Insight from the Security for Business Innovation Council

Translating Security Leadership into Board Value

What Boards Want to Know and CISOs Need to Say

MARCH 2017

An industry initiative
sponsored by RSA

RSA

TABLE OF CONTENTS

Introduction 1

Major Trends 2

Successful Board-CISO Collaborations Put Business First 3

Growing Business Impacts Grab Board Attention 4

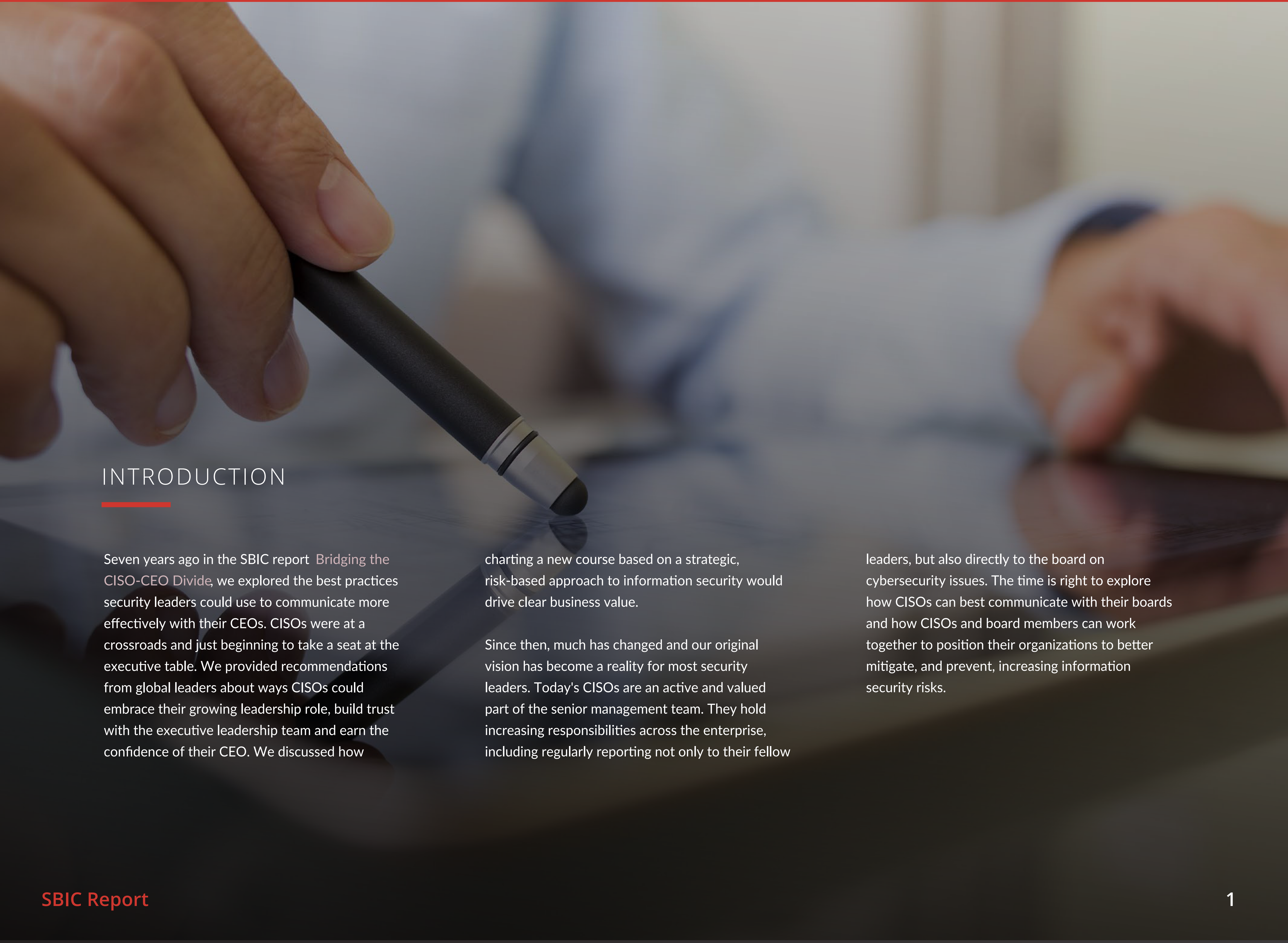
Five CISO Secrets to Better Board Meetings 5

