The Cyber-Resilient CEO

How confident CEOs are taking charge of cybersecurity

Voices of Change

From insights to action, the path to extraordinary value starts here.

accenture

CEOs are fully aware of the threats to their business from cyberattacks. Yet, our research shows most lack confidence in their organization's ability to avert or minimize such attacks. They learn how to be cyber resilient only *after* their organization experiences a breach. This reactionary way of treating cybersecurity results in greater risk of attacks and higher costs to remediate them. Our research finds that there is a better way for some. In this practical guide, we explore how CEOs are best placed to set in motion five actions that minimize risk and put cyber resilience at the heart of their reinvention efforts.

Authors

Paolo Dal Cin
Senior Managing Director
Global Lead
Accenture Security

Paolo works with C-suite executives, driving solutions and services on security strategy, business resilience, cyber defense, threat intelligence and managed services.

Valerie Abend
Senior Managing Director
Global Cyber Strategy Lead
Accenture Security

Valerie leads enterprise-wide security and resilience programs, and advises C-suite executives, boards, regulators and policymakers on managing cyber risk.

Rachel Barton
Senior Managing Director
Europe Strategy Lead
Accenture Strategy

Rachel specializes in growth strategy, working with C-suites and boards to help them grow sustainably through bold, transformational change.

Yusof Seedat
Thought Leadership Director
Global Research Lead
Accenture Security

Yusof leads cybersecurity research with a focus on shaping data-driven thought leadership to help guide strategic decision making and market positioning for organizations globally.

Acknowledgements

The authors would like to recognize Sarah Bird, Gargi Chakrabarty, Arlene Lehman, Eileen Moynihan, Manav Saxena, Ann Vander Hijde, Alissa Worley and Christine Yiannakis for their contributions to this report.

Contents

Executive summary

Is cybersecurity a business priority? It should be. It keeps business operations running smoothly, helps organization's optimize performance and secures customer and supplier relationships. CEOs that sideline cybersecurity expose their organizations to more risk.

Powerful forces are multiplying digital vulnerabilities. Technology innovation, including generative AI and quantum computing, environmental challenges, shifting consumer preferences, supply chain interruptions and geopolitical instability are colliding to disrupt boardroom agendas and make cybersecurity resilience a top priority.

A handful of organizations are taking charge of their own disruption by embracing Total Enterprise Reinvention, a strategy that leads to a new performance frontier. Their goal is to reinvent every part of their companies over time, centered around a digital core and a culture and capability focused on continuous reinvention.

In the context of these changing landscapes, Accenture studied the cybersecurity practices of 1,000 CEOs of large organizations to better understand what it means to be a cyber-resilient leader today. The research shows CEOs are fully aware of cybersecurity, with 96% agreeing it is a key enabler for organization growth and stability. Yet, 74% are concerned about their organization's ability to avert or minimize damage to the business from a cyberattack. It is a disconnect that highlights that a majority of CEOs lack confidence that their organizations are truly cyber resilient and their uncertainty is reflected in how they prioritize their cybersecurity investments.

Backed by our broad cybersecurity experience, Accenture has identified three issues that continue to challenge CEOs today:

Limited understanding of cybersecurity and its relationship to the business.

Cybersecurity gains are difficult to quantify. More than one-half of CEOs said the cost of implementing cybersecurity is much higher than the cost of suffering a cyberattack, yet this is the reverse of reality. Unsurprisingly, the lack of understanding results in limited strategic focus; only 15% of CEOs said they have dedicated board meetings for discussing cybersecurity issues.

Compartmentalizing cybersecurity risks as compliance issues.

Cybersecurity risks are seen as compliance issues that should be addressed by back-office control functions. Almost half (44%) of CEOs don't view cybersecurity as a strategic business matter and said it requires episodic intervention rather than ongoing attention, while 60% of CEOs said their organizations don't introduce "security-by-design"—that is, cybersecurity is not baked into business strategies, specific services or products from the outset.

Leaders' inability to keep pace with the business impact of fast-evolving risks.

Only 33% of CEOs strongly agree that they have deep knowledge of the evolving cybersecurity threat landscape and the potential cost their business could incur from failing to understand and act on new risks. Take generative AI, which is rapidly transforming everything. If it is not secure, organizations face increased risk of compromise, regulatory non-compliance, reputational damage and an inability to sustain competitive advantage. Limiting the scope and importance of cybersecurity in the business can be a missed opportunity for CEOs. It is often only after experiencing a cyberattack that the CEO understands the importance of cybersecurity and begins to personally engage time and effort into it. Such an approach is risky, given the exponential increase in cybercrimes and the potential impact on reputation and brand.

Our research and analysis examines how CEOs can proactively and confidently become cyber resilient.

We developed the Accenture cyber-resilient CEO action index to benchmark 25 leading practices that measure cybersecurity resilience. Using this index, we found a small group (5%) of CEOs that lead on cybersecurity resilience.

This group—we call them cyber-resilient CEOs—use a wider lens to assess cybersecurity across their organizations including talent, innovation, sustainability and customers.

Cyber-resilient CEOs don't rely on breach or compliance requirements to inform their cybersecurity approach; they proactively take the following actions:

1. **Embed cyber resilience in the business strategy from the start.**
2. **Establish shared cybersecurity accountability across the organization.**
3. **Secure the digital core at the heart of the organization.**
4. **Extend cyber resilience beyond organizational boundaries and silos.**
5. **Embrace ongoing cyber resilience to stay ahead of the curve.**

As a result, these leaders detect, contain and remediate cyber threats faster than their peers. Their breach costs are considerably lower and financial performance significantly better than the rest. Based on the Accenture study, this report details the practical steps CEOs can take to assess and enhance their own organization's cyber resilience.

Cyber threat complexities

Today, digital is at the core of everything, from policy and economic stability to profitability and access to ongoing pools of talent.

Yet, rapidly rising cyber threats and the risks posed when security is not embedded into an organization's digital core can hamper national and corporate competitiveness. For instance:

- The war against Ukraine and geopolitical multi-polarization has amplified many trends; in particular, global cybercrime costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015[1] and global cybersecurity spending is forecasted to reach $300 billion in 2026.[2]

- Simultaneously, ensuring resilience of digital infrastructure and operations requires examining fundamental beliefs in many industries, also impacting critical enablers such as the Internet-of-Things and cloud-based artificial intelligence (AI) services.

- Operational technology and products are increasingly vulnerable to cyberattacks, and securing these cyber-physical systems remains a challenge perceived as adding time, cost and complexity.

- Digital innovation, such as generative AI, is likely to introduce new forms of complexity. Sixty-four percent of CEOs said that bad actors could use generative AI to create new sophisticated and hard-to-detect cyberattacks.

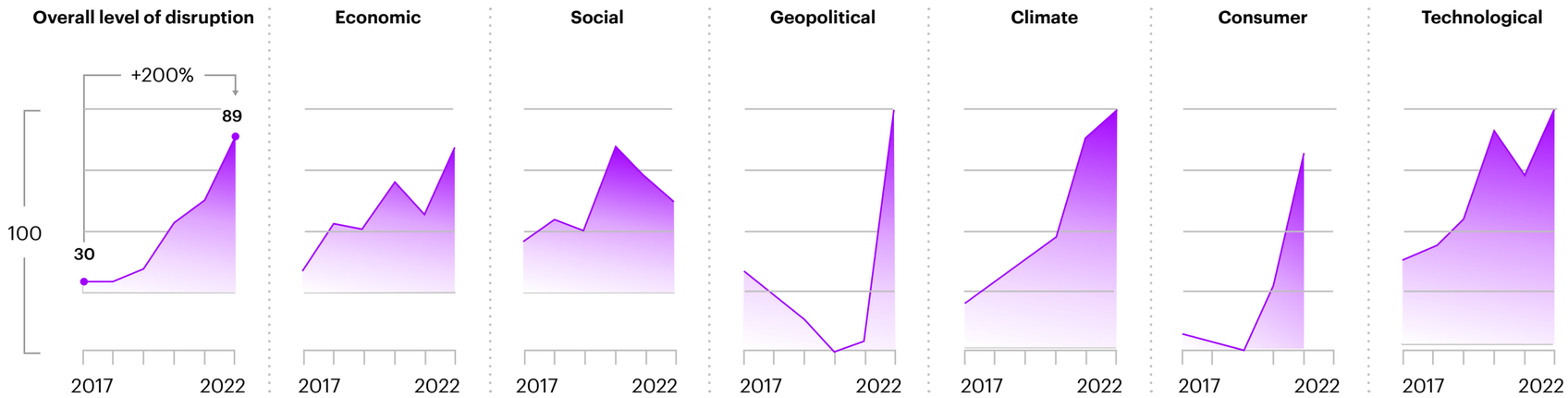
Ten years ago, Accenture foresaw every business as a digital business and today every organization is a technology organization, too. These businesses are using digital technologies extensively, such as cloud, edge computing, 5G and now generative AI, to transform in an increasingly disruptive world. In our research, 96% of CEOs said that technology plays a critical role in their current and future transformation and reinvention initiatives.

