

CYBER BUSINESS EXECUTIVE RESEARCH: CYBER BOARD COMMUNICATION & METRICS

Challenging Questions from the Boardroom: Perspectives
from Enterprise CISOs



Executive Summary

Boards of Directors are in a unique position to drive a proactive security agenda for their organizations. In the last years, we have seen increasingly willingness by boards of directors to drive proactive security agendas in their organizations, championing messages about the importance of enterprise security, setting cyber risk appetite, and ensuring cybersecurity investments align to business objectives.

The CISO has an unprecedented opportunity to empower the board to execute this role effectively. And he can do it – to adapt a famous saying – by walking a mile in their shoes. CISOs must try to see cybersecurity as a board member sees it: a business imperative, something that should align with risk appetite and business priorities.

Traditionally, CISOs have presented boards with a mass of technical and security operation metrics, which can fail to make a mark and engender trust in their ability as enterprise security leaders. The majority of CISOs, even seasoned ones, find it a challenge to understand what boards are looking for and provide the required information in a framework that resonates.

A new approach to communicating cyber risk is needed. CISOs need to engage in meaningful conversations with board members and be accepted as equal partners in executive business leadership rather than compliance chasers, technology spenders, and/or one-way cost centers.

A partnership between CISOs and their board of directors is crucial. The effectiveness of any company's security program depends on it; the endorsement of the ultimate decision makers will greatly increase its chances of success.

Table of Contents

Executive Summary	2
Preface	4
Most Challenging Questions from Boards	6
Question 1: Are we secure?	6
Question 2: How do we know if we have been breached?	10
Question 3: How does our security program compare to peers within the same industry?	13
Question 4: Do we have enough resources for our cybersecurity program?.....	15
Question 5: How effective is our security program, and is our current investment strategy aligned to it properly?	17
Structuring an Effective Presentation	19
Appendix A - Survey Questions & Summary of Answers	20
Reporting to the Board: Most Common Themes.....	20
Popular Dashboard Visuals in Board Decks	20
Common Frameworks Used to Measure Cybersecurity Program Maturity	20
Frequent and Challenging Questions CISOs Asked by Boards	21
Appendix B – Key Contributors	22

Preface

The Kudelski Security Customer Advisory Council is comprised of CIOs and CISOs of global enterprises who give insight and guidance on the solutions we offer clients.

In this research engagement we identified the need to focus on enhancing board awareness of the cyber challenges their organizations face, and in improving their confidence in the CISOs who are in charge.

We confirmed through industry surveys, focus groups and individual interviews our original hunch: CISOs need to communicate better programs and initiatives in a way that is meaningful to their counterparts and boards.

Key to helping boards understand cybersecurity is to work out what they really want to know when they ask challenging questions. This research outlines a strategy to answer these questions with suggestions for accompanying metrics and visuals.

ADVICE TO IMPROVE CISO COMMUNICATION WITH BOARDS AND INSTILL CONFIDENCE IN THE SECURITY PROGRAM



Long Term Focus

Get to know your board members, their backgrounds, the current boards they serve on, etc. The more you understand the board members, the better you'll be able to communicate with them.

Create a presentation that will resonate with the board



Some boards like VISUALS and others prefer DIALOGUE



Educate



Take a long-term approach to board education and address misunderstandings. FOR EXAMPLE: Being compliant does not equate to being secure.

Engage



Use the support of the board to encourage the organization to get behind the security program.



Deck Preparation

Metrics Research



Ask

and expect a business-relevant response: threats, risk, progress, priorities



Review

company reports to understand the business objectives that could help you create relevant metrics



Present

metrics that do not take too long to capture



Use

factual information in the deck, avoiding fear, uncertainty and doubt (FUD)

Focus on Context



Stories
with business
relevance



Examples
with business
relevance

**Provide the Bigger Picture
and Show Alignment with Business**

Focus on Strategic Elements — Instill Confidence in Your Program

Create a story that shows how:



You have aligned security program and investments to business priorities



Your controls are effective (show results, with related business outcomes)



Your strategies, investments and outcomes make the company secure and enable business



Your strategic plan is backed up by data and aligned to a framework and a maturity model



The cyber program has prioritized certain areas, and enforce messages around peer benchmarking

KEEP IN MIND:
Board members are not technology or security professionals - communicate in their language



One Week Before



Prepare for possible questions



Create a shorter version



Update presentation based on peer feedback

THE MEETING

Tell the board the story the way they want to hear it. The most productive board interactions happen when presentations become conversations.



