



**How can
cybersecurity
go beyond value
protection to
value creation?**



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



**Shape the future
with confidence**

Introduction

The 2025 EY Global Cybersecurity Leadership Insights Study examined benefits of earlier, more meaningful involvement of the CISO.

Whether in a fully integrated oil and gas company that oversees production, transport and refining operations around the world, or a global entertainment conglomerate that produces content and uses Artificial Intelligence (AI) to predict consumption habits, a fully engaged cybersecurity function not only protects against threats but also adds significant value.

In fact, our most recent research of global cybersecurity leaders, the 2025 EY Global Cybersecurity Leadership Insights Study, found that the cybersecurity function typically accounts for 11% to 20% of the value produced by enterprise-wide initiatives it is involved in, with this contributing a median of US\$36m in value to each of these projects.

Cybersecurity accounts for

US\$36m

in value for each enterprise-wide initiative it is involved in.

This figure reflects the evolution of the cybersecurity function and the CISO. In the past, cybersecurity functions focused primarily on protection, compliance obligations and reducing and quantifying risk. In recent years, with broad digital transformation; a move to cloud-based, distributed IT infrastructure; and rapid adoption of AI, leading cybersecurity functions are evolving into key enablers of business growth.

At the same time, the research found that cybersecurity budgets as a percent of annual revenue have decreased over the last two years, from 1.1% to 0.6%. This might indicate that organizations do not yet recognize investing in cybersecurity as a value-creating opportunity. As a result, many CISOs still have difficulty getting a seat at the table during early discussions of strategic initiatives, and cybersecurity functions are often not funded sufficiently to deliver their potential value.

As it stands, only 13% of CISOs in our study said they were consulted early when urgent strategic decisions were being made – but those CISOs reported creating more value than those who were consulted either late or not at all.

In brief

- The study found that cybersecurity contributes 11% to 20%, or a median of US\$36m, in value to each enterprise-wide strategic initiative it is involved in.
- Chief Information Security Officers (CISO) who are involved early in cross-function decision-making generate more value than those who were consulted late or not at all.
- CEOs, CFOs and boards should take steps to more meaningfully integrate cybersecurity into transformations and other strategic initiatives.

Equipped with a more accurate calculation of the value cybersecurity brings to strategic initiatives, CISOs can better articulate why they should be included earlier in key decision-making processes and why their role has evolved to be that of a business executive, rather than a technical practitioner.

This year's EY Global Cybersecurity Leadership Insights Study also aimed to identify how leading CISOs create value compared to their peers, measure cost optimization from cybersecurity automation and simplification, and provide practical steps for CISOs to articulate their worth and elevate their organizational influence.

The insights from this study are in part for CISOs – especially those whose organizations are embarking on a transformation, adopting a new technology, entering a new market, launching a new product or acquiring a high-growth company. In each initiative, the cybersecurity function should be involved to protect against new threats and risk exposure. This study's results indicate that cybersecurity functions can be engaged earlier, with more strategic integration, to increase the initiative's value.

But this study is also critical for CEOs, CFOs, board members and other executives involved in key strategic initiatives. Early, meaningful integration of the CISO into initiatives and decisions will unlock value for the entire enterprise.

About the research

In March and April 2025, the global EY organization conducted research to better understand how cybersecurity functions are creating value for their organizations. We surveyed 550 C-suite and cybersecurity leaders across 16 sectors and 19 countries covering the Americas, Asia-Pacific, and Europe, the Middle East, India and Africa (EMEIA). Respondents represented organizations with over US\$1b in annual revenue.

Building off the findings of the [2023](#) and [2024](#) EY Global Cybersecurity Leadership Insight Studies, we repeated the statistical modeling to identify Secure Creators – companies with better cybersecurity outcomes. These high-performing organizations were identified by leaders' evaluation of their organization against a range of objective and subjective cybersecurity metrics: mean time to detect (MTTD), mean time to respond (MTTR), number of cybersecurity incidents, integration of cybersecurity within the organization, and cybersecurity's impact on innovation and value creation. In the 2025 study, Secure Creators represent 47% of the survey sample while Prone Enterprises (lower-performing organizations) made up 53%.

What is the real value of cybersecurity?

CISOs and cybersecurity functions account for significant value across the enterprise. Calculating and articulating that value will help CISOs become more influential in strategic decisions.



While most cybersecurity functions have been involved in at least one value-adding business initiative, such as enterprise-wide technology adoption, business innovation or new market expansion, 58% of CISOs and cybersecurity executives say it is difficult to articulate their value beyond risk mitigation, according to our study.

To help with this, the EY organization created a framework to quantify the value cybersecurity adds to the enterprise through their contributions to revenue and cost savings on strategic business priorities. To calculate the contribution to enterprise value creation, we identified six key initiatives – based on EY teams' experience with clients – where cybersecurity should have significant involvement:

- 1** Adopting and building technology
- 2** Strengthening brand trust and reputation
- 3** Improving customer experience
- 4** Transforming and innovating across the business
- 5** Expanding to new markets
- 6** Developing new products and services

In our research, leaders provided the revenue generated and average annual cost savings from these initiatives and the proportion of the outcome attributed to the cybersecurity function. Together, these allowed us to calculate cybersecurity's enterprise value creation for each project or initiative where the cybersecurity function is significantly involved.

