PETRI
WE GET IT

FEBRUARY 2024

Active Directory Forest Recovery and IT Organization Readiness

a Petri.com Audience Survey

Sponsored By: Cayosoft

PETRI.COM
RESEARCH LAB

PETRI
WE GET IT

TABLE OF CONTENTS

PETRI.COM RESEARCH LAB PRESENTS:

Active Directory Forest Recovery and IT Organization Readiness

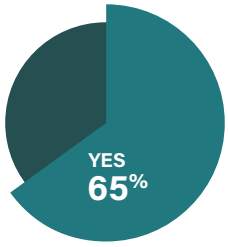
a Petri.com Audience Survey

Active Directory (AD) remains a linchpin in IT security and access control, despite its decades-long tenure. As enterprises juggle a complex array of applications, remote work demands, and escalating cyberattacks, the continuous availability of AD is not just ideal—it's critical for maintaining business operations.

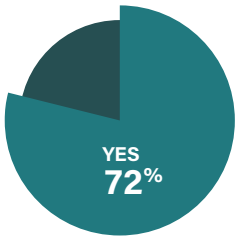
Have you experienced a forest-wide Active Directory (AD) outage?

72% of mid-sized organizations have experienced a forest-wide AD outage, and the risk climbs to over 90% for large organizations.

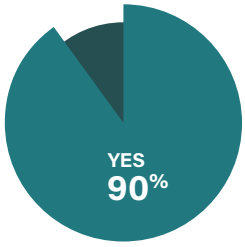
While AD is designed for scalability, the larger the organization, the greater the complexity of their AD infrastructure and the greater the challenge to ensure your critical infrastructure, systems, and data are secure and operational.



COMPANY SIZE OF
1-1,000



COMPANY SIZE OF
1,001-9,999



COMPANY SIZE OF
10,000+

"90% of enterprise-sized organizations have experienced a forest-wide Active Directory outage"

What caused the outage?

Our survey reveals a stark reality: Active Directory outages stem from a number of failure vectors — cyberattacks (30%), hardware/environmental failures (43%), human error (21%), and licensing issues (6%).

This data drives home the necessity for IT organizations to fortify their AD environments and to develop agile and ready-to-execute recovery processes to promptly bounce back from a myriad of potential disruptions.

The research also highlights that organizations with more than 10,000+ team members are twice as likely to experience AD downtime due to cyberattack.

