EXPERTS WITH IMPACT™

CISO: COMMUNICATIONS REDEFINED

Navigating the Journey from Control Room to Board Room

As new threats, technologies, and intelligence arise, the cybersecurity world — and the roles of industry experts — have had to change with it. According to the FBI's 2021 Internet Crime Report[1], reported threats are on the rise and attack tactics continue to evolve — in 2021 alone, victims of cyber attacks lost $6.9 billion. With this evolution of the cybersecurity environment and growing threats, Chief Information Security Officers (CISOs) and information security leaders have felt rising pressures – both internally and externally – on their role, leadership, scrutiny, and operations.

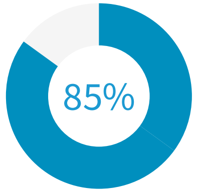
Against this backdrop, FTI Consulting conducted an online survey of n=165 CISOs and those in charge of information and cybersecurity, representing U.S. companies with $4.4 trillion in aggregated revenues and more than 528,000 employees, to delve further into these pressures and highlight key opportunities, as the expectations and realities of this role and the importance of communication continue to be redefined.

FTI CONSULTING™

[1] Internet Crime Report 2021," Federal Bureau of Investigation (March 22, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

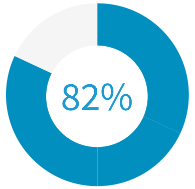
Executive Summary

Internal & External Scrutiny Has Increased



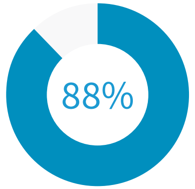
- **85%** of CISOs claim the prominence of information security and cybersecurity has increased on the Board's agenda in the last 12 months
- **79%** feel scrutiny from senior leadership over cybersecurity preparedness has increased
- **73%** believe external media attention and subsequent pressure on organizational cybersecurity preparedness has increased

CISOs Struggle to Communicate to Leadership



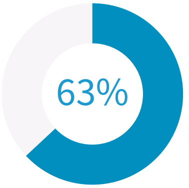
- **82%** claim they have to make things sound better than they are to the Board
- **66%** feel senior leadership struggles to understand their role
- **58%** struggle to communicate technical language in a way senior leadership can understand

Communication Is Critical, with Incidents on the Rise



- **88%** of CISOs have experienced a cyber attack or incident in the last 12 months
- Nearly half **(46%)** claim these incidents were not mitigated quickly
- **52%** claim managing communications with internal and external stakeholders is the biggest challenge when responding to an incident

Apparent Disconnect with Senior Leadership on Cyber Priorities



- **63%** claim their cyber concerns are not fully aligned with senior leadership
- **52%** feel their Board and senior leadership are not completely prepared for the cyber risks they foresee
- **40%** believe their organization is not fully prepared for proposed SEC rules on stricter cybersecurity governance

There is more pressure on CISOs to prove their worth

Against a backdrop of economic uncertainty and the constant shadow of threat actors working to undermine company security, it is clear that the role of the CISO and other equivalent information security roles are under more pressure than ever to demonstrate resilience, preparedness, and potential response, while also navigating the internal, and external expectations from many key stakeholders.

