2024

The State of Ransomware

A REVEALING REPORT FOR IT PROFESSIONALS
BY IT PROFESSIONALS

ransomware.org
understand · prevent · recover

POWERED BY ActualTech MEDIA

Executive Summary

Ransomware remains one of the most pervasive cybersecurity threats today.

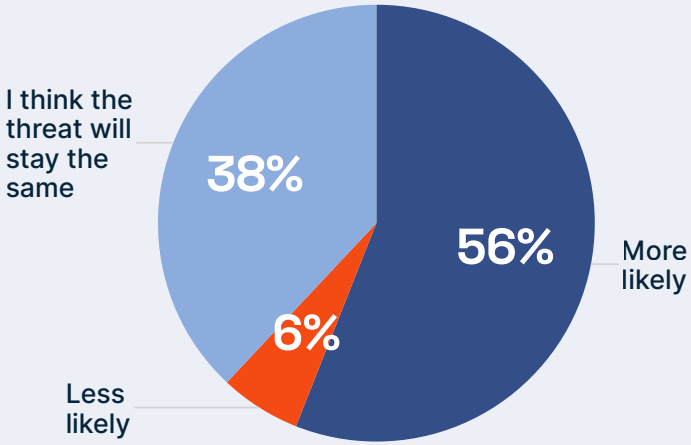
Despite some encouraging trends (fewer organizations are paying ransom demands) there are many equally disturbing trends (total ransomware payments exceeded $1 billion in 2023). In this survey report, we explore these trends and assess organizational preparedness for ransomware attacks including training and awareness, incident response capabilities, investment in security tools and technologies, and more.

Despite some encouraging trends (fewer organizations are paying ransom demands) there are many equally disturbing trends (total ransomware payments exceeded $1 billion in 2023).

Results and Analysis

QUESTION 1

Compared with 2023, do you think your company is more or less likely to be a target of ransomware attacks this year?



2023 was a record year for ransomware gangs and cybercriminals. Cryptocurrency-tracing firm Chainalysis reports that total ransomware payments nearly doubled to $1.1 billion in 2023, exceeding the $1 billion mark for the first time ever. Cybersecurity firm Record Future reports that the number of ransomware attacks increased from 2,581 in 2022 to 4,399 in 2023, based on media reports and public listings of victims by ransomware gangs on dark web sites.

Thus, ransomware attacks continue to be one of the top cybersecurity threats in 2024 for public and private sector organizations globally, regardless of their size and/or industry. Yet, despite the alarming trend in rising ransomware attacks and payments, according to a recent ActualTech Media (ATM) survey, only a slight majority (56 percent) of respondents believe there organization is more likely to be the target of a ransomware attack in 2024.

KEY INSIGHT

With ransomware attacks and ransom payments nearly doubling in 2023, it is statistically more likely that companies will be targeted by ransomware attacks in 2024 and beyond, as this trend shows no signs of slowing down.

QUESTION 2

Which of the following attack tactics has your team or organization observed?

(Select all that apply)

Of the respondents whose organizations have been targeted (whether successful or unsuccessful) in a ransomware attack, 55 percent observed traditional ransomware tactics (data encrypted for ransom). Alarmingly, many organizations are also observing tactics associated with double- and triple-extortion ransomware attacks including data exfiltration (38 percent), distributed denial-of-service (DDoS, 37 percent), threats to release customer data (34 percent), and direct contact with customers (21 percent).

KEY INSIGHT

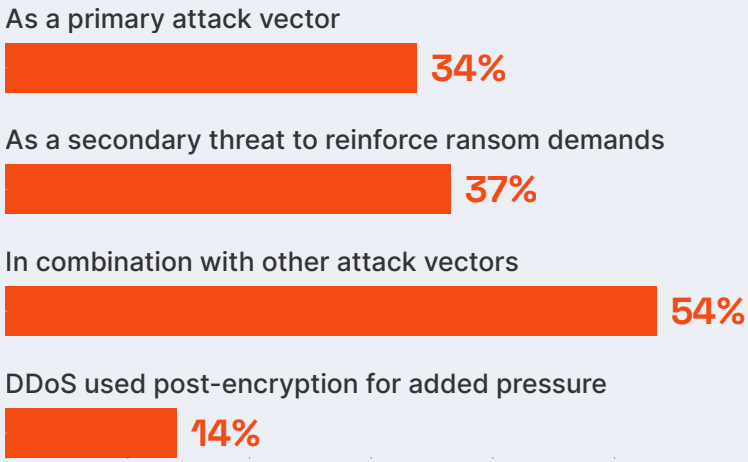
Ensure your security tools and incident response plans can effectively address increasingly advanced, multi-faceted ransomware attacks (including DDoS and data theft).