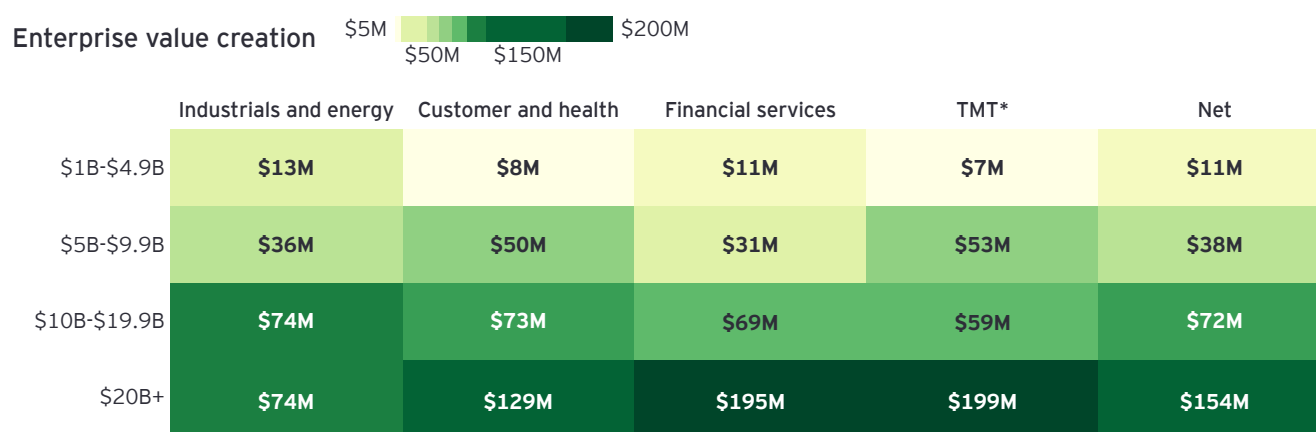
Notably, we saw consistent attribution of outcomes to cybersecurity across other senior roles, indicating that CISOs are not over-attributing their contributions.

In total, for each initiative that involves cybersecurity, the median value creation figure is US\$36m.

This varies significantly by organization size, ranging from a median of US\$11m per project for organizations with US\$1b-US\$4.9b in revenue, up to US\$154m for companies with US\$20b or more in annual revenue.

Cybersecurity functions contribute a median of \$36M in enterprise value creation across each business initiative they are significantly involved in

Median, USD (millions)

