ActualTech MEDIA

SEPTEMBER 2022

State of Ransomware Preparedness

How Organization Size Impacts Ransomware Readiness

SCOTT LOWE

COMMISSIONED BY

HYCU®

Contents

Summary: The Importance of Preparation

It's no surprise that smaller companies face greater challenges than larger ones in many ways, especially when it comes to funding what may be considered "optional" things such as robust data protection, disaster recovery, and ransomware mediation activities. However, these are critical elements of an ongoing business continuity strategy. If the worst happens, only those that have adequately prepared will be able to recover with less friction.

It's no surprise that smaller companies face greater challenges than larger ones in many ways, especially when it comes to funding what may be considered "optional" things.

KEY TAKEAWAYS

- Organization size matters when it comes ransomware preparedness outcomes
- Business disruption due to ransomware is not overstated; it's real and it's significant
- Common recovery metrics are impeded by financial, human resource, and skills constraints

Baseline Ransomware Awareness

Before you can plan for mitigation, you have to understand the context of what you're doing. You gain that context from prior experience and considering current trends.

QUESTION 1

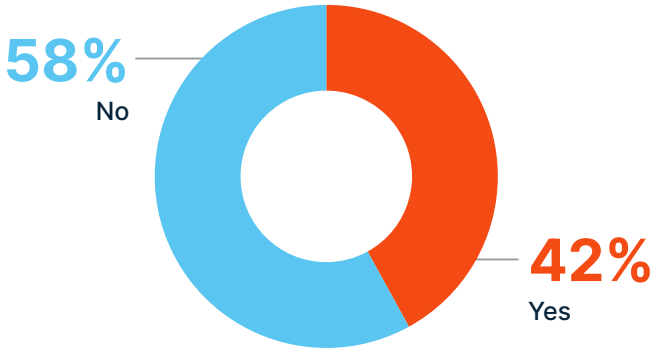
Has your organization ever experienced a ransomware incident of any size that resulted in an infiltration and/or encryption?

There are two types of organizations:

- Those that have been the victim of a ransomware attack.
- Those that haven't... yet.

It's already significant to find 42% of respondents indicating that they have been the victim of a ransomware attack — but also recognize that this figure doesn't include the 68 survey respondents who selected the "I am not allowed to disclose" option. If you thought ransomware news was just overblown hype, think again!

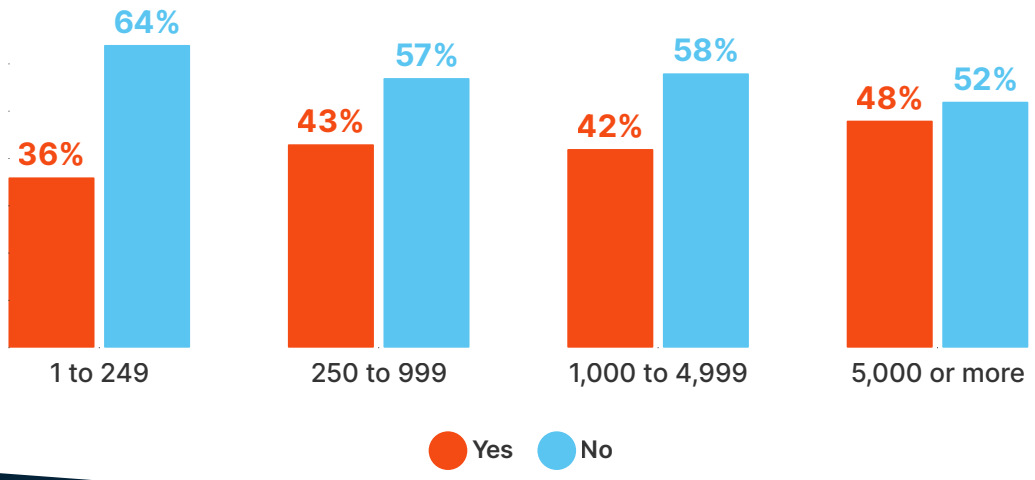
Experienced Ransomware Incident? (N=310)



ORGANIZATION SIZE

Organization size matters when it comes to attack patterns. For small companies of under 250 employees, 36% reported being attacked. Among larger companies, 48% indicated that their organization fell victim to ransomware at some point in the past. It's clear that larger organizations are more commonly targeted than smaller ones, likely due to the perception that a bigger target may offer a more handsome reward for the attacker.

