

CISO REDEFINED:  
**NAVIGATING C-SUITE PERCEPTIONS  
& EXPECTATIONS**

---

LIMITING RISK AND CLOSING THE CYBERSECURITY  
COMMUNICATIONS GAP



***Foreword from Meredith Griffanti*** - Senior Managing Director  
Global Head of Cybersecurity & Data Privacy Communications

As our Cybersecurity & Data Privacy Communications team continues to expand across the globe, I have had the opportunity to spend time in different countries with cybersecurity and business executives whose companies have vastly different ways of doing business as well as distinct cultural and communications norms, depending on where they are headquartered. The CISO Redefined research is a window into what our team sees as a common pain point in cybersecurity governance and management –no matter what geographical region the organization operates in– the CISO struggles to appropriately and confidently communicate with the Board and the C-suite.

Given that cybersecurity continues to be a top risk and governance issue for organizations globally, I recommend all Directors, C-suite leaders and CISOs alike read this research to better understand how to find common ground and where the disconnects lie. We often hear about “leveling up” the Board and C-suite leaders when it comes to cybersecurity, but seeking out training opportunities specifically for CISOs, like FTI Consulting’s Secure Your Seat program, is an important part of limiting risk and closing the cybersecurity communications gap, too.

I hope this research, conducted by our Digital & Insights team, encourages organizations to take action.

A handwritten signature in white ink, appearing to read 'M. Griffanti', located in the bottom right corner of the text area.

# Setting The Scene

The risk posed by cybersecurity vulnerabilities has never been greater. As senior executives face greater accountability for cybersecurity risk from regulators, investors and other stakeholders, FTI Consulting set out to build upon our inaugural CISO barometer – which surveyed CISOs and information security leaders on rising pressures on their roles, leadership and operations – to understand C-suite executives' perceptions and expectations of their CISOs. While the initial survey uncovered a communications gap between CISOs and executives, these new findings indicate the perceived gap feels even greater to the C-suite.

## Part I: 2022 CISO Survey Summary

### Methodology:

**165** CISOs surveyed

**U.S. only**

### Key Findings:

Internal and external scrutiny has increased

CISOs said they experienced difficulty in communicating with internal senior leaders

CISOs reported a communications disconnect with senior leaders regarding cybersecurity priorities

CISOs claimed they make things sound better than they are to the Board

## Part II: 2024 C-Suite Executive Survey Introduction

### Methodology:

**787**  
C-suite Executives surveyed

**Global Audience**  
5 continents

### Main Research Questions:

Do executives perceive the same communications disconnect as CISOs?  
Is this gap perhaps even more pronounced?

Is there consistent misalignment?

What are executives' thoughts on key cybersecurity priorities?

Is there need for additional training?




