
ttatum@kslaw.com

Shelby S. Guilbert
+1 404 572 4697
sguilbert@kslaw.com

Amy E. Dehnel
+1 404 572 3541
adehnel@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

of other attacks now surfacing in the wake of WannaCry that appear to have the potential to cause more destruction than WannaCry.[xi]

Costs associated with cyber attacks like WannaCry are increasing at a rapid pace,[xii] with annual financial impacts running into the billions of dollars.[xiii] In 2016, cybercrime cost the global economy over $450 billion in losses,[xiv] and as more data is stored on networks every year, those damages are expected to grow to more than $6 trillion by 2021.[xv] Despite these staggering costs, a recent survey indicated that more than half of all businesses are not prepared to deal with a cybercrime attack.[xvi]

The WannaCry attack is a reminder that every business should have in place a robust incident response plan in the event of a cyber attack. In addition, organizations of all kinds should consider cyber security insurance to protect against the risk of cyber breach losses.

Evaluate Your IT Systems Before Applying for Cyber Coverage:

Before considering cyber coverage, a company should analyze its potential exposure and shore up any information security gaps before engaging in the underwriting process. Roadblocks to coverage often include inadequate network security, inadequate information security policies and procedures, poor records management, outdated systems or a failure to install security patches, and inadequate employee training. It is important to address any issues prior to the insurer’s underwriting review to prevent a rejection of coverage or higher premium. Also work carefully with coverage counsel throughout the application process because cyber policies are unique and problems in the application process may negate coverage in the event of a claim.

Key Cyber Insurance Coverages:

Cyber coverage can vary widely amongst different insurers. Given the wide variety of types of cyber incidents that can occur, and the varying cyber risks that companies in different industry sectors face, it is imperative that companies carefully review their cyber coverage to address their unique risks and avoid potential gaps in coverage.

First-Party Coverages Available: Cyber insurance typically provides first-party coverage for a wide array of costs that a company may incur from a breach, including costs associated with, among other things: (i) forensic investigation costs; (ii) legal costs associated with a breach response; (iii) crisis management / PR costs; (iv) costs relating to mailing notifications to consumers; (v) credit monitoring costs; (vi) setting up a call center to handle consumer calls; (vii) business interruption costs, especially following a denial of service attack; (viii) restoration of systems; and (ix) remediation costs.

Third-Party Coverages Available: Cyber policies also provide third-party liability coverage. Following an announcement of a breach that involves consumer information, it is now increasingly likely that the company will be subject to a regulatory investigation by at least one, if not several, state and federal agencies. Additionally, class action lawsuits are now often filed within hours of a breach announcement. In the instance of a ransomware attack like WannaCry that targets institutions like hospitals, it is possible that personal injury lawsuits may also flow from the cyber security breach.

A company should ensure its cyber liability policy covers costs associated with regulatory investigations and litigation, including costs associated with regulatory settlements that often impose both monetary penalties and requirements to implement security enhancements and continued monitoring programs, which can be costly. Moreover, any company that collects credit card information should consider coverage for PCI-related fines or penalties.

Beware of Exclusions: Cyber policies may contain exclusions and limitations to coverage, some of which could exclude coverage for ransomware attacks like WannaCry. Keep in mind the following when evaluating a cyber insurance policy:

- *Ensure Adequate Business Interruption Coverage*. The WannaCry attack highlights the way that malware can bring businesses to a standstill. Pay careful attention to business interruption wordings to minimize waiting periods and ensure coverage for cyber incidents that interrupt your company's operations.
- *Review Insuring Agreements for "Phishing" and Fraudulent Wire Transfer Coverage*. Many cyber policies will not cover claims arising out of breaches that occur if an employee unwittingly causes a breach by clicking on a "phishing" link, or causes the company to fall victim to a fraudulent wire transfer scheme. Carefully review insuring agreements and exclusions to ensure coverage for these emerging risks.
- *Be Aware of Retroactive Dates*. Cyber policies often restrict coverage to breaches or losses that occur after a specific date and in some forms it is the inception date of the policy. Because breaches may go undetected for some period of time, it is important to purchase coverage with the earliest possible retroactive date.
- *Seek to Broaden Regulatory Investigation Coverage*. State and federal agencies have become increasingly active in regulating privacy issues, and it is important to ensure that a cyber policy covers all potential regulatory investigations following a breach, rather than a narrow enumerated list of agencies or agency actions.
- *Ensure Coverage for Data in the Cloud*. Companies should make sure that data stored with third parties or "in the cloud" is covered even if the third party experiences the data security breach.
- *Avoid Terrorism Exclusions*. Cyber policies may exclude coverage for terrorism, hostilities, and claims arising from "acts of foreign enemies." Given that many data security breaches originate abroad and may be perpetrated by groups that could be considered "foreign enemies," companies should limit the scope of these types of exclusions.
- *Pay Attention to Sublimits and Retentions*. High retentions and sublimits can greatly reduce coverage. Review any sublimits to confirm the coverage is adequate.

Potential Coverage Under Other Insurance Policies:

Commercial General Liability Policies: Although often overlooked, CGL policies may be another potentially valuable insurance asset in the event of a data security breach.

Directors & Officers/Errors & Omissions Policies: D&O and E&O insurance policies also may provide valuable sources of recovery in the event of a data security breach, depending on the claims brought against your company. D&O policies may protect directors and officers against claims arising out of cyber incidents, and also may protect companies against securities and shareholder derivative lawsuits arising out of cyber incidents.

