

SPONSORED BY



Building cyber resilience:

A survival guide for security teams

Why Active Directory is at the heart of cyber resilience

Security leaders are moving from a prevention-only mindset to one that focuses on cyber resilience. **Paul Wagenseil** explains why planning for recovery of Active Directory should be the first step.

OUR EXPERTS:

Marty Momdjian

*EVP of Services and GM
of Ready1 by Semperis*

Ari Harrison

Director of IT, BAMKO

Christian Khoury

*Founder & CEO,
EasyAudit*

Rick McElroy

CEO, Nexasure

What is cyber resilience?

Cyber resilience is "being able to continue doing what you're doing when it comes to people, process and technology when there's a cyber event," says Marty Momdjian, Executive Vice President of Services and General Manager of Ready1, Semperis' cyber crisis response platform. "It's having your house in order when there is any type of impact, cyber or cybersecurity-wise."

Though cyber resilience may seem like common sense, achieving it isn't always easy. It often requires an organization to restructure its operations and priorities and make [backup and recovery](#) a core business goal. Siloed teams like legal, IT and human resources may need to better communicate and work together in response to cyber crises.

Building cyber resilience

On the shore of St. Augustine, Florida, there's an old Spanish fort that withstood two prolonged sieges in the 18th century. Despite heavy pounding by cannon fire, the fort's walls stood strong. Their secret? The walls were built with coquina, an aggregate of seashells, coral and limestone that absorbs cannonballs like a sponge instead of cracking like regular stone.

Some cybersecurity providers would have you believe that repelling all attacks and intrusions is the purpose of their products and services, but the truth is that no system is 100% impenetrable.

More important than impregnable defenses is [cyber resilience](#). That's the ability of your IT systems to recover quickly from an attack and get back to normal business. It ensures that your defenses become like the Spanish fort's walls, rolling with the punches instead of cracking under the cannon fire.



"In a crisis, you don't rise to the occasion. You fall to the level of your preparation."

Marty Momdjian | EVP & GM, of Ready1 by Semperis

Most importantly, the impetus toward maximum cyber resilience must come from the top down. [Company leadership](#) needs to make sure that all departments, especially the IT and [security operations](#) teams, work toward organization-wide goals. But before that, leadership itself must be convinced of the importance of cyber resilience and how it differs from cybersecurity.

"Cybersecurity is about defense. Cyber resilience is more about survival," says Christian Khoury, Founder and CEO of EasyAudit. "Most organizations, most companies, stop at cybersecurity, and they assume resilience is just magically going to follow, but it doesn't."

The role of Active Directory in cyber resilience

For most organizations that run Windows systems, there's a further complication. For them, recovery and resilience start with [Microsoft Active Directory](#) (AD) and its cloud-based sibling, [Entra ID](#), [identity systems](#) that hold the keys to user access of resources across the organization. If AD goes down or is compromised, an organization may be dead in the water.

"In most enterprises, AD and Entra ID are the source of truth for authentication and authorization," says Ari Harrison, Director of IT at BAMKO. "If they are down – or worse, poisoned – servers reject service tickets, [Kerberos](#) fails, NTFS permissions are meaningless, conditional-access policies lock out admins, and SaaS apps that rely on SAML/OIDC [Open ID Connect] will not issue tokens."

It can be a difficult and painstaking task to get AD back to fully operational. You can't always flip a switch and copy over a backup. Instead, the entire AD system must be rebuilt piece by piece, regrowing the dependency trees until the entire AD forest is repopulated. That's a process that few IT teams drill for in their downtime.

"Most organizations don't practice recovering their AD environment," says Momdjian. "They restore the domain in some kind of clean room, but there's hundreds of actions and steps that need to be taken after restoration to make sure not just Active Directory is working, but that everything downstream – authentication and authorization – is working as well, especially on the application side."

In a Windows environment, restoring Active Directory is the key to resuscitating the entire business after an IT outage, regardless of whether that outage was caused by a cyberattack or a bad software update. Cybersecurity won't protect you from every scenario, but cyber resilience will make sure your organization gets through them as smoothly and quickly as possible.

"The faster you can restore access to business-critical applications and services, the less damage in lost revenue, customer dissatisfaction, legal ramifications and other collateral fallout from an AD outage," writes Semperis VP of Products [Darren Mar-Elia](#) in a recent blog post.

A widespread lack of resilience

A [recent survey of 1,000 organizations around the world](#), commissioned by Semperis, reveals just how pervasive the lack of cyber resilience can be:

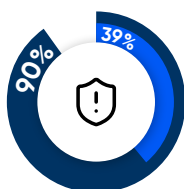


Although 96% of respondents claimed to have a [cyber crisis response](#) plan, 71% admitted to having had at least one IT-related event that halted critical business functions in the previous 12 months.