Organizations That Have Been Ransomware Victims By Company Size (N=314)

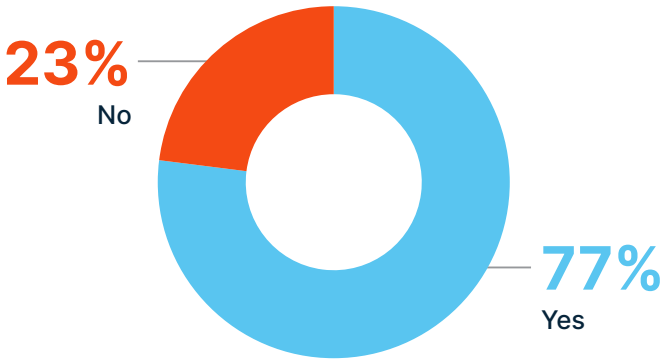


QUESTION 2

Does your organization's board have any level of involvement in your cybersecurity posture, including ransomware prevention efforts?

Cybersecurity is a board-level issue in most organizations today, as evidenced by the fact that 77% of our respondents' boards are involved in these discussions.

Board Involvement (N=294)

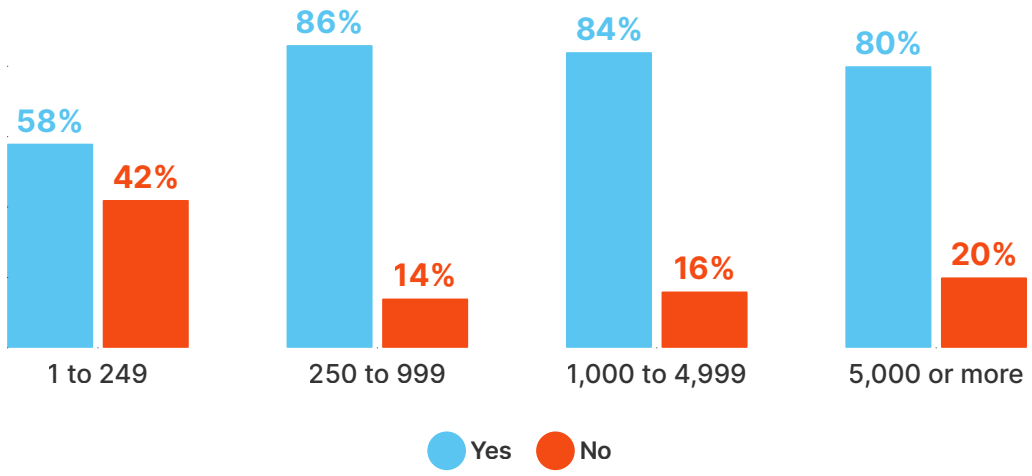


ORGANIZATION SIZE

Smaller companies — in this case those with fewer than 250 employees — are not engaging board-level leadership at nearly the rate of larger companies. Just 58% of small companies' boards have involvement in this critical risk management activity, compared to 80% to 86% of the boards of larger companies. In our research, we found organizations that involve their boards appear to expect far better outcomes in the event of a ransomware attack. Given that, smaller organizations may want to consider what results may come from engaging executive leadership in these discussions.

Just 58% of small companies' boards have involvement in this critical risk management activity, compared to 80% to 86% of the boards of larger companies.

Board Involvment in Ransomware Mitigation Planning By Company Size (N=297)



Ransomware Preparedness

It makes sense that how well an organization prepares for a potential threat generally dictates how well that organization will respond to an eventual attack. Again, several signs suggest company size plays a significant role when it comes to predicting outcomes. It's not always a "bigger is better" story, though, as smaller companies sometimes outperform larger ones.

