Driving the Cybersecurity Agenda with the C-Suite and Boards
A CEO / CISO / Risk Fireside Chat

October 22, 2020

SESSION SUMMARY

Speakers

- **Mahi Dontamsetti**, CTRO, State Street
- **Sam King**, CEO, Veracode
- **Jim Routh**, CISO, MassMutual

Moderator

Jon Chesto, Business Reporter, The Boston Globe

KEY DISCUSSION POINTS

Priorities

The Cyber Expertise Boards Should Have

- **Board members need at least a baseline knowledge of the digital aspects of the business** to ask important questions. In general, boards don't have a high degree of cyber expertise which is unlikely to change given the shortage of specialized expertise.

Tough Questions for Board Members to Raise with the CISO and Management

- Probing questions to gain a fuller picture of cybersecurity risks and priorities:
  - What are the "known unknowns"?
  - If you had another $10 million above your current budget, where would you spend it?
  - What's one thing that could occur that would embarrass you (the CISO)?
  - What's one area where we are doing poorly and need significant improvement?

Communicating Cybersecurity with Management and Boards

- **Business strategy and risk priorities should frame the review of cybersecurity issues and decisions**, internally and at the board level.
- **Resilience is the performance standard.** CISOs should frame expectations realistically, i.e. there will be incidents…what's important is the capacity to respond and recover quickly.
- **The "Designated Board Geek" (or DBG) is a critical partner for management and the CISO.** There is usually one board member with particular technical expertise, sometimes several, to whom the rest of the board looks for leadership on digital or cybersecurity issues. It's very useful to meet with this member separately and more frequently, as they have a higher appetite for detail than the rest of the board. The DBG can then be tapped to help frame issues during board discussions.
- **Board committees play a critical role, with working sessions to drill down on issues and test out approaches.** Content differs when communicating with the C-suite, with full boards and with board committees (e.g. Audit, Risk, Tech Committees).

    - Board focus is on business strategy and oversight, management on operations.
    - Board committees receive more detailed reports and generally meet quarterly. Full boards usually cover cybersecurity at a high level for 45 minutes annually.
- **Executive board sessions with the CISO, without other management present, are used** to ensure candid conversations without any appearance of conflicts of interest.

Integrating Cyber Risk with the Organization / Setting Priorities: Four Basic Steps

- **Place cybersecurity among the top business risks.** This assures cyber is part of business risk assessment and avoids having boards and management view is as an isolated issue.
- **Align cybersecurity priorities and investment with the business' strategic platforms and business goals.** This alignment will not be the same for all organizations – no one size fits all.
- **Reach across the organization to develop consensus on the top 10 cyber risks.** A "David Letterman list" with agreement on the major risks then targets spending.
- **Integrate cybersecurity fully with technology and business functions; avoid the silo and the perception that security is an impediment.** The cybersecurity organization should have authority, autonomy, and independence….and equally, be an essential part of business and digital strategy and product development to assure the function is – and is viewed as – an important partner.

Finally, the Security Case to Make for a Shift to Digital

- The more digital the process, the less room for human error.
- Defenders' machine speed matches the attackers' speed
- Data and automation provide a fuller picture of systems and behavior. An 'absence of evidence' isn't the same as the 'evidence of absence.' If you don't know about bad things, it doesn't mean they aren't happening.

For more information on Boards of Directors and Cybersecurity, see the ACSC's 2019 Report Leveraging Board Governance for Cybersecurity: The CISO/CIO Perspective **that can be found at** www.acscenter.org.

2020 Conference Sponsors