May 12, 2017

Cybersecurity consciousness in the C-suite

by Greg Masters, Managing Editor

Enterprises are better protected from repercussions of a breach with a board that's knowledgeable about security and which makes sure a comprehensive set of security policies are in place, reports Greg Masters.

With cybercriminal risk at an all-time high across the globe, it's only inevitable that your company will be targeted, experts say. But, they add, the manner in which a company prepares for a cyberattack is what separates winners and losers. The biggest differentiator is engagement by the board in cybersecurity matters and the adoption of best practices in IT departments.

OUR EXPERTS

Wils Bell, cybersecurity recruiter

Joyce Brocaglia, CEO, Alta Associates; founder, Executive Women's Forum

Domini Clark, principal, Blackmere Consulting; director of strategy, InfoSec Connect

Gary Clayton, shareholder in the workplace privacy and data security practice, Littler Mendelson

Rajiv Gupta, CEO, Skyhigh Networks

Scott Laliberte, managing director and leader of global IT security and privacy practice, Protiviti

Michael Potters, CEO, Glenmont Group

Kimberly Verska, partner and chief information officer, Culhane Meadows

The good news is that the C-suite is, in fact, improving its posture in these vital matters, according to a Protiviti security survey, "Managing the Crown Jewels and Other Critical Data," released in February. The study found that current board engagement levels are at 33 percent, compared to 28 percent in 2015.

But, while boards are, in general, increasing their management of IT security implementations, there is still more work to be done. “While the increase in boards of directors' and company management's engagement with information security is a positive sign, it's imperative that leadership keeps closer tabs on the state of their organizations' cybersecurity programs,” says Scott Laliberte, a Protiviti managing director and leader of the firm's global IT security and privacy practice. “Particularly as new technologies are introduced and

new approaches to generating revenue are deployed, it's increasingly important to reexamine existing data security and privacy processes on a regular basis – ensuring that the right systems and people are in place to keep pace with changes."

Kimberly Verska (left), partner and chief information officer at law firm Culhane Meadows, sees roles shifting in the C-suite, particularly in light of the hacks of corporations and their advisers. "Locking down data securely at every point of an enterprise's operations is finally getting the attention it deserves," says Verska, who concentrates her practice on corporate and technology transactions as well as regulatory issues, particularly in the arena of data privacy.

Data security has been a longtime focus in companies whose product is data, she explains. "It's only now, as a result of several highly publicized corporate exposures and CEOs losing their jobs as a result, that the issue of data security is getting serious attention."

No company or executive wants to be embarrassed on the front page of any news outlet for something like a data breach or hacked email or Twitter account, she says. "And when CEOs lose their jobs over these breaches, security tends to become a top C-suite priority. As a result, management is starting to recruit more 'tech savvy-ness' at every level of their organizations -- from operation to the C-suite, even to board-level positions."

Competition to get the right security professionals on board is fierce, says Verska, who speaks Russian, German and Spanish, and has authored and co-authored numerous articles on the laws of foreign jurisdictions relating to data privacy and e-commerce. But it's more than simply hiring a well-known security expert or a CIO. "It's not enough to hire a 'compliance lion' if no one is watching what the cubs are doing. The real shift in the C-suite is working to create a culture of compliance organization-wide."

In the past, a company's security functions fell to the CIO or CTO, whose top priorities are typically a mix of innovation and operations, and very few of the largest enterprises employed a CISO, says Domini Clark (*left*), a principal at Blackmere Consulting, an executive recruiter for the technical and cybersecurity industry. Even the U.S. government didn't have a C-suite security-focused executive in the role before 2016, when the first federal CISO was hired, she points out. "But times are rapidly changing, and corporations are learning that security is no longer purely a technological issue, and can no longer be constrained solely to IT."

Senior management is realizing that information security is really a risk issue, and risk is a business challenge that needs broader solutions, says Clark, also the director of

strategy at InfoSec Connect. "This realization means we will continue to see growth in the CISO function across organizations of all sizes."

Michael Potters (*right*), CEO of Glenmont Group, a Montclair, N.J.-based executive search firm, agrees that roles are shifting in the C-suite, but, he explains, it's taking shape in two forms: The CISO position is now showing up at most Fortune 500 organizations often not reporting to a CIO but to a CEO, he says. Plus, there is now a movement to see chief information governance officers (CIGOs) become an accepted role at the C-suite and have infosec in the silo.

