ActualTech MEDIA

SEPTEMBER 2022

State of Ransomware Preparedness

SCOTT LOWE

COMMISSIONED BY

HYCU®

Contents

Summary

It's clear that, while organizations continue their efforts to fully prepare for a potential ransomware attack, there is significant room for improvement in designing a strategy that minimizes the risk of potential long-term damage.

Every decision around risk mitigation comes with a set of considerations — typically revolving around financial resources, human resources, or technical capabilities — that companies must consider as they embark on these journeys.

We strongly encourage readers to routinely assess their current preparedness posture and consider the guidance provided in this report as they continually evolve their ransomware strategy.

Every decision around risk mitigation comes with a set of considerations that companies must consider as they embark on these journeys.

KEY TAKEAWAYS

- Proper preparation, detection, and recovery capabilities are vital regardless of an organization's history with ransomware
- Humans are the first line of defense in battling ransomware, so employee policies, procedures, and tools must ensure protection
- Business disruption due to ransomware is not overstated; it's real and it's significant, so preparedness is key
- Proper backup and recovery capabilities are directly impacted by how well you plan

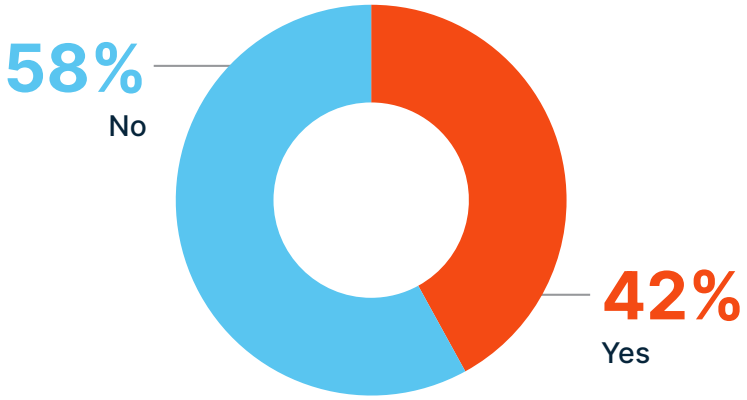
Section 1: Ransomware Risk and Preparation

QUESTION 1

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

We believe there are two types of organizations — those that have been the victim of a ransomware attack and those that haven't... yet.

Experienced Ransomware Incident? (N=310)



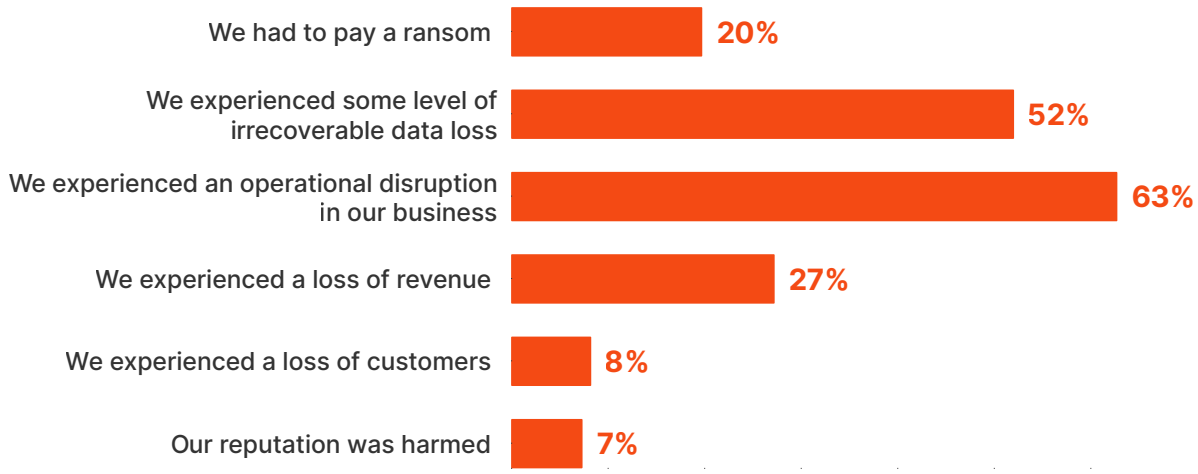
GUIDANCE: Proper preparation, detection, and recovery capabilities are vital regardless of your history with ransomware. The "Yes" figure of those reporting a ransomware experience, 42%, is not an insignificant percentage, and this figure doesn't even include the 68 respondents who selected the survey's "I am not allowed to disclose" option. If you thought ransomware news was just overblown hype, think again!

Proper preparation, detection, and recovery capabilities are vital regardless of your history with ransomware.

QUESTION 2

Did your organization experience any of the following?

Ransomware Experiences (Multiple answers allowed; filter: fell victim to a ransomware attack; N=121)



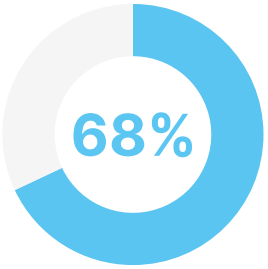
Key takeaways:

- About 52% of victims suffered data loss on some level
- Almost 63% of victims suffered an operational disruption
- Just under 20% were forced to pay a ransom

GUIDANCE: Your prevention strategy and recovery capabilities need to be on point. Both are equally important. Some view prevention as simply attempting to avoid ransomware altogether, but a comprehensive ransomware mitigation strategy's prevention component defines prevention as preventing consequences of a successful ransomware attack, as well. As such, your prevention strategy must include a robust backup plan to prevent your organization from being a part of the 52% that experienced data loss in the wake of a successful attack.

Whether or not you pay the ransom matters, but paying ransom does not guarantee that you'll prevent data loss; it simply reduces the potential for loss.

Whether or not you pay the ransom matters, but paying ransom does not guarantee that you'll prevent data loss; it simply reduces the potential for loss.



For those that **did not pay a ransom** (N=97), 68% experienced some level of data loss.

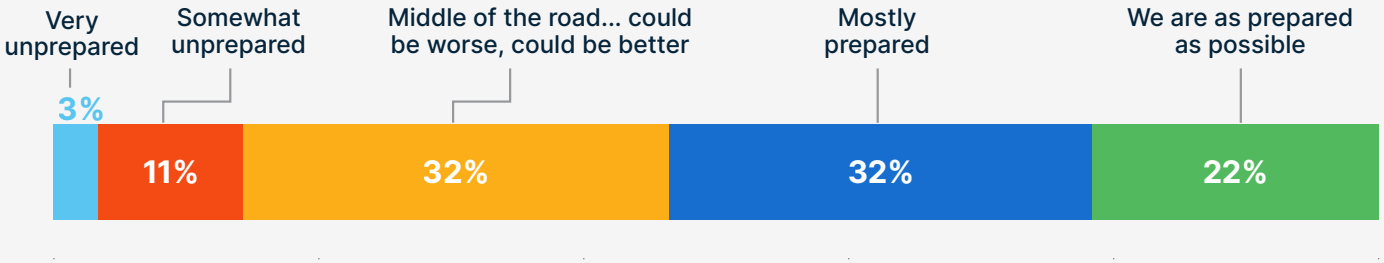
For those that **did pay a ransom** (N=24), 58% experienced some level of data loss.

