Gartner Insights

Cybersecurity Turbulence in 2025: 7 Forces That Will Threaten Your Organization

Marty Resnick, William Dupre, Chris Silva, James Hoover,
Pedro Pablo Perea de Duenas, Akif Khan

Gartner®

Cybersecurity Turbulence in 2025: 7 Forces That Will Threaten Your Organization

15 July 2025 - ID G00834670 - 23 min read

By: Marty Resnick, William Dupre, Chris Silva, James Hoover, Pedro Pablo Perea de Duenas, Akif Khan

Initiatives: Cyber Risk; Innovate with Emerging Technologies Adoption; Meet Daily Cybersecurity Needs

> Risks not only arise from technology, but also in political, social, economic, trust, regulatory and environmental areas. Security and risk management leaders must integrate these insights into threat assessment processes to address the evolving, expanding and complex threat landscape.

Overview

Opportunities

- Cybersecurity leaders have the opportunity to drive greater efficiency and effectiveness by rationalizing and integrating their security toolsets. By advocating for consolidation and reducing tool sprawl, they can improve team productivity, reduce complexity and enhance overall security posture.
- With shifting geopolitical landscapes and evolving alliances, cybersecurity leaders can proactively diversify and strengthen their threat intelligence sources. This is an opportunity to build more resilient, adaptive intelligence programs that do not rely solely on traditional partners, ensuring continued situational awareness.
- Amid economic uncertainty and frequent policy changes, cybersecurity leaders can champion flexible, risk-based investment strategies. By aligning security spending with business priorities and demonstrating value, they can position cybersecurity as a business enabler even during turbulent times.
- As tensions grow between organizational controls and workforce sentiment, cybersecurity leaders have an opportunity to engage employees as partners in security. By promoting transparency, empathy, and user-friendly controls, they can bridge divides and cultivate a security-aware culture.
- With CISOs increasingly involved in cross-departmental fusion teams, cybersecurity leaders can take the lead in integrating cyber risk with broader business, legal and reputational concerns. This holistic approach positions them as strategic partners in enterprise risk management.
- Given their central role in regulatory adaptation, cybersecurity and SRM leaders can use this as an opportunity to advocate for greater collaboration and shared ownership across departments. By fostering alliances with other business units, they can drive more effective and supported compliance initiatives.
- As AI and technology adoption accelerates, cybersecurity leaders can proactively address emerging risks such as power grid strain. By leading the development of robust cyber resilience and protection architectures, they can safeguard the organization against new classes of technology-driven threats.

Recommendations

- Evaluate the impact of single-purpose tools based on novel information or actions these tools can empower and based on these tools' capability to integrate into other, critical cybersecurity workflows.
- Work with cybersecurity vendors to understand where their threat intelligence is being sourced. Partner with them to make sure that intelligence is not disrupted as geopolitical events disrupt government sources.
- Explore more cloud-based solutions and shift from a capex to a more opex model. As trade becomes more uncertain, access to physical equipment may be restricted or drive up costs.
- Take a human-centric approach to cybersecurity control selection and design. Don't confuse workplace productivity demands with cybersecurity risks.
- Engage with disinformation cybersecurity vendors who can monitor web and social channels for narratives about your organization and categorize them by risk based on characteristics of how they are being spread and the nature of the content.
- Integrate cybersecurity compliance into existing governance forums (such as cybersecurity committees) by designating a regular agenda item for regulatory updates.
- Proactively update and test business continuity, disaster recovery and incident response plans to explicitly include scenarios such as blackouts, brownouts or grid-targeted attacks.

Strategic Planning Assumptions

Technological: By 2027, cybersecurity organizations that unite email security, endpoint security and SSE tools in a workspace security platform will experience 50% fewer successful cyberattacks than peers using siloed solutions.

Political: By 2027, Europe and the Middle East will have overtaken the U.S. as focal points for cyberthreat intelligence.

Economic: By 2026, cybersecurity leaders will put off necessary cybersecurity purchases due to trade restrictions, which will negatively impact risk visibility and vulnerability management efforts.

