JANUARY 2019

LEVERAGING BOARD GOVERNANCE FOR CYBERSECURITY

THE CISO/CIO PERSPECTIVE

Advanced Cyber Security Center executives weigh in on the Board's role as a strategic partner to management in balancing digital transformations and cybersecurity risks.

ADVANCED
CYBER
SECURITY
CENTER

PRODUCED FOR THE
ACSC BY MASS INSIGHT
GLOBAL PARTNERSHIPS

ACKNOWLEDGEMENTS

The ACSC would like to thank the executives from **the following organizations who participated in interviews and/or surveys:**

- Bentley University
- Blue Cross Blue Shield of Massachusetts
- Carbon Black
- Everbridge
- Federal Reserve Bank of Boston
- Foley Hoag LLP
- Harvard Pilgrim Health Care
- Harvard University
- Liberty Mutual Insurance
- Manulife
- MIT Lincoln Laboratory
- MITRE
- MUFG
- National Grid
- Northeastern University
- RSA/Dell Technologies
- State Street
- T. Rowe Price
- Veracode
- Worcester Polytechnic Institute

We would also like to extend a special thanks to **Larry Clinton**, Internet Security Alliance, **Colin Zick**, ACSC counsel at Foley Hoag, and **Chauncey Holden**, recently retired CISO at Citizens Bank, for additional interviews and their broad industry perspectives.

And a special thank you to Charis Anderson and Kathryn Plazak, Consultants to Mass Insight, for their invaluable contributions to this report.

IN APPRECIATION

We dedicate this report to a special friend, outstanding cybersecurity leader and creative thinker, **Bob Nesbit**, retired senior vice president at MITRE Corporation and member of the Defense Science Board who also provided guidance for the report. Bob co-chaired an important 2016 Defense Science Board report on cybersecurity management produced for the Secretary of Defense that we have referenced here. And importantly, Bob provided the concept for the ACSC a decade ago and launched MITRE's longstanding leadership in this unique cross-sector threat-sharing and effective practice network in the New England.

COMMMISSIONED BY AND IN COLLABORATION WITH:

MICHAEL FIGUEROA, ACSC Executive Director

ABOUT THE AUTHOR

WILLIAM GUENTHER is Chairman, CEO & Founder of Mass Insight Global Partnerships, and Chair of the ACSC Board.

Mass Insight Global Partnerships organizes public-private partnerships in the Commonwealth of Massachusetts through collaborations connecting university, industry and government. Mass Insight produces research, publications and project support for the *Advanced Cyber Security Center,* which it launched as an independent nonprofit in 2011. This report follows *Collaborative Defense,* a May 2018 white paper by Mass Insight with support from McKinsey & Company.

www.massinsight.com

Mass Insight
GLOBAL PARTNERSHIPS

TABLE OF CONTENTS

REPORT OBJECTIVE AND METHODOLOGY

The objective of this project is to create an initial benchmark and method of evaluation for the evolving role of corporate boards in cybersecurity governance, initially through the perspective of Chief Information Security Officers (CISOs), Chief Security Officers (CSOs) and Chief Information Officers (CIOs), the primary networks supported by the nonprofit, member-based Advanced Cyber Security Center (ACSC).

Some very good work has been done on the role of boards in cybersecurity, including the excellent **National Association of Corporate Directors (NACD) Cyber-Risk Oversight Handbook, part of their Director's Handbook Series, prepared by the Internet Security Alliance (ISA).**

This first annual ground level research focuses on the CISO/CSO/CIO perspective to assess evolving effective practices (we will use CISO as short hand for CISOs and CSOs in the report), and launches a collection of "artifacts" — samples from actual board presentations as a practical tool for management (accessible to ACSC members).

Through 20 executive interviews of ACSC member CISOs and CIOs, an online survey of the executives, and interviews with four other experts, the project offers a perspective on the current state of board engagement in cybersecurity; describes the benefits and challenges to maturing board engagement; and includes recommendations for model board engagement, all organized around five key elements of a cyber-mature relationship between a corporate board and management that were drawn from the interviews. (While the overall sample size is small, the data derived from the surveys was echoed in the executive surveys.)

The report is based on a "focus group" of diverse organizations. It is intended to surface major themes for effective board engagement and through the five key elements create a structure for ongoing assessment of an expanding board role in cybersecurity. Subsequent annual reports will build on this baseline study. We should note that ACSC members are among the more sophisticated executives and organizations in their cyber maturity, which undoubtedly influences the findings presented in this report. A survey of mid-sized and smaller organizations would very likely highlight the depth of the challenge boards and management face in balancing digital transformations and cybersecurity.

This report follows an earlier Mass Insight report produced for the ACSC with the support of McKinsey & Co., titled *Collaborative Cyber Defense*.[1] CISOs in those interviews encouraged further research on emerging effective practices to engage boards of directors as collaborative partners in cyber defense.

> **20 executive interviews of ACSC member CISOs and CIOs, an online survey of the executives, and interviews with four other experts**

[1] https://www.acscenter.org/blog/collaborative-cyber-defense-survey-of-top-cisos-shows-roadmap-for-improvements

SUMMARY

In 2014, one third of North American firms did not have a Chief Information Security Officer[2], according to an annual survey by PWC, and the U.S. government did not appoint its first Chief Information Security Officer until 2016. By 2018, many companies still didn't have key roles related to cybersecurity, such as CISOs or chief security officers, and even at companies that do have those roles, less than half think they have the right people in them, according to a 2018 global survey of executives conducted by PwC.[3]

Even five years ago, the focus was still too often on securing the perimeter when the attackers had already penetrated the organization; today, experts acknowledge the perimeter is "largely dead." Multiple ACSC CISOs noted that an organization's people — internal employees and those of the external partners and suppliers — are a new perimeter.

The ongoing digital transformation we see across organizations in *all* sectors — implementation of new technologies and IT platforms; reliance on cloud services and cloud-based vendors; the move to mobile and the Internet of Things (IoT) with vastly increased numbers of connected devices — is creating more complexity and new challenges for institutions seeking to manage their cyber risk.

[2] *Defending Yesterday — The Global State of Information Security,* PWC, 2014. Accessed at: https://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf

[3] PwC, *Digital Trusts Insights,* Fall 2018. Accessed at: https://www.pwc.com/us/en/services/consulting/assets/journey-to-digital-trust.pdf

To compete, organizations will accelerate digital transformations — after all, continued digital innovation is driving growth and driving down costs. That means corporate boards need far more expertise in digital risk and security and will require new digital-risk frameworks to manage the strategic tension between digital innovation and organizations' cybersecurity risks.

Today, organizations increasingly face more — and more sophisticated — cyber attackers, even as they have more value at stake and an increasing gap between offensive and defensive capabilities, as we reported in Collaborative Cyber Defense[4] earlier this year. Cybersecurity is a now a major business risk — and one that is dynamic and changing in real time without the historical data that support other risk decisions.

In this new and evolving cyber risk landscape, management must constantly adapt and improve its approach — and so too should boards if they are to be active governance partners in what the ACSC refers to as "collaborative cyber defense," the recognition that defending against cyber attackers requires collaboration across organizational functions and between organizations.

