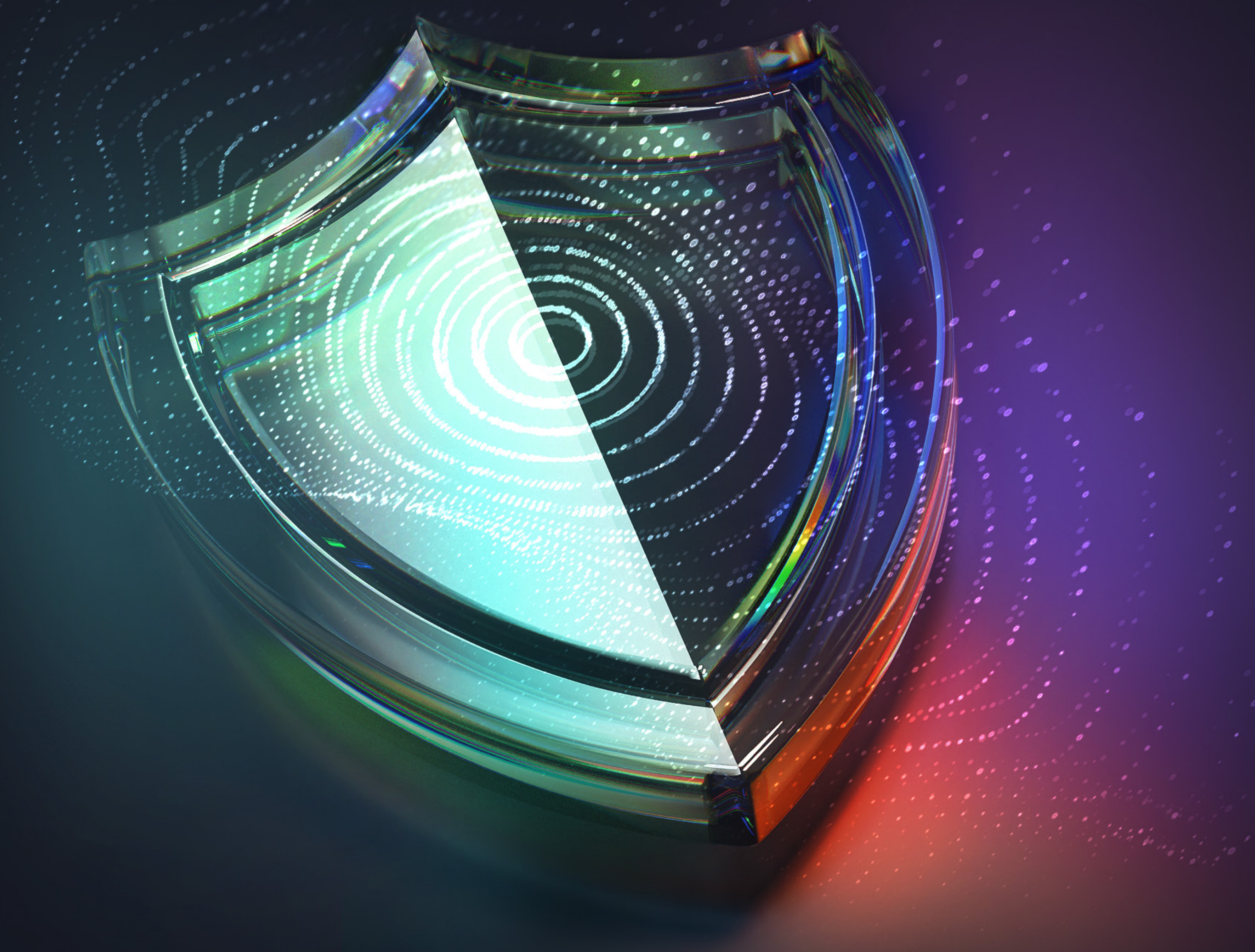
The CISO Circuit by
YL VENTURES

Top CISO Insights Edition 10

# CISO Reporting Landscape 2024



# About YL Ventures

YL Ventures funds and supports visionary cybersecurity entrepreneurs from seed to scale to help them evolve transformative ideas into market-leading companies.

YL Ventures is uniquely focused on supporting the go-to-market of early-stage companies and leverages a vast network of industry experts and Chief Information Security Officers (CISOs) of global enterprises as advisors, prospective customers and partners of its portfolio businesses. The firm's focused strategy allows it to conduct rapid and efficient evaluations for early-stage entrepreneurs and guide founders through their ideation processes pre-investment. The firm is also dedicated to providing unmatched, hands-on value-add support to each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

The firm's global network and footing in the U.S. have always counted among its most powerful assets. YL Ventures bridges the gap between very much needed innovation and market gaps. The firm has formalized and amplified this core competitive advantage through the launch of its Venture Advisory Board.

YL Ventures' Venture Advisory Board is composed of over 100 security professionals from leading multinationals, including Microsoft, Google, Amazon, Hearst, PayPal, Shopify, Etsy, and Kraft-Heinz. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature. The advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies with continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from introductions to pre-vetted cybersecurity innovations and receive direct exposure to the latest in Israeli and American cybersecurity innovation.

## Portfolio

MIGGO
Application Detection & Response
**www.miggo.io**

AIM
GenAI Security
**www.aim.security**

GUTSY
Data Driven Security Governance
**www.gutsy.com**

opus
Unified Cloud-Native Remediation
**www.opus.security**

PiiANO
Dev-First Data Protection Infrastructure
**www.piiano.com**

valence
Collaborative SaaS Security Remediation
**www.valencesecurity.com**

grip
SaaS-Identity Risk Management
**www.grip.security**

satori
Secure & Automated Data Access
**www.satoricyber.com**

cycode
Application Security Posture Management
**www.cycode.com**

orca security
Cloud-Native Application Protection Platform
**www.orca.security**

HUNTERS
SOC Platform
**www.hunters.ai**

VULCAN.
Cyber Risk Management
**www.vulcan.io**

Karamba Security
Embedded Security for Connected Systems
**www.karambasecurity.com**

## Acquisitions

eureka
Acquired by
tenable

Spera
Acquired by
okta

enso
Acquired by
snyk

MEDIGATE
Acquired by
CLAROTY

build.security
Acquired by
elastic

AXONIUS
Exited to
**Late-stage investors**

Twistlock
Acquired by
paloalto NETWORKS

HEXADITE
Acquired by
Microsoft

FIRELAYER
Acquired by
proofpoint.

Seculert
Acquired by
radware

BlazeMeter
Acquired by
ca technologies

Clicktale
Exited to
Amadeus Capital Partners

AcceloWeb Click. You're there.
Acquired by
Edgio

UPSTREAM COMMERCE
Acquired by
Walmart

# About the CISO Circuit

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions and cultivate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched "The CISO Circuit", an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove useful to aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

# Table of Contents

Introduction 5

CISO Reporting Structures 6

Scope of CISO Reports 7

CISO Reporting Challenges 10

The Impact of Recent Legal Events on CISOs 13

Cybersecurity Budgets in 2024 14

Conclusions 16

Outreach and Contact Information 17

Appendix 18

# Introduction

In this report of the CISO Circuit, our team set out to understand executive security needs around reporting and the impact of recent Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC) actions, including those taken against SolarWinds. Over the course of 50 interviews with distinguished cybersecurity executives hailing from a wide spectrum of verticals and company sizes, we collected responses to a series of questions (see Appendix) about the dynamics between enterprise security leadership and their board of directors, as well as the rise of personal CISO accountability.

Following the last edition of the CISO Circuit, which revealed a pronounced demand for cybersecurity governance tools and better means for communicating security posture, we sought to understand what kind of tools and features could best address these needs. Our previous conclusion's emphasis on reporting and transparency also raised questions about how last year's rise in cybersecurity legislation, as well as the high-profile criminal prosecutions of CISOs for nondisclosures, may have impacted this demand.

In the United States, both the SEC and FTC have adopted new rules on cybersecurity risk management with a focus on transparency and accountability around cybersecurity incidents. These legal shifts–which have formally introduced CISO liability–are underscored by the case of U.S. vs Joseph Sullivan and the actions taken against SolarWinds. Cybersecurity is an entrenched C-Suite priority that commands board attention, and we were curious to learn if these more recent developments led to meaningful changes in CISO report structures, frequency or content.

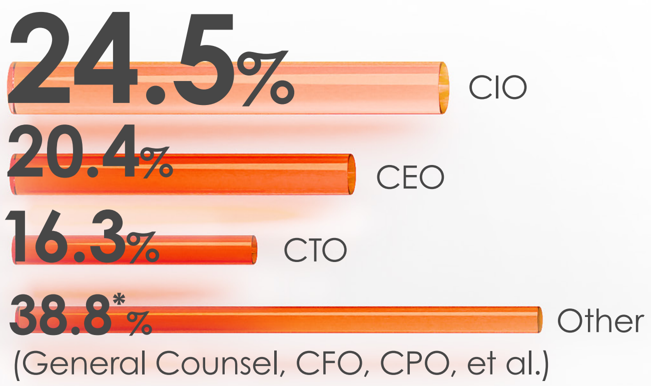
Our analysis indicates that while 2023's events have indeed taken a mental toll on enterprise cybersecurity leaders, they have not led to more organizational pressure around reporting. The most marked change we discovered was a highly pronounced interest in the business enablement of cybersecurity stacks. Whereas last year's report indicated that budgetary constraints and austerity were tempering CISO buying behavior, budgets are beginning to improve, with 42% of CISOs reporting increased investment in cybersecurity. Though consolidation and cost-saving still top their list of considerations, business enablement has gained more focus.

Our analysis also investigated features that would help security leaders best aggregate and communicate cybersecurity posture for presentations to non-security stakeholders. Many CISOs struggle to collect, analyze, translate and present information in a manner that is both accessible and interesting to the board. They require clear and engaging visualizations for quick and effective summaries.

Tying into increased interest in business enablement, CISOs are also expected to communicate more than just their organization's security postures in their reports. Today's successful CISOs are well versed in the business environment their companies operate in, as well as the business constraints their security programs may lead to, and make conscious efforts to promote business enablement wherever possible. Their current responsibilities include aligning cybersecurity efforts with overall organizational goals and minimizing the negative impacts of their stacks on business outcomes.

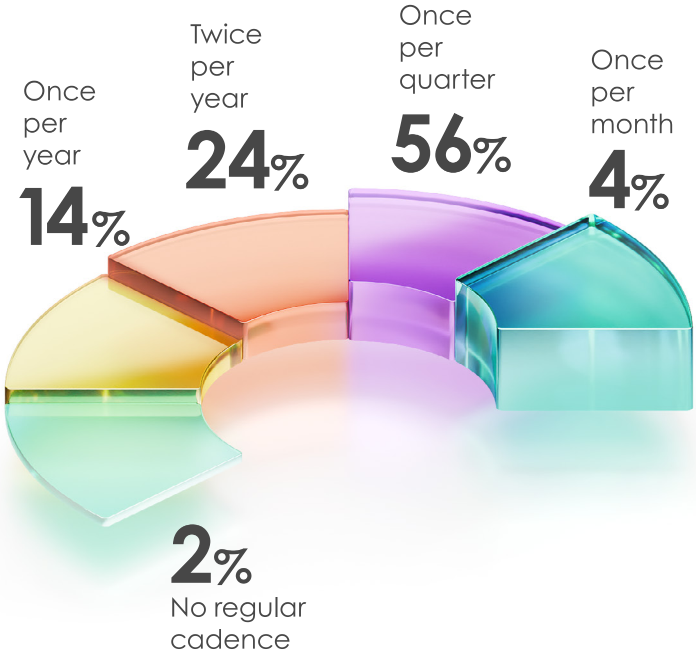
# CISO Reporting Structures

## Who are CISOs reporting to?



*This number is an aggregation of multiple positions that were not selected by a significant portion of our respondents.

## How often do CISOs report on security posture to organizational leadership?



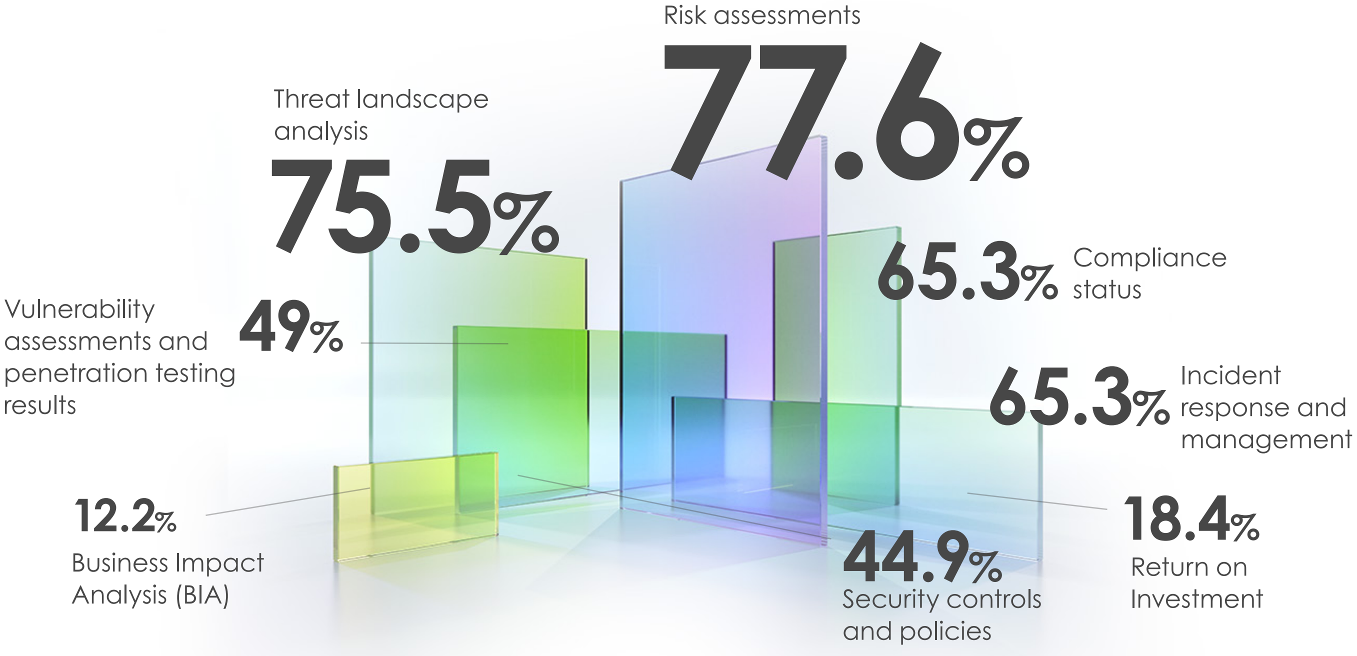
Today's organizational leadership is highly engaged in cybersecurity. This is reflected in both the high percentage of CISOs directly reporting to CEOs, which supports findings in SPMB's Spotlight that CEO-CISO reporting relationships are deepening, as well as the fact that 98% of respondents regularly report on cybersecurity posture to the board of directors.

> **The cybersecurity domain has long been considered a strategic organizational priority that requires CISOs to collaborate with leaders from many different departments, driving an expectation of CISOs to tailor their communication to the specific needs and interests of many different stakeholders.**

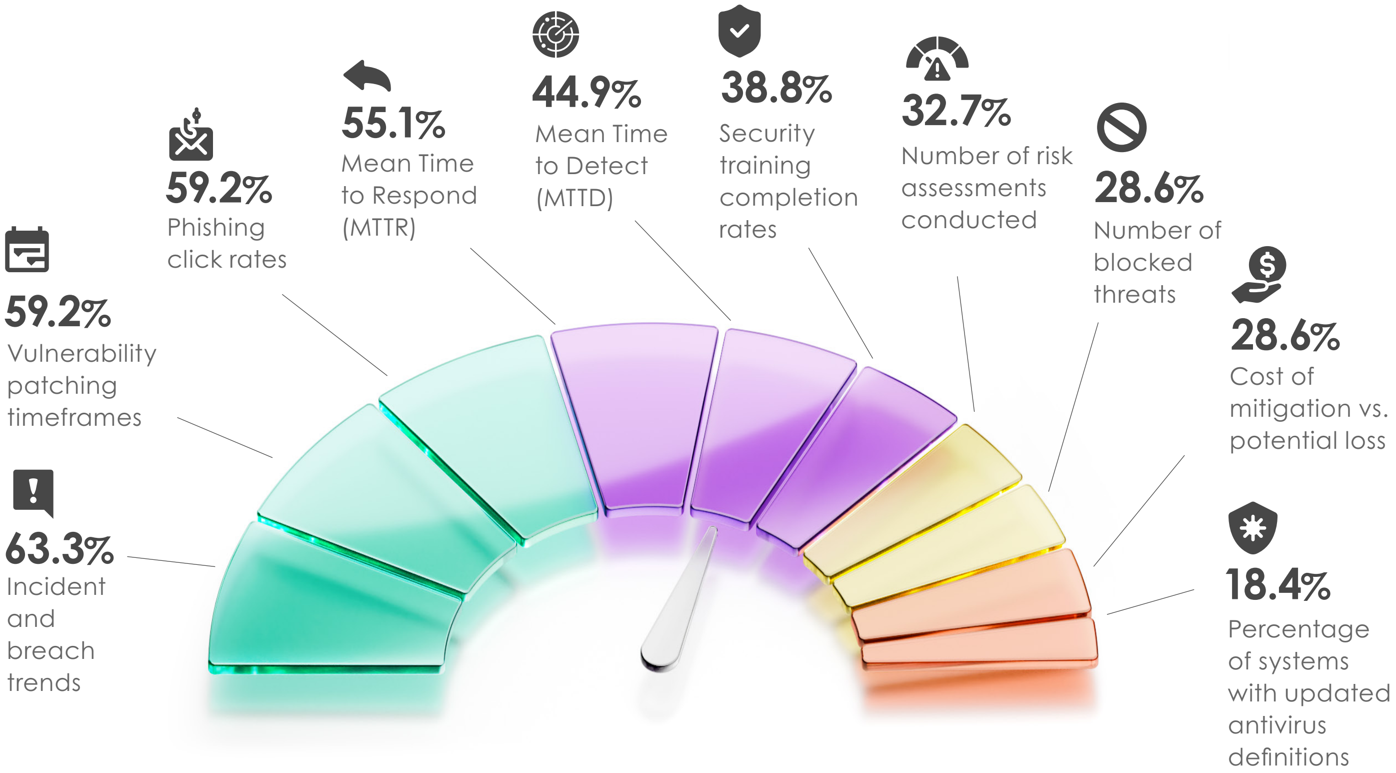
The cadence of CISO reporting further supports the importance organizations are placing on cybersecurity. More than half of CISOs (56%) report on a quarterly basis–arguably the upper limit of frequency before entering the realm of redundancy (although a further 4% manage monthly updates). With only 24% of respondents reporting twice a year, and 14% once a year, it is clear that the majority of CISOs have reporting structures in place to proactively maintain transparency and ongoing dialogue with top leadership.

# Scope of CISO Reports

## What types of data are included in CISO reports to leadership?



## How are CISOs measuring the effectiveness of their cybersecurity programs?



Today's CISO reports to the board transcend compliance checklists to instead offer a comprehensive view of the organization›s total security landscape. However, no consistent picture appears across the industry as to what that view looks like; barely a sixth of CISOs share any given element in their reporting. Reports can include anything from risk assessments (77.6%), threat landscape analysis (75.5%), compliance status (65.3%) to incident response and management (65.3%). This indicates leadership interest in gaining a broad, contextualized view of their organization's security posture by exploring both internal and external risk.

> **Today's boards value information presented in a manner that provides meaningful context rather than isolated metrics. They seek to grasp not only the threat landscape, but the potential business impact of breaches, and the organization's strategic position relative to these risks as well.**

To evaluate the effectiveness of their cybersecurity programs for these reports, our respondents rely on a varied set of key performance indicators (KPIs) and metrics, including incident and breach trends (63.3%), phishing click rates (59.2%), vulnerability patching timeframes (59.2%) and mean time to respond (MTTR) (55.1%). These metrics reflect a focus on detection and response capabilities, as well as user awareness. Additionally, metrics such as security training completion rates and the number of risk assessments conducted reflect a preference for measuring security efforts.

## How are CISOs gathering data for their reports?

**67.3%**
Vulnerability scanners

**65.3%**
SIEM

**63.3%**
IT and security team reports

**61.2%**
Compliance and audit reports

**59.2%**
Pentests

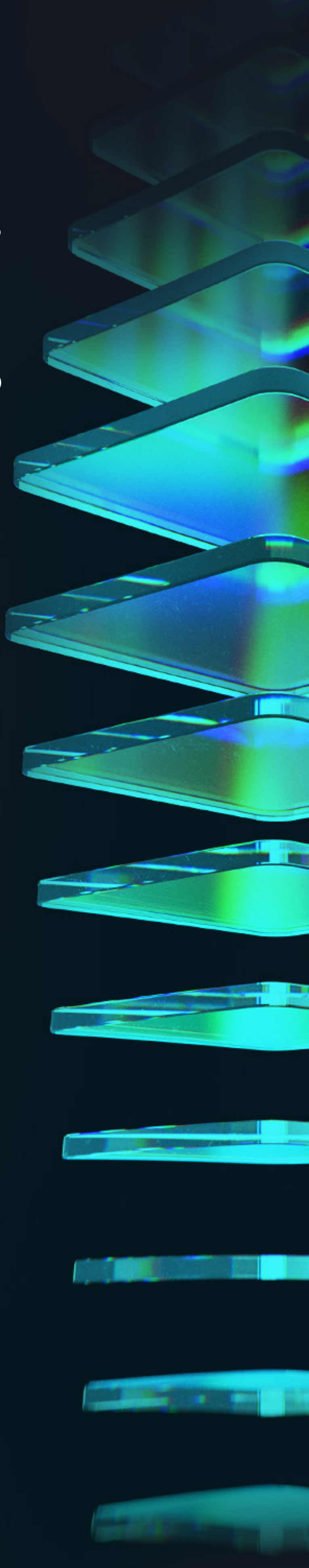
**59.2%**
Security awareness training metrics

**49%**
Incident post-mortems

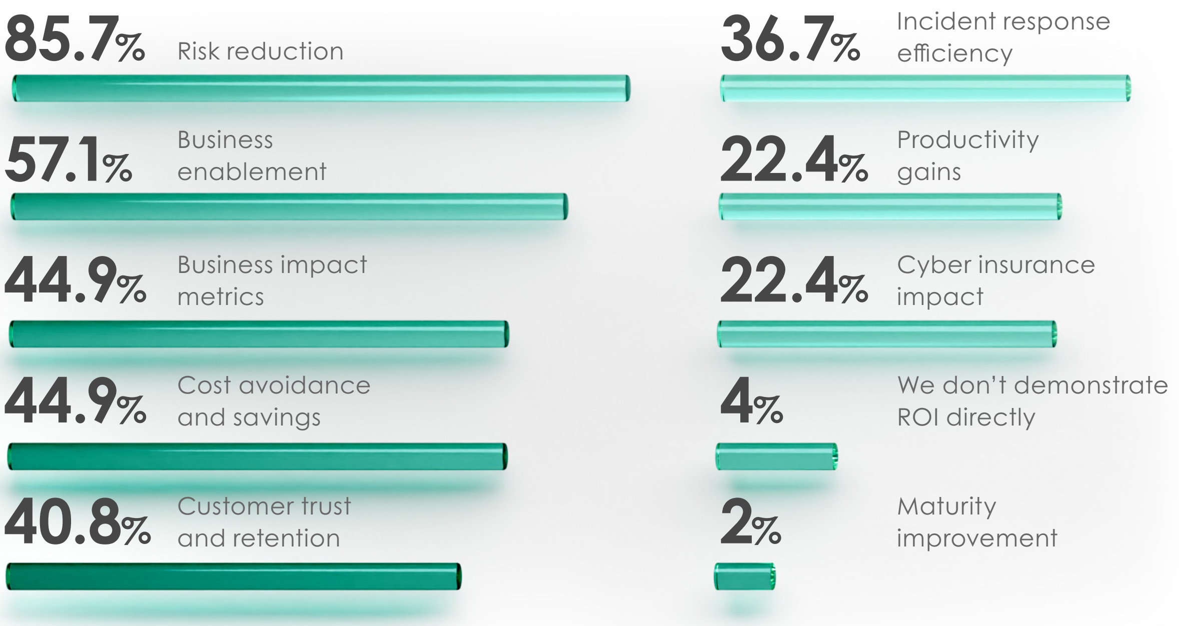
**44.9%**
Threat intelligence research

**24.5%**
Feedback and reporting tools

**14.3%**
Employee surveys and feedback



## How are CISOs communicating the ROI of their security stacks?

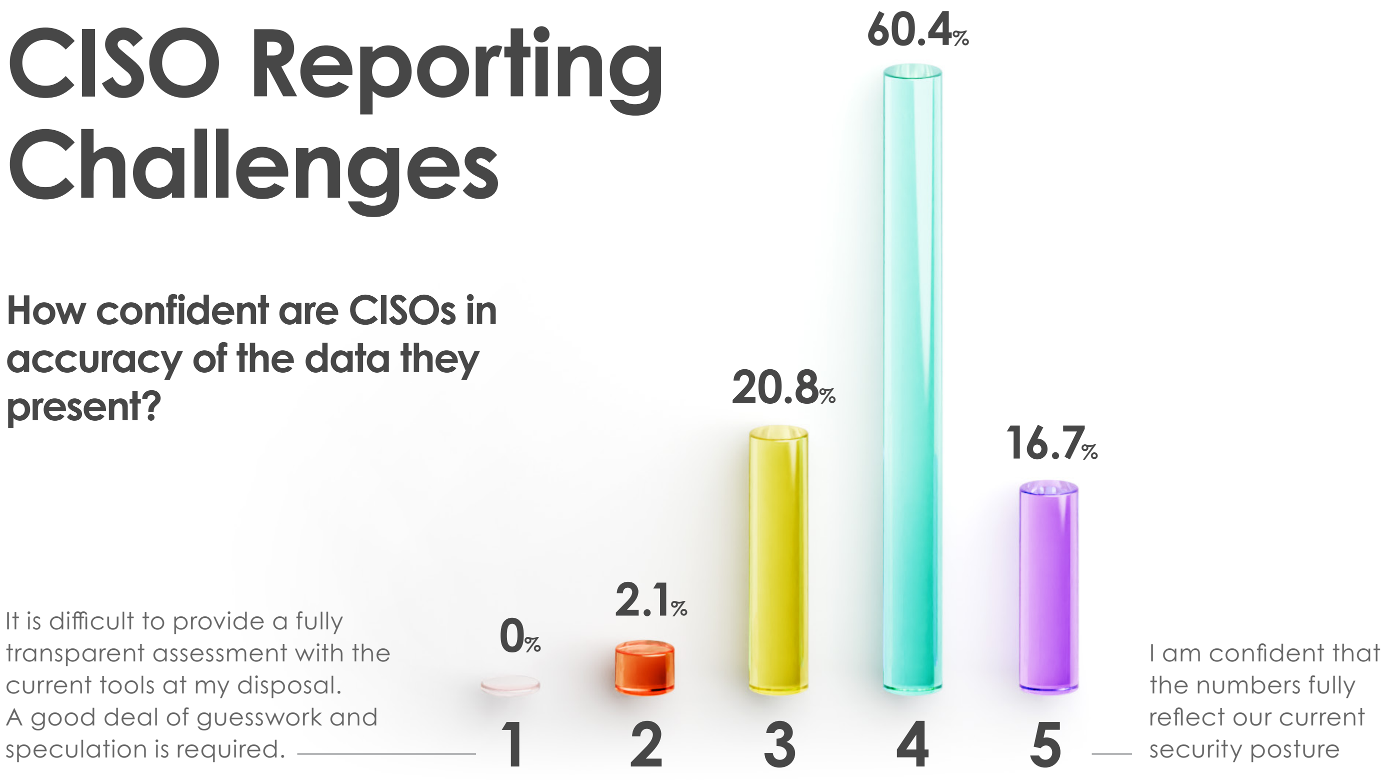


Our respondents are drawing insights from various sources to ensure that their reports offer comprehensive coverage of their organization's security posture and compliance obligations. They leverage reports provided by IT and security teams, compliance and audit reports, pentests, incident post-mortems and feedback from reporting tools. Vulnerability scanners (67.3%) and Security Information and Event Management (SIEM) systems (65.3%) ranked highest among our respondents, highlighting the importance of integrating scalable, automated tools and personalized analysis in effective cybersecurity management.

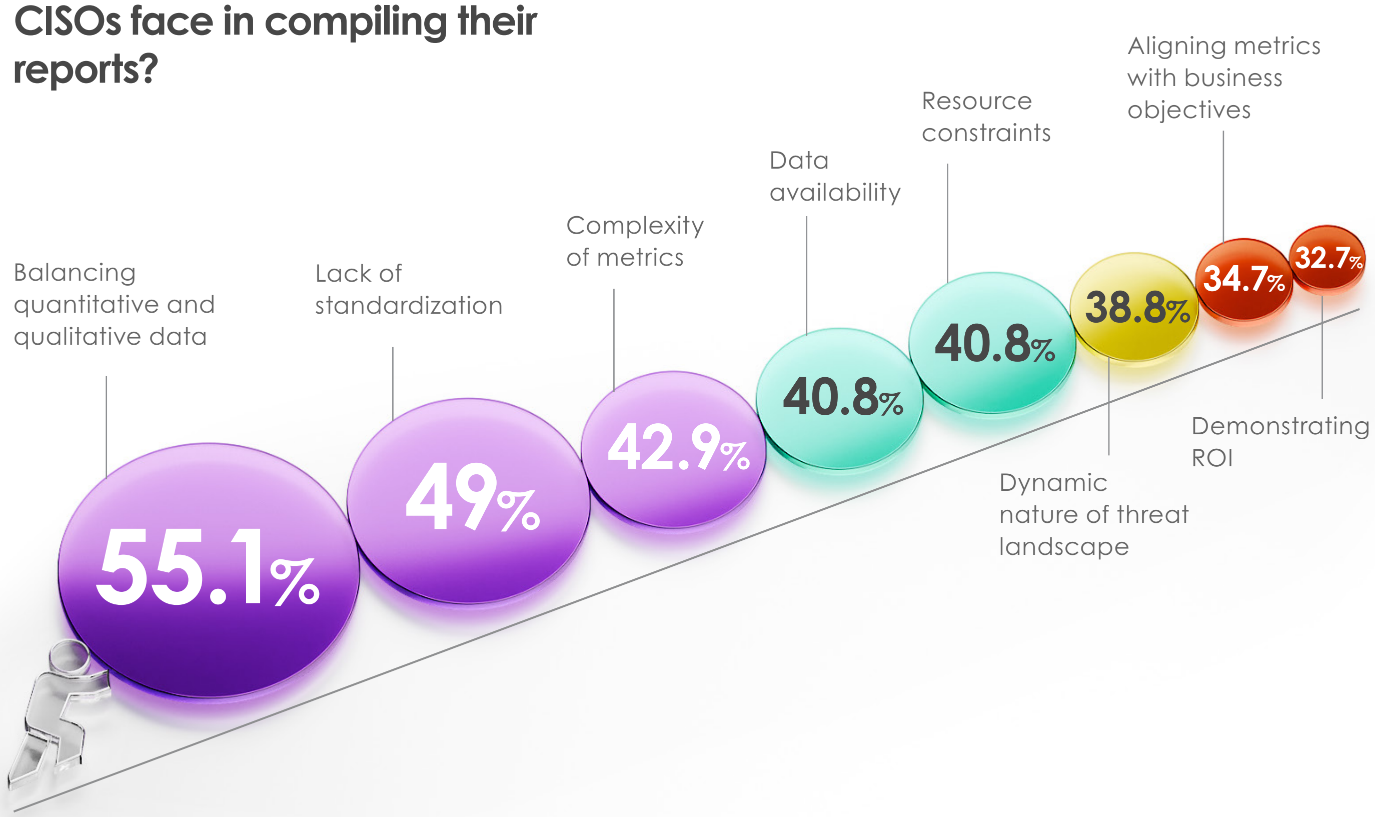
When articulating the return on investment (ROI) of their cybersecurity initiatives, our respondents are prioritizing outcomes that align with both security efficacy and business enablement. The challenge of quantitatively measuring risk is highlighted by only a quarter of respondents directly reporting risk reduction (85.7%, which may include qualitative risk reduction), with many CISOs instead focusing on the business impacts of robust cybersecurity programs, focusing on business enablement (57.1%), business impact (44.9%) or customer trust and retention (40.8%).

# CISO Reporting Challenges

## How confident are CISOs in accuracy of the data they present?



## What are the biggest difficulties CISOs face in compiling their reports?



The CISO Circuit by YL VENTURES

A substantial proportion of our respondents expressed high levels of confidence in the accuracy of the data they present in their reports, with 60.4% rating their confidence level at 4 and 16.7% providing the highest rating of 5. This suggests a prevailing sense of assurance among CISOs regarding the precision and reliability of the cybersecurity data they convey, although a notable percentage (20.8%) expresses a more moderate level of confidence.

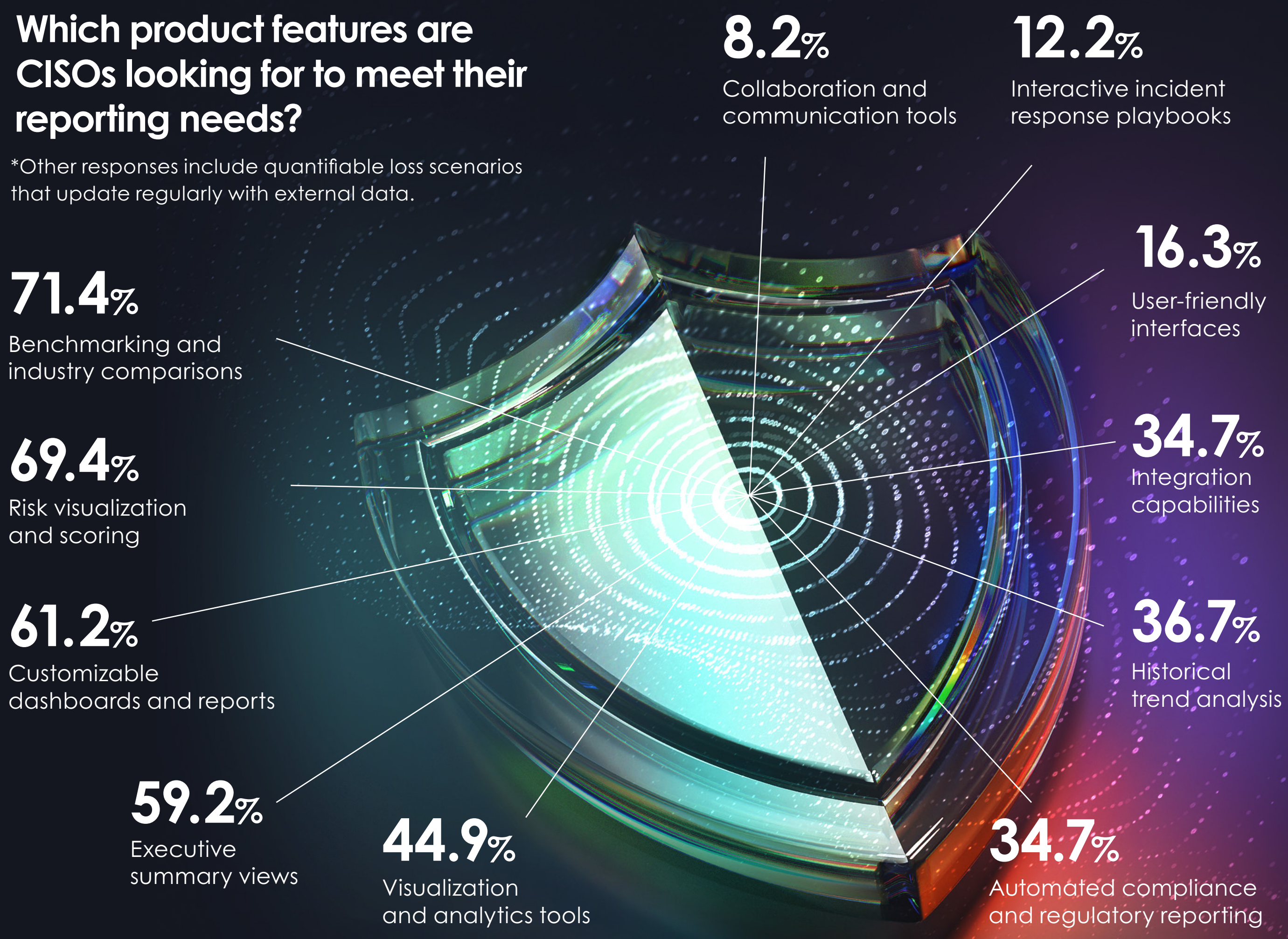
> **A recurring topic among our respondents was that they do not lack data–simply the means to aggregate and present it effectively.**

When compiling their reports for organizational leadership, our respondents struggle with balancing quantitative and qualitative data (55.1%), the lack of standardization for such reports (49%), the complexity of the metrics involved (42.9%) and data availability (40.8%). The dynamic nature of the threat landscape (38.8%) and the need to align metrics with business objectives (34.7%) pose notable additional difficulties.

The above highlights the need for comprehensive solutions that address the diverse nature of cybersecurity data and provide standardized, holistic and readily available insights. It also emphasizes CISO interest in the continuous improvement and investment in tools and processes to enhance the effectiveness and efficiency of cybersecurity reporting practices.

## Which product features are CISOs looking for to meet their reporting needs?

*Other responses include quantifiable loss scenarios that update regularly with external data.



Our respondents exhibited a preference for product features that cater to their Governance, Risk and Compliance (GRC) needs. They selected benchmarking and industry comparisons (71.4%), risk visualization and scoring (69.4%), customizable dashboards and reports (61.2%), executive summary views (59.2%) and visualization and analytics tools (44.9%) as key priorities. These features highlight CISOs' focus on translating complex cybersecurity data into understandable visuals and GRC information to facilitate clearer communication with stakeholders and organizational leaders.

Interest in integration capabilities (7.9%) and historical trend analysis (7.4%) also indicate a desire for comprehensive, contextual and insightful reporting tools that enable tracking progress and efficiency over time. Overall, our respondents' prioritization of these product features reflects a desire to leverage cybersecurity solutions to enhance their reporting capabilities and support informed decision-making in the fast-evolving landscape of cybersecurity threats and challenges.

Ongoing challenges in risk management and prioritization highlight the importance of balancing empowerment with accountability, while also addressing flaws in risk reporting.

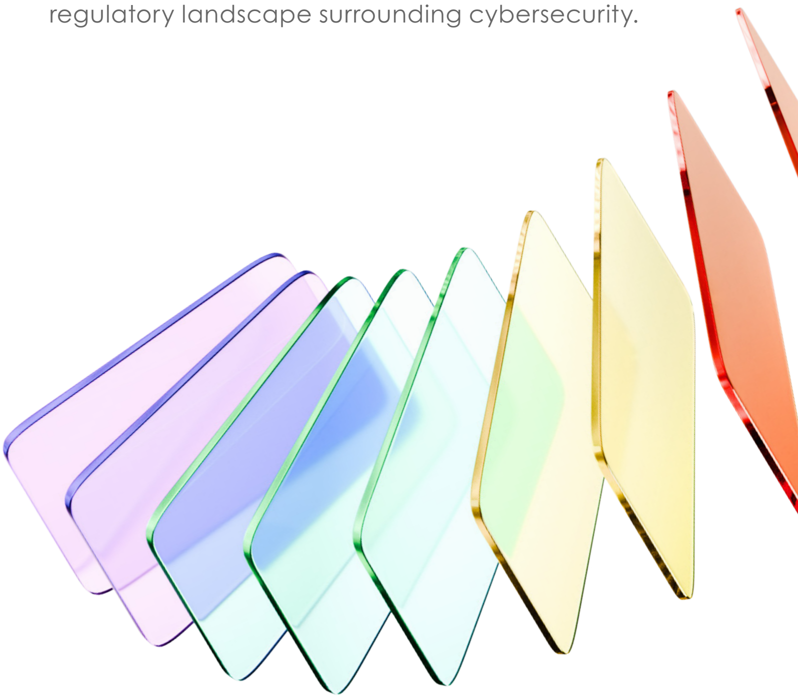
> **The absence of standardized metrics and benchmarks, coupled with data management issues, emphasize a need for cohesive measurement practices and integrated data solutions.**

## What do non-security leaders typically ask of CISOs?

During CISO reports, non-security leaders most frequently ask about current risk status, industry trends and preparedness for potential breaches (see Appendix for a more detailed breakdown). They are also concerned about how to best streamline cybersecurity processes, expedite vulnerability remediation and capitalize on automation for improved operational workflows.

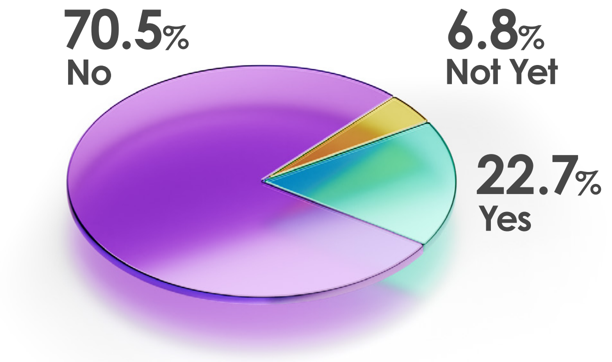
> **Business alignment emerges once again as a key theme, with inquiries focusing on how cybersecurity initiatives impact customer satisfaction, revenue growth and support for business and IT endeavors.**

Compliance remains another significant concern, with questions revolving around regulatory obligations, awareness of new compliance requirements and the organization's compliance status. Such questions reflect leadership's concern around the growing legal and regulatory landscape surrounding cybersecurity.



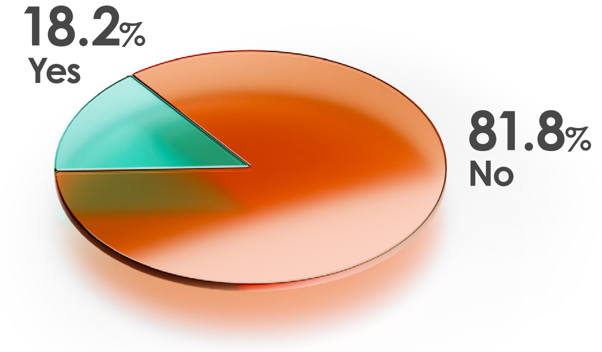
# The Impact of Recent Legal Events on CISOs

## Have the new FTC and SEC rulings or incidents like SolarWinds changed CISO reporting dynamics?



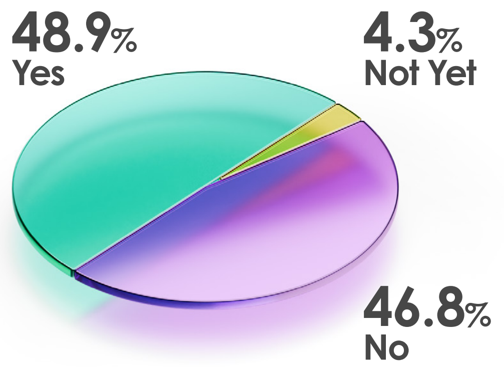
The majority of respondents (70.5%) suggest that recent regulatory rulings and incidents like SolarWinds have not prompted changes in their organizations' cybersecurity reporting dynamics. This may either indicate confidence in existing structures or is a byproduct of the size and maturity of the organization. However, a minority (22.7%) did report increased board involvement in response to 2023's events, signaling a shift towards more rigorous risk management processes and heightened cybersecurity awareness at the board level.

## Have the new FTC and SEC rulings or incidents like SolarWinds impacted the way CISOs acquire new solutions?



The vast majority of respondents (81.8%) indicate that recent regulatory rulings and incidents like SolarWinds have not influenced their approach to acquiring new solutions. However, a minority that reported changes (18.2%) specifically emphasized discussions around supply chain risks and deeper analysis capabilities– likely influenced by heightened awareness of the specific vulnerabilities that led to the SolarWinds breach. Consequently, this has prompted some of our respondents to revise third-party risk management protocols.

## Have the new FTC and SEC rulings or incidents like SolarWinds impacted the way CISOs perceive accountability in their roles?



The recent regulatory actions by the FTC and SEC, alongside incidents like SolarWinds, have triggered a significant shift in how our respondents perceive personal accountability within their roles. Nearly half (48.9%) acknowledge this impact, emphasizing newly intensified collaboration with their Legal department and the forefronting of personal liability concerns. Many have responded by implementing specific measures, such as establishing CISO employee agreements and securing Directors and Officers (D&O) insurance coverage.

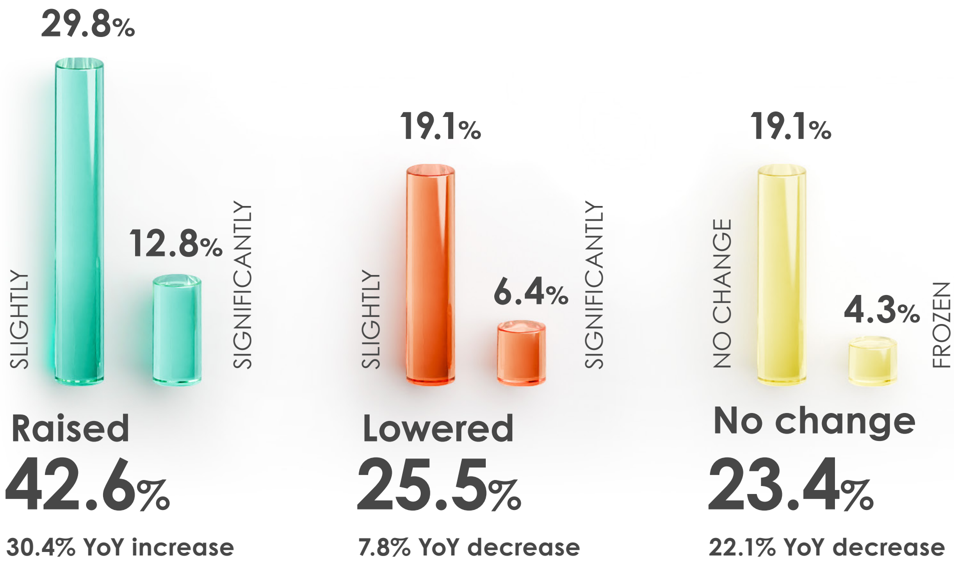
Some respondents express uncertainty regarding their newfound accountability, seeking additional guidance and using external resources for legal and HR consultation before finalizing their contracts.

> Others feel the weight of increased pressure with minimal perceived value addition, leading to more meticulous documentation of decisions and intensified focus on attestations and communications with senior leadership and the board.

Conversely, a notable portion (46.8%) have yet to perceive such changes, while a small fraction (4.3%) remains uncertain about the impact on their accountability roles.

# Cybersecurity Budgets in 2024

## Have cybersecurity budgets changed since last year?



A substantial 42.6% of respondents reported an increase in their budgets since last year. This represents a notable shift from the last CISO Circuit, and indicates a more than tripling of the number of CISOs reporting budget increases. These trends align with recently improved market conditions. 25.5% of CISOs reported budget decreases, which is 7.8% fewer than last year. Additionally, 23% of CISOs reported either no change or frozen budgets, a 22.1% decrease from the last CISO Circuit, suggesting greater flexibility in budgeting strategies and more CISO buying power.

A multitude of factors have influenced changes in cybersecurity budgets over the past year. Increased investments have been driven by a focus on business growth, with many organizations recognizing cybersecurity as integral to their success. Many CISOs interviewed for this report echoed this sentiment and greatly emphasized the connection between cybersecurity measures and business expansion. Moreover, organic business growth has spurred additional investments in capabilities aimed at enabling business operations while mitigating risks.

> The evolving threat landscape and expanding compliance obligations have further necessitated budget increases to address risk-based gaps and ensure regulatory adherence.

This includes expanding the scope of security measures, enhancing visibility into maturity and capability gaps and modernizing identity management practices.

However, economic downturns, poor business performance and financial challenges have also compelled some organizations to tighten their belts and streamline expenditure. In such cases, downsizing and cost-saving measures, coupled with uncertain economic outlooks, have resulted in scaled-back investments in cybersecurity.

A report by SPMB highlights CISOs' expectations of personal compensation rising in tandem with economic conditions, indicating optimism within the industry despite budgetary fluctuations. This optimism may stem from a broader understanding of market dynamics and the increasing personal risks assumed by CISOs in their roles.

> **As cybersecurity continues to evolve in response to emerging threats and regulatory demands, budgetary decisions will remain influenced by a complex interplay of these internal and external factors, requiring agile responses from vendors to effectively navigate the landscape.**

# Andy's Corner

When we went into data collection for this edition of the CISO Circuit, I was cautiously optimistic–I was hoping to see some convergence in how CISOs talked about risk and cybersecurity with their boards and executives. Most other C-level executives have some standardization, after all–whether it's the precision of the CFO with GAAP leading to EBITDA, FCF and EPS; or the laser-focus of the CRO on pipeline, commit and revenue; or the CMO with oft-maligned MQLs, share of voice, TOFU, MOFU and BOFU metrics–and the cybersecurity industry is mature enough that CISOs should be converging on the same.

