Deloitte.

Cyber & Strategic Risk

Lead through disruption

A guide to taking on cyber and business risk with confidence

LEAD THROUGH DISRUPTION

Table of contents

First, imagine this

You're on a racetrack—but the race isn't to get to the finish line. Instead of competing with other cars, you're working to confidently navigate uncertainty, build transformational capabilities, and drive exceptional performance at scale, irrespective of what's around the bend. Harnessing cyber and risk as strategic enablers is imperative and, at times, arduous.

Sound familiar?

When the stakes are high for cyber and strategic risk, a winning approach is about more than speed. You'll need grit and vision to hone your strategy and execution. Collaboration is also essential, especially when it's born from a diverse, interdisciplinary pool of perspectives. The value of applying an engineer's mindset, which allows you to see every opportunity with a precise, analytical, and creative viewpoint, cannot be underestimated. Most of all, you need an approach that instills the confidence to win because, when it comes to matters of cyber and strategic risk, losing isn't an option.

Your course becomes more precarious as stakes grow and risks reach every corner of your organization.

Your conditions create interdependencies between the domains and functions needed to prepare for unexpected circumstances and safely navigate the next corner.

Your competition isn't slowing down—in fact, they're gaining ground.

Your crowd cares deeply about who wins. You need their support to keep going and build a high-performing program.

Your collaborators require decisions from leadership on developing capabilities or bringing on third parties to build a consistent, winning team.

Your crew keeps moving forward, but intense, high-speed conditions increase the pressure—and the stakes.

Here's what we mean

The sophistication and frequency of threats are growing, with the magnitude of disruption staggering. Defending against attacks and mitigating risk depends on coordination across your organization, because today's threats to modern enterprise are no longer bound by defensible perimeters. Likewise, their consequences are just as pervasive.

Think about the many examples of geopolitical conflict over the past few years. Not only do they present political challenges to governments; they also raise threat levels and introduce numerous risks for businesses. Conflict creates supply chain disruptions, posing risks to brands operating in and alongside the conflict. It also escalates the stakes for organizations committed to protecting the safety and security of workers, mitigating the impact of operational disruptions, and executing effective responses to global incidents.

A coordinated approach with collaboration from an organization's leadership—including its CISO, C-suite, and board—is necessary both to address the complexity of today's cyber and risk challenges and to see the opportunities they create—especially the ones competitors may overlook.

An organization's winning cyber and risk posture depends on a blend of preparation, performance, and reaction. It introduces cyber and strategic risk considerations earlier and drives accountability across the whole organization. Because disruption isn't slowing down, your organization can't either. To face it head on, you'll need:

- Defense against increasingly frequent and sophisticated attacks to protect your team, assets, operations, and competitive edge.
- Dynamic insight into numerous, interconnected risk domains and how to drive organizational performance in the face of shifting scenarios and an ever-evolving regulatory landscape.
- Trust, engagement, and stakeholder support to maintain and grow positive brand perception.
- An agile culture, supporting processes, and technologies that accelerate the innovation required to outpace competitors.
- Vision and growth to prepare for what's around the bend and to build teams for peak performance and a podium finish.

This situation provides an opportunity to transform your organization by innovating through disruption. By recognizing both the stakes and the rewards, you can shift perspective in your organization and create a truly integrated risk approach that sustains outstanding performance through constant change.

Twelve key objectives to empower your organization

- Secure, connected devices
- Trusted data use
- Agile, secure modernization
- Secure, intelligent operations
- Dynamic risk programs
- Supply chain security and risk transformation
- Secure, efficient workforce experiences
- Resilient digital operations
- Future forward readiness
- Trusted customer experience
- Enhanced response and recovery
- Governance and optimization

By setting your sights on opportunities instead of obstacles, you'll be able to drive concrete outcomes and unlock value faster. This approach will help you stay on course, outmaneuver your competitors, and position your organization for the top of the podium.

Secure, connected devices

The recent proliferation of IoT (Internet of Things), IIoT (Industrial Internet of Things), operational technology (OT), and ICS (industrial control systems) is rapidly expanding both the number of connected legacy devices and their associated attack surfaces. This can leave companies struggling to secure assets and users—and attackers eager for the opportunity to exploit their vulnerabilities.

