Q&A

Mitigating Cybersecurity Risk

A Q&A With Raj Chaudhary and Dave McKnight of Crowe

Smart decisions. Lasting value.™

As cybersecurity threats occur more frequently, a growing number of companies are shifting their emphasis from trying to prevent every outside threat to protecting their most important assets and planning effective responses to emerging cyber incidents.

To understand how companies are engaging senior leadership, business units, and board members so they better understand their cyber threats, Financial Executives International (FEI) spoke with Raj Chaudhary, a principal in the Crowe Risk Consulting group and leader of the firm's cybersecurity solutions group, and Dave McKnight, a Crowe senior manager.

FEI: In general terms, what does the cybersecurity landscape look like today?

RAJ CHAUDHARY: The threat landscape is constantly changing, and the hacker community is much more organized than the corporate world when it comes to cybersecurity. Corporations are having a tough time keeping up with the ploys used by hackers.

For instance, 2016 was the year of "ransomware," and this threat continues to accelerate in 2017. Awareness is increasing, but people remain the weakest link in the trio of people, process, and technology.

DAVE MCKNIGHT: Attacks are happening more often, and perpetrators are finding new and different ways to compromise corporations. Attacks also are occurring at a faster pace and typically are executed through the easiest ways into a company's network. We have seen many examples of this due to the IoT (Internet of Things) trend, where simple devices, with potentially untested security controls, are being plugged into the internet. Perpetrators are using these easy-to-access devices to perform large-scale denial of service attacks and as a foothold to ultimately hold companies' networks or data for ransom, causing financial loss or unwanted publicity. Companies must be ready to respond rapidly.

FEI: Given the threat environment, are you seeing changes in how companies think about cybersecurity?

RAJ CHAUDHARY: Cyber is getting a lot of attention at both the management and board levels, and cyber is becoming a standard topic at board meetings. Companies realize that in the interconnected cyber world, they can do only so much to protect their perimeters. As the saying goes, it is not a matter of if but when a company will be subject to a cyber incident, and companies are shifting their focus to be better prepared to handle an incident and to minimize risks and losses.

DAVE MCKNIGHT: Organizations are now starting to recognize the necessity and value of knowing what information types they have and where each type is located within their walls and networks. By taking a new, or re-emphasized, look at information amounts and classifications, an organization can thoughtfully evaluate risk and calculate the most appropriate measures to protect the information. We're also seeing a rejuvenation of risk management and compliance to make sure companies are meeting their regulatory obligations.

FEI: How are companies addressing cyber risks at the board or management level?

RAJ CHAUDHARY: Generally speaking, there are three types of company management and boards. The first – and most mature – type requires frequent updates on the state of cybersecurity, and company boards and management hold special educational sessions at their periodic meetings to understand the company's risks and preparations. This type of company is more proactive and better capable of handling incidents, so its risk is lower.

The second type doesn't have updates as frequently but, as it sees its competitors being subject to incidents, recognizes a need to get more serious about cyber risk and to mature quickly.

The third type of company is still living in the Dark Ages and believes – incorrectly – it is not affected by cyber risks. This type of company actually is at the highest risk and, unfortunately, will be forced to wake up soon. Management tends to move toward maturity once companies have had a breach.

DAVE MCKNIGHT: The compliance and risk management functions usually have perspectives that are a few steps removed from front-line leadership, so they can look more at the broad picture and ask, "Do we really have an appropriate interpretation of our cybersecurity risks, and, as we report to either the board or a committee, has the organization employed the appropriate solutions to control or reduce risk?"

I don't see a lot of that yet, but it's starting to come together, particularly for large financial services companies. It's back to the basics in the sense that companies realize they need to know exactly where things are before they can start protecting themselves and determining how to refine the protections or detection methods already in place.

Cybersecurity is now recognized as not just an IT problem; it is being talked about in terms of being an overall business problem as well. Conversations are occurring on the boards, the committees, and the executive leadership teams of organizations.

FEI: Are you seeing that emphasis more in some industries than in others?

DAVE MCKNIGHT: I think it absolutely applies across the board, but the prioritization may be different. If a company is more consumer-focused, it may be more concerned with making sure it can continue interacting with customers and taking orders. Its regulations may be a little more relaxed or nonexistent – certainly not like in banking.