Six Ways Boards Can Step Up to Cybersecurity 7

Summary 9

About the SBIC 9

Report Contributors 10



INTRODUCTION

Seven years ago in the SBIC report Bridging the CISO-CEO Divide, we explored the best practices security leaders could use to communicate more effectively with their CEOs. CISOs were at a crossroads and just beginning to take a seat at the executive table. We provided recommendations from global leaders about ways CISOs could embrace their growing leadership role, build trust with the executive leadership team and earn the confidence of their CEO. We discussed how charting a new course based on a strategic, risk-based approach to information security would drive clear business value.

Since then, much has changed and our original vision has become a reality for most security leaders. Today's CISOs are an active and valued part of the senior management team. They hold increasing responsibilities across the enterprise, including regularly reporting not only to their fellow leaders, but also directly to the board on cybersecurity issues. The time is right to explore how CISOs can best communicate with their boards and how CISOs and board members can work together to position their organizations to better mitigate, and prevent, increasing information security risks.

MAJOR TRENDS

To get started, it is critical to understand the factors that led to this dramatic shift in the role and responsibilities of the CISO. Overall, there are three major trends to consider:

More Cyber Incidents

In just the first half of 2016, more than 500 million records were breached in 974 separate incidents. This translates to over three million lost or stolen records per day.[1] In addition, 52 percent of the time the total number of compromised records was not known. If we were able to account for all undisclosed attacks, the numbers would be even more significant. In today's environment, it would be unlikely to find an organization that has not suffered at least one cyber incident.

Increasing Business Impact

The increase in cybersecurity incidents is playing havoc with both hard and soft business metrics for companies worldwide. Consumer confidence, business reputation and rising costs are just some of the many painful pressure points. In 2015, Lloyd's, a British insurance company, estimated that cyber attacks cost businesses as much as $400 billion a year, a figure that combines direct costs plus post-attack business effects.[2] Looking ahead, a Juniper Research report predicts the cost of data breaches will grow to $2.1 trillion globally by 2019, increasing almost four times as compared to breaches in 2015.[3]

Greater Accountability

According to Deloitte, the business impact of cyber attacks spans key factors such as: public reporting requirements, theft of personally identifiable information (PII), payment data and personal health information (PHI), as well as on costs of notifying customers, credit monitoring and possible regulatory penalties.4 As the ramifications of cybersecurity incidents broaden, C-level executives and boards are feeling a new level of scrutiny and personal accountability. With their companies and personal leadership reputations on the line, Osterman Research found that the proportion of board members that consider cyber risk to be a "high" priority issue is growing quickly: from seven percent in 2014 to 30 percent today and an expected 44 percent by 2018.5 Personal accountability is also driving higher engagement. The same Osterman report found that 89 percent of board members are now very involved in making cyber risk decisions.

SUCCESSFUL BOARD-CISO COLLABORATIONS PUT BUSINESS FIRST

Today's CISOs are no longer tasked with tirelessly fighting to prove the potential business impact of cyber attacks. Clearly, combatting these risks and associated costs now falls squarely within the fiduciary responsibilities of a company's board of directors and the escalating threat of cyber attacks can no longer be ignored or dismissed. What started as an attitude of "it won't happen to us" and gradually changed to an "if," has now become a "when" and lately, even a "how often." The threat (and resulting business implication) is clear, and CISOs must now work hand-in-hand with the board of directors as members of the executive leadership team to take a more business-driven approach to security that puts security details into business context. This means consistently collaborating to bring the top-down business knowledge of the board together with security technology insights from the CISO to define a stronger security posture that reduces risk and accelerates business priorities.

