STATE OF DISRUPTION:
BUSINESS RESILIENCE

From Protection to Performance: Cyber Resilience as a Business Strategy

Complimentary report provided by:

AVANT | CA Communications Inc

Table of Contents

November 2025

Introduction

Business Resilience in the Age of Disruption

We are seeing the role of the CIO transform in real time. Once defined primarily by cost control and operational uptime, today's CIO is being asked to make career-defining decisions with a new perspective. From navigating ballooning cloud costs and managing complex IT estates to deciding where and how to invest in artificial intelligence, CIOs must balance risk and innovation under an intense level of scrutiny. Every decision they make impacts the business including revenue potential, competitive positioning, and shareholder confidence.

That pressure is redefining how organizations think about resilience. IT resilience — keeping systems secure, stable, and recoverable — is still foundational. Yet boards and CEOs now expect CIOs to deliver something broader: business resilience. That means ensuring the technology strategy strengthens the organization's ability to absorb disruption, adapt in real time, and continue to deliver value in the face of volatility. The shift reframes the CIO as a growth architect responsible not only for protecting the enterprise but also for enabling it to thrive in uncertain times.

Business Resilience vs. IT Resilience

Business Resilience	IT Resilience
Focuses on the entire technology environment—hardware, software, networks, data, cloud services, and virtualized solutions like Desktop-as-a-Service (DaaS).	Focuses specifically on applying concepts borrowed from cybersecurity to the rest of the IT estate—protecting systems, networks, and data.
Goal: Ensure business continuity by aligning technology programs with asset control, financial planning, risk mitigation, and operational excellence. Measured in terms of operational resilience: uptime, cost efficiency, ability to adapt to disruption across the IT estate. Owned by the CIO/VP of Infrastructure, who balances cost containment, performance, and resilience across programs.	**Goal:** Ensure the organization can anticipate, withstand and recover from all cyber incidents while minimizing downtime and data loss. Measured in terms of operational resilience: uptime, cost efficiency, ability to adapt to disruption across the IT estate. Led by the CIO with input from the CISO or security team, who builds resilient systems and owns virtualized systems, help desk, identity management, connectivity, patching, and recovery.
Example: Deploying DaaS to secure distributed call centers with BYOD (Bring Your Own Device) contractors while reducing risks from compliance and data leakage.	**Example:** Implementing strong identity programs to control access to proprietary data.

This shift places responsibility squarely on the shoulders of CIOs and VPs of Infrastructure. Once viewed as technical stewards, they are now accountable for ensuring the resilience of the entire IT estate. It's a role that extends well beyond the security team. Whether through desktop-as-a-service (DaaS), unified platforms, or program consolidation, the CIO is expected to deliver resilience as a measurable business outcome, containing cost, minimizing disruption, and enabling innovation.

> "Business leaders have learned resilience from their own experiences. They know the key to thriving in adversity is building strong, adaptable teams, processes, and technologies. Leaders expect their cyber defense to operate the same way: keeping the business open and profitable in the face of adversity."
>
> **– Stephen Semmelroth, VP of Cyber Resilience at AVANT**

What is an IT Estate?

A company's IT estate is the sum of all technology assets and services, including hardware, software, networks, data, and cloud environments, that power business operations. It impacts:

Asset Control – Visibility into what you own, lease, and use
Financial Planning – Optimizing technology spend
Risk Mitigation – Reducing exposure across infrastructure and services
Business Continuity – Ensuring operations remain resilient during disruption

1 The Business Value of Resilience: Turning Risk Into Advantage

For CIOs, the greatest risks aren't always external threats but the everyday realities inside and around the business that can erode resilience if left unmanaged—vulnerable third parties, cost overruns, generative AI exposure, outdated internal systems, remote workforces, and negligent employees. These challenges come to life in ways that directly test a company's ability to withstand disruption.

- **A departing Chief Revenue Officer** might walk away with sensitive sales data and bring it to a competitor.
- **Contract call center agents**, often working on outdated personal devices across international borders, may expose customer information to unnecessary risk.
- **Distributed Denial of Service (DDoS) attacks** could go unaddressed at the C-suite and board level despite their potential to halt operations.
- **Overworked teams** may be forced to deprioritize unpatched systems with multiple vulnerabilities.