This increase in pressure is underscored by our research results, where

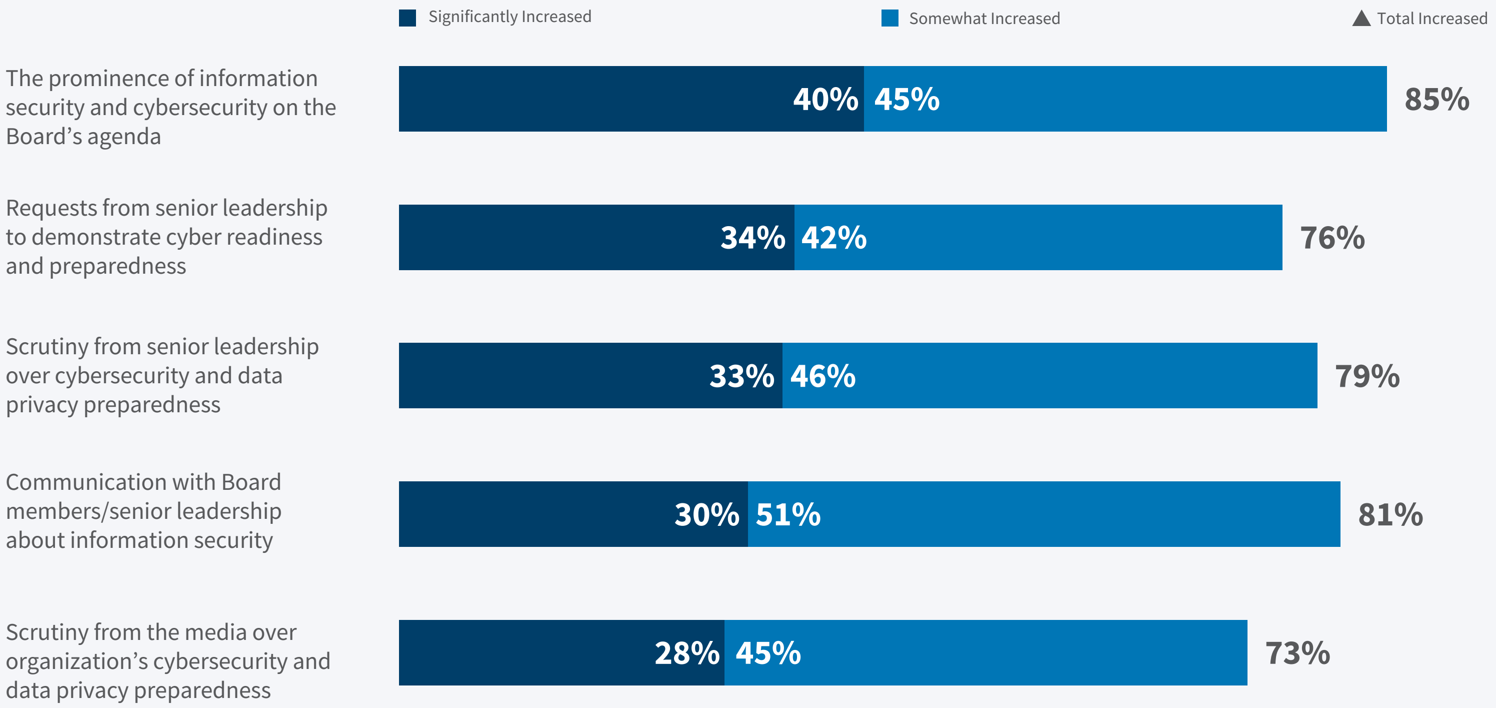
85% cited that the prominence of information security and cybersecurity in the Board's agenda has increased over the last 12 months, with 40% claiming it has "significantly increased."

Unsurprisingly, this correlates with far more activity and attention coming from senior leadership, with more than three quarters of CISOs claiming scrutiny from senior leadership over cybersecurity and data privacy preparedness has increased, followed by more requests from senior leadership to demonstrate the company's cyber readiness plans and preparedness.

Naturally, scrutiny abounds from external sources too, especially from the media. Over the last 12 months, CISOs claim the level of media scrutinization of their organization's cybersecurity and data privacy preparedness has increased, potentially magnifying the impact of any potential internal weaknesses or breaches into the public domain.

While 81% claim communication about information security with their Board and senior leadership has increased — and, with this, increased internal focus on the role of the CISO and the prominence of cybersecurity on the Board and senior leadership's agenda — pressure to more effectively and articulately communicate to this audience has become a priority.

Increase in Pressures over the Last 12 Months



> "It's undeniable that pressures on CISOs are rising as key internal stakeholders look to understand more about their organizations' cybersecurity vulnerabilities. It's now more important than ever for CISOs to communicate in a manner which transcends from technical jargon into operational, actionable intelligence.
>
> **JAMES CONDON**
> Senior Director
> *Digital & Insights*

CISOs and leadership struggle to communicate

This struggle potentially presents a problem for CISOs, with those who we surveyed suggesting there are a number of challenges they face when communicating to senior leadership.