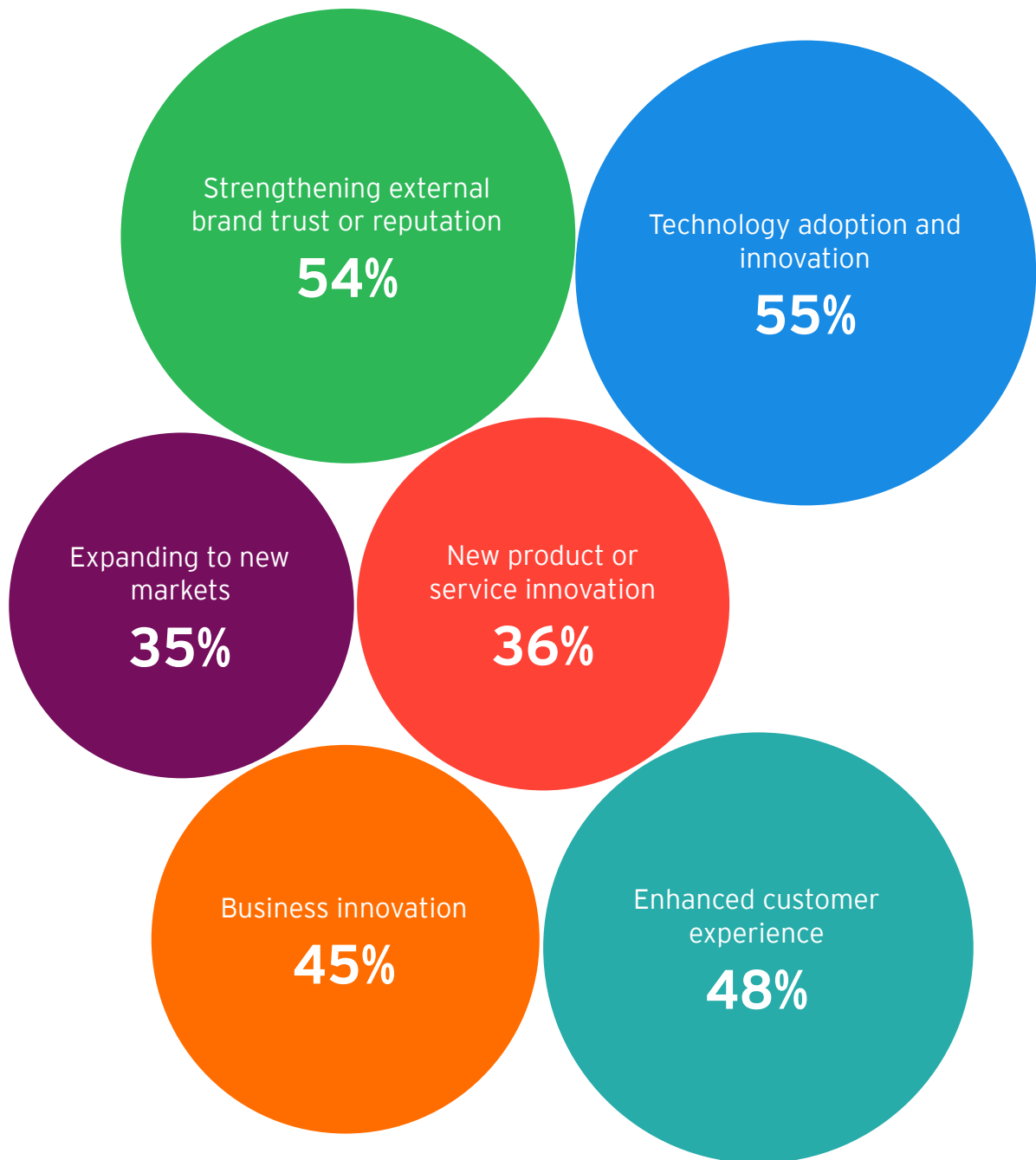


Organization's annual revenue

Note: *Technology, Media & Entertainment, and Telecommunications

But what does cybersecurity's involvement in enterprise value creation actually look like across different initiatives?

Where cybersecurity functions add value



Note: Values indicate the percent of cybersecurity functions who have been involved with these initiatives across the organization

Quotes from the survey

Strengthening external brand trust or reputation

"Customer complaints are resolved faster with safe communication channels, building stronger trust and reliability with customers."

"As we protected our sensitive data, our cybersecurity efforts attracted more clients who value privacy and security."

"The cybersecurity team collaborated with the product team to integrate cutting-edge encryption features into customer-facing software, positioning the company as a market leader in privacy protection."

Technology adoption and innovation

"We designed a secure framework for blockchain projects, allowing the organization to pioneer innovative decentralized applications."

"Creating a secure digital space for our innovation lab allowed creative projects to thrive without risking sensitive ideas."

"As we expanded our digital services, our cybersecurity team worked closely with developers to integrate security into every stage of the software development lifecycle."

Enhanced customer experience

"We implemented multi-factor authorization and real-time fraud monitoring on our bank's digital wallet, facilitating contactless payments."

"The cybersecurity team designed a cloud-based security framework that allowed seamless scaling during peak business periods, reducing delays and enhancing user experience."

"We safeguarded critical systems, like mail sorting and delivery schedules, to prevent disruptions that could have negative effect on our customers."

Business innovation

"During the acquisition of a company, cybersecurity was brought in to integrate their systems securely. After a thorough audit and vulnerability fixes, the cybersecurity team helped the acquired company's technology become a key part of our growth strategy."

"During our cloud migration project, cybersecurity played a key role in ensuring compliance with industry regulations and securing sensitive data."

New product or service innovation

"While developing a novel AI product, cybersecurity implemented data encryption and access controls to safeguard sensitive training data, ensuring timely launch and a competitive advantage in the market."

"Cybersecurity's involvement in a new mobile app that allows patients to view test results and book appointments, ensured the app was secure to use. As a result, more patients started using the app, which provided a better and more convenient experience."

"During the launch of a digital health platform, the cybersecurity team ensured compliance by implementing encryption, secure APIs, and access controls. This drove a 30% increase in user adoption."

Expanding to new markets

"We wanted to expand our SaaS platform into new markets, but compliance seemed like a huge hurdle. The cybersecurity team implemented data protection measures, conducted audits, and ensured all processes met regulatory standards, resulting in our organization successfully entering new target markets."

"With our cybersecurity team's help, we have managed to increase speed and transparency in international transactions, along with reducing costs."

How Secure Creators add value to key strategic initiatives

The study revealed a group of respondents known as “Secure Creators” – first identified in the [2023 EY Global Cybersecurity Leadership Insights Study](#) as organizations with more advanced cybersecurity functions than their peers – who were involved earlier and more deeply than their peers in their business’s key initiatives.

Secure Creators were more likely to help other business functions implement AI than “Prone Enterprises” (48% vs. 31%). Beyond the immediate benefits of more secure technology adoption, more frequent and closer collaboration with high-growth technology initiatives helps broker a better relationship between CISOs and front-office business leaders. Front-office leaders who work with Secure Creators will increasingly view the CISO as the true enabler of technology transformation, rather than the department that is only brought in to say “no.”

Secure Creators were also more likely to have positively impacted how external stakeholders perceive their brand (72% vs. 56% of Prone Enterprises). The obvious relationship between cybersecurity and brand trust lies in preventing reputation-damaging hacks and data breaches, and in minimizing loss or impact in the event of a cybersecurity incident. But for Secure Creators, that relationship goes even deeper and positions cybersecurity closer to the customer touchpoints that determine brand reliability. Examples from survey respondents include avoiding potential losses and reputation during a ransomware attack and ensuring secure data transfers, resulting in increasing trust with current clients as well as attracting new customers who value data protection.

Secure Creators

72%

positively impacted brand perception.

Prone Enterprises

56%

positively impacted brand perception.

Relatedly, Secure Creators were more involved in efforts to improve customer experience than their peers (53% vs. 42%). Uptake and usage of a service is partially driven by customer trust – especially when that service uses AI, with 64% of consumers worried about the way their personal data will be used in AI systems without their consent or permission, according to the [EY AI Sentiment Index Study](#). Examples of how Secure Creators in the study are improving customer trust and experience include enhanced internal communication security for better customer service and faster complaint resolution, and creation of customer portals that simplify access to services.

Secure Creators are more likely to say their approach positively impacts the pace of transformation and innovation. “We were developing a cutting-edge AI product, but the sensitive training data was at risk. Cybersecurity implemented data encryption and access controls to protect the AI training environment,” a Secure Creator said. “The AI product launched on time, and its success gave us a competitive edge in the market.”

Executives are increasingly recognizing the role of the cybersecurity function when expanding to new markets. A [recent Gartner study](#) found that 85% of CEOs consider cybersecurity critical for business growth. CISOs – along with risk executives – help their organizations consider the myriad implications of moving into new markets, from increased risk exposure to asset visibility. When involved early in market scouting, the cybersecurity function can both protect and add value to new market ventures.

Similarly, in new product and service development, the cybersecurity function adds value that isn’t always recognized. “Cybersecurity isn’t just about protecting new product and service value – it’s about creating it. When cybersecurity teams are embedded early in product development, they help build trust into core offerings. That trust becomes a differentiator in the market and a catalyst for growth,” said Jeremy Pizzala, EY Asia-Pacific Cybersecurity Consulting Leader.

Secure creators are likely to continue outpacing their peers

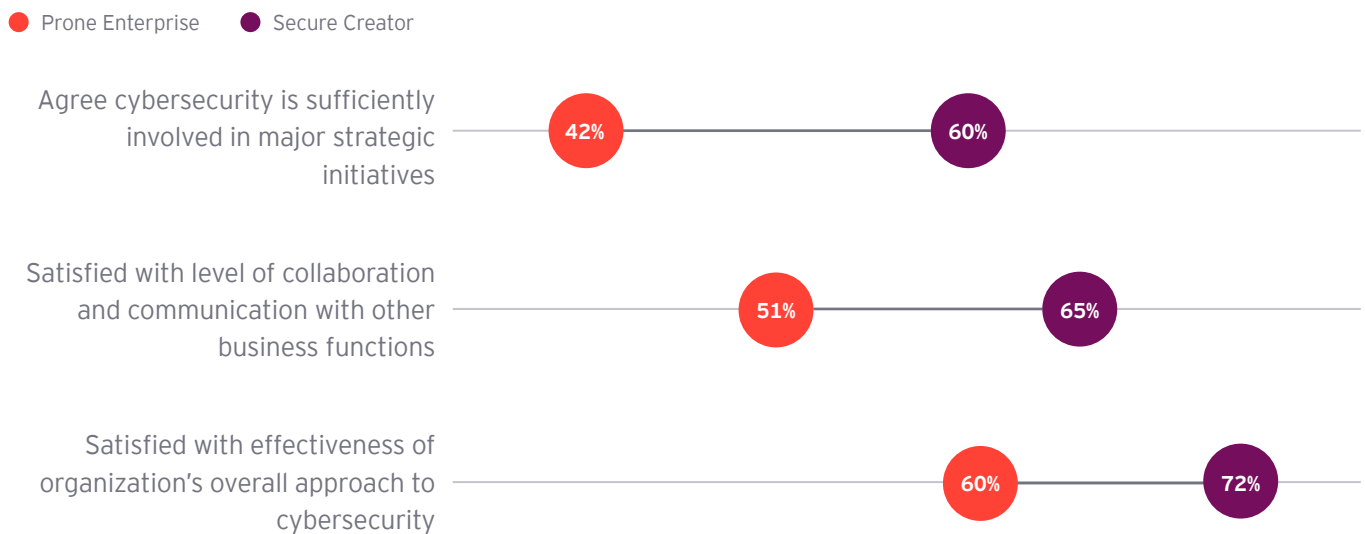
Seventy-three percent of our study's cohort of Secure creators believe their ability to add value will grow in the future. Successful, early involvement in key initiatives will give CISOs greater exposure to the board and greater power in the C-suite. It will also help CISOs develop as strategic executives – an evolution from their traditional role as a technical practitioner. Combined, it's clear to see why CISOs think their enterprise value creation is likely to grow.

"When CISOs are given a seat at the table early in strategic initiatives, they not only embed security into business planning from the ground up, but they add value by increasing speed of adoption and by building trust with consumers," said Rudrani Djwalapersad, EY Global Cyber Risk and Cyber Resilience Lead.

Our analysis shows some of the most impactful drivers of cybersecurity's impact on value creation are the core of Secure creators' approach to cybersecurity:

- Effective cyber approach: rather than just protecting value, shifting the focus to value creation, for example, by becoming early adopters of emerging technology.
- Strategic involvement: embedding themselves in core business priorities and strategies.
- Collaboration: brokering and using strong lines of communication and ties to the C-suite.

Secure Creator's approach to cybersecurity helps drive value creation



Most CEOs would acknowledge that cybersecurity must no longer be a siloed department that sits in the basement telling staff to avoid phishing emails, but something that cuts across the whole business. Encouragingly, our study indicates that there is a nascent understanding that CISOs should be involved earlier and should help inform the strategic direction of an organization beyond the cybersecurity function.

Cost savings from cybersecurity simplification and AI-driven automation

A woman in a black dress is standing in a room, reaching her right arm up towards the ceiling. The room is dimly lit, with several bright blue light beams emanating from the walls and ceiling, creating a futuristic or high-tech atmosphere. A large, faint number '2' is visible in the background, partially obscured by the light beams. The floor is dark and reflective, showing the woman's silhouette.

Leading CISOs are decreasing the complexity of their tech stacks to deploy AI more quickly, helping them reap the benefits of automation and cost savings.

The [2024 edition](#) of this study enumerated the ways AI is transforming cybersecurity. AI – or, more specifically, machine learning (ML) – is automating tasks like threat and anomaly detection, pattern recognition and identification of suspicious activities. Since that study, agentic AI has started offering a step-change improvement. For example, [CrowdStrike's Charlotte AI, powered by NVIDIA NIM microservices](#) is capable of handling the entire workflow, beginning with threat detection to resolution with no human intervention, dramatically reducing the time to resolution for cybersecurity threats.

This year's study examined a different aspect of AI: cost and time savings. The study found that cybersecurity simplification and automation have led to direct cost savings, with a median of US\$1.7m saved annually.

Since most cybersecurity functions are still in the early stages of meaningful AI integration – [a 2024 CrowdStrike study](#) found that only 6% of cybersecurity functions actively use generative AI (GenAI) tools – leaders expect the annual savings figure to grow rapidly in the coming years as AI programs mature.

Simplification and optimization

As CISOs continue the rollout of AI across the cybersecurity function, they should consider how they can simplify their approach. A recent report from ServiceNow shows that the most AI-ready enterprises take a platform approach that leverages a single codebase, simplifying management across the enterprise. This approach helps them more quickly employ new AI tools – like agentic AI – at scale, because they “don’t have to reinvent the wheel every time a new technology or application hits the market,” according to the report.

“Most organizations who are positioned to outpace their competitors in AI rollout, technology innovation and decision-making at scale are embracing a unified technology platform approach,” said Dan Mellen, EY Global and US Cyber Chief Technology Officer.

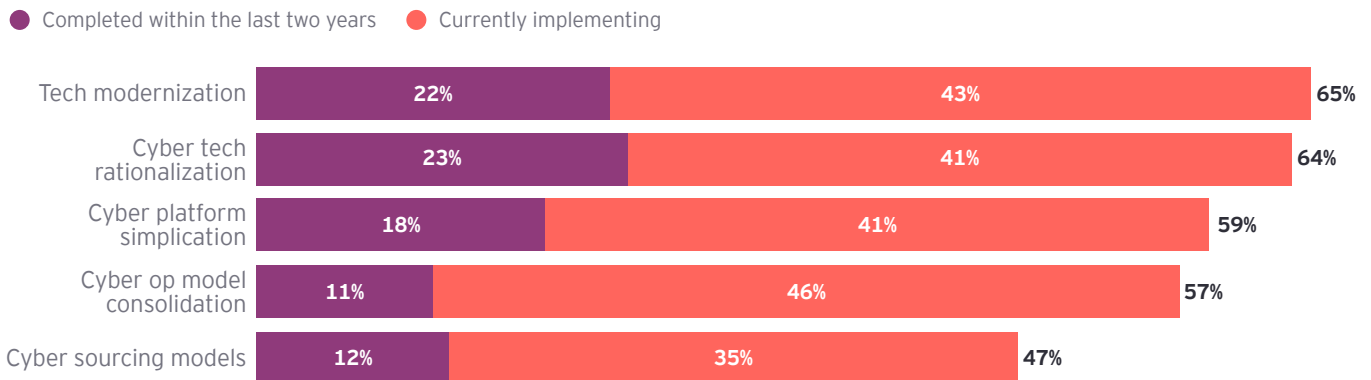
Optimizing legacy technology tools and simplifying cybersecurity tools can remove duplication and reduce costs, while also improving visibility and reducing the number of attack surfaces. Today organizations use a median of 35 different cyber tools, with 37% utilizing over 50 cybersecurity tools. Many CISOs are looking to simplify their tech stack, as well as decrease the spend on these resources: 23% of study respondents completed a technology rationalization effort in the last two years, and 41% are undertaking one. Similarly, 18% have simplified their tech platform, with 41% in the process of doing so.

Defining productivity gains

Productivity gains in organizations stem from two primary components: cybersecurity cost optimization and automation. In our survey, we asked respondents to identify the specific initiatives they have implemented within these areas and to provide the annual cost savings achieved from these completed activities. By aggregating these figures, we were able to quantify the overall productivity gains resulting from effective cybersecurity measures and automation strategies.

Cybersecurity functions are implementing simplification best practices throughout the function and enterprise

Percent of organizations who have undertaken cost optimization activities



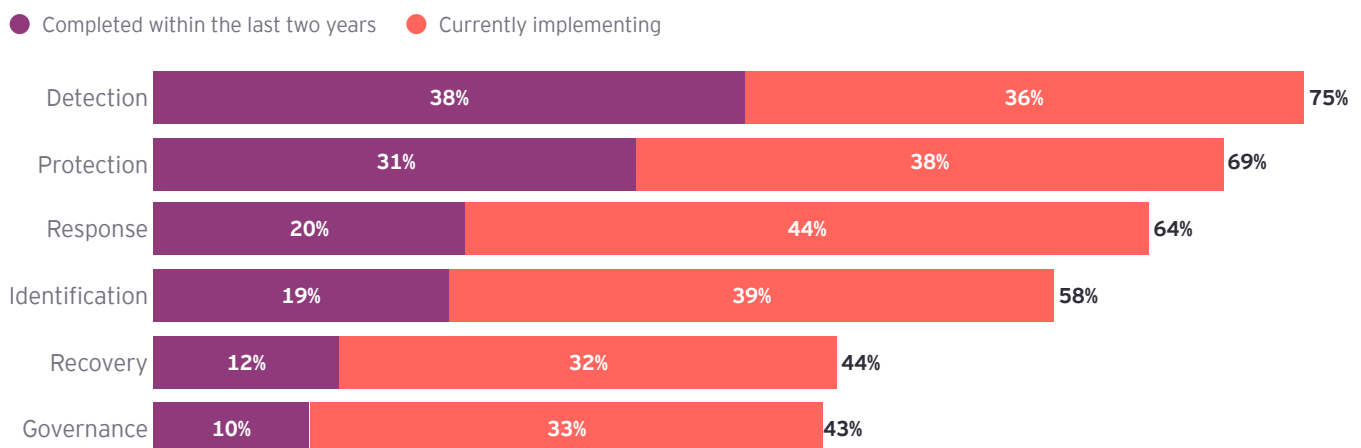
Such efforts can save money and have a positive impact on budget constraints. Secure creators have more advanced cybersecurity functions but require smaller budgets – 10% smaller on average – and are less likely to cite budgets as a key challenge.

AI and automation

AI and ML tools are helping automate processes throughout the cybersecurity function.

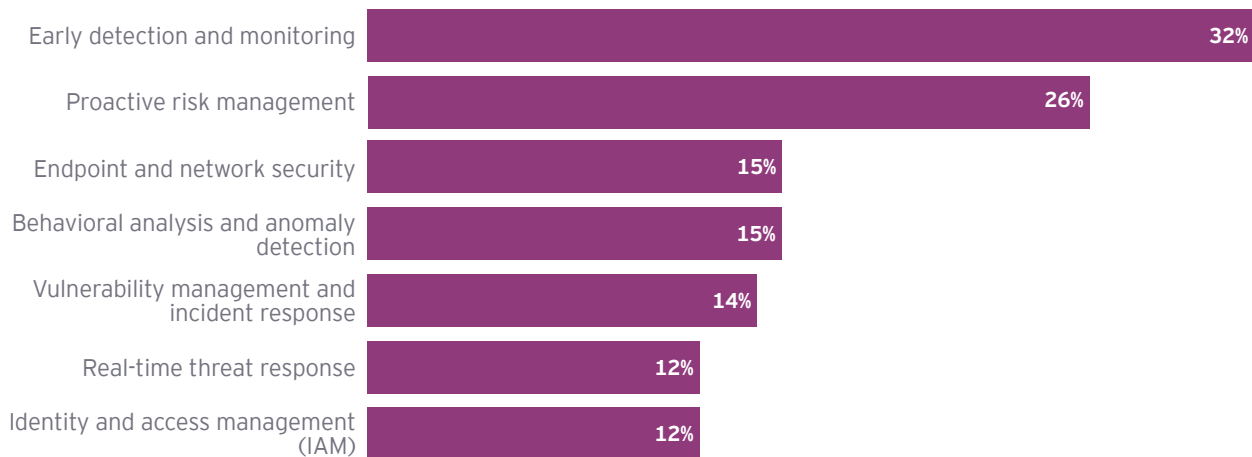
Most organizations are looking to automate core cybersecurity processes

Percent of organizations who have invested in automation for each cybersecurity process



Deployment of AI across cybersecurity priorities is leading to improved outcomes. In particular, CISOs say these automation efforts have decreased their mean time to detect (MTTD) and mean time to respond (MTTR) by 28%, on average. In addition, six in 10 respondents point to increased visibility across attack surfaces.

Highest priority cybersecurity areas for AI investment



Note: EY Insights analysis leveraging an LLM to systematically categorize and tag free-text survey responses according to a predefined curated taxonomy.

Using cost and time savings to provide more value

In addition to direct improvements to cybersecurity's effectiveness and cost savings, optimization and automation allow for more money and time to be focused on value creation, enabling organizations to stay ahead of emerging threats and enhance their overall security posture.

The combined savings – across automation, simplification and outsourcing – perhaps unsurprisingly were used to further enhance the cyber capabilities of an organization, with 74% reporting they invested to address control weakness and 46% using savings to increase coverage of the attack surface, ultimately leading to a more resilient defense against potential breaches.

More notably, two-thirds (68%) used the cost savings generated from optimization on innovation and other AI initiatives, indicating that CISOs who are ahead of the AI curve are likely to stay ahead.

Shifting this “realized” money into value creation initiatives such as AI not only benefits the wider organization but also shows that advanced cybersecurity functions operate more like strategic business units than cost centers.

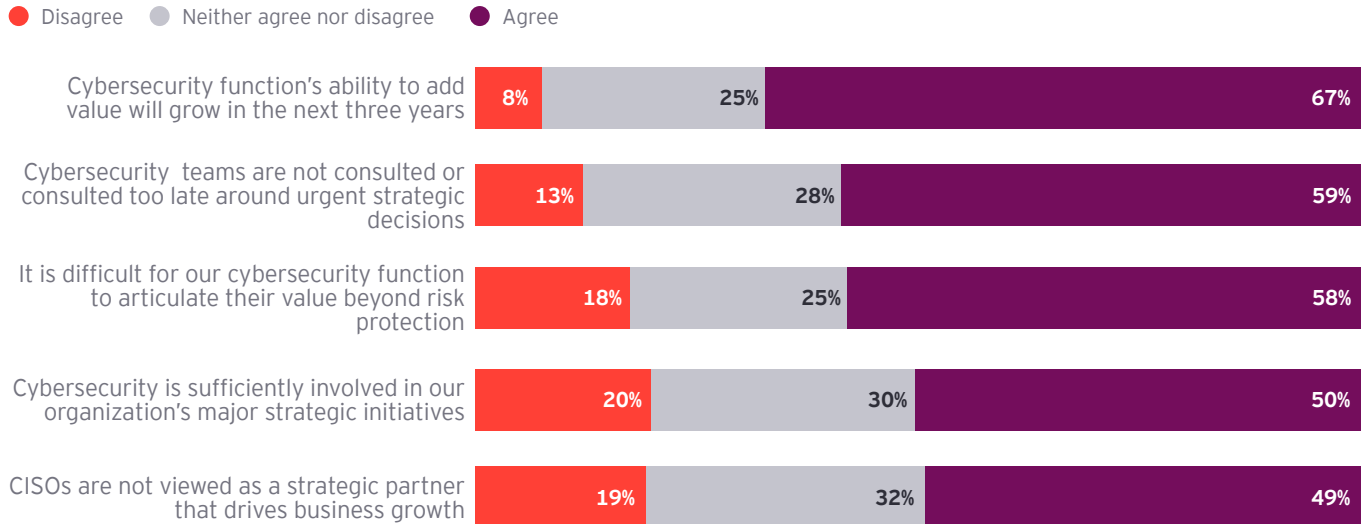
Three actions for CISOs to get a seat at the table

Despite its strategic importance, cybersecurity is still often sidelined. CISOs must act now to secure influence, funding and trust across the C-suite.



A [recent study from Ernst & Young LLP \(via ey.com US\)](#) examined the gulf between the importance of cybersecurity and the relative lack of sway CISOs hold in the C-suite, with 59% of respondents saying that the cybersecurity function is not consulted when strategic decisions are made.

CISOs find it difficult to articulate their value to the business



The US study also found a direct correlation between cybersecurity breaches and a company's share price declines. In the days following a cybersecurity incident, stock prices decrease – and can decrease up to 90 days after the incident – compared with companies that did not experience a cybersecurity incident.

Cybersecurity is also gaining importance in M&A activity. The EY Private Equity Value Creation Benchmark Survey found that PE firms are 2.3 times more likely to focus on cybersecurity during their due diligence than two years ago. CISOs should be involved earlier and more strategically to improve the dealmaking process.

