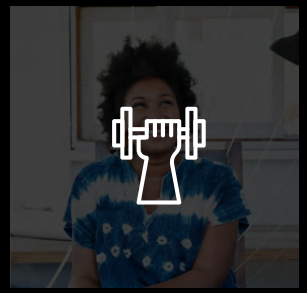
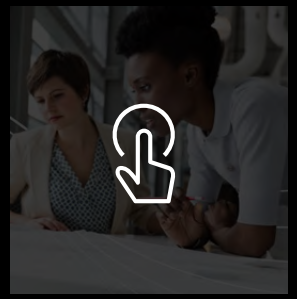
How cybersecurity boosts enterprise reinvention to drive business resilience

State of Cybersecurity Resilience 2023

Contents

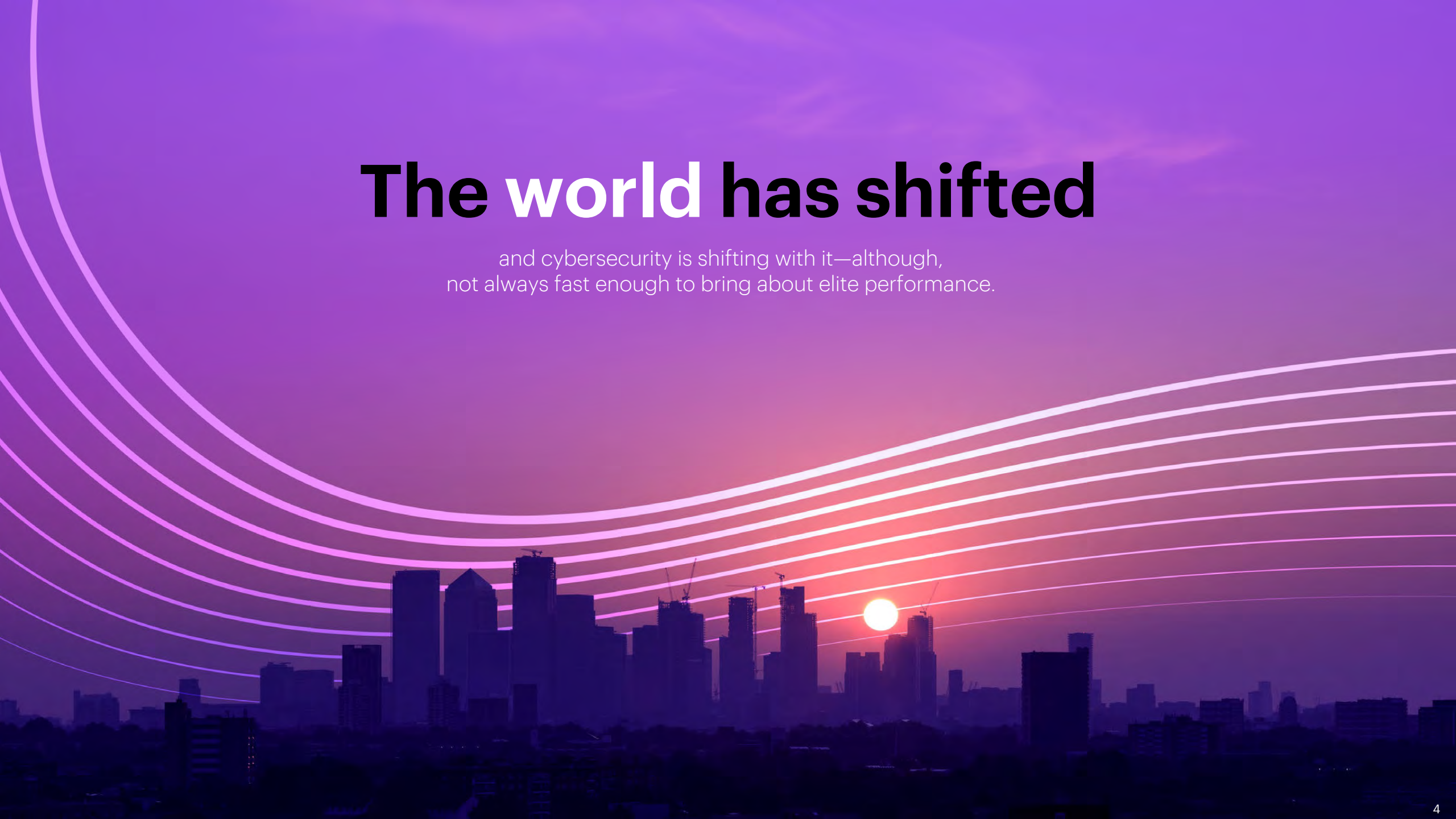




Securing transformation success

The world has shifted

and cybersecurity is shifting with it—although,
not always fast enough to bring about elite performance.



Securing transformation success

Market disruption—fueled by technological change, complex regulations, geopolitical tensions and economic uncertainties—is testing global organizations' approach to risk and resilience.

As our Total Enterprise Reinvention research shows, most large organizations are transforming faster and more frequently.

Our latest cybersecurity research reveals some organizations are using cybersecurity as a differentiator to deliver better business outcomes. Those organizations that closely align their cybersecurity programs to business objectives are 18% more likely to increase their ability to drive revenue growth, increase market share and improve customer satisfaction, trust and employee productivity.

What's more, organizations that embed key cybersecurity actions into their digital transformation efforts and apply strong cybersecurity operational practices across the organization are nearly six times more likely to experience more effective digital transformations than those that don't do both.