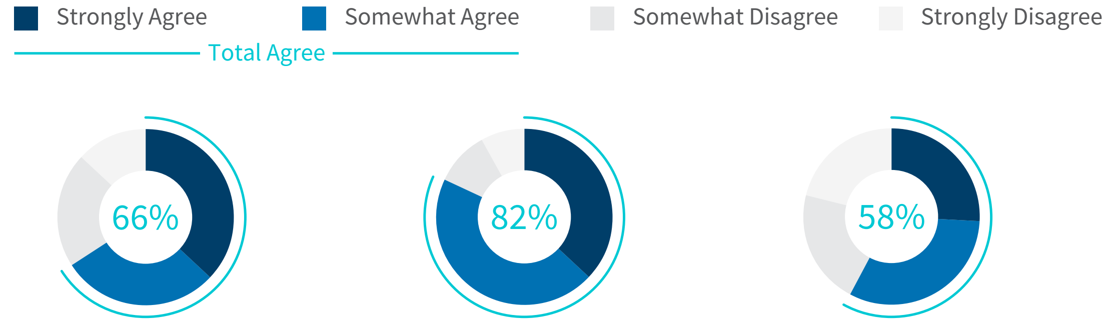
A majority (58%) claim they struggle to communicate technical language to senior leadership in a way that they can understand.

With mounting pressure, increasing requests, and expectations to hear more about the company's cybersecurity preparedness, communicating to senior leadership and other team members is a significant challenge for CISOs, who have to overcome technical jargon and explain their role in a clear, succinct, and impactful manner to those who may not have experience dealing with cybersecurity and data privacy related issues.

Moreover, 82% of respondents claim that when they do have the opportunity to communicate with the Board, they feel like they have to positively exaggerate in front of this audience, with more than one-third (37%) strongly agreeing with this statement.

With this perceived communications gap between CISOs and senior leadership, many feel misunderstood, and two-thirds (66%) believe senior leadership struggles to fully understand their role within the organization.

Challenges Communicating to Senior Leadership



Senior leadership struggles to fully understand my role within the organization

I feel like I have to make things sound better than they really are in front of the Board

I struggle to communicate technical language to senior leadership in a way that they can understand

> "Proposed changes to regulations, such as those led by the NYDFS and the SEC, will force companies to better capture the relationship between cyber risks and the balance sheet. By pushing companies to elevate the oversight of cybersecurity and treat cyber threats as a core business risk, regulators are also making a strong case to evolve the way and increase the frequency with which CISOs and the C-suite communicate.
>
> **ADRIANA VILLASENOR**
> Senior Director
> *Cybersecurity & Data Privacy Communications*

Leadership struggles to fully understand the role of the CISO

When diving deeper into this potential communications gap, the perception of those surveyed is that many in senior roles do not fully understand the CISO role.

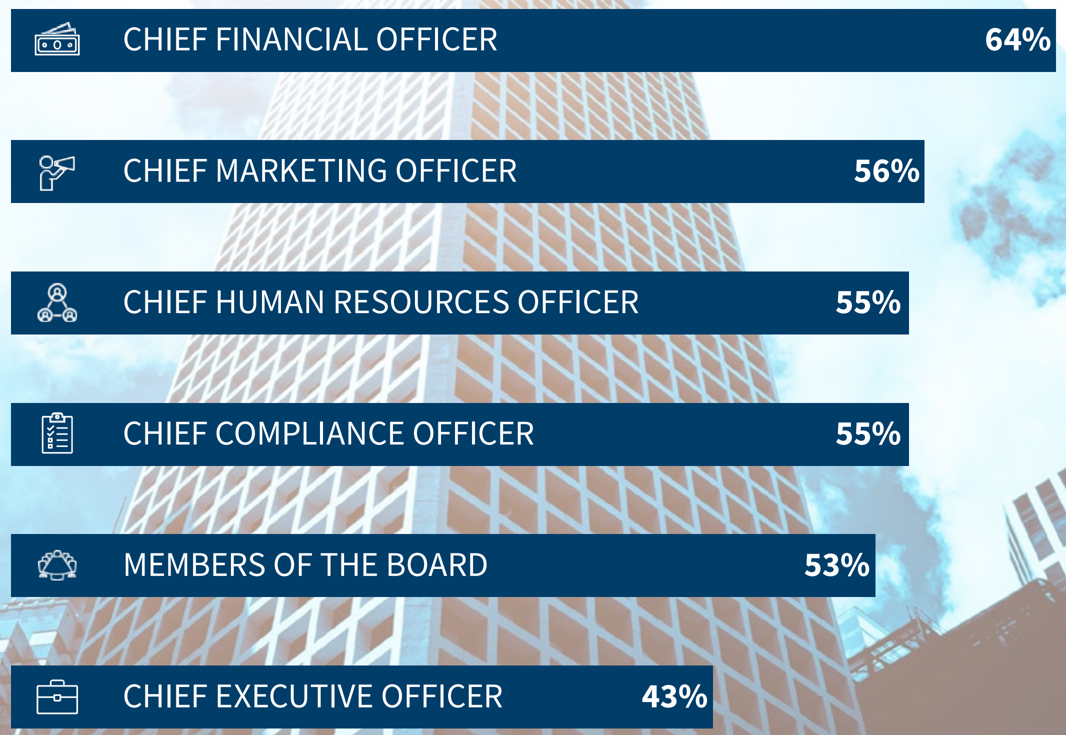
This disconnect is seen most strongly among Chief Financial Officers (CFOs), of whom 64% of respondents believe do not fully understand their role as CISO.