Secure, connected devices

What's at stake:

Your confidence operating in distributed, modern environments

The integrity of critical organizational data and the technologies you adopt to secure it

What you'll need:

- A comprehensive inventory of devices to prioritize security monitoring integrations across extended enterprise, supply chain, third-party, and security operations attack surfaces
- A tech-enabled data protection management system that incorporates data from a variety of asset classes
- A security-minded approach that embraces application modernization and innovation
- Talent with subject-matter expertise that spans the technical, security, and privacy aspects of 5G connectivity across a variety of smart devices
- Greater visibility across the organization to promote collaboration between business functions
- Integrated and consolidated security management to accelerate the identification and remediation of security vulnerabilities

FAST FACT:

It is estimated that by 2025, there will be as many as 40 billion connected devices across the globe.[1]

What's possible:

"Smart factories" bring opportunities to increase manufacturing efficiency while simultaneously introducing risks related to leaking proprietary information between connected factory components and external entities. To realize intended efficiency increases without exposing secrets, manufacturers should pay close attention to addressing data and security risks in their artificial intelligence (AI)-driven OT and IIoT devices as they build their smart factories.

Secure, intelligent operations

As IT environments become more complex and threats more sophisticated and interconnected, bolstering security operations and integrating actionable intelligence to prepare for, detect, respond to and remediate security events becomes an enterprise imperative. This requires constant monitoring of critical networks and devices to identify and contain potential threats before they become a problem.

Secure, intelligent operations

What's at stake:

Your entire IT environment, including the confidentiality, integrity, and availability of your data and systems

Your organization's plans for digital transformation, as well as its reputation, operations, and bottom line

Your ability to effectively drive continued improvements in security operations while also embracing the benefits of increased automation and actionable intelligence

What you'll need:

- Actionable threat intelligence that integrates security operations functions across the enterprise to reveal threat exposure, quantify risk, and predict threat paths
- Innovative technologies such as artificial intelligence (AI) and machine learning (ML) to improve existing threat detection and response via automation securely implemented in your environment
- Adequate security controls deployed across cloud and hybrid infrastructure environments
- Exercises in crisis simulation and wargaming to help prepare for inevitable attacks ahead
- Cloud engineering assets and expertise to drive security and functionality across the enterprise

What's possible:

Faster time to incident detection reduces the risk exposure of a major disruption. In telecommunications, service outages from cyberattacks mean lost revenue. Enhanced cyber analytics and ML technology solutions can prevent these disruptions before they happen.

FAST FACT:

91% of respondents in our 2023 *Global Future of Cyber Survey* reported at least one cyber incident or breach, compared to 88% in our 2021 survey.[2]

Secure, efficient workforce experience

In a boundaryless world, work isn't defined by jobs, the workplace isn't a specific place, and many workers aren't traditional employees. Organizations that partner with workers to securely transform their workspaces will create sustainable work models and elevated outcomes. They are also 1.8 times more likely to have a highly engaged workforce, two times more likely to be innovative, and 1.6 times more likely than their peers to anticipate and respond to change.[3]

Secure, efficient workforce experience

What's at stake:

Your organization's productivity and security of its virtual workplace environments, including that of its collaborative tools

The confidentiality of your data and the privacy rights of people who interact with your organization

The security of your organization's most sensitive data, credentials, systems, and financials

The productivity and efficacy of your cyber and risk teams

What you'll need:

- A Zero Trust framework that bolsters identity, access, and application security initiatives while reducing attack surface exposures
- Advanced identity access and authentication tools that can accommodate unmanaged devices without compromising security protocols
- Insider threat detection solutions that identify and secure all service, application, administrator, and root accounts across your enterprise and its service area
- Dedicated talent identification and retention solutions that enable scalable workforce transformation for years to come

What's possible:

