PULSE Cayosoft

Microsoft Directory Disaster Recovery: Business Impact, Mitigation Strategies, & Costs

Microsoft Active Directory (AD) and Azure Active Directory (Azure AD) contain critical user account data and other vital information needed for businesses to operate and for their employees to perform almost every aspect of their jobs. For that reason, AD has become an increasingly targeted area for cyberattacks. To prevent attack exposure and avoid costly business interruptions when disaster strikes, whether from malware campaigns, post-compromise extortion, or insider threats, companies must be prepared for the inevitable outage. While crucial to business continuity, AD recovery, including full forest recovery, if often overlooked, is becoming an increasingly complex process. If recovery is not completed properly or fast enough, companies can be left vulnerable to reinfection, expensive downtime, and possible loss of business reputation.

Pulse and Cayosoft surveyed 200 technology leaders that use an Active Directory tool to find out how common and costly AD outages are and how they are strategizing for effective recovery, in order to better prepare and defend against future cyber attacks.

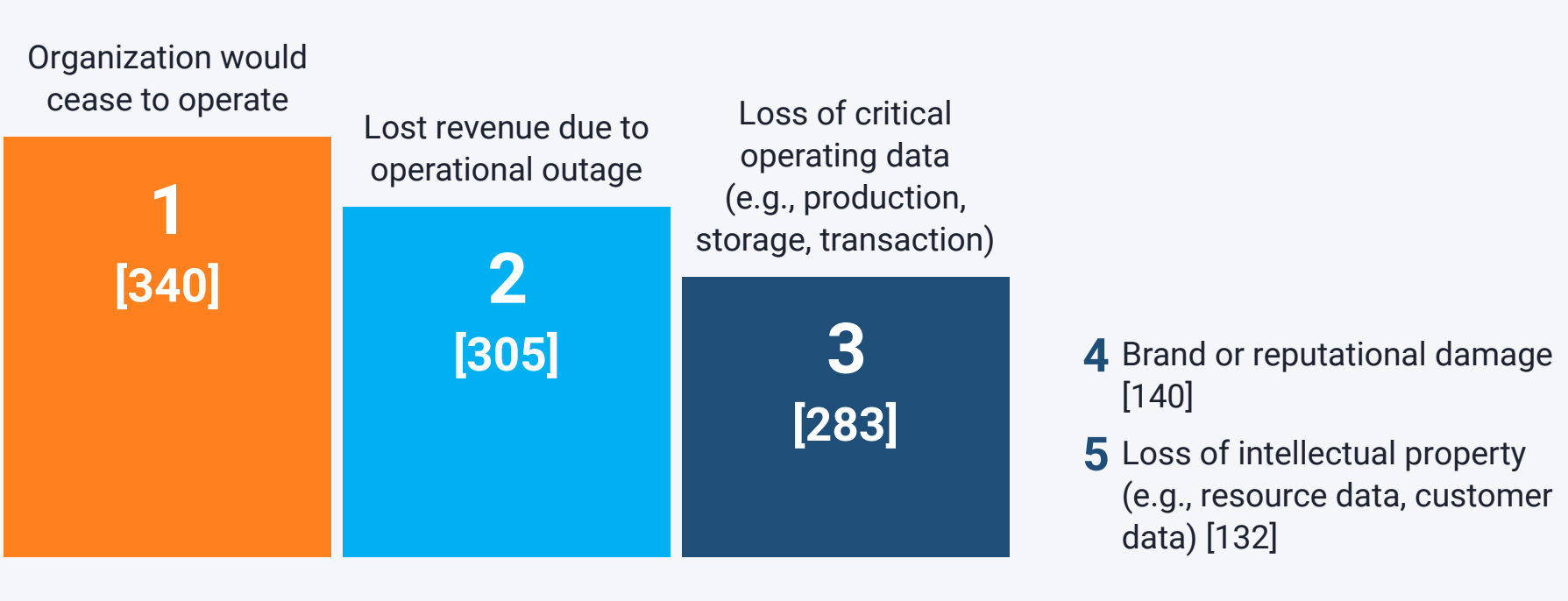
Data collection: October 29 - December 13, 2021

