semperis

After the Cyberattack: Assessing the ROI of a Quick Active Directory Recovery

WHITE PAPER

The Toll from Cyberattacks on Businesses, Services, and Public Safety Is Skyrocketing

Across every industry, cyberattacks are on the rise—wreaking havoc on day-to-day life by disrupting the flow of products and services to consumers, bringing businesses to a standstill, and threatening public safety. Justifying the time and resources to ensure a cyber-first business recovery plan might be difficult for organizations that have yet to experience an attack.

But as more cyberattacks make the headlines and the cost of ransom payments and cyber insurance soars, business leaders need to prioritize developing a tested cyber-first business recovery plan. The first step is securing Active Directory, the core identity store for most businesses worldwide.

Active Directory is the prime entry point for cybercriminals: Mandiant reported that 90% of the attacks their team investigates involve Active Directory—either as the initial attack vector or the gateway to elevated privileges. The vast majority of cyberattacks in the last year—including the massive SolarWinds breach—involved compromised identity credentials.

Companies that have experienced the nightmare of a cyberattack learn quickly that every minute counts when a breach is in progress. And although IT teams and business leaders might be tempted to simply get the business running again as quickly as possible, failure to properly restore Active Directory can lead to a second attack—often employing the same tactics that worked the first time.

The question is not how an organization can afford to invest time and resources in ensuring a quick, cyber-first Active Directory plan. The question is how it can afford not to.

THE COSTLY AFTERMATH OF CYBERATTACKS

$200M to $300M

Estimated revenue loss by Maersk, the world's largest shipping company, following the NotPetya cyberattack

$265B

Predicted cost of ransomware incidents worldwide by 2031

72%

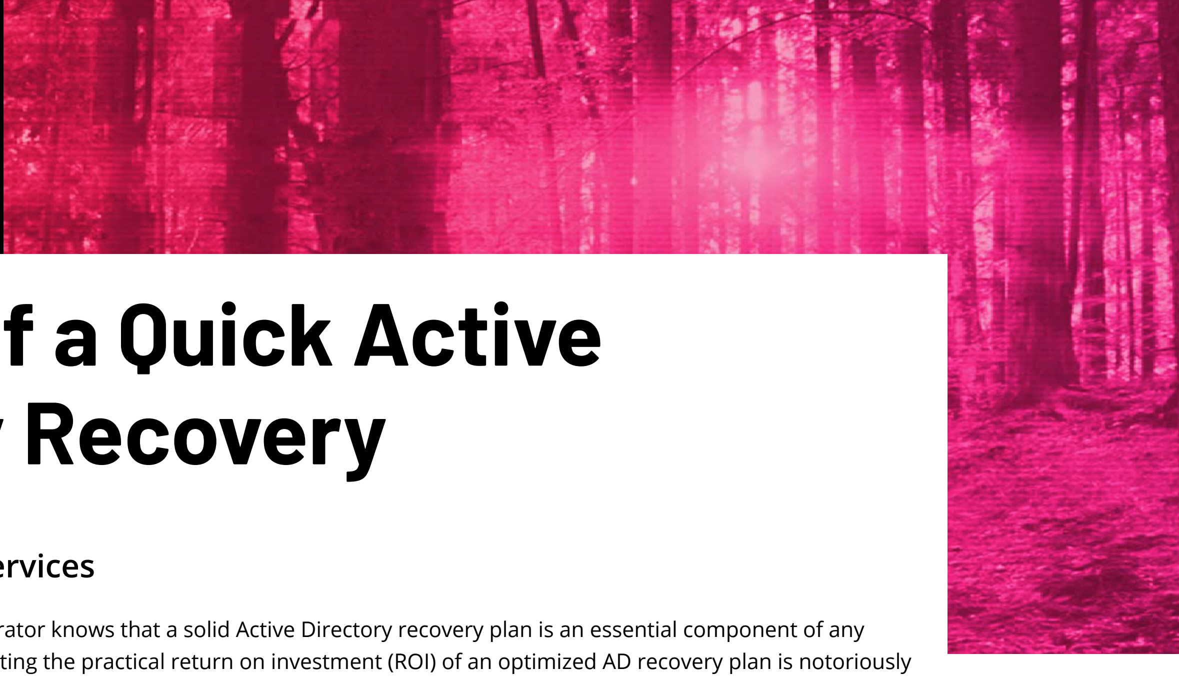
Cybersecurity workload increase since 2020 for IT teams in retail

$5M

Ransomware paid by Colonial Pipeline to hackers

40% to 60%

Rise in cyber insurance premiums between 2020 and 2021



The ROI of a Quick Active Directory Recovery

By Sean Deuby
Semperis Director of Services

While every IT manager or administrator knows that a solid Active Directory recovery plan is an essential component of any business continuity strategy, calculating the practical return on investment (ROI) of an optimized AD recovery plan is notoriously tricky. Too many variables are at play to generate a defensible, exact calculation. And to set expectations up front: I won't offer any sort of interactive ROI calculator here.

