semperis

Recovering Active Directory from Cyberattack.

A SURVEY OF IDENTITY-CENTRIC SECURITY LEADERS

Active Directory is in the attackers' crosshairs.

As the gatekeeper to critical applications and data in 90% of organizations worldwide, Microsoft Active Directory (AD) has become a prime target for widespread cyberattacks that have crippled businesses and wreaked havoc on governments and non-profits.

This report is based on a survey of over 350 IT security professionals from mostly midsize and large firms across six major industry sectors. The goal is to understand the state of cyber preparedness as it relates to recovering AD from ransomware and wiper attacks. Semperis chose this topic for several reasons:

The threat landscape is rapidly changing: Back in 2015, Microsoft estimated that 95 million AD accounts were under attack every day. [1] Fast forward to today, and COVID-19 has dramatically changed the workplace. In our cloud-first, mobile-first world, dependency on AD has rapidly grown—and so has the attack surface.

Ransomware attacks are incredibly costly: Ransom payments encourage additional attacks, fund terrorism, and do not come with any guarantees. But the alternative is often even more expensive, with global ransomware damages projected to reach 20 billion USD by 2021. [2]

Organizations are woefully unprepared: In a wide-spread outage, you must recover AD before you can recover your business. But according to a poll by the SANS Institute, only one in five organizations have a tested plan in place for recovering AD after a cyberattack. [3]

If AD isn't secure, **nothing is.**

NOTE: Since AD extends to cloud identity, any tampering of AD causes a ripple effect across the entire identity infrastructure.

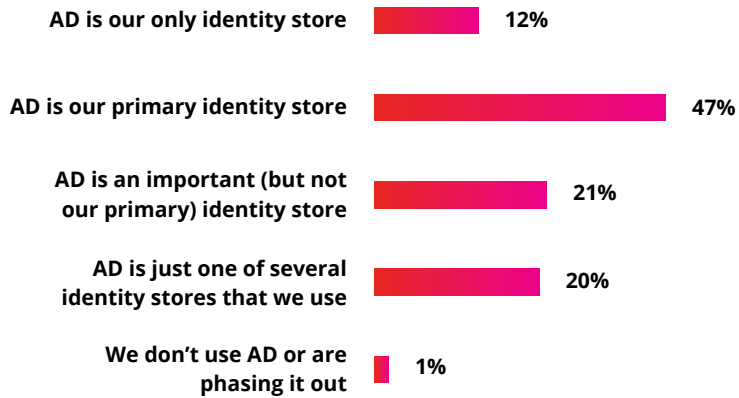
Heavy reliance on AD is universal.

AD is used to manage users, computers, and other devices on Windows networks. Without AD, employees can't log in to the network. They can't access file servers or business applications. They may not be able to use email, the company phone system, or building access cards. Since being introduced 20 years ago in Windows Server 2000, AD has been integrated with countless applications and systems, from the front office to the shop floor and beyond. At the same time, organizations have become increasingly dependent on all these digital resources and systems.

Perhaps it's not surprising then that 97% of organizations surveyed say that AD is mission-critical to the business.

This statistic includes organizations where AD is the only identity store (12%), the primary identity store (47%), or an important identity store (21%). Even in organizations where AD is just one of several identity stores, 76% report that the impact of a ransomware or wiper attack that takes out AD would be catastrophic.

Which of the following best describes your company's use of Microsoft AD?



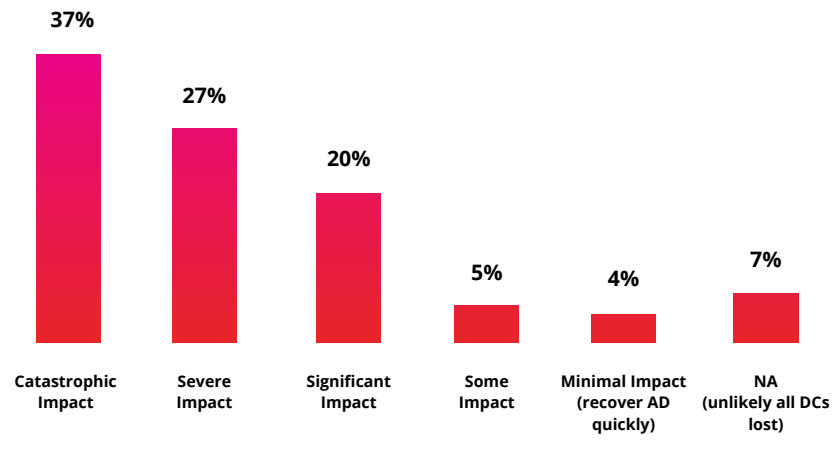
AD outages seriously impact business.

