Accenture Security

THE CYBER-COMMITTED CEO AND BOARD

by Kelly Bissell, Ryan LaSalle and Kevin Richards

When security and risk leaders make cybersecurity "business relevant", the cyber-committed CEO and board of directors become engaged, not just involved. In this document, we share three industry-leading practices chief information security officers (CISOs) can use to catalyze engagement.

THE CHALLENGE

HOW TO ENGAGE, NOT JUST INVOLVE

In a recent Accenture research study[1] among 2,000 security executives across 12 industries and 15 countries, 70 percent of the respondents agreed that "cybersecurity at our organization is a board-level concern and supported by our highest-level executives."

While this top-level concern is encouraging, especially considering what is at stake, the challenge is how to go beyond CEO and board "support" and involvement, to real engagement.

How do you create a cyber-committed CEO and board? The heart of the answer is that they must become engaged with how cybersecurity impacts the business, how it affects risk tolerance, and how it enables opportunities.

The CISO of a leading regional bank puts it this way: "There's a difference between passive and active CEO alignment. It's one thing to have an audience, and another to have a shared conversation. That's where we need to get."

THE CISO'S ROLE:

CATALYZE BUSINESS RELEVANCE

If engagement is the key to creating a cyber-committed CEO and board, then what is the key to engagement? And how does it differ from simple involvement?

Engagement means not shying away from or fearing cyber risk because it is new or they do not understand security. As much as the CISO needs to understand business, the CEO needs to understand security, and manage it like any other business risk.

Ryan LaSalle, global managing director, Accenture Security—Growth & Strategy, says the key is establishing business relevance.

"An involved CEO meets regularly with the CISO, reviews reports, asks questions, and provides encouragement and support in front of the board," says LaSalle. He adds, "An engaged CEO feels part of the team to create the answers, and assumes accountability for the risks the business is taking. The shift is one of relevance. If the CEO understands cyber risk to the same degree as any other business risk, is aware of the options, knows how to manage that risk and how it fits into what the company is doing to drive growth in the business, then he or she is more engaged."

The CISO serves as the catalyst for achieving this shift. Observes a CISO for a leading European energy producer and provider: "It is up to the CEO to decide whether to invest in cyber defense, but it is the CISO's responsibility to guide and inform the CEO. The CISO is the one who builds the case for the CEO and the rest of the management team."

The problem is, many CISOs fail to act in that business advisory role today. They are too focused on the technological and operational dimensions of cybersecurity, at the expense of business impact and risk management.

LaSalle explains: "We are at an inflection point in the industry, where CISOs have typically talked about an operational picture of security in the business, like how many critical vulnerabilities there are, how many unpatched systems, how many incidents. The board is looking for a more strategic picture, such as if the money they have invested is being used effectively, if the business is ready for what comes next, if the change being sought is sustainable, or even how to leverage security to enable the business to grow with confidence."

Accenture client experience has identified three industry-leading practices to help make a much-needed shift from a technology- and operations-focused posture, to one that is more strategic and focused on risk management:

1. Capture the strategic picture of cybersecurity in the business.
2. Speak the language of business impact in all cybersecurity communications.
3. Build "muscle memory" for threat response at the CEO and board level.

LEADING PRACTICE 1

CAPTURE THE STRATEGIC PICTURE OF CYBERSECURITY IN THE BUSINESS

To enable CEO and board commitment, CISOs can develop a strategic narrative around cybersecurity that captures four key components:

1. What are the threats to our most important lines of business—and how are they changing?
2. What are we doing—and how effective is it?
3. What are the strategic options and initiatives across our business—and what are we doing to manage the risks they pose?
4. What are the remaining risks—and what do we need to do about them?

Throughout, a foundational question to keep in mind is: What decisions or actions are we requesting from the board?

Regarding the first component—threats to the most important business assets and how they are changing—the key is to focus on threats that create real risks for the business. If that does not happen, the second component—what is being done and the effectiveness of it—is undermined, since the organization is failing to give the most significant contours of the threat landscape adequate focus or attention.

While CISOs understand cyber threats to the business, they sometimes struggle with conveying those threats effectively. Too many CISOs go to their CEOs and boards with scorecards that are overladen with volumetric data on compliance challenges or technology issues. As a result, business threats can be lost in a swamp of information, or at the very least their significance becomes diluted or dulled. That, in turn, can lead to a one-way communication which precludes discussion of the strategic impact of threats and the strategic decisions required.