As companies transform their strategies and operations around AI, CISOs are presented with a golden opportunity to be key enablers of trust, speed and value, and to position the cybersecurity function as a department of strategic growth. In doing so, CISOs are more likely to be included earlier and more meaningfully in their organization's other key initiatives.

Here are three steps CISOs can take to ensure cybersecurity is a key partner throughout the enterprise:

1

Reframe how the CISO operates

A refreshed view of the cybersecurity remit requires a reframing of how the CISO operates.

Traditional remit	Value creation
Reactive	Proactive
Source of friction	Enabling the rapid adoption of AI
Technical focus	Aligned to business strategy
Compliance-driven	Transformation and innovation focus
Siloed	Collaborative
Internal focus	Ecosystem-based

CISOs must shift from being technical practitioners within their functions to becoming strategic enablers – Secure Creators – across the enterprise. This shift requires building deep sector and business acumen to align the cybersecurity function with organizational goals. It also requires CISOs to prioritize funding that helps cybersecurity create value for initiatives like enterprise-wide AI adoption, front-office transformation, and acquisitions and divestitures.

This represents a paradigm shift in how the cybersecurity function is viewed and how it integrates into the enterprise – likely demanding broader organizational changes. Elevating the CISO to a strategic role can prompt a rethinking of how cybersecurity leaders are selected and developed, how teams are staffed and where certain business-oriented capabilities should reside. Some capabilities, such as value measurement or transformation planning, may be built within cybersecurity; others may be more effectively developed through tighter integration with finance, strategy or transformation teams, or through managed services. In this context, a value quantification framework is not just a planning tool – it can serve as a blueprint to guide more fundamental changes in how the cybersecurity function is structured, resourced and connected to the rest of the enterprise. Depending on the organization, this type of evolution may be led by the CISO or driven from above.

2 Re-evaluate your cybersecurity budget needs and allocation

In today's constrained budget environment, every functional leader must make a strong case for investment – cybersecurity is no exception. This study provides a new dimension to that case: Rather than viewing cybersecurity as a cost center or risk-reduction function, it should be positioned as a value multiplier. By connecting cybersecurity to enterprise-wide growth and transformation initiatives, and quantifying its contribution, the case moves from defensive to strategic, potentially unlocking a larger, more compelling share of the organization's value creation agenda.

CISOs also need to consider where to allocate their budgets. Broadly speaking, they can elect to spend on direct security investments or on value creation initiatives throughout the organization. According to the American Productivity & Quality Center (APQC), return on security investments (ROSI) is 19% on average.¹ Alternatively, value creation spend generates returns approximately 6.6 times greater. This new emphasis on value creation can help CISOs build budget justification and help increase their influence on key initiatives.

CISOs can simultaneously rationalize and optimize their security tools and work to reduce their associated technology costs. A best-of-suite or platform-first approach will help CISOs rationalize and transition their existing security tools to an existing strategic technology vendor platform, while earmarking forecasted savings on licensing costs for the enhancement of security controls through in-flight and planned projects.

3 Facilitate AI adoption to build trust across the C-suite and board of directors

According to our study, only 43% of cybersecurity functions are meaningfully involved in helping other functions adopt AI.

This – again – is a golden opportunity for CISOs: By positioning themselves as strategic partners in AI execution, they can earn greater trust and a seat at the table for broader transformation initiatives. The same logic applies to the other six key initiatives where cybersecurity adds significant value:

- Adopting and building technology
- Strengthening brand trust and reputation
- Improving customer experience
- Transforming and innovating across the business
- Expanding to new markets
- Developing new products and services

For CEOs, CFOs and board members, involving the CISO is more than an exercise in risk mitigation; it is an opportunity to unlock more value in each of your organization's strategic, revenue-driving initiatives. Earlier, more meaningful integration of the cybersecurity function can help drive faster deployments, trust in the market and the creation of products, services and experiences that sustain business value.

A narrow view of cybersecurity as a necessary expense aimed solely at risk mitigation leads organizations to underinvest in a capability that could drive broader enterprise value. This perspective must change. The call to action is clear: Shift budgeting decisions from a cost-centric to a value-centric lens, treating cybersecurity not as a defensive line item, but as a catalyst for growth, innovation and sustained performance.

Summary

The 2025 EY Global Cybersecurity Leadership Insights Study found cybersecurity adds a median of US\$36m in value to each strategic initiative it supports. Still, CISOs are often excluded from early decision-making, even though early involvement drives significantly greater value. To secure a seat at the table, CISOs must evolve into business executives, optimize budget allocations toward value creation and build trust across the C-suite – positioning cybersecurity as a catalyst for enterprise growth, innovation and transformation.

Authors



Richard Watson

EY Global Consulting Cybersecurity Leader
richard.watson@au.ey.com



Richard Bergman

EY Global Cyber Transformation Leader
richard.bergman@au.ey.com

Contributors

**Jim Guinn, II,
Piotr Ciepiela**

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2025 EYGM Limited.

All Rights Reserved.

EYG no. 005196-25GbI

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com