Yet, some organizations aren't engaging cybersecurity early enough to accelerate transformation and meet future challenges and opportunities.

We found that, when it comes to embedding security controls, 18% of our survey respondents still deploy them *after* they've finalized a transformation effort—and that's only if vulnerabilities are detected.

It could be a case of too little, too late. As 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.[1]

The next wave of business transformation will morph from managing isolated digital capabilities to creating the foundations of a shared reality. It will converge the physical lives we've been leading with the digital ones we've been rapidly expanding. In such an environment, organizations should embed cybersecurity each step of the way to better manage these high stakes.

Securing transformation success

By converting cybersecurity from an incident-driven reaction into part of the fabric of transformation efforts, organizations can not only boost cybersecurity resilience, but also position themselves to reinvent the whole enterprise and set a new performance frontier, safely.

Cybersecurity as a changemaker

Cybersecurity as a changemaker

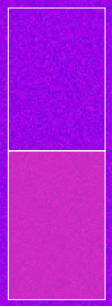
Our annual State of Cybersecurity Resilience research involved **3,000** global respondents from **15** industries across **14** countries.

Survey responses show that more than one-half of organizations are beginning to recognize the importance of being secure from the start in any transformation effort.

53%

said that cybersecurity is **part of the core transformation team**

&



53%

said that cybersecurity is **required before any solution is deployed**

Source: Accenture State of Cybersecurity Resilience 2023; N = 3,000 security executives and business leaders

Cybersecurity as a changemaker

We discovered that the majority of organizations undergoing digital transformation, in our sample, increase their chances of being fully satisfied with the level of cybersecurity embedded in their digital transformation efforts by **10%** if they follow three actions.

Three cybersecurity actions to boost transformation:

1.

Require cybersecurity controls before all new solutions are deployed

2.

Apply cybersecurity incrementally as each digital transformation milestone is achieved

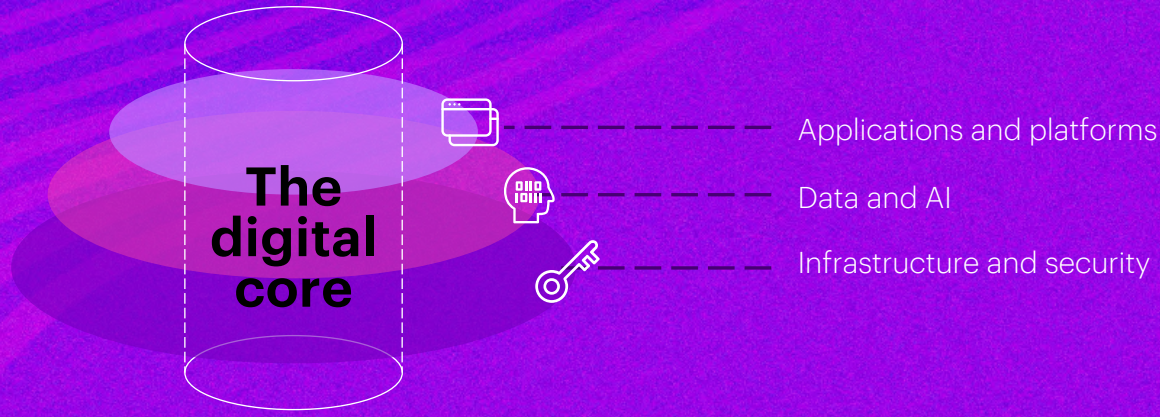
3.

Assign a cybersecurity representative to the core transformation team and a point person to orchestrate cybersecurity across all transformation initiatives

Cybersecurity as a changemaker

Our recently released Resilience for Reinvention study[2] shows that companies achieving long-term profitable growth display a commitment toward developing a digital core, which consists of three layers: infrastructure and security; data and artificial intelligence (AI); and applications and platforms.

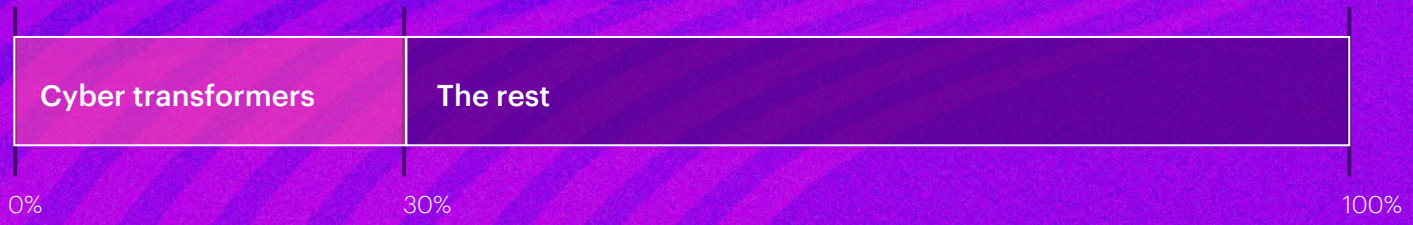
They also demonstrate a consistently higher share of investments in new technologies, innovation and cybersecurity.



Cybersecurity as a changemaker

In this latest State of Cybersecurity Resilience research, we find that some organizations—representing **30%** of respondents—are already proving how prioritizing cybersecurity makes a difference. These organizations—we call them cyber transformers—have accelerated digital transformation efforts and plan to continue accelerating them as their high-performing cybersecurity actions propel them forward (Figure 1).