QUESTION 3

How proactive is your organization in preparing for a potential ransomware attack?

The level of preparation by organizations is mostly strong, in 55% of respondent organizations, but the other 45% have work to do. In particular, 14% reveal that they are unprepared for an attack.

Level of Ransomware Preparedness (N=385)



GUIDANCE: Fix this! There are free resources available everywhere, including at gterscore.org and ransomware.org, showing how to develop a comprehensive ransomware mitigation strategy that will help your organization prevent attacks or mitigate the chaos that accompanies a successful attack.

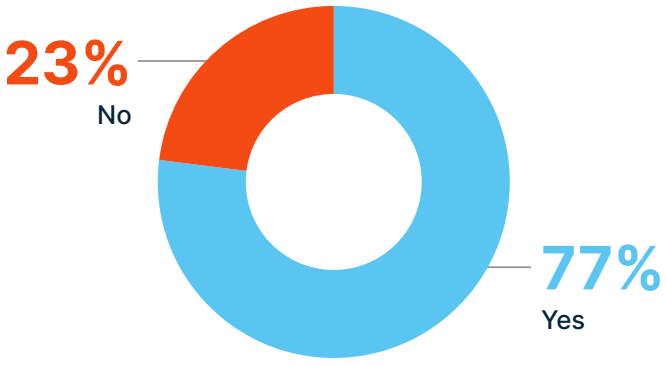
QUESTION 4

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

You demonstrate what's important to you through how you choose to spend your time. That holds true for ransomware preparedness and how boards of directors spend their time. 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.

GUIDANCE: For the 23% with boards that are not involved in ransomware strategy, we strongly encourage you to bring your boards into the discussion. Risk management is always a board-level issue, as legal and financial issues generally accompany a ransomware attack. Boards must be comfortable with the measures that the organization is taking to secure its assets.

Board Involvement (N=294)



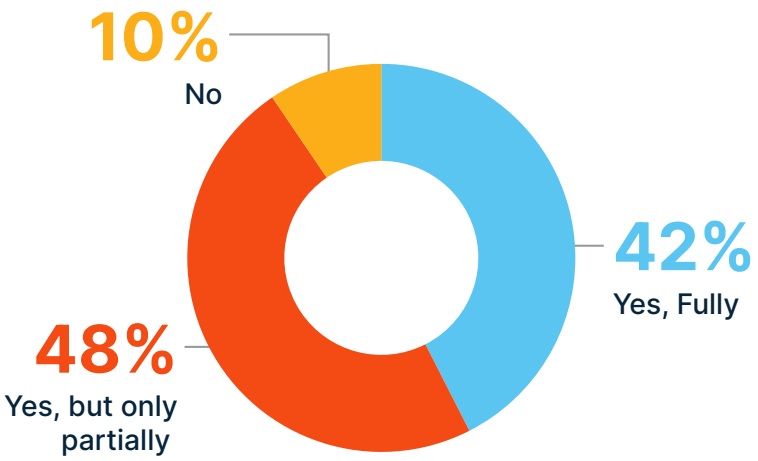
Note: We gleaned some intriguing results from organizations that have chosen to involve their boards of directors in overall ransomware planning. These results can be found in our sub-report focused on this single data point. <Link>

QUESTION 5

Have you implemented comprehensive information security, email, and ransomware training programs in your organization?

Humans are the first line of defense in battling ransomware, and that defense is often the first to fall due to poor training. The survey shows 42% of respondent organizations have taken this important step in a complete way, while 48% more have at least started the process. The other 10% have not even started yet.

Human Training Program Implemented (N=379)



GUIDANCE: Humans are the weakest link and it's almost always due to lack of training or simple human error. There are innumerable ways to address the issue of training, and these services are not generally very expensive. All organizations should be taking practical steps to make sure their employees don't accidentally become the victim that brings down the entire organization.

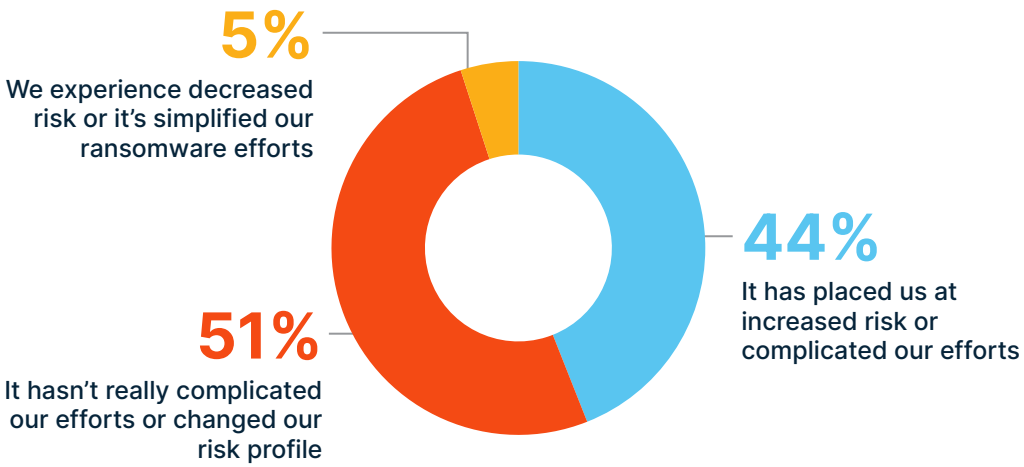
Humans are the weakest link and it's almost always due to lack of training or simple human error.

QUESTION 6

How has the rise of work-from-home impacted your ransomware protection and remediation efforts?

As the world has reacted to the emergence of a new threat, and as that world is still undulating with uncertainty, about 44% of respondents feel that the rise in work-from-home capability has created new risks and complications in terms of battling ransomware. For a few organizations, about 5%, the emergence of WFH has simplified their efforts.

Impact of Work-From-Home (N=364)



GUIDANCE: Although we don't suggest changing your WFH policy due to ransomware risk, the reality is that your policies, procedures, and tools must adapt to ensure protection regardless of employee and workload location. Choose tools that support a distributed workforce and that support both on-premises and cloud services to maximize your preventive posture, never forgetting that backup tools should be a central focus of this prevention strategy.

Your policies, procedures, and tools must adapt to ensure protection regardless of employee and workload location.

