DECEMBER 2022

LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY

FRONT LINE PERSPECTIVES ON HOW TO IMPROVE THE BOARD / C-SUITE PARTNERSHIP

"We are still immature at a board level in how we understand cybersecurity, and we're overseeing a function that is also immature and constantly changing."

CORPORATE BOARD MEMBER, RETIRED CIO

NEW FIELD RESEARCH;
CHALLENGING QUESTIONS FOR BOARDS

ADVANCED CYBER SECURITY CENTER

PRODUCED FOR THE ACSC BY MASS INSIGHT GLOBAL PARTNERSHIPS

ACKNOWLEDGMENTS

This report is produced by Mass Insight Global Partnerships for and in collaboration with the Advanced Cyber Security Center (ACSC).

Mass Insight and the ACSC would like to thank the executives, corporate Board members and advisors who participated in interviews, surveys and/or focus groups.

ACSC Leadership

WILLIAM GUENTHER, Executive Chairman
JOHN MCKENNA, President and CISO Chair
JAMES DINNEEN, Chief Operating Officer

ACSC members and partners contributing to this report

- Abacus Insights
- athenahealth
- CyberGRX
- Debevoise & Plimpton, LLP
- Dell Technologies
- Federal Reserve Bank of Boston
- Foley Hoag, LLP
- Harvard University
- Hathaway Global Strategies, LLC
- Manulife
- MassMutual
- MIT Lincoln Laboratory
- Munich Re
- Northeastern University
- Phenomenati
- State Street Corporation
- T. Rowe Price
- Takeda Pharmaceutical Company
- Veracode
- VHB

Author

WILLIAM GUENTHER, Chairman, CEO & Founder, Mass Insight Global Partnerships, and Executive Chairman, ACSC Board of Directors.

Mass Insight Global Partnerships organizes public-private partnerships in the Commonwealth of Massachusetts and New England through collaborations connecting university, industry and government and launched the Advanced Cyber Security Center in 2011 as an independent nonprofit 501(c)3 corporation. Mass Insight continues to produce research and publications for the ACSC.

Interview and Drafting Support

Emily Wiggin Communications

Graphic Design

Opus

Mass Insight
GLOBAL PARTNERSHIPS

www.massinsight.com

CONTENTS

SUMMARY

Board cyber governance is now at a pivotal point. Federal regulators and courts are demanding higher cybersecurity standards of Board due care and oversight. Four years after the publication of our 2018-2019 Mass Insight report for the Advanced Cyber Security Center, Leveraging Board Governance for Cybersecurity, we've updated our research.

Based on 27 new in-depth interviews and two focus groups, we examine the current state of management and progress against three of the five framing elements from the prior research:

- The Board's strategic risk role
- Developing cyber risk frameworks, metrics and measurement
- The evolving CISO role, management structures & Board governance

SPECIAL SECTION

Board Questions

Board members, advisors and legal counsels have proposed a program, *"Board Questions and Effective Board Engagement"* on pages 14–17.

Four years on, cyber risk governance remains a challenge, as regulators raise the stakes.

1. **DISCONNECT.** While ACSC CISOs and Risk Officers report progress in their Board's cyber maturity, Board members and advisors from a larger universe of organizations describe a continuing struggle with cybersecurity risk governance. Board members lament they continue to get overly-technical reports from management teams that fail to put governance in business and financial terms. While cyber risk has by all accounts become a higher priority for Boards, security executives are frustrated that too often cyber risk and cyber management continue to be secondary topics to enterprise strategic plans and success.
2. **A ONE-WAY CONVERSATION.** From all interviews, only a few examples show evidence of Boards challenging management and changing cyber strategy and practice in ways that the new SEC regulations will require. The discussions largely remain a briefing from CISOs and Risk Officers to Boards.
3. **CYBERSECURITY IN A BOX.** Cybersecurity continues to be dealt with at the Board and Board committee levels as separate and distinct from broader business strategy and risk management. Cyber agenda time for full boards is restricted to annual meetings, and generally, quarterly board committee sessions.
4. **FRAMEWORKS AND METRICS.** As we saw four years ago, frameworks that place cyber risk into a larger business context are a work in progress and fall short of what's needed for Board cyber risk governance.

While effective changes in cyber risk governance at the Board level have been slow to come, regulators are about to raise the stakes (see SEC expanding Board role callout box). Four years on, the evolving role and maturity of Boards in cybersecurity governance is even more timely.

