Why Cyberrisk is Not Just an IT Issue, But a Legal One Too

Christopher M. Brubaker

2015-03-11

Cyberrisk is a conundrum. While sharing characteristics with a wide variety of risks, it is unique in the way these characteristics mesh to form something that is difficult, if not impossible, to truly define or quantify. Consider some of the more common types of cyberrisk for which insurance coverage is available: physical damage to hardware; breach response costs; third-party liability; misuse of social media; and cyberextortion, to name a few. These coverages share characteristics with traditional property, liability, crime and directors' and officers' policies. Cyberrisk is a multidimensional threat with no surefire defenses. Firewalls and antivirus software just aren't enough anymore when it comes to cybersecurity. Whether you are looking at what is at risk, what the threats are, what the defenses are, or what your legal obligations are, there are no simple answers.

There are two main reasons for the complexity surrounding cyberrisk: the ubiquitous nature of computers in today's society, and people. In the last 40 years, we have gone from personal computers being unheard of to handheld devices that can do more than machines that used to fill a room. There are now more devices connected to the Internet than there are people on the planet, according to Cisco. Estimates from Morgan Stanley put the number of devices that will be connected to the Internet by 2020 at 75 billion (more than 10 for each person currently on the planet). Each device represents a potential access point, and thus a security threat.

This brings us to the human element. Connectivity has amazing advantages for business and productivity, but it creates the opportunity for large-scale, sophisticated criminal networks and hostile governments to attack your systems for profit, information and ideology. Not to mention the classic disruptive or mischievous hack by small groups or individuals. People are actively probing and attacking computer networks and monitoring and surveilling your employees, looking for vulnerabilities to exploit. Stolen or lost devices and credentials are a leading means of unauthorized access. Your employees, no matter how well trained, will make mistakes. Phishing email attacks have success rates of up to 45 percent, according to Google, and all it takes is one click for malware to download. Publishing information to the wrong website or system is another potentially costly, and common, mistake.

Now, perhaps more than ever, the adage that no computer system is truly secure needs to be a guiding mantra in dealing with cyberrisk. This brings us to the main premise of this article: Cyberrisk is just as much a legal issue as it is an IT issue. Given the prevailing consensus that the best way to address cyberrisk is through an integrated risk-management approach, you could even argue that it is more of a legal issue than a technical one. This is not to diminish the importance of the technical side, but to emphasize the importance of a global or holistic view to cyberrisk in your company. Determining the best approach for your company must be made with a full understanding of the legal and risk

consequences that come with the chosen technical approach. Ideally, cyberrisk will be dealt with in a manner that brings together the technical, business and legal areas of your company.

The first major legal issue is compliance. It is imperative to know if your company is subject to, or potentially subject to, any statutory or regulatory requirements that mandate a minimum level of cybersecurity, or if you maintain data that would subject you to breach notification laws. Are you a health care provider or financial institution, or do you do business with a company or individual that is? Do you do business with state or federal governments? Do you maintain personal information that would subject you to breach notification laws? Answering "yes" to any of the above means you are at least potentially subject to minimum security standards. But determining the correct answers is no easy task.

There are currently 51 different breach notification laws at the state and territorial level with differing definitions of "personal information," thresholds for notification, and requirements in event of a breach. You may also be subject to private standards, such as the payment card industry standards, or obligations imposed by contract. While regulatory compliance is no panacea against a breach, it does correlate to reduced costs in the event of a breach.

According to a report by the Ponemon Institute, the average cost of a data breach is $201 per impacted record, which can be lowered by as much as $27 when a company has a designated individual in charge of responding to a breach and a response plan in place prior to the breach. Having an appropriate response plan requires knowing the statutory and regulatory requirements that you are subject to or potentially subject to in the event of a breach. It also means staying on top of regulatory enforcement initiatives such as the Federal Trade Commission's practice of regulating cybersecurity in the context of unfair and deceptive trade practices, which is currently under review by the U.S. Court of Appeals for the Third Circuit in Federal Trade Commission v. Wyndham Worldwide, No. 14-3514.

Along with identifying your legal obligations, it is necessary to inventory the company's cyberassets. This involves understanding your computer systems, the data contained on them, how the data and systems are utilized and accessed, the potential risks in terms of unauthorized access and loss of functionality, and the potential liabilities. The assessment of potential liabilities overlaps with regulatory compliance but also entails a review of potential third-party liabilities and even shareholder derivative suits. This includes keeping up with the latest developments in case law dealing with breaches, as well as the coverage disputes regarding what types of losses are and are not covered by different types of insurance.

The next step is gathering information on protective measures, including the costs. While much of this will necessarily involve technical aspects, such as how the system is structured, accessed and monitored, it also should include a thorough review of available insurance coverage. Ideally, this will involve a legal analysis of the coverage already in place and additional coverage available. As noted, there are a wide variety of cyberspecific

coverages available, which sometimes may overlap with existing coverages, but this is by no means guaranteed. You also want to be sure you are looking at all potential exposures, from business interruption to cyberextortion, and not simply focusing on potential third-party liability.

Once this is complete, it is time to perform a cost-benefit analysis and select the appropriate combination of security techniques and insurance coverage for your company. This process will be greatly enhanced by having a legal perspective on how everything will fit together, and ensuring the choices made will satisfy your legal requirements and risk appetite. Finally, there is implementation and monitoring. Having a lawyer involved is obviously essential with respect to regulatory compliance issues when implementing the plan, but it is also important to keep an eye on the ever-changing legal landscape. It is imperative to monitor both legislative and regulatory changes. It is also important to keep an eye on the courts, as the myriad lawsuits related to large breaches continue to define both the scope of liability and the insurance coverage available in the event of a breach.

The legal nature of cyberrisk extends beyond regulatory compliance to touch upon every aspect of an integrated risk-management approach to cybersecurity. You should think about it as a legal issue with a large technical component, rather than a technical issue with legal ramifications.

Christopher M. Brubaker is an associate in Clark Hill's insurance and reinsurance practice group and concentrates his practice in commercial litigation, including appellate work. He also advises companies on regulatory matters involving insurance and environmental laws, rules and regulations. He can be reached at cbrubaker@clarkhill.com.