Social: By 2028, cybersecurity leaders will face increased resistance from the workforce to new controls, leading to a 50% increase in time to deploy new cybersecurity tooling.

Trust: By 2027, the share price of a global enterprise will have experienced a 25% drop as the result of an online disinformation attack, prompting one-quarter of the Global 2000 to engage with disinformation security vendors.

Regulatory: By 2027, cybersecurity leaders will spend 40% of their time managing and reporting on their organization's adaptation to new or revised regulatory requirements related to cybersecurity.

Environmental: By 2028, a prolonged power outage will cause at least one major cybersecurity attack to receive a delayed response, resulting in serious business consequences for the affected organization.

What You Need to Know

Security and risk management (SRM) leaders, including CISOs, are increasingly facing risks stemming from motivations beyond traditional cyberthreats that expand the attack surface unpredictably. Such threats create organizational turbulence marked by rapid, emerging threats, new vulnerabilities, and evolving attack methods. In this volatile environment, adaptive and resilient cybersecurity controls are imperative to effectively safeguard systems and data. Immediate actions based on strategic foresight are essential to navigate and mitigate these complex challenges.

Threats could come from all areas of what Gartner refers to as "tapestry" (technological, political, economic, social, trust, regulatory and environmental) . In order to survive and thrive in this fragmented world, SRM leaders need to think beyond just technology threats.

These are not specific threat vectors. Rather, they are forces and macrotrends that could lead to threats for SRM leaders. For more information on specific threat vectors, see How to Respond to the 2025-2026 Threat Landscape.

The seven threats detailed in this research (listed in Figure 1, the Table of Contents and in the attached downloadable PowerPoint deck) must be mitigated against to stabilize the organization in the midst of turbulence and enable it to thrive.

Figure 1: 7 Forces That Will Threaten Your Organization



Source: Gartner
834670

Gartner

Table of Contents	
Technological	“Best-of-Breed” Yields Response Inefficiency
Political	Global Intel-Sharing Is Disrupted by Private Industry
Economic	Policy Chaos Will Impact Cybersecurity Purchasing Decisions
Social	Fractured Workforce Relations Cause Increased Resistance to Security Controls
Trust	Disinformation Defense Becomes a CISO Priority
Regulatory	Policy Distractions Stretch Security Teams Thin
Environmental	Energy Instability Causes Massive Exposure to Cyber Resilience

Technological: “Best of Breed” Yields Response Inefficiency

Return to Table of Contents

Analysis by Chris Silva

Velocity: Uniform

Time: 25 to 36 months

Likelihood: Probable

Turbulence: Moderate

SPA:

By 2027, cybersecurity organizations that unite email security, endpoint security and SSE infrastructure tools in a workspace security platform will experience 50% fewer successful cyberattacks than peers using siloed solutions.

Description:

The average cybersecurity team is working across a portfolio of, on average, over 40 tools on a daily basis. This is due in part to internal politics and the need to secure niche technology. The addition of each individual tool saps overall effectiveness. According to the 2025 Verizon Data Breach Investigations Report, exploits of misconfiguration represent 45% of basic web app attacks, trivial avenues of exploit for attackers that can undermine overall defensive posture. [1]

The Gartner Technology Adoption Roadmap for Large Enterprises for 2025 showed respondents use an average of 45 cybersecurity tools. That towering stack of technology demands more operational time with each added tool, due to the additional complexity, cost and time of integrating and managing these tools. Add to this the likelihood of human error when trying to replicate ideal conditions, controls, reporting and visibility across such a vast estate of tools. For more, see Infographic: 2025 Technology Adoption Roadmap for Security and Risk Management.

Why Trending:

Each cybersecurity tool's unique value is undercut by its individual complexity and management interface. Navigating across multiple, discrete dashboards increases response time in the midst of an incident and escalates operational costs. Fewer tools will by default mean lower costs, but raises risks that there are unaddressed gaps by a vendor and/or concentration risks that increase an organization's exposure to threats.

If the use of niche tools is allowed to propagate with no central control, overall security operations center (SOC) efficiency will decrease. The increased availability of AI for attackers to automate and scale early-stage investigations allow for the discovery of misconfigurations. This accelerates the pace that attackers can discover misconfigurations and vulnerabilities and lower the barrier to entry for novice threat actors, a critical weakness for teams struggling to combine signals from multiple discrete tools.