> "After 15 years of presenting to the board on cybersecurity, I've found that their interest boils down to trust and execution. This is more true now than ever. Given the increasing importance of security to the business, they want to know that you know the most valuable assets, you have a plan of action in protecting those assets and are actively executing against that plan to manage risks to the company."
>
> Timothy McKnight, EVP & Chief Information Security Officer, Thomson Reuters

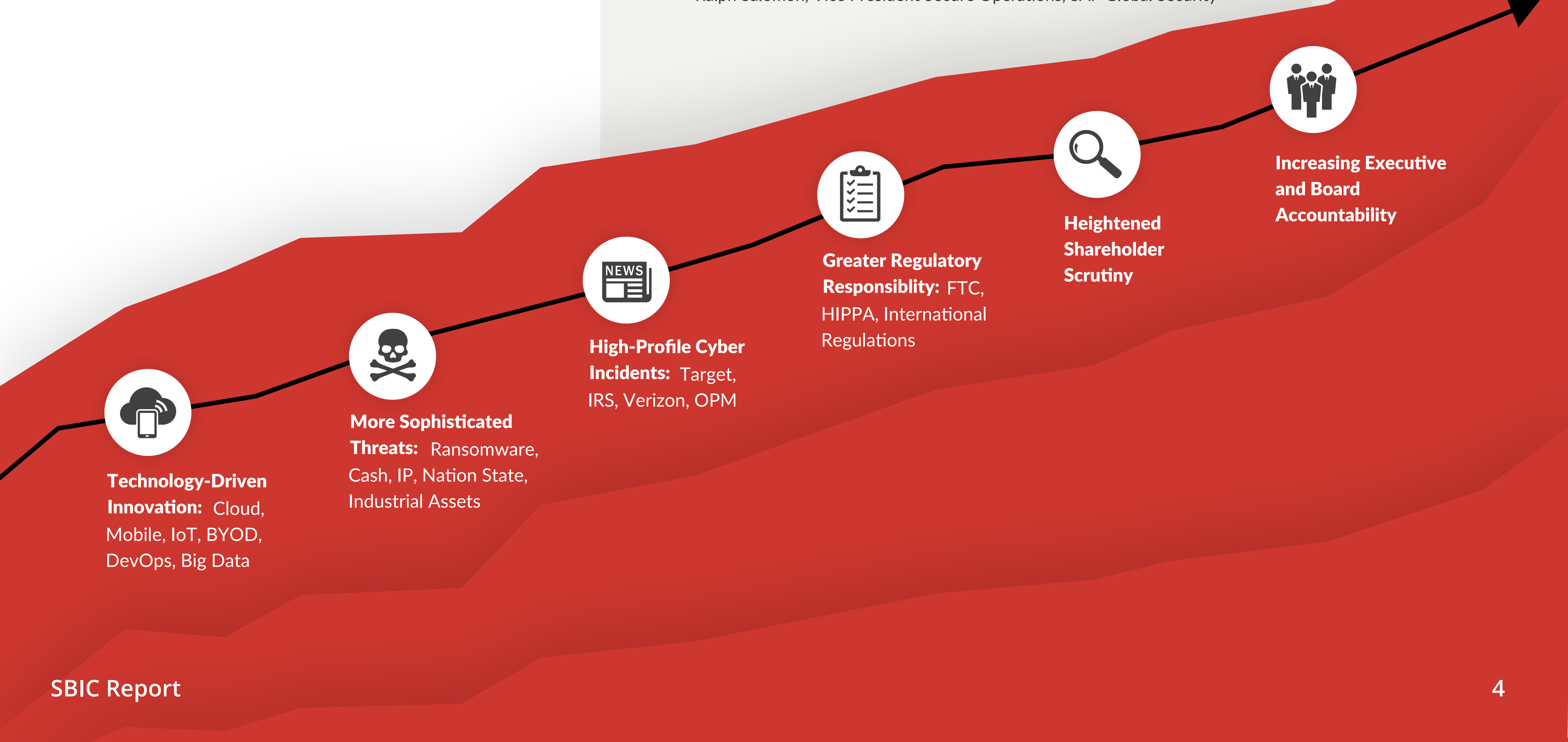
According to the 2016 RSA Cybersecurity Poverty Index, two thirds of respondents experienced incidents that impacted their business, and 75% reported significant cybersecurity risk exposure.[6]

There were 601 total breaches with over 21 million records containing Personally Identifiable Information (PII) exposed between January and mid-August 2016.[7]

GROWING BUSINESS IMPACTS GRAB BOARD ATTENTION

Increasingly garnering attention, and action, from shareholders, cybersecurity efforts must mature. As accountability for breaches and incidents now extends far beyond IT, organizations are beginning to push cybersecurity accountability into the hands of the executive team and board.