Kevin Richards, global managing director, Accenture Security—Strategy & Risk, offers this example: "Consider the CISO who reports that the organization's asset inventory is incomplete. Certainly that poses an operational challenge and may even show up as an audit or compliance finding. By itself, however, it isn't actually a risk—it contributes to a risk. But is it an item the board cares about or will understand the nuances? Compare that to presenting: "With our funded budget, we can effectively protect and monitor only 70 percent of our production manufacturing servers. The unprotected servers represent seven percent in annual revenue and if there is a cybersecurity incident within those unprotected servers it could impact our top five customers who are most at risk." Such a scenario is a clear business issue with quantifiable monetary impact and strategic implications for the organization."

The "right" scorecard can be an anchor piece in board communications, but, most important,

is telling the story of the threat landscape and the security initiatives underway to address those threats. The scorecard then underpins the discussion on how the business is performing against those initiatives, leading into a debate on the strategic decisions the board needs to make moving forward.

One way for CISOs to elevate cybersecurity decisions to a more strategic level is to focus on the risks posed to a specific division or line of business in the company, or by cross-business strategic initiatives such as M&A, digital transformation, business expansion and whatever else is keeping the CEO up at night.

A typical strategic decision could be the risk appetite of the enterprise and how much it is willing to accept. For example, the challenge a board faces when it looks at the current state of affairs compared with, say, the risks of an upcoming transformational initiative to "go digital." The board has to decide how to balance the immediate security issues facing the organization today, or to put a "band-aid" over those issues and shift the focus onto what might be coming next. Here, security becomes a board-level discussion centered on what should be the right strategic direction for the company: Do we fix the security issues of today systemically, or do we focus our resources on tomorrow? Or, is there another option? What is the recommendation and why?

Identifying the strategic decisions that need to be made by the CEO and board about cybersecurity is another way to elevate the conversation and create a truly strategic picture of cybersecurity in the business. However, this is not always as straightforward as it might seem.

Consider the situation where an enterprise decides to increase its budget for security risk management initiatives. Because CISOs and their teams often live within the larger CIO organization, it is not uncommon for a CIO to have discretionary power to reallocate additional security spend to other, non-security-related enterprise IT priorities. When that happens, an expected increase in security budget can become a decrease or even evaporate.

On the surface, the strategic decision required of the board in this situation might appear to relate to cybersecurity funding levels in the organization. But in actuality, it relates to a more fundamental discussion on where responsibility for security should reside within the business. Should it be part of a larger IT organization with potential conflicts of interest? Or should it belong to an independent part of the organization which is part of a larger risk management function? If the board wants greater line of sight into security budget allocations and their effectiveness, the security team would need to reside in an organization whose primary focus is business risk management, not operations and infrastructure. Some companies have already moved the security function into the Audit Committee or Finance organization, adding responsibility for security risk to their management of financial risk and operating risk.

These are the kinds of considerations a CISO should take into account to engage the CEO and board and to help elevate communications to a more strategic level.

LEADING PRACTICE 2

SPEAK THE LANGUAGE OF BUSINESS IMPACT IN ALL CYBERSECURITY COMMUNICATIONS

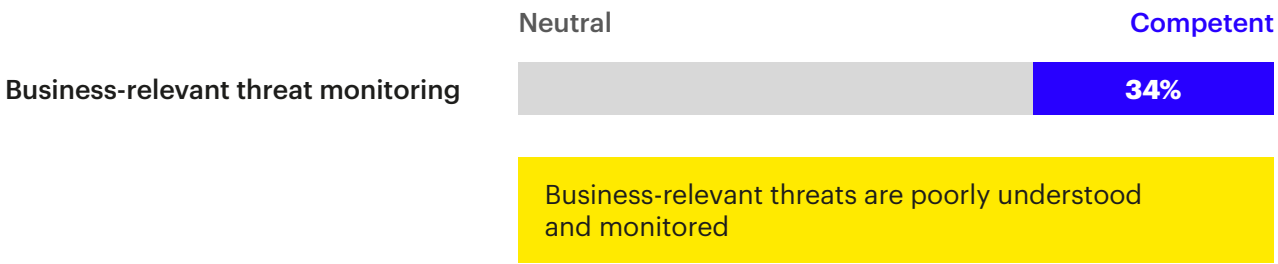
The fundamental requirement for strategic engagement of the CEO and board is to measure and communicate security risk in non-technical business terms that they will find relevant. CISOs must "take technical issues and elevate them to board-level business concerns and language," as Kelly Bissell, global managing director for Accenture Security has noted, and "through this process we can educate the CEO, board and management on the most important challenges, along with the options available to solve them."