Figure 1. Cyber transformers accelerate digital transformation



Cybersecurity as a changemaker

And like the cyber champions in our 2021 report, this year's cyber transformers strike a balance between excelling at cyber resilience and aligning with the business strategy to achieve better business outcomes.

Cybersecurity as a changemaker

Cyber transformers closely align cybersecurity programs to business objectives. In doing so, they are **18%** more likely to increase the following outcomes:

- Their ability to achieve target revenue growth and market share
- Improved customer satisfaction and trust
- Greater employee productivity

Additionally, cyber transformers are **nearly twice as good** as the rest at involving the cybersecurity team from the start of business planning. And they are far more comfortable with their organization's internal cybersecurity planning.

73%

of cyber transformers involve the cybersecurity team from the start of business planning

vs.

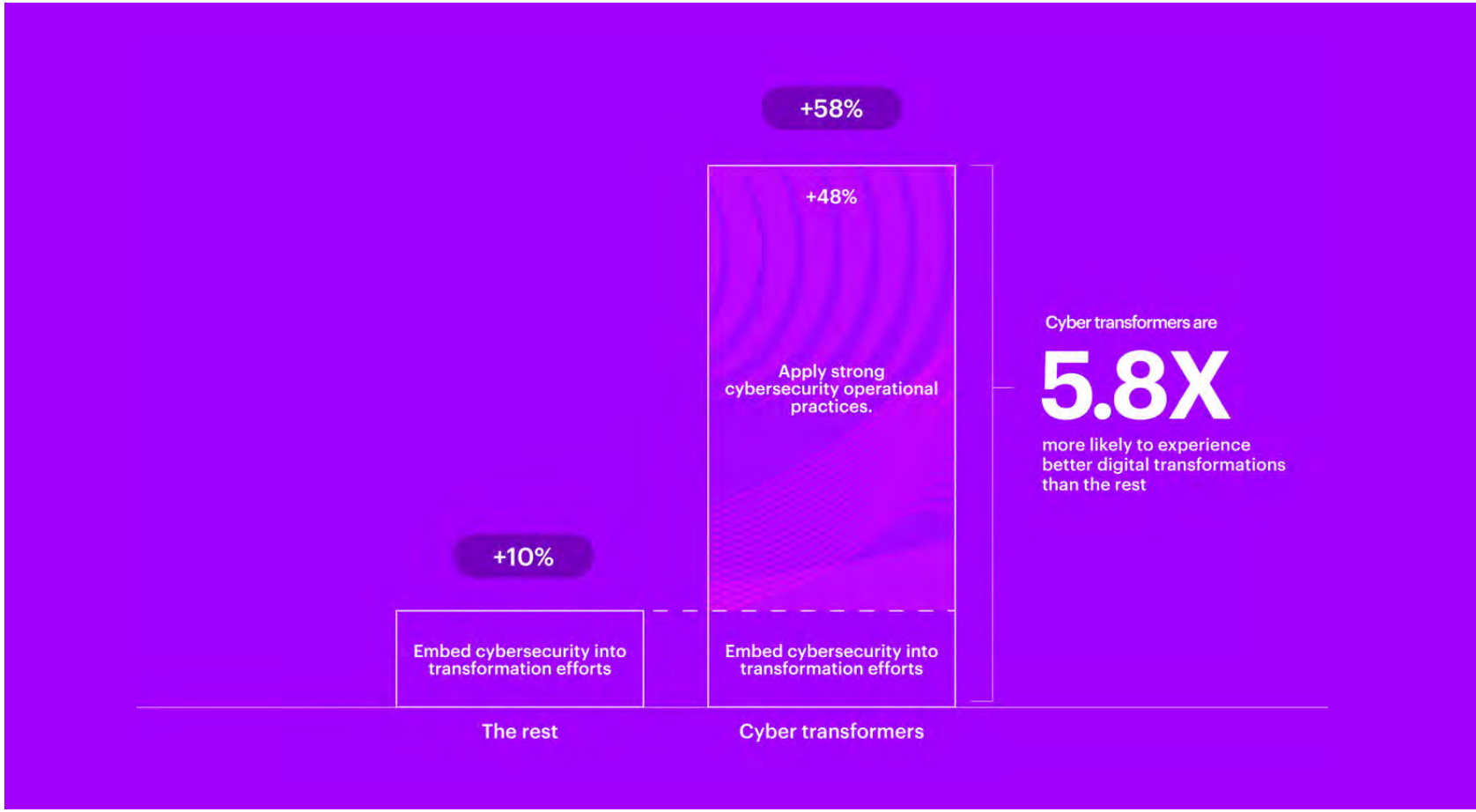
37%

of the rest involve the cybersecurity team from the start of business planning

Cyber transformers build transformation foundations in two ways

They not only embed three key cybersecurity actions into their transformation efforts, but also establish a better foundation by applying strong cybersecurity operational practices from the start. As a result, they are **5.8X** more likely to experience more effective digital transformations than the rest (Figure 2).

Figure 2. Cyber transformers build transformation foundations in two ways



Source: Accenture Research logistic regression analysis of State of Cybersecurity Resilience 2023 data; estimated probability premium from applying cybersecurity best practices when conducting digital transformation. N = 2,500 security executives.

Cybersecurity as a changemaker

Cyber transformers outperform the rest using strong cybersecurity operational practices.