Respondents: 200 technology leaders

ACTIVE DIRECTORY FAILURES ARE COSTLY

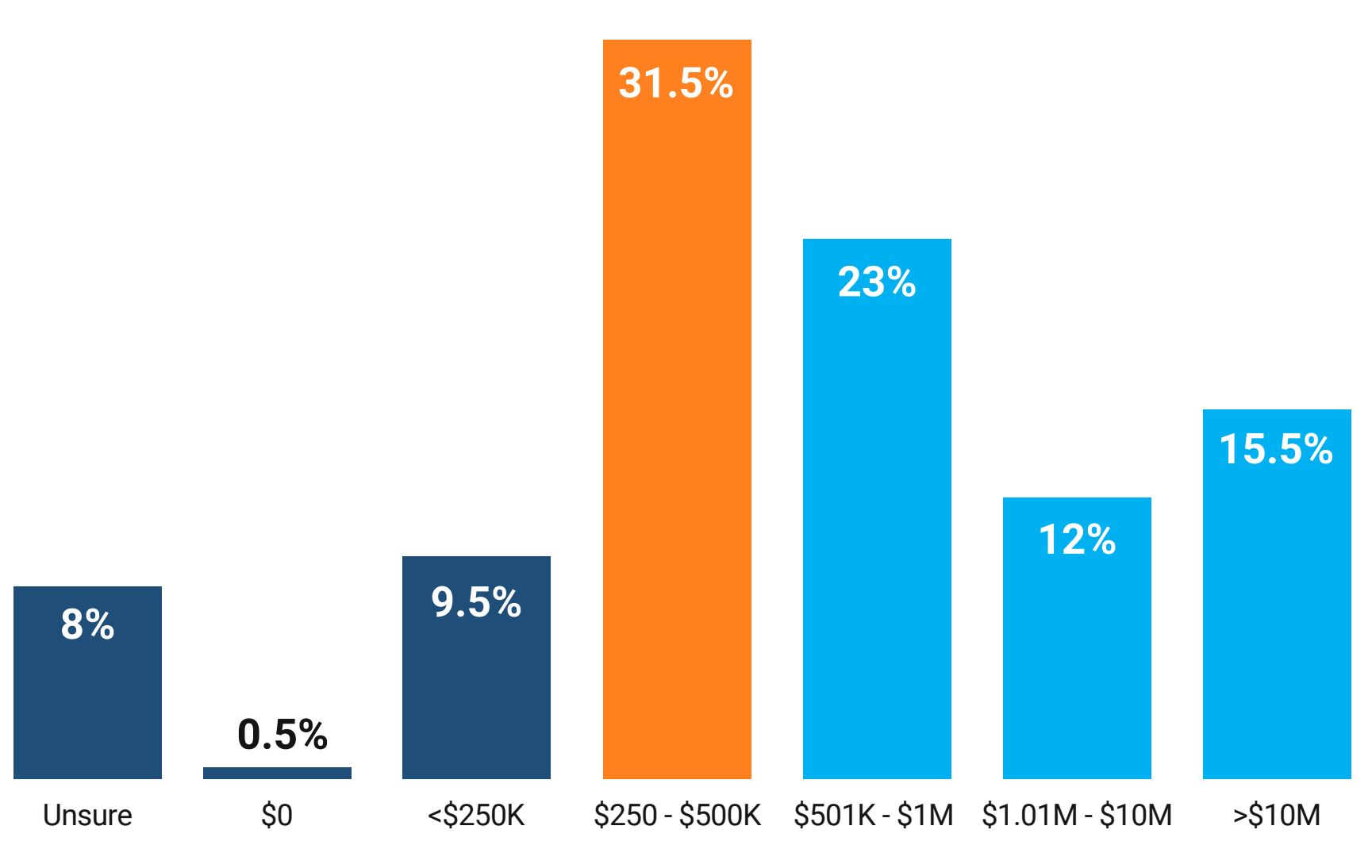
In the event of an Active Directory (AD) failure, technology leaders are most concerned about the organization ceasing to operate, lost revenue due to operational outage, and loss of critical operating data (e.g., production, storage, transaction).

WHAT THREE IMPACTS OF AN ACTIVE DIRECTORY (AD) FAILURE AT YOUR ORGANIZATION ARE YOU MOST CONCERNED ABOUT?



More than half of technology leaders estimate that their company would lose between $250 thousand and $1 million in revenue if their AD became unavailable for 1 week.

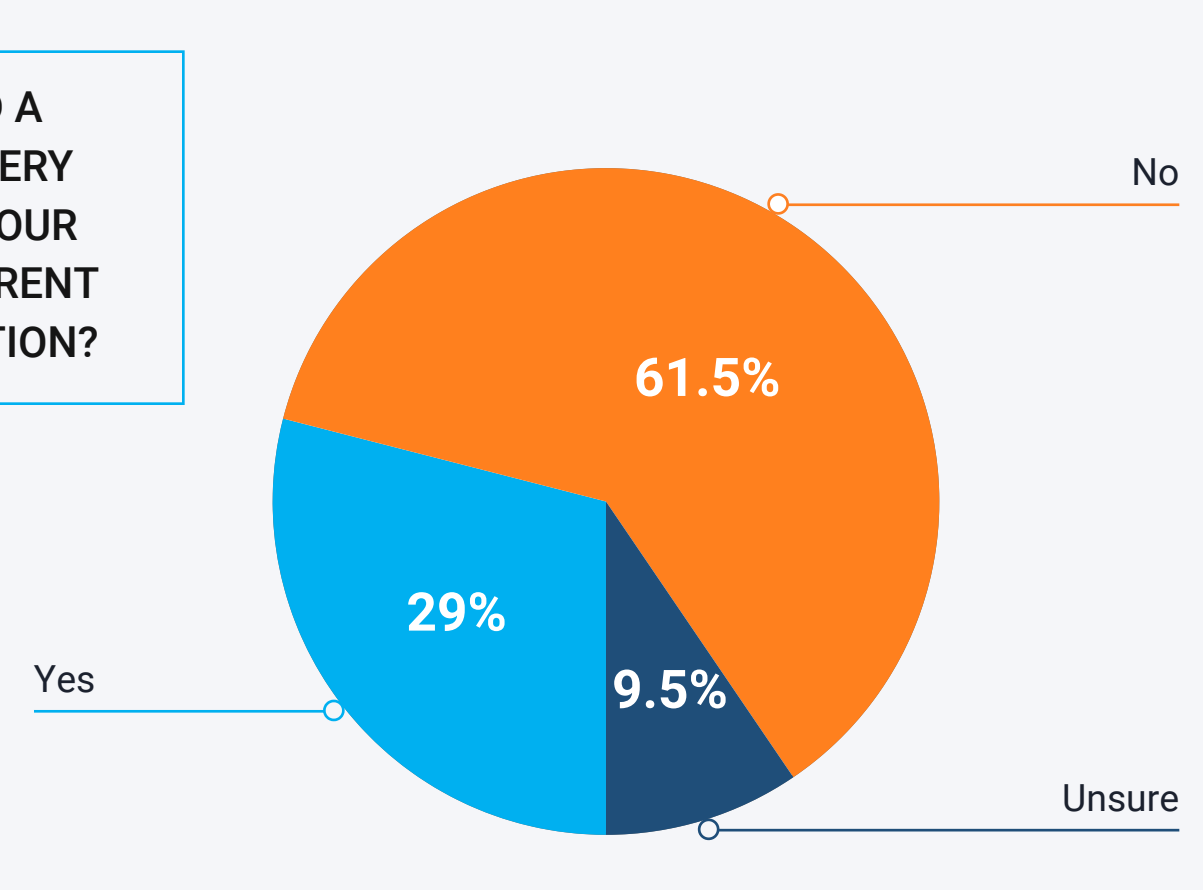
HOW MUCH REVENUE DO YOU ESTIMATE YOUR COMPANY WOULD LOSE IF YOUR AD BECAME UNAVAILABLE FOR 1 WEEK?