Instead, I want to take a look at a few practical ways to see a return on your investment in ensuring a proper AD recovery—allowing you to do your own calculations and come to your own conclusions. Rather than framing this discussion within a scenario that goes beyond the simple case of losing a domain controller, let's look at a more realistic scenario where the impact on AD can be significant, and AD recovery can be a white-knuckle, under-the-gun challenge: a ransomware attack.

In the last year, we've discussed scores of ransomware attacks where cybercriminals modified AD in one way or another—far beyond the basic changes to user accounts or passwords—to gain entry into information systems and move laterally to propagate malware. Ransomware architects now have engineers on staff who are dissecting AD and its security updates looking for opportunities to elevate permissions and quickly distribute malware across the entire organization. Post-attack forensics from previous ransomware attacks involving AD have revealed that threat actors primarily focus on changes to group accounts, user accounts, Group Policy objects, the SYSVOL, and domain controllers.

With these cybercriminal tactics in mind, consider the following factors in calculating your own AD recovery ROI:

- **Cost of operational losses:** It's likely that a material part of your operations relies on AD being up and running to authenticate users as the basis for providing access to applications, systems, and data. For every hour that AD cannot operate, how much revenue or productivity would your business lose? How many hours, days, or weeks would it take before the business passes a point of no return and cannot financially recover? Remember the ransomware attack on the City of Baltimore? Their recovery of operations took months and cost over $18 million.

- **Lack of a business continuity plan that includes AD**: If your organization is mature enough, you have a BC/DR plan in place defining the work needed to restore business operations after an outage. Most plans account for loss of infrastructure or loss of a location after a natural disaster. But few companies have a plan specifically for restoring business after a cyberattack—and especially one as unpredictable as a ransomware attack. The way you recover AD in a scenario like this depends on what changes cybercriminals made within AD. You might plan to recover AD back to a previous version, but how do you determine how far back you need to go to find a known secure version? What AD-dependent systems, services, and applications will be affected or won't function at all because of a broad-stroke recovery to an earlier AD state? Are you confident that you can even locate a recent, malware-free backup from which to restore? Without a plan or an ability to understand what was changed in AD before recovering, your organization will spend incalculable time fixing all the problems the recovery caused.

- **Recovery might not be the answer**: If all the changes being made by the bad guys during an attack boil down to, let's say, adding an account to the Domain Admins group, then recovering AD to a few days ago or last month might not be the right answer. Instead, perhaps the less costly method is to monitor changes in AD and have an ability to either disallow changes to "protected" accounts (like the Domain Admins group) or to automatically revert a change to a sanctioned configuration.

The considerations above summarize to three risks: the risk of a slow recovery, the risk of a recovery that creates more remediation work, and the risk of a recovery that might be considered overkill for the nature of the changes made to AD.