But the dramatic changes prompted by these digital transformation and reinvention efforts also introduce new avenues for cyberattacks that are not only proliferating but also upending business plans. The Accenture Global Disruption Index (Figure 1)—a composite measure that covers economic, social, geopolitical, climate, consumer and technology disruption—shows that levels of disruption increased by 200% from 2017 to 2022.[3]

Figure 1. Accenture Global Disruption Index

Levels of disruption increased by 200% from 2017 to 2022

Overall measure of disruption based on average of six sub-components, each of which is based on indexed scores of a set of indicators.



Source: Accenture, Total Enterprise Reinvention, 2023

When we asked CEOs in our research about disruptive forces that are creating cyber vulnerabilities for their organizations, they identified the following factors:

52%

Technology innovation

More than one-half (52%) ranked accelerated pace of technology innovation as the top risk for cyberattacks—with 86% rating cyber trust and resilience for emerging technologies, like generative AI and quantum computing, as highly relevant for their organizations.

51%

Supply chain disruption

Around one-half (51%) of CEOs ranked supply chain as the second highest external risk, underscoring the vulnerabilities of global organizations along their value chains spread over different locations.

90%

Environmental vulnerabilities

Environmental challenges are other external risks that CEOs rated highly, with 90% acknowledging the link to and vulnerability from environmental changes and initiatives.

CEOs also ranked shifting consumer preferences and geopolitical tension among the top 10 external factors impacting the cyber threat landscape, with 90% anticipating a catastrophic cyber threat event in two years.[4]

All of these factors have reshaped the cyber threat landscape, making cybersecurity a key enabler to driving business value with confidence, trust and resilience.

Size and scale

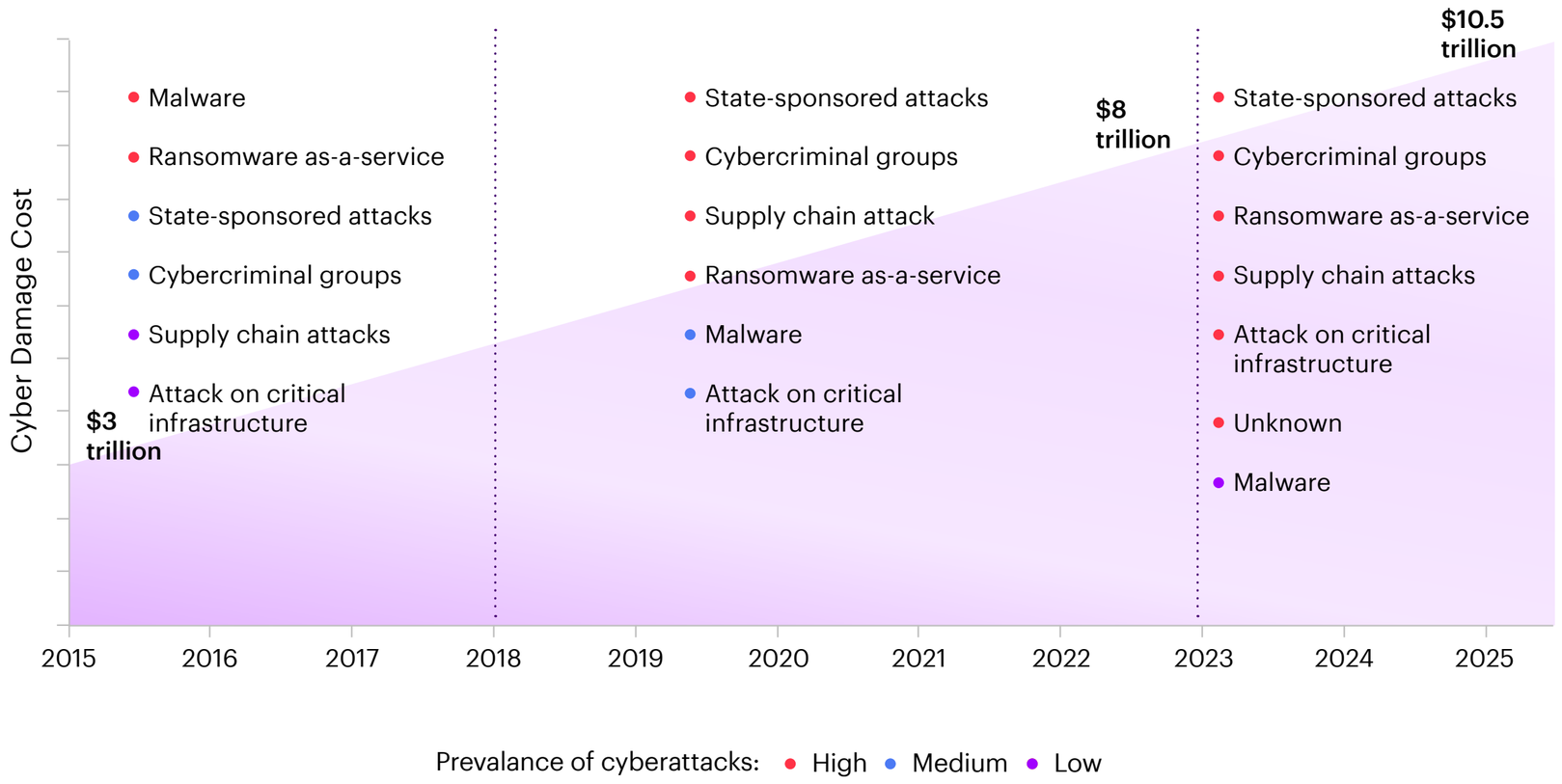
Cybercrime losses rose from $3 trillion in 2015 to $8 trillion in 2023 and are forecast to hit $10.5 trillion in 2025—the size of the world's third-biggest economy after the United States and China, according to research published by Security Ventures.[5]

Cyberattacks are becoming more complex and frequent and can cripple business operations quickly—even large global companies with sophisticated operations (Figure 2).

Take the example of Danish shipping and logistics company Maersk. A NotPetya ransomware attack served as a wake-up call to bolster its cybersecurity preparedness. The IT systems' impact was immediate: almost 50,000 computers were infected across 600 sites in 130 countries.

The business impact followed. Unavailable systems stranded ships and critical shipments at ports. The losses mounted to $300 million, affecting close to 90,000 workers, not to mention the port infrastructures, companies and consumers impacted by the disruption in global shipment. The ransomware attack resulted in a 20% drop in business volumes.[6]

Figure 2. Cybercrime damage costs and complexity



Source: Accenture Research analysis, Security Ventures

Risk and reward

CEOs are now paying more attention to cybersecurity risk. Recognition of the financial losses, reputational damage and operational disruptions that can arise from cyberattacks is fuelling a growing sense of urgency and is a driving force behind a shift in their mindsets.

A majority 96% of CEOs understand the importance of cybersecurity, acknowledging that it is a key enabler for organizational growth, stability and competitiveness.

Our analysis of earnings call transcripts of large companies supports this growing awareness—we found a sixfold increase in the number of mentions of the words cyber risk, cybersecurity and cyberattacks by CEOs from 2017 to 2022.[7] What's more, 90% of CEOs said they consider cybersecurity as a differentiating factor for their products or services to help them build trust among customers.

96%

of CEOs understand the importance of cybersecurity, acknowledging that it is a key enabler for organizational growth, stability and competitiveness.

Being risk-ready

In a fast-moving cyber threat landscape, knowledge is power. Yet, there is a growing gap between CEOs' increasing awareness of the business value of cybersecurity and what they understand about emerging threat actors—which, in turn, lowers their confidence to avert or mitigate cyberattacks.

Simply put, businesses are not yet cyber resilient and CEOs are unsure of how to measure cyber resilience or ensure that their businesses are on the right track. But since the digital world connects everything, securing it is essential, especially as digital exposure and vulnerabilities expand.

Just 33% of CEOs strongly agree that they have deep knowledge of the evolving cyber threat landscape leaving many unclear how to address the risks. Unsurprisingly, 74% are concerned about their organization's ability to avert or minimize damage to the business from a cyberattack. Around 60% of CEOs we surveyed said they perform common cyber-resilience practices but recognize that's not enough. In addition, almost half believe that cybersecurity requires episodic intervention, rather than considering cybersecurity as a key business enabler that requires ongoing attention.