CISOs

Communications Disconnect Between CISOs and Leadership

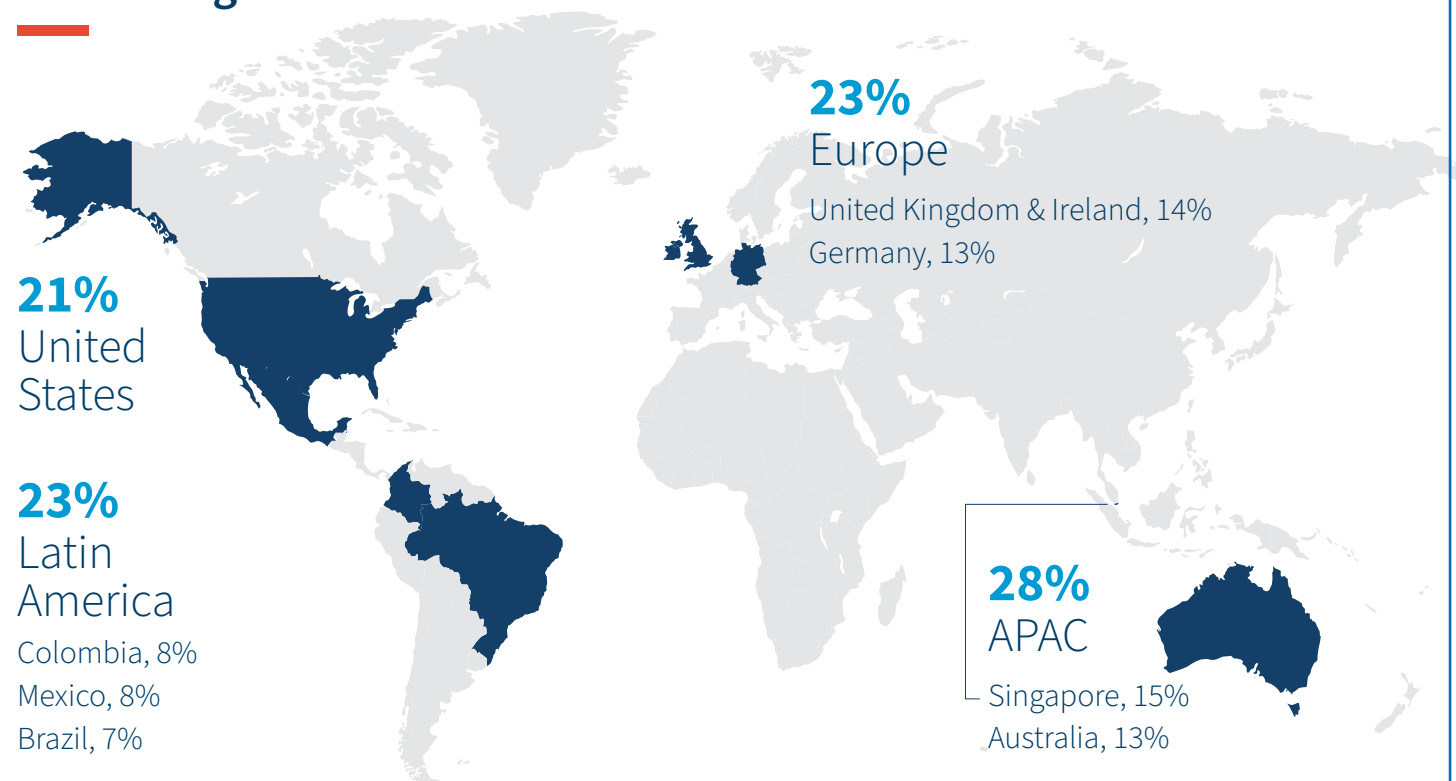
C-Suite



# Global Methodology

FTI Consulting's Digital & Insights team conducted a survey online among n=787 C-suite executives at organizations with 500+ employees across FTI's key industries. Conducted online in November 2023. Previous research<sup>1\*</sup> was conducted among n=165 CISOs (denoted throughout by  throughout the rest of the report). For any questions about the methodology, please contact [James.Condon@fticonsulting.com](mailto:James.Condon@fticonsulting.com).

## Global Regions



## Annual Revenue

**\$21.5 Trillion**

Sum Aggregate Revenue

**\$27 Billion**

Average Revenue

## Number of Employees

**3,690,000**

Total Employees

**4,700**

Average Number of Employees

## Industry Sectors

**18%** Retail

**14%** Industrials

**13%** Healthcare & Life Sciences (HCLS)

**13%** Financial Services

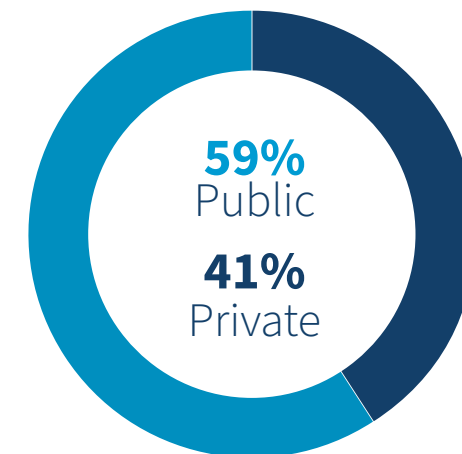
**13%** Technology, Media, & Telecommunications (TMT)

**12%** Public Affairs & Government Relations (PAGR)

**11%** Energy (ENR)

**5%** Other

## Public/Private



## Position

**19%** CEO

**10%** VP

**23%** CFO

**21%** Other C-Suite

**27%** Director/Manager

<sup>1</sup>"CISO Communications Redefined," FTI Consulting (2022), <https://fticonsulting.com/ciso-communications-redefined/>

# Key Insights



Companies remain vulnerable to cybersecurity threats while expectations of CISOs are increasing.

Incidents are increasing with **9 in 10 respondents** claiming they have experienced a cyber incident in the last 12 months.

**87% of execs** say they have increased their CISO's decision making responsibilities in the last 12 months, likely to account for the evolving cybersecurity threat landscape.



CISOs aren't fully prepared to communicate with leadership.

**One-in-three** senior executives perceive their CISOs as being hesitant to raise potential vulnerabilities to leadership's attention, with a similar proportion believing their CISO is making things sound more optimistic than they actually are.

**Nearly four-in-ten** of execs feel their CISO is not completely prepared to communicate with key internal and external stakeholders, with more than one-third not fully prepared to communicate with leadership.



CISOs struggle to demonstrate key leadership skills to Execs.

**31% of execs** do not fully understand technical concepts used by the CISO.

**62% of executives** reported their CISOs' direct communication skills do not exceed their expectations.

**58% of CISOs** struggle to communicate technical language in a way senior leadership can understand (from 2022 CISO Survey).

**66% of CISOs** feel senior leadership struggles to understand their role (from 2022 CISO Survey).



Execs support communications training programs for CISOs, with many citing it as an immediate need.