In considering the impact that an AD outage would have on the business, 11% of organizations surveyed say that they would experience only “some” or “minimal” impact. In contrast, 84% report that the impact would be significant, severe, or catastrophic. One organization even noted that an AD outage would be akin to a nuclear inferno.

Andy Powell, CISO at global shipping giant Maersk, likens an AD outage to sailing with a broken engine.

Maersk experienced a prolonged AD outage after it was hit by NotPetya in 2017. The lesson learned? According to Powell, “What we needed to do is ensure that if the business was hit again, we can recover quicker. You're not sailing anywhere with a broken engine. Active Directory, DHCP, DNS run your network. You've got to be able to recover that capability. We assume it will be taken down and build everything around recovering and operating it.” [4]

To what extent would your company be impacted if a ransomware or wiper attack took out your domain controllers (DCs) and AD was down?



Nine days for an Active Directory recovery isn't good enough, you should aspire to 24 hours; if you can't, **then you can't repair anything else.**

ANDY POWELL
CISO
MAERSK

The threat to AD from a cyber disaster is generally understood, but the complexity of forest recovery is not.

AD's distributed architecture and multi-master replicated database design can be leveraged in many "traditional" disaster recovery scenarios. For example, if a fire or flood destroys domain controllers (DCs) in one location, production DCs in other locations (or standby DCs in a DR site) can service requests until replacement DCs are in place. There's no need for backups or forest recovery in this scenario: replacement DCs are simply introduced into the existing AD infrastructure and populated via AD replication or Install from Media (IFM).

However, in the case of a ransomware or wiper attack, it's quite possible that all DCs will be destroyed at once. Such was the case in the cyberattack on the 2018 Winter Olympics. [6]

Most organizations surveyed realize the potential for a complete AD outage, with only 7% saying that it is unlikely that all DCs would be lost. That's the good news.

The bad news is that only 37% of organizations understand the complexity of forest recovery.

That's a concern because forest recovery is not a simple task. Microsoft provides a lengthy technical guide that details the 28 steps required to recover an AD forest. [7] The recovery process is mostly manual, and there's no indication if you do something wrong until the end, at which point you have to start over. In one training scenario (a rather trivial recovery in a classroom setting with all the steps spelled out), the failure rate was over 80%.

What does it take to recover an AD entire forest?

At a high level, the tasks to recover a "mini forest" are:

- Restore at least one DC in each domain from backup, ensuring that restored DCs don't start replicating before other DCs are restored
- Restore SYSVOL (must be restored authoritatively on one DC in the forest)
- Clean up metadata
- Clean up DNS
- Rebuild the Global Catalog

In a sufficiently large environment, this will not be enough capacity to service user authentication requests and tier 1 and 2 applications. So, you will need to promote additional DCs, which may need to be rebuilt. This re-promotion process must be staggered since many DCs trying to re-promote over the wire will cripple the newly recovered forest.

The bottom line
Going from one DC per domain to an enterprise forest at full capacity is not a challenge, it's THE challenge with forest recovery.

> **No one is perfect,** but when you are a system administrator you are often provided with a better stage on which to showcase that imperfection.

VERIZON DATA BREACH INVESTIGATIONS REPORT

Few organizations can recover AD quickly after a ransomware or wiper attack.

AD recovery was initially driven by concerns about software failure, database corruption, and administrative errors. As AD matured, those concerns largely went away. However, there's a scary new concern with a couple of twists.

The new concern, of course, is a cyberattack that takes out AD. And the twists are:

- Restoring AD to clean servers
- Restoring AD without reintroducing malware in system state or bare-metal backups