E&O insurance policies can provide coverage for companies against data security breaches arising out of the provision of professional services. For instance, if a healthcare company suffers a data breach while rendering professional services and compromises its clients' confidential information (or the confidential information of the patients of its clients), E&O coverage may help cover the resulting losses.

Crime Policies: Crime insurance policies may also provide insurance for a data security breach. If an employee is involved in a data security breach, crime insurance policies may provide coverage.

If You Experience A Cyber Event:

Gather All Policies and Closely Review Their Terms. Do not assume your losses are uninsured. As policy terms vary and may be subject to different interpretations, consult with coverage counsel to assist in evaluating coverage. You may have vendors pre-approved in your cyber policies to assist in your incident response.

Provide Prompt Notice of All Claims and Potential Claims. Policies often require policyholders to notify the insurer "immediately," "as soon as possible," or "as soon as practicable" after the insured becomes aware of a potential claim.

Collect and Preserve Evidence of Business Losses and Damages. It is important to work with counsel to collect all costs, expenses, and damages related to a cyber breach. Many policies also provide coverage for expenses associated with claim-related activities.

Be Careful About Internal and External Communications Regarding the Loss. Businesses should be careful when communicating with brokers and insurers concerning losses. In the event of a disputed claim, it is important to protect attorney-client privileged communications.

Coordinate Mitigation Efforts With Insurer. Mitigate losses and keep insurers informed about vendors and law firms that have been engaged to assist with incident response.

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,000 lawyers in 19 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

[i] Kelsey D. Atherton, *5 Things We Learned From WanaCryptor, The Biggest Ransomware Attack in Internet History*, Popular Science (May 17, 2017), http://www.popsci.com/time-to-start-thinking-about-how-to-survive-next-ransomware-attack; Steve Lohr & Liz Alderman, *The Fallout From a Global Cyberattack: "A Battle We're Fighting Every Day,"* The New York Times (May 15, 2017), https://www.nytimes.com/2017/05/15/world/asia/china-cyberattack-hack-ransomware.html; Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED (May 12, 2017, 2:03 PM), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/; David E. Sanger, Sewell Chan, & Mark Scott, *Ransomware's Aftershocks Feared as U.S. Warns of Complexity*, The New York Times (May 14, 2017), https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html.

[ii] Lohr & Alderman, *supra* note i; Newman, *supra* note i; Sanger, et al., *supra* note i; Alexander Urbelis, *WannaCrypt Ransomware Attack Should Make Us Wanna Cry*, CNN (May 14, 2017, 9:10 AM), http://www.cnn.com/2017/05/14/opinions/wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-urbelis/.

[iii] Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NPR (May 15, 2017, 2:31 PM), http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday; Zach Epstein, *How to Protect Yourself Against WannaCry Ransomware*, BGR (May 16, 2017, 8:49 AM), http://bgr.com/2017/05/16/wannacry-ransomware-how-to-stop-wanna-cry-windows-patch/.

[iv] Chappell, *supra* note iii; Epstein, *supra* note iii.

[v] David Z. Morris, *Microsoft Windows Now Patched Against WannaCry Ransomware Attack*, Fortune (May 13, 2017), http://fortune.com/2017/05/13/wannacry-ransomware-microsoft-windows-patch/.

[vi] Lily Hay Newman, *How an Accidental "Kill Switch" Slowed Friday's Massive Ransomware Attack*, Wired (May 13, 2017, 3:27 PM), https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

[vii] Chappell, *supra* note iii; Epstein, *supra* note iii.

[viii] Urbelis, *supra* note ii.

[ix] Bruce Schneier, *The Next Ransomware Attack Will Be Worse Than WannaCry*, The Washington Post (May 16, 2017), https://www.washingtonpost.com/posteverything/wp/2017/05/16/the-next-ransomware-hack-will-be-worse-than-the-current-one/?utm_term=.6fc85aa6e28d.

[x] Graham Kates, *Adylkuzz Hack, Called Larger Than WannaCry, Slows Computers Across the Globe*, CBS News (May 17, 2017, 4:33 PM), http://www.cbsnews.com/news/adylkuzz-hack-larger-than-wannacry-slows-computers-nsa/.

[xi] *See, e.g.*, Dell Cameron, *In WannaCry's Wake, A New Rapidly Spreading Ransomware Attack Appeared Today*, Gizmodo (May 19, 2017 5:31 PM), http://gizmodo.com/in-wannacrys-wake-a-new-rapidly-spreading-ransomware-a-1795385418; Andy Greenberg, *Hackers Are Trying to Reignite WannaCry with Nonstop Botnet Attacks*, Wired (May 19, 2017, 1:05 PM), https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/.

[xii] Adam Chandler, *How Ransomware Became a Billion-Dollar Nightmare for Businesses*, The Atlantic (Sept. 3, 2016), https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/.

[xiii] *Id.*

[xiv] Luke Graham, *Cybercrime Costs the Global Economy $450 Billion: CEO*, CNBC (Feb. 7, 2017, 10:00 AM), http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

[xv] Steve Morgan, *Cybercrime Damages Expected to Cost the World Trillion by 2021*, CSO (Aug. 22, 2016, 11:14 AM), http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

[xvi] Graham, *supra* note xiv.