Most Challenging Questions from Boards

Kudelski Security has curated responses from its CISO community about the top five most challenging questions from boards. The responses represent a range of strategies and approaches. Evaluate and implement what works best for you, based on your company's organizational profile and board requirements.

1 Question 1: Are we secure?

The question "Are we secure?" was by far the most common and challenging question, perhaps because it's so broad. As CISOs know, this is not a simple "yes" or "no" question and answering definitively can impact program credibility.

How to Nail It: Understand exactly what the board is asking and how much they already know about cybersecurity. This will also help you determine the proper metrics to report.

“ Always have data to back up your recommendations. **Stay away from opinions.** ”

Tony Spinelli, COO,
Fractal Industries

Response Strategies

1. Set Expectations

Make it clear that there is no such thing as perfect security. Even if it existed, it's unlikely the business could afford it and still grow.

Communicate the need for a risk-based approach to security that protects critical assets from ever-evolving threats and vulnerabilities. Be clear on the organization's risk profile and how it maps to the accepted risk appetite; the organization's risk profile will be the foundation of your security program's risk management and investment strategy

2. Fill in Knowledge Gaps

Understand how familiar your board is with cybersecurity concepts, and what they care most about – this is key to communicating the cyber program clearly.

Prioritize their training and education. Leverage NACD insights to drive awareness on the cyber program elements that are of interest.

Send pre-meeting reading material in a short memo, e.g. a

regulatory environment overview, helping them better understand the material you present in the meeting.

3. Communicate the Journey

Talk about security as a journey, showing where you're at today (current maturity) where you want to get to (target maturity, based on risk profile, risk tolerance and business context) and where you've made noteworthy progress. One council member uses a spider graph to communicate this journey, giving an instant snapshot of maturity gaps, initiatives, investments as well as effective spend and progress.



*CISOs spend an average **10-20 hours** preparing their response to this question.*

