Cyber-risks and insurance

The digital world continues to rapidly evolve, and our increased reliance on the internet and technology goes hand-in-hand with more frequent, sophisticated and professional cybercrimes. Instead of wondering if your business is a target, you now need to evaluate how and when you will become a target. By evaluating individual risk management, you can craft a cyberinsurance policy to meet and protect the unique needs of your business.

Five key questions that companies should ask themselves as cyberthreats continue to evolve:

1. **Do we have regular reporting to and representation among our top operating committees and the board of directors, to ensure a clear understanding of our current risk profile and strategy?**
2. **Do we monitor the cyber-risk landscape effectively as risks evolve?**
3. **Are we involving third-party experts enough (as opposed to in-house) to ensure adequate risk migration?**
4. **Do we have specific cyberinsurance coverage for our needs in the event of a claim?**
5. **Have we reviewed our insurance policies to understand how they might apply to a potential cyberincident?**

What then, are the types of exposures you can insure with a tailored cyberpolicy?

It is difficult to review coverage here in a comprehensive way, however, the span of this coverage may include:

- Third-party loss resulting from a security or data breach
- Direct first-party costs resulting from a breach
- Loss of income and operating expenses resulting from a security or data breach
- Threats to disclose data or attack a system to extort money

Risk mitigation

Risk mitigation can take many forms. The most effective is to invest in defenses for the attack modes and assets that are most at risk. For example, if you determine that your greatest threat is malware installations to point-of-sale software systems directed by domestic operatives via vendor access rights, then you might consider investments in end-to-end encryption, Application White Listing (AWL), File Integrity Monitoring (FIM), system access software, vendor access controls and regular reviews of all vendor access logs.

While investing in prevention is paramount, not all attacks can be fully mitigated. For these events, cyberinsurance is critically important. Cyberinsurance provides contingent capital and expert assistance in the event of a cyberattack or data breach.

The insurance industry has tailored a suite of products that help companies quickly restore their operations and pay financial obligations. Some cyberpolicies also include risk management and loss prevention services which can aid companies in assessing and mitigating their exposure to events before they occur.

A cyberpolicy can additionally respond to both the liability, as well as the first-party direct costs associated with a cyberevent. Some examples of first-party costs include forensic expenses, notification costs, credit or identity monitoring and loss of income from a network interruption. From a liability perspective, a cyberpolicy may also respond to regulatory and administrative actions, including fines and penalties arising out of the event. As with all policies, a cyberpolicy can be customized and coverage offerings can be added or removed based on the company's risk profile. Increasingly, we continue to help you by reviewing your other insurance purchases to ensure that you understand where there may be potential coverage gaps.

Loss scenarios

The following loss scenarios from an industry publication help us better understand a few of the areas a business may be vulnerable. Loss scenarios are for illustrative purposes only. Whether or not, or to what extent, a particular loss is covered depends on the facts and circumstances of the loss and the terms, conditions and endorsements of the policy as issued.

Take a look at these two claims situations a carrier recently shared:

Laptop stolen from exec's car results in invasion of privacy

Cause of action: negligence, invasion of privacy
Type of organization: energy firm
Number of employees: 100
Annual revenue: approximately $20 million

The event
An energy company executive's laptop was stolen from a corporate vehicle. The laptop contained significant private customer and employee information. Although the file was encrypted, the overall password protection on the laptop was weak and the PIN for accessing the encrypted information was compromised.

Resolution
After assessing the nature of the information on the laptop with a forensic expert and outside compliance counsel at a cost of $50,000, the energy company voluntarily notified relevant customers and employees and afforded a call center, monitoring and restoration services, as appropriate. While the additional first-party cost was $100,000, the energy company also incurred $75,000 in expenses responding to a multi-state regulatory investigation. Ultimately, the company was fined $100,000 for deviating from its publicly stated privacy policy.

Criminal scheme skims customers' payment card info from retailer

Cause of action: negligence, invasion of privacy
Type of organization: retailer
Number of employees: 35
Annual revenue: approximately $5 million

The event
A criminal syndicate attached skimming devices to a local retail chain's payment card systems at a variety of locations. This permitted unauthorized access to the credit and debit card information of 15,000 customers over a three-year period.

Resolution
The retail chain spent $850,000 performing forensics, engaging counsel for compliance assessment and providing notification and call center services to its customers. It also spent $900,000 reimbursing a variety of banks for costs associated with card cancellations and reissuance charges. Lastly, it spent $75,000 in defense costs responding to a regulatory inquiry and $250,000 in fines.

Cyber-risk is evolving into a complex area of insurance coverage. At KeyBank, we believe that cyber-risk should remain a priority as you continue to revise your company's practices and procedures. Please reach out to our team for help as you look at this area.

If you suspect you are a victim of fraud or malware, call **Key's Fraud and Disputes Hotline directly at 1-800-433-0124** for analysis of the situation and further direction. Then contact your Relationship Manager to make them aware of the issue.

To learn more, contact your Relationship Manager, or visit **key.com/security.**

KeyBank
Use the red key.®