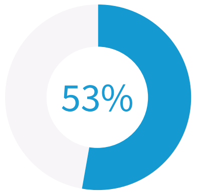
This is a particular concern considering many CFOs are directly in charge of the designation of cybersecurity budgets, and if they do not understand to what they are allocating financial resources, it could be allocated elsewhere in the business. This underscores the importance of CISOs to better communicate their role and their operational activity to this audience in particular.

The CISOs we surveyed clearly feel there was more of an endemic misunderstanding of their role across all levels of senior leadership. Perhaps surprisingly, a majority also believe those in the chief compliance officer role (55%) do no fully understand their role. Similarly, those in the chief marketing and chief human resources officer roles are perceived to struggle here. However, the Chief Executive Officer (CEO) is perceived to be the position most CISOs believe best understand their role, with 91% of respondents citing that the best way to help support them in their work is to report directly to the CEO.

That said, more needs to be done to communicate the role of the CISO effectively through company leadership structures to ensure alignment of information security and cybersecurity priorities. At the moment, over half of respondents (53%) do not believe these priorities are completely aligned with those of senior leadership.

Top Positions Who Don’t Fully Understand CISO Role





Say their information security and cybersecurity priorities are not completely aligned with those of senior leadership

> “
>
> Coordination at the executive level can take any incident response operation from good to great. In a cybersecurity incident, this need for top-level communication and organizational tactics is heightened because cyber is an extremely fast-moving and complicated environment. If CFOs and other executives do not have full clarity on the role of the CISO in managing risk, it can greatly impede a successful operational response.
>
> **JAMIE SINGER**
> Managing Director
> *Co-Head, Cybersecurity & Data Privacy Communications*

With incidents on the rise, communication between CISOs and leadership is even more critical

Of those surveyed, an overwhelming majority (88%) experienced a cyber incident over the last 12 months, the most common types of attacks being malware, ransomware, and distributed denial of service (DDoS).

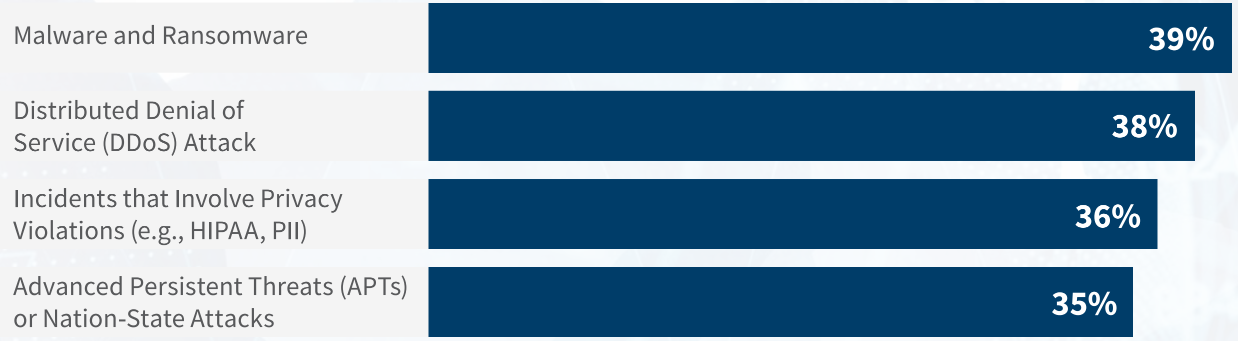
This reality has increased the pressure on CISOs to serve in a communications role.