Three major factors are driving the need for change at both the Board and senior management levels:

- **ACCOUNTABILITY.** Courts and regulatory bodies are signaling that Boards will be held to new levels of accountability, demonstrating active "cyber governance", and challenging the CISO and management on strategic risks and major operational choices.
- **COMPLEXITY.** The Board's strategic digital risk/ oversight role has grown more complex as challenges proliferate - underscoring the importance and value in engaging the Board in a full partnership.
- **CEO LEADERSHIP.** The time that CEOs commit to spending with Boards assessing cyber risk as an embedded part of business risk is an indicator of the organization's overall commitment to a security culture.

At the same time, Board members and advisors are raising concerns that many organizations have failed to:

- Clearly define the CISO role / responsibility, and demonstrate that operational, policy and audit responsibilities are distinct functions
- Fully account for the implications of operating in a larger digital ecosystem - with remote workers, regulations across multiple jurisdictions, and third-party risks
- Set up clear governance structures around data risk, privacy and security
- Frame cyber resilience - not as a technical review, but as a business risk

> "The importance of the Board's role in promoting a cyber-focused mindset and a cyber-conscious culture throughout the organization cannot be overstated."
>
> A NEW CHAPTER IN CYBER — ON THE BOARD'S AGENDA | DELOITTE, JUNE 2022

SEC expanding Board role

SEC rules, when enacted, will require prompt reporting of material cybersecurity incidents and disclosures in periodic filings focused on:

- Policies and procedures to identify and manage cybersecurity risks
- Management's role in implementing cybersecurity policies and procedures
- Corporate directors' cybersecurity expertise, if any, and the Board's oversight of cybersecurity risk
- Updates about previously reported material cybersecurity incidents

A new chapter in cyber — On the Board's agenda, Deloitte, June 2022

Boards and senior management continue to grapple with three key issues:

The Board's Strategic Risk Role

- ACSC member security and risk leaders rate their Boards as more mature than they did in 2018. Fully two-thirds report a "full partnership" — a 70% improvement over four years.
- However, as noted, only a few specific examples surfaced where the relevant Board committee had changed the direction of their organization's security posture, programs or strategic business decisions.
- Boards for the most part continue to treat cybersecurity in a separate box:
  - Isolated in agendas
  - Largely not included in strategic business planning or M+A reviews
  - CISOs invited in as needed to Board and committee meetings
- Most CISOs are given a short slot on a crowded quarterly agenda (15 – 45 minutes) at a Board risk, audit or technology committee with oversight responsibilities and similarly at the full annual Board meeting. In model cases, CISOs and Risk Officers build independent relationships with Board members.

Developing Cyber Risk Frameworks, Metrics and Measurement

- Cybersecurity risk is still dealt with as an operational issue.
- There is limited evidence of cyber risk being built into broader Board-level business and financial risk frameworks.
- NIST CSF continues to be used as a "check the box" tool in most organizations
- Risk management and measurement is shifting from prevention reporting towards resilience and business continuity reporting. After years of headline breaches, data and financial losses and brand setbacks, organizations are accepting that breaches will occur.

The Evolving CISO Role, Management Structures and Board Governance

- The continuing debate about where the CISO should report is a symptom of a larger problem — as interviewees reported, too many companies still haven't clearly defined the responsibilities of their CISO.
- There is an obvious tension between CIO and CISO priorities — regulators care, does your Board know how the organization has managed those conflicts?
- Boards should be asking — is the CISO taking a policy, audit or operational role, and how does that fit into the larger organizational structure?
- Is the CEO or the COO leading a cross-functional, executive leadership group that meets at least quarterly to oversee cyber risk and resolve internal conflicts? This was a leading indicator of a cyber mature culture identified in an earlier Mass Insight report produced with McKinsey & Co. for the ACSC.

The field's message to the SEC: Boards need more systems thinkers, not one cybersecurity expert.

In 2018, our interviewees cautioned against adding one cyber expert to a Board as a risk of placing too much responsibility on a single member. Experts today echo that caution and advocate for systems thinkers for Boards.

"What we need are well-qualified thinkers, who can take critical looks at operational systems and enterprise risk and ask intelligent questions."

This is not a surprise given typical Board cyber governance maturity and technical expertise

Board and committee cybersecurity governance at organizations interviewed reflects limited engagements

Board member perspective:

> "We are still immature at board level in how we understand and oversee cyber, in itself a function that is immature and constantly changing."
>
> MEMBER, THREE CORPORATE BOARDS, RETIRED CIO

Board maturity characterizations:

Early Stage: The Board is largely listening and learning from our briefings and will move towards a maturing partnership in the next year.

Maturing: The Board is developing expertise to become a full partner as described in above.

Full Partnership: The Board is well versed in the digital agenda and cyber risks and priorities, informed about the overall IT and related investments required to move to next generation, more secure systems and provides valuable feedback in their meetings with you.