Excel at integrating cybersecurity and risk management

Leverage cybersecurity as-a-service more frequently to enhance security operations

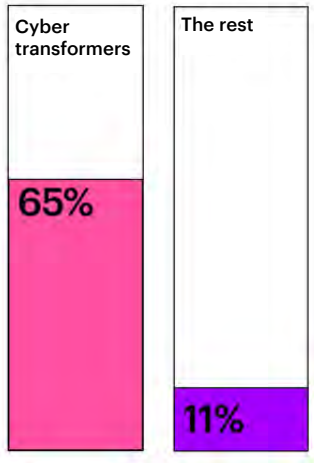
More committed to protecting their ecosystems from external attacks

Rely more heavily on automation

What it takes to be a cyber transformer

What it takes to be a cyber transformer

There are several factors that illustrate the differences between cyber transformers and the rest.



Source: Accenture State of Cybersecurity Resilience 2023; N = 2,500 security executives

65% of cyber transformers apply three leading practices to excel at risk management. By contrast, just **11%** of the rest adopt this "best-in-class" approach.

1. **Integrate cyber risk:** A cyber risk-based framework is completely integrated into their enterprise risk management program
2. **Agree on priorities:** Their cybersecurity operations and executive leadership consistently agree on the priority of assets and operations to protect
3. **Look at risk holistically:** They consider cybersecurity risk to a great extent when evaluating overall enterprise risk

Case study

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 and enhanced protection for its business and its customers.

This industry-leading and comprehensive approach to enterprise risk management enabled the company to gain a deeper, holistic understanding of the security risks associated with third-party vendors and IT systems, as well as better preparedness and recovery planning in the event of a breach.

Cyber transformers more frequently use cybersecurity-as-a-service to enhance operations.

40% of cyber transformers use third parties or managed services providers to administer cybersecurity operations and address talent shortages, versus **24%** of the rest.

Case study

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 focused security team by expanding into a cybersecurity-as-a-service model, initially running the company's security operations, such as threat intelligence and establishing a Security Operations Center (SOC).

Today, Accenture provides a range of services including data protection, identity management, network security, vulnerability management, security awareness and risk management.

Improving its cybersecurity operations enabled the company to innovate continuously, run its store operations without disruption and maintain consumer trust. The retailer gained improved cyber resilience and business outcomes by being secure from the start.

What it takes to be a cyber transformer

Cyber transformers are more committed to protecting their ecosystem.

Based on our analysis, cyber transformers performed better than the rest when it comes to taking action to protect their ecosystems.

For example, cyber transformers more often incorporate their ecosystem or supply chain partners into their incident response plan **(45% vs. 37%)** and also require them to meet strict cybersecurity standards **(41% vs. 29%)**. While these ecosystem actions provide cyber transformers with a 10% advantage over the rest, there is room for improvement.

Case study

A leading pharmaceutical company collaborated with Amazon Web Services (AWS) to accelerate drug development, increase operational agility, reduce technology costs and develop the workforce of the future.

To create a more scalable, reliable and secure architecture, the company moved 80% of its applications to the cloud, removing non-differentiating technology, reducing its internal data center footprint, decreasing capital expenditures and improving resilience.

Customers, employees and partners can benefit from the company's ability to respond with greater speed, agility and insights across the value chain which, in turn, improves patient experiences.

Accelerating the delivery of data services and capabilities can help the company increase secure connectivity and collaboration with the Life Sciences ecosystem and external partners.

Cyber transformers rely heavily on automation.

89% of cyber transformers rely heavily on automation, compared with just **57%** of the rest.

What's more, **96%** of respondents whose organizations substantially automate their cybersecurity programs recognize that automation helps them alleviate cyber talent shortages, a key challenge for any company seeking cyber resilience. As evidence of a man+machine approach becoming more mainstream, Accenture analysis has found that the share of cybersecurity-related AI patents increased **2.7X** between January 2017 and October 2022.

Case study

In our own organization of 738,000 employees, we've embraced AI and automation through our Intelligent Application Security Platform. The platform uses leading commercial scanning tools to perform application security testing at scale and to discover vulnerabilities and code issues. It also automates, orchestrates and scales onboarding applications as well as application testing and pipeline gating.

The platform uses an artificial intelligence-powered filter that removes and reduces vulnerabilities—from several thousand to a few—resulting in a curated and more manageable process.