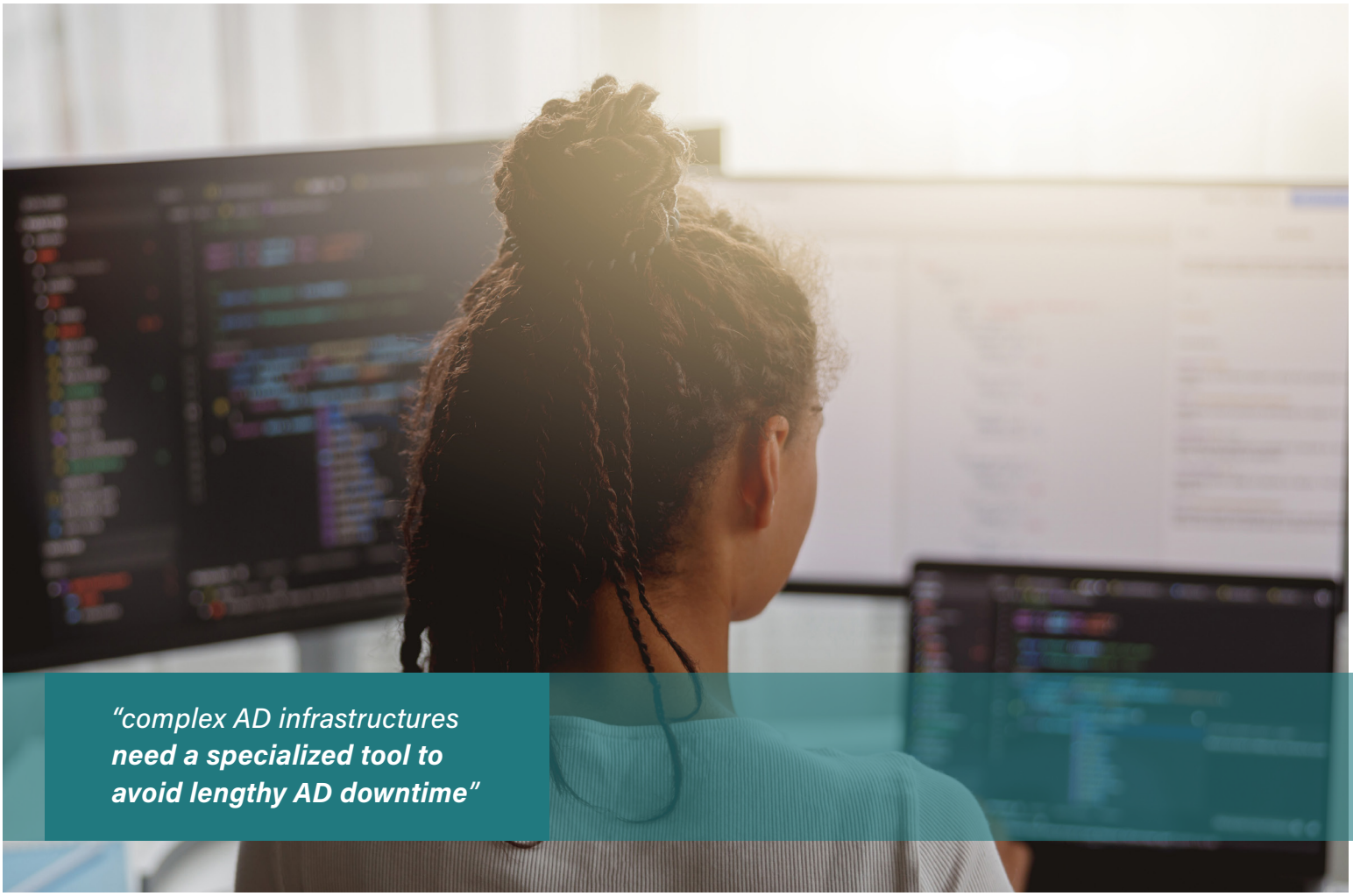
43%
FAULTY HARDWARE OR ENVIRONMENT

30%
CYBERATTACK

21%
HUMAN ERROR

6%
LICENSING ISSUES

*"Organizations with more than 10,000+ team members are **twice as likely to experience AD downtime due to cyberattack**"*

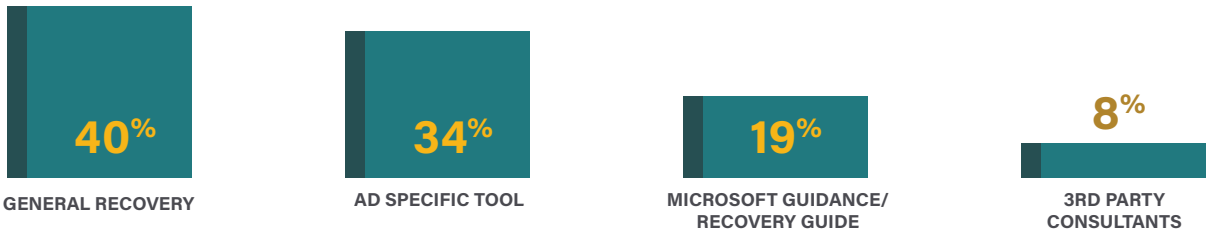


What did you use to expedite the recovery process?

For organizations that needed to perform an AD recovery, the responses showed that 40% of all organizations surveyed relied on general recovery tools versus an AD-specific disaster recovery solution. Specific AD recovery tools can help organizations recover from an outage much faster than a generic or general backup products.

Organizations are often fooled, or being penny-foolish, that a one-size-fits-all general backup solution can also recover AD quickly. They do not make the investment in tools that ensure their ability to achieve short recovery time objectives (RTO) for their business.

While recovering an AD forest, environments that only operate one or two domain controllers (DC), using a general backup solution might enable an acceptable RTO. Complex AD infrastructures need a specialized tool to avoid many hours, days, or weeks of downtime.