> **Alarmingly, many organizations are also observing tactics associated with double- and triple-extortion ransomware attacks.**

QUESTION 3

How are DDoS attacks being integrated into ransomware strategies against your organization?

(Select all that apply)



Looking closer at DDoS attacks, organizations are increasingly seeing DDoS as a primary attack vector (34 percent) in ransomware attacks or in combination with other attack vectors (54 percent). DDoS attacks are particularly effective because downtime can be one of the costliest aspects of any cybersecurity attack, as witnessed in the 2021 Colonial Pipeline ransomware attack which resulted in protracted and costly supply chain issues along the U.S. Eastern Seaboard in the wake of the attack. Although the ransomware attack did not have a DDoS component, the rapid (and correct) response by Colonial Pipeline to shut down critical systems, and their inability to quickly restart these systems after the attack was over, effectively resulted in a self-inflicted DDoS attack.

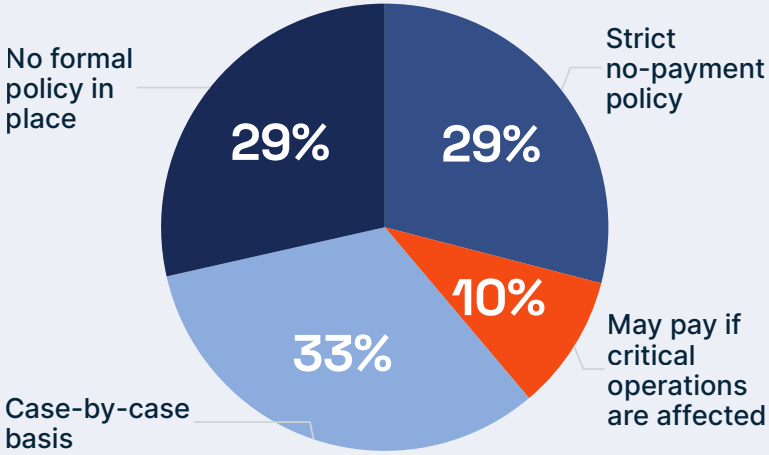
DDoS attacks are used by ransomware gangs and cybercriminals as a secondary threat to reinforce ransom demands (37 percent) and to increase pressure on victim organizations to pay the ransom (14 percent).

KEY INSIGHT

Regularly test (and update, as necessary) your business continuity and disaster recovery plans to ensure you can quickly restore critical systems to normal operation and minimize costly downtime associated with DDoS attacks.

QUESTION 4

What is your organization's policy regarding ransom negotiation and payment of ransom?



Despite the $1.1 billion record haul of ransom payments in 2023, the number of ransomware victims that actually paid ransom demands dropped to a record low of 29 percent in the fourth quarter of 2023 (compared to 85 percent at the start of 2019), according to ransomware negotiation firm Coveware.

A number of factors contribute to this decline in ransom payment. Ransomware gangs are often sponsored by rogue nation-states, as well as criminal and terrorist organizations. Paying a ransom puts an organization at risk of running afoul of the U.S. Federal Bureau of Investigation (FBI) and U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) sanctions. Even after paying a ransom, many organizations that pay a ransom have found that their data is still not recoverable or that it is still posted on the dark web for sale to the highest bidder(s).

> **Even after paying a ransom, many organizations that pay a ransom have found that their data is still not recoverable or that it is still posted on the dark web for sale to the highest bidder(s).**

Unfortunately, one of the simplest, least expensive, and most important things an organization can do to prepare for a ransomware attack is to define a ransomware policy that addresses whether or not to pay a ransom. During a ransomware attack, seconds count. You are literally racing against the attacker to prevent your data from being encrypted. Every critical decision must be made quickly with the best available information. There is no room for ambiguity, yet despite this fact, 29 percent of respondents have no formal policy in place regarding payment of a ransom demand. Nearly half answered they would decide whether or not to pay a ransom demand on a case-by-case basis (33 percent) or if critical operations are affected (10 percent) — both of these answers are effectively "let's wait and see" which, along with organizations that have no formal policy, greatly limits the options and increases the likelihood that 82 percent of organizations will either pay or suffer other serious financial consequences *when* they become the target of a successful ransomware attack.