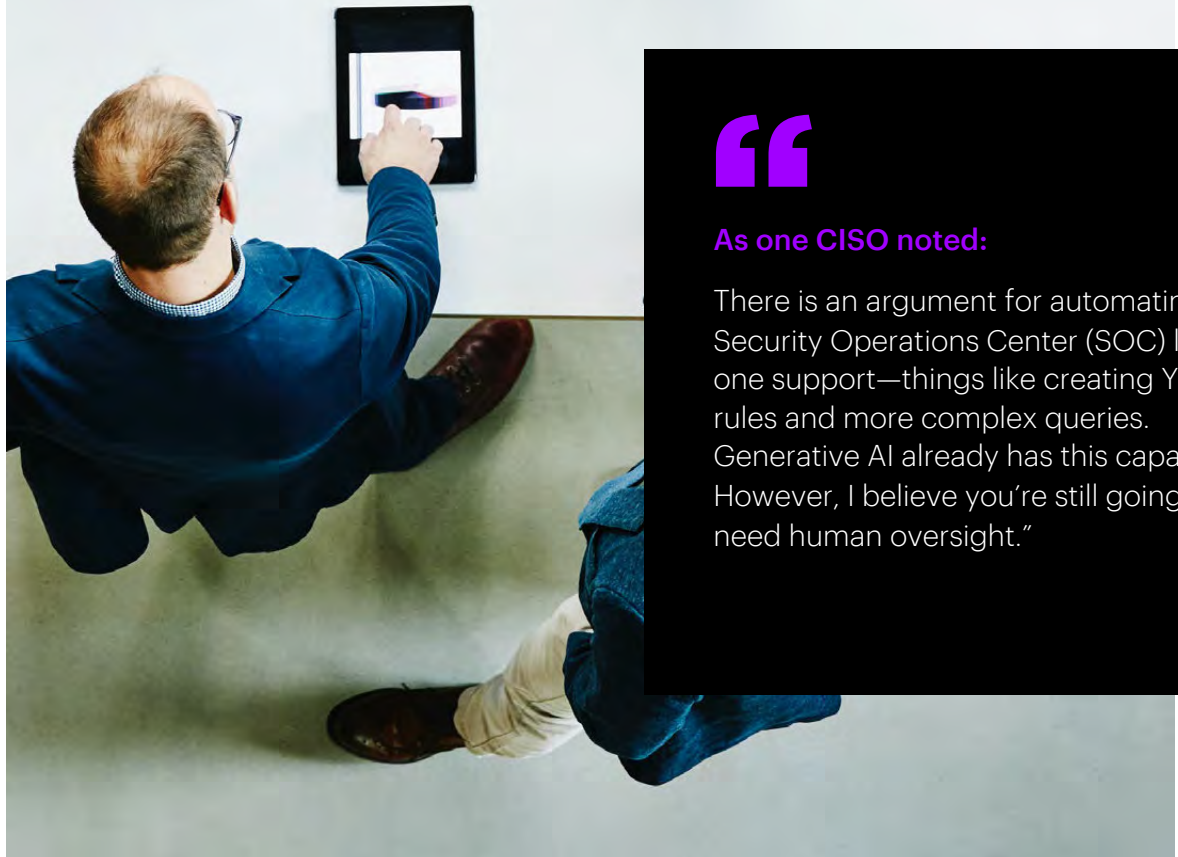
As a result, the scanning service has helped application teams save thousands of hours through the automated removal of false positive findings generated by scanning tools.

What it takes to be a cyber transformer

Fast-emerging AI developments such as generative AI can drive a new wave of cybersecurity advances.

In time, generative AI could support enterprise governance and information security, protecting against fraud, improving regulatory compliance, and proactively identifying risk by drawing cross-domain connections and inferences both within and outside the organization.[3]

Indeed, the emergence of ChatGPT has already brought both disruption and opportunity, offering the rapid advancement of cybersecurity capabilities such as threat detection, analysis and response and accelerated use of automation to reduce workload and augment staffing.



As one CISO noted:

There is an argument for automating Security Operations Center (SOC) level-one support—things like creating Yara rules and more complex queries. Generative AI already has this capability. However, I believe you're still going to need human oversight."

What it takes to be a cyber transformer

As our research shows, Total Enterprise Reinvention is a deliberate strategy that aims to set a new performance frontier for companies and in most cases, the industries in which they operate.

Cyber transformers are well placed to execute that reinvention strategy through gains that are a direct result of differentiated cybersecurity practices and behaviors.

And while cybersecurity incidents will still happen every day, on average, cyber transformers report **26%** lower cost of breaches and cybersecurity incidents in the past 12 months than the rest—that's more than a quarter of all costs that could be allocated across the enterprise to optimize operations, fuel growth and improve resilience.

Case study

A large retail and commercial bank introduced agile cybersecurity decision making while undertaking two digital transformations: moving to a private cloud and creating new product offerings using the public cloud.

The bank's decentralized operating model, coupled with embedding cybersecurity early in the digital transformation process, has helped 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.

Extra pressure points

Extra pressure points

While managing secure digital transformation is an important consideration, our research shows there are other ongoing issues that continue to put pressure on all organizations and influence the state of cybersecurity resilience. Looking across our entire set of global respondents, these additional pressure points were revealed.

An uncertain geopolitical landscape is accelerating threats and attacks

Organizations' cyber resilience is under pressure from ongoing geopolitical tensions, especially through their supply chains, physical infrastructure and external networks.

The whole approach to cyber risk is under scrutiny, inside and outside

Organizations are failing to keep pace with the scope and scale of cyber risk.

There's still room for improvement in cybersecurity and business alignment

Organizations are better aligning cybersecurity with business leadership, but there are gaps in the effectiveness of their approach.

Extra pressure points

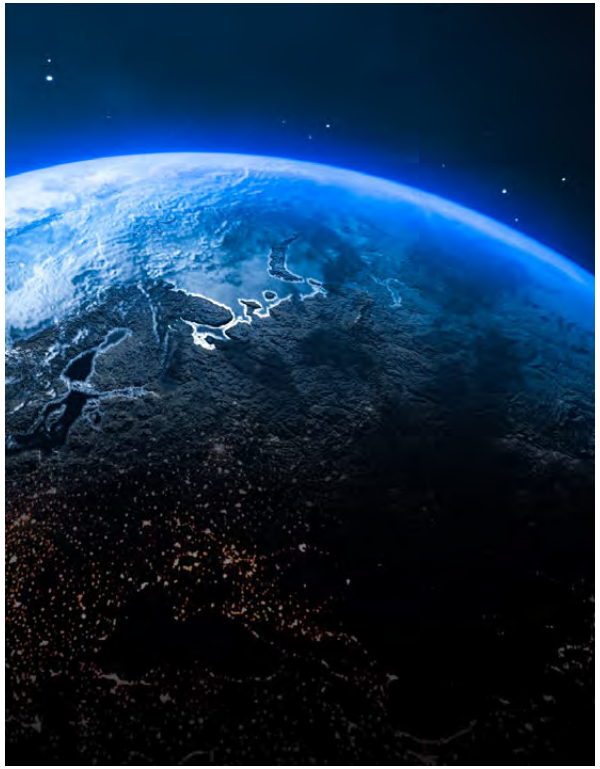
An uncertain geopolitical landscape is accelerating threats and attacks

Organizations' cyber resilience is under pressure from ongoing geopolitical tensions, especially through their supply chains, physical infrastructure and external networks, such as investment partners.