These scenarios illustrate that business resilience is not about "if" or "when" an incident occurs. It's about assuming the threats are already inside company walls and ensuring the organization is prepared to adapt and respond.

Boards and investors have taken notice. Gartner reports that 93% of non-executive board members see cybersecurity threats as a direct risk to shareholder value.[1] At the same time, Accenture finds that nearly 90% of organizations are not resilience-ready, with 63% sitting in an "exposed zone."[2]

The gap between risk and readiness represents a critical opportunity for CIOs. By focusing on resilience outcomes—maintaining uptime, ensuring workforce productivity, and safeguarding customer trust—CIOs can directly tie technology investment to business value. This means reframing conversations with boards away from tools and toward measurable resilience metrics.

2 Unified Platforms, DaaS, and the Resilient CIO

The most consequential resilience decisions now sit with the CIO, who manages infrastructure, cloud strategy, and user environments that directly influence how resilient the business can be. For these leaders, resilience is a business mandate that drives efficiency, ensures continuity, and supports growth, with a security mindset.

From Fragmentation to Unified Platforms

For years, companies attempted to buy their way to resilience with dozens of point solutions. The result? Redundant tools, rising costs, limited visibility, and fractured defenses. Today, more than half of executives cite tool sprawl as the single greatest impediment to effective security.[3]

As a result, IT and security teams are turning to unified platforms that consolidate programs across infrastructure, data, and applications. By aligning investments with existing ecosystems, CIOs can reduce redundancy, improve visibility, and create resilience outcomes without adding unnecessary costs or complexity. Three out of four enterprises are pursuing vendor and tool consolidation, up from just 29% in 2020.[4]

By consolidating controls, data, and workflows into integrated ecosystems, CIOs can reduce cost and complexity while gaining clearer visibility across their IT estate. Organizations that embrace unified platforms:

Detect incidents on average **72 days faster** and contain them **84 days sooner** than those using fragmented tools.[5]

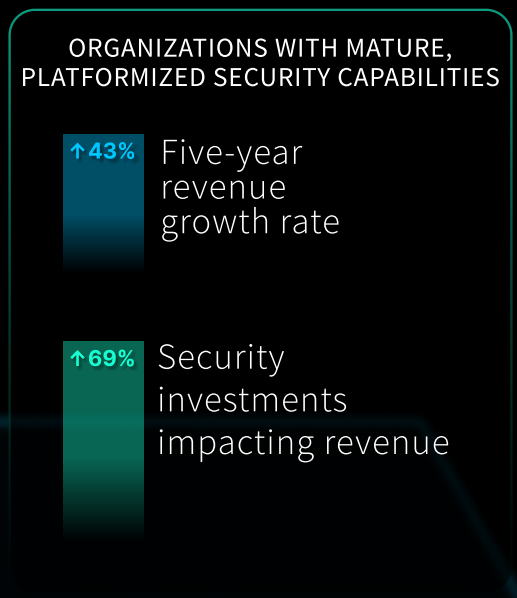
Run security teams that are **34%** more efficient.[6]

Cut annualized security-related platform costs by **10%**.[7]

Unified Platforms as Growth Enablers

The benefits extend beyond IT. IBM research shows organizations with mature, platformized security capabilities achieve a 43% higher five-year revenue growth rate and are 69% more likely to see security investments positively impact revenue.[8] Once viewed as a cost center, business resilience now becomes a driver of digital transformation and competitive advantage.

> "Platformized security organizations reap an average ROI of 101%, compared to 28% for those that are not yet embracing platformization."[9]
>
> **Capturing the Cybersecurity Dividend - IBM Institute for Business Value**



DaaS: Resilience at the User Edge

The rise of Desktop as a Service (DaaS) underscores this shift. For many CIOs, DaaS spending now exceeds total security budgets since it delivers a direct resilience outcome.
By moving high-risk groups, like call center contractors using outdated personal devices across geographies, into secure, cloud-delivered environments, CIOs achieve:

- Consistent patching and updates without relying on individual user devices.
- Centralized policy enforcement that reduces compliance risk.
- Greater workforce flexibility, allowing contractors or remote employees to securely access systems without jeopardizing data integrity.