Section 2: Executing Your Preparedness Plan

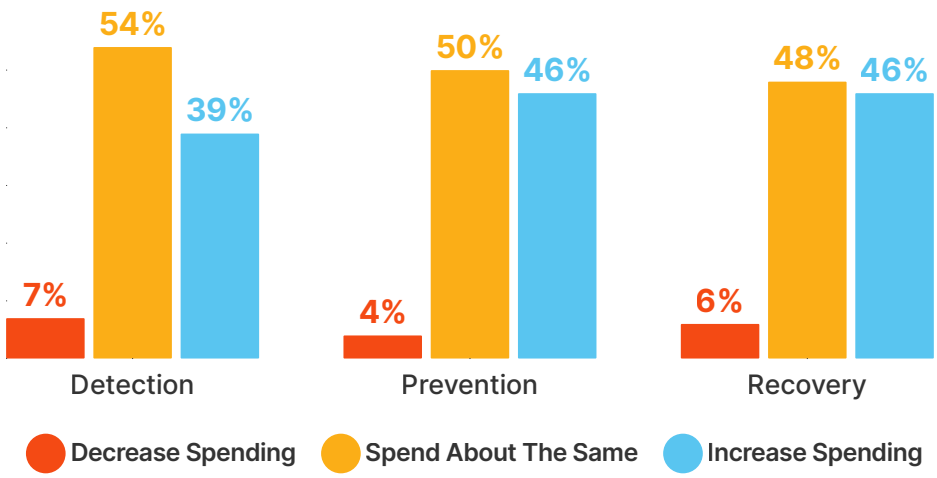
How well an organization prepares for a potential threat generally dictates how well that organization will respond to an eventual attack. In this section, we will detail answers to questions that revolve around how well our respondent organizations are executing against their preparedness plans.

QUESTION 7

As compared to 2020 and 2021, for overall ransomware prevention and recovery spending, and 2022 and 2023 we are expecting to a) decrease spending, b) spend about the same, c) increase spending

As we stated, where you spend time demonstrates your values and priorities, and the same is true for money. Across the spectrum of ransomware protection — detection, prevention, and recovery — spending is expected to be either stable or increases. Very few organizations intend to reduce their spending in any of these areas. That said, it's clear that for this year, the focus for many is on prevention and recovery versus detection. This could be because organizations feel detection is a "solved problem" or because people feel that the inevitable will evade detection.

Ransomware Preparedness Spending (N=363)



GUIDANCE: Determine where you fall in these charts and make sure that your current budget commitment supports the level of importance that is applied to ransomware in your company. If it is — even if you're reducing spending — that's okay. If it's not, however, begin devising a remediation strategy and business justification for changing your current level of support.

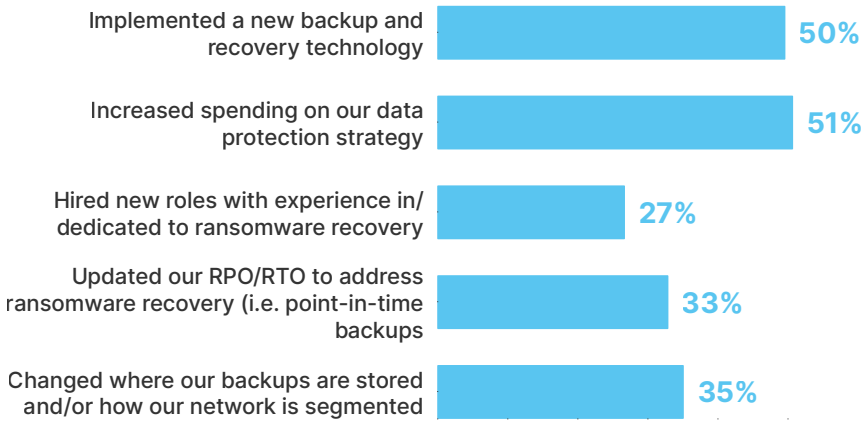
QUESTION 8

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?

About half 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! At the same time, about the same number of organizations have increased overall spending on their data protection strategy to help fend off attacks. About one-third of respondent organizations updated their RPO and RTO targets to improve recovery capability and also helped ensure that their backups are protected against ransomware attacks themselves.

GUIDANCE: For those still storing backups that are easily accessible over the network, it's time to stop! Air-gapped or immutable backups are the only ways to ensure that backups themselves don't fall to encryption worms when ransomware hits. At the same time, evaluate — *really* evaluate — your current backup provider as well as your standard backup and recovery metrics and make sure you can stay in business when your business gets attacked.

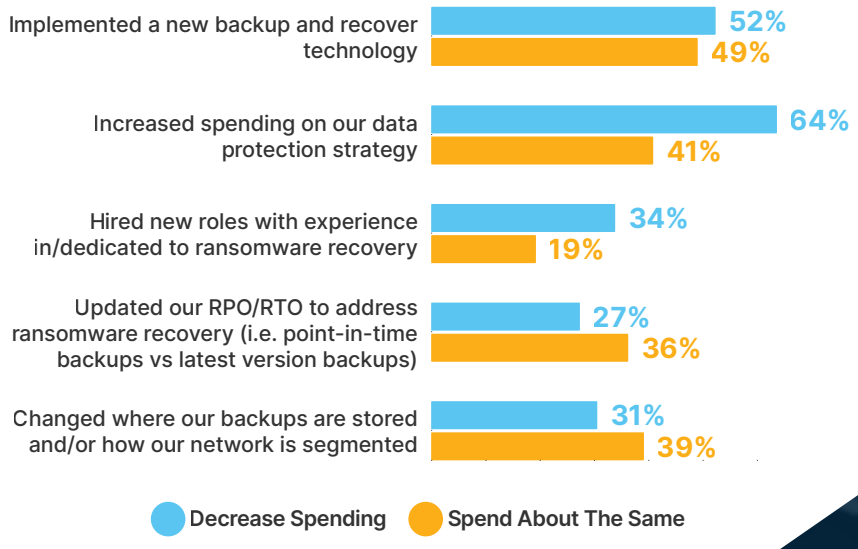
Changes Made Due to Ransomware Threat or Attack
(multiple selections allowed; N=358)



PRIOR RANSOMWARE ATTACK EXPERIENCE

Organizations that have previously experienced a ransomware attack are *far* more likely to have increased spending on ransomware avoidance and to have hired new roles dedicated to preventing another successful attack. In short, they've likely discovered that spending more on prevention is far less expensive and impactful that paying for a recovery.

Changes Made Due to Ransomware Threat or Attack Filtered By Attack Experience (multiple selections allowed; N=295)

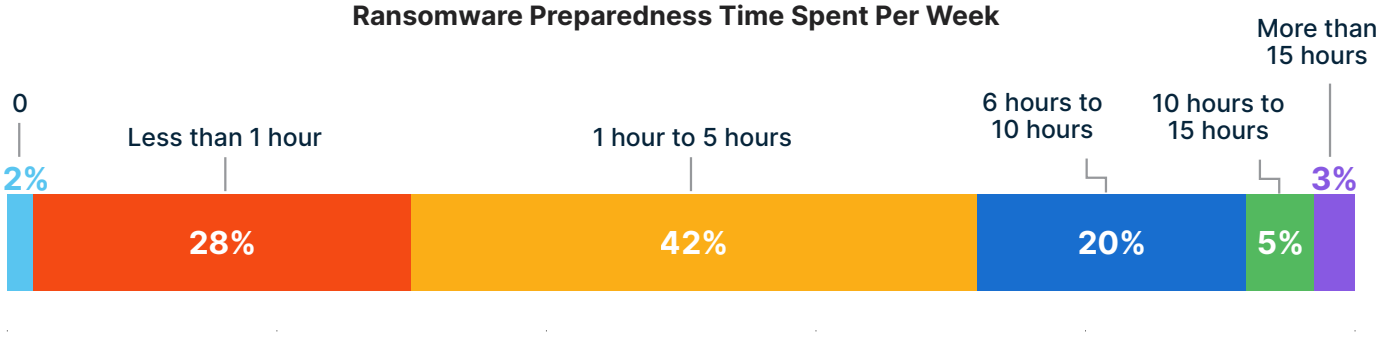


QUESTION 9

Approximately how many hours per week on average would you estimate you currently spend on ransomware preparedness?