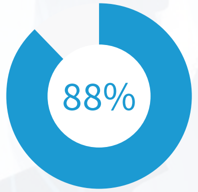
Ransomware and DDoS attacks in particular often need to be met with aggressive communications strategies, given the operational disruption commonly associated with these events.

More than any other cyber incident, ransomware most often places a communications burden on the CISO and information security (InfoSec) team. The fear that the malware may spread is extremely common – and customers, partners, suppliers, and other stakeholders may demand official assurances that there is no risk of contagion before resuming normal-course engagement with the victim organization.

With this overall rise in incidents, particularly in ones that require a fulsome communications response, it is critical for senior leadership and CISOs to coordinate closely and ensure their strategies – in terms of containment, remediation, restoration, and communications – are aligned and complementary.

Top Attacks/Incidents Experienced in the Last 12 Months





of organizations have experienced a cyber incident in the last 12 months

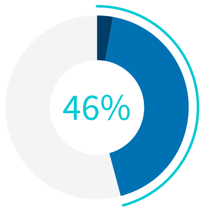
To best coordinate communications efforts in advance of an incident, organizations must have contingency plans in place to support their employees, investors, and customers and to offer accurate, timely responses to media interest. This means having the right resources and structures in place to support and inform key stakeholders. Poor communications or the lack of consistent communications during a crisis can create confusion and fear among stakeholders and lead to longer-term credibility issues. 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.

CISOs are challenged to manage communication with internal and external stakeholders in the face of an incident

Lack of preparedness can lead to a longer response time during an incident. For internal stakeholders, it creates fear and panic as they might feel that the company is hiding information or is not in the control of the situation. For external stakeholders, it gives them an opportunity to speculate and tell the story on behalf of the company if the company remains silent for too long. silent for too long. Instead, timely communications that reflect information the company is able to share, and in a transparent and supportive manner, can help mitigate reputational risks. This can occur simultaneous to the forensic investigation determining the cause and nature of the incident.

Almost half (46%) of the cyber attacks are not mitigated immediately in a number of situations because of roadblocks. Such challenges focused on managing communications between internal and external stakeholders account for more than half (52%) of those surveyed, responding to requests to complete security questionnaires (51%) and collaborating with multiple vendors during a crisis situation (47%).

After an incident, CISOs feel it’s difficult for them to rebuild trust with key stakeholders, either internal or external. Those challenges can be mitigated with a strong communications strategy, including crisis communications preparedness and incident response communications skills for C-suite, including CISOs.



of cyber attacks or incidents were not mitigated immediately. 3% of cyber attacks still cause lasting effects

- ■ Still trying to mitigate the effects
- ■ Mitigated but with delay
- □ Mitigated immediately
- — Total

Top 3 Challenges when Responding to an Incident

1. Managing communications with internal and external stakeholders
2. Responding to requests to complete security questionnaire and/or share indicators of compromise (IOCs) with external parties
3. Collaborating with multiple vendors in a crisis situation

> “Time is money, especially when it comes to responding to cyber attacks. In the midst of the chaos, it is incredibly important to manage communications efficiently and effectively, as to maintain the confidence of key stakeholders. If that doesn’t happen, trust will be lost which will be quickly followed by revenue.