**98% execs** support more funding for CISO communications and presentation training.

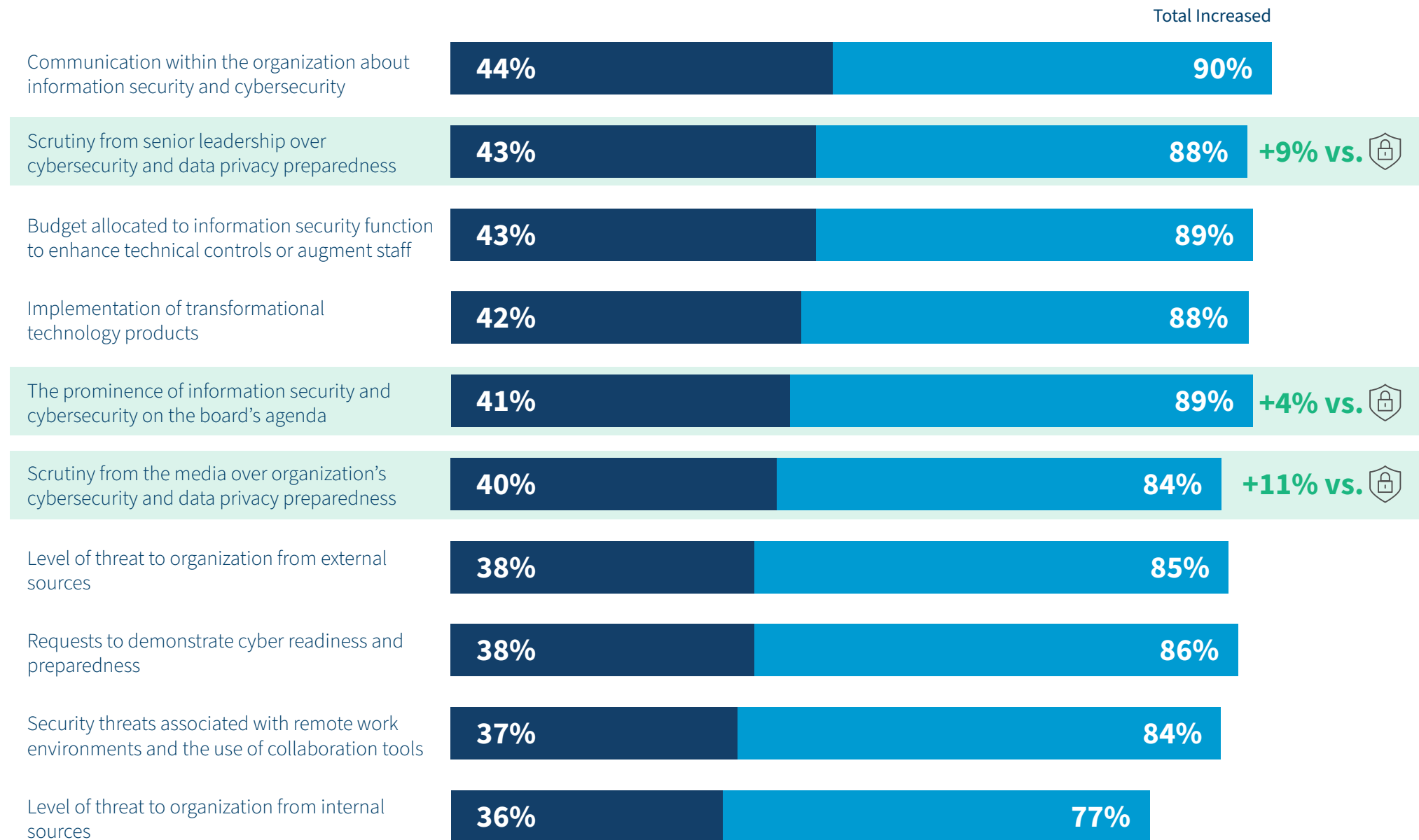
**45%** say there is an immediate need, especially for companies with more than 2,500 employees.

Executives say the biggest gaps to address in training are related to **anticipating threats, raising employee awareness, communicating ROI, and cyber risk.**

As incidents increase, scrutiny and pressures abound from all sources, forcing organizations to prioritize cybersecurity and shining a light upon the role of the CISO.

## Changes in organization over last 12 months<sup>1</sup>

Significantly Increased    Somewhat Increased



<sup>1</sup>Denotes the opinion of n=165 CISOs in FTI's 2022 Research, CISO Communications Redefined, <https://fticomunications.com/ciso-communications-redefined/>

## Information security and cybersecurity top the list of C-suite priorities in 2024.

**94% of executives say information security has increased in prominence over the past 12 months, and a majority consider cybersecurity to be a critical or high priority.**

Interestingly, this percentage was greater than that of CISOs in the October 2022 survey, as only 85% of CISOs reported that the prominence of information security and cybersecurity in the Board's agenda has increased. It is clear both C-suite executives and CISOs greatly feel mounting internal and external pressures on cybersecurity programs. Notably, cybersecurity lands 6% higher than customer experience and satisfaction when looking deeper into an organization's priorities.

These pressures are likely due to the evolving threat landscape, regulation, the prominence of cybersecurity incidents, and the attention and priority the programs are receiving from the Board level as well as external scrutiny from media and stakeholder groups.

**In fact, C-suite executives perceive even more scrutiny from senior leadership, board members, and the media on cybersecurity preparedness compared to the opinion of the CISOs we surveyed in 2022.**

**94%** say information security has increased in prominence over the past 12 months.

### Cyber Security Priority Level



### Organizations Top Priorities

- 1** **39%** Information and Cybersecurity
- 2** **36%** Operational Efficiency and Process Optimization
- 3** **33%** Customer Experience and Satisfaction
- 4** **32%** Supply Chain Optimization and Vendor Management
- 5** **31%** Environmental, Social, and Governance Initiatives

## As cybersecurity budgets increase, CISOs are expected to communicate the return on investment (ROI).

As cybersecurity advances in the risk register, senior leaders expect to make significantly increased investments in their cybersecurity programs-- with investments expected to increase across a range of areas, including ensuring appropriate IT infrastructure is in place, conducting employee training programs, and preparing the organization for cybersecurity incidents through incident response plans, preparedness projects, and senior leadership trainings.