New Expectations for CIOs

Executives increasingly expect IT leaders to act as strategic partners, guiding how resilience investments are prioritized, measured, and communicated at the business level. Organizations that embrace this shift benefit from stronger alignment, faster recovery, and improved efficiency.

CIOs must now step into this broader role by:

- Aligning technology with business outcomes such as uptime, cost savings, and secure Generative AI adoption.
- Championing unified platforms to leverage existing investments, reduce redundant tools, cut costs, streamline operations, and make hiring IT talent easier.
- Translating risk into financial and operational language for non-technical stakeholders.
- Guiding executive teams through disruption, balancing cost containment with resilience readiness.

5 Key Questions Executives Ask IT Leaders

1. How resilient are we?
2. Are our AI initiatives introducing new risks?
3. Where can we cut costs without increasing risk?
4. Are we compliant and audit-ready?
5. Do we have the right people and processes in place?

The Resilient CIO

The CIO role is no longer about managing servers or overseeing vendors. It's about leading business resilience across the IT estate; balancing cost containment, scalability, and risk readiness. CIOs who step into this role drive value in three ways:

Efficiency
Consolidating platforms and adopting solutions like DaaS lowers redundancy and unlocks measurable cost savings, especially around maintenance efforts like patching.

Control
Unified visibility across the IT estate strengthens governance and reduces unmonitored risk.

Continuity
Infrastructure-led resilience ensures the business can withstand disruption and keep operating, no matter the source.

3

AI as a Force of Disruption and Defense

Artificial Intelligence is reshaping how CIOs think about resilience. Its ability to accelerate attacks and enable faster defense makes it both a strategic risk and an essential tool. Within the IT estate, AI can either magnify weaknesses or enhance resilience when governed effectively.

3 AI Risks To Watch For:

1. Over-Privileged Use

AI systems often get granted wider access than they need. According to Deloitte, 58% of organizations report employees using generative AI without restrictions, creating blind spots in data privacy and compliance.[10]

2. Scope Creep & Misuse

AI initiatives launched for narrow use cases frequently expand when they aren't reassessed frequently. Without clear oversight, CIOs risk AI systems being repurposed in ways that increase liability rather than resilience. Gartner's AI TRiSM (Trust, Risk, and Security Management) programs control this kind of drift.[11]

3. Overconsumption & Hidden Costs

Generative AI is resource intensive. A single rogue workload can consume $100,000.00 per day in real cost to IT leaders. MIT estimates that training a single large AI model can consume millions of liters of water for cooling and drive up energy use significantly.[12] IDC adds that by 2025, AI workloads will account for more than 10% of total enterprise IT energy demand.[13] Overconsumption not only drives up financial costs but also raises sustainability concerns.

AI as an Advisor: Turning Data Into Actionable Insight

If AI as an Antagonist highlights the risks, AI as an Advisor underscores the opportunity. For CIOs, the value of AI lies in its ability to transform overwhelming volumes of alerts and outages and turn help desk tickets into prioritized, actionable intelligence. By summarizing incidents, identifying root causes, and highlighting business impact, AI enables faster, more accurate decision-making that keeps operations running smoothly even under pressure.

IBM reports that organizations using AI-driven security and automation cut the average time to identify and contain a breach by 156 days compared to those without it.[14]

Improving IT Service & Support

Beyond the SOC (Security Operations Center), AI also improves day-to-day resilience through IT operations. By analyzing large volumes of help desk tickets, AI can:

- Summarize and categorize issues, making patterns easier to spot.
- Translate technical jargon into clear, business-ready language.
- Recommend next steps to both end users and IT teams, reducing ticket resolution time.

This advisory role reduces pressure on overworked teams and allows CIOs to redeploy talent to higher-value activities.

AI as an Apprentice: Automating the Fundamentals

If the CIO's challenge is balancing speed and control, *AI as an Apprentice* provides a practical solution: automating repetitive, well-defined tasks that drain time and resources.

