A Pandora's Box of Cyberrisks

by Joshua Gold

In the last decade, the world has become a very small place when it comes to the ability of thieves to reach out and grab your property. In large measure, this is the result of breathtaking innovation in computer connectivity. While 21st century innovations have brought about great advancements in communication and real-time business decision-making, this cutting-edge tech has also opened a Pandora's box for new avenues of theft.

Recently, for example, the city of Atlanta was extorted by ransomware criminals who demanded bitcoin in exchange for returning computer functionality to the city's computer systems. A foreign government suffered an $81 million computer-enabled bank theft of an account held in New York considered to be hatched out of Asia. We have also seen countless computer extortion plots launched from Europe and Asia threaten U.S. businesses. And money is not the only target. Shippers, retailers and others have had their cargo and merchandise stolen by international thieves through cyber scams in warehouses, ports, and on the high seas.

It is also no longer enough for an organization to secure its computer systems and train its employees to practice safe computing. A substantial number of organizations have entrusted both data and access to their systems to third parties, including vendors, cloud platforms and countless others, which introduce new vulnerabilities. Security audits, smart contracting and careful decision-making about what data and access to entrust to others can go a long way to safeguarding sensitive data.

In addition, statutory frameworks are coming online in the European Union and in various states here in the United States that, in large measure, aim to place responsibility for the theft of stolen information on the target organization of the theft. The EU's General Data Protection Regulation (GDPR) and New York's Part 500 are two of the latest regulations that can subject theft victims to additional losses, including the GDPR's infamous fine of the greater of €20 million or 4% of worldwide turnover. Thus, strengthening defenses can not only protect property you own or have entrusted to you, but it can also greatly reduce the amount of third-party litigation you face.

If you manage risk for a public company, you are also undoubtedly aware of the SEC's proactivity in this arena, where investigations, fines and other claims are a distinct possibility for an entity that lost sensitive information to cyber theft. Accordingly, there is an expectation (and sound risk management demands) that organizations proactively address cyber theft from the most senior management ranks on down. The risk cannot simply be delegated to the IT department for handling.

CYBER INSURANCE CONSIDERATIONS

In a global world, insurance coverage needs to follow suit. Make sure that insurance policy territorial limits clauses indicate that first and third-party insurance products are worldwide (where applicable) and that you have coverage for claims where the security incident takes place on a third-party's servers or devices.

It is also important to read the fine print. For the past few years, policyholders and insurance brokers have watched an array of cyber-related exclusions creep into their property and liability insurance policies. Sometimes these cyber provisions are exclusions dressed-up in other clothing, such as sub-limit

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

June 2018

clauses that may offer insufficient protection against theft losses or claims enabled by cyber-related perils. Do your best to resist the imposition of cyber exclusions in your property, liability, cargo and crime insurance policies. At some point, even if a policyholder purchases state of the art cyber insurance protection, they are bound to face an argument that a gap in coverage exists somewhere in the program. The fewer, and more narrow, the cyber exclusions, the better. ■

Joshua Gold is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

June 2018