Interviews with the four experts and 20 ACSC CISOs and CIOs representing organizations from a range of sectors (and survey results from many of those cyber leaders) shed significant light on the current state of board engagement in cybersecurity. There were, of course, differences based on sector and context. In particular, university boards, and those organizations where the CEO also serves as the board chair, operate in ways that are specific to those contexts. On the whole, however, the CISOs and CIOs we interviewed and surveyed painted a common picture of board engagement organized around five key elements of the board-management relationship for which we identified related findings and recommendations.

These findings reinforce the message from the 2018 PWC global survey: "Most corporate boards are not proactively shaping their companies' security strategies or investment plans."[5]

> "Most corporate boards are not proactively shaping their companies' security strategies or investment plans."
>
> PWC, DIGITAL TRUSTS INSIGHTS, 2018

[4] https://www.acscenter.org/blog/collaborative-cyber-defense-survey-of-top-cisos-shows-roadmap-for-improvements

[5] PwC, Digital Trusts Insights, Fall 2018. Accessed at https://www.pwc.com/us/en/services/consulting/assets/journey-to-digital-trust.pdf

FIVE KEY ELEMENTS

of the Board-Management Relationship, Related Findings and Recommendations

> “Boards should be able to ask questions management hasn’t thought of.”

The Board’s Strategic Risk Role

The board’s role on cybersecurity, in line with its overall function, is to provide strategic guidance and help guide management’s strategic risk judgments.

FINDING

In most cases, the **board partnership with management is still “at an early stage” or “maturing” phase.**

RECOMMENDATIONS

Build board confidence in cyber operations and **frame strategic discussions around key risk issues and questions.**

Building Board Cyber Expertise

Boards will need to develop more cyber expertise to partner with executives and ultimately “boards should be able to ask questions management hasn’t thought of,” as one executive put it.

FINDING

Most **boards do not yet have sufficient expertise in technology or cybersecurity** to serve as strategic thought partners on cyber risk.

RECOMMENDATIONS

Recruit board members with broad digital/technology expertise; develop **an annual curriculum of cyber briefings;** provide **ongoing training; use third party assessments.**

Aligning the Board Role and Corporate Structures

To fulfill their strategic risk role, boards need a holistic and dynamic understanding of an organization's cybersecurity risks and responsibilities. The board also needs direct access to CIOs, CISOs and risk officers, along with all the business executives responsible for their own data risks in a distributed accountability model.

FINDING

Placing **cybersecurity in an organizational silo at the operational or board level makes it difficult to develop a holistic and nuanced understanding of cybersecurity's impact on business risk.** Boards generally spend one meeting a year on cybersecurity, delegating responsibility to the risk or audit committee, leaving the full board with little time to develop expertise on the cyber risks.

RECOMMENDATIONS

CISOs and CIOs should present jointly at board meetings to provide a holistic view of digital strategies and security. Boards as a whole should review **cybersecurity more consistently as a business risk;** the risk or audit committee should be used for **more frequent (at least quarterly) cyber reviews.**

Overseeing Cybersecurity and Digital Transformation Budgets

Boards should review digital transformations as a whole, with cybersecurity as an element of overall IT-related decisions.

FINDING

As cybersecurity budgets continue to grow, two issues have arisen. The first is budget fatigue, a frequent area of concern shared by CFOs, CEOs, and boards. The second is when **cybersecurity investments are seen as "separate" from IT investments and hence do not represent a complete picture of security spend.**

RECOMMENDATIONS

Present digital transformation budgets as a whole, with **cybersecurity investments as an element of overall IT-related decisions about where to invest in growth and security.**

Developing Cyber Risk Metrics and Measurement

Boards—and management—require cyber risk frameworks that provide a means to make informed risk judgments.

FINDING

Cybersecurity hasn't yet developed the standard, historically proven risk frameworks that financial and audit risk functions have refined over decades, leaving management to rely on NIST and other operational frameworks and metrics that can distract boards from the strategic issues they should consider.

RECOMMENDATIONS

Boards should prioritize and support senior management's **development of a new generation of outcome-based cyber risk management frameworks,** and in the meantime, executives should use only a few operational metrics with boards.

While there are challenges in the current state of board partnerships with management in cybersecurity, there are significant opportunities for management to work with boards to enhance their cyber maturity focused on the five key elements identified and recommendations from executives and experts interviewed.

The need has never been more pressing. Boards are responding to the public evidence of cyber risks, such as the increase in attacks targeting North American critical infrastructure, and the recent Meltdown and Spectre vulnerabilities, and to the priority management has placed on the cyber challenges to their organizations.

Boards have a particular role to play prioritizing management's development of new cyber risk frameworks that will support management's responsibilities and the board's governance of the organization, its strategy and risk tolerance.

As boards continue to develop expertise and maturity, it is important to assess the evolving board/CISO relationship and role in governance to ensure organizations adopt leading models for effective governance practices, and to single out cyber-mature boards as true strategic leaders for digital transformation and cybersecurity risk.

BOARD-MANAGEMENT RELATIONSHIPS:

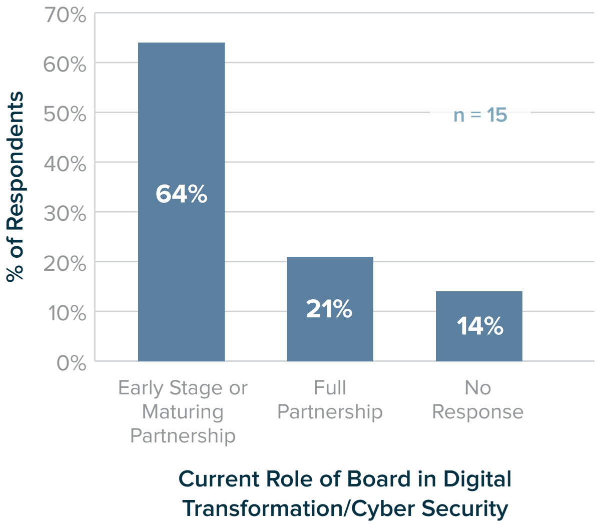
FIVE KEY ELEMENTS AND FINDINGS

The Board's Strategic Risk Role— Currently "Early Stage" or "Maturing"

The last five years have been an educational period for many boards. ACSC executives report that, in general, they have focused on cultivating cyber expertise through annual management briefings for the full board, quarterly briefings with the risk or audit committees, and periodic third-party briefings and independent security assessments.

Yet despite this focus, **many boards are still not where they need to be to become full governance partners in digital technology and cybersecurity. Most executives report their boards are "at an early stage" or "maturing" in governing cyber-security and the digital transformation of their organizations,** according to interviews and the online survey data. Board capacity and expertise on cybersecurity varies widely, from "awareness" to in a few cases, "sophistication."

MOST RESPONDENTS CHARACTERIZED BOARD PARTNERSHIP AS "EARLY STAGE" OR "MATURING"



Survey respondents were asked to characterize the current role of their boards in managing the digital transformation and cybersecurity of their organizations as one of the following:

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: 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.

What Boards Should Look For: Key Elements of a Cyber-Mature Corporate Culture

As reported by CISOs in the ACSC-Mass Insight report *Collaborative* Defense, corporate culture vis-à-vis cybersecurity is critical to reducing an organization's cyber risk. Organizations should continue to measure their "cyber-maturity" against the following characteristics of sophisticated cybersecurity programs:

- 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.

From: Collaborative Cyber Defense: *Barriers and Best Practices for Strengthening Cyber Defense by Collaborating Within and Across Organizations,* William Guenther, Michael Figueroa, Marc Sorel, May 2018 (https://www.acscenter.org/blog/collaborative-cyber-defense-survey-of-top-cisos-shows-road-map-for-improvements)

University Boards Can Be Collaborative Partners

As compared to the commercial world, **boards appear to play a different role within universities, where boards and management often collaborate on what would be considered operational issues for commercial boards.** At some universities, the board's technology expertise is tapped for major strategy and even some operational decisions when it is available.

One university executive also noted that "universities have different rules than commercial companies — they need to be more transparent with their community." Finally, at universities, faculty have the power to challenge or block recommendations — like a security process that would inconvenience them — so the board is an important ally that management can leverage to help overcome obstacles, another university executive noted.

This has led **many boards and their risk and audit committees, where cybersecurity oversight is generally delegated, to focus largely on compliance and regulatory issues and on cyber incidents reported widely in the media.**

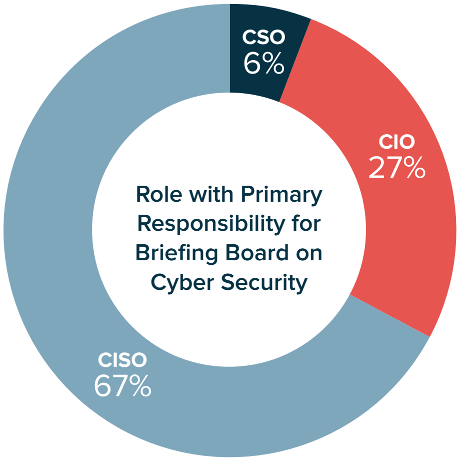
In the experience of our report sample, **it appears that board discussions have rarely played a role in shifting cybersecurity risk decisions or changing overall cyber strategies.** Nor is it evident that boards have been presented with cyber risk decisions in a way that would facilitate their guidance, compared to, for instance, the way boards often guide market growth strategies or financial risk considerations.

Building Board Cyber Expertise — More Cyber/Technology Capacity Needed

Most executives in our sample reported that boards are being briefed on cybersecurity issues, but don't currently have the capacity or expertise to be full governance partners. **Conversations are, in essence, one directional, with many boards not yet sophisticated enough to "ask questions that management hasn't already thought about,"** as one executive put it. This limits boards' abilities to serve as strategic thought partners for management.

IT IS MOST COMMON FOR CISOS TO BE RESPONSIBLE FOR BRIEFING THE BOARD ON CYBERSECURITY ISSUES.

n = 15



Full boards, as well as the audit or risk committees, need a baseline level of expertise on cyber issues sufficient to apply to the business risk at hand. As one executive noted, "they need to know the vocabulary and the framework, what's important and what is not, where to focus." *And* they need a risk framework that guides their thinking and discussions.

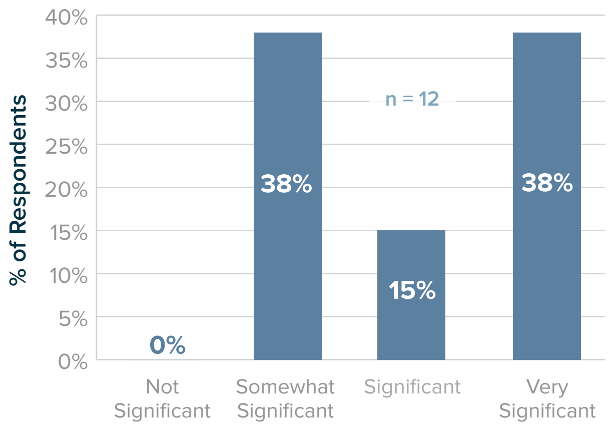
"The effectiveness of presentations is limited if the board doesn't understand the technology," said another executive. Absent a baseline level of expertise on cybersecurity and digital technology among board members, senior management may find they need to spend valuable time on explanations and background information.

Executives cautioned that **there is a shortage of individuals with the right cyber background available to serve on boards.** Board members are in many cases CEOs or former CEOs of other organizations. Few CEOs serving on boards have completed successful digital transformations in their own organizations, and fewer still have deep expertise in cybersecurity as a relatively new challenge.

> "[Boards] need to know the vocabulary and the framework, what's important and what is not, where to focus."

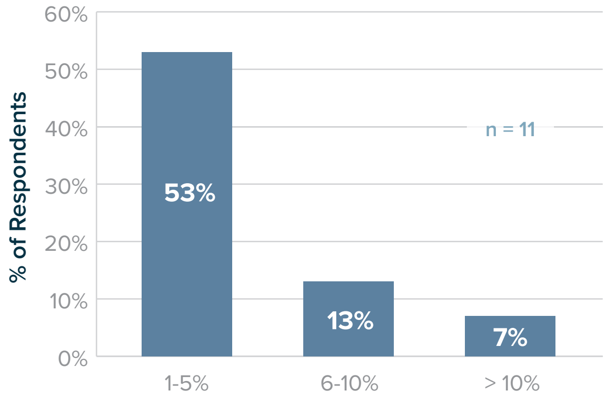
Aligning the Board Role and Corporate Structures — Too Many Opportunities for "Silos"

OVER 50% OF SURVEY RESPONDENTS SAID THEIR BOARDS VIEWED CYBER AS A VERY SIGNIFICANT OR SIGNIFICANT FACTOR IN BUSINESS RISK



Degree to which board views cyber as factor in business risk

BUT MANY FULL BOARDS MEET ONLY ONCE A YEAR ON CYBERSECURITY AND ALLOCATE 5 PERCENT OR LESS OF FULL MEETINGS TO CYBERSECURITY



Percentage of full board meeting devoted to cybersecurity

When managed effectively, cybersecurity is an embedded business function with distributed responsibility for information security across the organization, not simply the responsibility of the CISO.

Yet **the challenge of different — and overlapping — functions and departments that touch cybersecurity can make it easier to "silo" cybersecurity as the function of one department and one budget. This can complicate a board's ability to develop an accurate and holistic understanding** of an organization's cybersecurity and cyber risk, and is especially true if each function is reporting to the board separately.

While boards' awareness of cybersecurity has increased in recent years, the interview and survey data show that **full boards spend relatively little time on cybersecurity, usually at one annual briefing,** with quarterly meetings of the delegated committee responsible for oversight on average, although sometimes less, creating a silo on the board.

This suggests a fundamental disconnect between the importance boards are placing on the issue and the degree to which they are delegating the challenge to a committee. In one example, an executive reports quarterly to the board — but what's scheduled for 15 minutes often turns into 60. This points to the need for more frequent agenda slots to build the expertise of the full Board, and for discussions regarding the trade-offs between growth and security embedded in digital strategies and the risks the organization can afford to take or not.

Most executives in our sample advocated for deeper *overall* corporate board expertise and training in technology and digital transformations as opposed to recruiting one board member with specific cybersecurity background, upon whom the rest of the board relies. There is a concern that a single board member with cyber expertise, representing only one perspective, may present opinions that carry too much weight.

Our executive interviews also revealed **debates about the "optimal structure" for senior management roles related to cybersecurity.**

Despite indications that CISO positions have generally been accepted as necessary, there continues to be disagreement as to where they should fall in an organization chart. **Some executives felt strongly that the CISO should report directly to the CIO, while others thought they should be part of the risk function and report directly to the CEO.** The latter position suggests that security reporting to IT represents an inherent conflict of interest, as CISOs might be assessing the weakness of a CIO's organization. This position is disputed by some leading CIOs but supported by a recent report on board oversight of cybersecurity by the Institute for Business and Information Technology.[6] In either case, some corporate boards and their committees are asking the security executive to meet with them alone periodically to assure they are getting objective feedback.

The topic of internal management structures is an area where one outside expert expects boards will begin to examine closely. "There is a good deal of board interest in re-considering corporate management structures" to respond to the digital transformations and cybersecurity, this executive said. "Digital transformations will lead to flatter organizations."

[6] *Implementing Board Oversight of Cybersecurity: Advice for Boards Just Starting Out,* Richard Y. Flanagan, Janet L. Yeomans. The Institute for Business and Information Technology, March 2016.

Overseeing Cybersecurity and Digital Transformation Budgets — Increased Cyber Spend Can Lead to "Budget Exhaustion"

All but one survey respondent indicated that their cybersecurity budgets have increased significantly over the last five years, with the range of growth between 33 and 150 percent. Yet, for most respondents, security spend still represents a relatively small portion of their organization's overall IT budget. "There has been a much greater willingness to fund cybersecurity" although many firms are reaching "a degree of budget exhaustion," one expert with broad industry exposure noted.

Despite the sharp increases in security budgets, they give an incomplete picture of an organization's true spend on security-related resources, since investments that enhance security are often embedded in broader IT budgets.

Measuring and tracking security budgets alone is not sufficient for assessing an organization's commitment to improved security. Investing to upgrade outdated legacy IT infrastructure, for example, might be the most important step an organization could take to improve its cybersecurity, and yet would not necessarily be categorized as a "security spend."

At the same time, it can be difficult for executives to "sell" the benefits of cybersecurity investments. As one executive noted, "it's hard to sell an empty space." Organizations spend a lot of money, and all they have to show for it is that "nothing happened," he continued. This, of course, is the desired result — but it's not very visible, in the way other significant investments might be.

Developing Cyber Risk Metrics and Measurement— Lack of Historically Proven Frameworks

Boards' less than full governance partnership has been exacerbated by **the lack of historically tested and sophisticated cyber risk management frameworks of the type that exist for other corporate risks.**

Guidance such as the U.S. government's National Institute of Standards and Technology (NIST) Risk Management Framework elements now serve as a starting place for management and boards. Executives interviewed, with a few exceptions, use the NIST framework internally and with boards. However, they broadly agreed that boards must understand that most existing frameworks, such as NIST, are "operational check lists" focused on inputs, not on performance outcomes, and represent minimum standards—and as such do not provide a robust cyber risk framework.

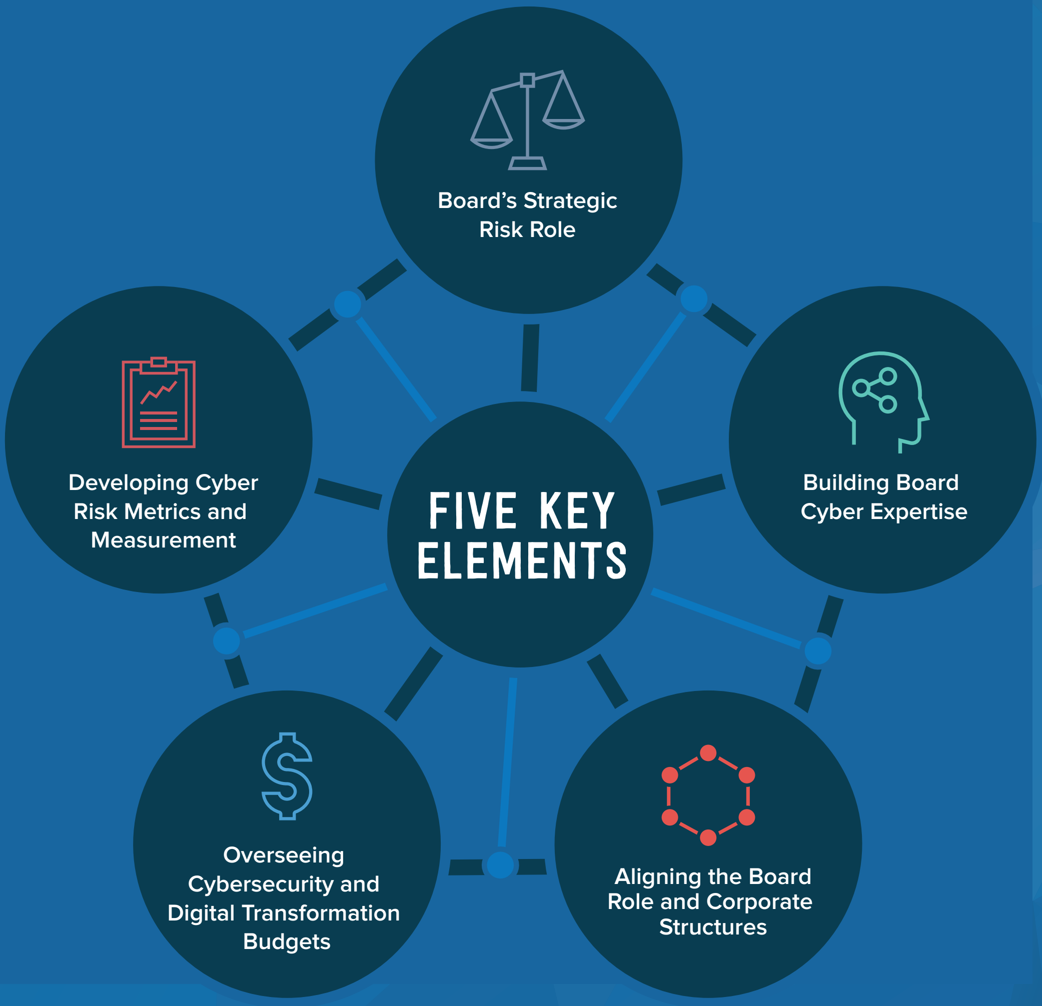
Unfortunately, cyber risk hasn't yet evolved into a standard risk management function in the way financial and audit functions have, and in some cases, board members have not yet recognized that cybersecurity involves making decisions about the relative importance of certain assets and a tolerance for the risk to them. "Over the past few years we have seen a fairly dramatic uptick in Board activity around cybersecurity as awareness has grown. But there is a big difference between awareness and understanding. Too many board members still talk about defending the perimeter and mistakenly refer to a zero appetite for cyber risk," an executive said.

> "Over the past few years we have seen a fairly dramatic uptick in Board activity around cybersecurity as awareness has grown. But there is a big difference between awareness and understanding."

BOARD-MANAGEMENT RELATIONSHIPS:

EXECUTIVE RECOMMENDATIONS

The above findings in the context of the five key elements of the board-management relationship helped summarize the current state of the board role on cybersecurity, and the strengths and weaknesses executives saw in their boards' progress toward cyber maturity. The five elements, taken together, and their associated recommendations, are useful in framing a board's journey toward cyber maturity and full partnership with management. It is important to note that these elements are interconnected, and should be taken as a whole, not in isolation, so as not to exacerbate the tendency toward cyber "silos" noted above.


FIVE KEY ELEMENTS

Board's Strategic Risk Role

Building Board Cyber Expertise

Aligning the Board Role and Corporate Structures

Overseeing Cybersecurity and Digital Transformation Budgets

Developing Cyber Risk Metrics and Measurement

THE BOARD'S STRATEGIC RISK ROLE:

The board's role on cybersecurity should be strategic and risk-focused in the context of digital choices, with a broad understanding of the cyber function in the larger business context, and without the distraction of too many operational details.

Multiple interviewees articulated key questions for boards to focus on, the essence of which are:

1. What are the cyber risks to our organization and what specific assets are at risk?
2. What is the organization's strategy to mitigate those risks, relative to the value of those assets, and how is success being measured?
3. Is the organization well prepared for a major cyber incident?

These questions can be treated at a high level, but they presume a level of understanding about an organization's cybersecurity operations that too few board members have developed, according to the cybersecurity and IT executives interviewed.

Boards considering an organization's strategic risk might ask further:

What "crown jewels" do we have to protect that are essential to our business?

How secure are we against the most dangerous cyber threats and what would the damage be if we failed to successfully defend against them?

What threats give us the most trouble and what are we doing to improve? Which elements of our defense suite are working well against real threats? Which defensive elements aren't working well? How far into our systems are the attackers penetrating?

ROBERT NESBIT

Retired Senior Vice President,
MITRE Corporation and Member,
Defense Science Board

When a CEO has a "split lens"

It's worth noting the distinction between organizations where the CEO serves as the chairman of the board and those with an independent chairman. At the former, the board chair is, by virtue of his/her internal management role, immediately aware of cyber incidents and much more aware of cyber issues within the organization. The CEO/chair has a "split lens," so to speak, which in turn can influence the way the board as a whole is involved in or considers those issues — or even what issues are raised at a board level.

One executive noted that "their CEO is also their Board Chair and sits on the Security Steering Committee...so he identifies key issues to bring to the board." When the board chairman is independent, he or she operates solely with the "strategic risk and oversight" lens, and thus a different relationship exists.

A board's role is to ask the strategic questions and guide and approve high-level decisions about risk — and then step back and trust senior management to operationalize this strategy. Management can support this focus by **framing, or anchoring, communications with the board around risk, not security controls.** This has the added benefit of helping to eliminate the security silo, and incorporating cyber risks into existing governance functions.

At the same time, a board's ability to function effectively in this role depends on the confidence it has in current operations, which requires initial briefings and updates on what's in place and ongoing reference to cybersecurity systems performance. Absent that confidence, boards may find it difficult to "step back" from operations and focus solely on risk tolerance and strategic opportunities. Boards "need an organizational risk profile, and then [can work from that] to achieve the agreed upon level of risk," one executive said.

Some cybersecurity executives said **they wanted their boards to "put them on the spot," asking questions such as: Do you have what you need to do your job?** However, this is another area where a board's ability, or willingness, to do so may rely on its own comfort level with cyber issues.

> Some cybersecurity executives said they wanted their boards to "put them on the spot," asking questions such as:
>
> "Do you have what you need to do your job?"

BUILDING BOARD CYBER EXPERTISE:

A board should have a baseline knowledge of cybersecurity — enough to be able to ask questions management hasn't already thought of.

As we noted above, most boards need deeper expertise and knowledge on both digital strategies and cybersecurity challenges in order to fulfill their primary role of risk oversight and governance. While it might be possible to "leap frog" the need for baseline training by recruiting board members with cyber expertise, executives cautioned that there's a shortage of individuals with cyber background available to serve on boards. (Indeed, this reflects the general shortage of cybersecurity professionals at all levels.) Instead, executives call for more board members who have successfully led technology strategies at their own organizations and for a board commitment to grow this experience from within. Interviews and survey results outline a four-point plan for building expertise:

1. **Broader board digital expertise versus a designated cyber board member:** While designating a "cyber seat" may be a way to seed the board with expertise, some executives noted that approach may place disproportionate weight and authority on one person's perspective. Executives encourage broader board technology expertise to support digital strategies and transformations, so that multiple board members bring informed perspectives to bear and ask the kind of challenging strategic questions that too often may be missing from current board discussions.
2. **An annual cyber curriculum for boards:** To assist boards in acquiring cyber expertise, forward-looking executives have informally organized an ongoing "cyber curriculum" — or "road map" for expertise — for board briefings that provides in-house development opportunities for board members. This curriculum is designed to move board members along a continuum, starting with purely educational topics and then moving into more analytical or strategic issues. This can help ensure a baseline level of expertise across board members, at least at the committee level, which in turn allows management to target their presentations more effectively.
3. **Outside cyber training for boards, and especially for risk/audit committees:** Beyond baseline training from security executives, many executives recommended ongoing board training — delivered either by internal staff or external vendors — to help keep pace with an evolving cyber landscape. "It's important to do continuous training for boards — especially important for specific committees, such as audit," one executive said. Another executive concurred: "Training is important, and should be a requirement."
4. **Board cyber consultants and independent board-management cyber audits:** Many executives endorse bringing external cyber experts — consultants, independent auditors, etc. — into the management-board relationship in order to validate and assess an organization's current cybersecurity strategy and performance. This is a less direct, but still valuable way to build board expertise, as these external consultants or evaluators can "model" for board members the types of probing, difficult questions that board members should be asking of senior management. "The important goal is to ensure a board's access to cybersecurity expertise," one expert noted.

> "Board training is important and should be a requirement."

ALIGNING THE BOARD ROLE AND CORPORATE STRUCTURES:

Boards need a holistic and dynamic understanding of an organization's cybersecurity responsibilities and regular direct access to CISOs and risk officers in conjunction with CIOs and other executives.

Cybersecurity executives underscored how critical it is that corporate functions related to security demonstrate strong internal collaboration to present to the board a holistic picture of an organization's security and IT functions in the context of business strategy. "Risk has to be understood and owned by the entire enterprise, every executive in the organization," one executive said. Management should be building leadership coalitions within the organization around cyber risk.

For many executives, this took the form of—at a minimum—having the CIO and the CISO do joint presentations to the board. Organizations "need to have a strong alignment between cyber and the broader corporate technology briefing, regardless of where the CIO and CISO report," one executive said. Another executive noted that "having the CEO and CFO in the room as the presentations and discussion occur helps ensure their support of any cyber initiatives." As we noted above, the topic of internal management structures is one where boards are increasingly likely to take an active interest.

At the same time, executives urge **boards to establish a clear internal structure and ownership for how, when, and who on the board will receive cyber updates and review digital strategies and risk.**

Cybersecurity should be assigned to a standing committee (e.g., enterprise risk, audit, or even a separate committee focused explicitly on security) that meets at least quarterly. Bimonthly meetings with the risk committee have produced an even stronger working relationship in one exceptional case in our sample. In this case, a bimonthly meeting schedule with the risk committee allowed the security executive to move from a 50-page report used by the previous executive to a five-page summary, while increasing the quality of discussion.

A regular—and frequent—meeting schedule will allow the board committee to develop deeper expertise in cybersecurity as a business risk decision and keep pace with the dynamic and evolving nature of the cyber landscape.

Having more frequent meetings allows meetings to become more focused and sophisticated, keeps cybersecurity front of mind in conjunction with choices about digital management and innovations, and brings cyber risks to the same level of attention given to other business risks.

> "Risk has to be understood and owned by the entire enterprise, every executive in the organization," one executive said.

OVERSEEING CYBERSECURITY AND DIGITAL TRANSFORMATION BUDGETS:

Boards should review digital transformation budgets as a whole, with cybersecurity as a specific component of overall IT-related decisions.

It is important to present to boards the interrelated nature of security investments and broader IT and technology commitments—allowing boards to understand the balance of digital growth strategies and enhanced security through a multi-year strategic IT plan. Some investments—like replacing old legacy systems—will appropriately be categorized as IT, but are a wise investment in an organization's overall cybersecurity. Security risks, in fact, can be used to justify operational and business enhancements.

"Tracking investment in replacing outdated legacy systems over time can be a valuable tool for management and boards," one executive noted.

The embedded nature of security spending also reinforces the importance of internal executive collaboration, and building security coalitions within an organization, to ensure that an organization's CISO and CIO (and other related functions) are aligned about budget priorities.

Finally, as a note on the risks of benchmarking industry security budgets, the ambiguity around what is, or is not, categorized as cybersecurity spending **can make it difficult to compare total spend across organizations, as budgets are allocated differently.** For example, in some organizations, the CISO "owns" the perimeter security, and at others, he/she might not. That said, within a given organization, **tracking budget trends over time—and aligning those trends to progress against key priorities—will contribute to an understanding of an organization's cyber maturity.**

"Tracking investment in replacing outdated legacy systems over time can be a valuable tool for management and boards," one executive noted.

DEVELOPING CYBER RISK METRICS AND MEASUREMENT:

Boards should prioritize and support senior management's development of next generation cyber-risk frameworks that take an outcome-based approach to measuring cyber risk.

Current Industry Standards and Frameworks Have Limited Applications in Making Choices About Risk

Executives cited a range of industry standards, frameworks, and metrics they use with their boards. These are operational in nature and limited in value for the boards' governance role as discussed in the prior Findings on "Cyber Risk Metrics and Measurement."

- NIST Risk Management Framework
- ISO Controls
- Hitrust (healthcare industry)
- CIS
- Gartner Maturity Index
- SANS20
- Bitsite
- CSF
- FFIAC Standard
- SOC2 certification
- Peer data from FSARC and other organization

There is an opportunity for boards to prioritize for management the challenge of how best to assess and measure cyber risk, and how to translate that approach into a sophisticated risk framework. Some boards are already embracing this leadership role, as one expert noted "an increasing desire at the board level to look at cyber-risk assessments to replace the check-list models like NIST."

Developing these types of sophisticated measurements and frameworks is increasingly important in today's evolving cyber landscape. As we noted earlier in this report, once sacred cyber maxims — e.g., protect the perimeter — are no longer relevant in an increasingly connected (and mobile) digital world, where companies are relying more and more on third-party vendors (and are accountable for those vendors' own security).

Executives broadly endorse the conclusion that using too many metrics can become "noise" and lead a board down an unproductive rabbit hole: "Metrics can be misleading," as one executive noted. At least one security executive, who has frequent meetings with the board risk committee, does not use any metrics in his briefings for that reason.

Boards and management should start by identifying the most important threats, and then select metrics that can illuminate progress in mitigating risk from those threats. In this way, metrics, whether presented as stand-alone data or as part of a summary dashboard, can serve as the starting place for a more sophisticated and nuanced discussion about risk and strategy. It's worth noting, though, that the value of metrics to guide these types of discussions is dependent on boards' expertise and knowledge; as one executive said, "[You] first need to educate the board before using metrics."

Using selected metrics **also can help create alignment between risk and investment.** By prioritizing those metrics aligned to the most important threats, boards and management can more effectively use metrics to drive the most effective spending decisions and to redirect funding and resources to mitigate the most critical vulnerabilities.

Finally, the right (but limited) number of metrics can help establish trust between a board and management on cybersecurity functions. For boards to stay at a governance, or oversight, level, they need to trust that management is making the right operational decisions. Selected metrics used in developing board confidence can help management establish the validity of its operational approach.

Management performance reports from Lockheed Martin, Goldman Sachs and the Australian Signals Directorate (the Australian NSA) were cited as exemplary in a 2016 Defense Science Board report co-chaired by Bob Nesbit, the former MITRE senior vice president who inspired the creation of the ACSC (see appendix A). The details of these charts may be too operational for every board update, **but by reviewing the performance reports, boards can develop a better understanding — and trust — for how management is assessing its own performance.**

Executives generally conclude that board presentations should ideally combine a few operational performance frameworks with new outcome-based cyber risk metrics that allow for a deeper understanding of relative risks. "Boards need enough detail to provide the feedback and support we hope to get," one executive said.

Operational Metrics Cited by Executives Make the Case for New Cyber Risk Frameworks

Our survey results identified metrics executives use in reports to boards and underscore their operational focus (in order of frequency cited):

1. Number of breaches per time period
2. Industry benchmark comparisons (i.e. are processes consistent with industry standards?)
3. Compliance metrics on basic cyber hygiene (passwords, access, phishing results)
4. Number of prevented attacks
5. Security ratings by independent sources
6. Percentage of IT budget spent on security
7. Mean time to patch after an update is released
8. Percentage of software running most recent version

> "Metrics can be misleading."
>
> "[You] first need to educate the board before using metrics."

CONCLUSION

Through this first ACSC annual report on the role of corporate boards in cybersecurity, our goal has been to begin to track evolving practices at a granular level to complement the broad scale guidance from the NACD's Handbook and other sources. This initial baseline will be refined over time to evaluate the cyber maturity and effectiveness of board-management relationships and provide important guidance to senior executives and their boards.

According to the executives interviewed for this report, boards are responding to the public evidence of cyber risks and the priority management has placed on the cyber challenges to their organizations. As cyber risk is still a relatively new risk at scale, organizations are still finding their way to incorporate cybersecurity risk into board governance roles.

The digital and cyber landscape is constantly shifting, and each year there are new threats for which management lacks historical trend data that would inform cyber risk management models. Boards have a critical role to play as a partner in what ACSC refers to as "collaborative cyber defense," especially in supporting the development of new risk frameworks that will help management's oversight of cybersecurity and the board's cybersecurity governance.

APPENDIX A:
Leading Operational Performance Charts, Measuring Defensive System Performance

From the Defense Science Board's Task Force on Cyber Defense Management, September 2016 | Robert Nesbit and Lou Von Thaer, Study Co-Chairs

FIGURE 1: LOCKHEED MARTIN PERFORMANCE CHART

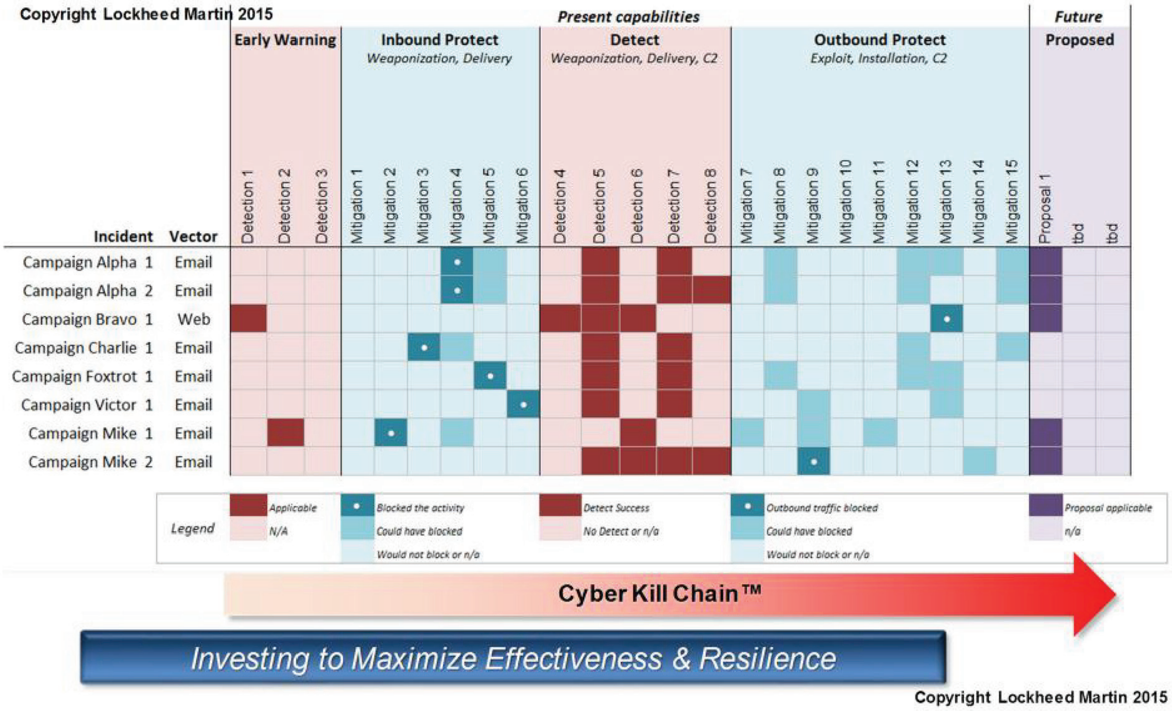
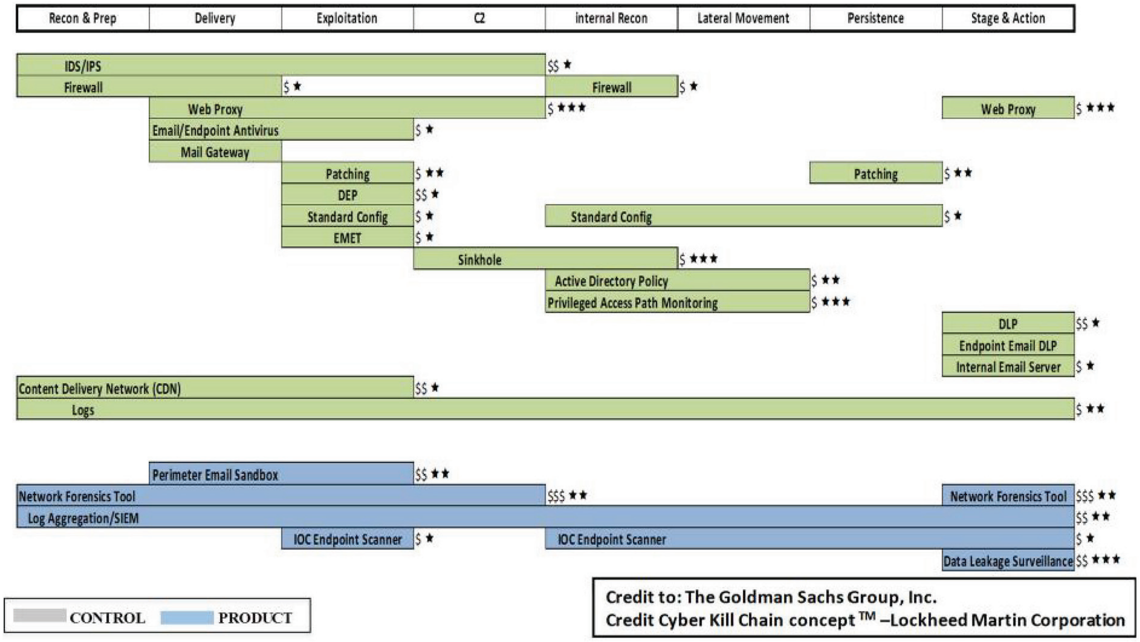
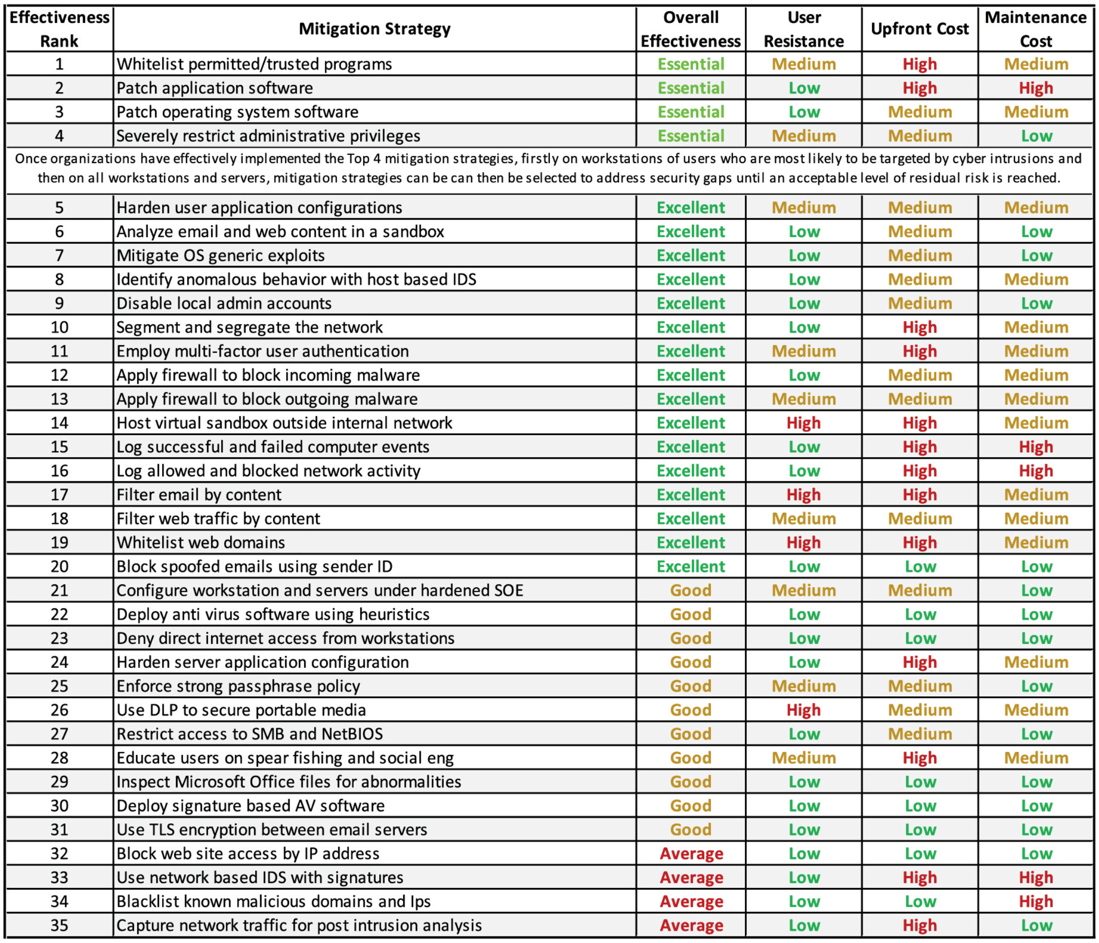