Tech expertise on Boards varies by sector:

- Corporate Boards, typically 10+ members, with 0 – 2 members with IT background
- At University and government organizations, Boards and/or executive councils are larger, include internal management, and more IT/security expertise
- Private Boards are typically dominated by internal management and investors

Limited time on full Board agendas for cybersecurity:

- Briefings to the full Board usually held annually in 15 – 45-minute sessions, led by the CISO, sometimes along with CIO and, less frequently, with the Executive Leadership Team
- Some mature firms report more frequent, longer Board sessions
- **Committees oversee digital risk and cybersecurity:**
- Risk, Audit, Technology Operations, Governance
- Meet at least quarterly, 6 – 12 times annually at some firms
- Typically spend an hour on cybersecurity at each meeting

Board participation in incident simulations/tabletops, cybersecurity development is still rare:

- Few Board members receive cybersecurity risk training or continuing development, outside of standard onboarding for new members
- While Board chairs may be the exception, most Board members typically do not participate in tabletops/simulations

KEY FINDINGS

The Board's Strategic Risk Role

THEN, IN 2018

Early stage and maturing.

Few ACSC Boards were rated "full partnerships": In our earlier report, most CISOs reported their Board partnership was still "early stage" or "maturing."

NOW, IN 2022

Progress, but not enough, and a disconnect between Boards and security issues.

Two-thirds of ACSC security executives interviewed report progress and a "full Board partnership."

Board members and advisors too often see a different picture in the wider corporate world, with a continuing disconnect between CISOs and Boards.

Interviews suggest little has changed even for ACSC members in the Board's treatment of cybersecurity in a separate box:

- Isolated in agendas
- Largely not included in strategic business planning or M+A reviews
- CISOs invited in as needed to Board and committee meetings

CISOs made the case four years ago that cybersecurity should be an embedded topic in Board strategic business risk reviews.

Today it still appears to be a separate Board topic, with limited time devoted to it.

While a Board committee takes most of the oversight responsibility, most CISOs are still given one agenda slot (15 – 45 minutes) to brief the full Board annually, and quarterly committee updates on a crowded agenda.

- Even model security presentations focus largely on operational risk reviews. Forward-looking risk and security executives present a series of "deep dives" to Board committees, but there is limited time on Board and committee meeting agendas even to drill down sufficiently on operational due diligence, let alone the cyber risks of strategic business decisions.
- And with cybersecurity in a separate agenda segment, the security connection to enterprise business planning doesn't reach the Board.

In a positive development, more security executives report using shorter presentations (no more than five slides), limiting metrics and consistently presenting the same framing of topics.

Four years on, a striking disconnect: CISOs, Board members/advisors present differing views on the maturity of Board governance.

We found convincing examples of more mature Board relationships among ACSC members, but only a few isolated examples or stories where the full Board or committee had changed the direction of their organization's security posture, programs or strategic business decisions.

Board members and advisors report a bleaker landscape across a larger universe of companies, expressing deep concern over both Board capacity for cybersecurity governance and management's presentation of the issues at a strategic risk level.

From Board members: Concerns, and a recognition of the challenge of the rapidly changing issues.

"We are still asking the same fundamental questions and getting the same bad answers … we are still immature at a Board level in how we understand cybersecurity, and we're overseeing a function that is also immature and constantly changing."

MEMBER, THREE CORPORATE BOARDS, RETIRED CIO

"The Board is not informed enough, not yet getting the right kind of information, but … When you are dealing with a space that has moved so quickly, changing rapidly with attacks/threats — what you are seeing is an inevitable consequence. It's incumbent on us to not criticize so much, but look at what IS the right governance structure, what are the right reports, keeping in mind, that will change again inevitably."

MEMBER, MULTIPLE CORPORATE BOARDS, RETIRED CIO

Some security executives reflect the shift in Board discussions to resilience.

"Until a year ago, the Board discussion was protection/defense. Now it's sustainability/resiliency. Still, the traditional basics don't go away. Even with all the sexy stuff, we have to manage this expectation and make sure the Board knows what still needs to happen."

SENIOR DATA OFFICER

TRENDS

Examples where the Board has had an impact

- A risk officer at a global financial services firm, described a fully engaged Board, with the best questions coming not from a DBG (designated Board geek), but from others, framed in "holistic, business thinking."
- A Board at a smaller firm was instrumental in pressuring engineers to develop secure code and test before pushing features to customers.

A MODEL

Three-year "information risk capabilities" road map reviewed and tracked with a financial services firm Board.

"We are currently two years into a three-year information risk capabilities roadmap shared with the Board alongside the CIO, with projections out five years to show new investments. The Board reviewed, all endorsed.

When we meet, we share metrics — green/amber/red with plans/resourcing — our view on if we will hit target numbers. If not, we discuss — Board questions if it's okay, do we need an intervention, if not, why are you comfortable with it."