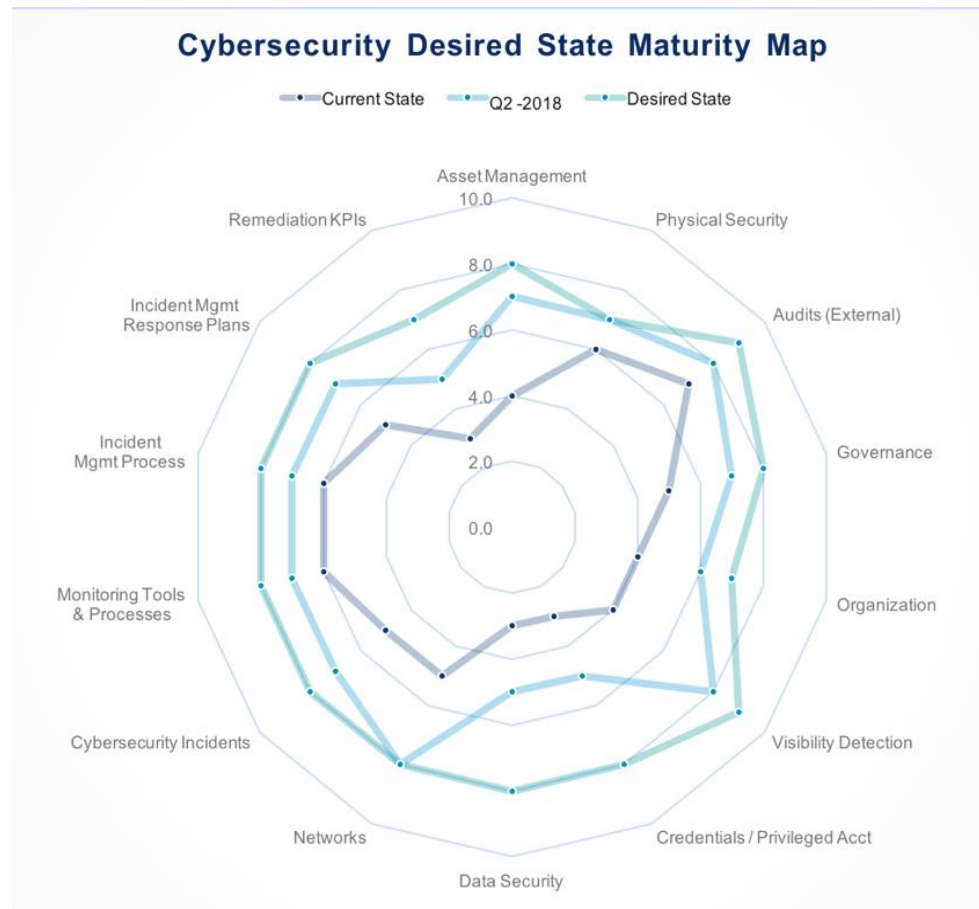


Figure 1 Journey communication graphic

4. Validate Your State of Security

Provide direct, fact-based answers that you can validate with metrics, event monitoring results, artifacts, or with third-party audits (e.g. a penetration test, or compromise assessment). Show the rationale for your decisions and their associated outcomes. Leverage industry frameworks and peer benchmarking to gauge how well you are doing in meeting industry requirements. Consistently leveraging both the CMMI scale with an ISO/NIST-based framework is a sound approach to measuring capability maturity over time and carrying out industry comparisons.

Presentation Tips

Keep the message on each slide focused and leave plenty of white space.

•

Show progress over time, including trends, outcomes, and risk reduction. A bar chart can show direction of trends such as number of vulnerabilities remediated.

•

Use a heatmap to demonstrate risk drivers.

•

Use spider charts to show multiple data points (i.e. previous, current, and target maturity of capability) simultaneously.

•

Show improvements in ability to respond and recover from an attack with examples of dwell time reduction for threat actors like phishing or malware.

Metrics

Boards prefer objective, quantitative evidence, rather than qualitative, judgement-based evidence. However, both can provide value when intentionally selected and presented.

The Client Advisory Council CISOs provided several qualitative and quantitative metrics to help you make your case.

Quantitative	Qualitative
<ul style="list-style-type: none"> • MTTD/MTTR, dwell time • Monitoring metrics • Trend of new vulnerabilities discovered vs. remediated • Control efficiency • Risk associated with critical assets • Effective SLAs for vulnerability remediation • Cyber hygiene of team activity • Patch management data • Number of incidents/vulnerabilities • Number of non-remediated risks 	<ul style="list-style-type: none"> • Outcomes of initiatives that aimed to reduce risk • How security has integrated with application development • Actions you have taken that improve security risk posture • Risks the organization has accepted and how it aligns to company's agreed-upon risk tolerance • Volume of threats and volume of attacks

“In a perfect world, the absolute metric for a CISO to have is the MTTD / MTTR of a more targeted attack.”

Pete Naumovski, VP and CISO, BCBSA

“Your ability to respond and recover is equally important to how secure you are.”

Ginny Davis, CIO and CSO, Technicolor



Question 2:

How do we know if we have been breached?

Associated questions asked by boards:

Have you seen anything or are you concerned about anything the board needs to be aware of?

•

If there are gaps in our security, what are we doing about them? What solution (e.g. processes and tools) are you bringing to the table?

•

Is there something we need to dedicate our time, money, or resources towards?

•

Do we detect and respond to incidents? what would the impact have been had we not responded in time?

When asking this question boards usually want to know how well you're prepared against the latest big attack, and what the impact would be if you were targeted.

How to Nail It: Know that this question is all about assurance. Boards know you can't guarantee 100% security. What they want is confidence that the response to any breach is crisp and effective.

Response Strategies

1. Tell a Story

Boards will be more familiar with some attack vectors, e.g. DDoS attacks, than others. Educate them, especially on relevant ones.

Use a storyboard.

