Cyber Risk: The Least You Need to Know

Directors of organizations in all sectors need to continue to improve cyber-risk oversight. The following five cyber-related issues should be on the public company board's agenda in 2016.

1. **Humans are the new network perimeter.** Organizations are only as strong as their weakest link, which is why cyber preparedness must permeate the entire work force from the top down. Resources must be allocated to constantly look for vulnerabilities, test the environment, train personnel, and ensure that there is a documented and practiced plan to follow should a breach occur.

2. **The Internet of Things creates more points of entry.** There are upwards of 5 billion networked objects and devices now being used, dramatically increasing the attack surface. Adversaries will continue to exploit the influx of connected devices to steal credentials and passwords to access financial and business accounts.

3. **Ransomware threats.** These attacks start with an employee opening a malicious link that then encrypts all company files. The attackers then request a ransom for the return of files, with the threat of deletion if the ransom is not paid. Ransomware stands to be a rapidly growing issue in 2016, especially since these programs are readily available on the Dark Web, a segment of the Internet that has acquired a notorious reputation for criminal behavior, as users are able to operate in total anonymity.

4. **The threat from within is real.** The theft of internal records and crown jewels, like patents or merger activity plans, is forcing the need to manage and protect all perimeters. The adequacy of the response to insider threats must be commensurate with the level of advanced preparation. Policies need to be established, procedures tightened, employees thoroughly trained, and remediation plans carefully laid out ahead of time. Compliance, however, does not equal security. Employees need to be continually re-educated and data security reinforced with monitoring, threat detection, and effective systems and procedures. Budgets and skill gaps should not deal the bad guys a winning hand.

5. **More federal regulations.** In December, President Obama signed the Cybersecurity Information Sharing Act into law. The new legislation offers legal protections to companies that share cyber-threat information with the government. That same month, the Cybersecurity Disclosure Act of 2015 was introduced in the Senate. This bill would require companies to disclose in their SEC filings whether they have a director who is a "cybersecurity expert" and, if not, what cybersecurity steps the company has taken. This effectively elevates cybersecurity from a board-level discussion to a key priority in 2016. —*Jeremy Kroll*

Got the Policy. Now What?

Directors are being found liable for cyber-systems failures. While not advantaged in designing cybersecurity systems, directors are fully competent to ensure the existence of proper insurance to protect their companies' financial assets. Here is a checklist of key insurance considerations to review and use to protect your company, your board, and yourself from the adverse financial consequences of a cybersecurity failure.

1. **Has your company asked its vendors to include it as an additional insured on its vendors' policies?** The increasingly common practice of outsourcing data handling, processing, and storage functions to third-party "cloud" providers and other vendors is one significant source of cyber risk. An effort should be made to shift these risks back to the vendor by including a broad form of vendor indemnity agreement and requiring the organization to be named as an additional insured on the vendor's cyber policy.

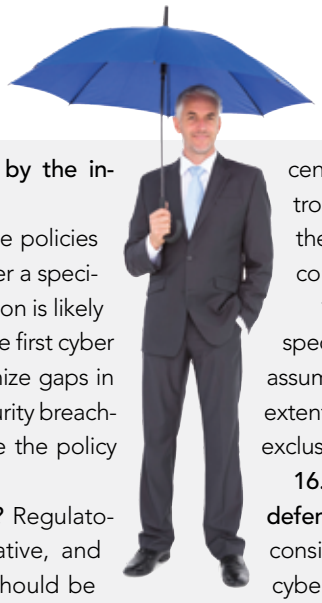
2. **Does the vendor's policy pay first?** To maximize any additional insured coverage, the insurance specifications and the vendor's policy itself should prescribe that the coverage afforded for the additional insured is "primary" insurance.

3. **What is the coverage territory?** Data, including personally identifiable information (PII), knows no boundaries. To avoid potential coverage gaps in additional insured coverage, the vendor's policy may need to include a coverage territory that is worldwide.

4. **What are the deductibles/self-insured retentions, and who can satisfy them?** To maximize its additional insured coverage under the vendor's policy, the insurance specifications and the vendor's policy should prescribe that no deductible or retention applies to the additional insured's coverage.