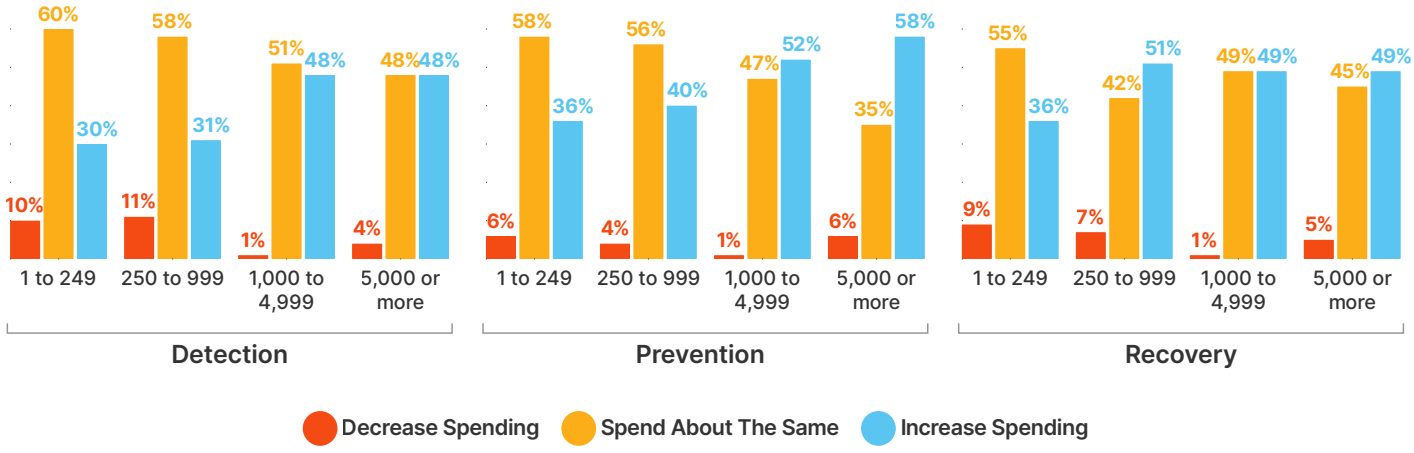
QUESTION 3

As compared to 2020 and 2021, for overall ransomware prevention and recovery spending, as compared to 2022 and 2023, we are expecting to...

It's clear that larger organizations, in general, plan to increase their spending more significantly than smaller ones. In addition, more smaller companies plan to decrease spending on ransomware activities. Some of this is likely a function of budget availability, but it can also be a simple question of priorities. Smaller companies have fewer resources, including people. Larger companies have more.

It's clear that larger organizations, in general, plan to increase their spending more significantly than smaller ones.

2022 and 2023 Ransomware Spending Plans By Company Size (N=363)