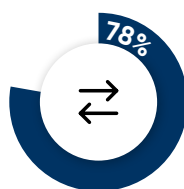


Thirty-six percent said they'd suffered through more than one such event.

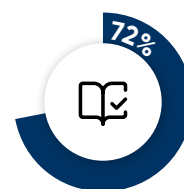
As for the crisis response plan:



Ninety percent said they'd activated it at least once in the previous year, with 39% having to activate it between 5 and 15 times.

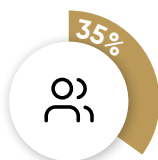


Seventy-eight percent of respondents said they ran tabletop exercises for crisis response monthly or quarterly.

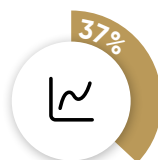


Seventy-two percent said their incident-response playbooks were updated on the same cadence.

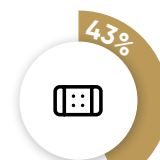
That does hint at a fair degree of cyber resilience, but how well are these organizations really doing? Many may be confusing cyber resilience with cybersecurity, because critical teams outside the IT department seem to be excluded more often than not. Regarding that, the survey found that:



Thirty-five percent of respondents included their finance, human-resources or legal teams in the crisis-response tabletops.



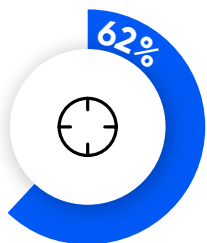
Only 37% brought in the business-continuity team.



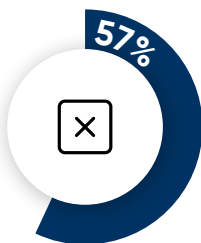
Most mystifying of all, only 43% thought to include their disaster-recovery teams, whose expertise is essential to cyber resilience.

The challenge for water and electricity providers

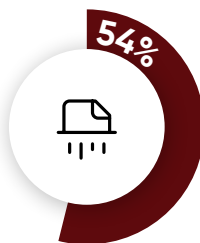
The numbers are similarly dire in a different Semperis-commissioned [survey of 350 water, water-treatment and electricity providers](#) in the United States and United Kingdom:



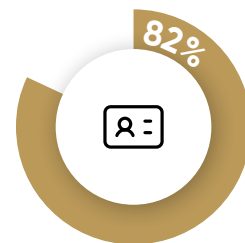
Sixty-two percent said they'd been targeted in the previous year – 80% of those more than once.



Fifty-seven percent said the attacks had disrupted their normal operations.



More than half (54%) of those said data or systems had been permanently corrupted or destroyed.



Eighty-two percent of the attacks "definitely or possibly" compromised core identity systems such as Active Directory or Entra ID, respondents acknowledged.

The upshot is that while many organizations, including those that are part of critical infrastructure, may think they're ready to fully and quickly recover from a cyber crisis, they're probably not. They likely haven't fully planned for and prioritized the essential parts of cyber resilience.

"Cyber incidents don't wait for organizations to be ready – they strike when you're least prepared," writes Momdjan in the report for the first survey. "In a crisis, you don't rise to the occasion. You fall to the level of your preparation."

What may happen if you're not resilient enough

In the past few years, we've seen drastic examples of a lack of cyber resilience among critical infrastructure providers. When the U.S. fuel distributor [Colonial Pipeline](#) was hit by a [ransomware attack](#) in May 2021, apparently because of a compromised password, the company quickly paid the attackers, who in return provided a decryption tool.

Yet the company took a week to get back to normal operations, causing panic and long lines at gas stations throughout the Southeast. This wasn't because Colonial Pipeline's pumps and other mechanical parts had failed. They worked just fine before, during and after the attack.

Rather, the company's metering systems had been taken down by the attack and proved difficult to bring back online. Without the ability to keep track of how much gasoline and jet fuel was dispensed, the company had no way of properly billing clients. So, it simply stopped distributing fuel until the metering and billing systems could be fully restored.

"When leadership treats resilience as a strategic function instead of just a technical function, it changes the entire culture of the company."

Christian Khoury | Founder & CEO, EasyAudit

What could have prevented this situation? An [academic paper](#) issued in 2023 by Miami University (Ohio) researchers said the lack of [multi-factor authentication](#) on an abandoned VPN account, plus the lack of a [zero-trust model](#), were the key reasons for the initial penetration. But it added that "Colonial Pipeline could have avoided paying the ransom if they had backed up their systems."

"The Colonial Pipeline hack was a wakeup call to the concerned authorities and vulnerabilities that exist within our infrastructure," said the paper. "The preventative measures were not put in place and the consequences were predictable."