CHIEF INFORMATION RISK OFFICER

Strategic Risk Frameworks & Metrics

THEN, IN 2018 In our earlier report, we reported that cybersecurity hadn't yet developed the standardized, historically proven risk frameworks that financial and audit risk functions have refined over decades.

Management relied on NIST and other operational frameworks and metrics that can distract Boards from the strategic issues they should consider.

NOW, IN 2022 The picture is largely unchanged, with NIST CSF providing a solid "check the box" operational framework, and some firms customizing their own.

Board members and management struggle with the challenge of translating operational risk into financial impact.

And security and risk leaders are searching now for financial metrics for resilience and business continuity.

Industry standards and frameworks

Commonly used and shared with Boards:

- NIST CSF
- SANS CIS Controls
- ISO/IEC

Emerging

NIST SP 800-160 — Focused on cyber-resiliency engineering

Other

- FAIR — Codifies cyber risks in monetary value
- ISA-ANSI
- PCI Data Security Standards
- FFIEC
- COBIT 5

Operational frameworks dominate; Board-level strategic digital risk and resiliency frameworks and financial metrics remain elusive

Four years after our original assessment, cybersecurity and risk executives are still largely working with operationally focused frameworks, and with the shift to broadly managing digital risk and resiliency, CISOs are seeking guidance on metrics and KPIs that can set targets and guide investments for resilience.

> "We are shifting discussions to think more broadly about business risk … what are the 10 most fundamental business processes that have existential connection to business outcomes. Are our security investments directly linked to those 10 processes?"
>
> SENIOR DATA OFFICER

> "NIST CSF is a benchmark tool. It leads to a false sense of preparedness — this is a point of time — it doesn't mean you are prepared for a digital disaster. What is the mean time to recovery? What is the cost for every hour and every day we can't do business?"
>
> BOARD ADVISOR

NIST CSF continues to be the workhorse; NIST 800-160 emerging?

CISOs are comfortable with NIST CSF, Boards understand it by now, it's customizable by program and spend and can be layered with industry-specific frameworks. NIST 800-160 is being explored by some as an emerging tool to better deal with resilience, with its focus on cyber resiliency engineering.

Some firms have created customized risk frameworks to better integrate with enterprise risk, sometimes layered into NIST CSF. Leading organizations are creating entirely new frameworks, in some cases vastly different (tied to the business value chain, in one example).

A MODEL

Senior risk officer & CIO partner on long-term cybersecurity budget strategy.

- Use benchmarking to determine a target for security within the total IT budget—10–12% for 15 years.
- Tie the budget to a critical risk program framework, with specific metrics and targets. If budget conflict arises, these critical programs are protected each time.
- Effectiveness of the programs and budget allocation is assessed continuously, through assurance testing, pen testing, red teams, etc.

TRENDS

Time for a GAAP for cyber? More executives calling for standards.

Citing the positive impact of the 2021 White House Executive Order on Improving the Nation's Cybersecurity, a CEO/Board member and a CTRO pressed for unified cybersecurity standards comparable to GAAP financial standards.

Many executives interviewed are also ready for a single standard that would "simplify lives for practitioners, auditors and Boards."

Others cautioned, "standards may raise the floor not the ceiling" and should leave room for emerging technologies and innovation.

The Evolving CISO Role, Management Structures & Board Governance

THEN, IN 2018 Placing cybersecurity in an organizational silo at the operational and Board levels makes it difficult to manage and govern effectively, blocking a full understanding of cybersecurity's impact on business risk.

NOW, IN 2022 The findings today continue to reflect this challenge.

The accelerating shift to data /digital business processes drives questions about the CISO role, where it reports and the overall management of data and digital risk, issues raised in the earlier report.

Aligning Board digital governance and corporate structure: Every system has its flaws — it's about the security culture, people and collaboration.

Whatever the organizational structure, the inherent conflict between setting policies/assessing security performance and operating security systems has to be resolved and transparent to the Board.

The CISO/CIO reporting structure was raised in our report four years ago and still produces even stronger opinions today.

> "The continuing debate about who the CISO should report to is a symptom — the underlying ailment is that companies still haven't clearly defined what their CISO does. If they did, it would be clear who they would report to."
>
> LEGAL COUNSEL

> "We have refused to truly define the role and responsibility of a CISO."
>
> CORPORATE BOARD CHAIR, FORMER CISO

The terms of the debate haven't changed:

- Those at one end of the spectrum argue that the CISO should never report to the CIO given conflicting priorities — "it's the fox guarding the henhouse!"
- At the other end is the view that the CISO should always report to the CIO — "the CIO is ultimately accountable and can help stake cyber risk as business risk."
- Those in the middle contend that relationships matter more than structure — and reporting is ultimately irrelevant.