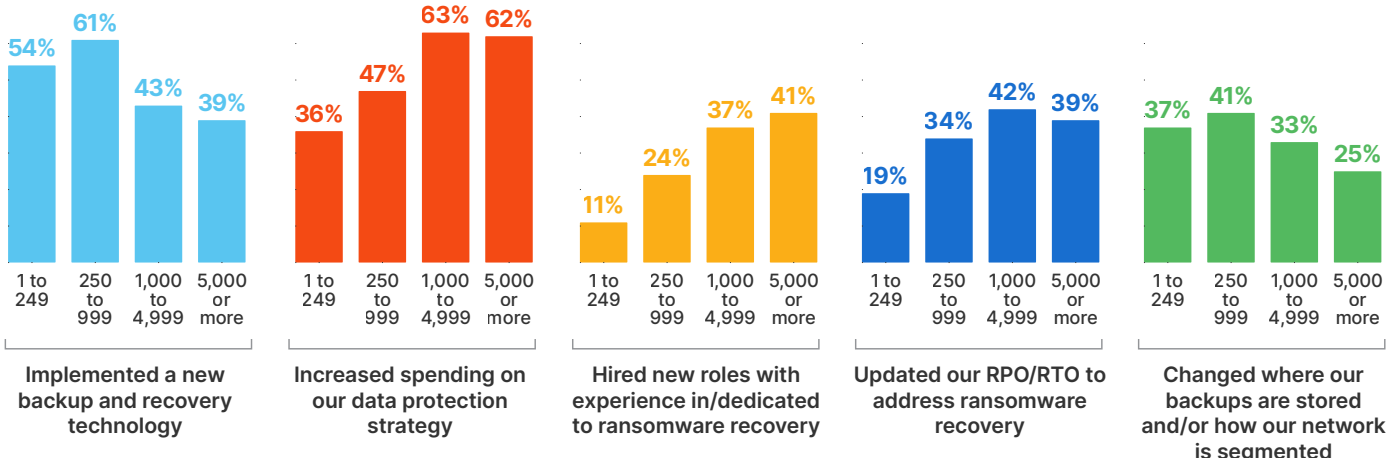
QUESTION 4

What changes have you made to your backup and recovery strategy as a direct result of the threat of ransomware or a successful ransomware attack?

In the overall results, 50% of respondents found their former backup and recovery tools insufficient to meet the looming threat of ransomware and took proactive steps to replace those tools with something else. This is not a positive statistic for the legacy backup industry! Breaking the data down by company size reveals additional insights. For example, just 11% of small companies have expanded staffing to directly address ransomware, while 41% of larger companies have done so. However, smaller companies have been much more likely than larger ones to make changes to the tools they're using: 54% vs. 39%.

50% of respondents found their former backup and recovery tools insufficient to meet the looming threat of ransomware.

Changes Made to Backup and Recovery by Company Size (multiple selections allowed; N=361)



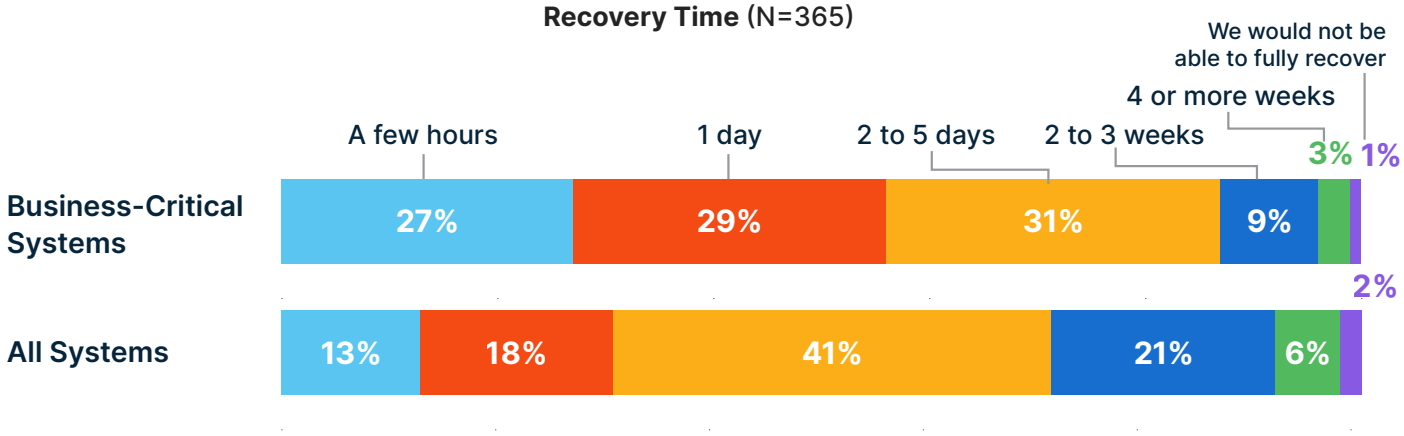
QUESTION 5

If your organization were to experience a ransomware attack that impacted all systems, how long do you think it would take you to recover to the following levels?

For business-critical systems:

- Fifty-six percent (56%) of respondents indicate that they can recover in one day or less.
- A staggering 40% would be without business-critical systems for between two and 15 days.
- The other 4% expect that they would not recover for more than four weeks, if ever — they will likely experience significant business disruption.