> “As organizations start to escalate cybersecurity programs to the board and executive team agenda, shared accountability will be the lynchpin for success. No IT department or CISO can tackle the cybersecurity challenge in a silo. Board support and culpability will become the norm in the years ahead.”
>
> Ralph Salomon, Vice President Secure Operations, SAP Global Security



Technology-Driven Innovation: Cloud, Mobile, IoT, BYOD, DevOps, Big Data

More Sophisticated Threats: Ransomware, Cash, IP, Nation State, Industrial Assets

High-Profile Cyber Incidents: Target, IRS, Verizon, OPM

Greater Regulatory Responsiblity: FTC, HIPPA, International Regulations

Heightened Shareholder Scrutiny

Increasing Executive and Board Accountability

FIVE CISO SECRETS TO BETTER BOARD MEETINGS

CISOs are still struggling to quantify cyber risks and the potential impact to their specific organization. The 2016 RSA Cybersecurity Poverty Index found that less than a quarter of the security professionals surveyed claimed to have a mature ability to catalog, assess and mitigate cyber risk while almost half described their ability as ad hoc or non-existent.[8] To proactively improve cybersecurity and risk posture by prioritizing risk mitigation and response, CISOs must build a better relationship with the board. Effective collaboration between the board and the CISO is fundamental for cybersecurity success. So where can CISOs start?

1 Embrace the "Trends Master" Role

While focusing on immediate operational and transactional priorities is an essential part of the CISO skill set, helping their businesses get ahead of and prepare for the next big technology trends is a critical CISO value-driver for the board. The best CISOs regularly point out coming trends well in advance, both overall and for their specific industry.

To help steer their organizations in the right direction, CISOs should make time to advise the board on these trends and their potential business impact. Before approaching the board, however, they need to make sure they think through required actions and be prepared to make recommendations on how the organization can prepare to successfully overcome future threats.

2 Talk the Talk

The nature of a CISO's role requires an in-depth understanding of a business' technology and systems and an ability to communicate with their teams with a level of detail that is required in an often complex environment. But this level of technology detail and associated jargon won't work at the board level. Board members are used to numbers and hard data, and prefer a higher level view of the overall business impact of this information.

CISOs must expand their skill sets to be able to fluidly speak to broader business reporting metrics while translating those into actionable intelligence that helps board members fully understand the opportunities and consequences of their cybersecurity decisions.

3 Collaborate Early and Often

Board members and CISOs agree that communication must move beyond a give and take in times of crisis to a continuous collaboration. For some CISOs, moving from putting out fires to fire prevention is a big transition. Figuring out how to pinpoint where, when and how a potential fire might start has become a critical skill and determining the right frequency for board interactions along the way is crucial. CISOs should collaborate early and often with cross-functional teams and include board members where appropriate to ensure best security practices.

Some companies are bringing the best of both worlds together, pairing business operations and security staff to bridge the gap and proactively integrate security into broader business strategies and conversations from the start. Forward-looking CISOs are reimagining the traditional boundaries that define their security team and using this new thinking to inform how they communicate with the board. They are providing a more holistic view of the critical elements of the business to drive a fully integrated security strategy that leverages the range of experience and expertise at an organization's disposal.

> "Our executive security council brings together finance, human resources, business unit leads, technology and quality heads, to ensure a complete view of what might impact our security posture. This collaboration mindset extends to our board, where we work together to define the most appropriate type, level and frequency of information to make the most informed decisions."
>
> Roland Cloutier, Senior Vice President, Global Chief Security Officer, Automatic Data Processing, Inc.

Organizations with proactive security strategies and strong C-suite backing are more confident about the future.[9]

4 Boost Credibility with Transparency

Communication with the board about innovation must balance the security risks new innovations carry while being realistic about possible ways to minimize these risks. CISOs must be transparent about the security risks new innovations carry and proactive and realistic about solutions to maintain credibility.