Healthcare is a little different. Those companies have regulations such as HIPAA (Health Insurance Portability and Accountability Act) and the different tech-related components of protecting information. Many of these regulations are newer than most in other industries. Depending on how much companies are required to do, that can affect the prioritization of their focus on cyber risk.

FEI: As companies recognize they need to do more on security, what are the typical weaknesses they tend to address first?

RAJ CHAUDHARY: Not having a baseline on the current state of security is the biggest weakness. If a company does not have a current gap summary, it does not have a road map for implementing the appropriate controls, and it cannot differentiate between the forest and the trees in relation to risks.

DAVE MCKNIGHT: With many companies, the folks on the front lines, who interact with customers or nonemployees the most, are sluggish when it comes to identifying what might be a security event that is worth talking about with management.

The biggest conduit of cyberattacks continues to be phishing and spear-phishing attacks that come through emails. But employees still are not identifying bad emails or suspicious emails directly and quickly. Many people – even executives – still aren't recognizing that these types of attack emails are exactly that. They're going through with clicking the link, running a file, or unsuspectingly providing the requested information.

While end users make up the broader targets of perpetrators, there's another component that must be considered: Management and the executive teams also need training to make sure they're asking the right questions and prioritizing the right kinds of initiatives within information technology and information security.

FEI: Given that most businesspeople or directors don't have a cyber/IT background, what are companies doing to help get them up to speed or understand the risk more effectively?

RAJ CHAUDHARY: Because a shortage of cyber talent exists in the marketplace, a lot of companies are retaining consultants for ongoing implementation of tools or technologies and are creating cross-functional teams that include marketing, communications, legal, IT, and external consultants.

DAVE MCKNIGHT: One of the things we're emphasizing is evaluating and selecting an available cybersecurity framework. I think the easiest one to talk about is the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), which has been around for a number of years. Companies have latched onto certain requirements and have used those as a successful foundation to build upon.

Along with whichever framework a company picks, there will be related terminology that everyone must become familiar with. In speaking about cybersecurity, the meaning of an attack, a breach, or an incident can vary for different individuals. In addition to picking a single framework to get all members of an organization on the same page, the company should pair that with a nomenclature that works for the organization so everyone within the company knows what various terms mean.

FEI: What kinds of tools are companies evaluating to help address their cyber exposures?

DAVE MCKNIGHT: Solutions exist to help expedite or make companies more efficient at either detecting or proactively identifying potential trends so IT or information security folks can make the proper infrastructure changes. For example, they might block certain known activity on the firewall so it never comes in, or they might change spam filters.

Newer solutions out now automate tasks that historically have been very manual. Machine learning also is starting to come into play, which is a little more advanced because it's taking into account different kinds of data feeds, processing them, and coming up with possible outcomes or scenarios, and it's helping expedite decision making and adaptability within an organization's security posture. And new solutions in the security intelligence field, for example, are pairing machine learning with security intelligence as well as analytics. They're pulling a lot of material to provide crisp outputs that tell organizations what they should be doing in order to prevent certain problems.

Depending on the solution or need a company has, there's an avenue to get some quick results and long-term strategic footholds as well. A lot of smaller organizations, regardless of the industry, recognize a need and create a response plan but realize they don't necessarily have the talent or the skill set should that plan need to be enacted, so, for example, many are using third parties.

Time will tell how the newer solutions resonate within organizations. I think another important success factor for organizations is choosing the correct integration opportunities connecting these new technology hooks into what organizations already have. Rather than dropping and replacing everything, companies should attempt to integrate newer solutions with existing tools and processes that these organizations already have. It's an interesting field that's still very much in development.

Crowe recently completed a report in collaboration with the Internal Audit Foundation showing the majority of organizations surveyed are integrating proactive measures or tools into their cybersecurity efforts.

Crowe

Learn more

Dave McKnight
Cybersecurity Risk Consulting
+1 630 575 4399
dave.mcknight@crowe.com

This Q&A discussion originally appeared on FinancialExecutives.org in August 2017. ©2017. Reprinted by permission.

crowe.com

Text created in and current as of April 2017; Cover and artwork updated in May 2018.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.