Billing clients, or the lack of ability to do so, was also key to the impact of the [Change Healthcare](#) ransomware attack in February 2024. The company provides billing and payment services for thousands of healthcare providers across the United States, ranging from hospital systems to doctors' offices, and the attack brought that activity to a standstill.

"Change Healthcare impacted the entire world, from literally patient registration, patient care claims, pharmacy, getting medication routing and approval for purchases and authorizations and so on," says Momdjian. "It took 90 percent of the U.S. healthcare systems offline."

Many of those billing systems stayed offline for more than a month as Change Healthcare's new parent company, UnitedHealth Group, scrambled to contain the damage. UnitedHealth made [advance payments of \\$6 billion](#) to healthcare providers unable to send out invoices due to the long recovery process.

"Change Healthcare was not resilient," Momdjian points out. "A lot of other vendors and third parties depended on Change Healthcare for their services to function."

Of course, you don't even need a cyberattack to bring critical infrastructure to a halt. The [CrowdStrike outage](#) of July 2024 resulted from malfunctioning cybersecurity software and knocked out companies worldwide as their Windows systems went offline. Major airlines were especially affected, and thousands of commercial flights were cancelled, stranding passengers across the globe.



"Don't treat your internal auditors as adversaries. Treat them as friends."

Rick McElroy | CEO, Nexasure

In the U.S., American Airlines and United Airlines resumed most flights within the first day of the outage. But Delta Air Lines took six days to recover, partly because the crew-tracking system, which logs and positions pilots and flight attendants to staff flights, [proved difficult to bring back online](#).

That resulted in not enough crew members showing up for flights, then "timing out" according to FAA rules as they waited for additional crew members to arrive, creating a snowball effect as more flights were delayed or cancelled.

The issue was made worse by the nature of the CrowdStrike issue, [a faulty update at the Windows kernel level](#) that required each machine to be manually rebooted. That meant, for example, that technicians had to climb up ladders to reach flight-status boards hanging

from airport ceilings. Ultimately, [Delta cancelled more than 5,000 flights and lost an estimated \\$500 million](#).

How could Delta have been more cyber resilient and able to keep pace with other affected airlines? Bringing the crew-tracking system back online more quickly would certainly have lessened the amount of disruption, although we don't know how frequently Delta ran exercises to restore that system before the outage.

"CrowdStrike decides to update a tool, and then it takes off a bunch of your servers and endpoints. Well, how come we never tested for that edge case?" rhetorically asks Rick McElroy, CEO at Nexasure. "We should have, and then we should, as an IT team, or a security team, have a playbook that's fairly automated to help restore that stuff as fast as possible."



How to improve your cyber resilience

How can you make sure that your organization isn't as vulnerable to cyber disruption as Colonial Pipeline, Change Healthcare or Delta were? There are several steps you can take – not necessarily in this order, although all are helpful.

1



Get the company leadership on board.

This is the first and most crucial step. If you are a CISO or an IT manager, you need to convince the rest of the C-suite that recovery and cyber resilience are mission-critical priorities. Use Delta and Change Healthcare as examples, but don't scare the suits. Instead, illustrate how much money and business can be saved by swift, smooth system-wide recovery.

2



Get the auditors on board too.

Nexasure's McElroy points out that while the C-suite may not always listen to the SOC team, they will listen to [auditors](#) who emphasize the importance of robust recovery preparations.

3



Get the leadership, IT and security teams on the same page.

Cyber resilience requires all teams to be working toward the same goals, which should be the company's primary business goals. This may mean forgoing implementation of a new cybersecurity tool if it doesn't directly contribute to cyber resilience. But again, it also means designating resilience itself as a business goal.

4



Adopt an "assume-breach" mentality.

As with zero trust, the assume-breach mentality starts off by acknowledging that intruders will get into your systems. How do you then limit the damage they can do? You can redesign your systems to make lateral movement difficult, implement the principle of least privilege to contain the impact of compromised accounts, and use monitoring tools to spot anomalous behavior.

5



Allocate more budget to recovery and resilience.

All too often, cyber resilience and its associated efforts are seen as part of cybersecurity, and companies don't want to spend another dime. Yet Delta's experience in the wake of the CrowdStrike outage shows that systems can go down without any cyberattack, and that far more personnel than the SOC or IT teams need to be involved in the recovery.

6 Clearly write out disaster-recovery plans.

Specific, predetermined procedures designed for the needs of your organization and industry should be in place to respond to likely critical scenarios. Those plans should be easily accessible to each responding team member, and should be hard-printed in notebooks or maintained in an out-of-band platform or tool instead of kept on a server. If your entire IT system goes down, you'll need those plans.

7 Have a specific plan to recover and rebuild your Active Directory.

Due to the central role of AD, it's especially crucial that it be recovered quickly to a trustworthy state so that the rest of the Windows environment can be restored with confidence. That takes a lot of skill and practice, secure AD-specific backups, and perhaps the assistance of outside tools like Semperis' Active Directory Forest Recovery.