As Jerry Geisler, Vice President and Assistant Global CISO for Walmart Stores, Inc., points out, "When we talk to the board about innovation versus security, we speak pragmatically. We don't ever want our board to say 'how could this happen?'. We make sure the message is balanced and realistic. Our goal is to make sure the business is successful, and making sure everyone is fully informed is a big piece of that."

One piece of advice board members consistently give in terms of reporting is that CISOs must not only understand the relevance of reporting metrics and trends, but also clearly articulate the possible actions the company could take based on the prevailing conditions. **One board member said it best – "Add value, don't just report."**

> "We know that in reporting, simpler is better and being fully transparent is critical. No excuses. This is how you establish trust with the board and maintain your credibility."
>
> Jerry R. Geisler III, Vice President and Asst. Global Chief Information Security Officer, Walmart Stores, Inc.

5 Make Cybersecurity Synonymous with Business Growth and Opportunity

Beyond the increase in high-profile cyber incidents, the increasingly central role of technology as a driver of business advantage has also put the CISO front and center for the board. As enterprises seek to gain digital advantage, technology grows as both a strategic dependency and a risk exposure. This means security risks can increase exponentially as companies pursue new technology-fueled revenue streams, business models and strategies to gain competitive advantage.

Today's CISOs have the opportunity to support innovation and business growth by prioritizing assets and creating a common organizational understanding of risk appetite that is recognized across the board.

"It's vital that security initiatives support business innovation as an enabler of business and revenue growth. An important part of the CISO's role is to clearly articulate the balance of risk and risk mitigation so the board can make well-informed decisions," commented Matt McCormick, Chief Security Officer, Dell EMC.

45% of 2016 RSA Cybersecurity Poverty Index respondents described their ability to catalog, assess and mitigate cyber risk as "non-existent" or "ad hoc" and only 24% reported maturity in this domain.[10]

SIX WAYS BOARDS CAN STEP UP TO CYBERSECURITY

With 75 percent of organizations citing a significant cybersecurity risk exposure,[11] organizations cannot afford to ignore the issue and the cybersecurity onus has become a shared responsibility. Board members take pride in their contribution to the business' successes, and it is time that they also step up to prevent potential business failures by taking ownership of their role in the ongoing cybersecurity battle. While CISOs must broaden their skill set to effectively communicate with the board, board members also have a special role to play to ensure success. Productive CISO-board collaborations are a two-way street.

1 Expand Board Expertise to Include Digital Directors

Directors are starting to understand that cybersecurity is an enterprise-wide risk management concern, not merely an IT issue. For some companies, a deeper level of business and security collaboration extends into how the board is shaped. While the CISO role is evolving, board members point out the makeup of the board is evolving as well. Basic cybersecurity knowledge and a deep understanding of the legal implications of cyber risks are becoming board member requirements. Corporate boards are looking for increased technical literacy and are actively pursuing digital directors and advisors that can deliver high levels of both technical and business acumen. All board members also need to fully understand the role they play in overseeing cybersecurity and push for board-specific reporting and cybersecurity transparency. This winning combination increases the board's ability to ask the right questions and provide the right communication opportunities for the CISO.

2 Build Collaborative, Ongoing Relationships with the CISO

The business threat of cyber attacks is now crystal clear, and executive leaders and board members must be proactive about working hand-in-hand with CISOs to position their companies to withstand the incessant onslaught of attacks. CISOs are not the only ones who must reimagine their role in the corporate dynamic; executive leaders and board members who proactively build relationships with their CISO counterparts create stronger cybersecurity defenses. All parties need to work together to ensure clear lines of communication and incident preparation.

Board members must work with CISOs to create meaningful conversations for all parties involved by telling them what information they want and how often they need it. An open dialogue about current threats, emerging attack patterns and incident-response protocol leads to stronger alliances, smarter decisions and better business outcomes.