FIGURE 2: GOLDMAN SACHS PERFORMANCE CHART



Credit to: The Goldman Sachs Group, Inc.
Credit Cyber Kill Chain concept ™ –Lockheed Martin Corporation

FIGURE 3: AUSTRALIAN SIGNALS DIRECTORATE ANALYSIS TEMPLATE FOR ANALYZING NIST ELEMENTS PERFORMANCE



Effectiveness Rank	Mitigation Strategy	Overall Effectiveness	User Resistance	Upfront Cost	Maintenance Cost
1	Whitelist permitted/trusted programs	Essential	Medium	High	Medium
2	Patch application software	Essential	Low	High	High
3	Patch operating system software	Essential	Low	Medium	Medium
4	Severely restrict administrative privileges	Essential	Medium	Medium	Low
Once organizations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, mitigation strategies can be can then be selected to address security gaps until an acceptable level of residual risk is reached.					
5	Harden user application configurations	Excellent	Medium	Medium	Medium
6	Analyze email and web content in a sandbox	Excellent	Low	Medium	Low
7	Mitigate OS generic exploits	Excellent	Low	Medium	Low
8	Identify anomalous behavior with host based IDS	Excellent	Low	Medium	Medium
9	Disable local admin accounts	Excellent	Low	Medium	Low
10	Segment and segregate the network	Excellent	Low	High	Medium
11	Employ multi-factor user authentication	Excellent	Medium	High	Medium
12	Apply firewall to block incoming malware	Excellent	Low	Medium	Medium
13	Apply firewall to block outgoing malware	Excellent	Medium	Medium	Medium
14	Host virtual sandbox outside internal network	Excellent	High	High	Medium
15	Log successful and failed computer events	Excellent	Low	High	High
16	Log allowed and blocked network activity	Excellent	Low	High	High
17	Filter email by content	Excellent	High	High	Medium
18	Filter web traffic by content	Excellent	Medium	Medium	Medium
19	Whitelist web domains	Excellent	High	High	Medium
20	Block spoofed emails using sender ID	Excellent	Low	Low	Low
21	Configure workstation and servers under hardened SOE	Good	Medium	Medium	Low
22	Deploy anti virus software using heuristics	Good	Low	Low	Low
23	Deny direct internet access from workstations	Good	Low	Low	Low
24	Harden server application configuration	Good	Low	High	Medium
25	Enforce strong passphrase policy	Good	Medium	Medium	Low
26	Use DLP to secure portable media	Good	High	Medium	Medium
27	Restrict access to SMB and NetBIOS	Good	Low	Medium	Low
28	Educate users on spear fishing and social eng	Good	Medium	High	Medium
29	Inspect Microsoft Office files for abnormalities	Good	Low	Low	Low
30	Deploy signature based AV software	Good	Low	Low	Low
31	Use TLS encryption between email servers	Good	Low	Low	Low
32	Block web site access by IP address	Average	Low	Low	Low
33	Use network based IDS with signatures	Average	Low	High	High
34	Blacklist known malicious domains and Ips	Average	Low	Low	High
35	Capture network traffic for post intrusion analysis	Average	Low	High	Low

APPENDIX B:
Cyber and Board Resources Cited by Executives Interviewed

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

ARTICLES AND PAPERS

Cyber Risk Oversight

Director's Handbook Series, National Association of Corporate Directors | Larry Clinton, President & CEO, Internet Security Alliance

Key principles for the role of Boards of Directors in cyber oversight, and useful appendices including dashboards and metrics and list of federal government resources

https://www.nacdonline.org/insights/publications.cfm?ItemNumber=10687

Implementing Board Oversight of Cybersecurity—Advice for Boards Just Starting Out

Institute for Business & Information Technology @ Fox School of Business, Temple University | Richard Y. Flanagan, PhD and Janet L. Yeomans

A 'Call to Action' for boards, including the context and importance of board involvement and creating a board-management partnership on the issue

http://ibit.temple.edu/wp-content/uploads/2016/04/IBITReport_CyberBoard.pdf

Defense Science Board Task Force Report on Cyber Defense Management, September 2016

Robert Nesbit and Lou Von Thaer, Study Co-Chairs

See section on Informing and Engaging Executives, and sample metrics

https://www.acq.osd.mil/dsb/reports/2010s/Cyber_Defense_Management.pdf

The Chief Information Security Officer: An Exploratory Study

Journal of International Technology and Information Management, Vol. 26, Issue 2, Article 2, 6-1-2017 | Erastus Karanja and Mark A. Rosso, North Carolina Central University

This exploratory study investigates the organizational security reporting structures using a dataset of all the firms that hired a CISO between 2010 and 2014

scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1299&context=jitim

The Role of Boards of Directors and CISOs in Overseeing Cyber-Risks

Speech at the Security Adviser Alliance Conference Dallas, TX, September 22, 2016 | Luis A. Aguilar, former SEC Commissioner

Includes extensive footnotes

https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2016/09/Louis-A-Aguilar-Security-Adviser-Alliance-speech-Sept-22-2016.pdf

EY: SEC Guidance on Cybersecurity: Considerations for Financial Services Boards

EY Center for Board Matters

Overview of the February 2018 SEC interpretive guidance on public company disclosure obligations; implications for board oversight of the management of cyber risks, including questions boards should consider

https://www.ey.com/us/en/issues/governance-and-reporting/ey-sec-guidance-on-cybersecurity-board-considerations

Getting the Right Cybersecurity Metrics and Reports for Your Board

NACD Board Talks | Jack Jones and James Lam June 22, 2018

Blog posting providing guidance on effective reporting of metrics

https://blog.nacdonline.org/posts/getting-the-right-cybersecurity-metrics-and-reports-for-your-board

PROGRAMS

National Association of Corporate Directors (NACD)

Events and courses on risk, security, cyber.

www.nacdonline.org

Leadership in the Digital Age: Managing Cyber Risk and Driving Business Growth

Center for Technology Management, Columbia University and the G100 Network

Designed for executive and non-executive directors from the world's largest and most significant companies — creating informed governance regarding digital maturity

https://ctm.columbia.edu/

APPENDIX C: Sample Board Cybersecurity Presentations (Available for ACSC Members)

Several participants shared examples of the presentations given to their boards and board committees. These are available to ACSC members as practical tools to inform and shape their own board presentations.

These presentations are available through the ACSC by contacting info@ACSCenter.org.

THE ADVANCED CYBER SECURITY CENTER (ACSC)

is a member-driven nonprofit that harnesses the power of collective resources to strengthen cyber defense, develop security talent, and advocate for well-informed public policies. The ACSC works to improve cybersecurity throughout New England via three focus areas:

- **Enhanced Cyber Defense:** Collaborating on effective security practices, and cooperative public-private cyber defense simulations, improving decision-making, and promoting resources that reduce duplication of effort across member organizations
- **Workforce Development:** Making security careers more attractive by improving talent/industry interactions, developing opportunities to strengthen local security community relationships, and encourage talent to come into the region
- **Community Engagement and Advocacy:** Engaging in cybersecurity policy debates and empowering more informed policy making

ACSC's membership includes organizations in the financial services, healthcare, technology, infrastructure, defense, government, and higher education sectors. **www.acscenter.org**

ADVANCED CYBER SECURITY CENTER

202 Burlington Road, Bedford, MA 01730
info@acscenter.org | twitter: @ACSCorg | 781-271-5173