COHESITY

6 PIVOTAL SHIFTS IN 2026

A closer look at the new forces shaping cyber resilience

Introduction

AI technology is advancing faster than most organizations can adapt. Its growing use across the enterprise is changing how data is stored, secured, and governed. At the same time, cybercriminals are exploiting AI to launch new attacks.

Beyond AI, rising economic, regulatory, and geopolitical pressures are forcing leaders to make hard choices about cost, control, and compliance.

In 2026, these forces will converge—creating both risk and opportunity for those responsible for resilience.

This eBook outlines six pivotal shifts that will redefine cyber resilience in the coming year. Each prediction highlights a trend already taking shape and recommends steps you can take now to adapt.

SECURITY

1 Cybersecurity budgets will pivot toward response and recovery

As agentic AI tools amplify attacker capabilities, IT and Security leaders will reallocate at least a third of their cyber resilience budgets toward response and recovery to limit downtime and reduce financial fallout.

Newly released research from a survey of 3,200 IT and Security leaders across 11 countries confirms this budgetary swing: 70% of publicly traded companies said they adjusted financial guidance following a major cyberattack, and 73% of private firms reported redirecting budgets from innovation and growth to incident response and recovery.

These findings reveal how the financial toll of destructive cyberattacks is reshaping investment strategies. By prioritizing response and recovery, IT and Security teams are looking to accelerate restoration and limit financial losses when incidents occur.

As part of this reprioritization, organizations are also investing in technologies that improve backup integrity. Malware scanning within backup data is becoming standard practice as attackers use stealthier tactics to evade detection and extend dwell time within systems. Together, these conditions signal a broader evolution away from purely defensive strategies to an embrace of resilience-oriented patterns and practices.

3 action items for your team:

- **Reevaluate your cyber resilience budget.** Shift more investment toward response and recovery to strengthen capabilities and ensure faster restoration after an attack.
- **Make malware scanning part of your backup routine.** Integrate threat scanning across your data estate to detect malicious code early and confirm your data is clean and reliable for quick restoration.
- **Run regular response simulations.** Build team expertise through hands-on "tabletop" exercises where IT and security teams work to solve a simulated cyberattack. The output: refined playbooks, improved coordination, and faster recovery when incidents occur.

Get our 4th annual Global Cyber Resilience Report to see this financial data in context. Regional reports are also available.

AI

2 Attackers will weaponize AI to scale ransomware operations

Ransomware gangs will use AI to automate attack operations—lowering the cost of launching attacks, modifying code to evade detection, and driving the volume of attacks higher.

In 2026, attackers will make their operations more efficient by using AI to accelerate every stage of the ransomware process. This shift will expand both the reach and sophistication of ransomware campaigns, making large-scale attacks cheaper and easier to launch.

As a result, organizations will need to monitor their data estate, improve incident response, and bolster recovery capabilities.

As AI-driven cyberattacks multiply over time, traditional defenses will struggle to keep pace. This new reality will raise difficult ethical and policy questions about how AI is used in the context of crime. Expect renewed debate over regulation, oversight, and accountability, as policymakers, enterprises, and researchers grapple with how to curb AI-enabled attacks without stifling innovation.

2 action items for your team:

- **Test your recovery plan often.** Run scheduled simulations to uncover weaknesses before a real attack uncovers them.
- **Automate where possible.** Use orchestration tools to speed up containment and recovery when facing machine-driven threats.

Learn cyber incident response lessons from experts from Cohesity CERT (Cyber Event Response Team) and Palo Alto Networks Unit 42. Watch their conversation on-demand.

CLOUD

3 Hybrid cloud architectures will continue to dominate as cost pressures surge

IT leaders will double-down on hybrid cloud strategies to manage costs while maintaining agility, control, and compliance.

Enterprises will increase their reliance on hybrid cloud—blending on-premises infrastructure for data sovereignty with cloud services for agility. By 2026, hybrid deployments are expected to reach 55% of total infrastructure budgets, even as overall IT spending grows by less than 3% under "do more with less" mandates.

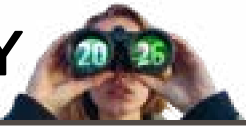
This trend reflects the growing need for flexibility. Organizations want the freedom to run workloads where it makes the most sense—without losing visibility or governance. Hybrid strategies also help optimize limited resources, giving leaders more control over cost, performance, and risk.

For many, the goal is balance: financial efficiency paired with operational resilience. As IT environments become more distributed, the ability to scale on demand while maintaining compliance and oversight will define success.