Nearly one-third of board members are dissatisfied with the quality of information they get regarding cybersecurity risk, and more than half are unhappy with the quantity of information provided.[15]

3 Walk the Walk

A report by The Economist Intelligence Unit (EIU)[12] emphasizes the importance of the board's role in protecting their organizations from cyber incidents. With a proactive cybersecurity strategy in place that is supported by the board, the report states that eight major types of cyber attacks have been reduced by an average of 53 percent. These dramatic numbers underscore the critical role the board plays in reinforcing the importance of security throughout an organization.

In addition to showing support for a company's cybersecurity strategy and initiatives, boards should actively engage the CISO to help keep the board up to date on other organizational approaches and security frameworks such as those from the National Association of Corporate Directors (NACD)[13] or KPMG's Global Cyber Maturity Framework for exercising board oversight responsibility.[14] A key example, board members should work directly with CISOs to ensure incident response programs—a core element of effective cybersecurity initiatives—are continuously reevaluated and updated to address increasing cyberattack activity.

While all SBIC members have developed an incident response function, 30% of at-large organizations surveyed do not have formal incident response plans in place, and 57% of those who do have a plan admit to never updating or reviewing them.[16]

SIX WAYS BOARDS CAN STEP UP TO CYBERSECURITY (CONTINUED)

4 Expect Security Reporting Discipline

Security is now a key business function, so treat it that way. Make sure CISOs know what reporting metrics and benchmarks are valuable to the board by applying a reporting discipline with consistent benchmarks and actionable information.

Although approaches and formats may vary, board members look for regularity in reporting from CISOs. Some look for program-level updates for defined benchmark presentations where any important changes are highlighted. According to EY's Cyber Program Management report,[17] boards should be regularly asking security leadership questions such as:

- How secure are the organization's assets and high-value information?
- Does the cybersecurity strategy align with business objectives?
- How can you measure cybersecurity program effectiveness?
- What are the security priorities and does current IT spending support them?
- How can we detect a breach?
- Are there adequate cybersecurity resources in place?
- How does the security program compare to other industry players and competitors?

With a proactive cybersecurity strategy in place that is supported by the board, eight major types of cyber attacks have been reduced by an average of 53%.[18]

5 Be Clear About Innovation Needs and Risk Appetite

As one SBIC board member points out, in an industry where every operational change is technology-driven, "You must continually invest in new functions and capabilities to spark innovation. At the same time, you can't introduce risks that pose new threats to business effectiveness. This creates a constant state of security and compliance catch up."

