BURR ALERT

Insurance Coverage for Cybercrimes in the Wake of COVID-19

By Taylor Johnson April 2020

Attorneys are well aware of the ways in which corporate clients are increasingly conducting their business and affairs electronically. A business may routinely place orders with trusted vendors via e-mail, rely on the fidelity of third-party software and API connections for key business functions, or collect massive amounts of customer data to enhance its services. The digitization of various products, services, and business processes has generally benefitted businesses, but it also poses new risks. Clever cybercriminals, eager to take advantage of an organization's reliance on technology and electronic communications or commerce, are constantly probing for ways to commit cyber thefts or frauds for their own financial gain or criminal purpose.

As COVID-19 has forced employees to work remotely (and potentially on unprotected networks or devices), the risk of cybersecurity incidents has increased dramatically. The FTC, WHO, and various news organizations have issued warnings of cybercriminals' attempts to prey on peoples' anxieties over the pandemic's spread and recent economic fallout.[1] For example, a fraudster may impersonate a company CEO using a "spoofed" e-mail that purports to contain a company's strategic response to COVID-19 disruptions, but in fact contains malicious code meant to grant the fraudster access to the company's system. Alternatively, a fraudster may impersonate a vendor using a misleading e-mail address and advise a company controller that it will apply a discount to an open account balance if the controller wires funds immediately. One analyst with the security firm Dark Shadows identified a February 2020 post on a Russian "dark-web" hacking forum (XSS) offering malware for sale that could be inserted into an e-mail attachment resembling the John's Hopkins real-time infographic map of confirmed COVID-19 cases. In these unsettling times it is paramount that companies review their cyber-liability policies as well as other insurance policies to assess whether there any coverage gaps in light of the current pandemic.

I. What Will A Cyber Liability Policy Typically Cover?

Cyber-liability insurance is a relatively new type of insurance coverage, which was introduced in the 1990's to address gaps in traditional insurance coverage, for losses incurred due to various types of cyber risks. Depending upon the type of claim at issue, a cyber liability incident might trigger coverage under any one of several policy types: D&O coverage, E&O coverage, Commercial General Liability insurance, Crime/Fraud policies, Fidelity insurance, and stand-alone *cyber insurance policies*. Cyber liability specific policies are generally intended to cover a variety of both liability and property losses arising out of data breaches, such as costs of notification, credit monitoring, defense of claims by plaintiffs for identity theft or claims by regulators, fines and penalties, liability arising from website

[1] https://www.consumer.ftc.gov/blog/2020/03/ftc-coronavirus-scams-part-2

media content, as well as property exposures which arise from business interruption, data loss or destruction, computer fraud, funds transfer loss, and cyber extortion.[2]

While this article addresses types of coverage provisions found in cyber liability policies, each policy will vary. Cyber liability policies are manuscript policies, which unlike other types of liability are not standardized. There are many types of coverage forms, many tailor-made for a particular company or type of business. Coverage is often provided for the following[3]:

First Party Data Breach Coverage: covers company's direct losses in connection with a data breach including: hiring professionals to assist in investigation and response; costs of notification of breach; costs of providing credit monitoring; establishing resources for affected persons; may also include coverage for business interruption and costs associated with restoring lost data.

All of the 50 states now have enacted data privacy laws which govern what types of information are protected; the steps which must be taken to protect that information; and the consequences and actions required in the event of a breach, among other things. Most allow for civil penalties to be assessed for knowing and willful violations of the law.[4]

Third Party Data Breach Coverage: covers losses from third-party claims resulting from a breach—for example, a lawsuit by a bank against a retailer like Target; or a customer against a company based on damage from release of personal protected information.

Computer Fraud Coverage/ Funds Transfer Coverage: Computer Fraud and Funds Transfer Fraud coverages typically cover losses sustained by some fraudulent use of a computer or electronic data that causes an insured or bank to transfer covered property to unintended persons or accounts.

Social Engineering Loss Coverage: covers losses originating from a "social engineering" fraud scheme, typically involving deception or manipulation of human actors to procure a fraud.

Cyber Extortion/ E-Threat Expense Coverage: covers reimbursement for extortion-type activities by cyber criminals, typically including coverage for funds or property an Insured surrenders, as well as fees for independent negotiation or consultant, among other related expenses.

Cryptocurrency Theft Coverage: A few insurers have started to offer products which cover some of the risks associated with the volatile digital currency market. Companies who accept or deal-in digital currency, like bitcoin, may have a limited amount of insurance products available, but do to the high risk of hacking, those products come at a significant price.

---

[2] Insurance Risk Management Institute, Glossary of Insurance and Risk Management Terms, www.irmi.com/online/insurance-glossary/terms/c/cyber-and-privacy-insurance.aspx

[3] See generally, Collins. Betsy, Business Liability Insurance Answer Book 2020, Ch. 11 "Cyber Liability Insurance", Practising Law Institute.

[4] Jeewon Kim Serrato, *US states pass data protection laws on the heels of the GDPR*, (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/

As with all insurance policies, cyber liability policies will include numerous exclusions which must be reviewed along with specific policy limits in order to assess whether you are adequately covered in light of the current pandemic.

II. The Unique Threat Posed by Coronavirus and the Need for a Robust Cyber Liability Insurance Policy

With the US workforce now working primarily remotely, there is increased pressure on company's IT security to defend against cyber-attacks. Cyber criminals love a panic- when employees may not practice the best cyber security practices. Thus, organizations should strive to be pro-active in defending against cyber-attacks, by taking steps which may include[5]:

- Verifying and reviewing IT security plans and anti-virus monitoring tools;
- Maintaining secure VPN or other multi-factor authentication remote portal networks;
- Testing system readiness;
- Encouraging use of company rather than personal devices for work;
- Increasing monitoring for attacker activities; and
- Continuing to train and inform employees on increased threats specific to coronavirus (such as running a simulated spear phishing attack), among other things.

Even if precautions are taken, cyber liability insurance provides a critical additional layer of protection in the event of an attack. It is important to have an experienced broker help coordinate multiple types of coverages including CGL, professional liability, crime/fraud, fiduciary liability, and employment with a finely-tuned stand-alone *cyber insurance policy* so that you get the maximum potential coverage for cyber incidents. All coverages should be reviewed in light of the current pandemic and the myriad of insurance issues which will arise in the wake of coronavirus.

To discuss this further, please contact:

Taylor Johnson at tjohnson@burr.com or at (251) 345 8235 or the Burr & Forman attorney with whom you normally consult.

[5] Sharton, Brenda, *Will Coronavirus Lead to More Cyber Attacks,* HARVARD BUSINESS REVIEW, March 16, 2020, available at https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks