How the C-suite disconnect is leaving organizations exposed

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

About the research

In December 2024 and January 2025, Ernst & Young LLP (EY US) commissioned a third party to conduct an online survey of 800 US C-level leaders (including 500 C-suite leaders and 300 Chief Information Security Officers (CISOs)). "C-suite leaders" refers to the total sample, "C-suite executives" or "rest of C-suite/C-suite counterparts" refers to full-time employed executives (n=105 Chief Operating Officer, n=106 Chief Finance Officer and n=289 other non-CISO C-suite executives) who are decision-makers for their organization's information security, including data and systems, and CISOs refers to full-time employed executives who are responsible for their organization's information security, including data and systems, across 10 industry sectors. The margin of error (MOE) for the total sample is +/- 3 percentage points; the MOE for CISOs is +/- 6 percentage points and the MOE for their C-suite counterparts is +/- 4 percentage points.

Industries surveyed include the health, life sciences, energy, technology media and telecommunications, government and public sector, consumer products and retail, advanced manufacturing and mobility, financial services, private equity and real estate, hospitality and construction industries. There is a minimum of n=50 per industry for C-suite leaders and n=30 per industry for CISOs.

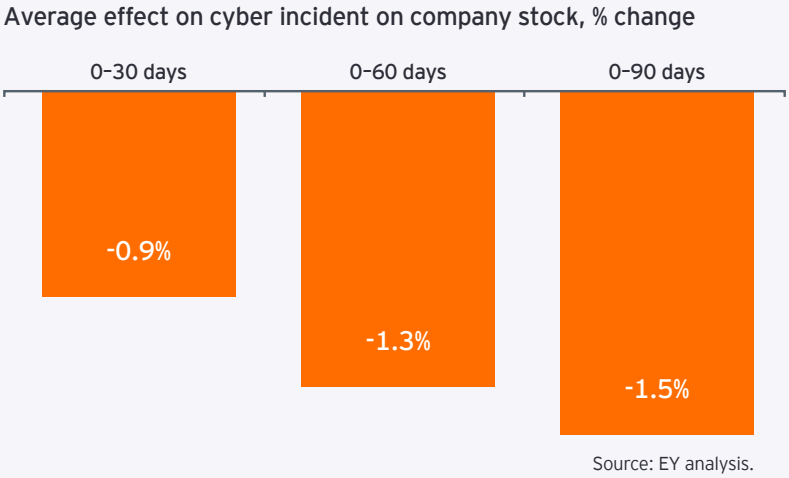
For the EY stock price analysis, a staggered difference-in-differences model was used to evaluate the impact of cyber incidents on the stock prices of 96 Russell 3000 companies with a market cap of at least US$1 billion in 2024 that experienced a cyber incident between 2021 and 2024.

New research from Ernst & Young LLP confirms that cybersecurity remains center stage: 84% of C-suite leaders say their organization's focus on cybersecurity has increased compared with three years ago. What's more, 85% also say their organization's cybersecurity focus will increase over the next year compared with today.

With the majority (84%) of C-suite leaders confirming their organization has experienced a cybersecurity incident in the last three years, the most common incidents in the past year are spyware, domain name spoofing and zero day exploits (when cybercriminals take advantage of an unknown or as-yet-unaddressed flaw).

Separate EY analysis of Russell 3000 companies also reveals that companies face significant financial risks from cybersecurity incidents, including far-reaching financial repercussions beyond immediate recovery costs. Our analysis shows a direct correlation between share price declines and cybersecurity breaches. In the days following a cybersecurity incident, company stock prices decrease not just upon disclosure but extending to 90 days after the incident, compared with companies that did not experience a cybersecurity incident. Companies are seeing real costs associated with cyber incidents, with a longer impact than envisioned.

Impact of disclosed cybersecurity incident on company stock price



Source: EY analysis.

The 2025 EY Cybersecurity Study: Bridging the C-suite disconnect also reveals an alarming divide between CISOs and the rest of the C-suite. This C-suite disconnect centers on how cyber threats are perceived by CISOs and the rest of the C-suite in four key areas:

1. How exposed is our organization?
2. How much is the company spending on cybersecurity?
3. What's making a difference?
4. Where are cyber threats coming from?

We provide insights and key questions to help organizations build a more united front on cyber to protect and build value, shaping the future with confidence.

Disconnect 1

How exposed is the organization?

QUESTION FOR EXECUTIVES

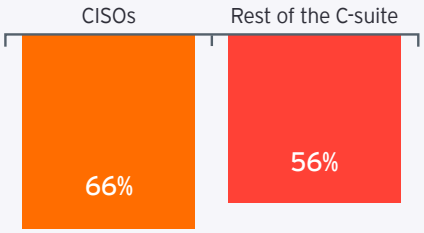
Do we understand the nature and likelihood of cyberattacks on our organization?

Our study reveals a divide between CISOs and the rest of the C-suite on whether cybersecurity defenses are keeping pace with threats and whether threats are being underestimated. CISOs (66%) are more likely than the rest of the C-suite (56%) to express worry that the cybersecurity threats their organization faces are more advanced than their defenses.

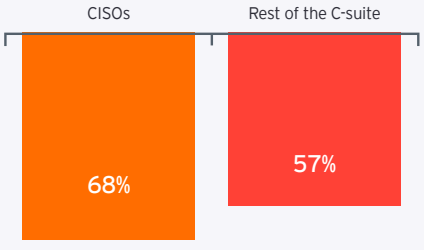
Many also worry that their organization has a history of underestimating cybersecurity threats, highlighting a lingering vulnerability. CISOs (68%) are also more likely than the rest of the C-suite (57%) to express concern about senior leaders at their organization underestimating the dangers of cybersecurity threats. For many CISOs, it's a matter of when and how – rather than if – their organization will experience a cybersecurity incident.

Interestingly, EY analysis found a correlation between experiencing cybersecurity incidents and higher levels of executive concern about cybersecurity. This suggests that concern is more reactive than proactive, since more attacks predict higher levels of concern.

Worried that the cybersecurity threats their organization faces are more advanced than their defenses



Concerned that senior leaders at their organization underestimate the dangers of cybersecurity



Source: EY analysis.

Disconnect 2

How much are we spending on cybersecurity?

QUESTION FOR EXECUTIVES

Do we have sufficient visibility of current cyber spending?

There is a lack of agreement across the C-suite on both current and future investment levels in cybersecurity.

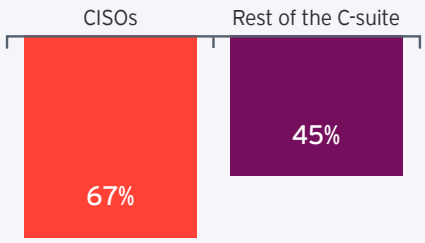
CISOs are more likely to report a higher budget than the rest of the C-suite, with 67% of CISOs saying their organization's current total cybersecurity budget are at minimum seven figures, vs. the rest of the C-suite (45%).

This gap widens when asked about next year's budget, with 82% of CISOs saying next year's total cybersecurity budget will be at minimum seven figures, compared with the rest of the C-suite (53%). This may, in part, be attributable to the lack of organizations with a stand-alone cyber budget, which obscures how much is being spent on cybersecurity.

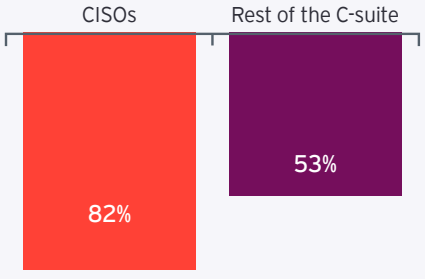
When it comes to artificial intelligence (AI), CISOs are particularly optimistic about AI's ability to positively transform their organization's cybersecurity strategy and preparedness: CISOs (90%) are more likely than the rest of the C-suite (81%) to say AI is a critical component of their cybersecurity strategy.

Interestingly, C-suite leaders whose organization has adopted AI into their cybersecurity practices (80%) are more likely to say their organization's cybersecurity budget should prioritize investment in people (for example, hiring cybersecurity talent and upskilling current employees) over new technology solutions compared with organizations that have not adopted AI (70%). AI is one of many factors making an impact as cybersecurity functions evolve.

Report their organization's current total cybersecurity budget are at minimum seven figures



Report that next year's total cybersecurity budget will be at minimum seven figures



Source: EY analysis.

Disconnect 3

What's making a difference?

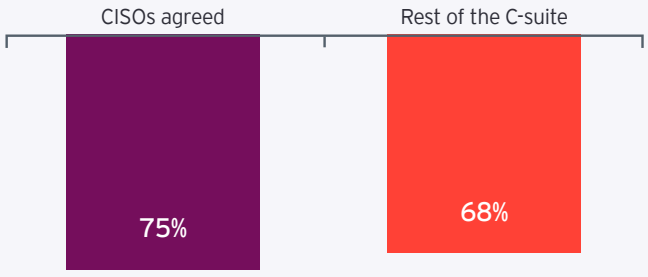
QUESTION FOR EXECUTIVES

Are we making the right investments today to prevent costly breaches tomorrow?

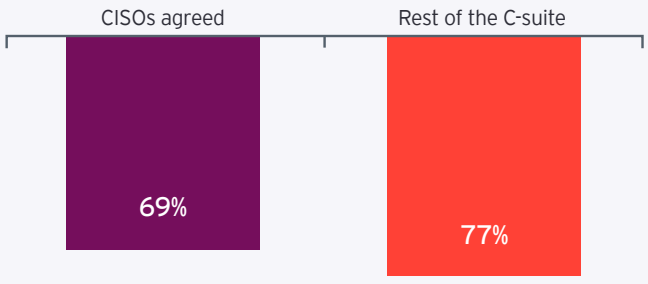
Across the C-suite, there are differing perspectives on which technologies or initiatives are helping to reduce cybersecurity incidents.

Surprisingly, CISOs are the most likely to attribute decreased cyber incidents to investment in AI. In fact, 75% of CISOs say their organization experienced a decrease in cybersecurity incidents following increased investment in AI, compared with the rest of the C-suite (68%). By contrast, the rest of the C-suite (77%) is more likely to attribute success in decreased cybersecurity incidents to increased investments in employee cybersecurity training than CISOs (69%).

The organization experienced a decrease in cyber incidents following increased investment in AI



The organization experienced a decrease in cyber incidents following increased investment in employee cybersecurity training



Source: EY analysis.

Disconnect 4

Where are cyber threats coming from?

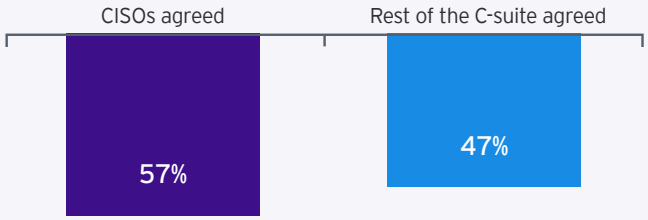
QUESTION FOR EXECUTIVES

Are we underestimating insider threats?

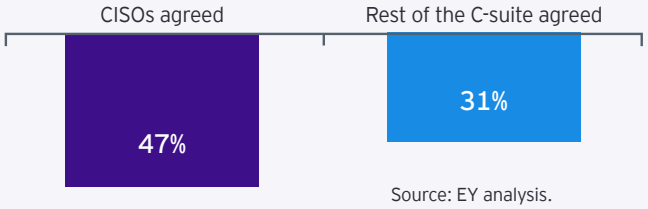
More CISOs (47%) say their organization has experienced a cybersecurity incident due to inside threats (i.e., employees intentionally stealing or leaking private information) in the past three years, compared with the rest of the C-suite (31%).

CISOs (57%) are also more likely than the rest of the C-suite (47%) to say their organization has experienced a cybersecurity incident due to cybercriminals in the past three years. This gap in understanding the historic source of incidents is problematic for building defenses against future threats.

Have you experienced a cybersecurity incident caused by cybercriminals in the past three years?



Have you experienced a cybersecurity incident caused by inside threats in the past three years?



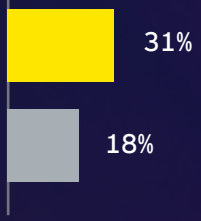
Source: EY analysis.

Industry Insight

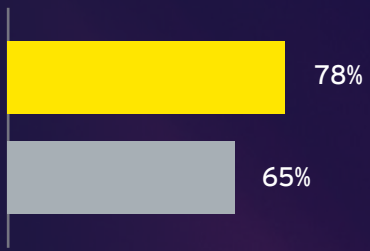
FINANCIAL SERVICES

Financial Services | Other

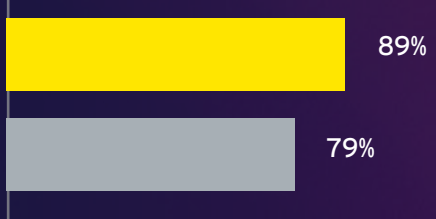
Among most likely to have a stand-alone cybersecurity budget



Concerned about current employee cybersecurity skill gaps at their organization



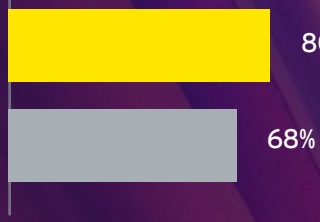
Believe their organization's cybersecurity budget should prioritize investments in people over new technology solutions



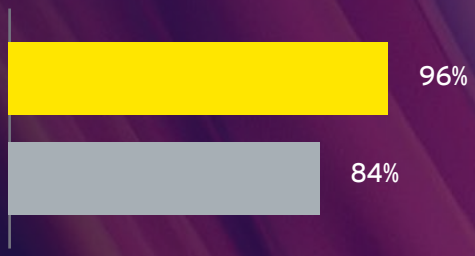
ENERGY

Energy | Other

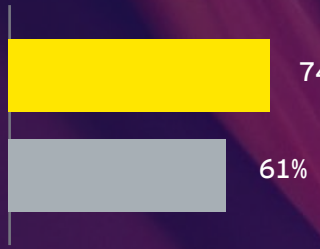
Cybersecurity typically included in overall IT budget



C-suite leaders at their organization consider cybersecurity investments as a cost center



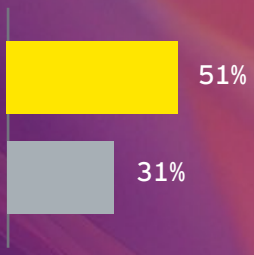
Noticed a decrease in cyber incidents after increased investment in machine learning



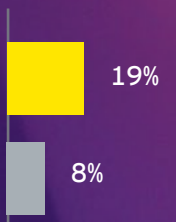
HEALTH

Health | Other

Worry their organization is not set up to handle cybersecurity threats of the future



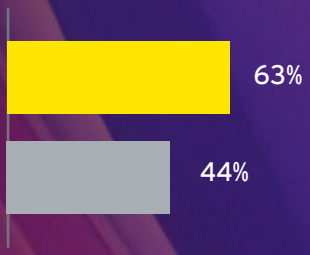
Say their organization's cyber investments are not keeping pace with ever-evolving threats



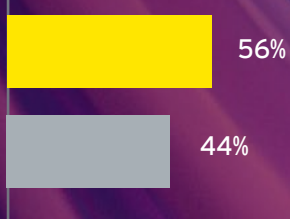
PRIVATE EQUITY

Private equity | Other

Among most likely to say their industry is not set up to handle cybersecurity threats



More likely to say their industry is falling behind others on cybersecurity defense



Stand-alone cybersecurity budgets and C-suite disconnects

Most (84%) C-suite leaders consider cybersecurity investments a cost center and many (68%) agree that their organization prioritizes short-term revenue generating investments over investments to protect the organization from cybersecurity threats.

This perception is reflected in where cybersecurity budgets are housed, with only 18% of C-suite leaders saying the cybersecurity is a stand-alone budget, in other words separate from the organization's overall or IT budgets.

For a majority (68%) of C-suite leaders, cybersecurity is part of the IT budget. This puts cybersecurity in direct conflict with a multitude of operational priorities, rather than on a footing with more strategic aspects of running the business, such as manufacturing operations, finance and business transformation.

60%

of C-suite leaders remain worried that the cybersecurity threats faced by their organization are more advanced than their defenses.

Four actions to overcome the C-suite divide

Current efforts on cybersecurity are not shifting the dial. Although most (83%) C-suite leaders who are investing in cybersecurity say their organization is investing the right amount regardless of how much, many (60%) remain worried that the cybersecurity threats their organization face are more advanced than their defenses.

Without transparency on what is being spent and clear performance metrics, there is clearly room for confusion, as reflected in the four C-suite disconnects reported here. CISOs see escalating threats and vulnerabilities, while the C-suite appears to often believe cybersecurity is handled. Certainly, CISOs (63%) admit they struggle with motivating other C-suite leaders to prioritize cybersecurity investments.

Our research reinforces the urgent need for leaders to come together and develop a comprehensive cybersecurity strategy that addresses the evolving threat landscape and includes clear communication, a shared understanding of the risks and opportunities and priority areas for investment.

Companies need to move beyond a "check the box" mentality and recognize cybersecurity as a strategic investment, not simply a cost center. It's time to push for not just the resources but the authority for cyber leaders to build truly resilient organizations. The cost of inaction is simply too high.

Here are four actions the C-suite can take to maximize value from capital investment amid heightened cyber risks and turbulent economic conditions:

- **Elevate the CISO role**
  Establish the CISO as a position of ownership over the organization's security posture and budget, with a mandate to drive strategic security initiatives and influence critical business decisions.
- **Invest strategically**
  Align cybersecurity investments with the organization's overall business objectives and risk tolerance, ensuring that resources are allocated effectively to address the most critical threats.
- **Embrace innovation**
  Continue reviewing and adopting new technologies and approaches to cybersecurity, including AI and machine learning, to enhance threat detection and response capabilities.
- **Develop a culture of cyber confidence**
  Promote a culture of cybersecurity awareness and responsibility at every level across the entire organization, empowering employees to identify and report potential threats.

Special thanks to Jim Quinn, David Cooper, Michelle DeLiberty, Tim Shanahan and Aman Rai for their contributions to this content.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 26849-251US
2503-11810-CS
ED None

ey.com