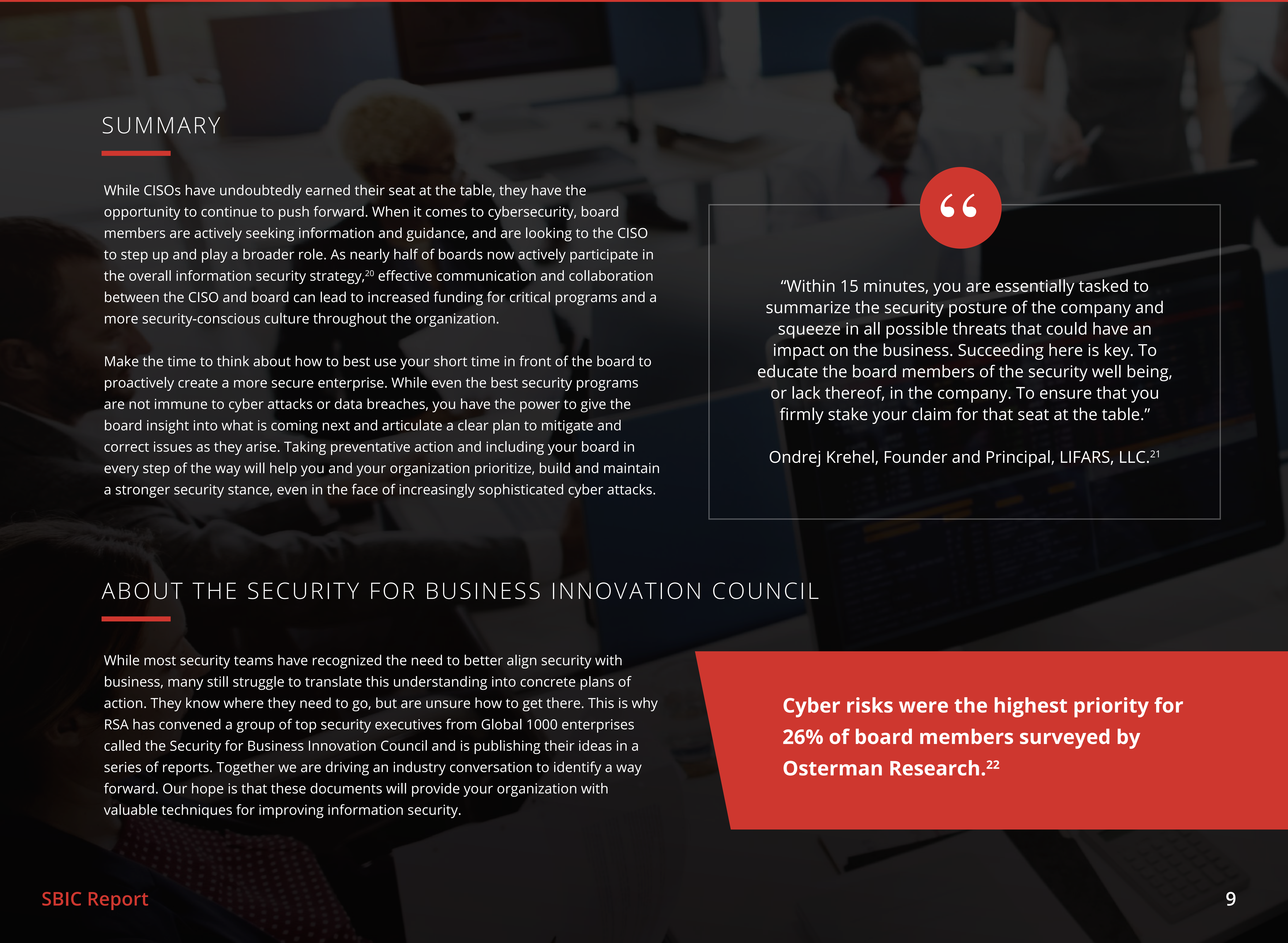
While business growth lies at the heart of most organizations, the board is charged with helping to determine the tradeoffs between risks and returns. All businesses have inherent risks and security risks need to be treated the same way, beginning with a clear understanding of the risk and the capacity to manage the risk. Clearly communicated financial, operations and reputational risk tolerance prioritization from the board and executive team allows the CISO to effectively manage expectations and realities.

6 More is Better

In the recent past, CISOs managed board reporting through the CEO or CIO. But as outlined previously, the increasing number and sophistication of high-profile security incidents and the aftermath of financial and reputational damage has pushed the CISO directly into the boardroom. Where CISOs were once asked to appear for a company specific or competitor incident, board members report that the CISO attendance at board meetings ranges from every board meeting at the top end to increased board meeting appearances with support from sub-committee attendance. Boards should proactively allocate time at board meetings to hear from the CISO and examine future trends and risks as well as more immediate priorities.

Securosis' Mike Rothman recently noted, "The job of a senior security professional is changing rapidly: It's more about persuasion and being able to navigate the political minefield of a large organization than it is about fighting bad guys." He continues, "Security professionals need to be able to allay fears by educating executives on the security program and its objectives, milestones and other aspects of daily security operations. These are valuable opportunities to set expectations, solicit funding and ensure that security is a high priority within the organization."[19]

> "Board oversight of our security investments means we need to communicate why we made choices and how effective they were. Staying on top of innovations and recognizing trends in security gives us insight into what is needed to be more effective as a strategic business function. This includes creating useful metrics—while it's not easy to put a value on a threat, translating the information we have into business language creates a level of trust with the board."
>
> Dr. Martijn Dekker, Managing Director, Chief Information Security Officer, ABN Amro



SUMMARY

While CISOs have undoubtedly earned their seat at the table, they have the opportunity to continue to push forward. When it comes to cybersecurity, board members are actively seeking information and guidance, and are looking to the CISO to step up and play a broader role. As nearly half of boards now actively participate in the overall information security strategy,[20] effective communication and collaboration between the CISO and board can lead to increased funding for critical programs and a more security-conscious culture throughout the organization.