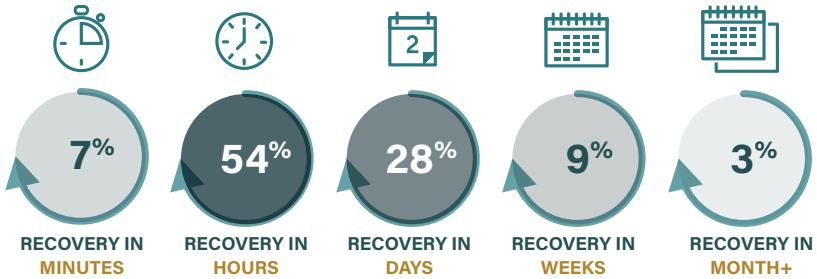


How long did the recovery process take?

An alarming number of companies are caught off-guard by AD outages, with significant downtime impacting even large organizations due to the complexities of restoring their AD infrastructure.

Given that 40% of large organizations, those with over 10,000 employees, needed "More than Days" to recover from a forest-wide AD outage, it's evident that the complexity of the restoration process is often underestimated. The significant financial implications of extended downtime warrant serious concern from every Board of Directors' audit committee.

This underscores an urgent need for organizations to prioritize their AD disaster recovery planning, ensuring rapid restoration to mitigate business interruptions.



* Companies with greater than 10,000 employees

*"Active Directory downtime: **A glaring blind spot in Enterprise Risk Management"***

Top advice for those who've not experienced an AD outage?

IT organizations must have the disciplines of planning, preparation, and practice, instilled within a culture of excellence and readiness to protect their organizations.

IT leaders must be able to advocate and guide the executive leadership teams within their organization to be aware of the risks and to ensure adequate investment in tools and resources.

Our survey respondents, 72% of whom have experienced a forest-wide AD outage, shared the following wise counsel.

18% "Have a clean environment on standby"

45% "Test your recovery process... Day of outage is not the day to find issues"

37% "Use a third-party tool (makes it easier & faster)"

How much money would your organization lose a day in employee downtime?

60% of companies in our survey stated that the daily employee cost due to an outage would exceed $100,000 per day, and 5% of companies stated the expense would exceed $1 million per day.

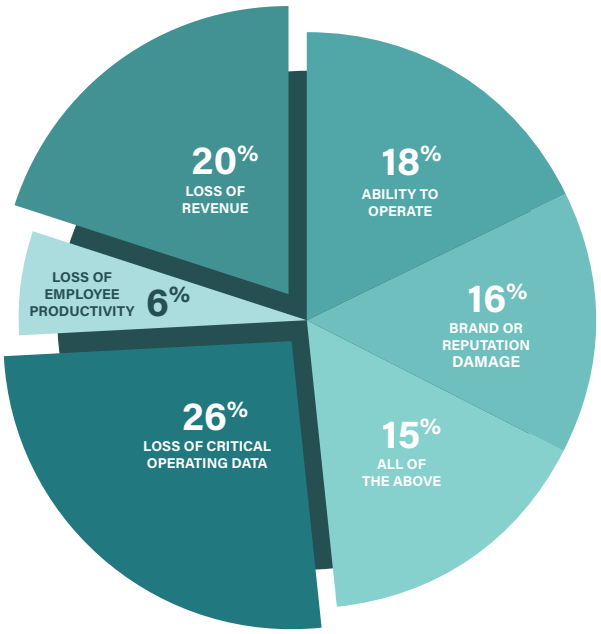
40% LOSE < $100K PER DAY

41% LOSE $100K-$500K PER DAY

15% LOSE $501K-$1M PER DAY

5% LOSE $1M+ PER DAY

Which scenario is of most concern during an AD outage?



Loss of critical operating data (26%) was the biggest concern, and maybe not surprisingly even more important than loss of revenue (20%). Loss of revenue is a temporary effect of AD downtime, but loss of critical data can put your organization's intellectual property at risk and out of business forever.

Powerfully, 16% of respondents understood the risk to the company's brand reputation. Years to build and seconds to break — brand reputation grows by spoonful but spills by bucket.