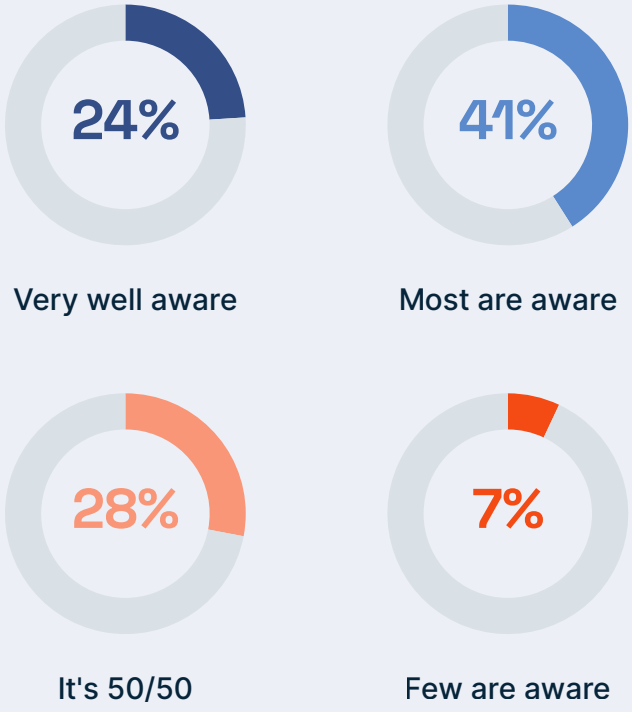
KEY INSIGHT

Update security awareness and training to ensure your users can recognize constantly evolving ransomware tactics and techniques.

During a ransomware attack, seconds count. You are literally racing against the attacker to prevent your data from being encrypted.

QUESTION 5

Do you think those in your organization are aware of the threat?



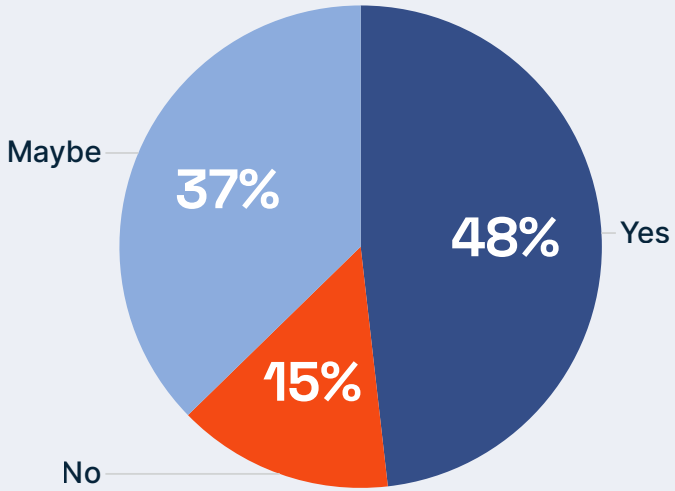
End-users have traditionally been considered the weakest link in an organization's security posture. As a result, security awareness and training initiatives have underpinned efforts to build a "secure culture". In the ATM survey, nearly two-thirds of respondents (65 percent) responded that the people in their organization were "aware" or "very well aware" of the ransomware threat. Despite this encouraging finding, it is imperative that organizations continue to evolve their training and awareness programs to keep pace with the constantly changing ransomware threat. Specifically, ransomware gangs have developed new and sophisticated tactics and techniques that go far beyond the basic (and common) misperception that a ransomware attack starts with an end-user unwittingly clicking on a malicious link in an email and a ransom note suddenly appearing on their monitor with ominous warnings.

KEY INSIGHT

Update security awareness and training to ensure your users can recognize constantly evolving ransomware tactics and techniques.

QUESTION 6

Do you believe your organization is ready for a ransomware attack?



Turning to incident response, less than half (48 percent) of respondents in the ATM survey were confident in their organization's readiness to respond to a ransomware attack.