Implications:

Short-term: Vendors with multiproduct platforms gain market share as buyers optimize their portfolio of tools for efficiency, though there are still multiple tools in play. Investments shift from new-to-market, niche technologies to ones that drive data and product signal integration. Organizations that fail to focus the adoption of new cybersecurity tools around integration and data sharing with existing tools will experience decreased efficiency in cybersecurity operations. The less-efficient SOC paired with fragmented visibility across multiple tools will lead to exploitable avenues of attack being left unaddressed and the organization's risk of attack growing as a result.

Long-term: The number of tools in use by SOCs will diminish as established vendors expand their offerings by building or acquiring novel features, allowing consolidation to tools from key technology suppliers. Achieving optimization is still a future state for the majority of organziations. Maintenance and administration continue to consume more working time, undercutting defenses and raising operational costs. Comparing findings, alerts and tasks across multiple consoles introduces human error and distraction, and defenses appreciably weaken over time.

Actions:

- Evaluate functional areas for optimization with existing key vendors, focus on integration of data from remaining third-party tools to facilitate seamless information sharing across cybersecurity tools, reducing information silos and enhancing overall cybersecurity posture.
- Assess data ingest and retention needs: Conduct a thorough analysis of annual data ingest and retention requirements across and among critical cybersecurity tools to accurately forecast future needs and foster information sharing among existing tools.
- Evaluate the impact of single-purpose tools based on novel information or actions these tools can empower and based on these tools' capability to integrate with other critical cybersecurity workflows.

Further Reading:

Forecast Analysis: Information Security, Worldwide

2025 Strategic Roadmap for Workspace Security

Securing Hybrid Work: Adopting the Right Workspace Security Strategy

Political: Global Intel-Sharing Is Disrupted by Private Industry

Return to Table of Contents

Analysis by William Dupre

Velocity: Accelerating

Time: 0 to 24 months

Likelihood: Likely

Turbulence: Critical

SPA:

By 2027, Europe, the Middle East and private industry will have overtaken the U.S. as focal points for cyberthreat intelligence.

Description:

The post-WWII alliances are evolving with isolationism and nationalism becoming more dominant. Transactional alignments, like one-off trade agreements as a condition of military assistance, will become the norm, creating geopolitical instability and increasing both kinetic and cyber conflict. Waning trust between traditional allies will disrupt cyberthreat intelligence sharing and increase risk for organizations.

The changes in geopolitical stability will have ripple effects across the cybersecurity landscape. Due to policy shifts affecting traditional Western allies, confidence in threat intel sources will wane. Trust between countries and regions will shift away from the U.S. toward Europe and the Middle East. These areas have growing and innovative threat-intelligence practices, which may attract the attention of organizations as the U.S. becomes a less reliable source.

Why Trending:

Recent tensions within existing political alliances are impacting how threat data is shared across countries and regions. Private industry and vendors are now collecting and seeing as much threat information as governments. In one possible future scenario, private industry takes over and becomes the gatekeeper of threat intelligence.

Implications:

Short-term: As transatlantic alliances — such as those between the United States, the United Kingdom and European Union member states — are strained, the immediate impact will be a significant restriction on established intelligence-sharing activities. Traditionally, these alliances have relied on robust, trusted channels for exchanging critical information on cybersecurity threats, terrorism, cybercrime and state-sponsored malicious activities.

Long-term: Centers of threat intelligence will shift to Europe and the Middle East, with the U.S. becoming less dominant. SRM leaders will have to look to additional sources for threat intelligence and guidance (as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) loses its relevance and influence). [1]

Actions:

- Examine your sources of threat intelligence and how threat intelligence is currently used within your organization. Determine the impact of possible disruptions to or loss of confidence in those feeds.
- Work with cybersecurity vendors to understand where their threat intelligence is being sourced. Partner with them to make sure that intelligence is not disrupted as geopolitical events disrupt government sources.
- Look for a diversity of threat intelligence sources to ensure that if attribution is necessary it can be verified effectively.