Unfortunately, many CISOs struggle to explain the business value of cybersecurity initiatives. Accenture research[2] shows that only one-third of cybersecurity executives believe their organizations effectively monitor business relevant threats, no doubt due in large part to inadequate communication and linkage of what makes a threat business-relevant from the start (Figure 1).

Reinforcing this point, the CISO at a leading digital content provider shares the following story regarding an identity and access control audit in his organization: "The results literally rolled up to the board of directors and in essence their reaction was: 'We do not understand why this is relevant because none of this makes any business sense for us.'" Despite the significant investment that had been made in the audit, and the threats that had been revealed, failure to communicate and convey what it all meant for the business rendered a meaningful response impossible.

To counter this, some CISOs have become very deliberate about drawing clearer connections to the business impact of the cyber initiatives they execute and the cyber metrics they measure. As a senior security executive at one of the largest global banks explains: "When we talk with our board, we're very careful to put our discussions of security risk in business terms rather than

Figure 1: Low competence with business relevant threats



technical terms. So, for example, we do not present the board with metrics on encryption. We present the board with metrics on protecting customer data. And we don't have metrics around patching. We have metrics around maintaining the integrity of our production environments."

But it is not just scorecards and metrics that need to be business-relevant—it is the explanation and communication of what they reveal. Can the business protect online customers so they continue to buy? Can we safeguard our most important assets such as contracts, pricing sheets or M&A data? Can we prevent employees stealing from the company? Can we protect our intellectual property from the devastating impact its theft would have on our marketing and business plans?

Consider an organization that monitors the metric "End of Life Assets." Following a spate of acquisitions, the organization finds that, after applying the metric across the enterprise, fully half of its network infrastructure products are beyond end of life.

A CISO must make a conscious, deliberate effort to translate that finding into business-relevant terms. For example:

- As an organization, we no longer receive security support from half of our vendors.
- That means we have to backstop multiple defenses that are years out of date.
- Industry peers have solved this problem by investing in significant capital management and vendor consolidation programs.
- If we cannot muster the capital to replace the lost footprint, these are the kinds of problems we can expect:
  - Quarterly findings from our auditors that show deficiencies in our controls.
  - Uncertainty in our business about whether or not the applications and customer data stored in the vulnerable different environments are safe and protected.
  - Possible citation by consumer protection agencies.
  - Significant brand damage if customer data is compromised.

In other words, what is revealed by the metric must be communicated in terms the CEO and board care about.

Notes LaSalle: "The CEO and board care less about whether you as a CISO have a capital budget of X and a replenishment rate of Y. They care about the outcome and the impact, communicated in business terms that relate to their fiduciary responsibility."

LEADING PRACTICE 3

BUILD "MUSCLE MEMORY" FOR THREAT RESPONSE AT THE CEO AND BOARD LEVEL

An engaged CEO and board are a prepared CEO and board. In fact, there may be no better way to establish the business relevance of cybersecurity than to engage the CEO and board hands-on in cybersecurity crisis drills, simulations and tabletop exercises. Through those experiences, they can see firsthand the criticality of threat response readiness and the consequences and impacts of being unprepared.