RECOVERY IS OFTEN EXPANSIVE AND HAS SIGNIFICANT SECURITY IMPACTS

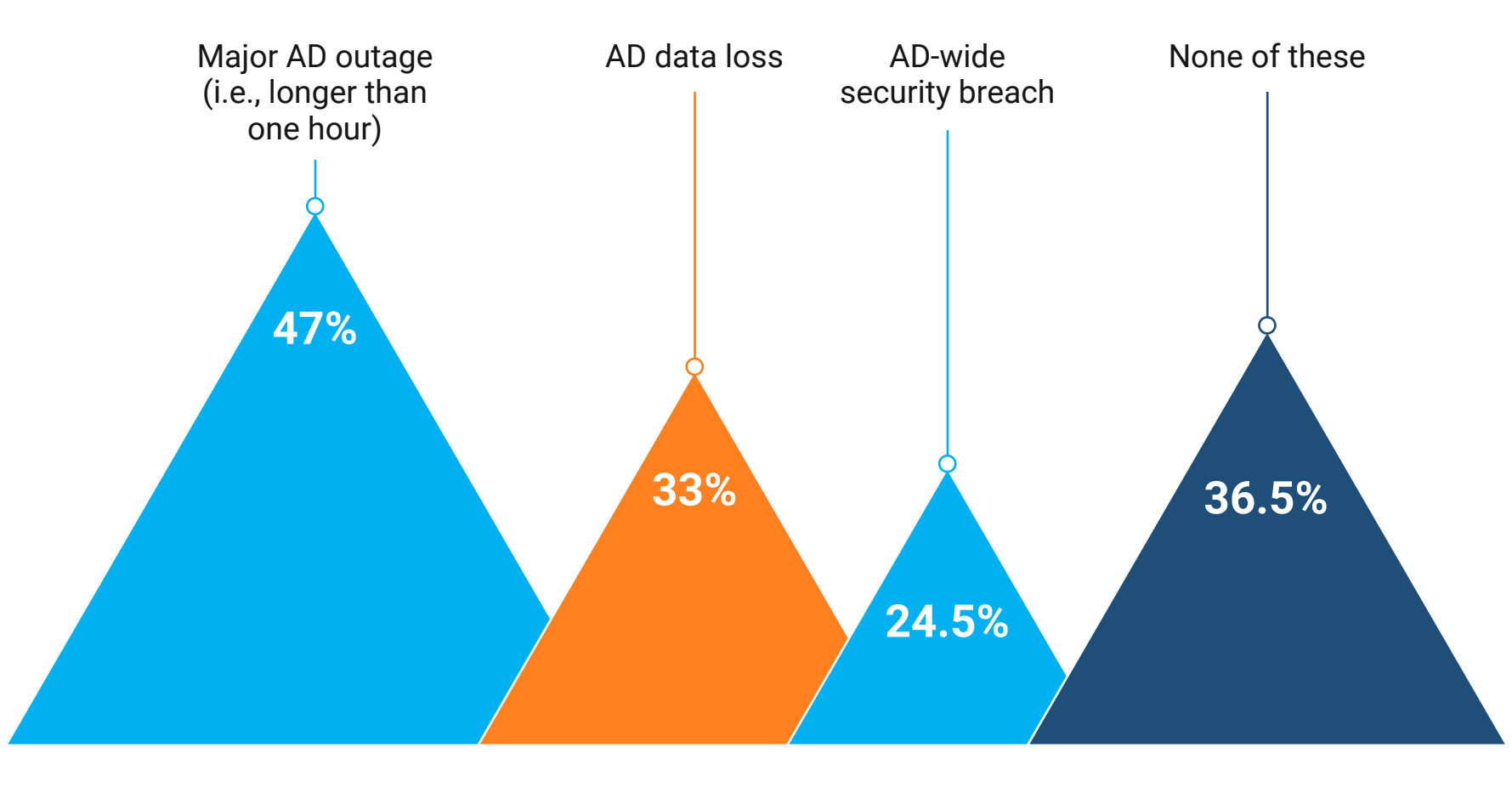
29% of respondents have experienced a forest-wide AD recovery at their current or previous organization.

HAVE YOU EVER FACED A FOREST-WIDE AD RECOVERY (I.E., HAD TO RECOVER YOUR ENTIRE AD) AT YOUR CURRENT OR PREVIOUS ORGANIZATION?



And 47% have experienced an AD outage lasting more than an hour. About one-third (33%) have experienced an AD data loss.

HAVE YOU EXPERIENCED ANY OF THE AD SECURITY INCIDENTS BELOW AT YOUR CURRENT OR PREVIOUS ORGANIZATION?



Describe in as much detail as you can the security impacts of the breach.

"Disastrous for many reasons like reputation and revenue."
- Director, telecommunication services, 5,001 - 10,000 employees

"We had to shut down AD as a result of the breach. Many systems that rely on AD were unavailable. We had to rebuild it from scratch. It was an all hands on deck situation."
- Director, software, 10,001+ employees