Further Reading:

- Quick Answer: Evolving State and Local Government Cybersecurity in Response to U.S. Federal Signals
- Guidance Framework for Using Threat Intelligence

Economic: Policy Chaos Will Impact Cybersecurity Purchasing Decisions

Return to Table of Contents

Analysis by William Dupre

Velocity: Accelerating

Time: 0 to 24 months

Likelihood: Likely

Turbulence: Critical

SPA:

By 2026, cybersecurity leaders will put off necessary cybersecurity purchases due to trade restrictions, which will negatively impact risk visibility and vulnerability management efforts.

Description:

A tariff war has begun and governments around the world are putting in place new trade and economic policies, mostly driven by a response to changes in U.S. trade policy. The U.S. alone is transforming its governing relationships both domestically and internationally. The changes are causing economic uncertainty as businesses try to keep up with the ever-changing landscape of policies. Where to continue to invest and what solutions to bring in or outsource will become uncertain as policy shifts create chaos.

Why Trending:

U.S. economic policy is being reinvented in a very short period of time. With tariffs and the destruction of trade agreements, global trade will see a dramatic slowdown. [2] [3]

Implications:

Short-term: The daily proliferation of executive orders and policy changes, as well as tariff discussions, will create uncertainty in the U.S. and world economies. Companies will find it hard to make long-term economic decisions, which may impact purchasing, including purchases in the cybersecurity space.

Long-term: If near-term buying decisions are put off due to economic concerns, long-term cybersecurity could be impacted. Organizations may be ill-prepared for future cyberthreats if the necessary technology and resources are not available. Also, long-term cybersecurity decisions could be impacted as global alliances shift and supply chains are impacted, as well as, in many cybersecurity cases, tools outside of certain geographic areas being hard to find or not enterprise-grade.

Actions:

- Inventory cybersecurity solutions to determine what could be impacted by trade disruptions. Identify high-risk solutions that could require significant budget adjustments as those vendors raise prices or discontinue services or features. Establish an alternate vendor strategy and identify strategic vendors who need replacement.
- Explore more cloud-based solutions and shift from a capex to a more opex model. As trade becomes more uncertain, access to physical equipment may be restricted or drive up costs.

Further Reading:

- How CIOs Can Manage the Geopolitical Risks of Cloud Deployments
- Quick Answer: Protecting Geopolitically Risky Cloud Workloads

Social: Fractured Workforce Relations Cause Increased Resistance to Security Controls

Return to Table of Contents

Analysis by James Hoover

Velocity: Accelerating

Time: 25 to 36 months

Likelihood: Likely

Turbulence: Critical

SPA:

By 2028, more than half of cybersecurity leaders will face increased resistance from the workforce to new controls, leading to a 50% increase in time to deploy new cybersecurity tooling.

Description:

Relationships between the organization and the people that make up the workforce are under increasing pressure. It becomes existential that SRM leaders take human-centric approaches to avoid vicious cycles that exacerbate this rift. Resistance to controls that are perceived as invasive or onerous is likely to increase this divide.

Why Trending:

Cybersecurity depends on trust and collaboration, not just technology and enforcement. If SRM leaders fail to adapt, organizations risk entering a vicious cycle: the more controls are tightened without employee buy-in, the more employees push back, further weakening cybersecurity and organizational cohesion. This makes it critical for SRM leaders to prioritize empathy, communication and user-friendly solutions — transforming cybersecurity from a source of friction into a shared responsibility.

Implications:

Short-term: Increased workforce resistance or bypass of controls perceived as onerous or invasive. Increased push from management to implement workforce surveillance tools with little to no meaningful cyber benefit. [4]

Long-term: Over the past several years, there has been a significant shift in how employees view their relationship with work and their employers — a change that holds critical implications for SRM leaders. [5] This transformation, fueled by the rise of remote and hybrid work, heightened awareness of mental health, and a stronger emphasis on work-life balance, is reshaping the risk landscape and the expectations placed on security teams.