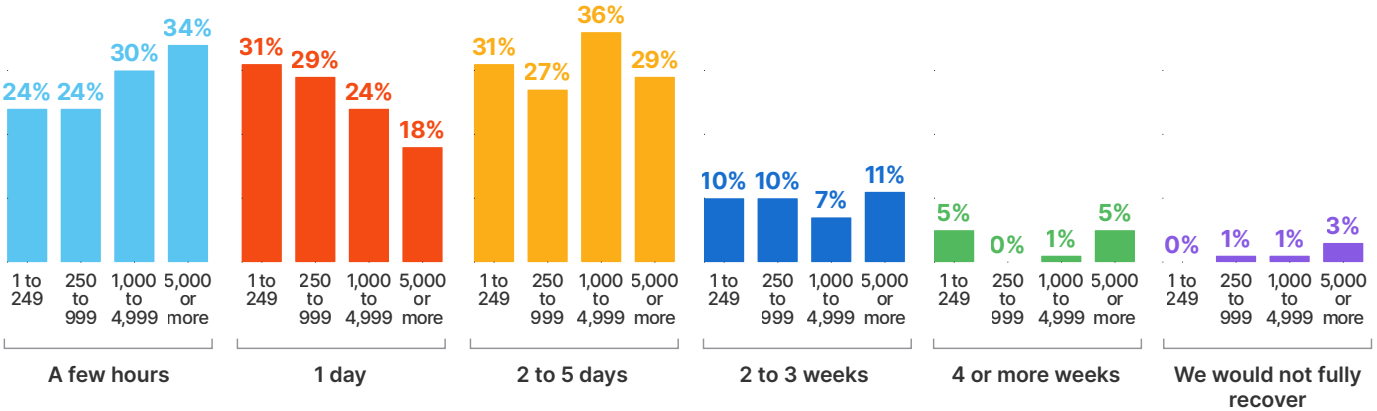
Recovery Time (N=365)



ORGANIZATION SIZE

Larger companies have an edge over smaller ones when it comes to recovery times. Just 24% of companies under 1,000 people felt that they could recover critical systems in a few hours, compared to 34% of companies with more than 5,000 employees.

Time to Recover Business-Critical Systems By Company Size (N=367)

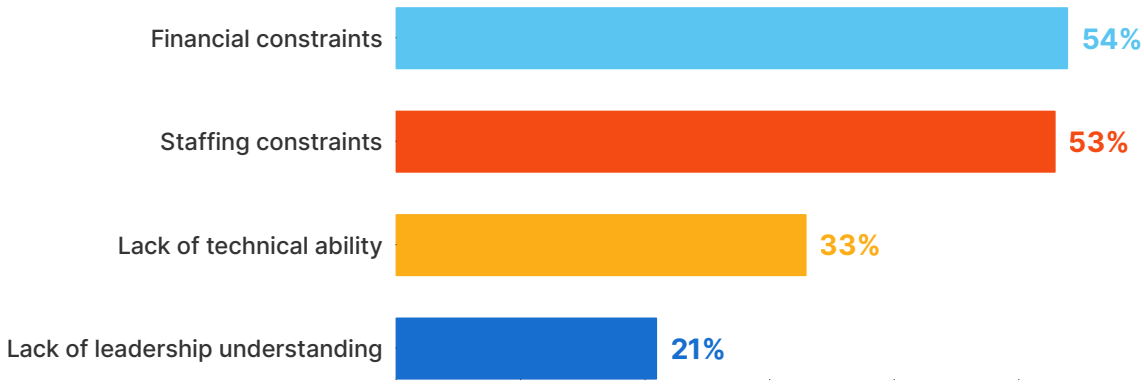


QUESTION 6

What prevents your organization from improving RTO and RPO metrics?

If RTO and RPO were cost-free and effort-free metrics to adjust, they would be zero all the time. There are, unfortunately, some important barriers that respondents identified as ones getting in the way of their organization's success in this area.