Make the time to think about how to best use your short time in front of the board to proactively create a more secure enterprise. While even the best security programs are not immune to cyber attacks or data breaches, you have the power to give the board insight into what is coming next and articulate a clear plan to mitigate and correct issues as they arise. Taking preventative action and including your board in every step of the way will help you and your organization prioritize, build and maintain a stronger security stance, even in the face of increasingly sophisticated cyber attacks.

> "Within 15 minutes, you are essentially tasked to summarize the security posture of the company and squeeze in all possible threats that could have an impact on the business. Succeeding here is key. To educate the board members of the security well being, or lack thereof, in the company. To ensure that you firmly stake your claim for that seat at the table."
>
> Ondrej Krehel, Founder and Principal, LIFARS, LLC.[21]

ABOUT THE SECURITY FOR BUSINESS INNOVATION COUNCIL

While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA has convened a group of top security executives from Global 1000 enterprises called the Security for Business Innovation Council and is publishing their ideas in a series of reports. Together we are driving an industry conversation to identify a way forward. Our hope is that these documents will provide your organization with valuable techniques for improving information security.

Cyber risks were the highest priority for 26% of board members surveyed by Osterman Research.[22]

REPORT CONTRIBUTORS

Marene N. Allison
Worldwide Vice President of Information Security,
Johnson & Johnson

William Boni
Corporate Information Security Officer and Vice President,
Enterprise Information Security, T-Mobile USA

Roland Cloutier
Senior Vice President, Global Chief Security Officer,
Automatic Data Processing, Inc.

Dr. Martijn Dekker
Managing Director, Chief Information Security Officer,
ABN Amro

Ben Doyle
Chief Information Security Officer Asia Pacific, Thales

Jerry R. Geisler III
Vice President and Asst. Global Chief Information Security Officer,
Walmart Stores, Inc.

Matt McCormack
Chief Security Officer, Dell EMC

Timothy McKnight
EVP & Chief Information Security Officer, Thomson Reuters

Kevin Meehan
Vice President and Chief Information Security Officer, The Boeing Company

Robert M. Rodger
Head of Security Operations and Deputy CISO, HSBC Holdings plc.

Ralph Salomon
Vice President Secure Operations, SAP Global Security

SOURCES

[1] www.breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf

[2] www.fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[3] www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[4] www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

[5] www.baydynamics.com/resources/how-boards-of-directors-really-feel-about-cyber-security-reports/

[6] www.rsa.com/en-us/perspectives/industry/cyber-security-poverty-index

[7] www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2016.pdf

[8] www.rsa.com/en-us/perspectives/industry/cyber-security-poverty-index

[9] www.eiuperspectives.economist.com/sites/default/files/DataSecurityArticle.pdf

[10] www.rsa.com/en-us/perspectives/industry/cyber-security-poverty-index

[11] www.rsa.com/en-us/perspectives/industry/cyber-security-poverty-index

[12] www.eiuperspectives.economist.com/sites/default/files/DataSecurityArticle.pdf

[13] www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=15879

[14] www.kpmg.com/BM/en/IssuesAndInsights/ArticlesPublications/Documents/Advisory/2015Documents/Cyber-Security-and-Board-Oversight.pdf

[15] www.forbes.com/sites/forbesinsights/2016/04/25/cybersecurity-threats-are-real-you-and-your-organization-are-in-danger/#33ee70ff70ee

[16] www.rsa.com/en-us/company/newsroom/new-rsa-breach-readiness-survey-finds-majority-not-prepared

[17] www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf

[18] www.eiuperspectives.economist.com/sites/default/files/DataSecurityArticle.pdf

[19] www.searchsecurity.techtarget.com/tip/How-to-get-information-security-buy-in-from-the-executive-team

[20] www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-technology.pdf

[21] www.lifars.com/2016/04/ciso-tips-effective-communication-boardroom/

[22] www.baydynamics.com/resources/how-boards-of-directors-really-feel-about-cyber-security-reports/

RSA