Streamlining Repetitive Work

Patching, log analysis, and system monitoring are critical but time-consuming. By applying AI to these activities, CIOs can accelerate cycles, reduce human error, and free staff for higher-value work. Gartner notes that through 2026, organizations using security AI and automation will see 40% faster remediation of vulnerabilities compared to those relying on manual processes.[15]

Enabling Faster Recovery

AI can also play a role in disaster recovery. From automating backup validation to predicting system dependencies, AI reduces recovery times and ensures consistency. IDC reports that enterprises deploying AI-driven resilience tools experience 20–30% faster restoration of critical systems after an outage.[16]

Only 20% of organizations express confidence in their ability to secure their generative AI models against cyber risks.[10]

Generative AI vs. Agentic AI: The Dual-Edged Sword

Generative AI

Security Risk: Reduces the skill barrier for attackers, enabling sophisticated attacks at scale.

Resilience Reward: Classification and summary allow overburdened teammates to make tech decisions and act faster.

Agentic AI

Security Risk: Reduces the skill barrier for attackers, enabling sophisticated attacks at scale.

Resilience Reward: Enables leaders to automate repetitive tasks and allow expensive talent to focus on what matters.

Measuring AI's Impact

Shadow AI

20% of organizations reported a breach tied to unsanctioned AI tools, adding **$670K** in costs.[17]

Defensive Payoff

IBM found that organizations using AI extensively saved **$1.9M** per breach and shortened breach lifecycles by **80** days.[18]

Offensive Risk

16% of breaches in 2025 involved AI, with phishing (**37%**) and deepfake impersonation (**35%**) as leading methods.[19]

> "Business leaders know the key to thriving in adversity is building strong, adaptable teams, processes, and technologies. Leaders expect their infrastructure to operate the same way; keeping the business open and profitable in the face of adversity."
>
> **– Stephen Semmelroth, VP of Cyber Resilience at AVANT**

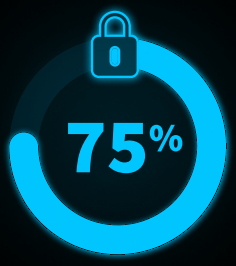
Making AI Safe to Scale: A Practical Framework

AI adoption can introduce new risks such as Shadow AI, sensitive data fed into public models, or attackers exploiting weak guardrails. To scale responsibly, many organizations are adopting Gartner's AI TRiSM (Trust, Risk, and Security Management) framework. TRiSM is a structured approach to manage AI's risks, ethics, and compliance.

The framework organizes governance into four pillars that guide IT and security leaders in embedding transparency, accountability, and continuous oversight into their AI systems.

1. **AI Governance**
   Establish cross-functional teams, policies (e.g., AI Acceptable Use), and an enterprise AI catalog.
2. **AI Runtime Inspection & Enforcement**
   Run real-time checks to block harmful uses and enforce policies.
3. **Information Governance**
   Implement strong data classification, access control, and lifecycle management.
4. **Infrastructure Security**
   Deploy Zero-trust protection for APIs, model weights, and runtime environments.

Neither GenAI nor Agentic AI are experimental technologies. CIOs must now manage both sides of the equation: curbing the risks of Shadow and adversarial AI while leveraging governed AI to drive efficiency, improve visibility, and keep the business operating through disruption. CIOs will continue to feel substantial pressure for change and adaptability.



By 2026, Gartner predicts that 75% of enterprises will adopt AI TRiSM programs.[12]

4 Strategic Imperatives for IT and Risk Leaders

CIOs face mounting pressure to deliver measurable value to the business. Budgets are under scrutiny, boards are watching closely, and the attack surface continues to expand. To succeed, leaders must align their strategies to three imperatives that balance security with business outcomes: performance, resilience, and agility.

Performance – Eliminate inefficiency, maximize ROI

Executives are demanding evidence that every dollar spent on IT drives results. Yet, Gartner estimates that nearly 40% of security spend and an additional substantial IT cost is wasted on underutilized or duplicated tools.[21]

- CIOs should consolidate on unified IT platforms that can also drive security outcomes, reduce overlap, cut license costs, and give teams more time to focus on resilience instead of tool management. By doing so, IT leaders can save on the order of 15% of annual IT estate costs and rationalize between 1-5% of total IT spend that would have otherwise been spent on security tooling.[22]

Resilience – Shift from protection to adaptation

Leaders are recognizing that incidents are inevitable, but disruption doesn't have to be catastrophic. Companies with strong resilience strategies reduce the impact of a major cyber incident by up to 48%.[23]

- Protect "crown-jewel" assets first, adopt a "bend, don't break" mindset into operations, and share accountability across business units and supply chains.