**Of note, executives reported that cybersecurity budgets will increase an average of 23% over the next one to two years, with an even further projected increase of 36% more than current budgets in the next three to five years.**

This increased spending--while no doubt welcomed by CISOs--will likely lead to greater scrutiny of the organization's cybersecurity strategy and the CISO's role in that. CISOs will need to engage with senior leadership to ensure investments are accurately allocated in line with senior leadership and board expectations, as well as tie the results of this investment to actual business outcomes that resonate with senior leaders.

**Notably, employee training and security awareness programs are listed as the second highest priority for organizations to make this year, as C-suite executives expecting their information security teams to invest time and money into internal information sharing.**



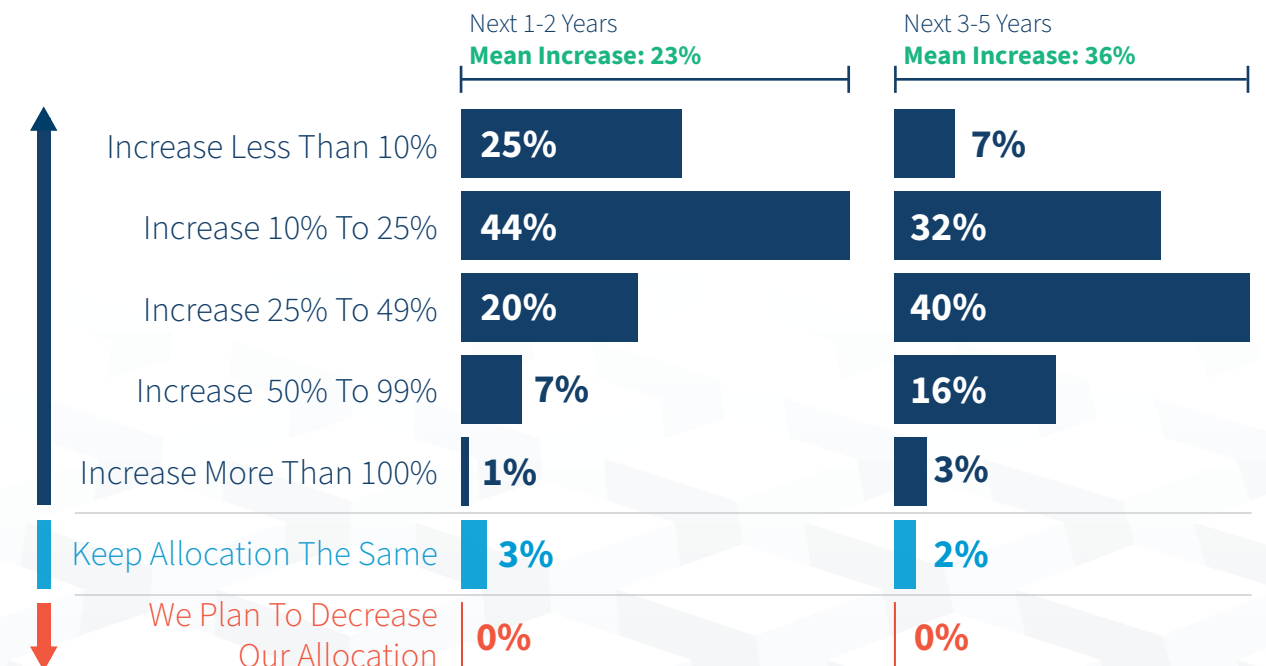
*“Cybersecurity is an increasing priority and spend for organizations, and with this, CISOs are being forced to step out from behind the keyboard and into the spotlight.”*

**Orla Cox** - Senior Director  
Cybersecurity & Data Privacy Communications

## Top 5 Expected Investments

- 1 **43%**  
Updating or Upgrading IT Infrastructure
- 2 **42%**  
Employee Training and Security Awareness Programs
- 3 **40%**  
Update Our Business Continuity and Disaster Recovery, Incident Response and Crisis Communications Plans
- 4 **38%**  
Assessing Cyber Crisis Preparedness And Conducting Tabletop Exercises or Simulations
- 5 **37%**  
Preparation of Senior Leadership Team to Manage Unexpected Crises

## Expected Increase Spend





As cybersecurity oversight grows and budgets increase, CISOs are expected to better articulate cyber risk and their strategic plans for mitigating it, but often fall short.

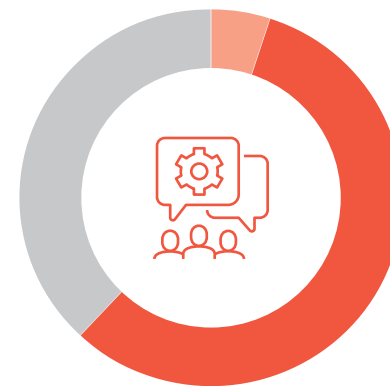
The combination of increasing budgets, expanded responsibilities of the CISO, and a push for greater leadership oversight of cybersecurity means that C-suite executives desire more visibility into the return on investment for cybersecurity programs.

