CROWDSTRIKE

STATE OF RANSOMWARE SURVEY

Organizations overestimate their ransomware readiness in the face of an evolving ransomware landscape

Table of Contents

Executive Summary

Artificial intelligence has redefined the ransomware battlefield as adversaries explore new AI-driven methods and hone their techniques. Many organizations think they are prepared to face it. The numbers tell a different story.

CrowdStrike surveyed 1,100 IT and cybersecurity decision-makers across Australia, France, Germany, India, Singapore, United Kingdom, and United States to ask how they assess their ransomware readiness and navigate the evolving ransomware landscape, including the emergence of AI-enhanced threats.

Of the organizations surveyed, 78% reported experiencing a ransomware attack within the past year. Of those, half believed they were “very well prepared” for ransomware, but fewer than a quarter recovered from an attack within 24 hours. Nearly 25% suffered significant disruption or data loss.

This is the confidence illusion: Organizations overestimate their ransomware preparedness as adversaries become more sophisticated in their use of AI-powered tactics. The threat landscape changes so rapidly that it’s easy for an organization to underestimate the sophistication of these modern attacks or misjudge its ability to recover.

The findings reveal clear security gaps. As adversaries harness the power of AI advancements and run their operations like an enterprise business, organizations should be aware that the confidence they have in their ransomware readiness may not match their actual security posture. Those that continue to rely on outdated defenses and fail to adapt their security strategy will remain vulnerable. Genuine ransomware readiness requires honest assessment, AI-enabled defenses, and embedded threat intelligence to keep pace with an intensifying cybercrime economy.

Top 3 Takeaways

1

Most organizations are not as ready as they think.

Despite perceived preparedness, 78% of respondents were hit by ransomware in the preceding 12 months. Only 22% of victims that felt "well-prepared" beforehand recovered within 24 hours, and just 38% fixed the issue that allowed the attackers to enter.

2

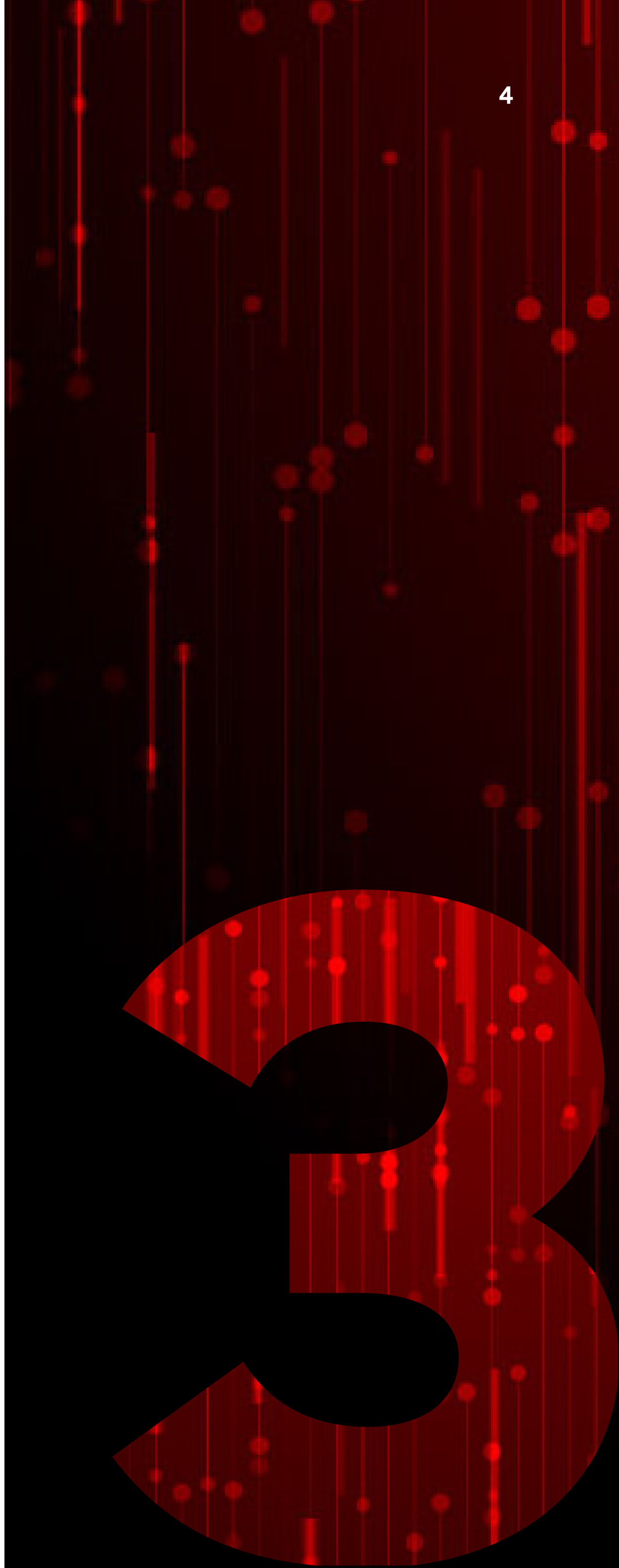
The AI arms race favors speed. Attackers are winning.