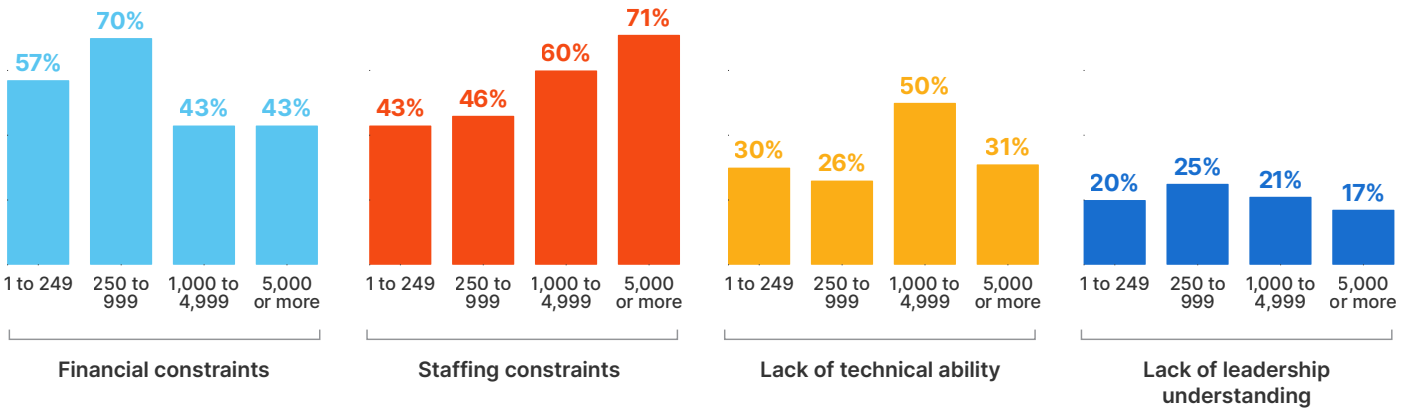
Reasons For Not Improving RTO/RPO Filtered To Those Dissatisfied With Current RTO/RPO (N=199)



ORGANIZATION SIZE

For small companies, the primary inhibitor is financial, with 57% to 70% of small companies indicating that lack of financial resources contributes to their inability to address RTO and RPO. For larger companies, 60% to 71% indicate that the key issue is one of personnel; there simply isn't sufficient staff to do it right.

Reasons For Not Improving RTO/RPO Filtered To Those Dissatisfied With Current RTO/RPO By Company Size (Multiple responses allowed; N=199)



Ability to Recover from Ransomware

Everything about data protection and ransomware preparedness comes down to the ability to recover business-critical data in the event of an attack.

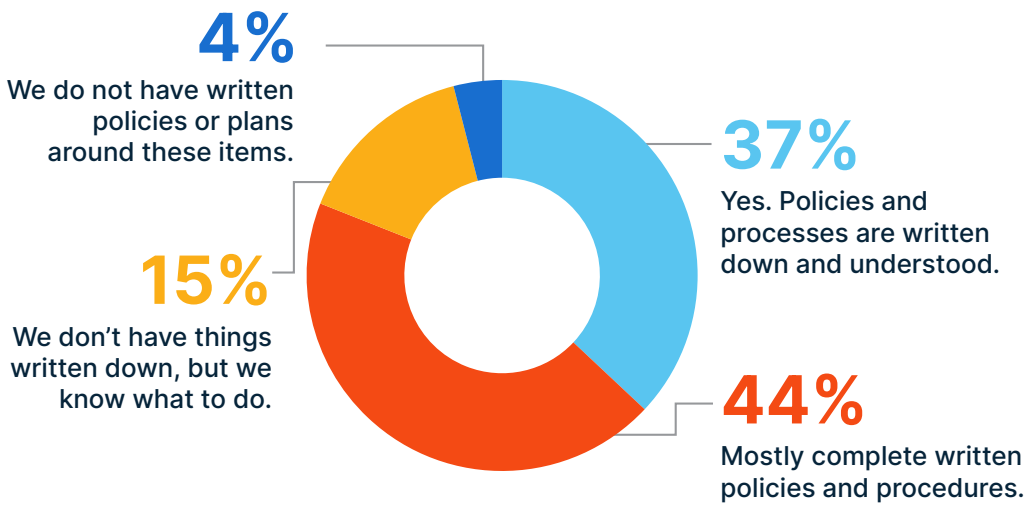
QUESTION 7

Does your organization have a complete and documented disaster recovery or ransomware remediation plan with associated policies and processes?