For example, show analysis of a previous breach - the timeline, response activities, lessons learned, and adjustments made. This method connects security investments to their real-world application in a much clearer way than comparing the number of incidents, quarter-over-quarter.

One Client Advisory Council member storyboards the anatomy of common attacks such as ransomware and shows the controls they have in place to protect against it.

Capability	Equifax Breach	Our Security Measures
Identify	Assets compromised: Full Names, Date of Birth, Address, SSN, Driver's license numbers, credit card numbers	<ol style="list-style-type: none"> 1. All sensitive data to be salted and encrypted prior to their storage in Databases. 2. Privacy preserving and privacy enhancing technologies to be implemented.
Protect	Infiltrated through a flaw in Apache Struts tool (software used by Equifax's web application). The compromise allowed unauthorized access to the company's systems and allowed the perpetrators to send users malicious software pretending to be Adobe Flash.	<ol style="list-style-type: none"> 1. Timely patching 2. Periodic security assessments and auditing.
Detect	<p>Attackers exploited the Apache struts tool vulnerability to gain access to the system.</p> <ol style="list-style-type: none"> 1. Escalated their privileges to that of an administrator on the system. 2. Took control over the Equifax network. 3. Accessed database credentials. 4. Extracted user data from the databases. 5. Used 30+ unique IP addresses to exfiltrate data and avoid detection. 	
Respond	<ol style="list-style-type: none"> 1. Lack of timeliness in disclosure: has been widely criticized for waiting more than a month to alert its customers and shareholders about the hack. 2. Provided a dedicated website for consumers to check if they were affected (which eventually fell prey to phishing attack). 3. Customers who sign up for free credit monitoring that Equifax is offering are seemingly required to promise not to sue the company for future losses. 	Best practice dictates an immediate disclosure and freeze on insider sales for a time, thereby protecting the company's reputation and avoiding the appearance of impropriety.
Recover	<ol style="list-style-type: none"> 1. The compromise is expected to haunt customers for years to come as sensitive information such as SSN is compromised (potential identity theft to increase over the years). 2. Lawsuits and Litigations: Those affected by data breaches can take their claims to court 3. Erosion of consumer 	<ol style="list-style-type: none"> 1. In the wake of the hack, government is looking to undo SSN 2. Legacy systems are to be upgraded and considerable amount of expenditure to be made for securing the infrastructure. 3. GDPR promises to put financial burden on companies that do tolerate breaches.

Figure 2. A storyboard example: mapping the anatomy of a high-risk attack to the security measures in place.

Presentation Tips

Show high level trends without going into too much detail to explain attack vectors observed and provide an update on remediation time.

•

Point out areas that need additional investment in the next steps or items for consideration section of the presentation.

•

Leverage line and bar charts to show increased detection activity.

2. Outline the Response Plan

Assure the board that your team is ready to respond.

Give an overview of your incident response plan. Demonstrate the steps you've taken to reduce potential dwell time (e.g. threat intelligence, 24/7 MSSP monitoring, control implementation, etc.). Back it up with metrics such as MTTR.

One Client Advisory Council member reports to the board on recurring tabletop exercises he conducts, which test the organization's response capabilities. He carries out simulations with IR/CERT teams, but extends tabletop exercises to other departments, e.g. human resources and public relations.

Talk about your cyber insurance policy and highlight any third-party companies that will be supporting your response.

.

3. Use Metrics to Validate

Show how your company has improved in its ability to identify and respond to security incidents. Use critical KPIs, such as MTTD and MTTR to back up your analysis.

Show your ability to perform continuous monitoring, using the number of tickets and log reviews as proof. Measure and trend the number of tickets that turn into incidents to show improvements in detection capability.

Show your ability to know if you've been breached by sharing results from internal threat hunting efforts

List the number and type of incidents since the last update, their business impact (e.g. monetary loss), and the steps taken to mitigate the attack.

Attest to your resilience against attacks with results from yearly penetration testing and compromise assessments; identify current known threats and the status of vulnerabilities and patching efforts.

Finally, share the number of times you have exercised the incident response process with real-world events. Practice makes perfect, and this metric will show that your team is well prepared to respond to attacks.



Question 3:

How does our security program compare to peers within the same industry?