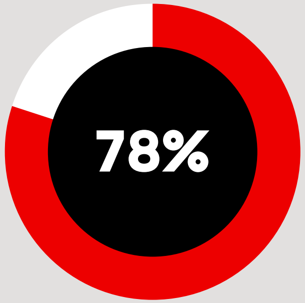
As adversaries automate intrusion and social engineering, defenders struggle to keep pace: 76% of respondents said it's getting harder to be fully prepared, and nearly half fear that they can't detect or respond as fast as AI-driven attacks can execute.

3

Ransom payments aren't paying off.

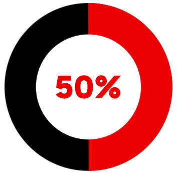
Payment offers no safety net: 83% of paying victims were attacked again, and 93% had data stolen anyway. Backups proved unreliable for many, with nearly 4 in 10 unable to fully restore the data they lost.





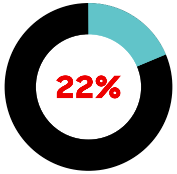
Experienced a ransomware attack within the past year

Of those who were attacked,

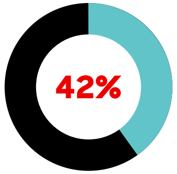


Believed they were "very well prepared" for a ransomware incident beforehand

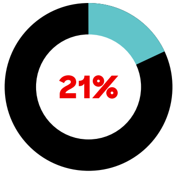
Of those ››››



Were able to recover within 24 hours



Suffered significant downtime



Paid ransom but still unable to recover all data

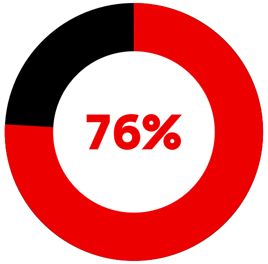
Ransomware Reality Check

The Leadership Disconnect

A staggering 76% of organizations report a growing disconnect between how leadership and the security team perceive their ransomware readiness. This gap is the widest in Singapore (92%) and the energy sector (94%).

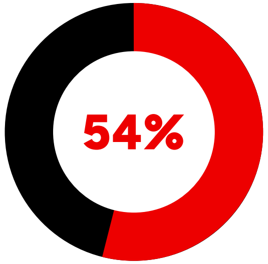
More than half (54%) of board members and C-level executives believe their organizations are “very prepared” to face ransomware, compared to 46% of security teams. This disparity is particularly concerning because security managers have more operational visibility into security capabilities and day-to-day threat management.

The disconnect hampers effective security investment. When leadership overestimates capabilities, they may resist requests for additional security resources or fail to prioritize critical improvements. Building readiness requires closing this perception gap through better communication and data sharing between security teams and executive leaders.

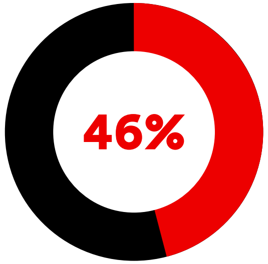


Report a growing disconnect between how leadership perceives their ransomware readiness and their actual level of preparedness

Believed they were very prepared prior to their most recent ransomware incident



Board member/C-level executive



Mid-level management

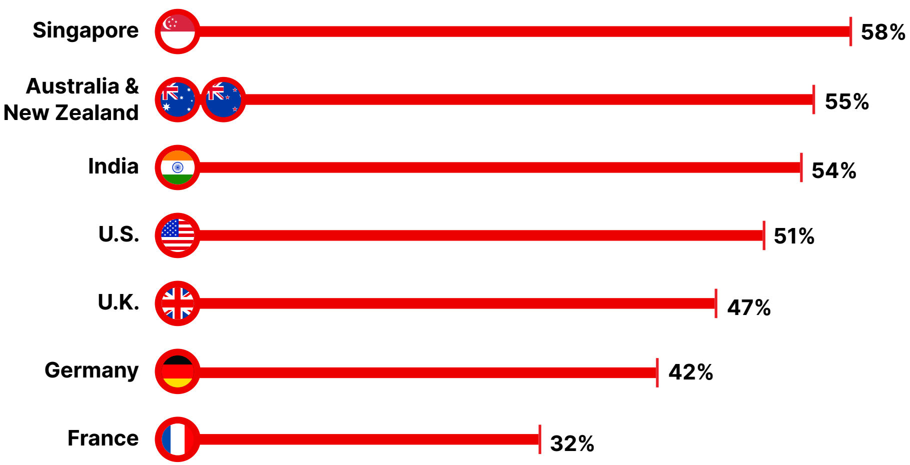
Regional Variations in Preparedness

In the United States, the largest survey base, 51% of respondents believed they were very well prepared for a ransomware attack, but only 17% of respondents recovered within 24 hours.