This report has indicated that *where you spend your time identifies your priorities*, but that doesn't suggest wasting that time in a valiant effort to raise visibility. Rather, make sure the time you spend matters! Survey respondents indicate that, for the most part, people are spending less than five hours per week on ransomware preparedness, but a full 28% are spending six or more hours a week on this task.

Ransomware Preparedness Time Spent Per Week

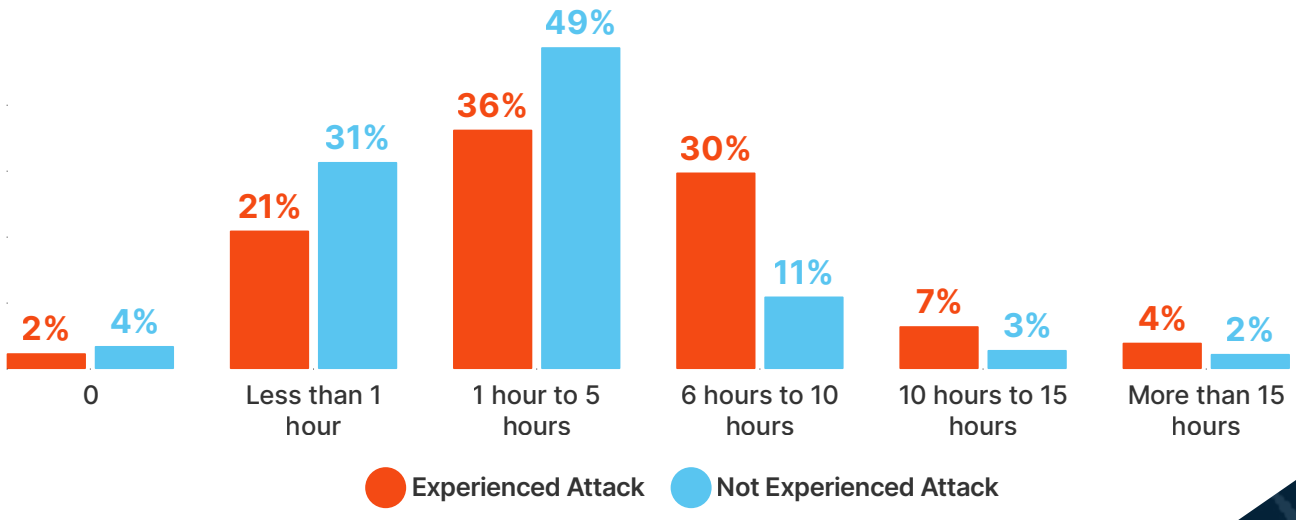


GUIDANCE: Ensure that the time spent on ransomware preparedness is strategic. Backup and recovery tools should enable a strategic focus on preparedness, not drag admins into tactical complexity that distracts from achieving the overarching goal of maximizing an organization's defense posture. Assess tools on the market that promise to reduce tactical complexity and put those tools through the gauntlet to make sure that the vendor's promises hold true. Then refocus your time on preparedness strategy and other organizations goals.

PRIOR RANSOMWARE ATTACK EXPERIENCE

Organizations that experienced a previous ransomware attack spend more time avoiding the next one. About 40% of these companies spend six or more hours per week on ransomware preparedness as compared to just 16% of those that have never experienced a ransomware attack.

Ransomware Preparedness Time Spent Per Week Filtered By Attack Experience (N=296)

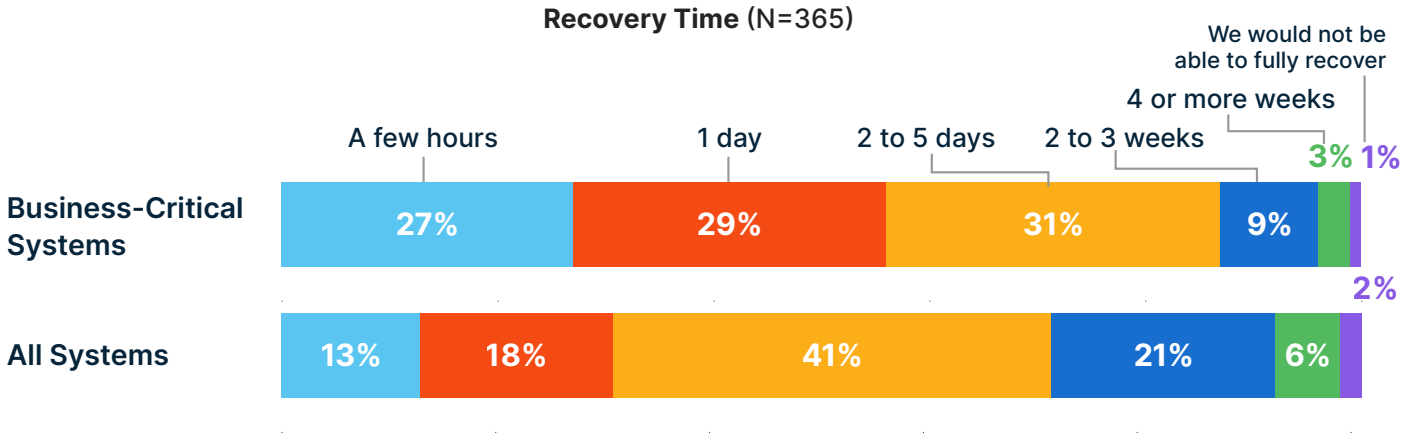


QUESTION 10

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:

- Just over 55% of respondents indicate that they can recover in one day or less.
- For other systems that number drops to 31%.
- A staggering 40% would be without business-critical systems for between two and 15 days.



GUIDANCE: Perform an assessment of all your systems and categorize them in terms of importance to the business. Next, realistically determine how quickly you would be able to recover each of those systems. Third, in conjunction with senior management, review these categories and assign to each one agreed-upon targets for recovery time objective and recovery point objective.

Finally, armed with this information, develop appropriate mitigation and recovery plans along with associated costs for each and, again, review in partnership with senior management to ensure there is complete transparency in the organization's current mitigation capabilities as well as an understanding of the potential risks based on the level of investment the organization is willing to make in each category.