Boards want to be equitable or even higher than peers within their industry but do not want to overspend in areas with diminishing returns on investment.

When asking this question, boards may be seeking information on two things: first, whether they're spending enough on security compared to peers; and second, whether they're spending too much, compared to peers. As the saying goes, you don't have to outrun the bear, you just have to outrun the person you're with.

How to Nail It: There isn't one correct way; each strategy outlined below can be used on its own, or in combination with others.

Response Strategies

1. Use an Industry Standard Framework to Benchmark

Approach 1: Benchmark your security program's maturity with an industry-standard framework. Start by communicating how the framework was selected and why your enterprise fits it. Then show how the program measures against this framework, highlighting your starting point and progress toward target state.

2. Compare Security Spend with Peers

Approach 2: Compare the average security spend within your organization's vertical, adjusting the number for organization size, complexity, and degree of innovation. A typical spend, not controlled for industry vertical, is 5-8%¹ of the IT budget; however, look behind the data to verify consistency with your business model and innovation appetite (firms that thrive on innovation or those going through digital transformation will spend more; traditional firms tend to spend less). A potential roadblock to this approach is the lack of a central database of anonymized data for comparison purposes. This approach requires extra effort to find this data, e.g. consulting with peers at industry events or forums. Research firms, e.g. Gartner and Forrester, can also provide insight. See the more complete list of channels at the end of the section.

¹ See Gartner IT Key Metrics Data 2017: Key IT Security Measures: by Industry, ID: G00316663 (12 December 2016)

3. Compare Maturity of Individual Program Components

Approach 3: Look at what functional or capability outcomes peers are trying to achieve, what gaps they are trying to close, and the steps they've taken to do so. This exercise provides a maturity benchmark and can give you ideas on how to move forward. It should be carried out for all important security program components. Don't forget to review the cost of improvements and verify alignment of those costs to the expected improvements in risk and maturity.

One Client Advisory Council member obtains their benchmarking information from an industry-specific cyber community hosted by the FBI. They meet monthly to get updates from the FBI on industry cyber trends, compare cyber programs and maturity (information sanitized by the FBI), and share the latest incidents that have impacted them.

Suggested Channels for Benchmark Data



4

Question 4:

Do we have enough resources for our cybersecurity program?

Ultimately, boards want to know if CISOs have the resources they need to do what they need to do. They want to ensure investments are used wisely as well as understand what the right spend on security is.

How to Nail it: Showcase the return on security investments in relation to the program strategy as well as the overall business objectives. Highlight any areas that are underinvested.

Response Strategies

1. Embrace a Strategic Planning Perspective

Show how the cybersecurity program supports the organization's mission, business model, and growth goals. To determine resource shortfalls (e.g. tools, staff, external partnerships) look at the program's current maturity and associated business risk, considering new threats and the new risk they present to the business. This approach is the best bet for getting approval on funding requests.

2. Demonstrate Good Stewardship

Show the progress you've made with the resources you have (people, process and existing technologies), as well as the potential ROI in program maturity improvements that additional resources would bring. Focus on current resource utilization, project output, and ability to take on new projects.

3. Identify Roadblocks & Present Recommendations

If resource constraints prevent you achieving your program goals come with a plan to address the roadblock.

- For example, you may struggle with the talent gap. In order to remove the skills shortage roadblock, you could choose to hire less experienced candidates with a passion to learn and train them up. Or you may partner with your HR team to attract high-potential employees through additional pay and benefits.
- For example, when determining which initiatives best improve program maturity, base recommendations on current cross-organizational resources, (people, tools, technology and processes), Show you are getting more efficient with existing resources and consider initiatives that refine and improve

processes first.

Metrics

- Resource utilization
 - Budget, current spend, headcounts
 - MTTR
 - Number of outages
 - Number of issues
 - Results from latest phishing exercises
 - Employee retention
 - Process improvements to minimize incident impact
-



Recommendation:

Work with business units on having dedicated business-oriented cybersecurity resources for within those units to ensure company-wide enforcement of security principles.



Question 5:

How effective is our security program, and is our current investment strategy aligned to it properly?

What question do the CISOs answer?