...Whatever the structure, Board members should be questioning how the policy, assessment and operational conflicts are resolved:

> "There is an obvious tension between CIO/CISO priorities — regulators care, does your Board know that"?
>
> LEGAL COUNSEL

> "Boards should be asking — is the CISO taking an audit or operational role, and how does that fit into the organizational structure?"
>
> CORPORATE BOARD MEMBER, CEO

... and if the CISO/risk officer has the necessary authority and visibility to do their job:

Board members and advisors stressed that reporting structure details are of less importance than whether the CISO/risk officer has the authority needed to act (often internal prioritization/politics present more of an obstacle than resources) and the access to and visibility into enterprise and broader technology programs required to secure them.

Legal and Board advisors urge an independent CISO, but it may not be that simple ...

Among legal counsels, Board members and advisors, there was consensus that the CISO should report to risk or legal — and align to the Board audit committee (not technology).

TRENDS

Some CISOs are offloading operational work to IT to focus on policy and assessment

The shifting of operational functions from security to IT has helped morph the role of the CISO and the definition of cyber in these cases.

New, forward-leaning titles are emerging, such as "Digital Risk Officer" and "Digital Trust Officer" — thinking about product through the lens of business.

And some CISOs are taking advantage of the trends to offload "high-responsibility, low-reward" operational functions to redefine their role as strategic policy and risk management

> "A lot of traditional cybersecurity jobs are high responsibility, low reward such as vulnerability management, vendor management, operations. I'm moving those over to IT.
>
> Push the responsibility to the business/IT owners to build and operate their tech securely... If those operational controls are stripped away over time, what is left for the CISO is real risk management — business risk, geopolitical, fraud; counterintelligence work."
>
> CISO, FINANCIAL SERVICES

But pitfalls await there as well. A CIO wrestled with downsides of moving the CISO:

- Move CISO out of IT, and report either to Legal, Risk or COO. But the CIO still needs to build secure assets, so replaces CISO with another role — creating conflict.
- And does that create a loss of respect if the CISO is not in the trenches keeping the enterprise secure (as well as a bad career move for the CISO?)

Especially when a CISO reports to the CIO, a CEO or COO-led Security Council that meets regularly brings the competing elements together to establish a security culture and resolve conflicts — a key recommendation from the executive interviews for the 2018 Mass Insight/ McKinsey "Collaborative Cyber Defense" Report produced for the ACSC on cyber mature organizations:

The previous report on cyber mature organizations went on to identify six characteristics to look for, starting with the senior executive committee:

- There is a cross-functional cybersecurity committee led by the C-suite at the enterprise level that meets quarterly
- There are consistent enterprise-wide policies and standards
- Cybersecurity responsibility is embedded across the operating model and business functions
- Investments are tied to top cyber risks
- Cyber team members are involved in key procurement and product development decisions
- Cyber risk culture management is viewed as a critical part of the security program

Some large organizations separate out three lines of defense.

Splitting the security operations and risk/policy and assessment functions into two lines is common at large financial organizations, for a "three lines of defense" structure.

A MODEL

Three lines of defense structure

FIRST LINE

- Business
- IT / security operations

SECOND LINE

- Chief Information Risk Officer, assurance/testing
- Chief Information Security Officer, policy / assessment

THIRD LINE

Internal audit

CIRO sits in parallel with CIO, CISO reports to CIRO, CIRO /CISO both partner with Technology operations/security function to implement policy and testing.

RECOMMENDATIONS

The Board's Strategic Risk Role

In their oversight role, Boards should assure that:

- Cybersecurity risks have been incorporated into strategic business decisions, including mergers and acquisitions
- A systematic risk framework and operational controls are in place, aligned with high priority risks and legal/regulatory/compliance requirements
- Through continuous assessment and performance metrics, those programs are producing more security.

Strategic Risk Frameworks & Metrics

Boards and management should:

- Both Boards and management should prioritize and support development of a new generation of digital risk and resilience-based frameworks (recommended in 2018 as well)
- Board and committee should push for continuous assessment results, beyond "check-the-box" updates in the context of operational frameworks. In particular, regular and continuing analysis on the real attacks occurring daily on company's IT systems, the performance of defenses against them and actions planned to improve on weak areas exposed in these attacks.

Management should:

- Use a limited number of operational metrics with Boards, and always connect them to business/financial risk
- Present risk visually and consistently, with risk registers, heat maps, etc.
- Use peer networks to explore emerging tools and metrics for digital resilience

The Evolving CISO Role, Management Structures & Board Governance

Boards should ask management how organizational structure might be impacting security and risk management, i.e.—does the CISO have the necessary authority? How are we creating a second and third line of defense, if it's not in the formal structure?