Alas. We're not there yet.

**As the data shows, even at the broad categorizations in this survey, there seems to be little agreement or consistency in reporting among CISOs, which confirms the anecdata I've gathered from talking to CISOs across multiple industries.**

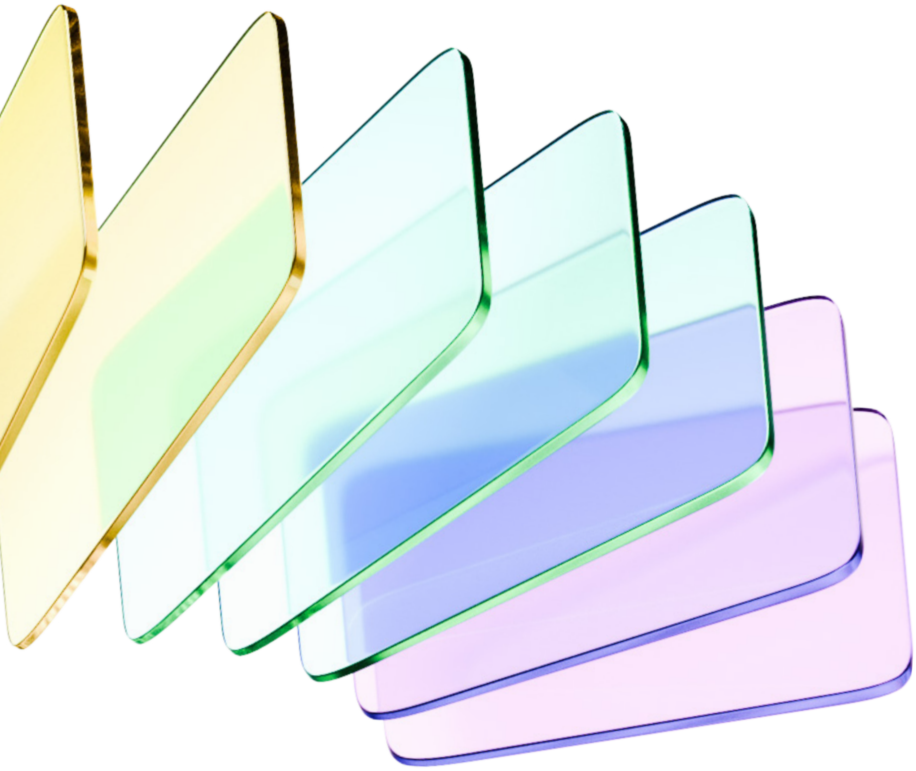
Many of the measures in use are activity measures–how much work does the CISO organization do–versus efficacy measures–how well are we delivering on our mission–and that may be a result of having primarily a preventative mission.

The other C-level executives listed above primarily have delivery missions. Their activity is designed to change the world in a measurable way (generally, from a world without revenue to one with revenue). CISOs, however, are doing the opposite: changing the world away from one with material incidents to a world with far fewer incidents. In a sense, CISOs are more like the General Counsel, keeping the company away from dangerous outcomes. Unfortunately, cybersecurity needs are more deeply intertwined with every business and technical decision in modern corporations, and the heightened expense to satisfy those needs won't let CISO budgets be viewed as just a cost of doing business. This means we're going to need to find a way to demonstrate the value those budgets are providing.

# Conclusions

The prevalence of CISO reporting to the board, with a significant frequency of quarterly updates, highlights cybersecurity's standing as a C-suite priority. Boards and executive leadership are actively seeking comprehensive insights into their organizations' cybersecurity postures, driving the demand for robust metrics and industry benchmarks to contextualize their risk exposure. However, CISOs are grappling with effectively communicating cybersecurity ROI to company leaders, who often lack security backgrounds. They are also increasingly preoccupied with emphasizing the dual objectives of risk reduction and business enablement.

Amidst heightened pressures around personal liability, spurred by recent high-profile prosecutions of their peers, CISOs are advocating for tools that offer executive summary views of their cybersecurity postures to promote transparency. So long as these reporting needs and expectations remain unmet by existing tools, there is a clear appetite for solutions that can facilitate transparency and enable informed cybersecurity decision-making at the board-level. The lack of available options for Governance, Risk, and Compliance (GRC) tools underscores the need for innovative solutions capable of translating data into actionable insights that can effectively guide leadership and strategy.



# Outreach and Contact Information

This report was compiled with cybersecurity entrepreneurs in mind. If you are a cybersecurity startup looking for guidance for seed-stage funding, we invite you to contact our Senior Partner, **Ofer Schreiber**, at **ofer@ylventures.com**. Any queries regarding this report are also welcome at the same address.

We would like to sincerely thank all of the CISOs who participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Circuit, please contact Partner **Justin Somaini** **justin@ylventures.com**.

# Appendix

## Survey Questions

1. What is the role of your immediate supervisor, or to whom do you report within your organization? Please include all roles/organizational bodies if you provide multiple reports.
2. Do you regularly report on the cybersecurity posture of your company to the board of directors or CEO? If so, how often?
3. What types of data are included in these reports?
4. What key performance indicators (KPIs) or metrics do you use to measure the effectiveness of your cybersecurity program?
5. How do you gather this data?
6. How confident are you in the accuracy of the final numbers presented in your report?
7. Do you experience difficulties measuring your program? If so, please select the top four difficulties you face:
8. Please select the top four methods you use to demonstrate the ROI of your cybersecurity program.
9. Please select 5 product features that would help you better communicate your cybersecurity posture.
10. Have the new FTC and SEC rulings or incidents like SolarWinds changed the reporting structure on cybersecurity postures in your organization? If so, how?
11. Have the new FTC and SEC rulings or incidents like SolarWinds impacted the way you acquire new solutions? If so, how?
12. Have the new FTC and SEC rulings or incidents like SolarWinds impacted the way you perceive accountability in your role?
13. What are the most common questions your supervisors ask you during your reports?
14. Are there any other challenges you experience around reportage and accountability that you would like to share?
15. Has your cybersecurity budget changed since last year?

## What are the most common questions your supervisors ask you during your reports?

### Risk Management and Preparedness:

Are we protected?

Are we prepared to deal with a cyber breach?

What is the current status of our security posture?

What are our real risk priorities?

How are we addressing residual risks?

What are the emerging threats, and are we prepared to address them?

How are external incidents impacting our risk and control environment?

Which of the projects you are working on will have the biggest impact?

### Processes:

Are we meeting industry benchmarks?

What are we not doing?

How can we speed up vulnerability remediation and improve phish click rates?

Are we sufficiently tapping into automation opportunities?

How have we demonstrably improved our security posture?

How can the board help the Security Program?

### Business:

Are we solving for customers' and suppliers' security requirements?

Is security enablement blocking other business or IT initiatives?

What are the business benefits and negative impacts of this cybersecurity program?

### Compliance:

What is our compliance status?

Are there any new compliance obligations we need to be aware of?

### Resources:

Do we have the resources we need?

How can we demonstrate ROI to justify more headcount?

Are we sufficiently invested in the right cybersecurity initiatives?