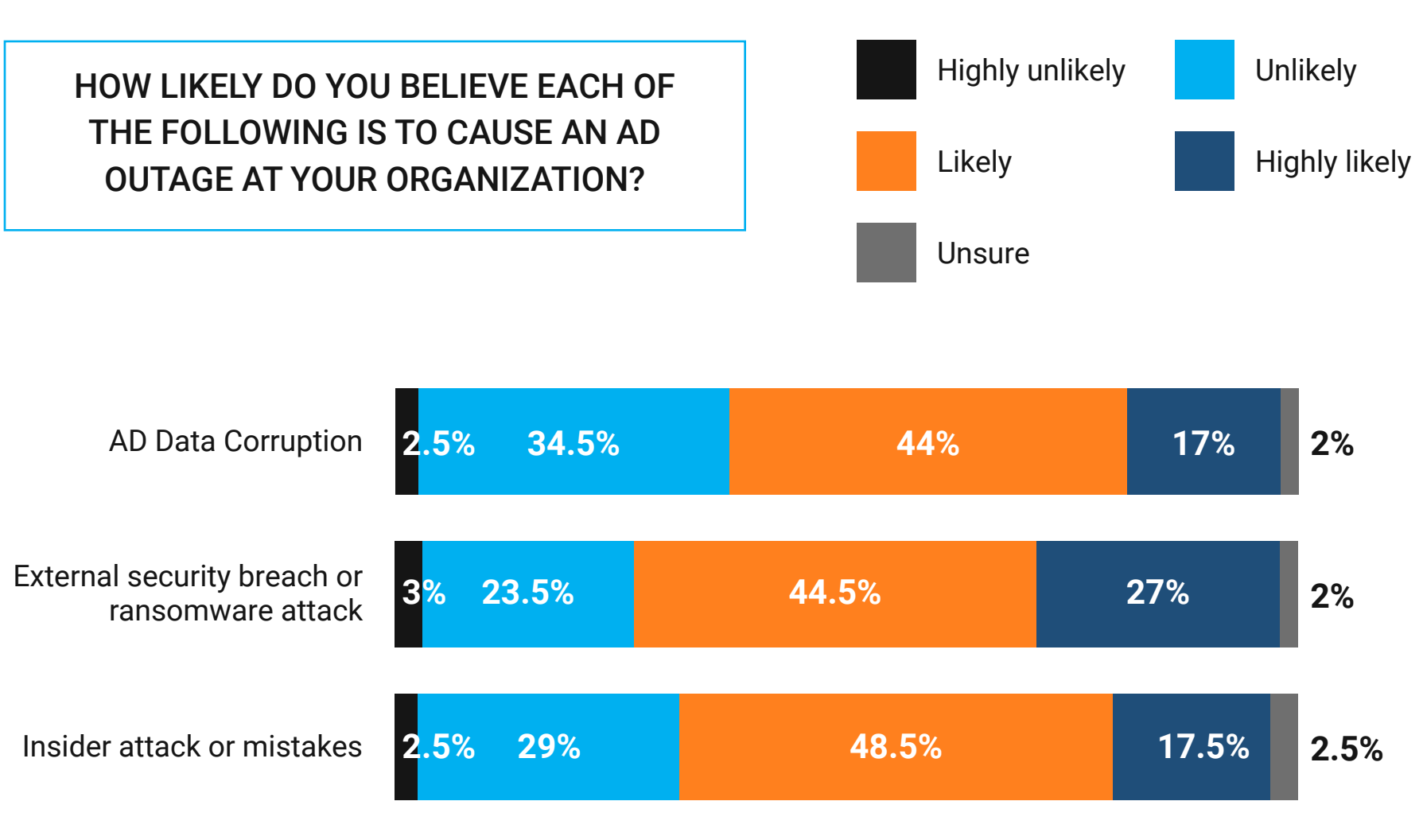
"There was not much of a security impact, but the organization came to an almost grinding halt during the outage."
- Manager, Government, 1,001 - 5,000 employees

"We lost intellectual property on the breaches and in the worst AD crashes it took over 2 days to restore."
- Director, finance, banking & insurance, 10,001+ employees

TECHNOLOGY LEADERS ARE AWARE OF RISKS TO THEIR AD BUT THEIR RECOVERY STRATEGIES MAY NOT BE ROBUST ENOUGH FOR EFFECTIVE RECOVERY

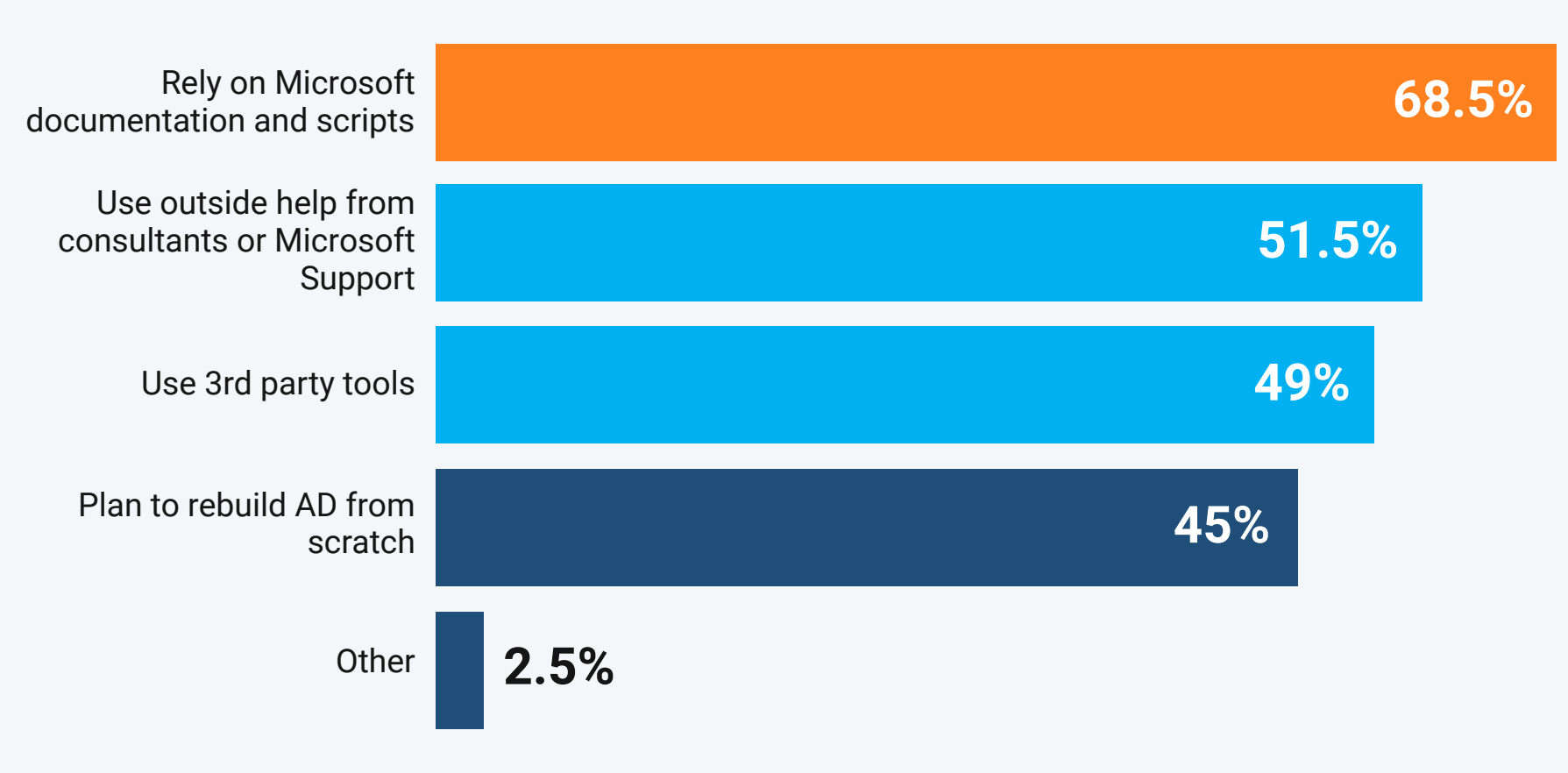
The majority of technology leaders consider it likely that AD data corruption (61%), an external security breach or ransomware attack (71.5%), and insider attacks or mistakes (66%) could cause an AD outage at their organization.