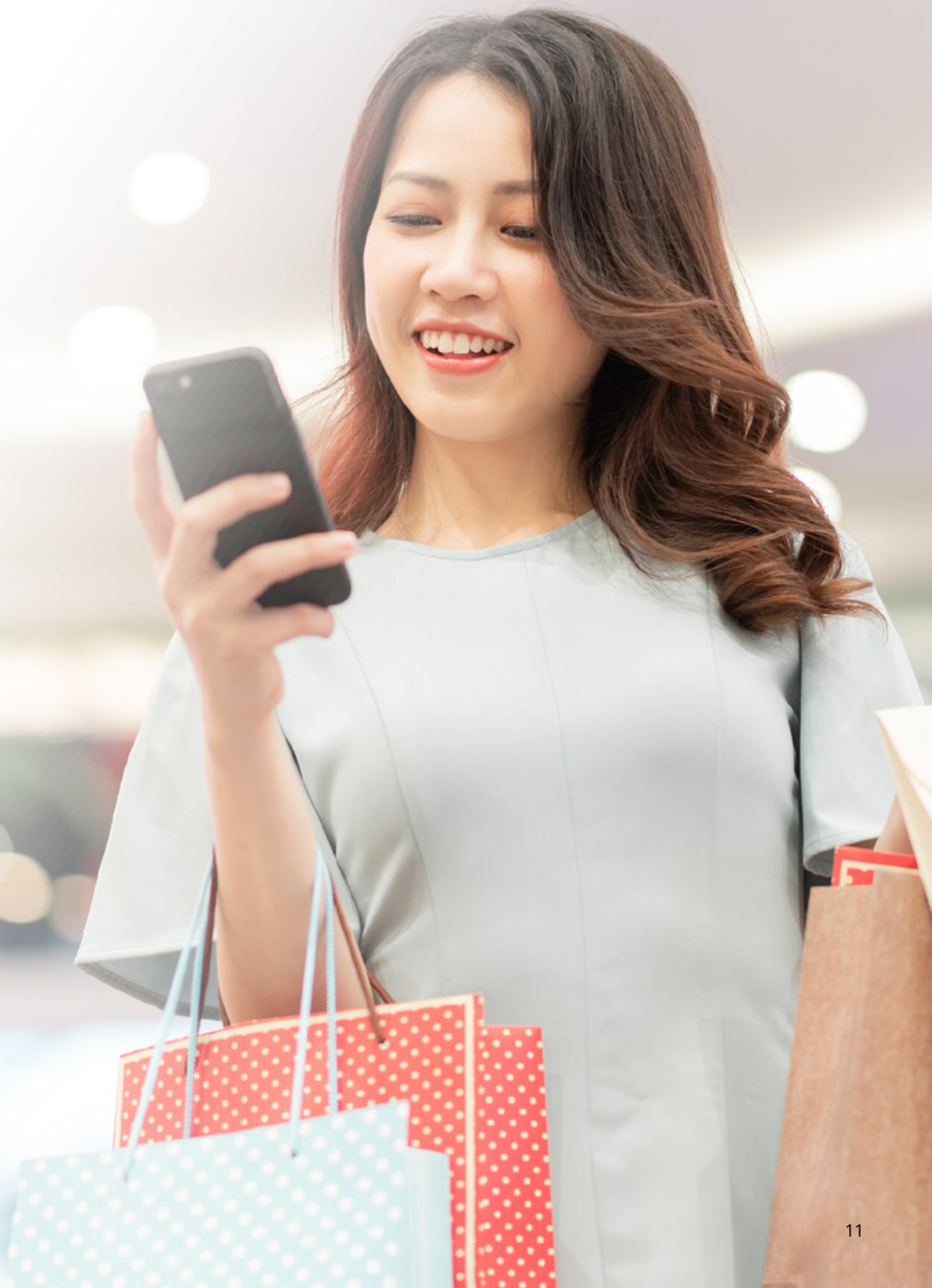
By properly implementing a Zero Trust architecture across your environment, you can reduce your organization's attack surface while ensuring that internal and external stakeholders have appropriate resource access. This will address the growing number of ransomware attacks on critical infrastructure that are highlighting the importance of enhanced authentication methods to protect high-value assets, especially among energy and utilities companies.

FAST FACT:

Employee error accounts for about 13% of all breaches and, in most cases, can be traced back to misconfigured cloud storage.[4]

Trusted customer experience

Digital customer experiences are quickly becoming the norm. As regulatory and customer expectations around privacy shift, your organization can strengthen customer relationships and improve stakeholder trust by creating secure, trustworthy, and compliant experiences that empower privacy, dynamic consent, and preference management.



Trusted, customer experience

What's at stake:

The health of your business's relationships with customers and stakeholders, as well as the security of their data and privacy

Your organization's ability to navigate regulatory hurdles and avoid costly financial penalties from unnecessary compliance risk

Positive perception of your brand, along with the trust and loyalty of your customers, stakeholders, and the public

What you'll need:

- Privacy practices that instill trust and give customers dynamic control over their data
- Protection designed to keep high-value data safe against a myriad of attacks
- Customer identity and access management to prevent fraud and bolster user experience
- Quantifiable insights into marketing- and advertising-related risks that contextualize the impact of customer trust on your brand
- A customer experience strategy and user experience design that positions your business to grow in line with evolving customer behaviors
- A transparent communication policy that fosters brand and customer trust

What's possible:

Omnichannel shopping experiences have become commonplace and are amplifying the need for a more secure and efficient user experience across device types and networks. By integrating robust privacy and data security protocols into your e-commerce platforms, you can help ensure your customers shop more confidently knowing their payments and carts will remain private and secure, no matter where they're shopping from.

