SpencerStuart

Digital Transformation

An Expert Perspective:

Art Coviello on the Board's Role in Cybersecurity

On Nov. 17, 2015, Spencer Stuart hosted a dinner for board directors to discuss the growing threat of cyber attacks and the board's responsibility for overseeing this significant risk. Art Coviello, the former CEO of RSA Security and one of the leading global experts on cybersecurity, led the discussion. Here, Coviello shares key themes from the discussion and his recommendations for boards.

There is a common refrain coming from boardrooms: "I am concerned about cybersecurity risk but I'm not sure how to get my arms around the problem." Because the issue is so complex and technical, there are general feelings of hopelessness, helplessness and ... fear. But as Nobel Prize winner Marie Curie once said, "Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may fear less."

I always make the point that while we are aware of the problem — hardly a day goes by that there isn't a report of some organization being breached — we don't understand the problem. We tend to start in the middle with the hackers and their latest attack methodology and sophisticated malware. Our eyes glaze over when we hear terms like "zero day vulnerability" or "APT" (advanced persistent threat).

In the following paragraphs, I'll summarize the recommendations I shared in my remarks and in the Q&A to help you gain that understanding and ultimately provide better oversight and support for management on this critical issue.

While it is important to know what types of hackers (e.g., nation states, criminals, non-state actors, "hacktivists" and terrorists) are likely to attack your organization and what methods they might use, you first need to understand why you are vulnerable in the first place and how those vulnerabilities may change in the future. Over the last 10 years, there are few, if any, organizations that haven't been massively affected by digital technologies in their business systems, operations and in the ways they serve their customers.

Consider that 10 years ago:

- There were no smart phones. Now there is ubiquitous communication and access.
- Most, if not all, applications were accessed and delivered internally. Now countless web-based applications are delivered on organizationally controlled portals, and are increasingly being hosted in the cloud along with data.
- There was no significant real-time analytic capability. Now an exponential increase in data, storage, computing power and network speed create big data applications that deliver content in ways and speeds we couldn't have imagined.
- Machines were analog and digital. Now they are overwhelmingly digital and increasingly Internet-enabled (e.g., Internet of Things).

Top five recommendations for the board:

1. Acquire a high level of understanding of how your organization uses technology and potential vulnerabilities.
2. Ask for a comprehensive annual review of your security program.
3. Have an independent audit conducted.
4. Review the breach response plan.
5. Bring experts onto the board.

From a security standpoint, the implication is that our attack surface has reached a point where breaches or intrusions are probable, if not inevitable. The perimeter defenses we have relied on historically have largely ceased to exist. This brings me to my first recommendation:

Acquire an understanding, at least at a high level, of how technology is deployed in your organization and how it has made you vulnerable.

While it is frightening to think that intrusions are inevitable, it doesn't mean that disruptions and losses are. But the situation requires security practitioners to think differently. Historically, security models have been reactive (find a hole and plug it) and perimeter-based, while the controls used to protect the perimeter are static ("yes" or "no" gates) and siloed (they don't add value to one another). The result is there is no in-depth defense. In today's open environment, to prevent the inevitability of an intrusion and to reduce the probability of loss, we need a different model, a more intelligence-based approach.

Let me illustrate:

HISTORICAL MODEL	TODAY
REACTIVE	***INTELLIGENCE-DRIVEN***
Perimeter-based	Risk-based
Static controls	Dynamic, agile controls
Siloed controls (no leverage)	Interactive (add value to each other)
Emphasis: technology	Emphasis: people, process, technology
Goal: prevent breaches	Goal: prevent loss

If the goal is to prevent loss as cost effectively as possible, a much more holistic (intelligence-driven) approach to security is required. That approach starts with having a much better understanding of risk: Which key information assets, applications, transactions and infrastructure that, if lost, disrupted or destroyed would have a material impact on the organization? But understanding risk also entails understanding who the threat actors might be as well as their attack methodologies.

Mitigating risk starts with having the right culture about security, one that is understood as broadly as possible among employees; involves extensive training of the people most vulnerable (e.g., system administrators); and has documented processes under a comprehensive system of governance, risk and compliance.

Next, to develop defense in depth, the control environment needs to be set up to:

- prevent attacks in the first place (eliminating vulnerabilities to the extent possible);
- prevent breaches with more intelligent controls that inform one another and that can react to facts and circumstances; and
- detect and respond to intrusions with advanced monitoring and analytic capabilities.