MEREDITH GRIFFANTI
Senior Managing Director
Co-Head, Cybersecurity & Data Privacy Communications

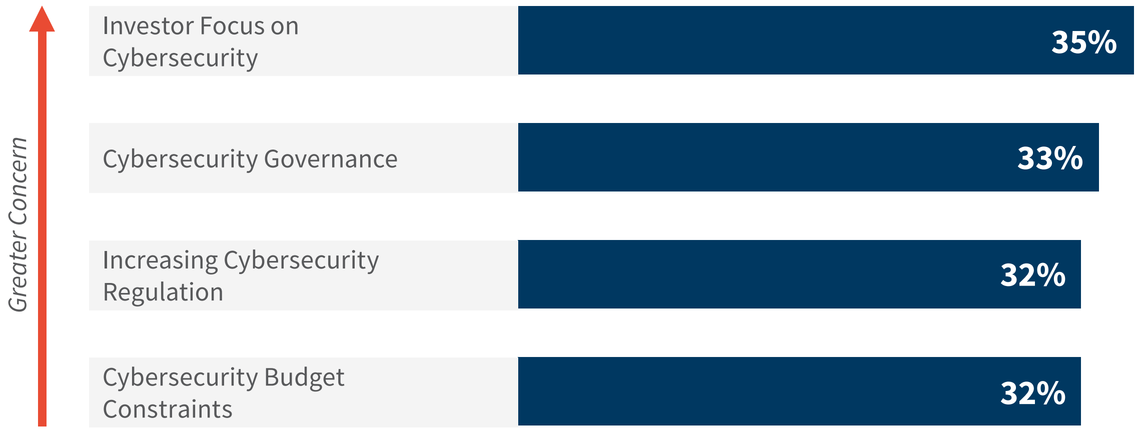
CISOs experience a disconnect with leadership on future cyber risk priorities & preparedness

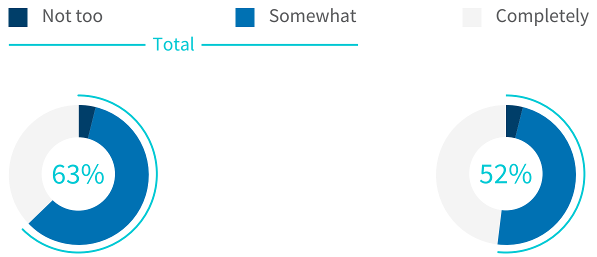
A third (33%) of CISOs surveyed cite cybersecurity governance as a concern, reflecting how investors and regulators alike are pushing for greater transparency and oversight of cybersecurity across the organization. CISOs recognize that, while this creates opportunities for them to raise their profile, it will also increase pressure on them, with budget constraints a concern for 32% of those surveyed.

Despite regulators and investors pushing for cybersecurity to be prioritized at the top level of the organization, over half of CISOs do not believe that their board and senior leadership are completely prepared for cyber risks, and 63% feel that their concerns are not aligned with senior leadership priorities – potentially leaving companies exposed to an incident or regulatory sanction.

To address this gap, and to prepare for the increased regulation that is likely on the horizon, CISOs will need regular engagement with the Board and senior leadership. However, they will need to be prepared for this engagement.

Future Top Risk Areas of Concern For Their Organization





Think their concerns are not fully aligned with those of senior leadership

Think their board and senior leadership are not completely prepared for risks

> A regulatory landscape that is pushing oversight responsibility up to board level means that the modern CISO needs to be able to communicate dynamic and fast-changing cyber risks in terms that resonate with both the business and the Board.