HOW LIKELY DO YOU BELIEVE EACH OF THE FOLLOWING IS TO CAUSE AN AD OUTAGE AT YOUR ORGANIZATION?



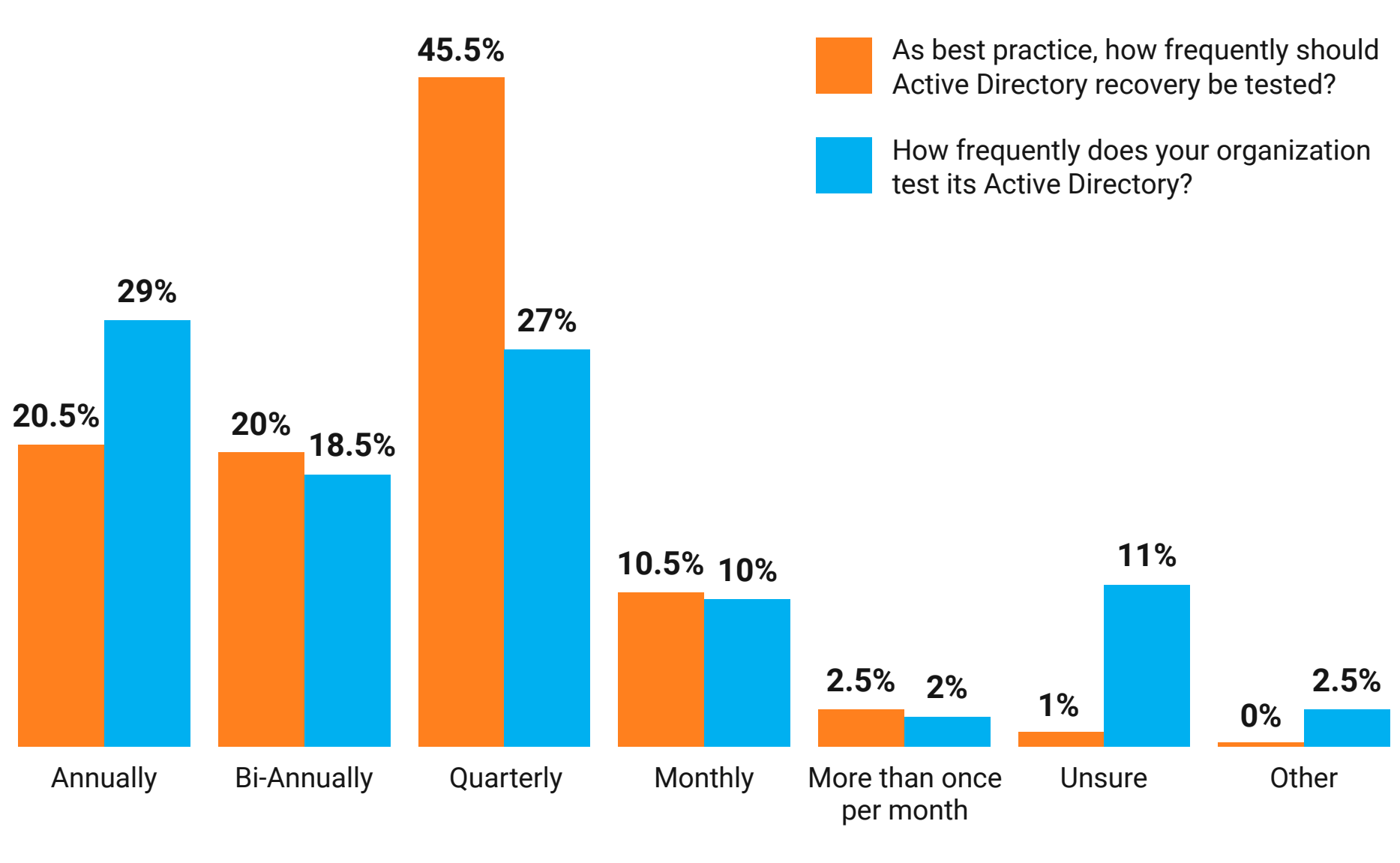
Most respondents rely on Microsoft documentation and scripts (68.5%) and/or use outside help from consultants or Microsoft Support (51.5%) as part of their organization's recovery strategy for on-premises AD after a security breach, AD outage, or directory data loss.

WHICH OF THE FOLLOWING ELEMENT(S) ARE INCLUDED IN YOUR ORGANIZATION'S RECOVERY STRATEGY FOR ON-PREMISES AD AFTER A SECURITY BREACH, AD OUTAGE, OR DIRECTORY DATA LOSS?



AD backup and recovery plans aren't tested as often as they should be. While most (45.5%) agree that testing for AD recovery should be conducted quarterly, only 27% of respondents are doing so. 47.5% test annually or bi-annually and 11% don't know how often they are testing their AD.