FAST FACT:

Trustworthy companies outperform non-trustworthy companies by 2.5 times,[5] and 88% of customers who highly trust a brand will buy again from that brand.[6]

Trusted data use

It's time to stop looking at data as a cost driver. Instead, unlock the value of your organization's data to drive better business outcomes by integrating emerging technologies while staying compliant, keeping your customers' trust, and applying data and privacy controls to align with regulatory requirements and facilitate ethical data use.

Trusted data use

What's at stake:

Your ability to prevent the theft or corruption of your organization's data

Your ability to maintain your organization's corporate reputation and value

Your organization's ability to avoid unnecessary regulatory fines and penalties

Your organization's ability to retain revenue and market competitiveness

Your power to drive more strategic and data-driven decisions

What you'll need:

- Data protection that protects and maintains confidentiality, integrity, and availability
- Privacy policies and processes that make it easier to navigate regulations and bolster governance
- Identity and access management that enables access to the right data in the appropriate context
- Data-driven advertising, marketing, and commerce strategies that translate insights into targeted customer outreach
- Ethical guardrails put in place to govern the use of AI and ML and reduce unintended analytical biases

Potential outcome:

Building trust with both internal and external stakeholders is a key factor in driving high performance, according to Deloitte's recent report on the future of trust.[7] Instituting data protection and privacy controls, as well as trusted ways to reduced unintended biases, can increase brand trust and contribute positively to your organization's bottom line.

FAST FACT:

By 2024, 75% of the world's population will have its personal data covered under modern privacy regulations.[8]

Dynamic risk programs

With a dynamic risk program, your organization can stay proactive when managing the multi-domain and interconnected nature of risk and crisis scenarios, increasing decision-making confidence, keeping business goals on track, and building resilience to disruption.

Dynamic risk programs

What's at stake:

Your organization's ability to stay on track in the face of widespread disruption

Operational efficiency and potential business opportunities

Ongoing compliance and avoidance of costly legal violations and fines

Your brand reputation; ecosystem relationships; and even the physical health and safety of your employees, customers, and third-party personnel

What you'll need:

- An integrated approach to managing risk and compliance, including risk frameworks, processes, governance models, and risk analytics that drive data into strategic insights
- Enhanced dashboards and visualizations that distill complex risk information into digestible insights that can inform more efficient decision-making
- Crisis simulation, modeling, and wargaming exercises to proactively prepare for a breach

What's possible:

Financial services institutions are challenged with correlating risks to make strategic investments and provide competitive products. To address this challenge, thriving organizations use integrated risk assessments, processes, and simulation capabilities. The result: strategic decisions made with confidence.

FAST FACT:

86% of companies believe they need to be more resilient, and only 5% believe their enterprise risk management systems are integrated into their enterprise's corporate functions.[9]

Resilient digital operations

Future threats promise to grow even more frequent and sophisticated than today's, creating an ever-greater need for business resilience. Building an agile mindset—alongside robust capabilities to plan, implement, and foster resilient practices—empowers an organization to address threats before they strike.

Resilient digital operations

What's at stake:

Your organization's ability to prevent and reduce downtime and potential losses from ensuing attacks

The health of your brand reputation and your customers' trust

Maintaining market share and competitive footing

Your organization's ability to remain compliant and avoid unforeseen regulatory violations and financial penalties

What you'll need:

- Technical, cyber, and business resilience to help your operations withstand a variety of disruptive scenarios
- Crisis simulation, modeling, and wargaming exercises to better prepare your cyber defenses against today's most likely threats and address a variety of disruption scenarios
- Integrated supply chain and network security operations to more proactively identify risks from third-party and extended Nth-tier vendors
- Cyber incident response, threat intelligence, threat hunting, and governance models that employ advanced data analytics to predict and mitigate security challenges
- Data-driven risk management and predictive risk capabilities to limit business disruptions

Potential outcome:

Energy organizations are major targets for cyberattacks, and after a recent US fuel pipeline was attacked by ransomware, companies were jolted into action. By performing resilience assessments and developing business service maps to determine interdependencies, companies can reduce vulnerabilities, recover operations faster, and mitigate damage.