ORLA COX
Director
Cybersecurity & Data Privacy Communications

Steps to improve disconnect between CISOs and leadership teams

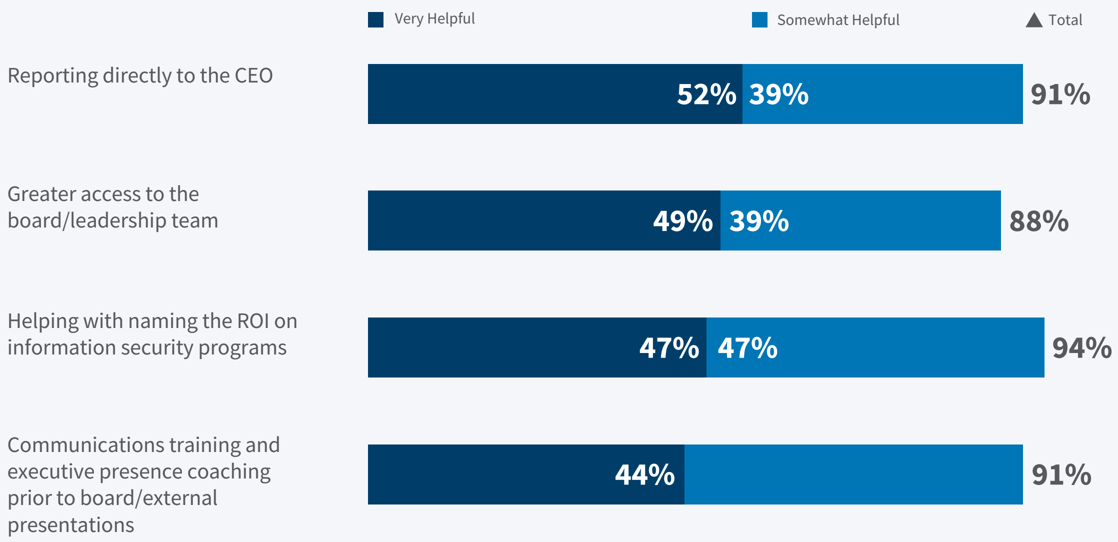
Increased threat activity and a growing focus on companies' governance and oversight of cybersecurity means that, more than ever, CISOs are having to present to boardrooms and executive leadership on cybersecurity preparedness. FTI Consulting's survey revealed that 97% have been asked to present in the next 12 months.

When it comes to being set up for success, 88% of CISOs recognize the importance of greater access to their Board to ensure effective management of cyber risk and possibly support their professional development. Similarly, 91% of CISOs feel that reporting to the CEO would help them achieve greater success in their role.

However, despite a desire to move up the corporate ranks, many CISOs feel they need practical support in translating technical matters into terms that will resonate with business leaders. Return on investment (ROI), for example, is a key metric, with 95% of CISOs having to present on this subject. However, articulating the ROI on cybersecurity measures remains a challenge for over half of CISOs surveyed.

Ultimately, the CISO role is evolving, with many CISOs needing help navigating this transition. As the CISO gets closer to the Board, they will need to speak the language of the boardroom and will need to arm Board members and leaders with the necessary information to make appropriate risk decisions. **91% state that communications training and coaching on presenting to boards is key to helping them make the transition**.

Most Helpful Types of Actionable Support



> "How many CISOs around have 20 to 25 years of experience in cybersecurity? I think there's a maturity gap, and there is a communications gap.
>
> **SHAUN MARION**
> **CISO, McDonald's Corp**[2]

> "The role of the CISO has taken center stage as cybersecurity incidents have become top-of-mind risks for C-suites and Boards of Directors. Yet there often remains a disconnect between the needs of the business and the needs of the information security team. This in turn has placed additional communications responsibility on CISOs, both as internal advocates and external spokespeople, requiring CISOs to develop strong communications skills in order to protect and enhance their organization's reputation.
>
> **EVAN ROBERTS**
> **Managing Director**
> *Co-Head, Cybersecurity & Data Privacy Communications*

[2] McDonald's Security Chief on Building Bonds With Corporate Directors," Wall Street Journal Pro Cybersecurity (August 29, 2022), https://www.wsj.com/articles/mcdonalds-security-chief-on-building-bonds-with-corporate-directors-11661765402?tpl=cs

Research Methodology

FTI Consulting's Digital & Insights team conducted an online survey from June 27 to July 5, 2022 among n=165 CISOs and equivalent heads of information and cybersecurity for large U.S. based companies with global operations, representing a sum aggregate revenue of $4.4 trillion and more than 528,000 employees in the U.S. For more details on the methodology, please contact james.condon@fticonsulting.com