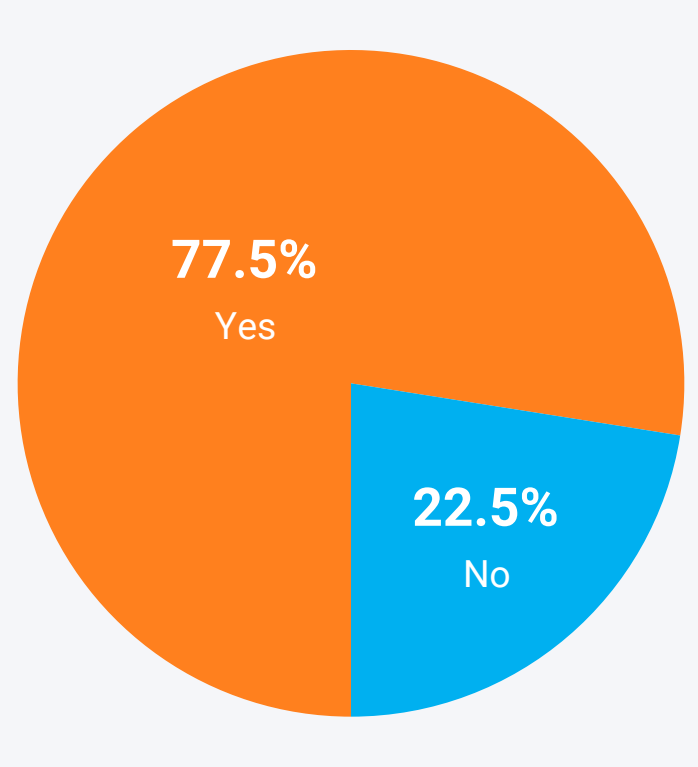
BEST PRACTICE VS CURRENT FREQUENCY OF AD RECOVERY TESTING



ALTHOUGH RESPONDENTS WITH AZURE ACTIVE DIRECTORY TAKE A SIMILAR APPROACH TO AD RECOVERY, THE ADDITION OF CLOUD ADDS TO THE COMPLEXITY OF THE RECOVERY

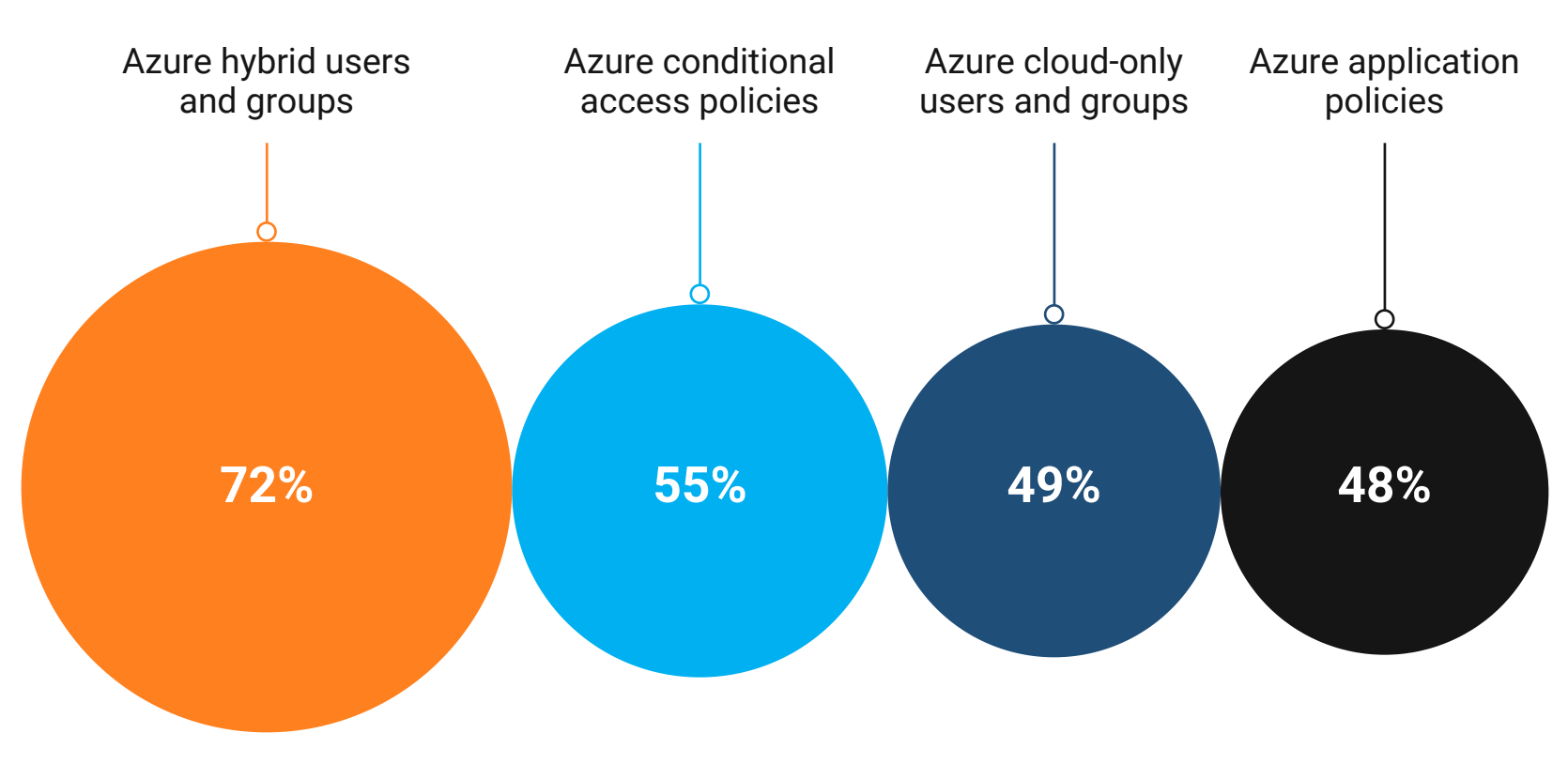
77.5% of technology leaders use Azure Active Directory (Azure AD).

DOES YOUR ORGANIZATION USE AZURE ACTIVE DIRECTORY (AZURE AD)?