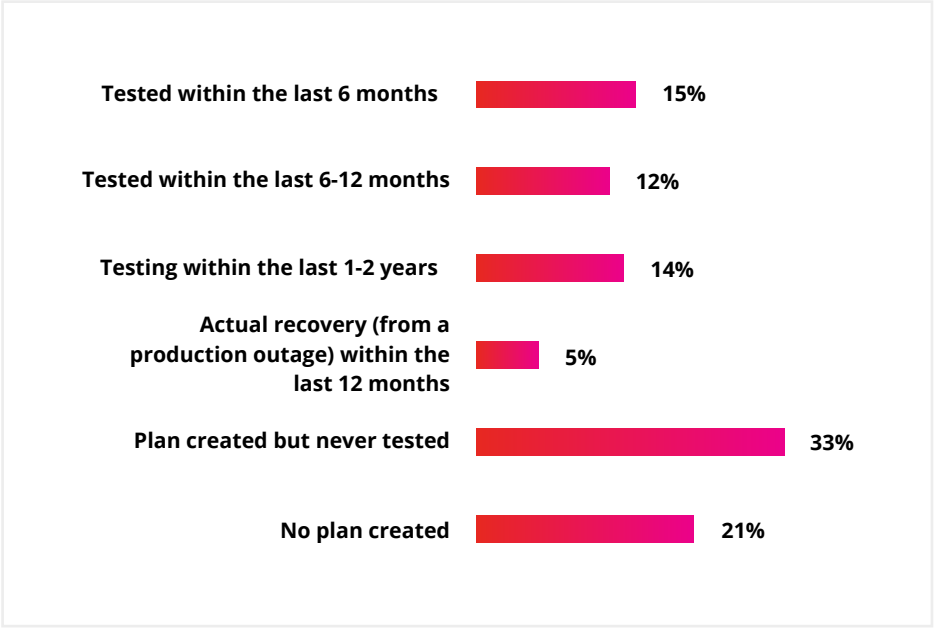
In "the good old days," AD recovery meant recovering AD on existing DCs. But cyberattacks changed all that. And it appears that organizations haven't kept up.

While AD recovery after a cyberattack requires the ability to recover to new servers, the majority of organizations surveyed (69%) are only somewhat confident, not confident, or unsure of their ability to accomplish this in a timely fashion. In fact, only 3% of organizations surveyed are "extremely confident" that they can recover AD to new servers in a timely fashion.

More than 50% of responders have never actually tested their AD cyber disaster recovery process, or have no plan in place at all.

Can you prove that you're meeting your SLAs?

When is the last time you tested your AD cyber disaster recovery process?



Lack of testing tops the list of concerns around AD recovery.

Organizations expressed many concerns about AD recovery, with the lack of testing being the #1 concern. This includes organizations that haven't tested AD recovery at all and those who have tried but failed.

For organizations that rely on a manual recovery process, testing is cumbersome and prone to failure. Even for organizations with some level of an automated process, testing can be difficult if scripts and information about AD topology haven't been kept up to date. Verified backups, advanced automation, the ability to restore to alternate hardware, and IP mapping can facilitate periodic DR tests and alleviate concerns about lack of testing.

Interestingly, some organizations cited a concern about the absence of clear responsibility for AD recovery. The same concern was reflected in a recent Forrester report on ransomware recoverability, which found that poorly defined responsibilities and poor communications slow down ransomware attack response times. [9]

Top 5 concerns for recovering AD after a cyberattack:

01 Haven’t tested AD recovery

02 No cyber recovery plan for AD

03 Backups get encrypted or wiped

04 Can’t recover AD quickly

05 Responsibility for AD recovery has not been defined

Looming threats take a personal toll.

When NotPetya wiped out Maersk's network, Adam Banks, chief technology and information officer, didn't go home for 70 days while directing the recovery effort. [10]

And even the mere threat of a cyberattack can take a toll on IT executives and staffers. In our survey, 69% of respondents report increasing stress about the impact that a cyberattack would have on their career.

But while respondents are feeling the pressure, they're not backing down. In fact, only one respondent indicated that they're considering a career change. Let's hope that the computer networks of the organizations in our survey are as resilient as their employees!

"How has the threat of a cyberattack on your company affected you personally?"

TOP 5 RESPONSES:

01 My stress level is increasing.

02 I'm concerned that my reputation or career would be damaged if we were hit by a cyberattack.

03 I spend personal time trying to keep up with new threats and security recommendations.

04 I feel compelled to document my attempts to improve our recovery capabilities.

05 I'm concerned that I could lose my job if we were hit by a cyberattack.

> Mr. Hawkins [the IT director] said he had warned the city about its vulnerability long ago – urging the purchase of an expensive, cloud-based backup system... But there was no money. Once the city's entire computer network crumbled in the space of a few hours, there was an intense round of finger-pointing, and it ended with Mr. Hawkins. [11]

When Ransomware Cripples a City, Who's to Blame? This I.T. Chief Is Fighting Back The New York Times | August, 2019

Conclusion

Today, the prevalence and increased sophistication of ransomware mean that companies must deal with the real possibility of a threat actor crippling their entire IT environment—everything, including AD. Microsoft recently reported that opportunistic attackers are compromising targeted networks several months before deploying the ransomware, waiting to monetize their attacks until they see the most financial gain. [12] Like during a global pandemic, for example. The idea of having to recover AD from scratch is no longer theoretical. It now must be a critical part of incident response planning.