Are we effectively implementing our control strategy, and are we aligned to our spending forecasts?

Answers to this question need to provide assurance that you are able to do what you need to do.

This question is all about alignment between security program and investment strategy.

How to Nail It: Focus on the program strategy and associated initiatives to enable the organization to meet business objectives.

Response Strategies

1. Reiterate the Security Program Strategy

We know that perfect security is impossible; there's always room for improvement. Reiterate current and target security states and update on maturity level and risk posture. It's important to show that the program comprises several components, each one with a different target state. Show how supporting resources and systems fit into the security program, and where the gaps are. Show how you plan to close them and what investments you need.

2. Show Alignment with Business Objectives and Evolving Contexts

Show how the cybersecurity roadmap, supports the business's overall objectives. Make the connection between cyber risk and financial risk. Effective security can play a role in how well the business is able to go-to-market, operate efficiently, minimize downtime, and reduce costs.

Moreover, as new business strategies and assets are adjusted, the security strategy must also adjust in order to account for new cyber risks. Annual threat landscape reviews can also require adjustments. As top threats shift, inform the board of the impact on the security program.

Several Council members recommend Partnering with internal departments, e.g. Audit teams and IT, to get buy-in on the program strategy. This cross-department alignment strengthens the effectiveness of the security program.

3. Demonstrate Success

Highlight the successes of your programs by sharing positive outcomes. Use examples and stories that demonstrate program

“**MTTD, MTTR are key measures of maturity.**”

Don Kleoppel, CSO,
Cerner Corporation

effectiveness in the context of business objectives. Leverage peer benchmarking to help make your case, bring in a third-party to help validate your outcomes, and share internal audit results from your chief auditor. On a tactical level, highlight your control strategy, show top controls implemented and emphasize your ability to implement year-round, not only at audit time.

“Present the business value of what you are trying to protect, why you are protecting it and from who.”

Mark Butler, CISO, Qualys

“Be best of breed in detection, have goals aligned with performance objectives.”

Pete Naumovski, VP and CISO, BCBSA

Recommended Metrics	Recommended Visuals
<ul style="list-style-type: none"> • Process maturity objectives and progress • Three-year outlook for target maturity of each process • Metrics on what has changed in the environment • Staff utilization • MTTD, MTTR • Patch/vulnerability management trends • SOC metrics 	<ul style="list-style-type: none"> • Present the roadmap and the maturity level for each domain of the cyber program, and include the number of effective controls for each domain • Show process maturity milestones within a spider graph • Diagram the different business assets and their associated security level • Diagram the security architecture and the planned improvements over time. • Graph trends and progress around security and risk posture improvement. For example: patch management trends, vulnerability management trends, SOC trends.

Structuring an Effective Presentation

Facts about CISO Board Presentations

Frequency

The majority of CISOs present to boards once a quarter for 30 minutes, with an annual deep dive that may take an hour. They reported that their allotted presentation time is often reduced.

Preparation Time

For each 30-minute session, it takes between 40 and 85 hours over a period of two to three weeks to prepare the board presentation.

This includes 5 to 25 revision cycles as part of the internal review process.

Length

As a best practice, board presentations should be 5-7 slides at most.

Ensure there is a way to present key information in two slides in case of time shortage.

Recommended Outline for a Typical Board Presentation

There are 4-7 top categories to present to a board. For consistency, keep the same format in every presentation.











- **Situational Awareness:** Present current and emerging trends from your sector and their relevance to the board. Show who, why, and what they are attacking; and how to mitigate risks.
- **Incident Response:** Present noteworthy incidents that didn't need immediate escalation. Show how each issue was handled, including the controls in place you found helpful. Use a storyboard to depict an external breach, or an incident tracked internally (see example in figure 2)
- **Risk/Threat Lens:** Define the organization's risk appetite and risk tolerance and present your operational and continuous assessment processes. Summarize in business terms the critical, unresolved security risks, your remedial action and controls and the residual risk expected following remediation.
- **Capability Maturity Aligned to a Common Framework** – Measure maturity across all entities and in all locations and show weak links. Show trends quarter by quarter. Note that many CISOs from all industries align their security program to the NIST Cybersecurity Framework.
- **Strategy:** Provide an 18-month outlook, based on an assessment of threats, regulations, business objectives, risk profile, and program maturity. Two slides are proposed: i) a refresher on program drivers and capability tied to the drivers, and ii) a summary of how the security program is moving toward the target milestones. Demonstrate progress, pace, alignment, and continuous improvement.