Overall, 19% of respondents are on the very cusp of having a *Really Bad Day*. When disaster strikes, those 19% do not have documented policies and procedures to help guide a recovery and will essentially have to hope for the best. In fact, just 37% of respondents work in organizations with fully documented and understood policies and procedures for recovery.

19% of respondents are on the very cusp of having a *Really Bad Day*.

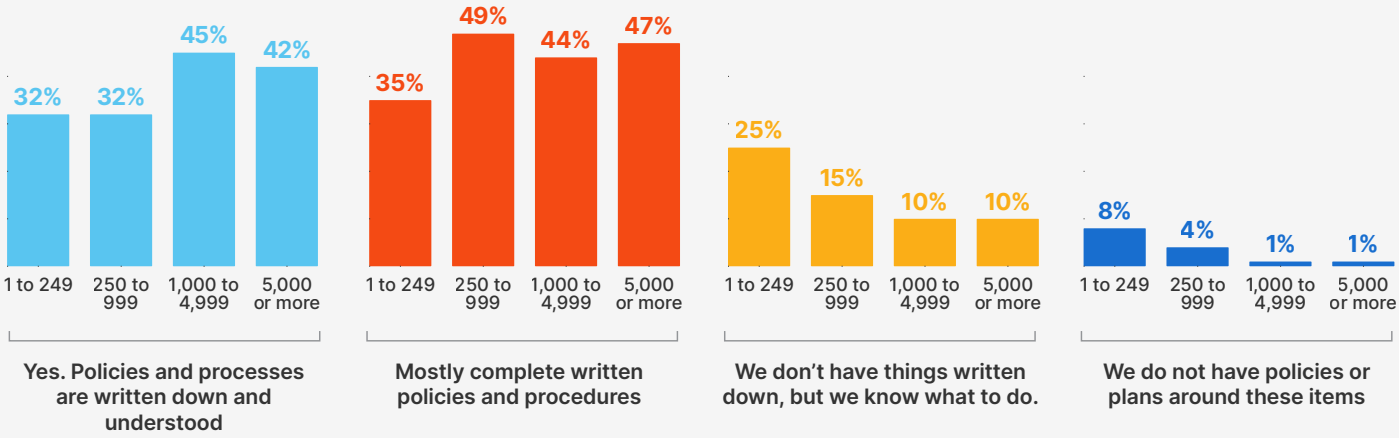
Does Documentation Around Recovery Exist? (N=373)



ORGANIZATION SIZE

Organization size plays a role here, as you might expect. Larger companies are quite a bit more likely (44%) to have comprehensive DR plans as compared to smaller companies (32%). Smaller companies need to increase their efforts here or face far more difficult recoveries in the event of a disaster.

Does Documentation Around Ransomware and Recovery Exist By Company Size (N=373)



Yes. Policies and processes are written down and understood

Mostly complete written policies and procedures

We don't have things written down, but we know what to do.

We do not have policies or plans around these items

NOTE TO READER

HYCU commissioned ActualTech Media to create and conduct a broad survey around the topic of ransomware. The full report can be downloaded from <link>. This document delves into a single premise, with associated insights that were gleaned from this research.

PREMISE

The overall size of an organization correlates to ransomware preparedness.

ABOUT THIS REPORT

The scourge of ransomware has spurred an entire ecosystem dedicated to combating its spread and preventing organizations from becoming victims of an increasingly motivated set of criminals. Our research suggests a strong correlation between company size and the perception of ransomware readiness. This report highlights outlier data points from our primary research report, focused on the differences between large and small companies in terms of ransomware preparedness and outcomes.

Thank you to HYCU for commissioning this research. To learn more about how HYCU can help your organization prepare its defenses against a ransomware attack, please visit www.hycu.com.