As originally reported by CISOs in the 2018 ACSC report produced by Mass Insight and McKinsey & Co.— Collaborative Cyber Defense, six signs of a cyber-mature organization are:

1. There is a cross-functional cybersecurity committee led by the C-suite at the enterprise level that meets quarterly
2. There are consistent enterprise-wide policies and standards
3. Cybersecurity responsibility is embedded across the operating model and business functions
4. Investments are tied to top cyber risks
5. Cyber team members are involved in key procurement and product development decisions
6. Cyber risk culture management is viewed as a critical part of the security program

BOARD QUESTIONS AND EFFECTIVE BOARD ENGAGEMENT

A PROPOSED PROGRAM

3 Strategic Oversight Responsibilities

Board members should assure:

1. Cybersecurity risks have been incorporated into strategic business decisions, including mergers and acquisitions
2. A systematic risk framework and operational controls are in place, aligned with high priority risks and legal/regulatory/compliance requirements
3. Through continuous assessment and performance metrics, those programs are producing more security

Board advisors, legal counsels and experts interviewed stressed that Board members must be able to demonstrate to themselves and regulators that they are challenging management. Despite traditional norms dictating minimalist Board minutes, there were suggestions that with new regulatory scrutiny, Board minutes for highly regulated firms will need to demonstrate that challenging discussions occurred.

Board "due care" for cybersecurity means taking reasonable steps to secure and protect assets, reputation, and finances. Recent Delaware court decisions have called upon directors to "ensure that companies have appropriate oversight systems in place."

Regulators are raising the stakes for Boards:

> "Regulators ask, what are you doing? Show me the investments and what has improved. Show me the management process to prioritize your investments. The Board must demonstrate that they are able to challenge the CISO — not sure Boards are listening."
>
> BOARD ADVISOR

Boards must understand/question risk frameworks, process controls, decisions about security investments:

> "As a Board member, I can't and shouldn't review every process control you are using but: What is the risk management system at the control level that you have put in place and how do you know it's working? I want to know management thought this through and has a system with metrics attached to it."
>
> BOARD MEMBER

> "What are the 10 most fundamental business processes that have existential connection to business outcomes? Are our security investments directly linked to those 10 processes?"
>
> SENIOR DATA OFFICER

Boards need evidence that the CEO and COO are personally driving a security culture:

> "How often are digital risks viewed and managed in the governance structure? How often is it discussed at senior management level?"
>
> BOARD ADVISOR

> "Talent gaps: Boards should ask about them. Most organizations have significant skills and capacity weaknesses and don't raise this with Boards. Where are we weak, how are we covering for that, are we compensating with vendors?"
>
> BOARD ADVISOR

Advisors and legal counsels cautioned: Board members will be unable to fulfill their oversight responsibilities without a full understanding of current compliance posture, as well as assessing current risks and strategic operational decisions.

5 Lines of Board Questions

Corporate Board members and advisors proposed five key lines of questioning for management:

1. **Compliance with legal and regulatory requirements — today and planning for the future**
   - **A comprehensive review and plan:** Are we satisfying our legal, regulatory and compliance obligations in every jurisdiction and planning for future requirements?
   - Does our broader business and technology roadmap account for emerging cybersecurity issues and legal requirements, including risks of AI, for example?
2. **Managing strategic digital security risk as business risk**
   - **Strategic risk and business planning:** Are cybersecurity and/or risk officers at the table for enterprise strategic planning — and for mergers and acquisition decisions?
   - **Risk frameworks and controls:** What are the fundamental business processes supporting our business outcomes, the risk framework and management system at the business process and control level and the metrics to track performance?
   - **Risk transference:** What risks have we transferred — contractually to third parties, through cyber insurance?
   - **Third parties:** What is our level of reliance on third parties — who are our most critical partners?
   - **Risk in an agile environment:** What are we doing to respond to an "agile" decentralized control environment and remote work? How are we implementing zero trust?
   - **Risk level agreements:** Have we put in place risk level agreements that confirm shared cross-functional executive risk responsibilities?
   - **Risk acceptance:** What risks are we accepting — are we comfortable with those?
3. **Security culture, organizational structure and the CISO role**
   - **Management security culture:** How are we communicating business responsibility for digital risk?
   - **CISO role:** What are the CISO's defined responsibilities? How have we resolved the inherent conflict where CISOs have both policy/assessment and operational responsibilities if we do not have three lines of defense (business/IT, risk policy/assessment, internal audit)? Does the CISO have both the necessary authority politically and the visibility into broader technology/enterprise programs required to secure them?
   - **CEO/COO leadership:** Does our CEO or COO lead a cross-functional executive council or regular review sessions to oversee cybersecurity and business continuity risk management and performance on at least a quarterly basis?
   - **Executive responsibilities:** Are there digital risk performance requirements C-Level executive jobs?