However, many executives feel that their CISOs struggle to communicate ROI, are more optimistic with their assessments than perhaps reality suggests, and often fail to effectively translate their plans into terms that resonate with the broader business.

**One-in-three executives indicate that they do not fully understand technical concepts used by CISOs and suggest the level of direct communications around cybersecurity does not exceed their expectations.**

As discovered in 2022, 66% of CISOs reported senior leadership struggles to fully understand their role within the organization--meaning that CISOs also seem to be aware of this gap in understanding. Notably, with the budget increases, this disconnect was seen most strongly among Chief Financial Officers (CFOs).

Although there are greater expectations for CISOs, communication concepts like risk acceptance, return on cyber investments and progress against long term strategic plans for security maturity are complicated and can be nebulous – but critical for leadership and the Board to understand. Therefore, there is an even greater need for CISOs to hone their communications skills and deliver an update to the Board in a clear, concise and crisp presentation each quarter.



**62%**  
say level of direct communications from CISO **does not exceed expectations**







▲ *Latin America, 65%*



**31%**  
**do not fully understand**  
technical concepts used by the CISO

### Top Positions Who Don't Fully Understand CISO Role



|   |            |
|---|------------|
|  Chief Financial Officer       | <b>64%</b> |
|  Chief Marketing Officer       | <b>56%</b> |
|  Chief Human Resources Officer | <b>55%</b> |
|  Chief Compliance Officer      | <b>55%</b> |
|  Members of The Board          | <b>53%</b> |
|  Chief Executive Officer       | <b>43%</b> |

CISOs seem to be falling short in demonstrating the key leadership proficiencies expected from executives. They struggle to manage internal and external relationships—dynamics that can directly impact the bottom line and reputation of an organization.

As CISOs are given more responsibility and have higher expectations to be business leaders, there is a push for organizations to build a top-down “culture” of cybersecurity to raise the profile and influence of CISOs both within and outside of the organizations.

**100% of the top five attributes a CISO needs, according to executives, focus on leadership qualities—notably, 4 out of 5 attributes clearly define a need for CISOs to harness core proficiencies rooted in communications.** Yet these same skillsets are the ones in which CISOs currently struggle the most, despite executives wanting their CISOs to be more visible to leadership and across the wider organization.

**While 36% of executives expect their CISOs to be adept at building and managing external relationships, in 2022 52% of CISOs claimed managing communications with internal and external stakeholders is the biggest challenge when responding to an incident.** Ultimately, this gap in communication highlights the importance and value of managing relationships both internally and externally prior to, during, and following a live incident.

**Additionally, 36% of executives also reported they expect CISOs to build and manage internal relationships, but 23% of executives believe there is a siloed approach to information security.** This “silo” mentality can lead to misinformation and could cause confusion and lack of communication around cybersecurity across an organization.

Overall, CISOs must now approach their role as business leaders and not just technical experts.

## Top 5 Attributes CISOs Need



1

45%

Effectively Manages Security Budgets And Resources



2

38%

Easily Translates Technical Jargon Into Understandable Terms



3

38%

Skillfully Leads During Times of Crisis



4

36%

Adept At Building And Managing External Relationships



5

36%

Able to Develop and Maintain Internal Relationships



**“Amidst today’s risk landscape, new regulations, and increasing scrutiny, CISOs must work to master a business-centric skillset to meet the new demands of their evolving role.”**

**Jamie Singer** - Senior Managing Director  
Co-Head, Cybersecurity & Data Privacy Communications

Executives also do not feel strategically aligned with cybersecurity leaders, posing additional organizational risk.

**Despite this increased decision-making power, budget spend, and expectations for CISOs to take on leadership roles, nearly half of C-suite respondents do not consider their leadership priorities to be completely aligned with those working in their information security and cybersecurity function. 53% of CISOs also reported their priorities are not completely aligned with those of senior leadership.**

Further, in 2022, 82% of CISOs claimed they felt a need to positively exaggerate in front of the Board, and interestingly, 31% of executives surveyed also recognize this as a CISO's greatest challenge. This likely occurs because cybersecurity and information security leaders do not know how to appropriately communicate risk and are afraid it will reflect poorly on their programs.

**Further, 30% of executives felt their CISO is hesitant to raise concerns about the organization's vulnerabilities, thus perpetuating skepticism within the cybersecurity program.**

This misalignment and inability and hesitation to appropriately communicate cybersecurity risk and poses a significant challenge for organizations. With regulators and other stakeholders increasingly holding senior leadership accountable for cybersecurity, it is critical that they have a clear and accurate picture of organization's level of cyber risk and that the appropriate measures are being put in place to manage this. While both executives and CISOs both agree that there is a misalignment of priorities, many organizations have not yet identified a plan to address this gap.