For SRM leaders, this new dynamic demands a fundamental rethinking of how workforce security and trust are managed. The traditional boundaries of the corporate network have dissolved, requiring cybersecurity programs that respect employee privacy, support flexible work arrangements and foster a culture of trust. Employees now expect cybersecurity controls that are not only effective but also minimally intrusive and supportive of their well-being.

Failing to adapt can result in increased insider risk, higher turnover among skilled cybersecurity staff, and reputational damage (and financial penalties, depending on region) from privacy missteps. As such, SRM leaders must lead with empathy and agility, ensuring that cybersecurity policies and technologies align with evolving workforce expectations while still protecting the organization's critical assets. Recognizing that the traditional employer-employee relationship is being fundamentally redefined is essential for building resilient, secure and trusted digital workplaces.

Actions:

- Take a human-centric approach to cybersecurity control selection and design. Don't confuse workplace productivity demands with cybersecurity risks.
- Include analysis of the social and lifestyle impacts of cybersecurity controls on both customers and employees to more accurately assess how these measures are received and adopted.
- Resist calls for cybersecurity theater — security measures that give the appearance of being secure without actually providing meaningful protection — especially at the expense of relationships with your broader user community.

Further Reading:

- 5 Communications Tactics to Get People to Take Cyber Risk More Seriously
- Tool: Security Behavior and Culture Program Dashboard

Trust: Disinformation Defense Becomes a CISO Priority

Return to Table of Contents

Analysis by Akif Khan

Velocity: Accelerating

Time: 0 to 24 months

Likelihood: Possible

Turbulence: Moderate

SPA:

By 2027, the share price of a global enterprise will have experienced a 25% drop as the result of an online disinformation attack, prompting one-quarter of the Global 2000 to engage with disinformation security vendors.

Description:

The public cannot necessarily trust what they see and hear about your organization. The rise of narrative attacks and information warfare is resulting in disinformation being propagated about organizations. Examples include use of social media, chat forums and Telegram channels to spread messages to attack an organization (e.g., short the share price based on false news, malicious attacks, political attacks based on geopolitical friction, spreading malware to unsuspecting customers) . Dealing with disinformation that can impact business operations is a challenge with no clear owner.

From conversations with clients, Gartner has observed that CISOs are increasingly being pulled into C-level fusion team approaches. These involve legal, marketing, branding, risk and even physical security considerations (e.g., are execs under threat due to disinformation) in an attempt to identify threats, understand business impacts and develop mitigation strategies. Disinformation includes GenAI deepfakes and fabricated content that alters context.

Why Trending:

Attackers have observed how state actors have been able to manipulate public discourse and attempted to influence elections using malicious narratives online. GenAI and other tools for creating malicious content are now readily available to many types of bad actors, and use of social media botnets is now a commodity sold on the dark web.

Implications:

Short-term: Although this is a multidisciplinary challenge with no clear owner, CISOs will need to partner with chief marketing officers on short-term activities such as proactive monitoring to assess whether narrative attacks are taking place. CISOs will need to engage with vendors in the emerging market of disinformation and narrative intelligence to build up a picture of how an organization is being portrayed and discussed online. This goes beyond typical PR sentiment analysis and will need to involve analysis of the networks of social media accounts, websites and Telegram channels involved to discern between natural organic information dissemination vs. malicious artificially boosted spreading of information. This is difficult to achieve without the use of specialist vendors — CISOs are well-positioned to procure such vendor services accordingly, although the source of the budget for such tools will be contentious.

Long-term: Work with senior leaders responsible for corporate reputation and communications to formulate a response playbook for dealing with narrative attacks. This could include a wide range of approaches, such as introducing counter-narratives, not responding but adjusting cybersecurity posture, adjusting the cybersecurity posture of executives specifically, reporting to social media platforms with a view to having offending accounts taken down and more. Many, but not all, of these activities will be outside of the CISO's remit, but CISOs will need to be heavily engaged.

