Complex Risk
SYMPOSIUM·2023
JUNE 7-8 • ST. LOUIS, MO

What's Next in Cyber? 3 Important Questions

Despite the vast unknowns of cyber, Deborah Hirschorn, Managing Director of U.S. Cyber & Technology Claims at Lockton Companies, explained at this year's Symposium that markets are stabilizing and prices for excess layers are more competitive, in part because companies have better controls.

Hirschorn and Timothy Smit, Global Privacy & Cyber Risk Consulting Practice Leader at Lockton Companies, discussed how evolving technology has helped defend against cyber threats, but healthcare's abundance of data continues to be targeted. Manufacturing is also perceived as an easy target, but Hirschorn explained that personal data is her primary focus: "Privacy keeps me up at night, not so much ransomware." Because fines following breaches are often based on organizational behavior, companies such as Meta and LinkedIn, for example, have paid huge fines as a result of privacy issues. New local and national laws requiring updated protocols that are not yet clearly understood are also complicating the cyber landscape.

Smit advised that we consider the impacts. What is your business backup plan for interruptions? "What does no business for 16 weeks cost?" And what's your financial impact if you can't deliver to your supporting organizations? Business interruption can be much more costly than ransomware.

Both panelists also described how the war in Ukraine has created new threats. "Bad actors know that your weakest link are third parties. What can you control? What can your third parties control? Asking tough questions is the key to preparedness."

While the current regulatory landscape includes huge fines, final numbers are unclear because of appeals. Fines may climb to multiple millions. Also worth noting is that China has its own privacy statutes. Every organization must understand what OFAC requires.

The issue of meta pixels is a current primary focus of cyber. "If you've gone on any website and then ads related to your search appear, that's the result of meta pixels." It's the tracking of your data for targeted advertising. Medical conditions are an especially sensitive issue and may be actionable. Hirschorn explained that the actionability of meta pixels emerged from last year's Dobbs v. Jackson decision overturning Roe v. Wade, creating concerns about the legal ramifications of searching for abortion data online. More lawsuits are settling and being dismissed because consumers have the ability to control cookies that share data. Courts have ruled that because consumers can turn off or choose sharing, companies aren't liable.

Unfortunately, however, ransomware claims are on the rise again. Ransomware organizations are increasingly agile in staying off the OFAC list, and the emergence of small new subgroups makes it difficult to understand the current threats.

Smit pointed out that virtually every organization has been compromised. According to Smit, if we think our organization hasn't been hit, we're just not aware that is has.

Bad actors exploit vulnerability by blocking response efforts. Smit suggested that every organization needs to ask questions about its data: What information is regulatory? What are the classifications? Where does that data go? What external organizations have access to our data? How do you contractually indemnify your organization and third parties?

Most importantly, Smit cited 23 recent cyber claims where organizations were compromised because they had no data map. Having a data map is critical to protecting your organization.

Smit then explained the importance of having a Breach Coach, an external law firm on your insurance. The first phone call after an incident should not be to a third-party advisor. The first call after an incident should be to your Breach Coach/Counsel. The Breach Coach then contacts forensics and authorities.

Hirschorn described the Breach Coach as the quarterback of your response team. She also recommended that all stakeholders have hard copies of response information and advised against having that information on a computer. Smit built on Hirschorn's quarterback analogy with calling 911: A Breach Coach is the emergency response contact who will then contact all necessary players.

Smit described the usefulness of tabletop exercises to prepare for a breach. Such exercises can help identify areas of weakness and vulnerability but must be updated regularly. HR, PR, and Marketing also need to be involved because cyber threat is a far larger issue than just IT. Hirschorn advocated that a forensic accountant should be part of your First Response Team as well as a financial decision-maker.

Consider the business risks for each department. What is the root cause of the risk? Often it's human error. Also consider your third-party risks. Organizations and vendors need to make sure their data is mutually protected. Ensure that the data you are focused on is within the scope of protection.

Hirschorn warned of allowing IT to take over cyber issues. "Just as you shouldn't let people grade their own homework, it's probably not wise to let IT make all the decisions about cyber security."

Hirschorn had one final thought regarding AI, in that organizations are collecting, sorting and storing data that you may not have given consent for. Think of using AI as giving your information to a third party vendor. Do you trust how it's being used? "Just something to think about."

If your organization suffers a cyber incident, how will you:

1. Identify abnormal activity?
2. Contain abnormal activity?
3. Respond appropriately and quickly to your breach coach?