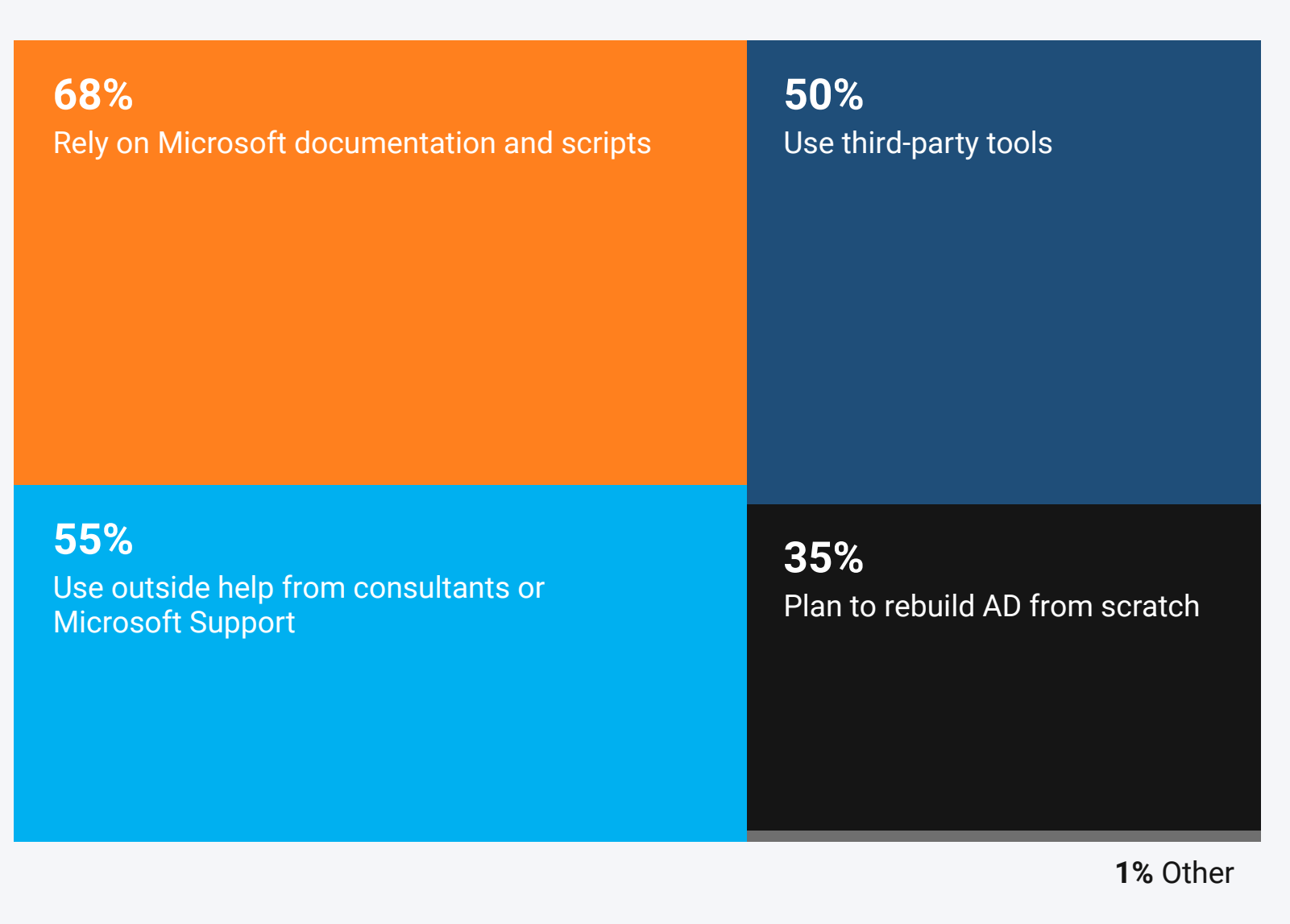
Not all respondents include Azure hybrid users and groups (72%) or Azure AD conditional access policies (55%) in their directory recovery strategies, indicating gaps in the recovery plan.

WHICH OF THE FOLLOWING AZURE AD OBJECTS ARE INCLUDED IN YOUR DIRECTORY RECOVERY STRATEGY?