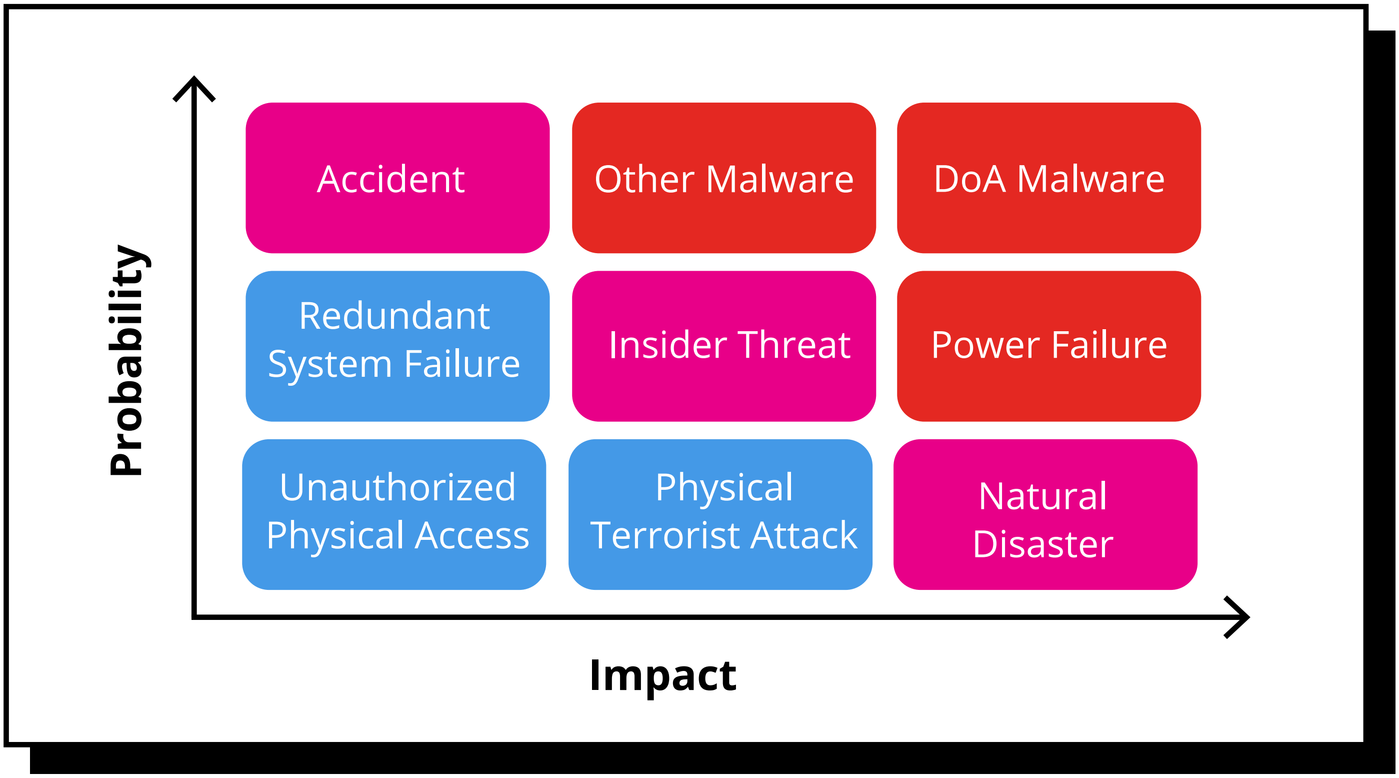
A different approach to calculating the ROI of AD recovery

Instead of looking at the ROI of AD recovery using some calculator you found online, the better choice is to work through several real-world scenarios and evaluate how your current means of AD recovery would fare by answering the following questions based on the factors outlined above:

- What critical parts of the operation depend on AD to function? What is the estimated cost of their downtime?
- How long will it take to recover AD based on the changes made during an attack?
- Do you have visibility into what malicious changes were made in AD and, if not, how far back will you need to investigate and how long will that take you?
- Will the recovery impact any other parts of operations that you will need to fix and, if so, how long will that take? (Remember that some number of both user and computer account passwords will not match, impeding the ability to log on to the domain. Plus, earlier versions might be missing accounts, group memberships, DNS records, etc.)
- Are you confident that recovery will put you into a known-secure state? Beware of the difference between resuming business operations and recovering business operations: If you don't have a clean, malware-free backup from which to recover, you run the risk of reintroducing the same vulnerabilities that left you open to attack in the first place.

In short, the ROI of AD recovery has much more to do with your current ability to recover to a known-productive and known-secure state post-attack than it does with an online ROI calculator that doesn't account for the myriad variables involved in a ransomware attack. By walking through some scenarios and thinking specifically about what your current recovery abilities are, you will expose costs that can be eliminated by having a proper AD recovery solution in place—one that is designed to protect against, prevent, and recover from malicious changes to AD.

Cyber-First Disaster Recovery Risk Matrix



Accident	Other Malware	DoA Malware
Redundant System Failure	Insider Threat	Power Failure
Unauthorized Physical Access	Physical Terrorist Attack	Natural Disaster

Quick stories from the field

Semperis provides top-rated cyber-first disaster recovery for Active Directory. Some of the results our customers have reported after deploying Semperis Active Directory Forest Recovery:

- Israeli airline El Al deployed Semperis ADFR and reduced complete AD forest recovery time from 24 hours to two hours.
- A global retailer with 2.2 million users and 500 DCs switched to Semperis ADFR from their existing solution and reduced the time to recover an AD forest from 6 days to 6 hours.
- A healthcare company with a 65GB DIT reduced time to recover the AD forest from 1.5 days with their existing solution to under 4 hours with Semperis ADFR.

> *We have protected 3 forests with ADFR. Our test restores are reliable, and I feel confident that we could fully recover our AD forests in a short amount of time using the Full Forest Recovery option.*

Microsoft Active Directory System Engineer
Services Industry (500M-1B)

Semperis
IT Resilience Orchestration
5 ★★★★★
Source: Gartner Peer Insights

Want to learn more?

Check out the following resources from our team of AD experts for more information about ensuring a complete AD recovery plan.

- ↗ Cyber-First Disaster Recovery for Active Directory
- ↗ Recovering Active Directory from Cyber Disasters
- ↗ Recovering Active Directory Cleanly: Without Re-introducing Malware

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

221 River Street
9th floor
Hoboken, NJ 07030

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.

semperis