Also, the role of the general counsel at the Fortune 500 has had cyber issues dotted lined to them as they are under fire to makes sure that this is being addressed properly to prevent “break the bank,” large-scale litigation caused by not addressing cyber issues in a proactive way, he says.

Others also see more direct reporting to the C-suite and activities with the board. C-level and boards are seeking trusted advisers, says Gary Clayton, shareholder in the workplace privacy and data security practice of Littler Mendelson. Although there is a caveat, he points to: Many who would be potentially great advisers are so concerned about personal and professional liabilities that they are reluctant to accept these positions.

Meanwhile, Laliberte at Protiviti, also sees some movement within the C-suite. "In some organizations, security is now reporting into risk management rather than IT," he says. More C-level personnel are becoming involved in cyber and security issues, he says. "Organizations are realizing cyber is not just an IT issue, but needs involvement of the business as well."

Joyce Brocaglia (*left*), CEO at security executive recruitment firm Alta Associates, says that as her firm seeks out CISOs, she is seeing that the role itself is being elevated in many companies. "We are conducting many searches where the C-suite realizes that what got them to here isn't going to take them to the future, so they are hiring more strategic thinking CISOs with a broader set of responsibilities than just cybersecurity," says Brocaglia, also the founder of the Executive Women's Forum. "Some are now reporting to the CEO and no longer sit under a CIO in technology. Cybersecurity has become a board level imperative. The C-suite is interested in how cybersecurity can make the overall company more resilient."

Today's top cybersecurity personnel, particularly in the CISO position, are using more tools to help monitor the enterprise's risk and planning ahead for what to do when they

are breached, according to Wils Bell, a cybesecurity recruiter for 15-plus years. Bell says he's seeing people that are more technical and have a good knowledge of enterprise risk as well as the overall business.

More tech speak in the corner office

Are boards enlisting more tech savvy personnel? Bell emphatically says "Yes."

Verska, though, says the answer depends on the industry and, in some cases, board members' comfort with technology. Historically, among the Fortune 100, the shift to nominate tech-savvy members is slower, aside from the obvious positions of chief technology officer (CTO) or chief information officer (CIO), she says, adding that this slow adoption results in an interesting phenomenon: Vulnerability at the very top of the pyramid, when, for example, an otherwise savvy executive uses the word "password" or "12345678" as a password, or unwittingly falls victim to a spear-phishing attack. Familiarity with the risks and with technology is critical, Verska emphasizes. And as board membership evolves, more board members will have grown up with technology and have been thoroughly schooled to know better than to disclose passwords, account numbers or other critical data to the sender of an unexpected email, she says.

"The executives who joke that they 'are helpless with all this new technology stuff,' may end up being the weak link that creates a major hole in a company's security systems," says Verska. "Because no matter how effective or cutting-edge the security technology one implements, in the end, the best defense against cyberattack is an organization-wide culture of security."

At the board level, she says, this means that every member must understand that as part of their "a duty of care," neither they nor the company's employees engage in or overlook practices that pose risks like security breaches. "It's a responsibility that board members increasingly know they must consider and to which they are beginning to respond," she says.

Clark agrees, saying that technology in the workplace is growing at an explosive rate. "There is currently more technology in use enterprise-wide than there has ever been before," she points out. "It is clear that security is influencing conversations at the highest executive levels and boards are becoming more and more savvy about technology and cyber risk."

Brocaglia at Alta Associates, says her firm places many CISOs who must have the skills to directly present to the board. And, validating that requirement is new legislation recently introduced in the Senate that would require publicly traded companies to disclose to regulators whether any members of their boards of directors have cybersecurity expertise.

The Cybersecurity Disclosure Act of 2017, or S. 536, would *not* mandate that companies retain a cybersecurity expert on its board. Rather, the proposed legislation would require companies to explain – in their filings with the Securities and Exchange Commission – whether such expertise, in fact, exists on their boards and, if not, why this expertise is redundant owing to other procedures put in place by the company.

Brocaglia says she expects that this legislation will raise the issue more frequently with board members and result in their evaluation of the executives they have in place driving their security and risk teams.

But, for Rajiv Gupta (right), CEO at Skyhigh Networks, boards have paid lip service to adding members with cybersecurity expertise. CISOs often take on the responsibility of educating the board, he says, making business-minded CISOs a hot commodity on the job market. "They say the CIO is the new COO, and the CISO is the new CIO. Technology is now a core function for companies reinventing themselves as digital businesses. The CIO leads digital transformation and the CISO is responsible for overcoming the principal technology barriers of cybersecurity and privacy."

