Futurum RESEARCH

Everpure

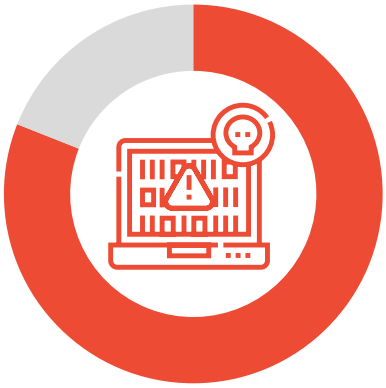
Cyber Resilience Is Now the Mandate: A CXO Checklist

SEPTEMBER 2026

Cyber Resilience Is Now the Mandate: A CXO Checklist

Most organizations will face a cyber incident this year, yet few have tested whether they can actually recover: 81% of security leaders reported a significant incident in the past 12 months (see Figure 1). Prevention and detection still absorb most of the budget and attention, and they still matter. They no longer decide the outcome. In an assume-breach world, the question a board should ask is not whether the organization will be compromised, but how quickly it can resume operations. Resilience, the ability to recover fast and cleanly, is what separates a costly but survivable event from an existential one.

Figure 1. Security Leaders Reporting a Significant Security Incident in the Past 12 Months



81% of security leaders reported a significant incident in the past 12 months

Source: Futurum Research, 1H 2026, Cybersecurity Decision-Makers Survey.

AI is changing the picture on two fronts: it broadens what attackers can do, lowering the cost and skill required to mount a capable campaign; and it deepens an organization's dependence on data, because AI systems increasingly read from and act on that data, raising the cost of losing or corrupting it. A cyber event has become a business event the whole C-suite owns, not a technical problem to hand to the CISO alone.

This is a decision aid for leadership teams, written to be useful before any product enters the conversation. It sets out the questions a team should be able to answer, and where those answers point, it shows how one layer of the recovery stack fits.

A disaster-recovery plan assumes a clean restore point. A deliberate attacker will not leave one.

Cyber Recovery Is Not Disaster Recovery

Confidence is running ahead of proof. Some 65% of security leaders say they are very or extremely confident they can recover from a major incident. The experience of those incidents tells a different story: operational downtime is one of the consequences security leaders report most often, named by 37% (see Figure 2). Self-reported confidence is not a timed, tested recovery, which is the distance the checklist that follows is built to close.

Figure 2. Confidence Meets Reality.

65% of security leaders are very or extremely confident they can recover, yet operational downtime is among the consequences they report most often when incidents hit (37%).

Many organizations still rely on disaster-recovery plans built for hardware failures and natural disasters. Those plans assume a clean restore point and a cooperative environment, and a modern attack offers neither. Ransomware and destructive malware rank among the top three incident concerns for a third of security leaders. Increasingly, the goal is disruption rather than a ransom, which removes the option of paying to make the problem disappear and leaves recovery as the only way back. Essentially, ransomware's real cost is operational continuity, not just data loss.

AI raises the stakes here, too. Some 57% of security leaders are highly concerned about agentic AI operating in their environment. As more processes and decisions run on live data, the damage from losing or corrupting it grows, and recovery has to keep pace.

Ten Questions That Define a Credible Recovery Posture

The questions in Table 1 move from the strategic to the tactical. They work best when asked together, with security, infrastructure, finance, and operations in the same room, which for many organizations happens for the first time only after an incident.

Table 1: The Ten Questions

1	**Do you know your minimum viable business?**	Identify which processes and data must return first, and in what order, to keep operating. This is a business judgment because only the business can rank the value of an application. Additionally, how efficient, automated, and repeatable is this process? As business changes frequently, this mapping must be kept up to date.
2	**Have you graded your data stores and applications by business impact?**	A systematic, repeatable scoring of every system, rather than a one-off spreadsheet, is what makes recovery tiers consistent across teams and defensible to an auditor or a board.
3	**For your most critical data and applications, do you know every system, process, and dependency that would be affected if they went down?**	Beyond the ranking, pinpoint the sensitive and regulated data whose loss or exposure does the most damage, and map the identity, directory, and other services that cannot be restored without. For AI pipelines, this should include model state, vector stores, and more.
4	**Have you quantified the costs of downtime in revenue, regulatory exposure, and recovery labor, and can you state your Tier-1 RTO in hours, not days?**	Account for lost revenue, regulatory and legal exposure, and the human cost of a prolonged, all-hands recovery.
5	**Who owns cyber resilience, and specifically, who owns "proof of recovery" versus who owns daily operations?**	Resilience behaves like profit: many functions contribute, but one leader must be accountable for the result. Where ownership is spread across security, infrastructure, and continuity teams, decisions stall for years.
6	**Does your recovery plan match today's threat, or yesterday's disaster?**	Test the plan against a deliberate, adaptive attacker rather than a flood or a failed disk. A plan that predates the threat offers false comfort.
7	**Have security and infrastructure teams ever rehearsed a joint recovery – not just planned one on paper?**	Recovery lives in the seam between teams that rarely share tools or reporting lines. The first joint rehearsal should not be the live event.
8	**Can you recover fast enough to stay viable, and have you proven it?**	Recovery speed is what separates a blip from a material event, and a successful backup report is not proof. Test against a realistic attack scenario.
9	**Are your recovery copies isolated, immutable, and indelible, and protected even from an attacker holding full administrative credentials?**	If an attacker who controls the environment can also reach the backups, there is no recovery plan. Confirm what an isolated recovery environment would hold.
10	**Can you trust what you restore?**	Recovery that quietly reintroduces the intrusion restarts the incident. Validate the integrity of the data before it is returned to production.

Closing the Gap: Everpure on Data and Recovery

This checklist is foundational. It's the baseline any organization now has to clear, regardless of which vendors sit in its stack. Several of the questions map directly onto Everpure's cyber-resilience portfolio. SafeMode's snapshots are immutable and indelible, so an attacker cannot alter or delete them, even with full access to the environment, while the isolated recovery environment keeps clean copies out of the production blast radius, addressing the isolation and recovery speed questions head-on. Everpure has also worked with partners on scanning recovery points, aimed squarely at the integrity question: the risk that a restore inadvertently carries an intrusion back into production. For the data questions at the top of the list, Everpure Data Intelligence classifies data at the entity level across structured and unstructured sources, providing organizations with a map of where sensitive and business-critical data actually resides and a basis for prioritizing what to protect.

Even so, no single vendor covers the full recovery stack. The identity, directory, and network dependencies that enable a full restore require an ecosystem of partners, and Everpure operates as one layer within it. Recovery posture is only as strong as the coordination across those layers, and the organizations that work through these questions before an incident are the ones that treat a breach as survivable rather than existential.

Methodology: Survey figures are drawn from the Futurum 1H2026 Cybersecurity Decision-Makers Survey, an unweighted survey of 929 cybersecurity decision-makers.

Important Information About This Report

AUTHORS

Fernando Montenegro
Vice President & Practice Lead,
Cybersecurity & Resilience | The Futurum Group

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

This document, including any supporting materials, is owned by The Futurum Group. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of The Futurum Group.

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Everpure

ABOUT EVERPURE

Everpure allows organizations to take control of their data with an industry-leading, ever-evolving storage and data management platform. We help companies unleash the power of their data by ensuring it is secure, accessible, intelligent, and ready to perform in the AI era. By replacing rigid infrastructure with a platform that operates like a living system, Everpure makes data management effortless. Learn more at Everpuredata.com.

Futurum®

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum®
CONTACT INFORMATION: The Futurum Group LLC | futurumgroup.com | (833) 722-5337

© 2026 The Futurum Group. All rights reserved.