FAST FACT:

58% of executives who participated in our 2023 Global Future of Cyber Survey noted that, between 2021 and 2023, cyber incidents and breaches most frequently resulted in operational disruption.[10]

Enhanced response and recovery

From climate disruptions to external attacks, a major incident is a “when,” not an “if.” With greater resilience, faster timelines to business as usual, and improved communication, your organization can handle these inevitable challenges. Better preparation, speed, and collaboration sooner will keep business moving and reduce damage later.

Enhanced response and recovery

What's at stake:

Your organization's operational continuity and ability to recover from a major event

Your organization's ability to maintain revenue amid disruption

Your ability to avoid high costs from legal or regulatory penalties

The health of your organization's brand reputation and customer loyalty

The physical safety of your employees, customers, and third-party personnel

What you'll need:

- A crisis management program to establish plans, processes, and systems to enable a faster, more integrated cyber incident response
- Early warning systems and scenario and contingency plans to facilitate proactive, continuous decision-making
- Virtual and physical simulations to test the effectiveness of existing mitigation processes and resource collaboration
- Continuous, enterprise-wide security operations that support security at scale
- Real-time access to data to facilitate faster, more informed identification and mitigation of incidents that restore operations more quickly

What's possible:

Energy companies can insulate their core technology operations from future disruption by regularly evaluating and updating their disaster response and recovery plans, as disasters such as those listed above are expected to continue, if not increase.

FAST FACT:

Between 2012 and 2021, the United States experienced 142 natural disasters that resulted in $1 billion or more in damages, with much of this damage dealt to power grid infrastructure.[11]

Agile, secure modernization

Build security and compliance into your organization while embracing transformative technologies by implementing cloud environments and applications that are more agile, secure from the start, and designed to facilitate business transformation.

Agile, secure modernization

What's at stake:

Availability of critical systems and infrastructure

Security against data theft and breach

Your organization's ability to avoid high-cost regulatory penalties

Organizational reputation with customers and business partners

Time to value of expected benefits from digital transformation

Maintained agility and fast releases of new software features

What you'll need:

- Security architectures that function across cloud and traditional IT environments to increase and integrate security performance
- Developer automation and orchestration tools to design, build, and deploy to the cloud faster, as well as built-in compliance and regulation guardrails
- Emerging enterprise resource planning solutions to maximize organization-wide resource planning capabilities
- Technologies that manage activities for known and unknown governance, risk, and compliance requirements
- An evolution in culture that shifts security left and embeds it throughout development processes to facilitate more robust applications and infrastructure

What's possible:

Technology companies are constantly pressed to develop code and release new features faster, without compromising on security. By using "secure by design" principles, they can integrate security management, visibility controls, and automated testing into each software release, along with cloud infrastructure orchestration from configuration to deployment.

FAST FACT:

75% of organizations with mature cloud and cyber strategies reported that advanced technologies had made them both more resilient and agile, versus 53% of organizations overall.[12]

Supply chain security and risk transformation

Mitigate threats, improve customer relationships, and drive better business outcomes by increasing visibility into supply chains, third-party relationships, and process efficiency.

Supply chain security and risk transformation

What's at stake:

Securing your hardware and software components

Preventing financial penalties, catastrophic damage, and loss of life

Maintaining operational continuity

Your ability to minimize wasted labor, service redundancies, and missed deadlines

Availability of critical systems and infrastructure

Your ability to prevent intellectual property or trade secret theft

Your organization's ability to navigate regulatory requirements and avoid costly penalties

What you'll need:

- Governance frameworks and tech-enabled assets that increase monitoring over supply chain and products
- Identity and access management capabilities to better enforce third-party access to systems and data
- Blockchain-enabled resourcing to ensure smooth logistics and distribution operations
- Operational security controls adapted for supply chains to integrate loss prevention with security
- Security controls embedded throughout the product life cycle to maintain compliance and regulatory adherence and mitigate costly oversights
- Proactive monitoring of third-party and extended Nth-tier relationships to proactively identify major risk indicators
- Increased real-time or near-time identification of risks across supply chains to accelerate mitigation and response

What's possible:

Major supply chain vulnerabilities and geopolitical unrest have a significant impact on organizations that need to get products to customers. By leveraging tech-enabled risk solutions, such as inventory demand planning and omnichannel order fulfillment, consumer organizations can position themselves to better anticipate and prepare for the inevitable disruptions to their supply chains in the future.

FAST FACT:

51% of organizations have faced one or more third-party risk incidents since the beginning of the COVID-19 pandemic in March 2020.[13]

Future forward readiness

Disruption equals opportunity for the organizations that are ready—and challenges for those that aren't. With vision, persistence, and a cyber and risk strategy as adaptable as tomorrow's challenges are unpredictable, you can future-proof security, risk, and business functions.