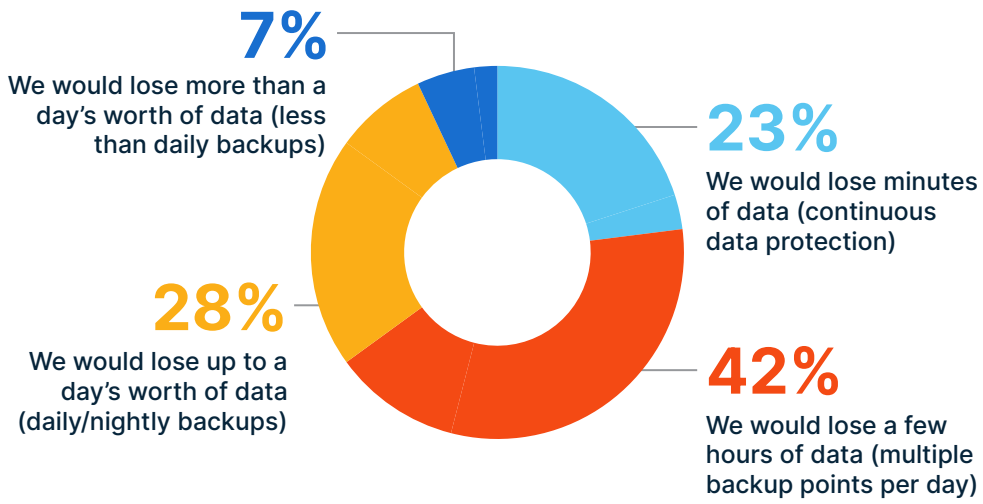
A staggering 40% suffering a ransomware attack would be without business-critical systems for between two and 15 days.

QUESTION 11

If you were to experience a ransomware attack, what is the most recent backup from which you could recover for mission-critical systems? In technical terms, what is your recovery point objective (RPO) granularity?

Along with recovery time objective (RTO), which is a common metric used to detail how long it would take to recovery from a disaster, recovery point objective (RPO) is a critical metric that indicates the level of data loss that an organization would incur if it were to require a complete rebuild of the environment from backups. The closer to zero, the less data loss occurs, but getting to zero can sometimes add cost and complexity to the equation. As such, as with anything related to risk management, organizations take a risk/reward approach that generally results in a non-zero number for RPO.

How Much Data Loss Would you Incur Due to a Disaster? (N=368)



GUIDANCE: Today's data protection solutions provide far more options for reducing both RPO and RTO than legacy solutions could provide. Continually review the data protection market to see what's new and what may be able to help your organization close the RPO gap.

The closer to zero, the less data loss occurs, but getting to zero can sometimes add cost and complexity to the equation.

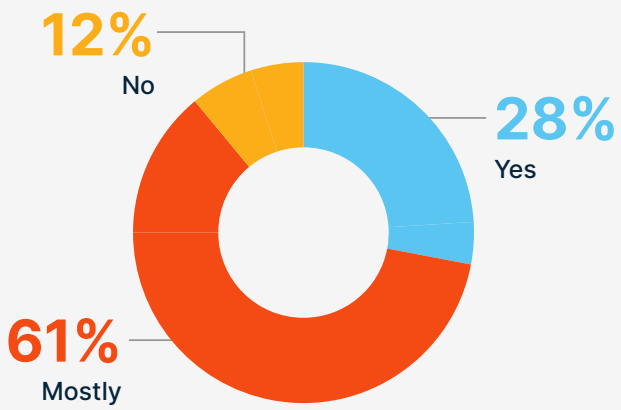
QUESTION 12

Do your current RPO and RTO metrics meet your organization's needs?

RTO and RPO are key metrics in data recovery. It's concerning that just 28% of respondents feel that their RTO and RPO metrics are sufficient to meet the needs of their organizations.

GUIDANCE: Ensure that the C suite and board risk management are aware of exactly how RTO and RPO metrics impact the organization and that they sign off on the potential risks that insufficient RTO/RPO may have, particularly in a world in which disasters — including crippling ransomware attacks — happen almost daily.

RTO and RPO Sufficient? (N=287)

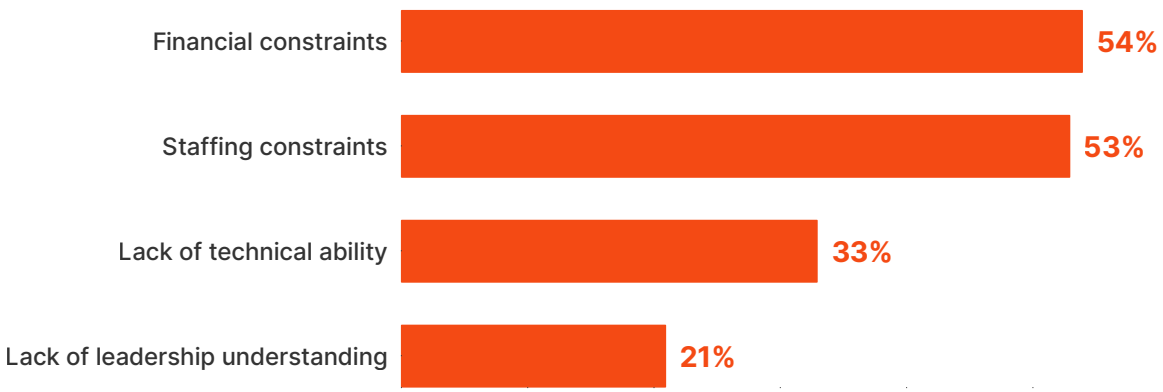


QUESTION 13

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
(multiple selections allowed; N=199)



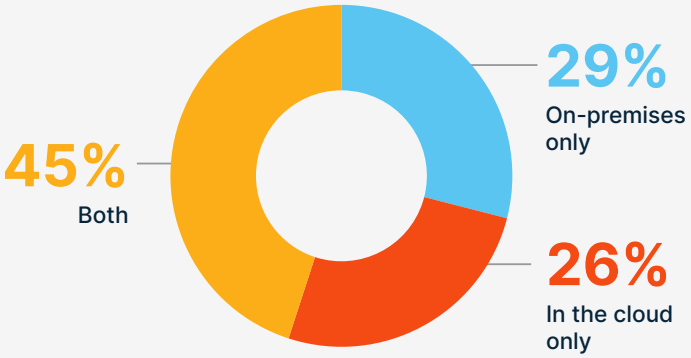
QUESTION 14

Where do you run your primary workloads?

Less than one-third of respondents (29%) still operate workloads in on-premises environments only. About 26% of respondents operate solely cloud-based workloads while 45% run both. As such, there is a consistently increasing level of complexity when it comes to protecting these workloads from ransomware infiltrations.

When combined, 74% of respondents are operating on-premises workloads and 71% are operating workloads based in the cloud.

Where Do You Run Your Primary Workloads? (N=379)



GUIDANCE: Your ransomware protection and recovery strategy needs to consider the location of the workload. Too many organizations believe that cloud-based services automatically protect data, but a review of their Terms of Service often reveals that there is significant risk in this belief. Choose tools that protect your data wherever it resides, and if you do choose to rely on a provider's built-in protection capabilities, ensure that they adhere to best practices in the event that they become victim to an eventually successful attack.