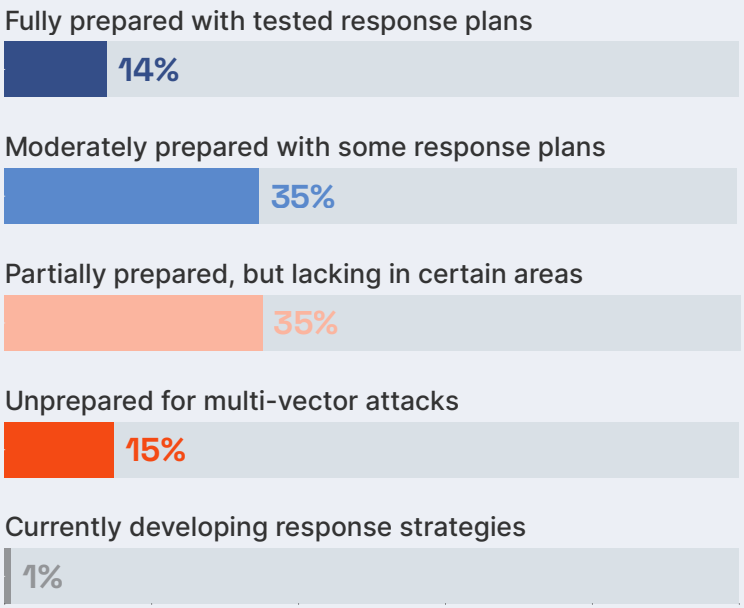
KEY INSIGHT

Regularly test (and update, as necessary) your incident response plan and ransomware playbook to ensure everyone knows what they need to do to effectively contain, eradicate, and recover from a ransomware attack.

> **Less than half of respondents were confident in their organization's readiness to respond to a ransomware attack.**

QUESTION 7

How prepared is your organization to respond to multi-vector ransomware attacks?



This perception continues when asked specifically about multi-vector ransomware attacks (such as increasingly common double- and triple-extortion attacks). 14 percent of respondents answered that their organizations were fully prepared (with tested response plans) and 35 percent answered that they were moderately prepared (with some response plans). Alarmingly, more than half acknowledge that their response capabilities were lacking in certain areas (35 percent) or that they were unprepared (15 percent) or currently developing response strategies (1 percent).

KEY INSIGHT

Ensure your incident response plan and ransomware playbook adequately addresses traditional ransomware, as well as double-and triple-extortion ransomware attacks.

QUESTION 8

What is the size of your organization's incident response team who would be directly responsible for responding to a ransomware attack?

Delving further into incident response, nearly half (46 percent) of respondents have incident response teams comprised of only 1 to 5 members and nearly three-fourths (73 percent) have fewer than 10 members. Even for a smaller organization, incident response teams will generally require a broad range of roles and skills including security, IT, communications, legal, and business leadership, as well as outside resources such as managed detection and response (MDR), cyber threat intelligence, forensics services, ransom negotiators, and law enforcement.

KEY INSIGHT

In addition to IT and security, your incident response team needs to include representatives from business leadership, communications, legal, and third-party resources.

> **Even for a smaller organization, incident response teams will generally require a broad range of roles and skills.**

QUESTION 9

How do you view law enforcements' role in ransomware response?

With regard to law enforcement involvement in ransomware response, only 30 percent of organizations answered that law enforcement provided a helpful and responsive presence. This generally negative attitude toward law enforcement is another unfortunate revelation that can be relatively easily (and inexpensively) addressed. Law enforcement agencies at local, state, and federal levels have widely varying skills and capabilities for dealing with ransomware attacks. But having law enforcement support during a ransomware attack is never a bad thing, regardless of their cybersecurity depth. Take the time to cultivate formal relationships with local and state law enforcement, in particular, as well as federal law enforcement agencies through organizations such as InfraGard.

KEY INSIGHT

Be proactive in cultivating strong relationships with law enforcement and other external resources *before* a ransomware attack happens.

QUESTION 10

As you build your ransomware incident response team, which of these skills are you prioritizing in your hiring and training processes?

(Select all that apply)

Survey respondents understand that incident response team members must possess a broad range of skills and knowledge as evidenced by their hiring and training priorities including cybersecurity fundamentals, incident response and management, and network security and architecture (64 percent each); advanced threat intelligence analysis (47 percent), forensic analysis (37 percent), and legal and compliance knowledge (29 percent).

KEY INSIGHT

Ensure you have the right mix of skills and experience on your incident response team and address any deficiencies through training and hiring (if necessary).

QUESTION 11

How does your organization approach training and development for ransomware incident responders?

(Select all that apply)

When it comes to training and career development, only 43 percent of survey respondents provide access to external training and certification programs for their ransomware incident responders. On-the-job training and regular in-house training sessions are the predominant methods for training and development at 58 percent and 51 percent, respectively. Theoretically, on-the-job training and regular in-house training can be some of the most effective methods, giving individuals an opportunity to realistically train and learn with the actual incident team members and in the actual IT environment where there skills and experience will be needed. However, there can be a great deal of variability in these internal efforts: in-house training sessions may be limited by the knowledge and skills of the internal training facilitators and on-the-job training sometimes (if not, often) translates to "whenever we have time".