Future forward readiness

What's at stake:

Continued ability to understand potential risks introduced by emerging trends and technology

Avoiding substantial or unnecessary risk arising from hasty technology adoption

Preventing theft, loss, or misuse of customer or company data

Anticipating and mitigating interruptions to business-critical operations

The security, privacy, and physical health/safety of employees, customers, and/or patients

Ongoing and effective communication among business leaders

What you'll need:

- Strategy development to build and inform investment around new organizational capabilities
- Security embedded into the adoption of emerging technologies to enable innovation without inviting greater risk
- Flexible, organizational cyber and risk transformation strategy and implementation that can be tailored to your specific purposes
- Data and brand measurement to drive operational performance and strengthen the overall health of your brand
- End-to-end supply chain visibility to spot risk vulnerabilities before disruption takes hold

What's possible:

By preparing for the approach of quantum computing now, you can keep your organization a step ahead of potential "hack now, decrypt later" attacks—and their future consequences. While quantum offers opportunities to solve use cases beyond the limits of traditional computing, it also presents attackers with a weapon to break encryption algorithms used today.

FAST FACT:

By 2026, 25% of people will spend at least one hour a day in the metaverse for work, shopping, education, social events, and entertainment.[14]

Governance and optimization

Strengthen your organization's cyber and risk governance and optimization, and boost the effectiveness of your activities by quantifying risks, fine-tuning operating models, updating policies and processes, and transforming communication and reporting.

Governance and optimization

What's at stake:

Your ability to reduce the gaps in governance that can lead to security breaches and undue risk exposure

Your organization's ability to prevent duplicated effort and conflicting lines of ownership for key responsibilities and functions

Your ability to make the ongoing updates necessary to prevent outdated and inadequate security, compliance, risk, and privacy policies

Your organization's ability to identify weaknesses in its cyber and risk programs

Your cyber and risk program's ability to readily adapt to changing regulations and standards

The ability to capitalize on opportunities for increased efficiency, improved resource allocation, and financial optimization

Your ability to measure and prioritize cyber and risk investments

What you'll need:

- Greater visibility into your organization's cybersecurity posture and program maturity to better identify vulnerabilities and make informed decisions
- Future-state benchmarks that balance your organization's specific needs with its risk appetite
- Governance and operating models built to operate efficiently and foster continuous improvement
- The ability to accurately measure and communicate the ROI of your cyber program investments to nontechnical decision-makers
- A sturdy foundation of policies, standards, and processes to grow security and efficiency at scale for years to come
- Optimized technical support to ensure your organization is getting the most out of its existing investments

What's possible:

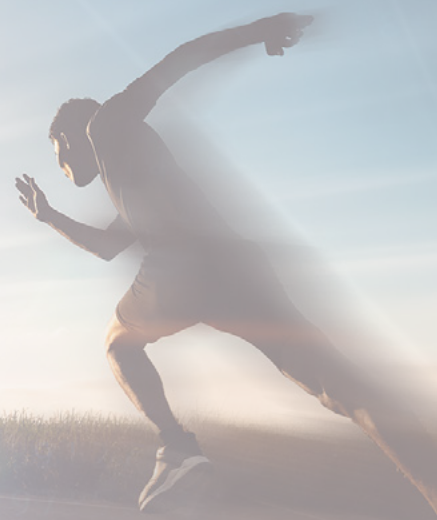
Health care organizations constantly experiment with new ways to provide services to patients, health care workers, and others while navigating evolving standards. Periodic reviews of cyber policies and processes can help to keep cyber activities aligned with ongoing business initiatives and ever-changing compliance requirements.

FAST FACT:

88% of director boards said they view cybersecurity as a business risk as opposed to a technology one.[15]

Here's what leaders need to know, no matter what

The stakes are high—and talent is hard to find.
As leaders across industries and geographies know, the talent shortage is real, and it's even more dire in the realm of cyber and technology. The cyber workforce gap has grown to 3.5 million jobs worldwide, a number unexpected to change much in the coming years. An increasingly stringent regulatory field is requiring skills that most cyber professionals don't have, and constantly evolving technologies require a talent pool that can evolve along with them. Organizations are going to have to get creative in how they grow and equip their teams for success.