Unfortunately, many budgets today are skewed toward the old model's goal of breach prevention. A holistic model of security should have a distribution of resources based on how to best — given the risk environment — prevent loss over a continuum of attack prevention, intrusion prevention, detection and response capabilities.

The obvious question now becomes: "OK, what do I do with this information?"

I recommend the following:

Ask for a comprehensive annual review of your security program.

This is probably already being done by the audit or risk committee, but should at least be reported to the full board. Start by asking the CEO about the culture he/she has set; the support of the CEO is vital. Ensure you gain an understanding of risk as it's been described. Look for periodic updates to the risk profile based on new deployments of technology and changes in the business. Review the backgrounds and capabilities of your security team. There is a critical shortage of skilled personnel and you don't want to be on the wrong side of that shortage. One way to get a handle on the competence of the team is to assess how well they have implemented some form of an intelligence-driven model, such as a system of governance, risk and compliance, control environment and resource allocation. You should already be looking at these issues as part of the review.

Have an independent audit conducted.

Because you likely won't have the expertise to understand the technical details of the review, you should have a separate audit of your security program by a firm that is neither your financial statement auditor nor a contractor you are already using for security work.

Review the breach response plan.

There are breaches that are handled routinely and there are significant breaches that result in some form of increased risk or loss. In today's world of social media, you need to be ahead of the story, so customers, regulators and other interested parties are hearing directly from you first. The response can't be done serially. All functions have to work together and in parallel as soon as it's determined that a significant breach has occurred.

Bring experts onto the board.

Given the role of technology and its complexity and associated risks, consideration should be given to having expertise on the board that can help on technology and security-related issues.

SpencerStuart

ABOUT SPENCER STUART'S BOARD PRACTICE

For more than 30 years, our Board Practice has helped boards around the world identify and recruit independent directors and provided advice to chairmen, CEOs and nominating committees on important governance issues. In the past year alone, we have conducted nearly 700 director searches. We are the firm of choice for both leading multinationals and smaller organizations, conducting more than one-third of our assignments for companies with revenues less than $1 billion.

Our global team of board experts works together to ensure that our clients have unrivaled access to the best existing and potential director talent, and regularly assists boards in increasing the diversity of their composition. We have helped place women in more than 1,400 board director roles around the world and recruited roughly 600 minority directors.

In addition to our work with clients, Spencer Stuart has long played an active role in corporate governance by exploring — both on our own and with other prestigious institutions — key concerns of boards and innovative solutions to the challenges facing them. Publishing the Spencer Stuart Board Index (SSBI), now in its 30th edition, is just one of our many ongoing efforts.

ABOUT SPENCER STUART

At Spencer Stuart, we know how much leadership matters. We are trusted by organizations around the world to help them make the senior-level leadership decisions that have a lasting impact on their enterprises. Through our executive search, board and leadership advisory services, we help build and enhance high-performing teams for select clients ranging from major multinationals to emerging companies to nonprofit institutions.

Privately held since 1956, we focus on delivering knowledge, insight and results through the collaborative efforts of a team of experts — now spanning 56 offices, 30 countries and more than 50 practice specialties. Boards and leaders consistently turn to Spencer Stuart to help address their evolving leadership needs in areas such as senior-level executive search, board recruitment, board effectiveness, succession planning, in-depth senior management assessment and many other facets of organizational effectiveness.

For more information on Spencer Stuart, please visit **www.spencerstuart.com**.

Social Media @ Spencer Stuart

Stay up to date on the trends and topics that are relevant to your business and career.

Amsterdam
Atlanta
Bangalore
Barcelona
Beijing
Bogotá
Boston
Brussels
Buenos Aires
Calgary
Chicago
Copenhagen
Dallas
Dubai
Frankfurt
Geneva
Hong Kong
Houston
Istanbul
Johannesburg
Lima
London
Los Angeles
Madrid
Melbourne
Mexico City
Miami
Milan
Minneapolis/St. Paul
Montreal
Moscow
Mumbai
Munich
New Delhi
New York
Orange County
Paris
Philadelphia
Prague
Rome
San Francisco
Santiago
Sao Paulo
Seattle
Shanghai
Silicon Valley
Singapore
Stamford
Stockholm
Sydney
Tokyo
Toronto
Vienna
Warsaw
Washington, D.C.
Zürich

ARCL_BOARDRULECYBER_12|15