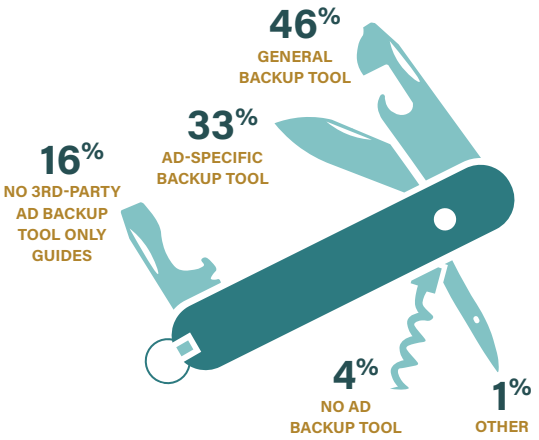
*"Years to build and seconds to break — **brand reputation grows by spoonful but spills by bucket**"*

Pick the scenario that best represents your current AD backup/recovery situation.

Only 1/3rd of organizations have a specialized AD backup and recovery tool.

Nearly 5 in 10 companies rely on a general backup tool, increasing their risk of a costly and lengthy business outage.

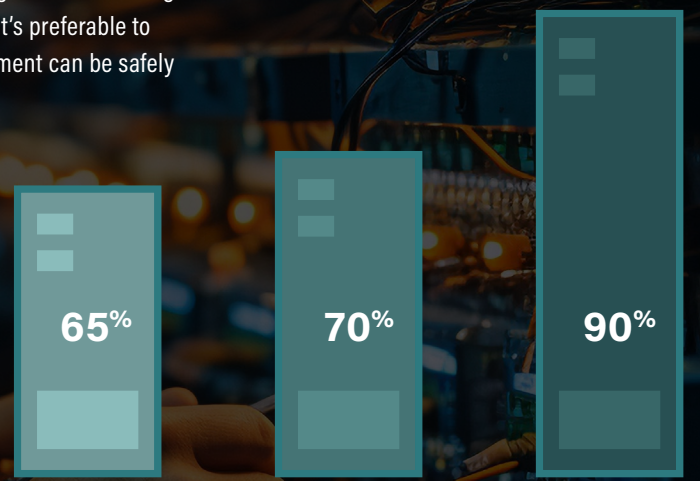
Even more frighteningly, 4% of all companies reported they had no AD backup tool in place, and 16% reported having no AD backup and recovery tool and relied on guides and scripts.



Does your AD recovery plan mandate rebuilding servers or standby hardware?

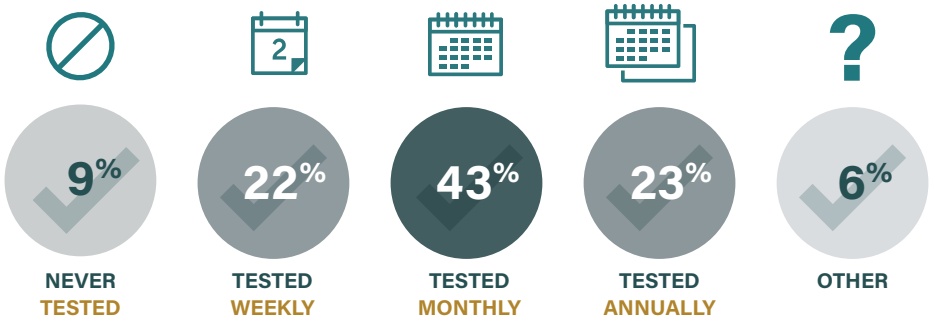
73% of organizations need to rebuild or have clean servers available as part of their recovery plan. But rebuilding servers is time consuming. And maintaining clean servers is costly. For the ability to recover AD quickly, it's preferable to switch to standby cloud DCs until your on-premises environment can be safely used for a complete AD restore operation.

REQUIRING SERVERS TO BE REBUILT OR TO MAINTAIN CLEAN HARDWARE



How often do you test the recovery of your AD?

Nearly 1/3rd of organizations only test AD restores annually, or worse, never. Those testing weekly or monthly either have less complex environments to restore or are most likely automating restore operations, enabling them to test restore operations more frequently and achieve shorter RTOs.



Conclusion

a Petri.com Audience Survey

Active Directory has been around for more than 20 years and it is considered a mature technology. But it hasn't seen any significant updates since 2016 as Microsoft has instead focused on its cloud Identity and Access Management (IAM) solution, Microsoft Entra ID (previously Azure AD). But despite the stagnation, Active Directory is still the most common on-premises IAM solution used today.

