Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Role Of Insurance In A Cyber Risk Management Strategy

By **James E. Scheuermann**
July 14, 2017, 11:34 AM EDT

James E. Scheuermann

Property insurance for commercial operations universally includes coverage for fire losses. But no CEO or risk manager thinks that fire insurance encompasses the whole of prudent risk management for fire. No prudent warehouse owner would operate a warehouse without some type of fire control devices or alarms. No reasonable safety officer in an office tower thinks that fire insurance is a good substitute for evacuation plans. And, fortunately, it is equally rare for corporate insureds to treat cyber insurance as the whole of their cyber risk management plans. But many insureds make a closely related, and potentially equally serious, mistake — they treat cyber insurance as a distinct and independent silo, not an integrated part of a comprehensive cyber risk management strategy.

Effective risk management requires coordinated strategic action on many fronts. For any known risk that presents itself to a corporation, the responsible decision makers need to decide whether the risk in particular is to be avoided, accepted, mitigated or transferred.[1] With few exceptions, the risk manager is not in a position to decide entirely on her own, with respect to any particular cyber risk, which of these four options is most cost-beneficial and risk-beneficial for the company. Her function focuses on risk transference, and even as to that only through insurance policies and not also through other vehicles (e.g., indemnification clauses in vendor contracts). Effective management of cyber risk typically involves, then, a dialogue among the CEO, other responsible corporate executives and the risk manager, at a minimum.

The decision whether a risk is to be avoided, accepted, mitigated or transferred is the end-product of a deliberative process, not the beginning. For cyber risk, this is the space in which business objectives and judgment loom large, where risks are identified and assessed, where subject matter expertise from the CEO, CIO and CISO, CFO, the GC and the risk manager must be considered, and where cost-benefit and cost-risk analyses come into play.

That deliberative process is far more likely to reach reasoned and desired outcomes when the risk manager is at the table and actively engaged in the discussions. If the CISO advises that a specific cyber risk cannot be entirely avoided as a technical matter, for example, and if the CEO declares that commercial constraints prevent it from being transferred to vendors, customers or business partners, then risk transfer through cyber insurance may be the preferred vehicle for the management of that risk, if that vehicle is available. If cyber insurance is not available, in-house mitigation strategies may

need to be developed. Because financial resources are never infinite, whether some portion of the cyber risk management budget would be better spent by the IT department, or by the risk manager's purchase of additional cyber insurance limits, can only be answered by a vetting and common understanding of the company's cyber risks and technical and insurance tools available to manage them.

One of the risk manager's tasks in that pre-incident dialogue is to educate her colleagues on both the scope of cyber insurance coverage and its limitations so that the management team knows what cyber risks it can transfer to insurers and those risks whose management requires other solutions. Cyber insurance covers many cyber risks, and it usually is negotiable to cover more than the insurer initially offers, but it doesn't cover all cyber risks. Consider the following examples:

- Most cyber insurance policies do not cover bodily injury or property damage caused directly by a cyber event. When the responsible officers know that the company bears that risk uncovered, alternative risk management strategies can be implemented.

- Virtually all cyber insurance policies provide coverage for the costs of notification to third parties (usually consumers or healthcare patients) whose personal information has been stolen. Some of these policies limit the notification coverage to a specified number of people. The insurer will not cover the notification costs to individuals beyond that defined universe. Does the company need an excess policy to cover that risk or can it negotiate a number sufficiently large, at a premium it can afford, to address that risk?

- Most, but not all, cyber policies provide business interruption coverage for lost profits and ongoing expenses following a cybersecurity event that disrupts the company's computer systems' operations. For purposes of calculating covered business interruption losses, some cyber policies limit the period of restoration of the computer systems to normal operation after a cybersecurity incident to 30 or 60 days. While that limitation often can be negotiated to a longer period, unless the CIO and the risk manager are communicating with each other on the CIO's best estimate of how long it will take to be back to normal operations after a data breach, a ransomware attack, an infection by malware or a virus, or a denial of service attack, the risk manager is forced to guess at the right number of days.

- Many cyber policies contain subrogation clauses that provide that the insured will not do anything to impair the insurer's subrogation rights against third parties. The risk manager is uniquely positioned to raise the question whether the indemnification provisions in vendor and customer contracts have been drafted such that they may defeat the cyber insurer's subrogation rights, and thus create a defense to coverage by the insurer.

The consideration of the principal legal consequences that may result from a data breach of personally identifiable information or personal health information also illuminates the need to make the risk manager an integral part of the company's cyber risk management team. These legal consequences include:

- notification obligations to affected individuals
- regulatory investigations and information requests
- regulatory fines or penalties
- Payment Card Industry ("PCI") fines or assessments
- preservation of evidence
- dealings with law enforcement (the FBI, DOJ)

- disputes and/or litigation with:
- business partners (e.g., joint venture partners, joint IP development partners)
- vendors
- customers
- consumer class actions

Each of these consequences likely will implicate the company's cyber insurance. How the GC handles them may bolster the insurance claim or seriously undermine it. The GC's favorite law firm may not be on the cyber insurer's list of panel counsel. The company's breach response plan may have provisions for the conduct of a forensic investigation that is not sufficiently attentive to the insurer's contractual right to be part of that investigation or even to conduct that investigation through its hand-picked vendor. Moreover, the inadvertent destruction of evidence in that forensic investigation may create defenses to coverage (e.g., the "hostile action" defense or causation defenses) that otherwise would not exist.

In addition to these legal consequences, consider the adverse business consequences of a data breach, ransomware attack or other cybersecurity incident. To identify just a few, these exposures include:

- loss of profits arising out of business interruption
- the additional expenses to mitigate such loss of profits
- damage to data, software, computers, and other tangible property
- the loss of goodwill and brand reputation

Again, each of these adverse consequences is packed with cyber insurance implications. Some of these effects are likely to be covered in whole or in part (depending on policy retentions, limits and sublimits or applicable time limitations) and some may not be covered at all. The CEO and her financial team would benefit from knowing, before a cybersecurity incident, how much and what types of business risk the company has transferred to its carriers or third parties, how much it has retained, and how it is managing the retained risk through other methods. Equally, the risk manager needs to know the answers to these questions to advise her colleagues and the board on the adequacy of the company's cyber coverage. Cyber insurance limits in the tens of millions of dollars may be more than sufficient or far from adequate, depending on a number of factors.

Cyber insurance is a critical part of a proactive, comprehensive and integrated corporate strategy of cyber risk management. The terms of cyber policies are negotiable, which is especially good news since "off-the-shelf" cyber policies often have coverages that an insured does not need or lack coverages that may be critical to the risks faced by a discrete subset of corporate insureds. A risk management dialogue among the responsible executive management, including the risk manager, to decide which risks to transfer through cyber insurance, and in what amounts, and which risks the company can and will manage by other means, promises to lead to better, cost-effective outcomes both prior to and after a cybersecurity event.

James E. Scheuermann is a partner of K&L Gates LLP, where he represents policyholders in insurance coverage matters.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 at 5 (Feb. 12, 2014), available at www.nist.gov/sites/default