The influence of Russia's aggression in the Ukraine is being felt by almost everyone. Nearly all organizations **(97%)** have seen an increase in cyber threats since the start of the Russia-Ukraine war and almost all survey respondents have taken some action.

51% of organizations have updated their business continuity and enterprise risk plans and nearly half have increased their incident response capabilities. At the same time, only **39%** of organizations are prioritizing close collaboration with government agencies on policies and recommendations in response to the war. More than half **(54%)** see third parties and external networks as the most susceptible areas for attack.

Indeed, consistent with last year's findings, the percentage of successful breaches from outside the organization remains high, even nudging slightly ahead (**61%** compared to **60%** last year), while for some industries, such as Utilities, supply chain partner threats are higher again at **62%**.



Extra pressure points

The whole approach to cyber risk is under scrutiny, inside and outside

Organizations are failing to keep pace with the scope and scale of cyber risk.

Cyber risk management is challenging inside the organization. Less than half of all survey respondents said that just one aspect of enterprise risk management—their cyber risk-based framework—is completely integrated within the enterprise risk management program.

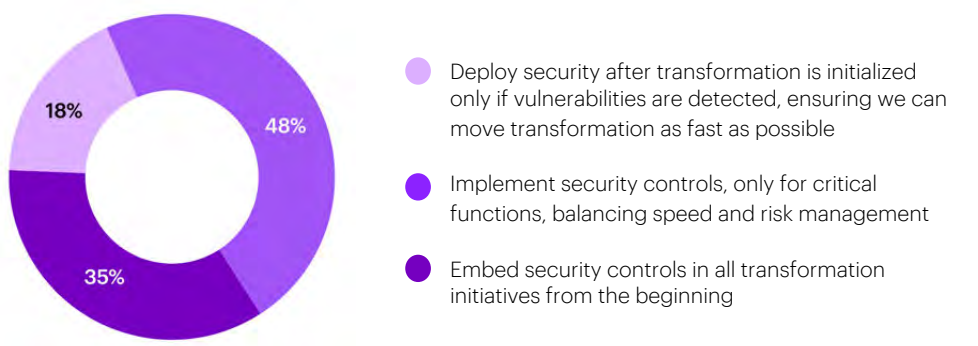
The regulatory landscape plays a part here, with risk integration leaping to **81%** in the highly regulated Banking industry or **65%** for the Software and Platforms sector.

And accelerating transformation without addressing security along the way can open the door to greater risk.

While **35%** of respondents said they embed security controls in all transformation initiatives from the beginning, there are still **18%** who deploy security after the event. To transform at speed, security should be baked in, otherwise organizations can expect to incur more cost or rework down the line (Figure 3).

Cyber risk is also mounting outside the organization, where cyber threats are increasing due to changes in the threat landscape and cybersecurity omissions leave organizations exposed.

Figure 3. The security of digital transformation efforts



Source: Accenture State of Cybersecurity Resilience 2023
N = 2,500 security executives and 500 business leaders

For example, Russia's invasion of Ukraine spurred reaction from executives to address cybersecurity practices, such as updates to business continuity, incident response and increasing employee cyber awareness.

Indeed, only one-third of all respondents **(35%)** consider cybersecurity risk "to a great extent" when evaluating overall enterprise risk; this highlights there is still some way to go to make cybersecurity a proactive, strategic necessity within the business.

Extra pressure points

There's still room for improvement in cybersecurity and business alignment

Organizations are better at aligning cybersecurity with business leadership, but there are gaps in the effectiveness of the approach.

Business leaders (CEO and CFO respondents in the research) expect CISOs to go beyond their traditional technical role to act as a representative of the organization. Business leaders reported the importance of CISOs adopting certain characteristics, such as translating the technical aspects of cybersecurity to the CEO and Board **(44%)**, leading the response during breaches **(42%)** and establishing trust with customers **(41%).**

As one CISO reported:

"The biggest hurdle security leaders have is executive presence. You need to demonstrate business capability and value and engage in conversations that are about more than just security."

These findings underscore the importance of having a business-led CISO who acts as an educator and collaborator with non-security audiences.

In particular, there's a gap between CISOs and business leaders when it comes to a post-breach communication strategy to the general public. And yet, as every organization who has experienced an attack knows, in the middle of a crisis, it's critical to provide quick, transparent communications to inform and reassure stakeholders.

Nearly half of CISOs said that no defined executive was responsible for communicating externally during a breach.