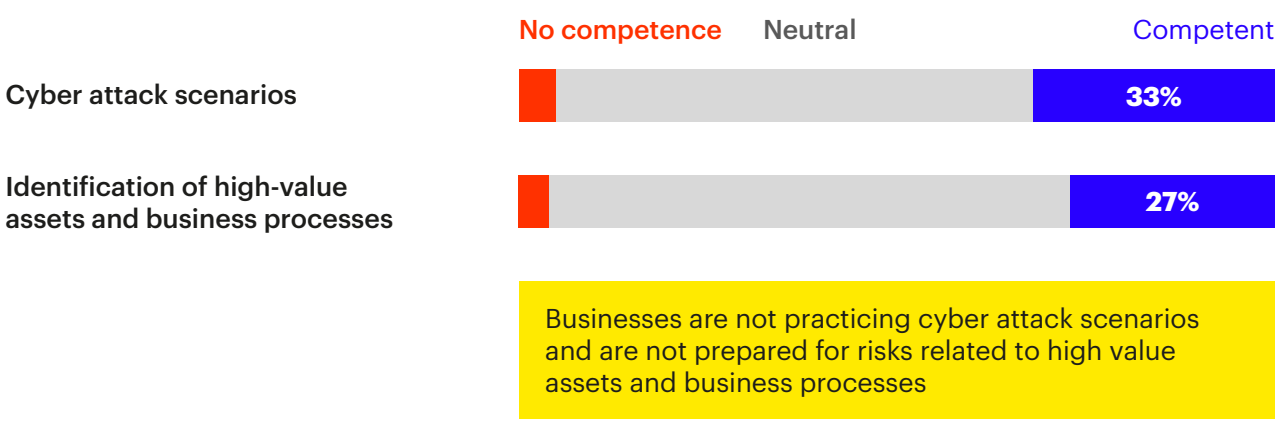
A senior security executive at a top global bank draws on a sports analogy to make the point: "What happens during a crisis is just like what happens during a football game. You've got to practice what you're going to play—and run through the playbook several times so you are ready to execute by game time."

Unfortunately, preparation of this sort is sorely lacking across many organizations. Accenture research[3] shows that only one-third of organizations are competent at practicing cyber attack scenarios, and even fewer have adequately identified (let alone protected) the high-value assets and processes that could be targets of a cyber attack (Figure 2).

Even when security organizations do engage in drill and practice, such exercises seldom extend beyond the security team into the business and up to the C-suite. In fact, Accenture research[4] shows that essentially two-thirds of organizations do not adequately involve stakeholders in cybersecurity incidents, and lack clear escalation paths for involving senior and top management (Figure 3).

To improve readiness, Nadav Zafrir, co-founder of Israeli cybersecurity incubator Team8 advises that CISOs must engage with CEOs to identify high-impact scenarios and how the organization will respond. CISOs must make CEOs and boards more comfortable with, and literate about, cyber risks in particular.

Figure 2: Low response readiness



"CEOs are managing risk all the time," Zafrir observes. "They understand financial risk and regulatory risk and fraud. That is how they got there, to be CEO. They've seen everything. With conventional risks, they know what to do, how to act." But with cyber risks, they are out of their element. "The problem with leadership and cyber is that it is so nascent and novel that most leaders that rise to be CEOs don't get it. And it scares them."

Zafrir advocates advance preparation through simulations, drills and other techniques. "They have to understand high-tech cyber scenarios in a controlled environment—not when the attackers are actually inside the enterprise," he says.

LaSalle notes that even in the comparatively few organizations that do make the effort to prepare for threat response. "Security teams tend to do these drills for themselves and their first-line partners in the business. Very, very few engage the top level of the company."

When CEOs, other C-suite executives and board members do participate in drills and simulations, results can be eye-opening. "Three things happen," LaSalle says. "First, they get a sense of what can go wrong, second they get a sense of how sweeping it is, and third, there's a clear focus on what their role is in shepherding the company through the crisis."

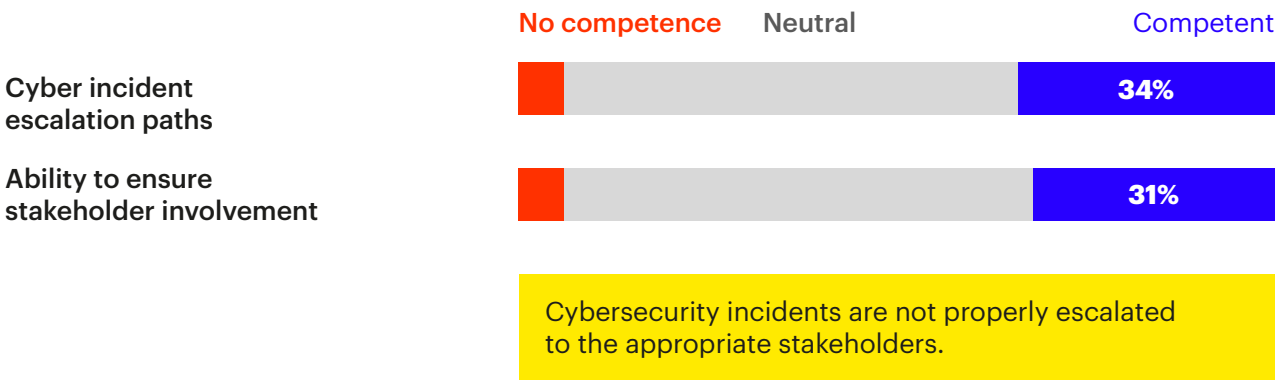
One guide of cybersecurity at a leading global bank cites a progression of techniques that have been effective in preparing and engaging senior leaders in his organization.