8 Clearly define team roles and responsibilities.






The worst-case scenario is that a real IT incident happens and no one knows what to do or who's in charge. Designate specific people to perform specific tasks and make sure that all crucial tasks have someone assigned to them. Then run drills to instill "muscle memory" so that when the real thing happens, no one has to think about what to do – they just do it.

9 Improve communication among teams and have them participate in recovery exercises.

You can't run company-wide recovery scenarios without the entire company, and to set the stage, you have to get the different teams to know each other and their priorities. Break down the silos by getting teams to work together on crisis response planning and execution, and ensure that cyber crisis response is included as an integral aspect of your overall enterprise crisis response plan.

10 Set up out-of-band communications.

As with those hard-printed notebooks, you'll need staffers across the company to keep talking even if the email or messaging systems go down. Distribute lists of mobile and home phone numbers. Set up chatrooms on third-party services that can be easily accessed from smartphones. But don't make these out-of-band communications too hard to access – too much cybersecurity can sometimes be an obstacle to cyber resilience.

- 11**  **Run full recovery drills, not just tabletops.**
[Tabletop exercises](#) can be useful, but they're often not conducted as [full incident-response drills](#). Only by creating genuine panic and urgency, even among company executives, can key players learn what it's like to perform under stress and see what breaks.
- 12**  **Train, train, train.**
Your IT and SOC teams will already be familiar with ways to bring systems back online, but the rest of the company might not be. Since cyber resilience is a company-wide effort, [train personnel in other departments](#) on what they can do and what their roles should be in a recovery scenario – and make them attend the tabletop exercises and participate in the drills.
- 13**  **Make recovery and resilience part of the company culture.**
Backing up data, running tabletops and drills, conducting audits and inventorying assets are often seen as undesirable tasks best left to the IT nerds in their windowless server rooms. Yet these activities should be routine efforts that the entire company participates in.
- 14**  **Don't forget [third-party risk](#).**
Delta Air Lines was offline for several days because it wasn't cyber resilient, but it went down in the first place due to a flaw in third-party CrowdStrike software. Keep in mind that your software and hardware suppliers might have their own vulnerabilities and take that into account when making recovery and resilience plans.
- 15**  **Don't be afraid to ask for help.**
Many organizations think they can handle disasters themselves, but there's no shame in reaching out to others who may have more experience in dealing with dire situations. Consider keeping disaster-recovery experts on retainer or contract them to help train your staff or write up incident-response plans.

Not a tool, but a mindset

One must remember that cyber resilience is not simply a tool, not something you can plug in and turn on. Rather, it's a mindset, a refocusing of your company priorities to include the entire team working together to recover from what could have otherwise been a total disaster.

"Cyber resilience isn't just about technology," writes Semperis CEO and Co-Founder [Mickey Bresman](#) in a company blog post. "It's about people, processes, and the ability to act decisively when everything is on the line. It's about discipline, preparation, confidence, and the ability to adapt under pressure."



CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications.

To learn more, visit CyberRiskAlliance.com.

SPONSORED BY



Semperis protects critical enterprise identity services for security teams charged with defending hybrid and multi-cloud environments. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' AI-powered technology protects over 100 million identities from cyberattacks, data breaches, and operational errors.

As part of its mission to be a force for good, Semperis offers a variety of cyber community resources, including the award-winning Hybrid Identity Protection (HIP) Conference, HIP Podcast, and free identity security tools Purple Knight and Forest Druid. Semperis is a privately owned, international company headquartered in Hoboken, New Jersey, supporting the world's biggest brands and government agencies, with customers in more than 40 countries.

Learn more: <https://www.semperis.com>

Follow us: [Blog](#) / [LinkedIn](#) / [X](#) / [Facebook](#) / [YouTube](#)

MASTHEAD

EDITORIAL

SVP, HEAD OF CONTENT

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

How can you protect your core identity system – before, during, and after a cyberattack?

Semperis offers cybersecurity's most comprehensive defense for identities, so you can sleep easy knowing you've got lifecycle defense covered. And for a dose of good dreams, know that we have a dedicated incident response team, too.

Protect Your Critical Identity Infrastructure

- ✓ Minimize the attack surface.
- ✓ Detect advanced attacks.
- ✓ Automate remediation.
- ✓ Accelerate incident response.

Simplify Disaster Recovery Planning

- ✓ Malware-proof your backups.
- ✓ Automate AD forest recovery.
- ✓ Recover to any hardware.
- ✓ Accelerate incident response.

Semperis' AI-powered identity security and cyber resilience provides the industry's most complete hybrid identity protection. Learn more at www.semparis.com.