Extra pressure points

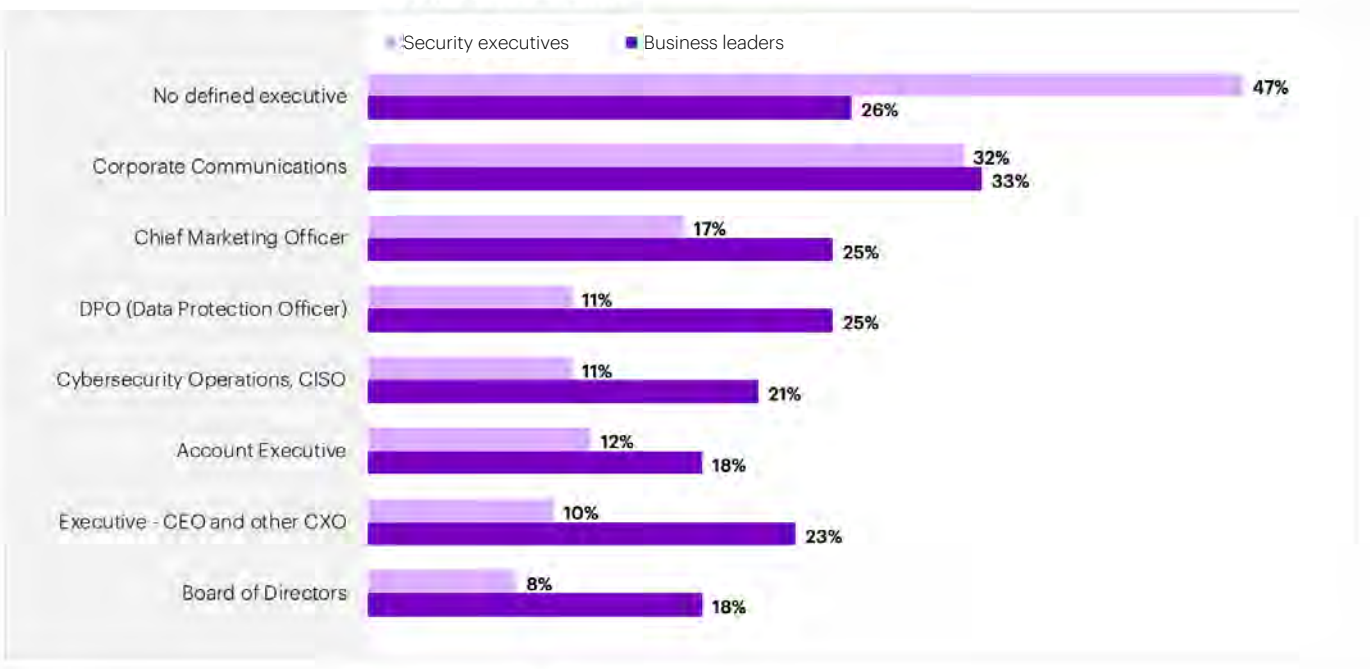
There’s still room for improvement in cybersecurity and business alignment

In addition, the differences in opinion between CISOs and business leaders about this responsibility may indicate a lack of clarity for post-breach communication (Figure 4).

This is a red flag for the whole enterprise as it attempts to limit the damage of a breach to its brand and customer satisfaction scores, identified as the most important consideration following a breach by **50%** of our survey respondents.

Organizations have a responsibility to define a crisis communications strategy that is agile, that considers the complexities of cyber events and that clearly defines roles and responsibilities for communicating with stakeholders.

Figure 4. Communication responsibilities during a breach



Source: Accenture State of Cybersecurity Resilience 2023. N = 2,500 security executives and 500 business leaders

Where next?

Where next?

Realistically, if you're not looking at cybersecurity holistically, you're not fully protecting your business

Where next?

Here's how you can employ cybersecurity to drive better results

Embed cybersecurity to protect the digital core

Security is critical to enabling business agility and scalability as well as driving continued innovation and establishing an organization's digital core—one that empowers employees and departments to experiment and scale while mitigating risk.

What you can do Take the three cybersecurity actions and establish a strong foundation with cybersecurity operational practices to improve business outcomes and overall performance.

Apply cybersecurity to reconcile digital and physical worlds

Increased access, devices, software and connectivity across the Cloud Continuum and legacy environments has resulted in an ever-expanding threat surface. And while generative AI[4] can herald a new era of agility and cyber protection, it also acts as a new threat vector for cyber criminals.

What you can do

Invest in understanding your data, its value and who has access. Re-examine enterprise and customer identity to better bridge the physical and digital worlds. Establish enhanced monitoring and visibility across both legacy and cloud environments using endpoint detection and response (EDR) and security orchestration, automation and response (SOAR) technologies.

Make cybersecurity part of the fabric of transformation

The traditional approach to cybersecurity is unsustainable. A global shortage of cybersecurity talent to handle ongoing threats is compounded by fewer people available to handle the effects of cyberattacks on an organization's business continuity, economics and reputation. The lines are becoming blurred around when transformation begins and ends.

What you can do

Make cybersecurity a cornerstone of your transformation efforts and elevate the CISO reporting so that the function is fundamental to business transformation efforts.

Where next?

From risk assessment and management to security control implementation, and from security awareness and training to incident response and recovery, cybersecurity is essential to maintain dynamic protection in every transformation program. What's more, as our cyber transformers show, business leaders have an opportunity to make cybersecurity's impact extend beyond protecting the business in the here and now, to actively influence continuous, dynamic reinvention.

About the research

Demographics

Our State of Cybersecurity Resilience 2023 research involved 3,000 global respondents from 15 industries across 14 countries. We wanted to understand the role of cybersecurity in organizations' approach to transformation and the broader cybersecurity practices that facilitate secure digital transformation. The respondents represent organizations with annual revenues of $1 billion or more across North and South America, Europe and Asia Pacific.