"We have over the past couple of years had a substantial set of tabletop exercises that have included members of senior management," he explains. The exercises led to the creation of a set of "crisis management playbooks" that cover everything from who needs to be contacted and how, to who initiates crisis management calls, to knowing the agendas for the calls and the desired outcomes."

"As we developed those playbooks, we wanted to make sure that all of the people in senior positions who need to be engaged during a crisis have gone through the experience of using them."

"Generally what happens during a crisis is chaos," he summarizes, "unless people have gone to practice enough times so that they understand the set of activities that are necessary to take effective action. Really critical is creating playbooks in advance and practicing them."

Figure 3: Low response readiness



Andy Vautier, the CISO for Accenture, has found the same approach to be effective. "We do the same thing in terms of having a very prescriptive playbook and the kind of fire drills that build muscle memory," he says. "And we do that with varying levels of impacts, including the senior management team in the organization and our Emergency Management Committee."

CISOs can supplement tabletop exercises, drills and simulations like these that engage the CEO and board with more basic "cyber literacy" efforts, such as:

- Make it a priority to educate the CEO and board on cybersecurity basics, including case studies, new technologies, industry standards, legal risks and more.
- Bring in outside perspective with practitioners from the field, forensic security specialists or other industry experts.
- Provide the board with the results of "red teaming"* exercises and the remediations and successes that resulted.
- Introduce hands-on familiarity of threat response capabilities through site tours at cybersecurity defense centers, where top executives and board members can witness firsthand the hub of an organization's cyber defense efforts. One CISO observes that for his CEO, board and business unit heads, the cybersecurity demonstration center at his organization has been "a great tool for demonstrating how the security organization does its day-to-day work to protect the company."
- Consider "board-to-board collaborations" where boards of non-competitive organizations can meet to share cybersecurity knowledge and leading practices.
- Include other corporate players—such as line of business leads, Legal and HR—as the situation demands.

Of course, there are times when there is no substitute for closed-door one-on-one meetings. As an insurance company CISO puts it, "To the extent you've got the ear of the CEO, a lot of things become much easier." His one-on-one meetings create the opportunity to inform, educate and engage his CEO, who in turn "really drives the alignment across the business."

* Red teaming is the process of using third parties, or ethical hackers within the organization, to act as advanced attackers to test the organization's defenses.

THE ENGAGED CEO

The cyber-committed CEO and board are engaged, not just involved, with cybersecurity initiatives. Responsibility for catalyzing that engagement falls to the CISO, who must make cybersecurity "business relevant" to top leadership.

CISOs can use three industry-leading practices as guiding principles to help ensure business relevance:

1. **Capture the strategic picture of cybersecurity in the business and use the right scorecard**
2. **Speak the language of business impact in all cybersecurity communications**
3. **Build "muscle memory" for threat response at the CEO and board level**

These practices enable and cultivate leaders who are informed, educated and engaged, and fully prepared to make the right risk management and investment decisions regarding cyber threats.

CONTACT THE AUTHORS

Kelly Bissell
Global managing director,
Accenture Security
kelly.bissell@accenture.com

Ryan M. LaSalle
Global managing director,
Accenture Security—Growth & Strategy
ryan.m.lasalle@accenture.com

Kevin Richards
Global managing director,
Accenture Security—Strategy & Risk
k.richards@accenture.com

REFERENCES

1. Accenture High Performance Security Research, August 2016.
2. Ibid.
3. Ibid.
4. Ibid.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

17-1059