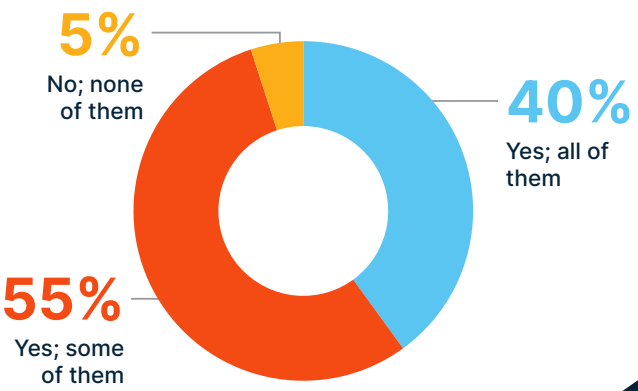
QUESTION 15

Do you back up all or some of your cloud-based workloads?

Those operating cloud-based workloads are, in most cases, doing something to protect themselves against disaster. That other 5%, though, may have future regrets!

GUIDANCE: *Your cloud or SaaS provider is probably not responsible for your data!* Read your agreements very carefully to determine what level of responsibility your provider takes with regard to backing up your data. Many have services in place to protect *themselves* against data loss — e.g. having the ability to recover customer data if the provider experiences an outage — but their protection stops there. Always understand what your providers are on the hook for and do a gap analysis to determine if they're supporting your requirements. If not, augment the service with a backup tool that can get the job done.

Do You Back Up Cloud-Based Workloads? (N=259; filtered to those running cloud-based workloads)



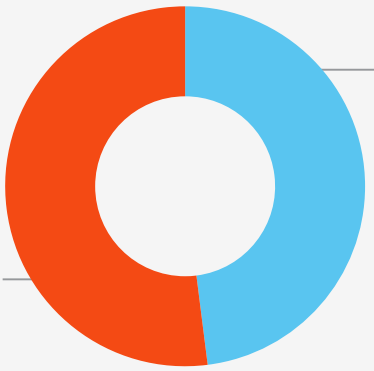
QUESTION 16

Do you use the same backup tools to cover both your on-premises and cloud-based solutions?

In a relatively even split, respondents indicated that some use the same tools to back up both cloud-based workloads and on-premises workloads while the other half use separate tools.

GUIDANCE: Always review the actual capabilities of the backup and recovery tools you're using! Not all backup tools are well-suited to protect cloud-based workloads. Make sure that the tool you're using has robust support for *all* of your workloads.

Do you use the same backup tools for both on-premises and cloud-based solutions? (N=148; filtered to those running both cloud-based and on-premises workloads)



48%
No. We use different tools to back up our on-premises and cloud-based workloads

52%
Yes. We use the same tools for both.

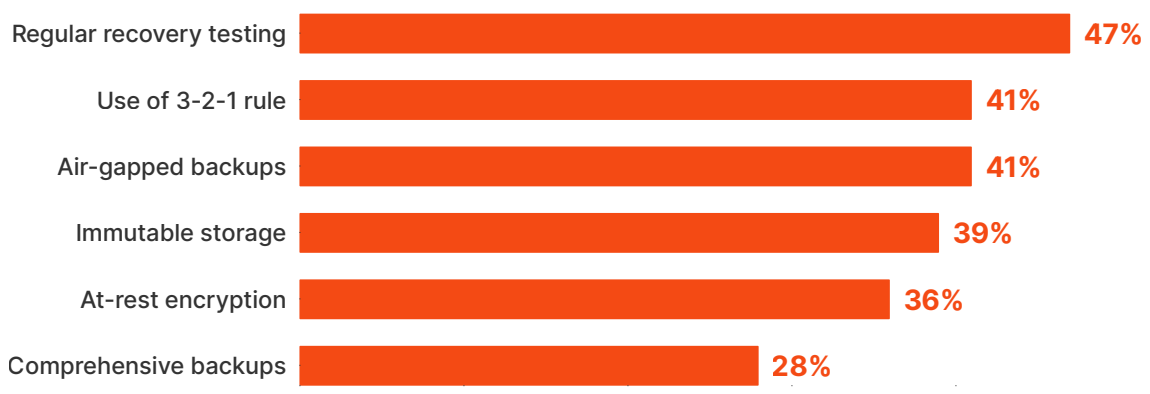
QUESTION 17

Which of these best practices are true for your organization?

There's a lot of room for improvement in terms of adherence to best practices in data protection. None of the best practices identified are adopted by even half of the respondent audience. Just 41% air gap their backups. Just 47% routinely test their backups. Just 29% have comprehensive backups that include their cloud-native data.

GUIDANCE: These are critical items. Make sure you understand why each of these best practices is considered so important and help your organization move forward to adopt each one to ensure maximum protection for all your workloads.

Backup and Recovery Best Practices Employed (multiple responses allowed; N=393)



Section 3: Ransomware Recovery Capabilities

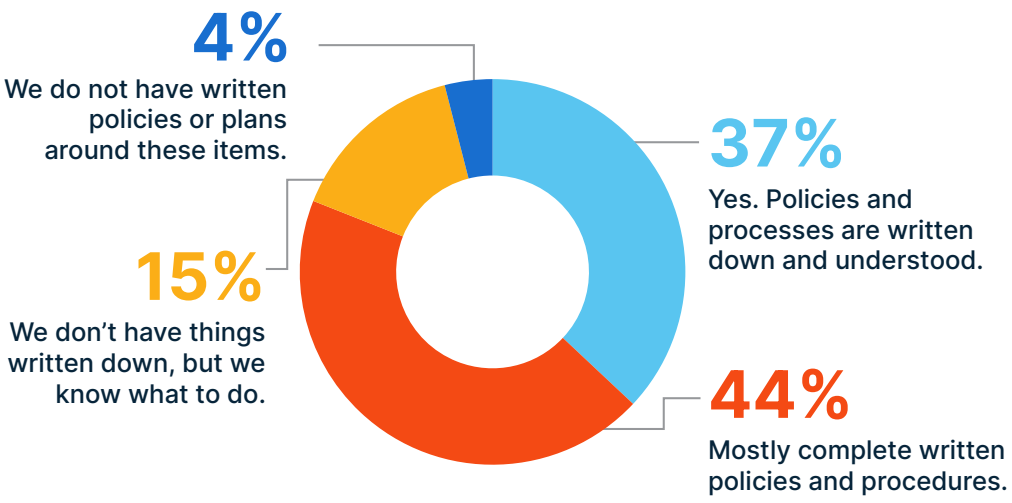
What's the point of preparation if you can't recover? In this section, we'll explore the expected outcomes that respondent organizations expect to achieve when it comes to their ability to recovery from a ransomware infiltration.

QUESTION 18

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

Proper preparation ensures recovery success. Your recovery capabilities are directly impacted by how well you plan. The survey suggests 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.

Does Documentation Around Recovery Exist? (N=373)



GUIDANCE: When stress is high, that's not the time to discover that you don't really know how to recover critical systems. Take the time now to get started on this process. It doesn't have to be overwhelming and can be done a bit at a time... as long as it gets done.