## Organizational priority versus cybersecurity actions



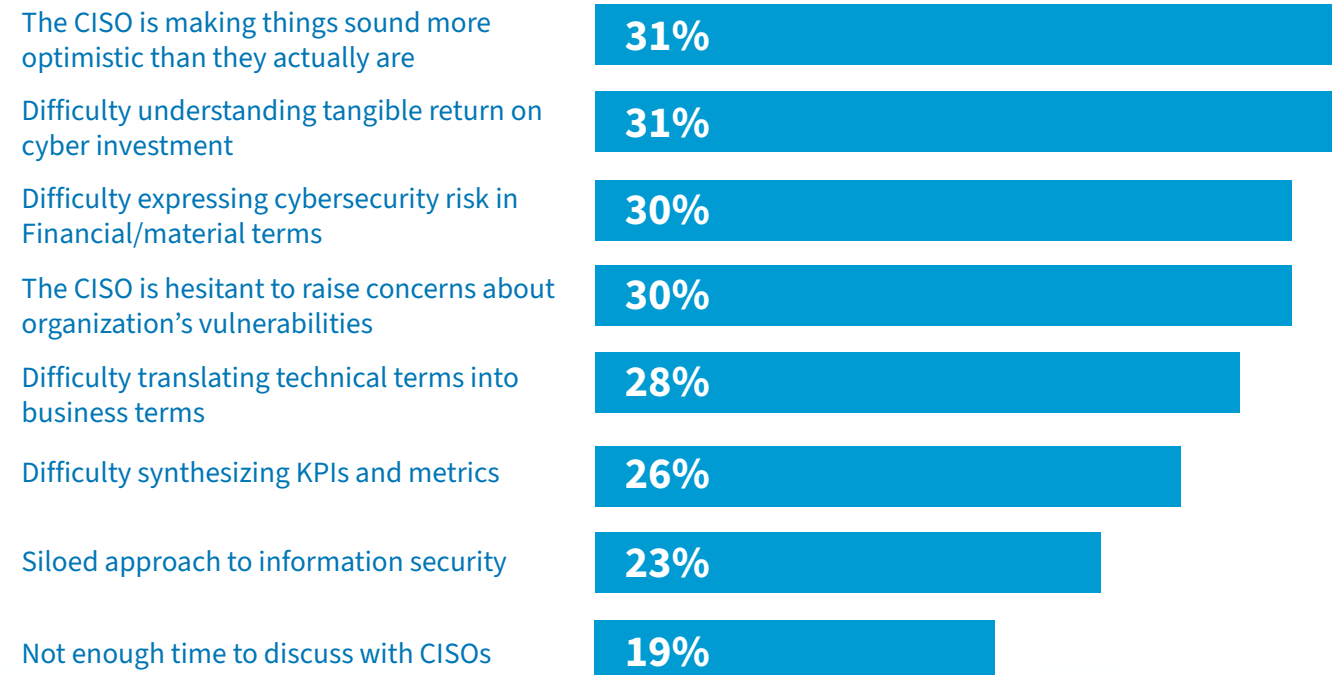
**46%**

Of Executives do not feel completely aligned with their CISOs

**53%**

Of CISOs do not feel completely aligned with their Executive team 

## Common Challenges





***“We see it so often where CISOs tend to paint a rosier picture than reality. This is a huge issue – company leadership MUST accurately understand the cyber risks they face – otherwise they can’t govern them effectively and they’re blindsided when a breach happens.”***


**Meredith Griffanti** - Senior Managing Director  
Global Head of Cybersecurity & Data Privacy Communications

Interestingly, both CISOs and C-suite executives recognize the misalignment and challenges facing the CISO role within an organization.