Agility – Adapt to disruption without losing momentum

Agility requires reprioritizing roadmaps as regulations shift, partnering across functions for collaborative risk management, and resetting data security programs for new digital environments. According to IDC, 72% of enterprises with agile programs report faster digital transformation, underscoring the competitive advantage agility provides.[24]

- CIOs can embed agility into vendor contracts and cloud strategies, ensuring that when disruption hits, the IT estate can scale up or pivot quickly without derailing business continuity.

The 2025 IT Leadership Mandate

Performance

Focus:	Actions for Leaders:	Supporting Insight
Streamline and maximize ROI	• Consolidate redundant tools • Use AI/automation to optimize processes • Prioritize staff well-being to reduce burnout	**87%** of technology executives plan to increase cyber/ information security funding in 2025 - Gartner

Resilience

Focus:	Actions for Leaders:	Supporting Insight
Shift from protection to adaptation	• Protect crown-jewel assets first • Share accountability across departments and supply chains • Embed a “bend, don’t break” mindset into culture	Resilience ranked as the **#1** functional priority for CISOs in 2025 - Gartner

Agility

Focus:	Actions for Leaders:	Supporting Insight
Adapt without losing monentum	• Reprioritize roadmaps when threats/ regulations shift • Partner across functions for collaborative risk management • Reset data data governance programs for new environments	Estimates vary, but studies show between **80-90%** have an AI initiative that is driving change in the IT estate. - Gartner

Adapted and modified from Gartner (2025) — Leadership Vision for Security & Risk Management

5 The Resilience Dividend: Cutting Costs Without Adding Risk

Organizations have a sharpened focus on cost control. Economic uncertainty, AI disruption, and global trade pressures have created a climate where large-scale technology investments are delayed, and every budget line is under review. The result is a “wait-and-see” mindset; one where growth initiatives often take a back seat to cost containment.

But cutting costs without a strategy can create hidden risks. Overlapping tools, underutilized platforms, and deferred security investments can leave organizations more exposed just as threat actors are scaling their capabilities with AI. The resilience dividend comes from doing both—cutting vendor sprawl, streamlining operations, and eliminating waste while strengthening the ability to withstand, recover, and adapt to disruption. Companies that embed resilience into cost strategies not only lower total spend but also preserve trust, stability, and long-term competitiveness.

Strong cost containment and consolidation allows leaders the adaptability to make larger, more meaningful changes when appropriate because they have reduced their operational risk.

Resilience as a Business Value Multiplier

In a climate where budgets are tight and risks keep rising, executives want proof that security investments also enable efficiency and growth. Business resilience is increasingly recognized as a strategic driver of value, delivering measurable gains across three dimensions:

Operational Efficiency

Enterprises that consolidate tools can lower annualized security-related costs by up to 10% while making teams 34% more efficient.[25]

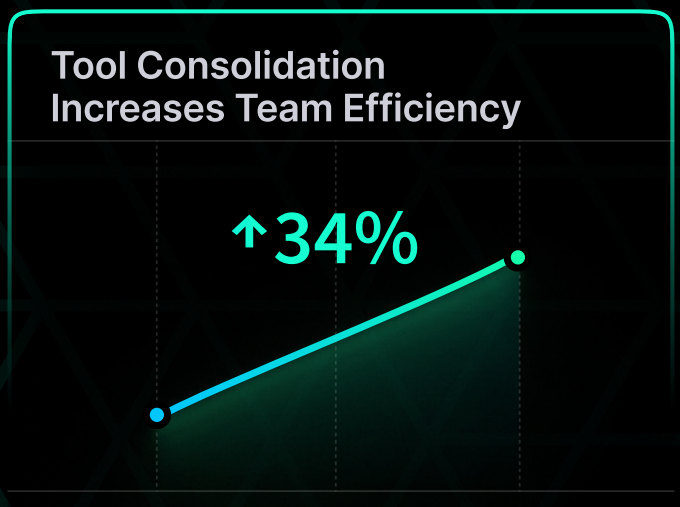
Risk and Loss Avoidance

According to the ASD Essential Eight (ASD 8), developed by the Australian Cyber Security Centre, the eight most powerful security outcomes are owned by CIOs.[26]