What you'll need:

- Leadership and executive engagement from the very top to make identifying and retaining talent a top organizational priority
- A resourcing plan that combines in-house and outsourced services to deal with the limited technical and cyber talent market
- An unconventional talent pipeline that focuses on nontraditional, high-potential candidate pools to break through the stiff competition for today's technical and cyber talent

Your ability to execute a plan will depend on a horizontal, cross-organizational approach.
With cyber and risk, it's vital to shift left and drive more responsibility across business functions. Success can't happen in a silo.

- Cross-organizational collaboration and responsibility that harnesses individual strengths across teams to achieve shared objectives
- Stakeholder engagement across levels and leadership from the top to drive positive outcomes
- Careful orchestration between cyber and risk functions across the business life cycle—from prevention and preparation to response and recovery—to fully address the interdependencies of today's cyber and risk landscape

Disruptions are inevitable, so balance is necessary.
Any cyber and risk strategy must balance security, trust, and resilience, which requires an equal consideration of preparation, performance, and reaction.

- Coverage for a business's full incident or crisis life cycle that encompasses prevention, identification, response, and recovery
- A focus on incorporating lessons learned that enables continuous improvement that can scale
- An agile posture and communication structure that can tell the story of successes and leverage them for future positioning

So, what does it all mean?

Building the mindset required for a future-forward cyber and risk program that secures your organization today and prepares it for tomorrow's inevitable disruptions and opportunities can feel daunting—especially when those disruptions appear seemingly overnight. Start by asking the right questions, however, and you'll be able to confidently build a cyber and risk vision for your organization, map it to a concrete plan, implement it through sound solutions, and move forward fast toward a more agile and secure future. You'll also be better prepared to hire the top talent, as well as adopt more efficient processes and safer technologies to support it.

Where to begin

Start with these questions:

- How do my cyber and risk capabilities stack up to threats and potential risk?
- Will I be able to keep my organization out of the headlines if an attack or crisis event happens?
- Do I have the talent I need? Am I allocating the right resources?
- How can I engage stakeholders across the business to collaborate and improve our response rather than operating in silos (because risk does not)?
- Which capabilities do I have—and which ones do I need—to really move the needle?
- How can I position my organization to achieve its goals for sustained success, no matter what comes our way?

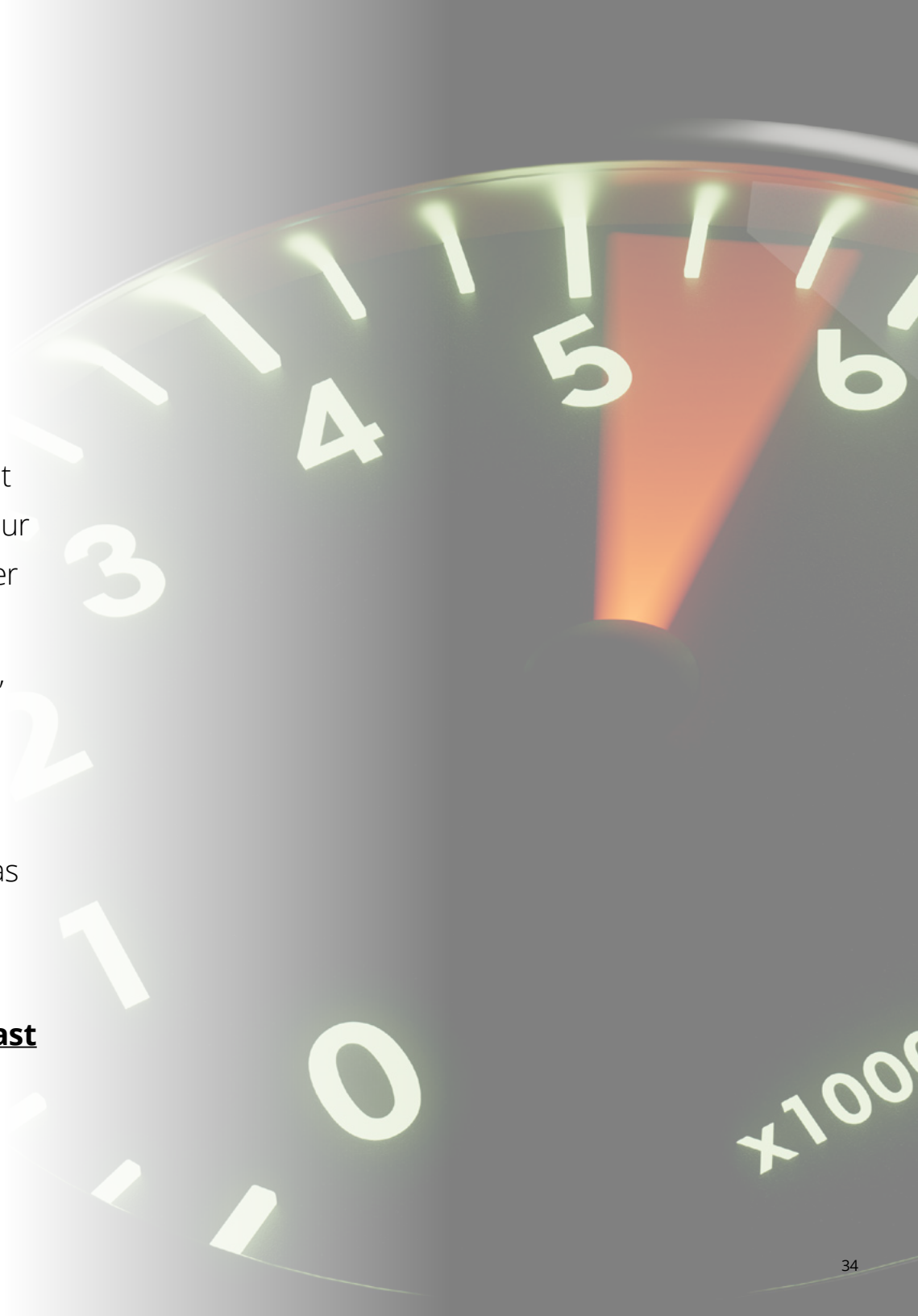
Focus on what matters most—and get moving