5. **What types of losses are covered (e.g., liability, property damage, computer damage, business interruption)?** Cyber coverage may extend to losses that include costs for the defense of lawsuits brought by customers; credit monitoring, call centers, public relations efforts, forensics, and crisis management; regulatory investigations; misappropriation of intellectual property; post-breach remediation costs, including notification requirements; receipt or transmission of malicious code; the restoration or recovery of data that is lost or damaged; and extortion demands.

6. **What are the policy limits and sublimits for particular types of losses?** In addition to total policy limits, sublimits that may be imposed for certain covered costs should be carefully assessed.



7. Does coverage extend to losses caused by the insured's third-party vendors?

8. Is there a retroactive date? Cyber insurance policies typically limit coverage to breaches that occur after a specified "retroactive date." The date of policy inception is likely to be the retroactive date the insurer selects for the first cyber policy it issues to a particular company. To minimize gaps in coverage, "retroactive" coverage for network security breaches that occurred but were not discovered before the policy inception should be requested.

9. Is there coverage for fines and penalties? Regulatory coverage, which extends to civil, administrative, and regulatory investigations, fines, and penalties, should be requested. The $25 million penalty that the Federal Communications Commission (FCC) levied against AT&T in April 2015 following a data breach exposing the PII of 280,000 of its customers is just one example of how costly data-breach-related fines and penalties can be.

10. Is there an "acts of foreign governments" exclusion? Off-the-shelf cyber policies often contain exclusions for terrorism, hostilities, and claims arising from "acts of foreign enemies." Such exclusions should be eliminated or limited to ensure that the insurer cannot deny coverage where a cyberattack or breach originates in a foreign country.

11. Is there an exclusion covering programming or processing errors, mechanical failures, and the like? Cyber policies commonly exclude coverage for losses caused by mechanical or electrical failures and breakdowns. Mechanical failures can be caused by hackers who, for example, launch spam attacks or a virus that overloads or shuts down a system. To avoid gaps in coverage, policyholders should request an exception that provides coverage for mechanical/electrical failures that are intentionally caused by hackers.

12. Is there an exclusion for any loss caused by an employee? This sort of exclusion should be eliminated during the policy negotiation process to avoid disputes. Companies' own negligence often contributes to data-breach losses.

13. Is there an exclusion for an insured's failure to follow minimum required practices? A number of forms contain exclusions that seek to eliminate coverage when the policyholder fails to follow specified minimum practices.

14. Is there a "portable devices" exclusion? Some cyber insurers are including a so-called "laptop exclusion." A surprisingly high percentage of data breaches have been traced to portable electronic devices. Some of these insurers will agree to remove the exclusion provided the insured agrees to encrypt all data contained on its portable devices.

15. Is there a contractual liability exclusion? Subject to any specified exceptions, this exclusion typically applies to liability assumed by an insured under a contract or agreement. To the extent a third-party claim can be styled as breach of contract, this exclusion may come into play.

16. What are the provisions regarding the selection of defense counsel? Choice of counsel is likely to be a critical consideration in the event your company suffers a significant cyberattack. While cyber insurers frequently have the right to select defense counsel or require the insured to choose from a preapproved list of "panel counsel," it is often possible to negotiate a provision entitling the insured to select counsel subject to the insurer's approval.

17. Is there a specific breach coach or notification company that the policyholder desires to use in the event of a breach? Negotiate for specific vendors before buying the policy. If you want to use a particular breach coach or notification company, insurer approval should be obtained before coverage is placed.

18. Does the policy contain a provision that shifts the costs of settlement to the insured if it declines to settle a case when the insurer wants to? Off-the-shelf cyber policies often contain "hammer" clauses that require the insured's approval prior to settling a claim for a specific amount, but which shift some or all future defense and settlement costs to the insured if it does not consent to the settlement.

19. Does the policy say that the carrier has a right to recoup defense costs under certain circumstances? As a limitation on recoupment rights, most insurers will agree to "final adjudication" wording that specifies a final and non-appealable determination that such acts were committed before recoupment can be sought.

20. What are the policy's terms and conditions regarding dispute resolution? Off-the-shelf cyber policies frequently contain mandatory alternative dispute resolution provisions, requiring arbitration in lieu of litigation or a combination of mediation followed by arbitration. Insurers will often agree to modify such provisions to allow the policyholder to choose the type of ADR process.

This checklist will allow you to ensure that you are protecting your company, your board, and yourself from adverse financial impact should a breach occur. —*Allan Grafman* and *Helen K. Michael*

THINKSTOCK BY GETTY IMAGES