Actions:

- Accept that as a CISO you will need to play a part in the cross-functional effort to mitigate business risks arising from disinformation and narrative attacks. Due to the overlaps with cybersecurity threat intelligence and the risks associated with disinformation being used as a means to spread malware to users, resulting in credential compromise, cybersecurity teams must play a role in identifying disinformation attacks.
- Engage with disinformation cybersecurity vendors who can monitor web and social channels for narratives about your organization and categorize them by risk, based on characteristics of how they are being spread and the nature of the content. Note that these vendors are not making decisions about whether a narrative is true or false.
- Formulate a playbook for response actions, such as social media account takedown activities, counter-narratives, and improving the cybersecurity and possible physical security posture for your executive team.

Further Reading:

- Top Strategic Technology Trends for 2025: Disinformation Security
- Emerging Tech: Leverage Disinformation Security to Mitigate Influence Operations
- Emerging Tech: Defend the Digital Attack Surface With Disinformation Security

Regulatory: Policy Distractions Stretch Security Teams Thin

Return to Table of Contents

Analysis by Pedro Pablo Perea de Duenas

Velocity: Accelerating

Time: 0 to 24 months

Likelihood: Likely

Turbulence: Critical

SPA:

By 2027, cybersecurity leaders will spend 40% of their time managing and reporting on their organizations' adaptation to regulatory requirements related to cybersecurity.

Description:

SRM leaders are facing increasing pressure, triggered by new regulations like NIS2, DORA and U.S. federal cybersecurity policies. Due to the high cybersecurity and cyber risk management components of these regulations, SRM leaders often end up assuming the main burden for adaptation projects, sometimes finding themselves more isolated than they should be, with limited support from other key departments and business units. [6]

This intense focus on compliance comes at a time when cybersecurity teams are already stretched thin and understaffed, making them insufficiently resourced to take on large compliance projects. As a result, the added pressure can further exacerbate cybersecurity staff burnout, negatively impacting their performance and decision-making abilities. SRM leaders and their teams often have to neglect other important cybersecurity tasks, such as certain security operations, threat intelligence, workforce management, awareness activities and strategic planning.

Why Trending:

The growing wave of cybersecurity-related regulations is reshaping a SRM leader's focus. With most of these mandates heavily focused on elements that SRM leaders oversee, whether it is core items in a cybersecurity program or adjacent areas where cybersecurity teams share responsibilities, SRM leaders are being pushed to carry most of the weight of the regulatory adaptation efforts, adding pressure that exacerbates burnout and sometimes in isolation.

Implications:

Short-term: SRM leaders are forced to choose between core critical operational duties and compliance responsibilities as regulatory adaptation dominates their agenda, given the strong focus of these regulations on cybersecurity and adjacent areas of responsibilities for SRM leaders.

Long-term: If this imbalance continues, organizations will gradually erode the strategic value of the SRM leader. Instead of focusing on building cybersecurity capabilities and anticipating emerging risks, SRM leaders could become primarily responsible for managing and adapting regulatory updates. This shift can lead to a compliance-driven cybersecurity posture where excessive time spent on evidence gathering, control testing, policy creation and documentation comes at the expense of operationalizing security, ultimately undermining real risk reduction.

Actions:

- Integrate cybersecurity compliance into existing governance forums (such as cybersecurity committees) by designating a regular agenda item for regulatory updates. Use these forums not only to track its progress but also to highlight impacts and escalate resource needs, shifting from a reactive approach to proactive one.
- Enhance cybersecurity regulatory compliance and oversight through automation and integration by utilizing Cyber GRC to streamline the compliance process, tracking progress and demonstrate compliance, and Continuous Control Monitoring capabilities to reduce tedious and manual efforts to get near real-time visibility into the effectiveness of certain requirements.

Further Reading:

- 2025 Strategic Roadmap for Cyber GRC
- Innovation Insight: Cyber GRC Streamlines Governance
- The Cybersecurity Leader's Playbook: Navigating the NIS2 Directive

Environmental: Energy Instability Causes Massive Exposure to Cyber Resilience

Return to Table of Contents

Analysis by James Hoover

Velocity: Accelerating

Time: 25 to 36 months

Likelihood: Probable

Turbulence: Critical

SPA:

By 2028, a prolonged power outage will cause at least one major cybersecurity attack to receive a delayed response, resulting in serious business consequences for the affected organization

Description:

An overload in AI usage/technology usage has the potential to cause strain on the power grid, causing massive exposures in an organization's cyber resilience and/or protection architectures. Power availability issues will become mainstream, and SRM leaders must prepare to address availability in a world in which regular blackouts or brownouts are to be expected. This may change the calculus on distribution of energy, ultra high availability, or adoption of net new technology. Energy demand will need to be baked into requirements and weighed against the tangible value provided by a given technology. [8]

Why Trending:

SRM leaders are not only dealing with widescale third-party (such as hyperscaler) outages, but also increased cyber attacks because the mean time to contain/detect rises exponentially during pervasive power failures.