This reactive mindset is also apparent in the limited time that CEOs personally invest to address cybersecurity; only 15% have dedicated board meetings for discussing cybersecurity issues. And the fact that cybersecurity is hard to quantify makes it easier to overlook—54% feel the cost of implementing cybersecurity is much higher than the cost of a cyberattack—yet our research shows those that prioritize cyber investments experience up to three times lower cyber breach costs compared with their peers.

33% of CEOs strongly agree that they have deep knowledge of the evolving cyber threat landscape

74% are concerned about their organization's ability to avert or minimize business loss from a cyberattack

60% of CEOs said they perform common cyber-resilience practices but recognize that's not enough

15% have dedicated board meetings for discussing cybersecurity issues

54% feel the cost of implementing cybersecurity is much higher than the cost of a cyberattack

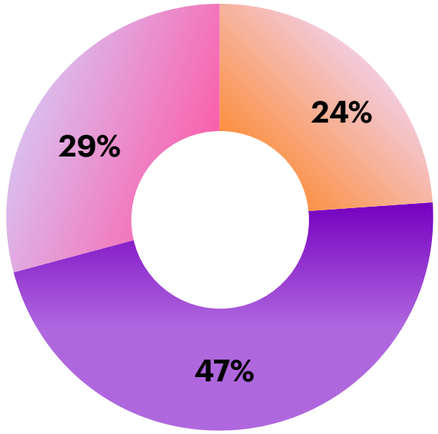
The result is that many CEOs tend to treat cybersecurity as a technical function that is incident- and compliance-driven.

Consider that a massive 76% of CEOs said they only implement security controls for critical functions or deploy them after transformation is finalized or when vulnerabilities are detected. The majority (91%) said cybersecurity is a technical function that is the responsibility of the CIO or CISO, with 95% saying compliance is one of the key drivers of their cybersecurity strategy (Figure 3).

Figure 3. CEOs view cybersecurity as a siloed technical function that is incident- and compliance-driven

7 in 10

CEOs implement security controls for critical functions or deploy after transformation is finalized and vulnerabilities are detected



- Embed security controls in all transformation initiatives from the start.
- Implement security controls only for critical functions, balancing speed and risk management.
- Deploy security after transformation is finalized only if vulnerabilities are detected, ensuring we can move transformation as fast as possible.

~50%

CEOs said cybersecurity requires **episodic intervention** rather than ongoing attention.

91%

CEOs said cybersecurity is a **technical function** and they rely on the expertise of their CIO or CISO to drive it efficiently.

95%

CEOs said that **compliance drives their cybersecurity** strategy to ensure their organizations adhere to standards and regulatory requirements.

Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Unfortunately, it is often only after CEOs live through a material cyber incident that they proactively invest time, resources and expand expectations beyond the CISO and technology functions.

A cyberattack on Colonial Pipeline in May 2021 illustrates how many CEOs are being asked to handle this massive shift in cyber vulnerabilities while they are still uncertain about their ability to keep pace with changes. The attack not only disrupted the company's operation, but also disrupted fuel supplies to the United States Southeast, leading to panic buying and a spike in gasoline prices. The attackers stole 100 gigabytes of data within a two-hour window. They infected the company's IT with ransomware, including billing and accounting.

In response, Colonial Pipeline shut down the pipeline to prevent the ransomware from spreading, leading to a supply crunch in the market. The CEO accepted in a Senate hearing that the company did not have a plan in place to prevent a ransomware attack. After the attack, the company revamped its Security team, hired its first Chief Information Security Officer (CISO) and began rebuilding its cybersecurity program.[8]

Five cyber-resilient actions

For CEOs, closing the cyber resilience gap is a business priority.

Our cyber-resilient CEO action index, comprising 25 practices that measure cyber resilience (see About the Research), identified the practices that CEOs who prioritize cybersecurity undertake to drive business value with confidence, trust and resilience.

We grouped these practices into five broad actions:

01 **Embed cyber resilience in the business strategy from the start.**

02 **Establish shared cybersecurity accountability across the organization.**

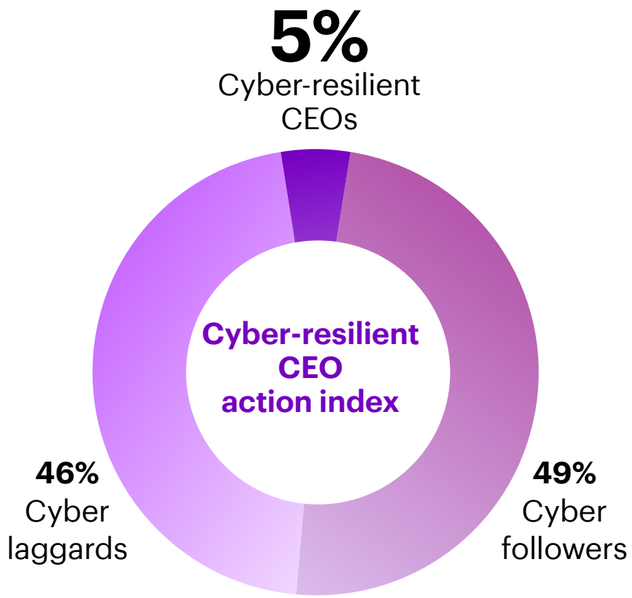
03 **Secure the digital core at the heart of the organization.**

04 **Extend cyber resilience beyond organizational boundaries and silos.**

05 **Embrace ongoing cyber resilience to stay ahead of the curve.**

Using the index, we found just 5% of CEOs are leaders in cyber resiliency. These cyber-resilient CEOs consistently take three or more of these actions, without waiting for a breach or compliance deadline.

At the next level are the cyber followers. Comprising 49%, these CEOs rigorously follow at least two of the five actions and adopt some practices from the remaining actions. The cyber laggards, 46% of our sample, don't consistently or rigorously take any of the actions and are typically stuck in a reactionary mode.



What does a cyber-resilient CEO look like?

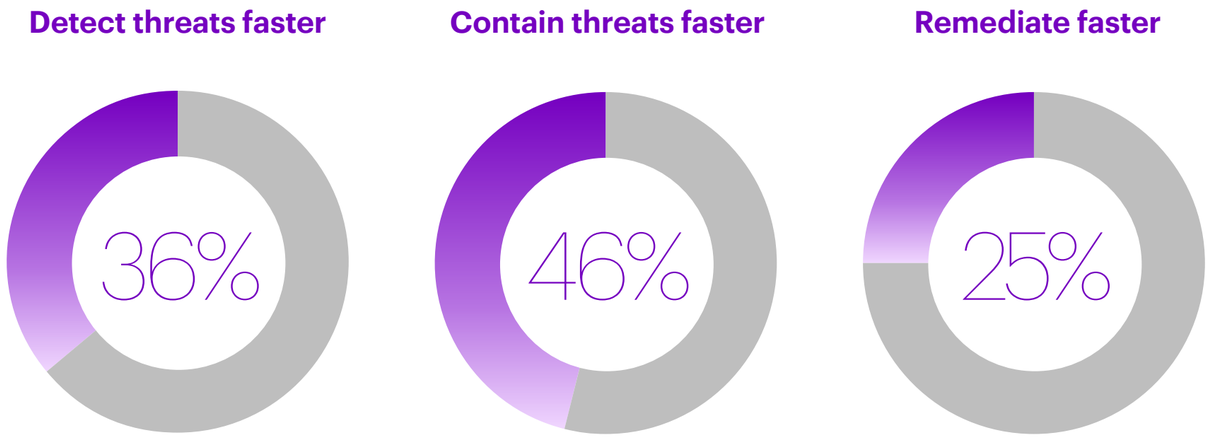
The research shows that cyber-resilient CEOs:

Act confidently

They are more confident that their organizations are cyber resilient—60% of them said they are cyber resilient compared to 24% of the cyber followers and cyber laggards combined. And their claims are supported by their ability to detect, contain and remediate threats faster (Figure 4) and the fact that their breach costs are almost 2X lower than cyber followers and 3X lower than cyber laggards.

Despite suffering 25% more attempted intrusions in 2022 over 2021, the success rate of breaches for cyber-resilient CEOs (total successful breaches as a percentage of total attempted breaches) is lower compared to cyber laggards (14% lower) and cyber followers (6% lower).

Figure 4. Cyber-resilient CEOs take action



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)
Percentages represent cyber-resilient CEOs vs cyber laggards.

Embrace reinvention

All cyber-resilient CEOs we surveyed adopt enterprise-wide strategies to reinvent their functions and business units, building capabilities that cut across functional and departmental siloes and establishing new performance frontiers. In addition, they take a holistic view of cybersecurity, embedding it in their strategies from the outset.

Assess holistically

Cyber-resilient CEOs use a wider 360-degree lens when considering their cybersecurity posture—up to 1.8 times more than their peers—across non-financial measures, such as sustainability, talent, technology innovation and customers (Figure 5).

Figure 5. Cyber-resilient CEOs take a 360-degree approach to cybersecurity

360°cyber awareness scores assess how well CEOs perceive and associate cybersecurity across non-financial measures

Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

As a result, on average, cyber-resilient CEOS are achieving higher business value than their peers.

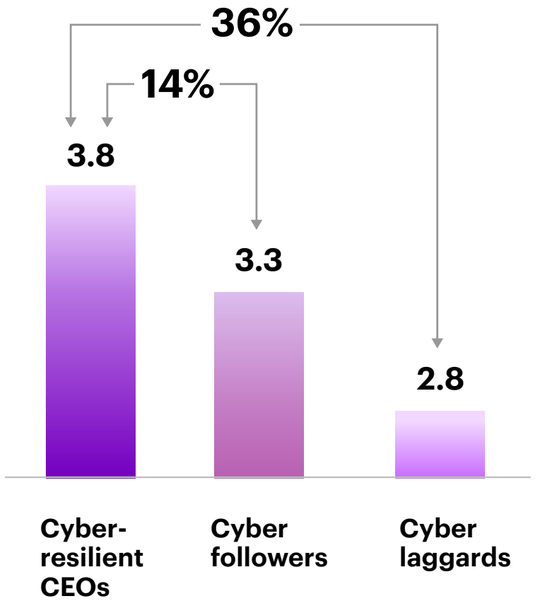
Figure 6. Cyber-resilient CEOs outperform peers financially

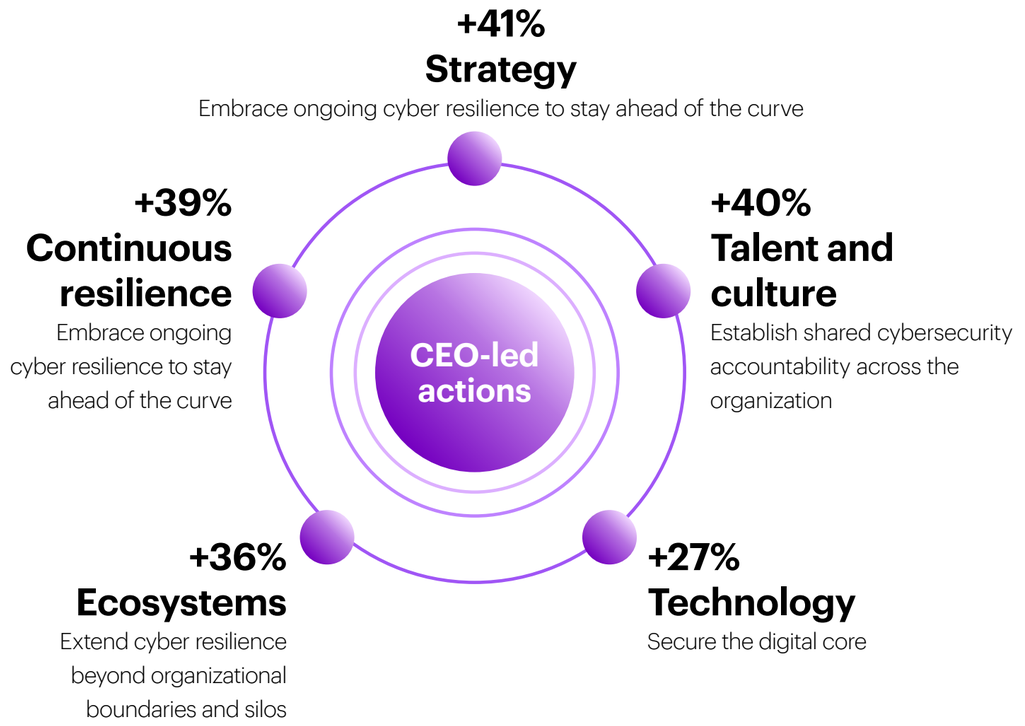
+16%	Higher incremental revenue growth
+21%	More cost reduction improvements
+19%	Healthier balance sheet improvements

Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Overall, cyber-resilient CEOs outperform their peers in each of the five actions on our index—strategy, talent and culture, technology, ecosystems and continuous resilience—beating cyber followers by 14 percentage points and cyber laggards by 36 percentage points (Figure 7).

Figure 7. Cyber-resilient CEOs outperform peers on the CEO action index





Cyber-resilient CEOs vs. cyber laggards

Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

The cyber-resilient CEO handbook

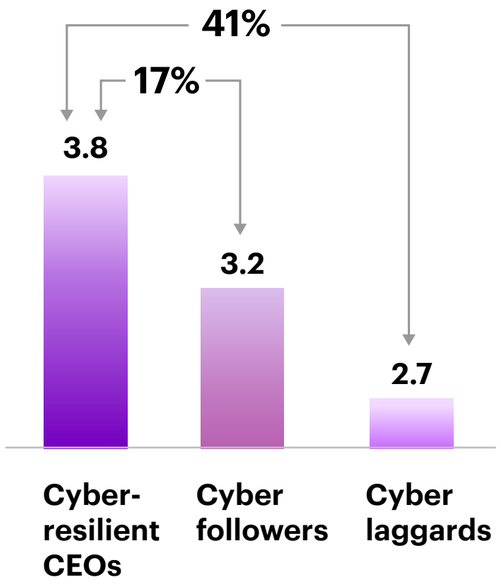
By applying all five actions, CEOs can shift from viewing cybersecurity as a purely technical function—handled by IT alone—elevating it to an organization-wide priority and establishing processes for reporting and accountability from the C-suite to the board.

Embed cyber resilience in the business strategy from the start

For cyber-resilient organizations, a bold vision for cybersecurity that's embedded in the business strategy is a key competitive differentiator.

On the **strategy** dimension of the CEO action index, cyber-resilient CEOs outshine their counterparts. They excel in embedding cyber resilience into their business strategies from the outset, scoring 3.8 points. This performance stands significantly higher, with a 41% advantage over cyber laggards and a notable 17% lead over cyber followers. By integrating cyber resilience into their strategic approach, cyber-resilient CEOs demonstrate their commitment to safeguarding their organizations against evolving cyber threats and maintaining a robust security posture (Figure 8).

Figure 8. Cyber-resilient CEOs embed cyber resilience into the business strategy



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Practical steps: Strategy

1. Endorse cybersecurity as a strategic business enabler to identify new value

Embed cyber resilience into the fabric of a business by treating it as a strategic enabler from the outset. This involves CEOs endorsing and championing a framework for evaluating cyber risks and mandating use of the framework to inform strategic business decisions and investments. When business leaders have a strong business case and understand why and how cyber risk management is a business enabler, they are more likely to embed strong practices from the start. Cyber-resilient CEOs (almost 70% vs. 38% of cyber laggards) distinguish themselves in driving this leading practice. The value potential is compelling; our earlier research has shown that those organizations that closely align cybersecurity programs to business objectives are 18% more likely to achieve target revenue growth and market share, improve customer satisfaction and trust and realize greater employee productivity.

2. Treat cyber performance like financial performance, linked to executives' personal performance outcomes

Ensure leaders embrace cybersecurity as an integral part of decision-making processes, from strategic planning to budgeting, enabling effective risk management and mitigation strategies. This demonstrates the organization's commitment to protecting sensitive data, maintaining operational continuity and safeguarding customer trust—ultimately boosting resilience in the face of evolving cyber threats. Sixty percent of cyber-resilient CEOs manage cyber performance in the same way they manage financial performance, compared to one-third of cyber laggards. Consider how executives embed and involve cybersecurity in their business strategies and decision-making. Hold them accountable for the volume and severity of risk exceptions when they aren't meeting the policies and standards that are aligned to the company's risk appetite.

3. Review cyber risk assessments throughout the lifetime of all critical initiatives

Whether launching new products, expanding services, making acquisitions, or establishing operations in new locations, integrating cyber risk management continuously enables businesses to quantify and address potential cybersecurity complexities in their business strategies. CEOs should set clear targets and then request reporting on how, when and where security was consulted, with risks identified and solutions provided throughout the strategic planning, implementation and lifetime of a business initiative. Close to 70% of cyber-resilient CEOs versus 41% of cyber laggards do this.

Practical steps: Strategy

4. Reduce organizational and technological complexity

Organizational and technological complexity introduce cyber risk. By simplifying complex organizational hierarchies, decision-making processes and operational workflows, CEOs enable better responses to risks and potential breaches and improved visibility and control over cybersecurity measures. This improves a CISO's ability to detect, respond to and mitigate cyber threats faster and with greater reliability. This structural simplification enables improved coordination, faster decision making and more effective implementation of security measures, ultimately enhancing overall cyber resilience.

5. Lead with transparency with all stakeholders

Over two-thirds of cyber-resilient CEOs prioritize transparency by openly disclosing cyberattack attempts and the corresponding actions to address them with stakeholders. This includes internal and external stakeholders who may be impacted by the organization's cybersecurity practices or have an interest in its security posture, such as customers, suppliers, or regulators. By openly sharing information about cyber incidents, organizations demonstrate their commitment to transparency and their proactive efforts to tackle cyber threats while maintaining strong relationships with stakeholders.

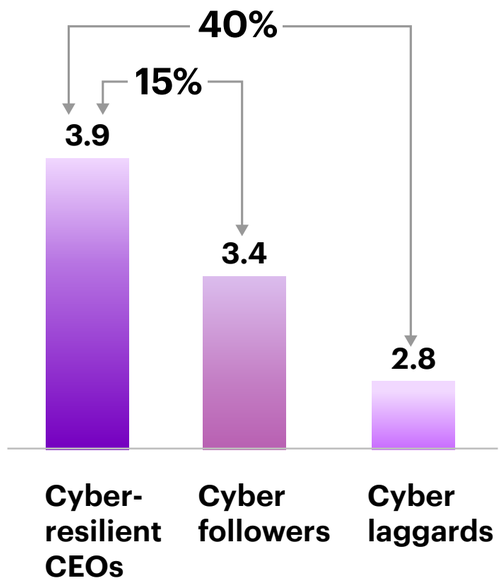
What's more, organizations have increasing interdependencies with their stakeholders, so leading with transparency and setting expectations for ecosystem partners to do the same improves cyber resilience. The United States Securities and Exchange Commission's (SEC) latest regulations to improve cyber risk management transparency are a call to action to support greater information sharing—not only to meet compliance-based expectations, but also to improve stakeholder engagement and cyber resilience across ecosystems.

Establish shared cybersecurity accountability across the organization

Cyber-resilient CEOs recognize that a security-oriented culture starts with awareness at the highest levels and includes everyone in the organization.

In the **talent and culture** dimension of the CEO action index, CEOs' performance was evaluated based on their adoption of security practices that promote shared cybersecurity accountability throughout the organization. Cyber-resilient CEOs achieved a score of 3.9 points, outperforming cyber laggards by 40% and surpassing cyber followers by 15%. Cyber-resilient CEOs are more proactive in establishing a culture of cybersecurity involving employees at all levels (Figure 9).

Figure 9. Cyber-resilient CEOs are more proactive in establishing a culture of cybersecurity



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Practical steps: Talent and Culture

1. Instil a culture of shared accountability across the C-suite

Establish a culture of shared accountability, inspiring business leaders to view cybersecurity as a competitive differentiator that enables innovation while ensuring safety. Two-thirds of cyber-resilient CEOs said they have established a stronger relationship with the CISO to encourage and set an example for other leaders. Accountability requires the CEO to align the incentives for the C-suite and their leadership team. For example, current incentives for technology leadership almost always stress the speed of upgrades, new technology rollouts and security incentives to eliminate vulnerabilities that could lead to a breach. But with shared business incentives, leadership teams can move at pace with shared accountability and strong risk management practices.

Almost 70% of cyber-resilient CEOs adopt shared accountability, in contrast to only 37% of cyber laggards. CEOs should instil shared cybersecurity accountability within their leadership teams, using both incentives and consequences to drive effectiveness. This includes measuring C-suite and leadership accountability based on their specific roles and empowering organizations to support these accountabilities. For example, consider CFO/COOs; they must govern the playbook and process for determining and reporting financial materiality of cybersecurity incidents. This requires insights from other leaders within the organization, such as business heads that are intimately aware of transaction volumes and business loss impacts or IT leadership who know the specific interdependencies of applications, infrastructure and processes. Similarly, the CHRO should lead recruiting and upskilling cyber talent in a competitive market and partner to ensure the organization has ongoing security and awareness approaches that address the human risk factor of cybersecurity. While elevating the C-suite's relationship with the CISO is essential, CEOs need to make sure that common accountabilities enable cyber-resilient outcomes.

2. Build a cybersecurity-first culture across the enterprise

CEOs can play a critical role in building a cybersecurity-first culture within their organizations by emphasizing the importance of cyber-savvy behavior across all levels. CEOs should lead by example, speaking out about the importance of cybersecurity and demonstrating the efforts they take to expand their personal knowledge of cybersecurity. They are empowered to set the tone for their employees and make their accountability for cyber risk management transparent to leadership in a way that filters down to each member of the executive team. Notably, cyber-resilient CEOs are 62% more likely to actively cultivate this cybersecurity-first culture compared to cyber laggards. Doing this can infuse the practice of safe digital habits across functions and operations, from payroll to supply chain to the customer relationship.

Practical steps: Talent and Culture

3. Spearhead the call to action to drive innovation and resilience

Innovation has never been more accessible. Widespread availability of AI, specifically generative AI, presents cybersecurity challenges and significant opportunities for organizations to optimize and automate their security processes. Collaborate with CISOs to proactively explore both the risks and use-cases for generative AI. By harnessing the power of generative AI, organizations can effectively manage workloads, eliminate labor-intensive tasks and enhance their cyber defense capabilities. Cyber-resilient CEOs indicated automated threat detection, cyberattack simulation scenarios and manual security task augmentation as their key uses of generative AI for cyber defense. More than half of cyber-resilient CEOs work closely with their CISOs to assess and manage the risks of generative AI, ensuring that the technology is used safely and effectively compared with 33% of cyber laggards.

For example, Accenture has embraced AI and automation through our Intelligent Application Security Platform. Using both leading commercial scanning tools and artificial intelligence to identify, test and reduce vulnerabilities at scale, application teams saved thousands of hours and improved risk reduction.

4. Support efforts to bridge the security talent gap

Close the growing security talent gap by investing in talent development alongside hiring efforts. Identify roles that can be automated or augmented with generative AI. Move from being a talent consumer to talent creator by hiring individuals who possess traits such as curiosity, critical thinking and problem-solving skills, while also providing training to fill any existing skill gaps. Almost 64% of cyber-resilient CEOs plan to increase investment in upskilling and reskilling their cybersecurity workforce in the next three years, compared to 38% of cyber laggards.

5. Adopt Cybersecurity-as-a-Service (CaaS) for highly critical security areas

Almost 60% of cyber-resilient CEOs prioritize this practice. Most agreed CaaS offers benefits such as cost reduction, vendor consolidation and addressing the talent gap.

For example, when a North American retail chain became a standalone public company, it needed to rethink its IT operations. Accenture was asked to support the retailer's information security team by incorporating cybersecurity-as-a-service, initially running the company's security operations, including threat intelligence and a Security Operations Center (SOC). Today, Accenture provides data protection, identity management, network security, vulnerability management and security awareness and risk management as-a-service improving the retailer's cyber resilience and business outcomes by being secure from the start.

Secure the digital core at the heart of the organization

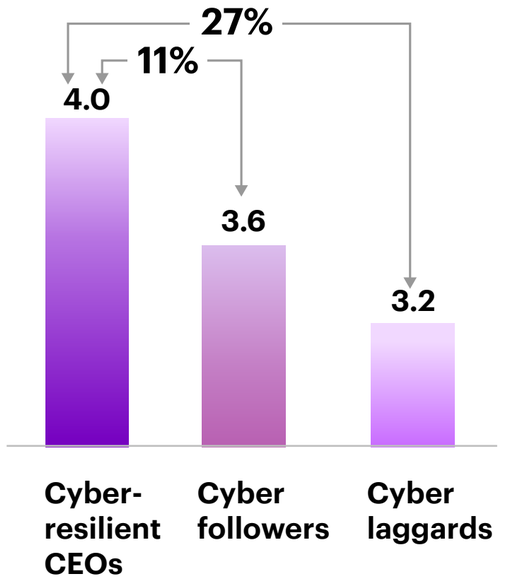
CEOs need to prepare now for the future when threat actors use new technology, such as quantum computing, to break most of the (public key) encryption algorithms and decrypt confidential personal and business information, creating huge risk around data confidentiality and privacy.