If time permits, add others:





- **Peer Parity** shows your maturity level and how you compare with other similar brands and the broader sector.
- **Cyber Insurance** – Provide a qualified answer to the question “Do we have enough?”
- **Emerging / Hot Topics** – Focus on trending topics (e.g. third-party risk management, targeted threat detection, rapid response, business-driven strategies on cloud adoption, mobility).

Appendix A - Survey Questions & Summary of Answers








Reporting to the Board: Most Common Themes

Topics typically included in CISOs board decks	Popularity
Executive Summary: Threat vectors for your industry	69% 
Cybersecurity Program Maturity Chart & Progress towards Goals	69% 
Top Cybersecurity Risk Exposure / Highlight Progress Accomplishments	67% 
Executive Summary: Recent breach headlines, lessons learned and impact to your organization	64% 
Top Cyber Program initiatives and business outcomes	59% 
Changes in the Business Landscape that impact cyber program	46% 
Next Steps / Final Ask	46% 
High-Level Business Goals and Objectives	36% 
Comparison Benchmarking	21% 
Other topics	3% 



Popular Dashboard Visuals in Board Decks

Dashboards presented in board decks	Popularity
Current State of Security Program	54% 
Controls in place and status	33% 
Other	8% 
High level SOC metrics	3% 

Common Frameworks Used to Measure Cybersecurity Program Maturity

Frameworks used to measure Cybersecurity Program Maturity	Popularity
NIST CSF	36% 
ISO 27001	18% 
SANS Top 20	10% 
Internal framework	5% 
FFIEC Cybersecurity Assessment	3% 
Gartner	3% 
HIPAA/HITECH	3% 

Frequent and Challenging Questions CISOs Asked by Boards

Frequent questions CISOs are asked from Board	Question Popularity	Degree of Challenge to the CISO (each question ranked 1-5; numbers below show aggregated scores)
Are we secure? How do we know?	61% 	141
How do we know if we have been hacked or breached?	48% 	122
Are we spending the right amount on our cybersecurity program?	39% 	107
How do we compare to peers within the same industry?	48% 	98
How effective is our security program?	39% 	98
Is our investment in cybersecurity going towards the right priorities?	43% 	97
What are the key cyber threats that influence the company's cybersecurity risk strategy?	43% 	87
How confident are you that we will be out of the news?	35% 	85
Do we have cyber insurance? How much coverage do we need?	13% 	82
Have we been breached? What was learned? How will breaches be prevented in the future?	35% 	80
What do we consider our most valuable assets?	30% 	73
How are we managing risk? What is our risk tolerance?	22% 	63
Is our security program aligned with our business revenue streams?	9% 	59
Where do management and our IT team disagree on cybersecurity?	9% 	53

Appendix B – Key Contributors

Kudelski Security

- Mark Carney, Vice President Global Services
- John Hellickson, Global Managing Director, Strategy and Governance
- Ryan Spanier, Global Director of Research
- Shiri Band, Global Solutions Marketing

Client Advisory Council

- Almir Hadzialjevic, VP, Enterprise Risk & Security, Aaron's Inc.
- Scott Goodhart, VP and CISO, AES Corporation
- Jason Lish, CSO, Alight Solutions
- John Hochevar, CISO, American Transmission Company
- Pete Naumovski, VP and CISO, Blue Cross Blue Shield Association (BCBSA)
- Don Kleoppel, CSO, Cerner Corporation
- Kyle Starkey, CISO, Early Warning
- Tony Spinelli, COO, Fractal Industries
- Robert A. Drawer, Global Director of IS, Mayer Brown LLP
- Ginny Davis, CIO and CSO, Technicolor
- Erik M. Hart, CISO, Zebra Technologies
- Mark Butler, CISO, Qualys