Despite Active Directory's longevity, it's hard to find expertise. And it is often poorly understood, leading to inadequate preparations in the event of a disaster recovery scenario. And the results of our survey show that at least half of all organizations, regardless of size, are either inadequately prepared for an AD outage or if somewhat prepared, would be unable to meet a short RTO. And as many AD attacks have shown, the potential for outages to lead to considerable losses is real.

Methodology

a Petri.com Audience Survey

Petri.com is often approached by industry leaders to survey our audience on topics that are important for IT organizations. We then ask our audience to respond to a survey of ten, clear, concise, and relevant questions. Our highly engaged audience of IT practitioners and leaders is the perfect audience to gage market trends. This topic struck an enthusiastic chord, and we received nearly 1,000 responses from IT professionals and managers from a wide variety of industries and company sizes.

Survey results are analyzed to draw meaningful insights and the findings are then presented with the raw numbers and visualizations that help guide and sharpen strategies for leading IT solution providers, IT Pros, and IT organizations to understand their business implications. We also include editorial commentary to assist putting the results into context and how they fit into the current marketplace.

In this survey on Active Directory recovery, Cayosoft commissioned us to survey our IT Pro audience but otherwise remained hands off. The survey was designed with a set of quantitative and qualitative questions intended to get respondents thinking about their organization's own preparedness for a forest-wide Active Directory outage. The survey also provide Petri.com's editorial team and contributing experts with the market's current state of Active Directory disaster recovery readiness.

APPENDIX: RESULTS 1-2

PETRI

1. Have you experienced a forest-wide Active Directory (AD) outage?

Response	1-1000	1001-9999	10,000+	Total
No	56	11	6	140
Unsure	1	2	2	8
Yes	108	48	74	387
Grand Total	165	61	82	535

No	34%	18%	7%	26%
Unsure	1%	3%	2%	1%
Yes	65%	79%	90%	72%
Grand Total	100%	100%	100%	100%

2. What caused the outage?

Response	1-1000	1001-9999	10,000+	Total
Cyberattack	19	15	34	69
Faulty hardware/environment	58	16	24	98
Human error	23	8	16	47
Licensing issues	5	7	2	14
Grand Total	105	46	76	228

Cyberattack	18%	33%	45%	30%
Faulty hardware/environment	55%	35%	32%	43%
Human error	22%	17%	21%	21%
Licensing issues	5%	15%	3%	6%
Grand Total	100%	100%	100%	100%

3. What did you use to expedite the recovery process?

Response	1-1000	1001-9999	10,000+	Total
3rd party consultants	9	6	3	18
AD specific tool (Quest, Semperis, Cayosoft)	30	21	27	79
General recovery (CommVault, Veeam, Rubrik)	48	13	32	93
Microsoft guidance/recovery guide	21	9	14	44
Grand Total	108	49	76	234

3rd party consultants	8%	12%	4%	8%
AD specific tool (Quest, Semperis, Cayosoft)	28%	43%	36%	34%
General recovery (CommVault, Veeam, Rubrik)	44%	27%	42%	40%
Microsoft guidance/recovery guide	19%	18%	18%	19%
Grand Total	100%	100%	100%	100%

4. How long did the recovery process take?

Response	1-1000	1001-9999	10,000+	Total
Matter of Days	31	10	21	63
Matter of Hours	45	22	41	108
Matter of Minutes	19	7	5	31
Matter of Weeks	12	5	7	24
More than a month	2	3	2	7
Grand Total	109	47	76	233

Matter of Days	21%	21%	28%	27%
Matter of Hours	41%	47%	54%	46%
Matter of Minutes	17%	15%	7%	13%
Matter of Weeks	11%	11%	9%	10%
More than a month	2%	6%	3%	3%
Grand Total	100%	100%	100%	100%

5. Top advice for those who've not experienced an AD outage?

Response	1-1000	1001-9999	10,000+	Total
Have a clean environment on stand-by and ready-to-go!	21	15	4	41
Test your recovery process, day of is not the time to find issues	52	20	34	106
Use a 3rd party tool (just makes it easier and faster)	36	14	37	87
Grand Total	109	49	75	234

Have a clean environment on stand-by and ready-to-go!	19%	31%	5%	18%
Test your recovery process, day of is not the time to find issues	48%	41%	45%	45%
Use a 3rd party tool (just makes it easier and faster)	33%	29%	49%	37%
Grand Total	100%	100%	100%	100%