- Many organizations understand the importance of AD but are a step behind in securely managing it, particularly as they support an expanding ecosystem of mobile workers, cloud services, and devices.
- When a ransomware or wiper attack takes out DCs, traditional forest recovery can drag on for days or even weeks and reintroduce the malware in the process. Lack of regular testing multiplies the risk of errors and can delay recovery.
- The risk model for AD recovery has changed, but recovery playbooks haven't. Considering that cyberattacks inflict more damage and strike more frequently than natural disasters, it's time to think "cyber-first."

It's not all bad news. We can help you shorten the recovery time of your entire AD forest by 90%.

Semperis AD Forest Recovery fully automates the forest recovery process so you can avoid human errors, reduce downtime to minutes instead of days or even weeks, and eliminate the risk of malware reinfection. Core capabilities include:

Cyber-first disaster recovery
Recover AD even if domain controllers are infected or wiped

Anywhere recovery
Restore AD to alternate hardware (virtual or physical)

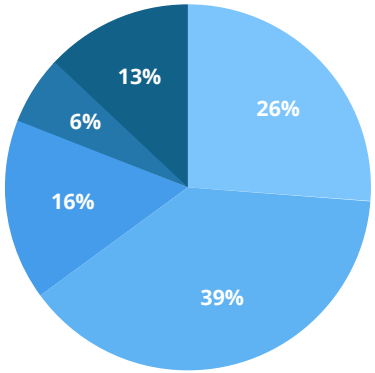
Clean restore
Eliminate reinfection from malware in system state and bare metal backups

Advanced automation
Automate the entire recovery process to reduce downtime and eliminate errors

Be a hero →

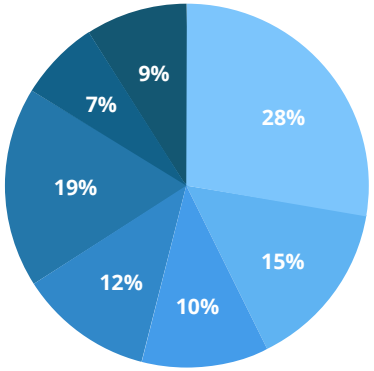
Methodology

Throughout 2019 and 2020, Semperis surveyed identity and access management (IAM) leaders, architects and technical professionals, C-level executives, and IT security professionals to capture top trends related to recovering Active Directory from cyber disasters. Over 350 participants, representing mostly midsize and large firms across six major industry sectors, answered ten custom survey questions. We gathered the insights from this survey at security-focused conferences and digital polls. Participants were offered a $25 Amazon gift card to take part in the survey. Many thanks to those who participated!



Company Size (employees)

- < 5,000
- 5,000-25,000
- 25,000-50,000
- 50,000-100,000
- 100,000+



Industry

- Financial Services
- Technology & Telecomm
- Government
- Manufacturing
- Healthcare
- Energy & Utilities

About Semperis

Semperis is the pioneer of identity-driven cyber resilience for cross-cloud and hybrid environments. The company provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services—the keys to the kingdom. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors. Semperis is headquartered in New York City and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference. The company has received the highest level of industry accolades; most recently being named Best Business Continuity / Disaster Recovery Solution by SC Magazine's 2020 Trust Awards. Semperis is accredited by Microsoft and recognized by Gartner.

+1-703-918-4884
info@semperis.com
www.semperis.com

7 World Trade Center at
250 Greenwich Street, 10th floor
New York NY 10007

Endnotes

01. Source: “Active Directory czar rallies industry for better security, identity,” Zdnet.com, June 9, 2015.
02. Source: “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021,” Cybersecurityventures.com, October 21, 2019.
03. Source: “A Cyber-First Approach to Disaster Recovery,” SANS Institute, July 25, 2019.
04. Source: “Rebuilding after NotPetya: How Maersk moved forward,” Csoonline.com, October 21, 2019.
05. Source: “Maersk CISO Says NotPeyta Devastated Several Unnamed US firms,” Darkreading.com, December 9, 2019.
06. Source: “The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History,” WIRED, October 17, 2019.
07. Source: “Active Directory Forest Recovery Guide,” Microsoft, August 09, 2018.
08. Source: “2019 Data Breach Investigations Report,” Verizon, May 08, 2019.
09. Source: “Ransomware Recoverability Must Be A Critical Component Of Your Business Continuity Plans,” Forrester, October, 2019.
10. Source: “Maersk’s Adam Banks Reflects on NotPetya Response and Recovery,” Infosecurity-magazine.com, September 10, 2019.
11. Source: “When Ransomware Cripples a City, Who’s to Blame? This I.T. Chief Is Fighting Back,” The New York Times, August 22, 2019.
12. Source: “Ransomware groups continue to target healthcare, critical services; here’s how to reduce risk,” Microsoft, April 28, 2020..