### CISOs' Challenges Communicating to Senior Leadership

**66%**  Feel senior leadership does not fully understand the CISO role within the organization.

**82%**  Feel like they have to make things sound better than they really are in front of the board.

**58%**  Struggle to communicate technical language to senior leadership in a way that they can understand.

### Senior Leadership's Challenges Communicating with CISOs

**30%**  
The CISO has difficulty expressing cybersecurity risk in financial/material terms

**31%**  
The CISO is making things sound more optimistic than they actually are

**31%**  
Difficulty understanding tangible return on cyber investment

**28%**  
The CISO has difficulty translating technical terms into business terms

**30%**  
The CISO is hesitant to raise concerns about organization's vulnerabilities

**19%**  
Not enough time to discuss with CISOs

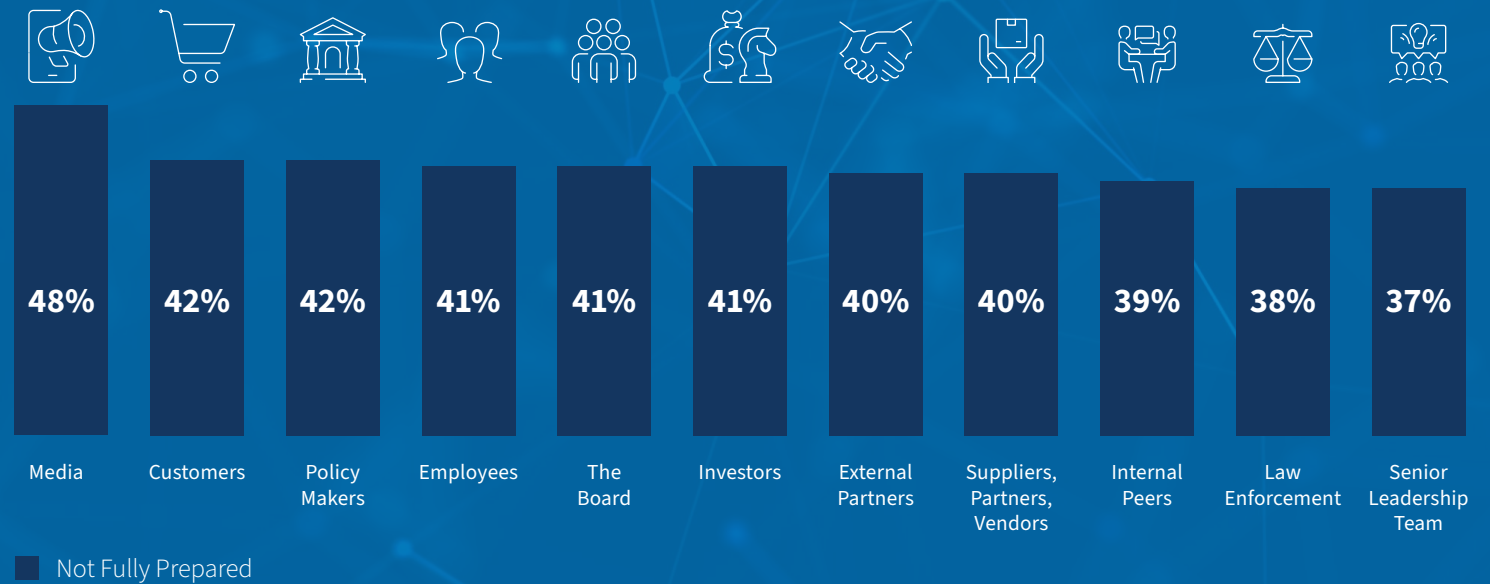
Concurrently, a plurality of executives feel CISOs are not fully prepared to communicate with the Board or leadership.

In the event of a cyber incident, many executives surveyed believe CISOs are not completely prepared to communicate with the most important internal and external stakeholders of their business. Notably, executives cite a lack of preparedness across a variety of critical internal and external stakeholders, who both serve as a mouthpiece for an organizations' response to an incident or whose opinion directly impacts the organization's bottom line. Though CISOs need to evolve into business leaders and develop new skillsets in the current landscape, executives largely do not feel as though they are prepared to communicate with key stakeholders, which could have significant business impact.

**Further, executives cited a lack of preparedness to effectively communicate the issues at hand to law enforcement and policymakers.**

With this newfound decision-making power, articulating their response, the decision points, and answering executive questions--especially related to actions taken during a live incident-- is now critical for CISOs. This will become more of an issue in the coming years as regulators look critically at CISOs and their role as the cybersecurity advisor to their Boards. Cognizant of the risks and vulnerabilities is one task, but fail to resolve the issue or, at times, sufficiently raise them within the company, creates inherent liability for the CISO and their organization's leadership team. This can lead to dramatic consequences for a business, including loss in customers, loss in revenue, legal action, and lasting harm to an organization's reputation.

## Preparedness Challenges For Stakeholder Communications



*“There’s a clear friction point between C-suite communication expectations and a CISO’s operational reality. CISOs are being asked to serve as company spokespeople but many are simply not prepared to do so.”*

**James Condon** - Managing Director  
Head of Research, Digital & Insights

To close this perceived communications gap and address the resulting organizational risk, executives support more funding for CISO communications and presentation training, with many characterizing this as an immediate need for CISOs as part of their organization’s cybersecurity preparedness.

With enhanced responsibility and expectations, executives are more than willing to invest in their CISOs and support training programs that will ultimately lead to fluid communications internally around cybersecurity and impact the bottom line.

Because failing to address these issues could lead to larger implications for the business, nearly all respondents support more funding CISO communications and presentation training, with nearly half characterizing this as an immediate need.

Currently, executives feel there are several large gaps that could be addressed with expert trainings, including an emphasis on better methods of communication and quantification of risks for stakeholders. As the role of the CISO continues to evolve, there remains a communications responsibility on CISOs, both as internal advocates and external spokespeople.

Executives want to set CISOs up for success, understanding that having the ability to quantify cyber risks and returns is a skillset now required for cybersecurity leaders. Communications training and coaching will not only make the life of the CISO easier, but it will ultimately set the company up for success and lead to smarter, quicker decisions down the line.

**98%** support more funding for their CISO’s presentation and communication training.

### Cyber Security Priority Level



### Top 5 Topics for CISO Communications Training

- 1 31%** Strategies to Anticipate and Counteract Future Cyber Threats and Trends
- 2 27%** Collaborative Approaches to Security Awareness Training for Employees
- 3 27%** Methods for Quantifying and Communicating Cybersecurity Risks to Stakeholders
- 4 27%** Guidance on Communicating Technical Information in a Clear and Precise Manner
- 5 26%** Approaches to Building a Proactive and Adaptive Cybersecurity Culture



*“Your two greatest allies [in a breach] are communication and optionality. Communication is being able to lay out the story of where things are, and to make sure everyone is rowing in the same direction. It’s being able to communicate the current status, and your plans, to regulators—and at the same time being able to reassure your customers and make sure they have confidence that you’re going to be able to navigate to the other side.”*

**Evan Roberts** - Senior Managing Director  
 Co-Head, Cybersecurity & Data Privacy Communications

# Invest in Addressing the Communications Gap through FTI's CISO Communications Training Program



FTI Consulting's Data Privacy and Cybersecurity Communications practice has an unmatched ability to take complex cybersecurity issues and break them down into easy-to-understand concepts. We often hear from CISOs after an incident that they want our continued help refining their quarterly Board presentations or general communications skills so that they better resonate with company leadership. We welcome CISOs to lean into our expertise in both cybersecurity and communications with the launch of **Secure Your Seat (SYS)**, a research-driven communications and board readiness training program uniquely created for CISOs.