KEY INSIGHT

Use a mix of both formal and informal training that includes both internal and external programs to develop a more effective ransomware incident response team.

QUESTION 12

What are the biggest challenges you face in recruiting new hires for ransomware prevention and incident response?

(Select all that apply)

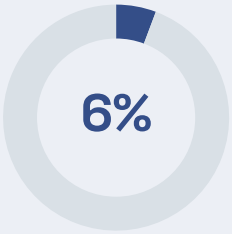
Recruiting and retaining cybersecurity professionals continues to be a major challenge for organizations everywhere, and finding candidates with specific knowledge or experience with ransomware incident response can be particularly challenging. The ISC2 2023 Cybersecurity Workforce Study found that the global security workforce grew to an all-time high of 5.5 million (nearly double the 2019 cybersecurity workforce), but the gap between supply and demand has increased to 4 million. ATM survey respondents report that their biggest recruiting challenges include budget constraints (61 percent), finding candidates with specialized skills (49 percent), and lack of awareness or interest in ransomware defense roles (29 percent).

KEY INSIGHT

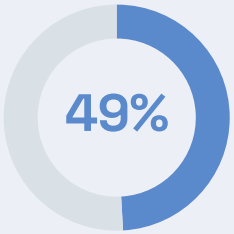
The global security workforce shortage is improving, but it's still challenging to hire and retain qualified professionals. Focus on developing and retaining your top talent to ensure your team has the skills necessary to effectively respond to ransomware and other threats.

QUESTION 13

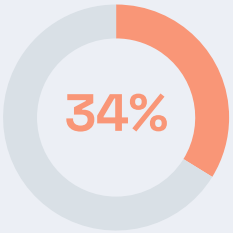
To what extent does your organization rely on outsourced services for ransomware prevention and incident response?



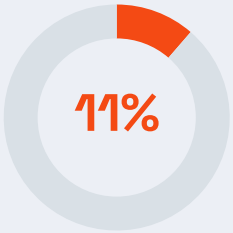
Entirely outsourced



Partially outsourced, but we have an in-house team as well



Minimal outsourcing, primarily in-house



Do not use outsourced services for ransomware defense

To address the challenges of recruiting and developing an effective ransomware incident response team/capability in a job market with such a wide gap in the availability of qualified candidates, many organizations turn to outsourced services for ransomware prevention and incident response. Among survey respondents, 6 percent outsource entirely, and 49 percent partially outsource to supplement their in-house capabilities.

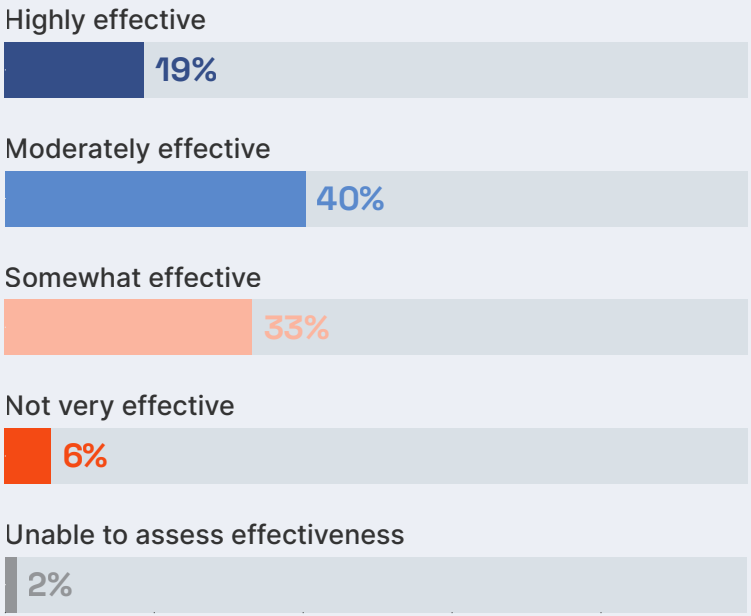
KEY INSIGHT

Augment your in-house ransomware response capabilities with outsourced and/or managed services from trusted partners.

> **Among survey respondents, 6 percent outsource entirely, and 49 percent partially outsource to supplement their in-house capabilities.**

QUESTION 14

How confident do you feel in the efficacy of your current technology solutions to prevent and mitigate ransomware attacks?