Other experts agree that there is a gap between the talent required and positions filled. Potters at Glenmont Group, says this is a huge problem. "The boards are still being populated by investor types (VCs and PEs) or old school leaders who are too far away from cyber issues to understand the importance of cybersecurity," he says. "When I talk with board members it is scary to hear how detached they actually are on this issue."

Meanwhile, Clayton at Littler Mendelson says that many boards try to recruit board members that have cyber knowledge but the skillsets and personality combination are relatively rare. "There's too much techno-babble by most of those who are knowledgeable cybersecurity personnel," he says.

Laliberte too says it is extremely difficult to find tech savvy board members. "Instead boards are enlisting external help of subject matter experts to assist them in understanding cyber risks."

Data theft response

But, while companies do what they can to hire the appropriate security personnel, in the C-suite security is certainly rising up the ranks as a business enabler.

Bell says he sees companies realizing that there is no way to avoid a data compromise if they are singled out for a hack, but, he explains, they can avoid large financial loses and branding issues. "No one wants to be the next Target or Home Depot," he says.

The solution he opts for is to reduce the damage. "I see some companies tie the CISO's bonus or reduce it for breach activity or perhaps direct financial loss. Companies need to realize that there is just as brilliant a mind on the other side of the desk (hacker) as they have on staff."

Breaches, he says, are inevitable for most firms, but how well they are mitigated or how the damage is contained makes the difference.

Potters says execs are finally looking at this issue proactively as opposed to reactively and are now willing to invest money (though not enough) to address the problems before they happen and not after they happen.

Verska agrees that the C-suite folks are paying attention. "Episodes like the Target data breach, which resulted in the exit of that company's CEO, certainly got the attention of industry," she says. "We see increased emphasis on employee and executive training – including the C-suite and board level – particularly of those with a fiduciary responsibility of due care. Companies are spending millions of dollars on data security and training. This is a good thing if people take training seriously because sometimes it's the little things that trip companies up."

Security breaches are the quickest way for a company to get its name – the names of its executives, or the names of its board of directors – on the front page of the Wall Street Journal, she adds. "Worse is when it's for neglecting to patch vulnerabilities that in hindsight look quite obvious, like permitting employees to transfer confidential customer data onto their unencrypted personal laptops so they can work at home."

In the not-too-distant future, companies will be looking at block chain and cutting-edge technology as the standard of due care evolves, Verska (left) says. "But in the meantime, they can and should use the tools that exist. Have firewalls and monitoring software to check whether someone is trying to breach those firewalls," she advises.

She also advises considering encryption. "It is the industry standard of care for many types of data, legally required in many cases."

What's shocking about encryption technology is how many companies don't even do that, she says. "They may rely on third-party providers who may or may not have upgraded their own systems. We recommend that clients carefully consider the chain of operations and what happens when their data comes to rest in a third-party service provider -- are they secure or are they leaky?"

Too often, she says, companies think their data is encrypted and protected as they move it from point A to point B, but it's not. "Nor do I think a lot of companies realize how many ways there are for intruders to hop into the pipeline when they send sensitive data via ordinary emails."

Companies are realizing that an ounce of prevention is worth a pound of cure, says Blackmere's Clark. "Data theft is a risk from outside the organization from hackers and phishing attacks, but increasingly a risk from the inside – from both intentional employee theft and unintentional employee negligence," she says. "Just like we've seen the emergence of the role of the CISO who is overseeing responsibility for corporate risk, we are also seeing the shift in mentality that data theft is not just an IT issue, but one that needs to be prevented through technology measures and continuous cybersecurity training geared toward the non-technical employee."

Executive teams are beginning to understand that the responsibility for protecting their company's data is truly a team effort, and that the responsibility for data loss risk management, while led by the CISO, truly belongs to the organization as a whole, Clark adds.

And what will it take to attract and retain the right people?

Corporations need to come to terms with the compensation needed to get these highly skilled and highly desirable cyber experts, says Potters. These workers can save your company, he explains. "Don't try and squeeze someone with $200k skills into a $100k pay band," he advises.

Also, he adds, hiring authorities need to understand that time is of the essence when looking at candidates. "If you think you have found someone that is worth bringing in on your team, move quickly," Potters says. Streamline the interview process so it only takes a couple of weeks, and not a month or more. "You will lose out on that candidate as they start hearing about other opportunities – or, at the very least, you will have to give them more than the 15 percent recruiting bump that is typical."