Cyber risk is bigger than an IT issue

Cyber risk is bigger than an IT issue

By Sean M. Donahue, Cyber & Technology, XL Catlin

March 10, 2016

One thing is becoming clear about cyber risks: the problem is much bigger than any organization's information technology department.

My background as an IT leader and information security professional before I joined XL Catlin gives me a good vantage point on how businesses can make the mistake of thinking that cyber risk begins – and ends – with their technology operations. Regardless of a company's size and resources, IT operations play a critically important role in cybersecurity. But the total cost of cyber risk affects the entire enterprise, and a cyber incident frequently causes problems that no IT professional, however talented, can solve.

Business continuity, third-party liability, reputational damage and regulatory compliance – those are beyond the purview of IT. A well-run IT department can minimize downtime and get systems back up, which is critical. The value of data and the cost of a disruption, however, are ultimately determined by the data owners in the business operations. While a system shutdown can be catastrophic for some organizations, business interruption and data recovery insurance are available to mitigate that risk. Regulations regarding cyber security are evolving, and insurance is available to manage that uncertainty too."

The complexity of responding to a cyber incident and communicating with stakeholders are strong reasons to have a team, such as an executive control group."

But the business itself must communicate with its employees, customers, investors and perhaps regulators, after an incident. If a data breach has occurred, a forensic investigation and

notification of affected parties are likely required. A strong, unified message is critical to convey, and that is best delivered with the help of senior executives and crisis communication professionals. One of the valuable benefits of cyber insurance is access to expert resources, from PR to forensics to IT specialists, who can quickly come in to assist.

The complexity of responding to a cyber incident and communicating with stakeholders are strong reasons to have a team, such as an executive control group. The composition of such a team depends on the size of the entity and the nature of its business. In larger organizations, it likely will include enterprise risk management staff as well as C-level leaders, such as the chief technology or chief information officer. For smaller and midsize organizations, the team might include the general counsel, chief operating officer and the head of IT, for example. Regardless of the specific titles, the functions that need to come together to discuss cyber risk include risk management, operations, IT, legal, marketing and communications. Ideally, a cyber risk steering committee or group is convened to ensure that all relevant areas of the organization are represented and kept informed. The job of managing cyber risk shouldn't fall to one person, however; a cyber risk team can ensure that the entire organization understands the risk and adjusts procedures accordingly.

It's important to think about cyber insurance as similar to property or commercial general liability – as a form of protection that your organization needs to continue operating.

Midsize companies have particular challenges when it comes to cyber risk. Often they have fewer IT resources, which makes them attractive targets for cyber attacks. Statistics on cyber attacks bear this out. The 2015 Cyber Claims Study from risk assessment firm *NetDiligence* found that 71% of cyber claims came from organizations with less than $2 billion in revenue, and 56% came from those firms with less than $300 million.

Many midsize companies also have contractual requirements with bigger organizations that increase their need for high cyber insurance limits. Based on their own perceived exposure, a midsize organization might not think it needs to purchase a lot of cyber insurance coverage, but that situation can change if a business relationship requires it. The lesson here is to look closely at your business and all risks relating to your systems and networks. How long could your firm afford to remain offline, if a cyber incident disrupted your IT operations? Could your company lose revenue or customers if that happened? Would you be able to meet your obligations to business partners?

There is a lot to understanding and managing cyber risk. A team approach is a good way to cover the bases, as well as working with expert resources and strong insurance partners to help protect your business.

About the Author

Sean M. Donahue is assistant vice president and underwriter, Cyber and Technology Insurance, at XL Catlin. Before joining XL Catlin in 2014, he was an information technology professional and holds the designations of Certified Information Systems Security Professional and Certified Ethical Hacker.