Our research shows that cyber-resilient CEOs ensure their teams secure the digital core which consists of three layers: an infrastructure and security layer, a data and AI layer and an applications and platforms layer. They create and sustain a trusted environment for customers, employees and supply chain partners and are better prepared for reinvention.

In the **technology** dimension of the CEO action index, CEOs' performance was evaluated based on their adoption of technology-related security practices to safeguard the digital core. Cyber-resilient CEOs achieved a score of 4.0 points, outperforming cyber laggards by 27% and surpassing cyber followers by 11%.

Cyber-resilient CEOs are more proactive in adopting security practices that enhance the security of their digital infrastructure (Figure 10).

Figure 10. Cyber-resilient CEOs ensure their teams secure the digital core



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Practical steps: Technology

1. Prioritize and promote security by design

Endorse leadership efforts to build and implement agile security strategies that can swiftly respond to minimize the impact of attacks. By doing so, organizations can ensure seamless operations even in the face of a cyberattack. To grow with confidence, business competitiveness requires more digitalization and better cyber resilience. As a result, it is crucial to recognize that high-tech debt should not lead to reduced investments in security. More digitalization can bring more resilience if cybersecurity isn't treated as an afterthought. Notably, one in every two cyber-resilient CEOs embed cybersecurity in the digital core from the outset. As an example, a large retail and commercial bank introduced agile cybersecurity decision-making early in its digital transformation process to reduce risks and vulnerabilities, improve data protection and enhance its overall security posture. What's more, the bank has reduced costs and downtime while improving compliance—and enhancing its reputation as a secure and trustworthy organization. On the other hand, a recent study found the discovery of an error due to poor application security in an app's coding phase, instead of during initial planning, costs five times as much to fix—and that soars to 30 times the cost post-release.

2. Champion a zero-trust approach

At the forefront of CEO responsibilities is the pivotal role of championing future-proofing strategies, particularly the proactive adoption of a zero-trust framework. This strategic approach not only redefines conventional security paradigms, but also serves as a catalyst for cultivating resilience while spearheading the transformation of the digital core. Incorporating a zero-trust mindset involves a fundamental shift in how security is perceived and enacted within the organization. It entails treating every access attempt as potentially unauthorized, regardless of the user's origin or the network's location. By advocating for continuous verification of user identities, device attributes, and network components, CEOs pave the way for a culture of heightened security awareness.

The significance of this approach extends beyond bolstering security practices. By embracing and championing zero-trust principles, CEOs trigger a comprehensive transformation of the organization's digital architecture. It encompasses recalibrating data access controls, implementing robust encryption mechanisms and deploying cutting-edge real-time monitoring and anomaly detection systems. This holistic, proactive approach not only ensures that CEOs position their organizations at the vanguard of secure digital transformation, but also cultivate resilience by empowering their teams to navigate the evolving threat landscape with confidence and agility. Seventy percent of cyber-resilient CEOs have already embraced the zero-trust approach, compared with only 41% of others.

Practical steps: Technology

3. Make building digital trust a priority

Collaborate with the Chief Data Officer and CISO to ensure that they implement robust data governance and protection measures for customer data and other highly confidential information. More than half of cyber-resilient CEOs have embraced this approach. Consumers have made it clear that trust matters; they are prepared to abandon brands that don't support their reimagined values. Be prepared for constant change as new tech becomes mainstream. For example, to ensure long-term security in the face of quantum computing advancements, adopt crypto-agile encryption. It is crucial to be aware of the potential risks and implement quantum-resistant algorithms now to secure systems and protect customer data for the future.

4. Secure emerging technologies

Foster a sense of responsibility throughout teams regarding the development and usage of emerging technologies. Allocate increased resources to their cybersecurity budget as they progress on their journey of adopting and implementing emerging technologies. Remarkably, 76% of cyber-resilient CEOs (vs. 41% of cyber laggards) intend to boost their cybersecurity budget as the adoption of emerging technologies intensifies.

Half of cyber-resilient CEOs see generative AI as a core cyber defense technology they could use to improve cyber resilience. Assess and manage the risks associated with generative AI and hold everyone in the organization responsible for its safe and effective utilization, working closely with the CISO. Develop a security framework with guidelines, protocols and compliance benchmarks and build it into generative AI and quantum systems from the start. Generative AI and machine learning (ML) have the potential to detect and respond to security threats like malware, phishing and distributed denial-of-service (DDoS) attacks in real-time, enhance security automation and analyze vast datasets to identify patterns, anomalies and trends indicative of security breaches. However, the adoption of generative AI should be approached cautiously, accompanied by clearly defined governance, standards and oversight.

Extend cyber resilience beyond organizational boundaries and silos

Cyber resilience is a broader goal than improving the maturity of the information security function. While information security teams need to continuously improve capabilities to thwart a changing threat landscape, if the CEO's focus is only on holding the CISO accountable, the result will be a siloed capability that is not aligned to the business risks of the company.

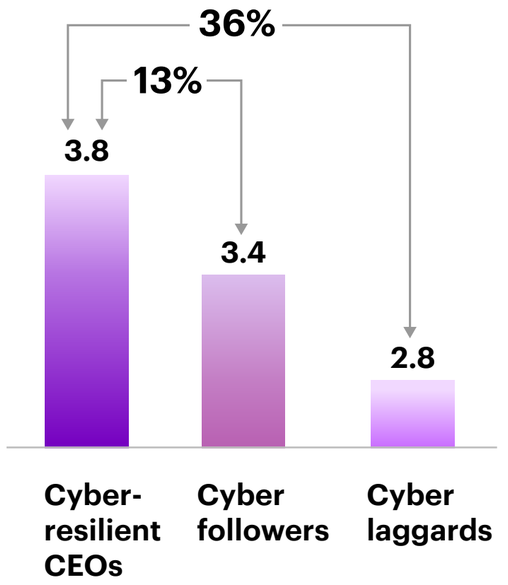
Since cyber risk has become a top business risk, CEOs need to ensure that executive management is assessing and addressing risks as part of their company's overall Enterprise Risk Management (ERM). This is reinforced by the SEC's recently adopted regulation, which requires that public companies report the cybersecurity expertise of its board members, officially moving cybersecurity into the boardroom.

Cyber risks are expanding across all aspects of the enterprise, including cyber-physical environments such as the manufacturing or distribution floor, digital infrastructures such as offshore platforms, smart digital products such as medical devices and supply chains and third parties.

Recent attacks have exposed how greater interconnectivity, network access and supply chain and ecosystem vulnerabilities can affect even the most secure businesses. Cyber-resilient CEOs actively establish a trusted environment and prepare their organizations for future threats.

In the internal and external **ecosystems** dimension of the CEO action index, cyber-resilient CEOs are proactive in safeguarding their ecosystems against vulnerabilities. Cyber-resilient CEOs achieved a score of 3.8 points, demonstrating a 36% higher performance compared to cyber laggards and a 13% over cyber followers (Figure 11).

Figure 11. Cyber-resilient CEOs are more proactive in protecting their ecosystems



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Practical steps: Ecosystems

1. Set expectations that strategic partnerships make supply chains cyber resilient

Recognize the critical role of supply chain in every business and prioritize partnerships with companies that have strong cyber-resilient postures. Implement tailored policies and controls for third parties and involve them in shared cyber crisis assessments, preparations and simulations. Cyber-resilient CEOs outperform cyber laggards by 40% in their likelihood of implementing specific policies and controls for third parties.

2. Openly collaborate to contain cyberattack surprises

Foster transparent and collaborative environments to contain surprises and minimize the impact of cyberattacks. Begin with transparent procurement practices that prioritize cybersecurity as a shared value throughout the supply chain. Build strong relationships with internal stakeholders who possess cybersecurity expertise. Also participate in knowledge-sharing initiatives with industry peers and cross-industry partners. These initiatives facilitate the exchange of timely and actionable intelligence, including indicators of compromise and leading practices for identifying malicious actors to stay one step ahead of emerging threats. Around 86% of cyber-resilient CEOs recognize the value of engaging with cybersecurity service providers to gain sector-wide cybersecurity risk insights.

3. Proactively engage regulators and public-private partnerships (PPPs) to enhance cyber resilience

Collaboration between government entities and the private sector is crucial to address systemic cyber risks and safeguard the digital economy. Regulators continue to widen and deepen their approaches to cyber resilience in the face of ever-increasing breaches that impact consumers and critical infrastructure. CEOs should proactively engage regulators to encourage a risk-based approach to resilience and use trust- or data-based cloud adoption such as hybrid or sovereign cloud. Additionally, CEOs that are engaged in PPPs facilitate greater information sharing, technology development and joint efforts to combat cyber threats. To achieve this:

- **Foster collaboration**: Work within companies and through public-private partnerships to bolster cyber defense and resilience. Collaborate with governments and private sector entities to establish sector-specific cybersecurity frameworks and regulations.