Implications:

Short-term: Cybersecurity teams need to run simulated scenarios, ensure resilience exercises account for power interrupting events, and ensure they manage third-party concentration risk in the event of a large third-party outage, including the use of backup generators while isolating and containing any incidents.

Long-term: Organizational goals focused on the adoption of new technology will need to be justified on the basis of energy consumption, as well as on business impact analysis and recovery time objectives, to ensure appropriate backup power is available, and critical assets are accounted for and protected during a large-scale power outage.

Actions:

- Ensure BIAs capture key facilities and third parties for power and telecommunications, especially if the organization is deemed to be critical national infrastructure (CNI).
- Proactively update and test business continuity, disaster recovery and incident response plans to explicitly include scenarios such as blackouts, brownouts or grid-targeted attacks.
- Incorporate energy consumption and grid dependency as explicit criteria in technology procurement, deployment and life cycle management decisions.

Further Reading:

- Quick Answer: Minimizing Business Impacts From IT Infrastructure Disruptions
- How to Perform a Business Impact Analysis
- Toolkit: Expeditors for Performing a Business Impact Analysis

Evidence

[1] 2025 Verizon Data Breach Investigations Report (page 90), Verizon.

[2] CISA Loses Nearly All Top Officials as Purge Continues, Cybersecurity Dive.

[3] OECD Economic Outlook, Volume 2025 Issue 1: Tackling Uncertainty, Reviving Growth, OECD.

[4] Global Economic Outlook Shifts as Trade Policy Uncertainty Weakens, OECD.

[5] 65% of Employees Bypass Cybersecurity Measures, New Study Finds, Forbes.

[6] From Burnout to Career Stagnation: 7 Reasons Why Young Employees Are Walking Away From In-Office Jobs, The Times of India.

[7] Breaking Down Silos in Cybersecurity, Help Net Security.

[8] Smaller Nuclear Reactors Spark Renewed Interest in a Once-Shunned Energy Source, Stateline.

[9] World Environment Day: CISO Checklist, Economic Times, CISO India.

Acronym Key and Glossary Terms

Brownout	A temporary reduction in voltage in an electrical power supply system, often caused by high demand or grid issues

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Tapestry Predicts 2025: Geopolitical Unrest

Tapestry Predicts 2025: Transforming Humanity

Gartner Futures Lab Podcast: Future of Identity

Gartner Futures Lab: The Future of Identity

© 2025 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's business and technology insights organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Although Gartner publications may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by the Gartner Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its business and technology insights organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner insights may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Table of Contents	
Technological	“Best-of-Breed” Yields Response Inefficiency
Political	Global Intel-Sharing Is Disrupted by Private Industry
Economic	Policy Chaos Will Impact Cybersecurity Purchasing Decisions
Social	Fractured Workforce Relations Cause Increased Resistance to Security Controls
Trust	Disinformation Defense Becomes a CISO Priority
Regulatory	Policy Distractions Stretch Security Teams Thin
Environmental	Energy Instability Causes Massive Exposure to Cyber Resilience

Experience Gartner insights live

Join Gartner experts and your peers at **Gartner Security & Risk Management Summit 2026, June 1 – 3, in National Harbor, MD,** to gain valuable insights on cybersecurity strategy and vision, leadership, AI, metrics, risk and compliance management, cyber resilience, cloud security, data security, security behavior and culture, emerging threats, and more.

Learn more about the conference and register at
gartner.com/us/securityrisk

© 2025 Gartner, Inc. and/or its affiliates. All rights reserved. EVTM_1019_4227700

Gartner®