- Application Control
- Patch Applications
- Configure Microsoft Office Macros
- User Application Hardening
- Restrict Administrative Privileges
- Patch Operating Systems
- Multi-Factor Authentication
- Regular Backups

Sustainable Performance

Organizations that embed resilience into operations report up to 30% lower disruption costs after an attack—positioning them not only to withstand uncertainty but to rebound faster and maintain business continuity.[27]



6 The Trusted Advisor's Role: Guiding the Journey to Resilience

Expertise and Simplification

Trusted Advisors bring deep, specialized knowledge of the security landscape, helping clients cut through the noise and simplify complex decisions.

Objectivity and Rationalization

A Trusted Advisor provides an objective, third-party perspective, helping clients navigate the "platform vs. point solution" dilemma and design an integrated architecture that is both effective and cost-efficient.

Resources and Portfolio Access

Trusted Advisors have access to powerful resources and tools, like AVANT's Pathfinder, which aids in systematically assessing a client's needs and matching them with vetted technology vendors.

Business Acumen and Justification

Perhaps most critically, the Trusted Advisor helps bridge the gap between the security leaders and their executives and boards, translating technical requirements into a compelling, ROI-driven business case.

The critical role of the channel is validated by AVANT's own market research, which shows that **68% of companies rely on Trusted Advisors for the security component of cyber resilience.**

Conclusion

The conversation about cybersecurity has changed into one of resilience, continuity, and trust. Leaders now recognize that that cyber criminals, insider threats, and operational mistakes will cause disruptions. The question isn't whether disruption will occur; it's whether the business can continue to operate when it does.

Contributors

This report is brought to you by AVANT Analytics, a division of AVANT, where our mission is to provide timely research and insights for today's new and emerging technology services, including live and on-demand reports, podcasts, briefings, and alerts with the goal of accelerating technology decision making.

Alex Danyluk – Managing Director
Allison Bergamo – Author
Stephen Semmelroth – VP of Cyber Resilience
Rick Mischka – Cybersecurity Engineer
Juan Ochoa – Senior Data Analyst and Researcher
Emilio Alvarado – Data Analyst and Researcher
Melissa Joy Kong – Editor
Amy Ridder – Editor
Jay Sojdelius – Creative Director
Nadir Mian – Designer

Sources Appendix

1. Gartner – Top 3 Strategic Priorities for Security and Risk Management Leaders, 2025. Link
2. Accenture – State of Cybersecurity Resilience 2025.
3. IBM – Unify Your Fragmented Security.
4. Gartner – Top 3 Strategic Priorities for Security and Risk Management Leaders, 2025.
5. IBM – Cost of a Data Breach Report 2025.
6. IBM – Unify Your Fragmented Security.
7. IBM – Unify Your Fragmented Security.
8. IBM – Capturing the Cybersecurity Dividend.
9. IBM – Capturing the Cybersecurity Dividend.
10. Deloitte – State of Generative AI in the Enterprise 2024.
11. Gartner – AI in Cybersecurity: Define Your Direction.
12. 1MIT Technology Review, 2023.
13. IDC – Future of Digital Infrastructure, 2025.
14. IBM – Cost of a Data Breach Report 2025.
15. Gartner – AI in Cybersecurity: Define Your Direction.
16. IDC – Resilience in Digital Infrastructure, 2025.
17. IANS Research – State of the CISO 2025.
18. IBM – Cost of a Data Breach Report 2025.
19. World Economic Forum – Global Cybersecurity Outlook 2025.
20. IANS Research – State of the CISO 2025.
21. Gartner – AI in Cybersecurity: Define Your Direction.
22. Gartner – Top 3 Strategic Priorities for Security and Risk Management Leaders, 2025.
23. IBM – Unify Your Fragmented Security.
24. Accenture – State of Cybersecurity Resilience 2025.
25. IDC – Future of Digital Infrastructure, 2025.
26. Australian Cyber Security Centre – Essential Eight Explained
27. Accenture – State of Cybersecurity Resilience 2025.
28. Accenture – State of Cybersecurity Resilience 2025.