The six-week program guides CISOs through customized, weekly one-on-one training sessions that enable them to better communicate with senior leaders, navigate the expectations of the Board, translate technical language and KPIs into layman's terms and enhance their quarterly and annual Board presentations. Participants also receive hands-on, one-on-one messaging and presentation training, with an opportunity to practice their Board presentations in front of our Advisory Council, comprising a diverse group of C-suite executives and sitting Board directors with cybersecurity know-how.

## Introducing Secure Your Seat: A CISO Communications Training Program

- Survey to Identify Areas for Improvement
- Goal-Setting
- Brand Analysis
- Public Speaking
- Message Refinement and Presentation Delivery Workshop
- Quarterly/Annual Cyber Board Deck Enhancement
- Board-Ready CV Development
- Mock Board Presentation & Feedback Session (in front of our SYS Advisory Council)

For more information about Secure Your Seat, please contact [SYS@fticonsulting.com](mailto:SYS@fticonsulting.com) and a team member will be in touch.



*"FTI's Secure Your Seat Program is run by a team of world-class experts who live and breathe cyber communications. Whether you are a CISO new to the role, or a seasoned CISO like myself, this program is essential to preparing cybersecurity leaders to clearly articulate cybersecurity objectives, risks and opportunities to the senior-most executives in your organization."*

**Jesse Whaley**  
Chief Information Security Officer, Amtrak

# CISO REDEFINED: NAVIGATING C-SUITE PERCEPTIONS & EXPECTATIONS



**MEREDITH GRIFFANTI**  
Senior Managing Director  
Global Head of Cybersecurity & Data Privacy Communications  
meredith.griffanti@fticonsulting.com



**EVAN ROBERTS**  
Senior Managing Director  
Co-Head, Cybersecurity & Data Privacy Communications  
evan.roberts@fticonsulting.com



**JAMIE SINGER**  
Senior Managing Director  
Co-Head, Cybersecurity & Data Privacy Communications  
jamie.singer@fticonsulting.com



**JAMES CONDON**  
Managing Director  
Head of Research, Digital & Insights  
james.condon@fticonsulting.com



**CLEMENTINE BOYER**  
Senior Director  
Cybersecurity & Data Privacy Communications  
clementine.boyer@fticonsulting.com



**ORLA COX**  
Senior Director  
Cybersecurity & Data Privacy Communications  
orla.cox@fticonsulting.com



**COURTNEY BERRY**  
Director  
Cybersecurity & Data Privacy Communications  
courtney.berry@fticonsulting.com



**ELIZABETH MURPHY**  
Director  
Cybersecurity & Data Privacy Communications  
elizabeth.murphy@fticonsulting.com



**BRANDON CHATTIN**  
Director  
Digital & Insights  
brandon.chattin@fticonsulting.com



**ALLISON HUFNAGEL**  
Senior Research Analyst  
Digital & Insights  
allison.hufnagel@fticonsulting.com

## About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. ©2024 FTI Consulting, Inc. All rights reserved. [fticonsulting.com](https://fticonsulting.com)

FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals. ©2024 FTI Consulting, Inc. All rights reserved. [www.fticonsulting.com](https://www.fticonsulting.com).

## About FTI Strategic Communications

C-suites, Boards of Directors, and business leaders from around the world come to FTI Consulting with their most complex, business-critical issues that require diverse skill sets and integrated disciplines.

Our Strategic Communications division supports dozens of senior executives and high profile individuals with their social media strategies, content, and channel management — helping them mitigate risk and enhance their reputation by combining decades of deep subject matter expertise with functional and disciplinary experience.

## About FTI Cybersecurity & Data Privacy Communications

Our Cybersecurity & Data Privacy Communications offering is one of the premier cybersecurity communications groups in the industry. Named the Cyber PR Firm of the Year by the Cybersecurity Excellence Awards in 2021, 2022, and 2023 and recognized by Chambers & Partners as a top global crisis communications provider, the group provides expert crisis communications counsel and support in cybersecurity preparedness and throughout the entire lifecycle of an incident, helping organizations around the world mitigate risks, improve continuity, and protect their relationships with stakeholders before, during, and after an incident.

Put simply, we help our clients to communicate effectively – across any channel – to protect and enhance their interests with key stakeholders.

## About FTI Digital & Insights

The Digital & Insights practice sits at the center of FTI Consulting’s multifaceted offering. Bringing together experts across data science and primary research, as well as digital and creative strategy and execution, we work alongside our subject matter colleagues to deliver a comprehensive, audience-first approach. These insights become the foundation on which integrated communications campaigns are built.



For more information and to contact our team please visit our **CISO Redefined webpage** ►