Practical steps: Ecosystems

- **Join global alliances**: Engage in cross-border international collaborations, such as those between the United States and European Union, to effectively address cross-border cyber threats. Involvement in international forums, initiatives and agreements facilitates cooperation, sharing of leading practices, harmonization of cybersecurity standards and the establishment of responsible behavior norms in cyberspace. Also, promote collaboration and information sharing within and between countries to strengthen collective cyber defense capabilities.
- **Bilateral collaboration that is industry specific**: Publicly share timely and actionable intelligence, including indicators of compromise, tactics, techniques and leading practices for identifying known bad actors including continuous monitoring and threat intelligence.

4. Engage leaders in protecting the cyber-physical world

Organizations are expanding their global footprint by building new branches, manufacturing sites and delivery centers. With the increasing intersection between the physical and cyber worlds and expansive use of operational technology (OT), protect new operations from attacks that are seeking to disrupt operations directly or through new geographic-specific supply chains.

5. Address and recognize links and vulnerability exposure between environmental measures and cybersecurity resilience

Address and acknowledge the interconnection between the growing significance of environmental initiatives and cyber resilience. As organizations reduce their dependence on fossil fuels—for example, migrating toward a more distributed power grid via wind farms, rooftop solar and battery projects, each with connected control systems and more complex protocols—could expose new cybersecurity challenges. Many of these assets were not designed with cybersecurity in mind from the outset. It is essential to associate climate resilience and sustainability with cybersecurity resilience. Failure to do so could result in increased vulnerabilities. Cyber-resilient CEOs are 61% more likely to recognize the cybersecurity vulnerabilities that exist within environmental initiatives compared with cyber laggards.

Practical steps: Ecosystems

6. Evaluate cyber resilience beyond information security maturity

While it is important to assess the company's cyber maturity, simply reviewing the information security function's capabilities is insufficient to achieve cyber resilience. Rather, CEOs should understand and ensure these capabilities intersect with the overall resilience of the business. This means having a framework to evaluate and measure the pervasiveness and effectiveness of controls across critical functions of the business value chains, ensuring they can operate at scale and speed to support business reinvention and navigate disruptions. In many circumstances, businesses are not yet able to articulate what is most critical to them and where they feel they are most at risk. For resilience to work, there needs to be a clear alignment of strategy, risks and resource allocation between the business, technology and information security as well as third parties.

7. Excel at integrating cybersecurity and risk management

Integrate a cyber risk-based framework into the enterprise risk management program. Align cybersecurity operations and executive leadership to agree on the priority of assets and operations that should be protected. Consider cybersecurity risk to a great extent when evaluating overall enterprise risk. Cyber-resilient CEOs promote an enterprise-wide risk assessment approach (64% of cyber-resilient CEOs vs. 41% of cyber laggards) that cuts across business units and functions. This comprehensive view enables a more holistic understanding of vulnerabilities and strengthens the organization's ability to proactively defend against cyber threats.

For example, by choosing to integrate cybersecurity risk into its broader enterprise risk management framework, a global travel company was able to gain better risk management, improved compliance with regulatory requirements, enhanced protection for its business and its customers. What's more, cyber-resilient CEOs prioritize testing cyber operations across the entire organization. By conducting regular assessments to detect vulnerabilities, they minimize the element of surprise in cyberattacks. This proactive approach enables them to identify and address potential weaknesses, reducing the impact of cyber incidents. Seventy percent of cyber-resilient CEOs employ this practice, compared with only 36% of cyber laggards who do the same.

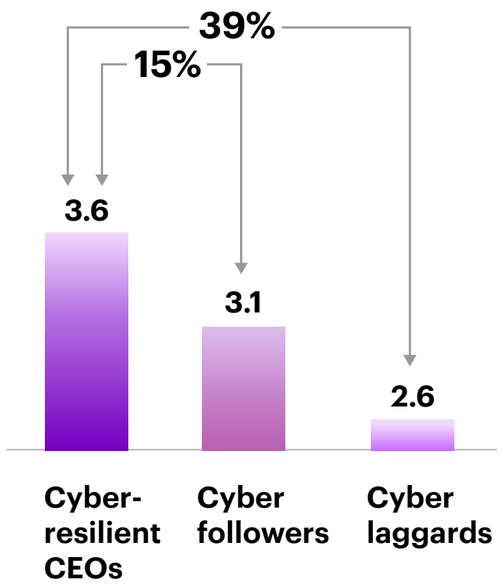
Embrace ongoing cyber resilience to stay ahead of the curve

Cyber-resilient CEOs are committed to implementing practices that foster a safe environment within their organizations and ecosystems.

They understand that cybersecurity is not a one-time initiative and recognize the need for ongoing efforts to fortify their defenses and adapt to stay ahead of the curve.

In the **continuous resilience** dimension of the CEO action index, cyber-resilient CEOs outperform cyber laggards by 39% and cyber followers by 15% (Figure 12).

Figure 12.
Cyber-resilient CEOs recognize cybersecurity as an ongoing effort



Source: 2023 Accenture cyber-resilient CEO survey (n=1,000)

Practical steps: Continuous Resilience

1. Redefine the risk profile

Commit to continually establishing industry-leading cybersecurity measures that take into account the changing risk landscape and align with business priorities. Cyber-resilient CEOs consistently enhance their cyber performance benchmarks to keep pace with the evolving threat landscape. By expanding their risk definitions and tolerance, 60% of cyber-resilient CEOs distinguish themselves by embracing this proactive approach, compared with only 34% of cyber laggards.

2. Seek independent reviews and continuous enhancement of security programs

Assess the organization's security program by seeking third-party reviews and implement enhancements to align with evolving threat landscape. Almost two-thirds of cyber-resilient CEOs embrace this practice, outperforming cyber laggards by a substantial margin of 27 percentage points.

3. Build cybersecurity blackout readinesss

Create and implement a comprehensive cyber crisis response playbook that encompasses key aspects such as executive decision making, internal and external communication protocols, collaboration with external legal counsel, law enforcement agencies and third-party cybersecurity incident response teams. The playbook ensures an effective response to severe scenarios, like widespread ransomware attacks, targeted assaults, or zero-day vulnerabilities. Furthermore, organizations should isolate critical application backups within a secure cyber vault, enabling them to restart operations while reconstructing production systems at the same time.

4. Champion AI and advanced ML for proactive threat protection

Direct your executives to seize the power of data, generative AI and advanced machine learning for proactive preparation, prediction and protection against cyber threats. Integration revolutionizes cyber resilience, enabling proactive threat detection, automated incident response, adaptive defenses, predictive analytics and enhanced security measures. All cyber-resilient CEOs plan to lead and direct their workforce in using data, generative AI and advanced machine learning to detect and protect themselves from cyberattacks before they happen, gaining competitive advantage.

Checklist for the cyber-resilient CEO

Strategy

- Establish a cyber protection strategy that is shaped to protect your strategic initiatives and corporate value.
- Cybersecurity should reduce organizations' risk and optimize capabilities and should be given the same level of importance as financial performance.

Talent and culture

- Require business leaders to implement cybersecurity in their respective departments and provide cybersecurity training among employees.
- Foster a culture of cyber-savviness at all levels.
- Conduct required trainings to upskill the team and, if needed, bring in managed security service providers.

Technology

- The digital core should be built with security by design, and it should have secure access.
- Customer data is key to building digital trust and it is important for organizations to secure it.

Ecosystems

- Understand and manage third-party risks to help reduce your exposure to attacks.
- Cyber risk assessment shouldn't be limited to specific departments or functions, it should be an enterprise-wide exercise.
- Conduct attack simulations to test your cyber resilience.
- Closely monitor your time to detect and time to contain threats.

Continuous resilience

- Use your contacts who have experienced a serious incident to help educate and prepare for potential attacks.
- Develop a collaborative relationship now for sharing threat intelligence and shaping national and international cybersecurity policies.
- Build industry-leading security benchmarks and use tech to predict threats before it happens.

About the research

We took a multi-method approach

The Accenture cyber-resilient CEO survey was conducted in June 2023 and involved 1,000 global CEO respondents from 15 countries across 19 industries. Respondents were asked questions to test their knowledge and understanding of cybersecurity and determine their cyber resilience, as well as their organization's approach to cybersecurity business practices. The respondents represent organizations with annual revenues of $1 billion* or more across North and South America, Europe, Asia Pacific and the Middle East.