ANNUAL REVENUE

$4.4 Trillion

SUM AGGREGATE REVENUE

$26 Billion

AVERAGE REVENUE

# OF EMPLOYEES IN US

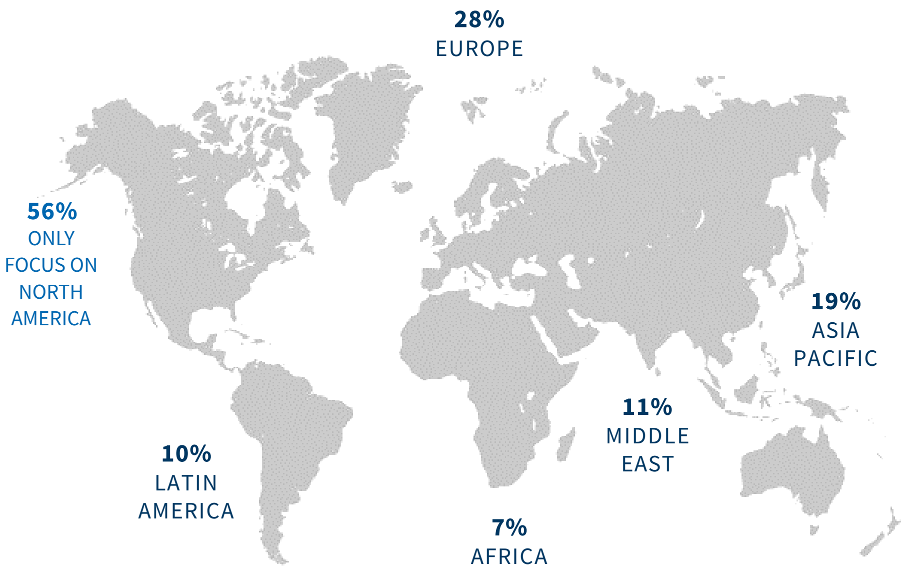
528,000

TOTAL EMPLOYEES

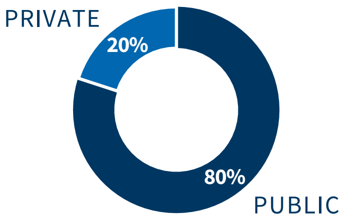
3,200

AVERAGE # OF EMPLOYEES

OPERATIONS IN OTHER REGIONS



PUBLIC/PRIVATE



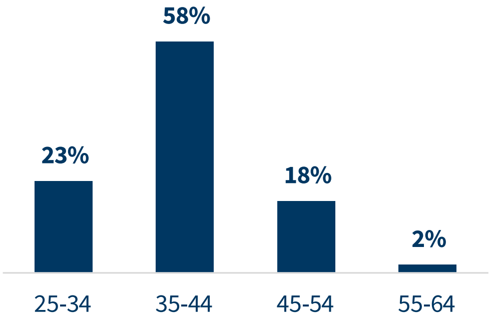
INDUSTRY SECTORS

23%	INDUSTRIALS
15%	TECHNOLOGY, MEDIA, & TELECOMMUNICATIONS (TMT)
14%	HEALTHCARE & LIFE SCIENCES (HCLS)
12%	RETAIL
11%	FINANCIAL SERVICES

POSITION

92%	CISO OR EQUIVALENT HEADS OF INFORMATION AND CYBERSECURITY
8%	CHIEF SECURITY OFFICER (CSO)

AGE

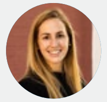


EXPERTS WITH IMPACT™

MEREDITH GRIFFANTI
Co-Head, Cybersecurity & Data Privacy Communications
meredith.griffanti@fticonsulting.com

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

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



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

ADRIANA VILLASENOR
Cybersecurity & Data Privacy Communications
adriana.villasenor@fticonsulting.com

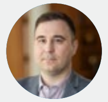
JULIJA SIMIONENKO-KOVACS
Digital & Insights
julija.simionenko-kovacs@fticonsulting.com

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

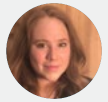
JAMES CONDON
Digital & Insights
james.condon@fticonsulting.com

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

COLIN WRIGHT-PRUSKI
People & Transformation
colin.wright-pruski@fticonsulting.com



JON SPERRY
Digital & Insights
jon.sperry@fticonsulting.com



ELIZABETH MURPHY
Cybersecurity & Data Privacy Communications
elizabeth.murphy@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. For more information, visit www.fticonsulting.com and connect with us on Twitter (@ FTIConsulting), Facebook and LinkedIn.

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.

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 both 2021 and 2022, 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.