1 action item for your team:

- **Broaden and deepen your data protection coverage.** With hybrid cloud, IT leaders must safeguard more data sources in more places than ever before. Protecting them remains the foundation of cyber resilience, so ensure your strategy—and minimum viable recovery capability—accounts for the growing breadth and depth of data environments.

Find best practices, design considerations, and data resilience approaches to guide your enterprise modernization efforts.
Get the white paper



AI, CLOUD

4 AI initiatives will fuel sovereign cloud growth

In a world of growing regulatory scrutiny, enterprises will turn to sovereign clouds to keep sensitive data local, safeguard IP, and maintain control.

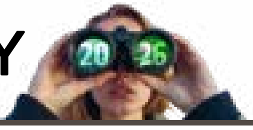
In 2026, enterprise AI initiatives will accelerate the adoption of sovereign clouds. These environments give organizations the ability to process and store data within national borders, ensuring compliance with regional privacy and security requirements. As AI projects become more data-hungry and reliant on proprietary information, enterprises will use sovereign clouds to retain control over intellectual property and reduce exposure to regulatory risk.

This trend is most visible in highly regulated regions such as the EU, the Middle East, and APAC, where data protection laws and national security concerns are shaping cloud decisions. Increased scrutiny of AI data flows will push organizations to adopt localized, trusted infrastructure that balances innovation with compliance.

1 action item for your team:

- **Evaluate sovereign cloud options.** Assess offerings from hyperscalers and their certified partner ecosystems to ensure mission-critical workloads can run in compliant, localized environments. When planning proof-of-concept projects, include success criteria for maintaining control and resilience in fast-changing regulatory conditions.

Interested in digital sovereignty and how Cohesity keeps you in control of your sensitive data? Read the blog



SECURITY

5 Nation-state alliances will form global cyber defense pacts

Amid escalating global tensions, NATO and allied nations will strengthen cooperation by sharing intelligence, aligning cyber resilience frameworks, and defending critical infrastructure from state-sponsored attacks.

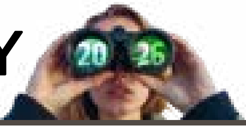
In 2026, NATO and its allies will expand formal cyber defense partnerships to counter increasingly sophisticated, state-sponsored threats. These alliances will coordinate intelligence sharing, standardize response protocols, and create joint mechanisms to protect critical infrastructure across borders. Increased resilience will be a focus of this effort.

For enterprises, this shift will bring both opportunity and complexity. Shared intelligence and global frameworks can improve visibility into emerging threats—but they also introduce new obligations around data sharing and compliance. As governments move toward greater collaboration, leaders across industries will need to align internal security programs with evolving standards and cross-border reporting requirements.

1 action item for your team:

- **Consider new global frameworks in your cyber resilience strategy.** Such frameworks can be a helpful starting point—or a reality check—for your own organization's plans. But remember, there's no magic elixir against cybercriminals. As new alliances form, keep tabs on how shared intelligence and coordinated response efforts evolve, and be mindful of your own risk profile. Use threat intelligence from credible third parties to strengthen your protection and recovery practices.

Read about what you can do to build cyber resilience in a world of destructive cyberattacks. Get the white paper



CLOUD

6 Data locality and sovereignty will become board-level priorities

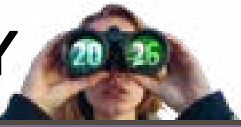
With rising data risks and changing global conditions, boards will treat sovereignty as a top strategic priority—accelerating plans to diversify deployment of critical workloads across sovereign, hybrid, and regionally controlled clouds to ensure operational continuity and compliance at scale.

By 2026, most large enterprises will track data sovereignty and control of data flows as part of their board-level risk oversight. CIOs will lead new initiatives to distribute critical workloads across multiple trusted environments—including sovereign, hybrid, or regionally governed clouds—balancing flexibility with stronger governance expectations.

The urgency is growing. Public cloud outages, political instability, and new regulations are revealing the potential risks of relying too heavily on global providers. As sovereignty gains board attention, leaders will act to strengthen business continuity, maintain compliance, and reduce dependence on a single vendor.

3 action items for your team:

- **Map workloads by sensitivity and risk.** Identify which data must remain under tighter control.
- **Launch or accelerate programs for sovereign data zones.** Focus on on-premises, private cloud, or regionally controlled cloud environments.
- **Plan for vendor diversity.** Develop fallback options to reduce reliance on a single cloud provider.



Ready to strengthen your cyber resilience?

Learn more about our AI-powered data security solutions at **cohesity.com/solutions/**

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054