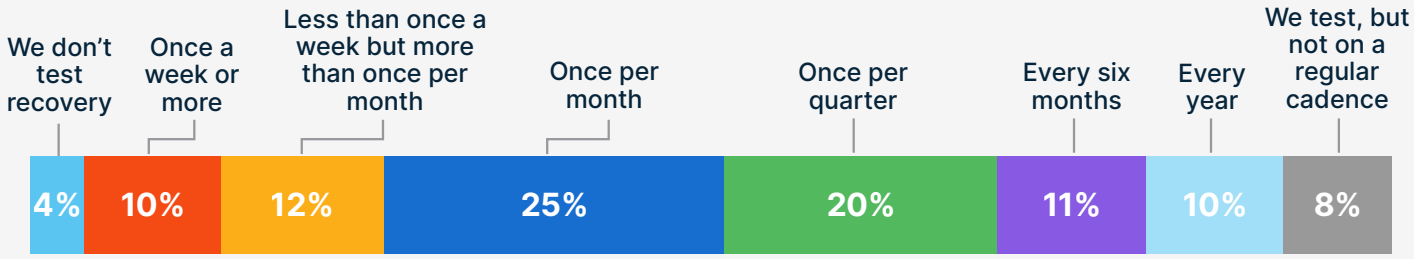
Your recovery capabilities are directly impacted by how well you plan.

QUESTION 19

How often do you test your recovery capabilities?

Diving a little deeper into one best practice — recovery testing frequency — shows that 47% of respondents test at least once per month with 22% testing even more frequently. Just 4% don't test at all while 8% test, but in an ad hoc way. Everyone else, 41%, tests less than once per month.

Recovery Testing Frequency (N=366)



GUIDANCE: "Trust but verify" is a common phrase for a reason, and it applies to backups. You never want your first clue that backups aren't working to appear just as you need to recover. It's also important to practice your recovery processes regularly so everyone knows exactly what to do when there is an incident. Test more!

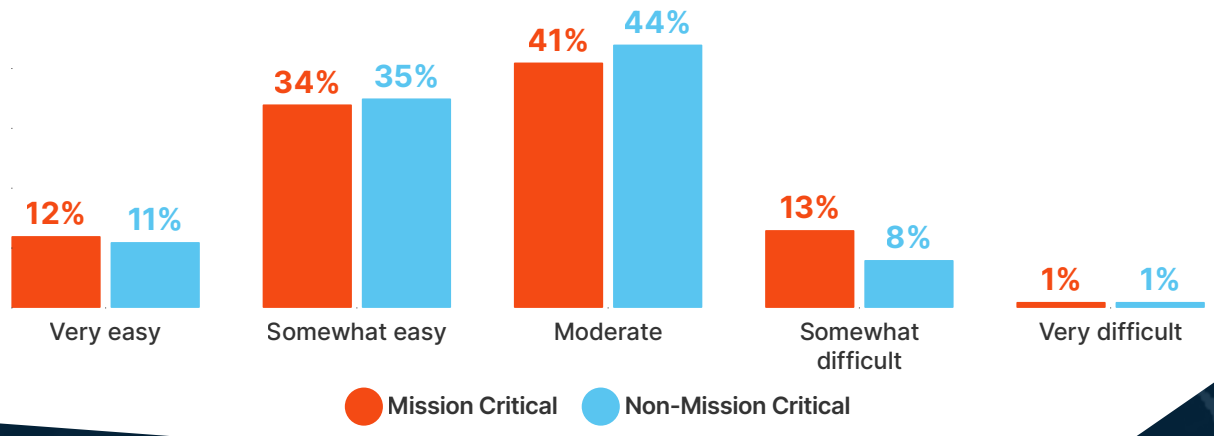
QUESTION 20

Beyond RTO and RPO, how easy is it for you to recover business-critical systems?

Ease of recovery is important, which makes it disappointing to learn than just 45% of respondents indicate that recovery is very or somewhat easy. Another 14% admit that recovery is difficult while everyone else, 41%, is squarely in the middle. The results are pretty similar for non-mission-critical systems, with only a slight variance.

GUIDANCE: Recovery is too important to be complicated. Develop process and choose tools that begin with recovery in mind. While backing up is important, it's not actually the focus of your data protection efforts. Recovery is, and that element should be the center of your efforts as you develop your organization's plans.

Ease of Recovering Systems (N=373)



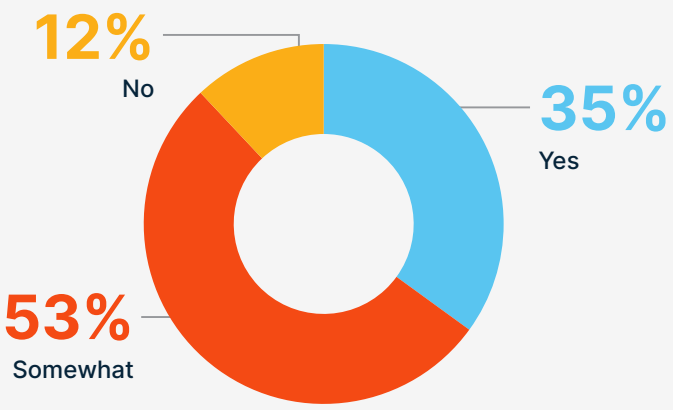
QUESTION 21

Do you believe your current backup and recovery tools are sufficient in the event that your organization suffers a major ransomware attack?

Just 35% of respondents feel that their current backup and recovery tools are sufficient to meet the needs of their organizations, leaving 65% wanting more — 53% say their tools are somewhat sufficient and a full 12% indicate that their tools and simply not able to get the job done, leaving their organizations at massive risk.

GUIDANCE: As mentioned, it's important to routinely review your technology stack, including your backup and recovery tools, to determine if they continue to be suitable for your company's needs. Constantly be on the lookout for new and innovative solutions that can help your company avoid becoming the next headline.

Are Your Backup and Recovery Tools Sufficient?
(N=373)



ABOUT THIS REPORT

The scourge of ransomware has resulted in an entire ecosystem necessary to combat its spread and prevent organizations from becoming victims of an increasingly motivated set of criminals. Our research, which gleaned insights from close to 400 survey responses in July of 2022, provides provides key data points that infer strong correlation between organizations with board involvement in ransomware preparedness and positive outcomes related to it.

PREMISE

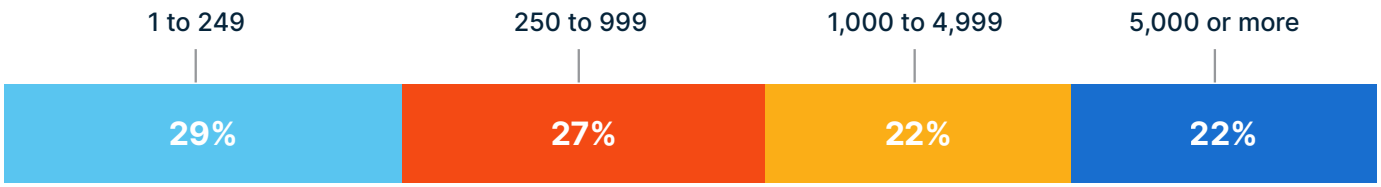
We sought to understand respondent organization preparedness to withstand a ransomware attack, the level of effort required to execute on a ransomware preparedness plan, and gain insight into the resulting overall recovery capabilities of these respondent organizations.

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.