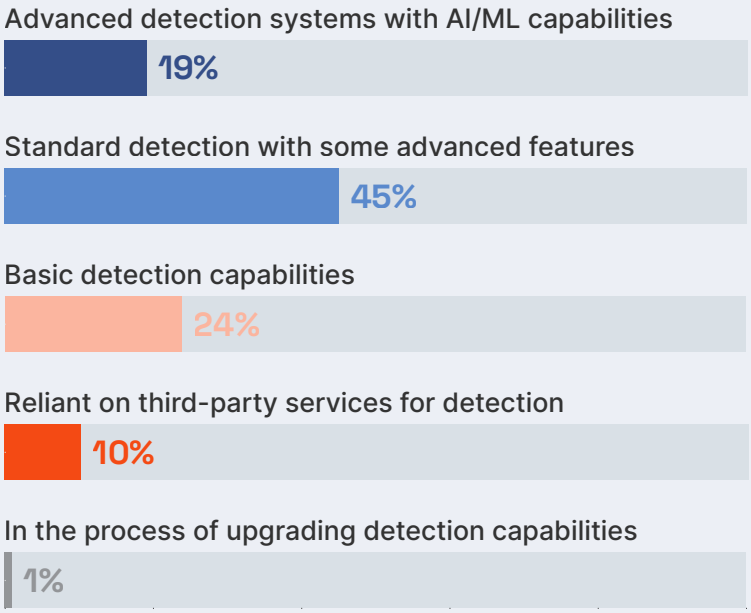
Among survey respondents, the majority are confident that their current technology solutions are highly effective (19 percent) or moderately effective (40 percent) in preventing and mitigating ransomware attacks.

KEY INSIGHT

Regularly train with and test your security tools to ensure your incident response team can use them effectively during a ransomware attack. Continuously evaluate new technology solutions to take advantage of the latest innovations to increase your incident response effectiveness against constantly evolving threats.

QUESTION 15

What is your organization's capability in detecting advanced ransomware techniques?



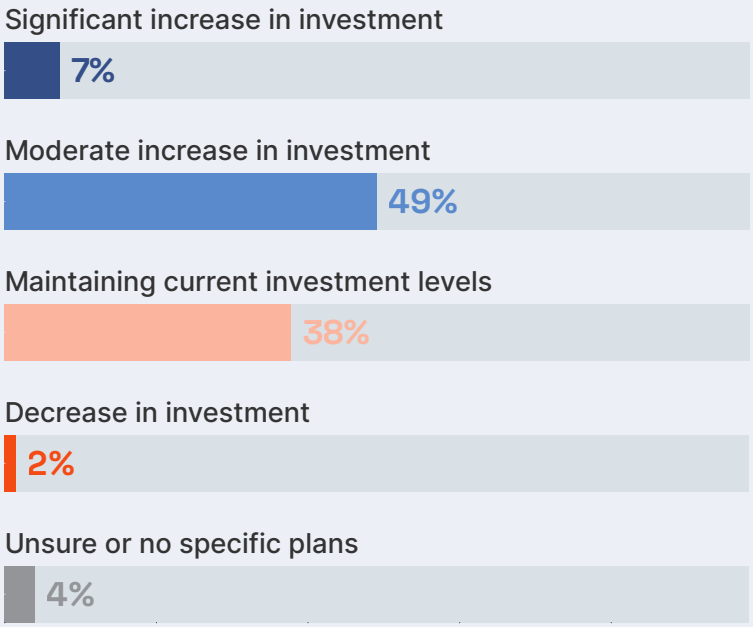
Nearly three-quarters of organizations are currently using advanced detection systems with artificial intelligence (AI) and machine learning (ML) capabilities (19 percent), have standard detection capabilities with some advanced features (45 percent), or are reliant on third-party services to detect ransomware.

KEY INSIGHT

Update your technology stack and services to take advantage of the latest innovations for advanced ransomware detection.

QUESTION 16

How is your organization planning to invest in new technologies for ransomware defense in 2024?



Despite their confidence in the effectiveness of their current technology solutions, the majority of organizations are planning to increase their spending on new tools and technologies for ransomware defense, commensurate with the growing and rapidly evolving nature of the ransomware threat. 7 percent of respondents are planning a significant increase in their investment in this area for 2024, while 49 percent are planning a moderate increase and 38 percent plan to maintain their current investment levels for ransomware defense.