6. How much total salary/employee expense* would be lost a day at your organization when employees cannot work?

Response	1-1,000	1,001-9,999	10,000+	Total
Between $101K – $500K/day	52	34	39	126
Between $501K – $1M/day	30	7	9	46
Less than $100K/day	77	16	30	123
More than $1M/day	6	4	4	14
[blank]	0	0	0	0
Grand Total	165	61	82	309

Between $101K – $500K/day	32%	56%	48%	41%
Between $501K – $1M/day	18%	11%	11%	15%
Less than $100K/day	47%	26%	37%	40%
More than $1M/day	4%	7%	5%	5%
[blank]	0%	0%	0%	0%
Grand Total	100%	100%	100%	100%

* How it was calculated (#employees × avg salary ÷ 260 workdays) per or in a day

7. In the event of an Active Directory outage, which of the following scenarios are you most concerned about?

Response	1-1,000	1,001-9,999	10,000+	Total
Ability to operate	36	8	12	56
All of the above	32	6	7	45
Brand or reputational damage	19	16	14	49
Loss of critical operating data	44	16	18	79
Loss of employee productivity	12	2	4	18
Loss of revenue	22	13	27	62
Grand Total	165	61	82	309
Ability to operate	22%	13%	15%	18%
All of the above	19%	10%	9%	15%
Brand or reputational damage	12%	26%	17%	16%
Loss of critical operating data	27%	26%	22%	26%
Loss of employee productivity	7%	3%	5%	6%
Loss of revenue	13%	21%	33%	20%
Grand Total	100%	100%	100%	100%

8. Pick the scenario that best represents your current AD backup/recovery situation

Response	1-1,000	1,001-9,999	10,000+	Total
Other (please specify)	2	1	0	3
We do not have an AD backup tool in place	7	3	1	11
We have a general backup tool like CommVault, Veeam, Rubrik for AD recovery	84	16	42	142
We have an AD specific backup tool like Quest, Semperis, Cayosoft	46	24	30	101
We have no 3rd party AD backup tool but have guides and scripts to help	24	17	9	50
We have several domain controllers in place in case one should fail	1	0	0	1
Windows backup	1	0	0	1
Grand Total	**165**	**61**	**82**	**309**

Other (please specify)	1%	2%	0%	1%
We do not have an AD backup tool in place	4%	5%	1%	4%
We have a general backup tool like CommVault, Veeam, Rubrik for AD recovery	51%	26%	51%	46%
We have an AD specific backup tool like Quest, Semperis, Cayosoft	28%	39%	37%	33%
We have no 3rd party AD backup tool but have guides and scripts to help	15%	28%	11%	16%
We have several domain controllers in place in case one should fail	1%	0%	0%	0%
Windows backup	1%	0%	0%	0%
Grand Total	**100%**	**100%**	**100%**	**100%**

9. Does your AD recovery plan require you to re-build servers/have clean servers available to recover to?

Response	1-1,000	1,001-9,999	10,000+	Total
I don't know	10	6	2	18
No	47	12	6	65
Yes	108	43	74	226
Grand Total	165	61	82	309

I don't know	6%	10%	2%	6%
No	28%	20%	7%	21%
Yes	65%	70%	90%	73%
Grand Total	100%	100%	100%	100%

10. How often do you test the recovery of your AD?

Response	1-1,000	1,001-9,999	10,000+	Total
Annually	45	10	17	72
Monthly	65	23	44	132
Never	20	7	1	28
Other	7	3	0	10
Weekly	28	18	20	67
Grand Total	165	61	82	309

Annually	27%	16%	21%	23%
Monthly	39%	38%	54%	43%
Never	12%	11%	1%	9%
Other	4%	5%	0%	3%
Weekly	17%	30%	24%	22%
Grand Total	100%	100%	100%	100%

These survey results were gathered from the global Petri.com IT professional audience. The survey was commissioned by Cayosoft and was independently created and managed by the Petri.com Research Lab.

PETRI.COM
RESEARCH LAB

About the Sponsor:

Cayosoft

Cayosoft delivers the only unified solution enabling organizations to securely manage, continuously monitor for threats or suspect changes, and instantly recover their Microsoft platforms, including on-premises Active Directory, hybrid AD, Azure AD, Office 365, and more. To learn more visit cayosoft.com