3,000

Total Respondents

2,500 Security executives
500 Business leaders (CEO, CFO)

US $1B+

Revenues

14

Countries

Australia (234)
Brazil (100)
Canada (115)
France (201)
Germany (223)
Ireland (102)
Italy (200)
Japan (221)
Netherlands (101)
Norway (100)
Saudi Arabia (55)
Spain (100)
United Kingdom (360)
United States (888)

15

Industries

Banking (265)
Capital Markets (177)
Chemicals (186)
Consumer Goods & Services (288)
Energy – Oil and Gas (277)
Healthcare Payers (102)
Healthcare Providers (130)
High Tech (209)
Insurance (209)
Life Sciences (199)
US Federal Services (100)
Retail (259)
Software & Platforms (135)
Telecommunications (202)
Utilities (262)

Methodology

Survey data analysis

We used standard survey data analysis to understand the overall landscape as well as characteristics of various groups in our sample; in particular we compared cyber transformers who made up 30% of the security executives in the sample (741 respondents) and the rest of the security executives (1,759 respondents). We defined cyber transformers as organizations that have accelerated digital transformation efforts and plan to continue accelerating them over the next two years.

Composite indicators

We constructed two independent indexes to capture how advanced companies are in more complex areas.

1. **Ecosystem protection index.** Incorporates our survey data and is based on the number of positive answers to questions on ecosystem protection actions that an organization is taking. Equal weighting was applied. The index is distributed on a scale 0-100.

2. **Alignment and governance index.** Using last year's definition of alignment, we applied this year's survey data to construct the index. The index is based on answers to questions on how organizations align their security to business objectives and what governance practices they apply. Equal weighting was applied. The index is distributed on a scale 0-100 and was part of the metric used in our logistic regression analysis.

Logistic regression econometric algorithm

To estimate the relationship between the probability of a successful outcome and organizations' practices, we applied a logistic regression approach. Both models were controlled with respect to the organizations' size, geographic location and the industry where they operate:

1. **Business outcomes analysis**—we analyzed the relationship between the level of business alignment and governance, measured with the alignment and governance index, and the probability that a company positively impacts with cybersecurity in all of the following outcomes:
   - Increased ability to achieve target revenue growth
   - Increase in market share
   - Increase in customer satisfaction and trust
   - Increase in employee productivity.

2. **Secure transformation efforts analysis**—we looked at the probability of being highly satisfied with secure transformation efforts. We tested the relationship with secure transformation key practices for selected cohorts in the survey sample.

NLP and trend analysis of publicly available data

We used LexisNexis patents data in our Natural Language Processing (NLP) approach to select patents related to cybersecurity, including AI. Using publication data between January 2017 and October 2022, we ran trend analysis to understand the evolution of AI-related patents' share in the overall number of cybersecurity-focused patents.

Glossary

Compressed transformation is transforming multiple parts of the business at the same time or executing a single large transformation much faster than ever before.

Digital core is fundamental to all other strategic needs of an enterprise. Amplifying the role of technology in reinvention means shifting from a technology landscape of static, standalone parts to interoperable pieces intentionally integrated and leveraging the cloud. The digital core consists of three layers: an infrastructure and security layer; a data and AI layer; an applications and platforms layer. Building a strong digital core is not a one-time project. It must be continuous to incorporate new technologies and business capabilities.

Total Enterprise Reinvention is a deliberate strategy that aims to set a new performance frontier for companies and in most cases, the industries in which they operate. Centered around a strong digital core, it helps drive growth and optimize operations. It requires a strategy for continuous, dynamic reinvention. It becomes a unifying force, across the C-suite and every function and business area, because, by definition, all are involved and accountable for its success. It demands an outside-in perspective that connects what's happening at the organization with what's happening in the world. And it requires new skills and an increased depth of understanding of technology, change management, communication and how to work with partners to achieve results faster (Figure 5).

Figure 5. The six differentiating characteristics of Total Enterprise Reinvention

1. **Reinvention is the strategy.** It is no longer an execution lever.
2. **The digital core becomes a primary source of competitive advantage.** It leverages the power of cloud, data, and AI through an interoperable set of systems across the enterprise that allows for rapid development of new capabilities.
3. **Reinvention goes beyond benchmarks, embracing the art of the possible.** Technology and new ways of working create a new performance frontier.
4. **Talent strategy and people impact are central to reinvention,** not an afterthought. These companies consider change management a core competency.
5. **Reinvention is boundaryless and breaks down organizational silos.** It tackles capabilities end-to-end.
6. **Reinvention is continuous.** It is no longer a time-defined one-off, but a capability continuously tapped by the organization.

References

1	Dig8ital	Link
2	Reinventing for resilience, Accenture 2023	Link
3	A new era of generative AI for everyone, Accenture 2023	Link
4	Ibid	Link

About the authors

Paolo Dal Cin
Lead
Accenture Security

Jacky Fox
Senior Managing Director
Accenture Security
Europe Lead

Harpreet Sidhu
Senior Managing Director
Accenture Security
North America Lead

James Nunn-Price
Senior Managing Director
Accenture Security
Growth Markets Lead

Acknowledgements
The authors would like to recognize Sarah Bird, Edward Blomquist, Katarzyna Furdzik, Corbin Lazier, Anna Marszalik, Eileen Moynihan, Juan Pablo Romero and Ann Vander Hijde for their contributions to this report.

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 738,000 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 Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including strategy, protection, resilience and industry-specific cyber services. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Cyber Fusion Centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.

Visit us at www.accenture.com/security

About Accenture Research

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 250 researchers and analysts spans 23 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Singularity—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.

Visit us at www.accenture.com/research