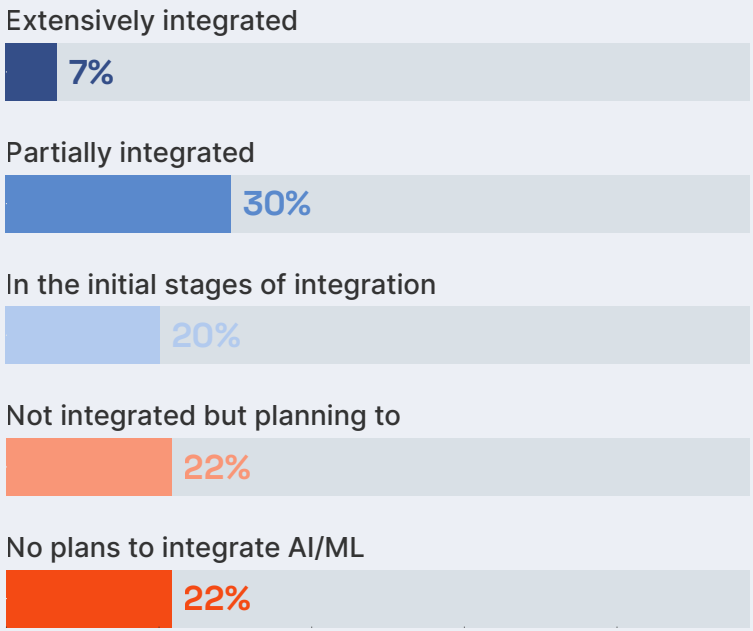
KEY INSIGHT

Plan for additional investments in ransomware defense as the threat landscape continues to evolve and adversaries develop new tactics and techniques.

> **49 percent are planning a moderate increase and 38 percent plan to maintain their current investment levels for ransomware defense.**

QUESTION 17

To what extent is your organization integrating AI and machine learning in ransomware defense strategies?



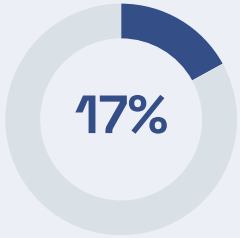
Security tools for ransomware defense — including extended detection and response (XDR), user and entity behavior analytics (UEBA), data loss prevention (DLP), cyber threat intelligence (CTI), security information and event management (SIEM), and security orchestration, automation, and response (SOAR) — are increasingly leveraging artificial intelligence (AI) and machine learning (ML) to enhance their effectiveness. The majority of organizations are aligned with this trend with 7 percent of respondents reporting that AI/ML technologies are extensively integrated in their ransomware defense strategies, 30 percent are partially integrated, 20 percent are in the initial stages of integration, and 22 percent are planning to integrate.

KEY INSIGHT

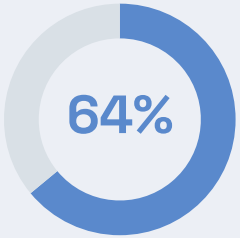
AI/ML technologies are rapidly maturing. Ensure your ransomware defense strategies fully leverage these innovations to effectively counter the ransomware threat.

QUESTION 18

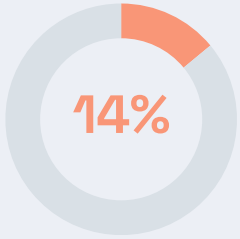
How reliant is your organization on cloud-based security solutions for ransomware defense?



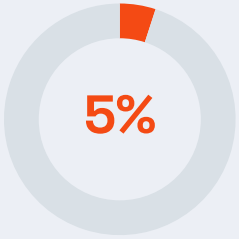
Fully reliant on cloud-based solutions



Partially reliant, in combination with on-premises solutions



Minimal reliance on cloud-based solutions



Not using cloud-based security solutions

The speed, scale, and flexibility of cloud-based services and solutions can be a force multiplier for an organization's ransomware defense. Organizations are overwhelmingly leveraging these capabilities with 17 percent of respondents being fully reliant on cloud-based solutions and 64 percent leveraging a combination of cloud-based and on-premises solutions as part of their ransomware defense strategy.

