



How cybersecurity boosts enterprise reinvention to drive business resilience

State of Cybersecurity Resilience 2023



Contents



**Securing
transformation
success**

Page 3



**Cybersecurity as
a changemaker**

Page 7



**What it takes to
be a cyber
transformer**

Page 16



**Extra pressure
points**

Page 23



Where next?

Page 29



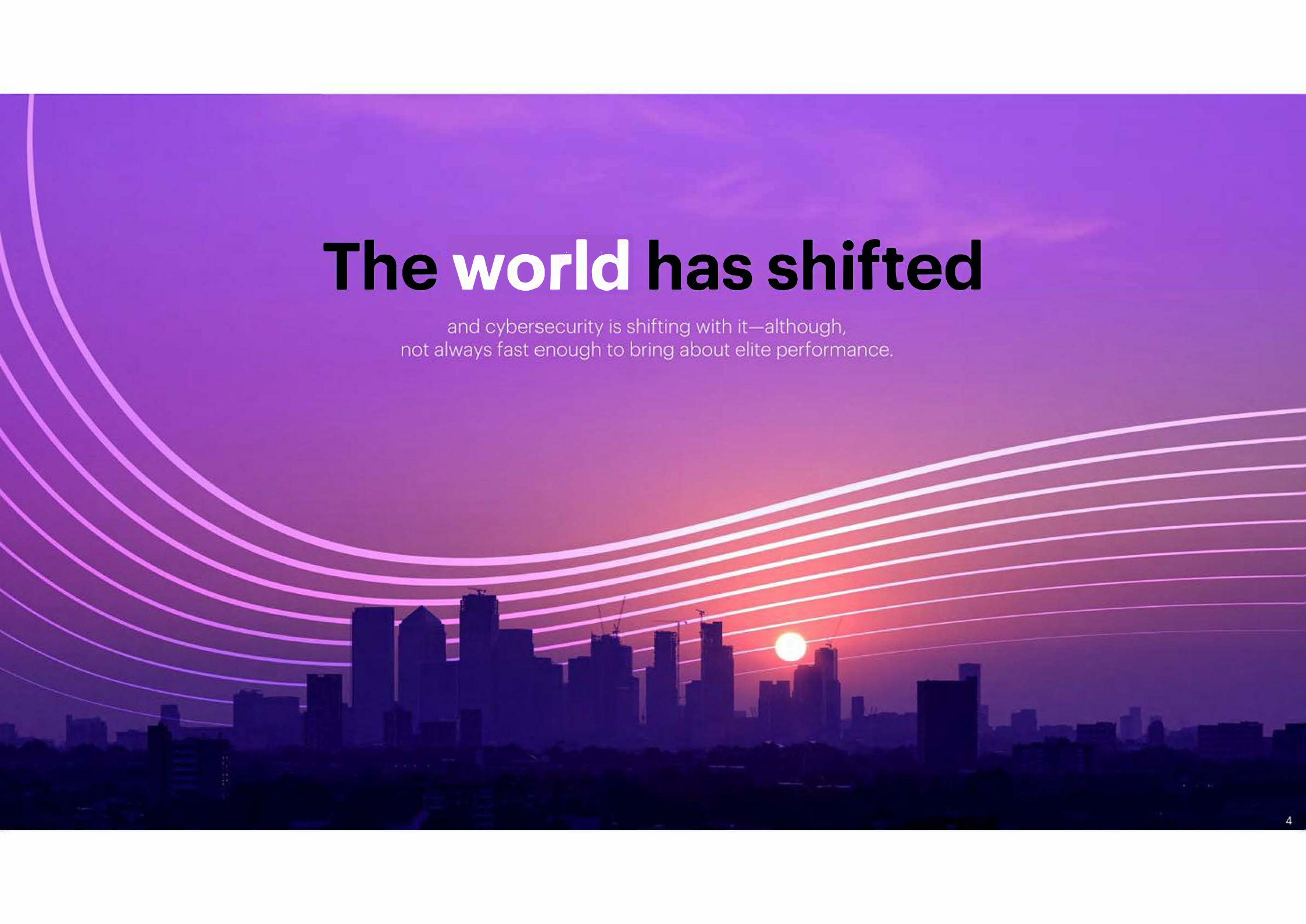
**About the
research**

Page 33



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.





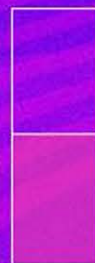
Cybersecurity as a changemaker



Cybersecurity as a changemaker

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

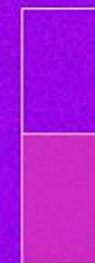
Survey responses show that more than one-half of organizations are beginning to recognize the importance of being secure from the start in any transformation effort.



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

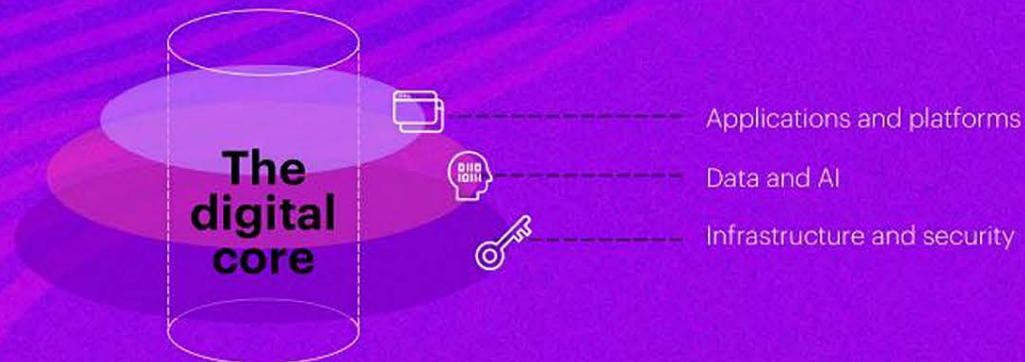
3.

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](#) study² 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

Cybersecurity as a changemaker

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

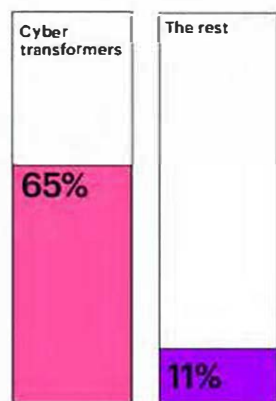


What it takes to be a cyber transformer



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.

What it takes to be a cyber transformer

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.

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/815021212230011103>