1,000 CEO respondents

15 countries

Australia (68)
Brazil (67)
Canada (67)
France (67)
Germany (68)
Ireland (68)
Italy (65)
Japan (66)
Netherlands (66)
Norway (66)
Saudi Arabia (63)
Spain (67)
United Arab Emirates (64)
United Kingdom (67)
United States (71)

$1B+ revenues

19 industries

Aerospace (55)
Automotive (52)
Banking (53)
Capital Markets (53)
Chemicals (53)
Consumer Goods & Services (53)
Energy – Oil and Gas (54)
Healthcare Payers (52)
Healthcare Providers (52)
High Tech (52)
Industrial (53)
Insurance (53)
Life Sciences (51)
Public Service (47)
Retail (54)
Software & Platforms (54)
Telecommunications (52)
Travel (54)
Utilities (53)

*<1% of sample have revenues between $500 million and $1 billion to fill the survey quota

Cyber-resilient CEO action index

We identified five leading action themes from a study of 25 cybersecurity-related CEO practices. These action themes can help organizations assess and redefine their strategies to lay the foundation for world-class cybersecurity resilience.

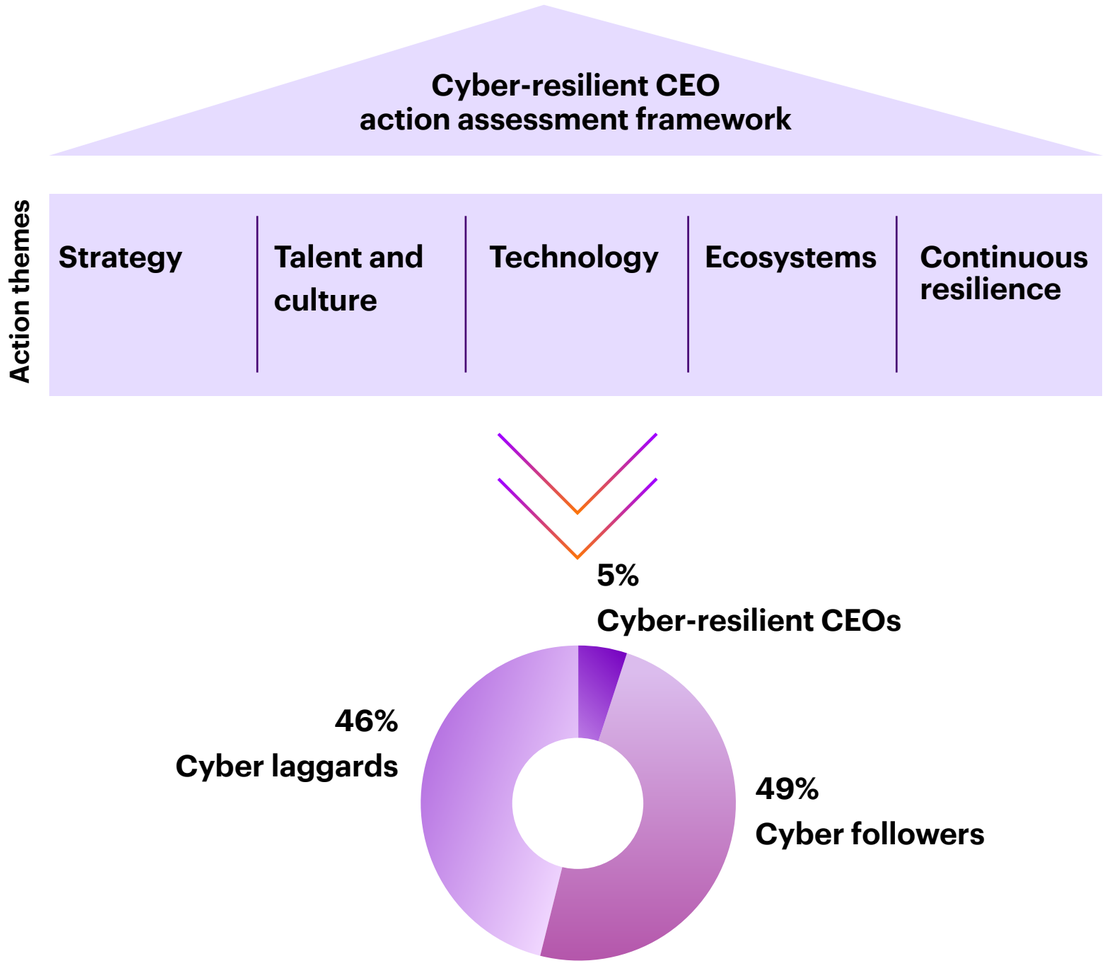
How we did it

To identify the top 25 cybersecurity practices of cyber resilient organizations, we undertook extensive discovery work, reviewing empirical literature on cybersecurity, obtaining input from internal and external subject-matter experts on the topic, and drawing on our own experience in working with high performing organizations. We then grouped the 25 practices into five action themes and developed a diagnostic asset, the cyber-resilient CEO action index. This Index benchmarks and computes a company's security action adoption score. We define an index as a measure of performance of companies along a continuum. The continuum used in this study was based on one to five points. The index is used to benchmark companies to understand how they rate relative to one another on this continuum. To determine the scoring mechanism—each question response was given a "scoring" that contributes to the index.

To validate the index, we studied and statistically tested the adoption of the 25 practices across the five action themes with 1,000 CEOs of large companies globally.

As a result, we identified three CEO archetypes:

- **Cyber-resilient CEOs**: Making up just 5% of our 1,000 sample, these companies scored one standard deviation above the mean score on the index and have adopted at least 60% or more of the actions.
- **Cyber followers** :These companies scored one standard deviation above the mean score on the index but have adopted less than 60% of the five actions. They make up 49% of our sample.
- **Cyber laggards**: The 46% of our sample that did not score one standard deviation above the mean on the index across any of the actions.



Accenture Global Disruption Index

We created an overall measure of disruption to assess the level of volatility and change in the external business environment. The index is based on the average of six sub-components, that cover the economic, social, geopolitical, environmental, consumer and technological spheres. Each of the sub-components is based on a set of indexed scores for a range of indicators. The economic component is based on economic risk ratings, Volatility Index (VIX), Gross Domestic Product (GDP) volatility and inflation volatility. Geopolitics is based on the risk of geopolitical instability. The social component reflects social unrest and non-participation in the labor market. The environmental component reflects the frequency of climate-related disasters and climate-driven risk. The consumer component reflects pessimism at a global level, based on the inverse of the OECD's Consumer Confidence Index. Finally, the technological component is based on an index comprised of 24 indicators, which use the presence of disruptors and performance of incumbents as proxies for the level of disruptive innovation in industries.

Data-science analysis of investor communications

We used prompt engineering and GPT3.5 to analyze the earning call transcripts of the world's largest 2,000 companies between 2017 and 2022. We analyzed the CEO comments to check the frequency of mentions of keywords related to cyber risk, cybersecurity, and cyber strategy. This exercise helped us to understand the growing awareness of cybersecurity among CEOs.

360° cyber awareness scores

We used our survey to assess and score how well CEOs perceive and associate cybersecurity with the following parameters:

- **Sustainability**: Did CEOs develop a broader perspective of sustainability initiatives where they see cybersecurity as a core part of their environmental goals?
- **Talent**: How well did CEOs recognize the importance of addressing the talent gap in cybersecurity?
- **Technology innovation**: Did CEOs adopt and implement emerging technology securely?
- **Customer trust**: Did CEOs understand that a cyberattack would have a negative impact on their customer trust and could result in customer attrition?

Finally, we supplemented our study with case study analysis as well as literature reviews and additional secondary research across various sources.

References

1 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, November 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2 Global cybersecurity spending to top $219B this year: IDC, Cybersecurity Dive, March 2023, https://www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/#:~:text=Global%20security%20spending%20will%20reach,an%20IDC%20forecast%20released%20Thursday

3 Accenture, Total Enterprise Reinvention, 2023, https://www.accenture.com/us-en/insights/consulting/total-enterprise-reinvention

4 World Economic Forum and Accenture, Global Cybersecurity Outlook 2023, https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

5 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, November 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

6 NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs, ZDNet, January 26, 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

7 Accenture NLP Transcript Analysis of Top 2000 global companies, 2017 to 2022

8 Colonial Pipeline CEO acknowledges paying hackers to restore pipeline, Reuters, June 7, 2021, https://www.reuters.com/business/energy/colonial-pipeline-ceo-paid-ransom-swiftly-restart-pipeline-testimony-2021-06-07/

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth, and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 733,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise, and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners, and communities.

Visit us at **www.accenture.com**

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity.

For more information, visit **www.accenture.com/research**