KEY INSIGHT

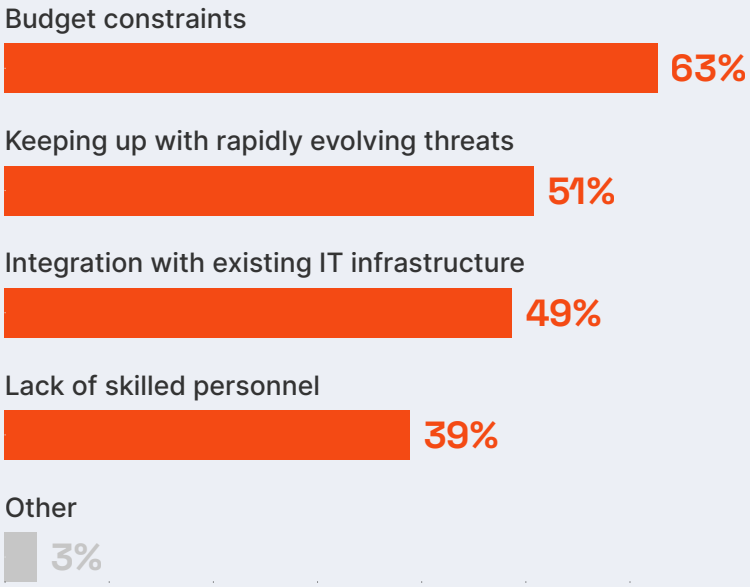
Cloud-based solutions bring the benefits of the cloud — such as agility and on-demand scalability — to ransomware defense.

> **The speed, scale, and flexibility of cloud-based services and solutions can be a force multiplier for an organization's ransomware defense.**

QUESTION 19

What are the primary challenges your organization faces in implementing technology solutions for ransomware defense?

(Select all that apply)



Despite their willingness to spend on new tools and technologies (including cloud-based solutions), and to leverage AI/ML in their ransomware defense efforts, organizations continue to face real challenges implementing these technology solutions including budget constraints (63 percent), keeping up with rapidly evolving threats (51 percent), integrating with existing IT infrastructure (49 percent), and lack of skilled personnel (39 percent).

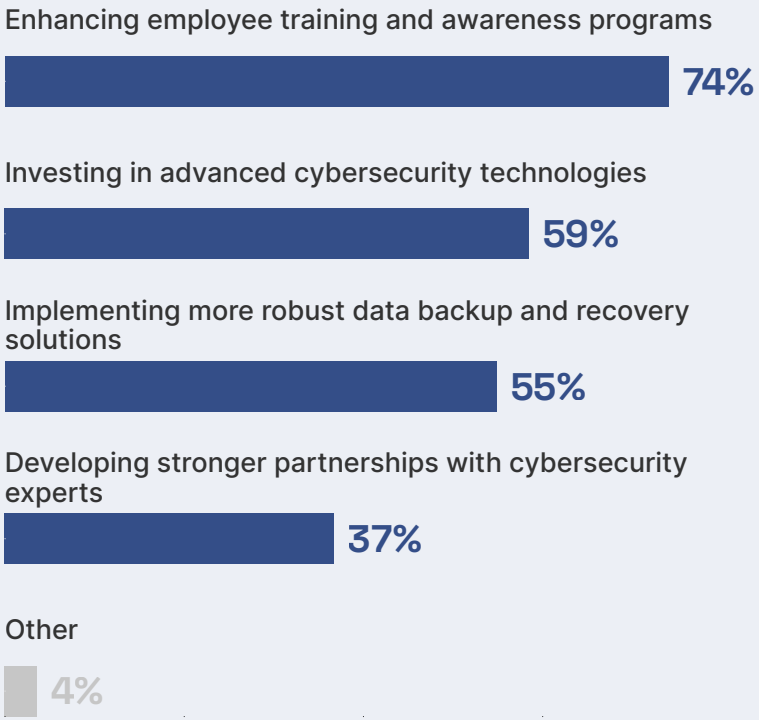
KEY INSIGHT

Dedicate the necessary resources to properly implement and integrate ransomware defense tools and technologies, and provide appropriate training on how to use these solutions for your incident response team.

QUESTION 20

How is your organization preparing for future, more sophisticated ransomware threats?

(Select all that apply)



Looking to the future, organizations are planning to further enhance their employee training and awareness programs (74 percent), invest in advanced cybersecurity technologies (59 percent), and implement more robust data backup and recovery solutions (55 percent).

KEY INSIGHT

Training and awareness, implementing advanced cybersecurity tools and technologies, and ensuring a robust backup and recovery capability are all key to an effective ransomware defense strategy.

Conclusion

These are all important aspects of a robust ransomware defense strategy.

Despite an increasingly sophisticated and ever-changing ransomware threat landscape, there are many initiatives that organizations can undertake as part of their ransomware defense strategy that are relatively easy and inexpensive, such as enhancing employee training and awareness, creating and implementing ransomware policies (including whether or not to pay a ransom demand), developing and regularly testing ransomware incident response playbooks, and building strong partnerships with cybersecurity experts, industry peers, and law enforcement agencies.

There are many initiatives that organizations can undertake as part of their ransomware defense strategy that are relatively easy and inexpensive.