HUNTON ANDREWS KURTH

Lawyer Insights

Spring 2019

SECURITY ALERT: So You Think You Are Fully Insured? Think About Cyber Breaches And Then Think Again

By Lorelie S. Masters, Sergio F. Oehninger and Patrick M. McDermott

Published in NCBJ Conference News

Rarely does a week go by without news of a new data breach, raising worrisome security issues for businesses and individuals.

Data breaches expose individuals' personal identifying information ("PII"). The Equifax hack alone led to the disclosure of the PII of more than143 million people, nearly all of them in the United States.

The Many Types of Cyber Breaches

Hacks can lead to the loss of money, as in the case of increasingly common "social engineering" schemes (i.e., attacks that involve deceiving a target into cooperating). Those schemes often involve a fraudster posing as someone he is not and persuading an individual to send money to the fraudster. As an example, a hacker may gain access to your email account. The hacker then monitors your email and waits for an opportunity like the purchase of a home. The hacker then sends you a fraudulent email that looks like an email you are expecting, containing wire instructions for your down payment. You make the payment per the wire instructions only later to discover that the sellers never actually received the money and that the money instead went to the hacker. This scheme has been replicated countless times in the business setting, whereby the hacker poses as a vendor or other counterparty and swindles a company's employee to wire funds to the fraudster in what seems like a legitimate transaction.

Ransom requests are yet another peril. In this situation, a hacker gains access to your computer and uses malware to encrypt your files. The hacker then threatens to destroy the files unless you pay a ransom. The recent "Wanna cry" attack was a ransomware incident that reportedly infected more than 230,000 computers in over 150 countries within one day.

Security risks are not confined to PII and money. Cyber breaches can also affect personal security. For instance, in Austria, hackers shut down a hotel's keycard management system, trapping hotel guests inside their rooms until ransom was paid. Concerns abound about risk to property and personal injury. For instance, property damage could result if a dam is hacked and ceases to work, causing rampant flooding. And personal injuries could result from the hack of a driverless car's electronic systems.

Even the most cutting-edge technologies like blockchain are not risk free. Blockchain is the distributed ledger technology that lies at the foundation of the cryptocurrency Bitcoin and other cryptocurrencies. "Forbes has described it as 'a distributed and immutable (write once and read only)record of digital events that is shared peer to peer between different parties (networked database systems).'"

The use of blockchain across industries is increasing. A major automobile manufacturer has partnered with MIT's Media Lab and others to identify the uses of distributed ledger technology in the automobile industry. A global retailer teamed up with a multinational technology company and recently announced the results of a test using blockchain in which it traced a food product from farm to shelf in seconds, as compared to the days-long process without blockchain. A number of international banks selected a multinational technology company to use blockchain technology to build an international trading system called Digital Trade Chain.

Observers continue to predict the expanding use of blockchain and tout its security. However, it is not foolproof. For instance, a Bitcoin exchange (Mr. Gox) handling 70 percent of all Bitcoin transactions back in 2013 suffered a technical glitch resulting in Bitcoin temporarily shedding a quarter of its value. In 2015, Interpol identified an opening in blockchain used for cryptocurrencies that hackers could exploit to transfer malware to computers.

Insurance Coverage for Cyber Events

Given these risks, insurance is an important aspect of protection from loss related to cyber events. While courts have not dealt frequently with individuals seeking coverage for cyber-related losses, one recent example shows the benefit of keeping insurance in mind as part of your cyber security plan. *Kimmelman v. Wayne Insurance Group*, No. 18-cv-1041 (Ohio Ct. Common Pleas, Sept. 25, 2018) involved a dispute over insurance coverage for the theft of Bitcoin from an individual's online account. The individual sought coverage under his homeowners' policy, which had a sublimit for monetary losses. The court found that cryptocurrency was property, not money, and therefore not subject to the sublimit for money losses.

Other courts have found coverage for cyber losses under crime policies. For instance, one court found coverage under a crime policy for a manufacturer's loss, reasoning that the fraudulent email that prompted wire transfers to fraudsters was an immediate and proximate cause of the loss. *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am*.,895 F.3d 455 (6th Cir. 2018). Another court found coverage under a crime policy for a cloud-based service provider's loss resulting from an employee being deceived into transferring funds in response to an email that looked like it was from the company's president when it was actually from a fraudster. *Medidata Sols. Inc. v. Fed. Ins. Co*., 729 F. App'x 117, 2018 WL 3339245 (2d Cir. 2018).

However, other court decisions highlight the risks in relying solely on traditional coverage like homeowners, general liability, and crime coverages for cyber-related losses. See *Zurich Am. Ins. Co. v. Sony*, No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014)(finding no coverage under a general liability policy for losses resulting from hack); *Am. Online, Inc. v. St. Paul Mercury Ins. Co*., 347 F.3d 89 (4th Cir. 2003) (finding no coverage for individuals' claims against AOL for loss of stored computer data because damage to data was not damage to "tangible property" as the general liability policy required for coverage).

Thus, to better protect against losses resulting from data breaches or other cyberattacks, individuals should consider purchasing coverage specifically written to cover cyber-related losses. Major insurers are beginning to offer coverage to individuals for this purpose. One insurer provides a cyber coverage add-on to its homeowners' policy that it says provides "enhanced protections for cyberattacks that lead to extortion and ransomware, financial loss, cyberbullying, cyber disruption, and breach of privacy" and "discounted access to third-party resources, with tools ranging from how to secure network and mobile devices to how to spot signs of online manipulation." Another insurer offers cybersecurity coverage as an endorsement to its renters' and homeowners' policies and claims its cyber endorsement contains "an innovative cyber coverage for computer attacks, cyber extortion, online fraud and the breach of personal information of others involving smartphones, computers and connected home devices."

Applications for cyber coverage can be particularly time-consuming because of the technical nature of some of the inquiries. Individuals should take the time needed to provide accurate answers rather than later face an insurer's claim that an allegedly inaccurate answer on the application voids coverage.

When purchasing cyber coverage, individuals should consider their potential losses to help identify the areas in which coverage is needed. Possible losses include those related to forensic analyses undertaken post-breach: legal fees; lost digital assets; repair, including restoring or replacing data; ransom; identity theft fees; credit monitoring for victims; and notifying affected individuals.

Because of the wide-ranging nature of potential losses and the differences in coverage provided by cyber-related policies, price alone should often not be the determining factor in choosing a policy. The cheapest policy may also provide drastically less coverage than a pricier policy.

Finally, after purchasing cyber coverage, it is advisable to maintain the policy in an easily accessible location. This includes maintaining a hard copy of the policy since you may need it most when your electronic files and computers are unavailable. If you are subject to loss resulting from a data breach or other cyber incident, identify all potentially applicable policies — whether cyber-specific or not —and comply with the notice requirements in those policies.

Lorelie S. Masters *is a partner in the insurance coverage group in the Washington, DC office. Lorie handles all aspects of complex, commercial litigation and arbitration. She can be reached at +1 202 955 1851 or lmasters@HuntonAK.com.*

Sergio F. Oehninger *is counsel in the insurance coverage group in the Washington, DC office. He represents companies in complex insurance coverage disputes nationally and internationally. He can be reached at +1 202 955 1854 or soehninger@HuntonAK.com.*

Patrick M. McDermott *is an associate in the insurance coverage group in the Richmond office. Patrick counsels clients on all aspects of insurance and reinsurance coverage. He assists clients in obtaining appropriate coverage and represents clients in resolving disputes over coverage, including in litigation and arbitration. He can be reached at +1 804 788 8707 or pmcdermott@HuntonAK.com.*