> "CISOs — many of them — and Boards are ignorant about legal/regulatory risks, which creates blind technical risks, so the board doesn't know what they don't know — they can't possibly ask the right questions.
>
> CISOs must learn to translate all operational risk into business continuity/financial risk — what parts of the business are affected if they have a problem."
>
> CORPORATE BOARD ADVISOR

Board Questions — Continued

4. Business continuity and resilience, planning and simulations

- **Simulations:** What incident simulations have we run — e.g. Ransomware, insider threat — and what corrections have we made based on them? Are Board members participating?
- **Shifting from continuity to resilience:** What systems are/aren't going to be operational in the face of attack? What have we done to compensate for those losses?
- **Business disruption target:** What is our maximum acceptable time offline for our most important business processes, and the financial impact associated with cyber incident scenarios?

5. Continuous performance assessment of people, process and technology

- **Strategic security investment bets:** Where have we over-weighted investment to defend against our most significant, existential threats/risks and how are we measuring the value of the additional investment (threat intel, 3rd party risk, new detection tools and programs)?
- **Framework:** What is our risk framework, what was the process to design it, are you confident it works — and why?
- **Benchmarks:** What is our benchmark for cybersecurity/business continuity performance — externally with peers or internally against business controls or both? What are our business continuity metrics?
- **Unsupported systems:** How many legacy systems do we have, how are we patching, what's our plan?
- **Defender team assessments:** Are we conducting red team, "live fire" exercises with our defender teams and benchmarking performance — are they improving? Can we benchmark performance against peers?
- **Talent and skills gaps:** With talent shortages in the market, what are greatest talent and skill gaps that threaten our security and business continuity — how are we covering for those with

Comprehensive industry resources on the role of Boards in cybersecurity include:

- National Association of Corporate Directors (NACD) Handbook on Cyber-Risk Oversight (2020 Edition)
- NACD Cyber-Risk Oversight Resource Center

Models for Effective Board Engagement

Building Board confidence with consistency in briefings — A mature model

Contributed by a Chief Information Risk Officer, global financial services firm.

Management needs to demonstrate a logical approach that the Board members can evaluate and hopefully gain confidence that the risks are appropriately and effectively managed. At the center of this approach is a systematic, defensible risk model that's been applied to set and track priorities.

A three-part approach, in the context of a three-year risk capabilities development plan:

1. **Risk framework** — we use the NIST CSF model to evaluate our maturity, benchmark against similar companies, and target specific areas for investment or maintenance.
2. **Ongoing control performance** — I use a set of metrics aimed at measuring control performance — when mapped to NIST CSF categories we can then report on progress aligned to our overall maturity targets
3. **Culture** — I use phishing simulation test results, which can also be benchmarked, IT secure code training and overall awareness training completion rates as well as employee engagement surveys with questions about risk awareness to gauge risk culture.

High-level risk registers are a critical component for Board governance:

- Follow a standard, consistent construct, with individual risk scenarios with both qualitative and quantitative impact, and very specific descriptions of threat.
- Helps Board focus on specific scenarios and understanding that investments can change values.
- Threat descriptions approached with combination of art and science (just the right level of detail).

Best in Class Incident Response — Global Financial Service Firm

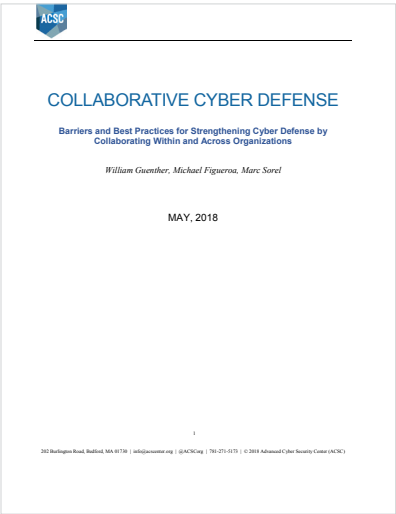
Financial Services Firm — Global Management Board oversees Local Entity Boards

- Entity-level tabletop exercises with board participation — monthly
- Members of Global CISO's response team participate in each entity simulation
- Each entity operation retains breach coach, legal counsel, and special negotiator (negotiator varies depending on type of attack)
- Specific scenario playbooks/policies, i.e. ransomware, detail protocol on decision-making roles by level, notification protocol, etc.
- Local operation simulations used as lab — results/recommendations/corrections are aggregated up to global management board for adoption