No matter where you are in your journey, it's important to build your organization's cyber and risk posture with an eye on what matters most, from defining your vision and understanding your organization's current and future threat landscape to implementing strong capabilities, building a network of trusted partners, and adopting creative processes and services to operate your capabilities, no matter what disruptions or challenges lay ahead.

How Deloitte can help accelerate your journey

With a confident strategy, you can navigate the threat landscape, find opportunity in risk, and transform your organization by focusing on the outcomes that matter most: trust, resilience, and security. Deloitte's cyber and risk professionals have the experience, the tools, and the vision to move your organization forward. Our team can help you build a strategy that fits your needs, implement tools, improve your capabilities, and operate through disruption as well as business as usual. That's an organization built to lead and win.

Learn more at deloitte.com/us/MoveForwardFast



Endnotes

1. Verizon, *Mobile Security Index 2021 report*, 2021.
2. Deloitte, *2023 Global Future of Cyber Survey*, 2023.
3. Kraig Eaton et al., 2023 *Global Human Capital Trends*, Deloitte Insights, 2023.
4. Verizon, *Data Breach Investigations Report*, 2022.
5. Stephen M. R. Covey and Douglas R. Conant, "The connection between employee trust and financial performance," *Harvard Business Review*, July 18, 2016.
6. Deloitte, Deloitte HX TrustID™ Survey, May 2020.
7. Deloitte, "The Future of Trust: A new measure for enterprise performance," 2021.
8. Amita Jain, "5 ways to show prospects you take data privacy seriously," Gartner, December 7, 2022.
9. Tim Archer and Helen Hodge, *A refocus on risk and resilience*, Deloitte, 2021.
10. Deloitte, *2023 Global Future of Cyber Survey*.
11. Adam B. Smith, "2021 U.S. billion-dollar weather and climate disasters in historical context," Climate.gov, January 24, 2022.
12. Deborah Golden et al., "An integrated cyber approach to your cloud migration strategy," Deloitte Insights, March 2, 2021.
13. Kristian Park, Danny Griffiths, and Sanjoy Sen, *Gaining ground: A digital path to third-party oversight*, Deloitte, 2021.
14. Gartner, "Gartner predicts 25% of people will spend at least one hour per day in the metaverse by 2026," press release, February 7, 2022.
15. Partha Iyengar, *Roadmap to renewal: The 2022 Board of Directors Survey*, Gartner, October 28, 2021.

Acknowledgments

Authors and contacts

Deborah Golden
Hallie Miller
Stephen Ruzzini
Kate Seif

Contributors

Sunny Aziz
Ranjit Bawa
Ed Bowen
Criss Bradbury
Keri Calagna
Dave Couture
Wendy Frank
Vikram Kunchala
Hila Mehr
David Mapgaonkar
Mike Morris
Kiran Nagaraj
Kieran Norton
Pete Renneker
Chris Ruggeri
Irfan Saif
Alex Seton
Daniel Soo
Colin Soutar
Adam Thomas
Damian Walch

Deloitte.