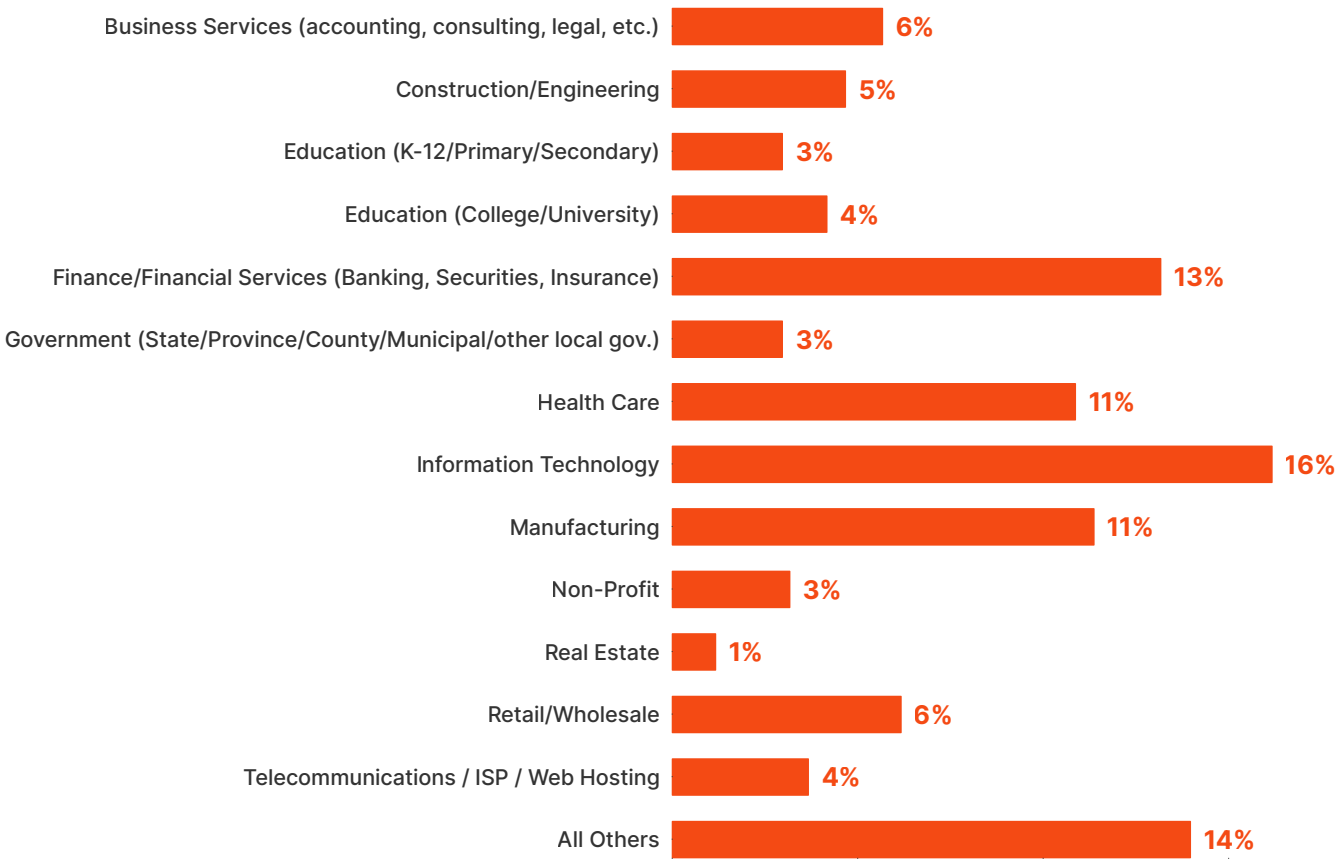
Appendix: Answers to Other Survey Questions

Respondent Demographics

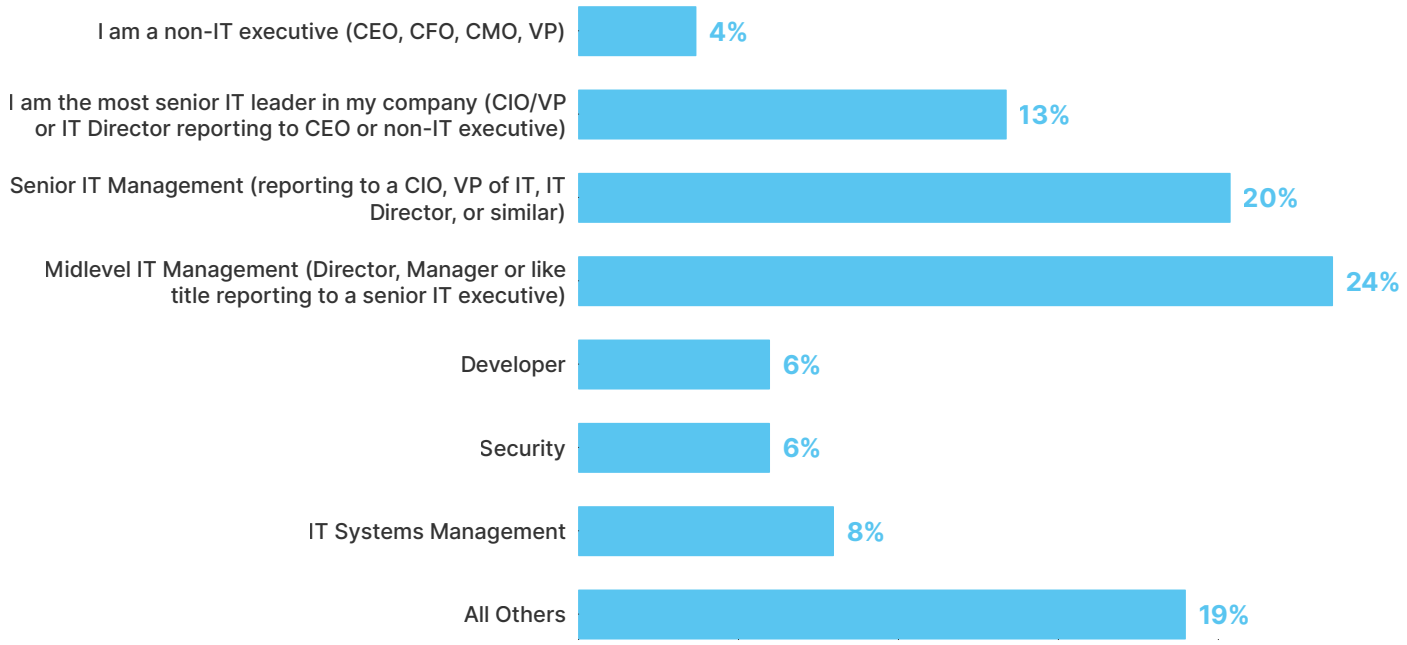
How many people are in your organization? (N=404)



Which of the following best describes the principal industry of your organization? (N=402)



Which best describes your primary functional responsibility? (N=402)



Other Interesting Statistics

In terms of your role as it relates to ransomware and ransomware recovery, in what areas do you contribute? (check all that apply)