APPENDIX A

PRIOR COLLABORATIVE CYBER DEFENSE REPORTS

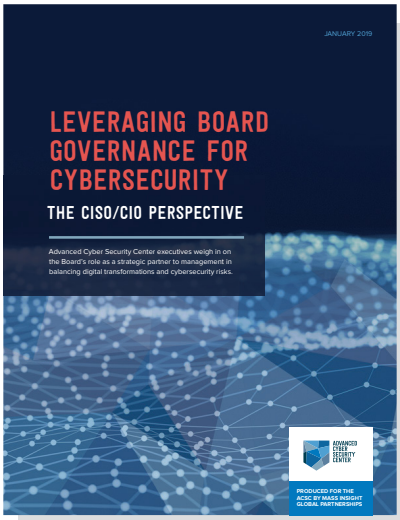
ACSC/Mass Insight Global Partnerships research series launched in 2018.



[Collaborative Cyber Defense: Barriers and Best Practices for Strengthening Cyber Defense by Collaborating within and across Organizations]

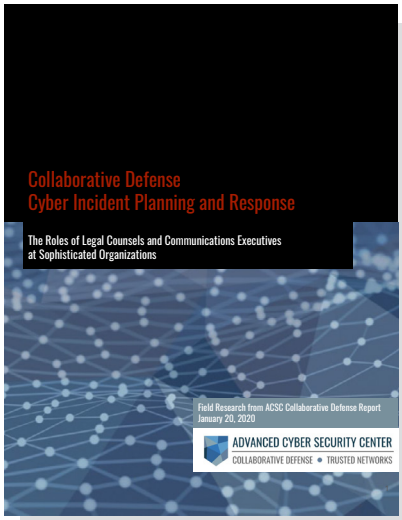
Produced in Collaboration with McKinsey & Co.

May 2018



[Leveraging Board Governance for Cybersecurity: The CISO/CIO Perspective]

January 2019



[Collaborative Defense: Cyber Incident Planning and Response]

January 2020

APPENDIX B

CYBER AND BOARD RESOURCES CITED BY PARTICIPANTS

Resources our interviewees cited as particularly useful, among the many sources available on this topic.

ARTICLES AND PAPERS

Boards will increase scrutiny of and expectations for cybersecurity
The Top 8 Security and Risk Trends We're Watching
Gartner, Nov 2021

Board oversight role a fundamental aspect of governance
A New Chapter in Cyber—On The Board's Agenda
Deloitte, June 2022
Authors: Mary Galligan, Carey Oven

Cyber is No. 1 business risk
PWC Pulse Survey: Managing Business Risks
PWC, August 2022

Evolution of the CISO role
Pulse Survey: The CISO in The C-Suite: Educator, Innovation Partner and Collaborative Risk Manager
Harvard Business Review Analytic Services, Sponsored by PWC, August 2022

Proactive steps for CISOs to build credibility with boards
How CISOs Can Wield More Power in Organizations
Wall Street Journal, December 2022
Authors: Anthony Vance and Michelle Lowry

SEC proposed rules, cyber risk implications
SEC Cyber-Risk Governance and Its Boardroom Business Resilience Implications
NACD BoardTalk blog, August 2022
Author: Chris Hetner

PROGRAMS

NACD: National Association of Corporate Directors
Digital Directors Network
World 50

APPENDIX C

OBJECTIVE/METHODOLOGY

Objective

The objective of this project is to provide an updated view on how Board and management strategic partnerships in cybersecurity governance have (and haven't) matured since the publication of our original 2018 research, and ***actionable insights and practical tools to advance the strategic oversight role of corporate Boards in cybersecurity governance.***

The findings and recommendations are a synthesis of the candid perspectives and generous contributions of Chief Information Security Officers (CISOs), Chief Information Risk Officers (CIROs), Chief Information Officers (CIOs), corporate Board members, advisors and legal counsels, and industry experts — and the report is in turn written for them and their peers to support the continuing development of the Board and management partnership governing cybersecurity

Methodology

- Interviews and an online survey, conducted under NDA, with 27 CISOs, CIOs and Risk Officers, corporate Board members and advisors, and legal counsels
- Focus groups with legal counsels, senior advisors across industries

While Board and management views expressed in the report are mainly representative of larger organizations, a survey of a broader range of organizations would no doubt highlight similar challenges in governing cybersecurity.

The conclusions and recommendations in this report are a product of interviews and focus groups conducted with ACSC members, partners and collaborators. Mass Insight Global Partnerships and the Advanced Cyber Security Center (not the member/partner organizations) are responsible for the content.

THE ADVANCED CYBER SECURITY CENTER (ACSC)

is a New England-based alliance that advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders - and provides professional opportunities for rising talent.

ADVANCED CYBER SECURITY CENTER

info@acscenter.org | www.acscenter.org