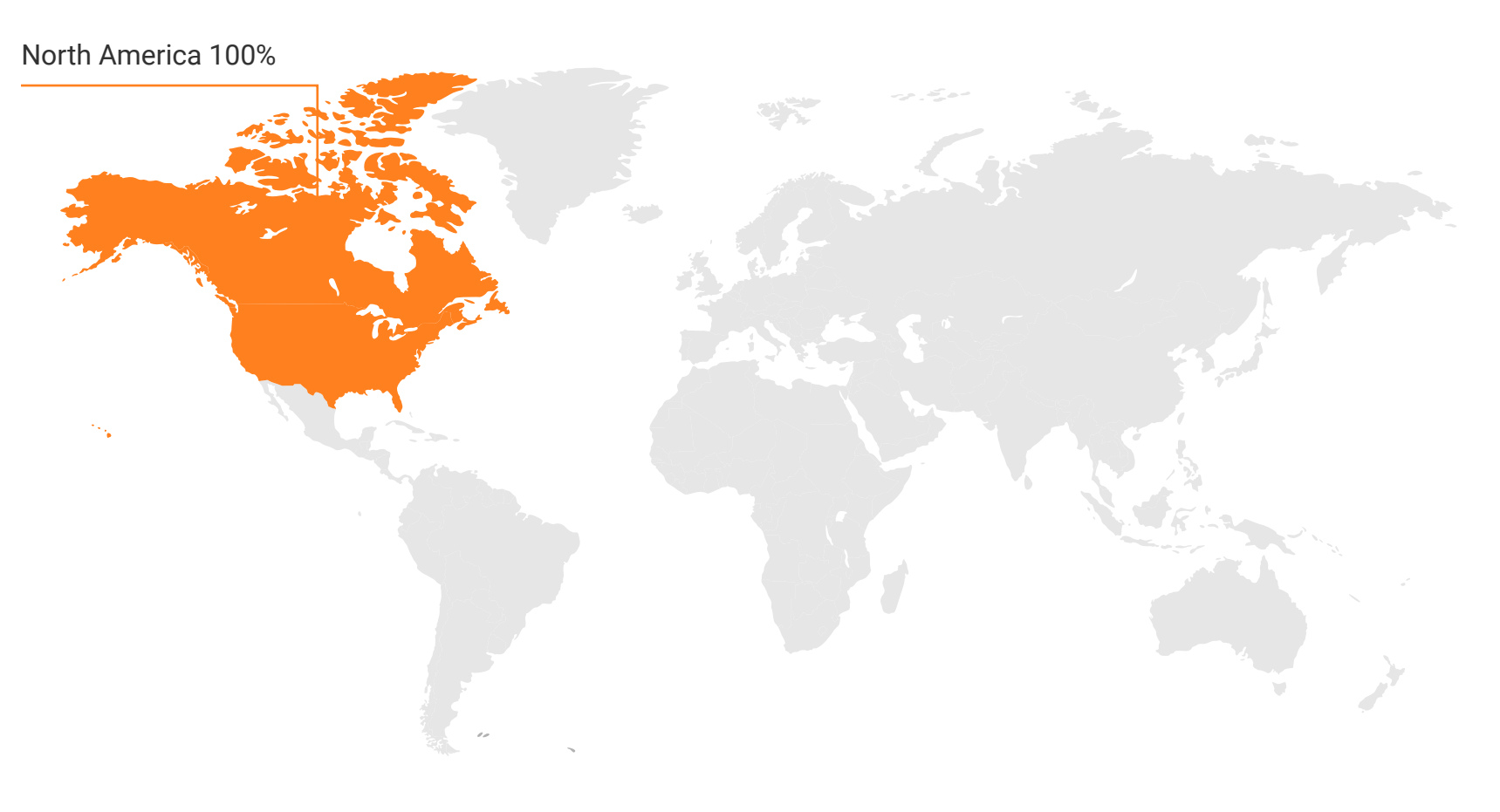
Similarly to on-premises AD recovery strategies, Azure AD recovery strategies mostly involve reliance on Microsoft documentation and scripts (68%), using outside help from consultants or Microsoft Support (55%), and using third-party tools (50%).

WHAT IS YOUR ORGANIZATION'S RECOVERY STRATEGY FOR AZURE AD AFTER A SECURITY BREACH, AZURE AD OUTAGE, OR DIRECTORY DATA LOSS?

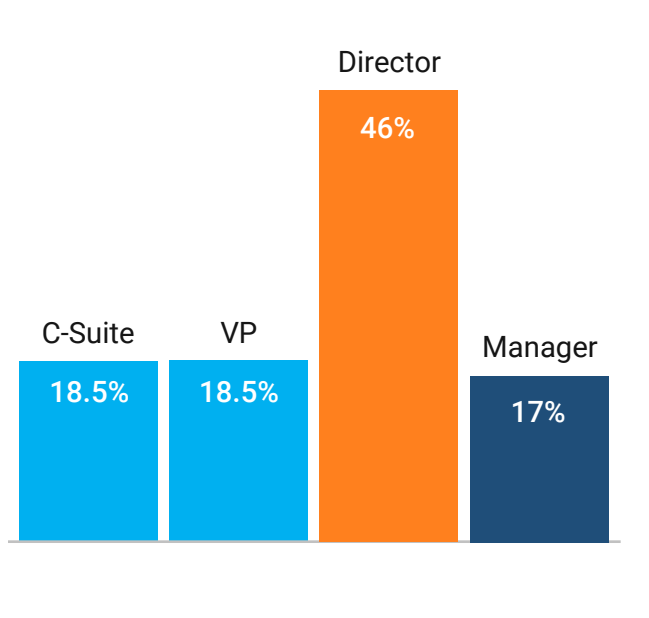


RESPONDENT BREAKDOWN

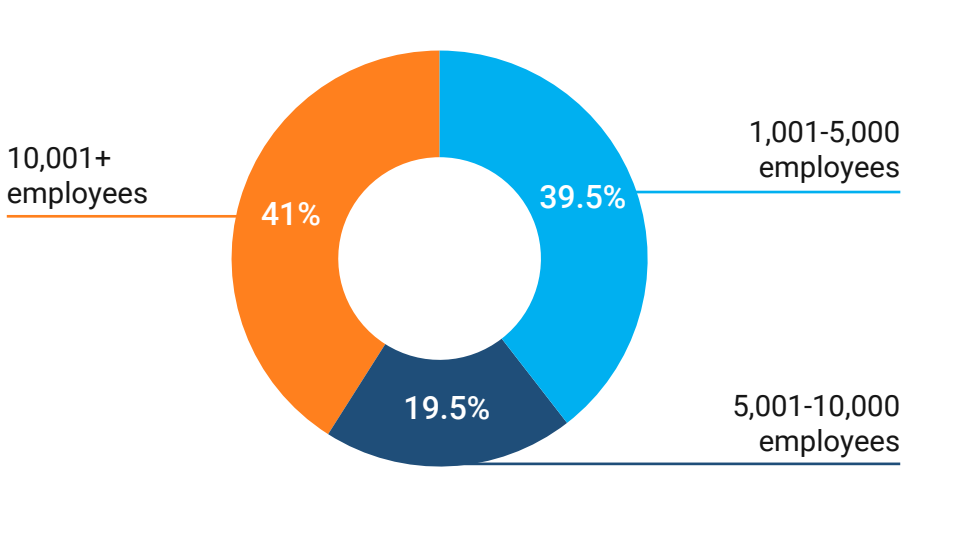
REGION



TITLE



COMPANY SIZE



As the prevalence of ransomware and the sophistication of cyber attackers continues to increase, companies must be prepared for when, not if, their Active Directory gets hit with an outage and the business stops. With Cayosoft Guardian Forest Recovery, get back to business faster with immediate Microsoft Directory recovery, without scripting. With features like one click immediate recovery, clean restore, advanced automation, and virtual labs, Cayosoft Guardian Forest Recovery was designed to do it all, in a single solution.

To see how Cayosoft Guardian Forest Recovery can help your company achieve cyber resilience with a personalized demo visit **www.cayosoft.com/demo**.

Insights powered by PULSE