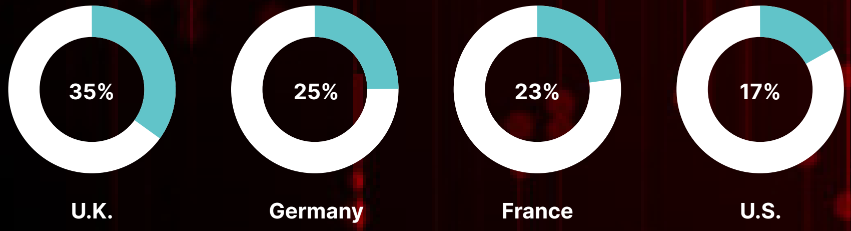
European organizations show a different pattern: Though they were less likely to rate themselves as "very prepared," they achieved faster recovery times overall. U.K. organizations led recovery performance, with 35% recovering within 24 hours, despite only 47% rating themselves as very prepared. Among German organizations, 25% achieved same-day recovery, with 42% rating themselves as very prepared, while 23% of French organizations were able to recover within 24 hours, with just 32% rating themselves as very prepared.

This conservative self-assessment contrasts sharply with both the United States and Singapore. In Singapore, 58% of respondents believed they were very well prepared, but recovery performance lagged significantly, with only 7% able to recover within 24 hours.

Believed they were very prepared before their latest ransomware attack



Countries most likely to have recovered within 24 hours of their latest ransomware attack



Readiness Across Sectors

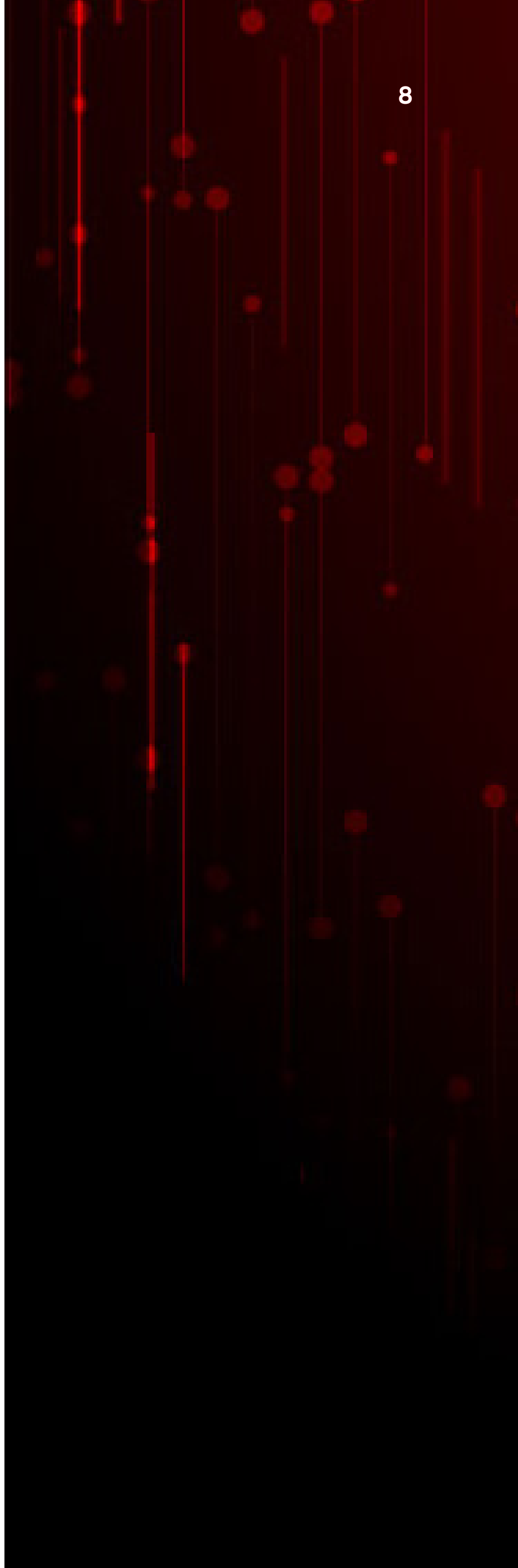
Certain industries show concerning gaps between confidence and capability:

Public sector organizations, where 60% of respondents said they are very well prepared, demonstrate the poorest recovery performance. Only 12% recovered within 24 hours, and 42% suffered significant disruption. This disconnect is troubling given the critical services these organizations provide and the sensitive citizen data they protect.

Manufacturing and production organizations similarly show high confidence, with 58% saying they are very well prepared, but they also had poor recovery performance: 12% recovered in the same day, and 40% had significant disruption. The sector's reliance on operational technology and production makes extended downtime particularly damaging.

Financial services stands out as the exception: 52% of financial services organizations rated themselves very well prepared, and 38% achieved same-day recovery.

Sector	% that rated themselves very well prepared	Of those rating themselves very well prepared		
		% recovered within 24 hours	% that suffered significant downtime or disruption to business operations	% that had data publicly released or stolen
Public Sector	60%	12%	42%	30%
Manufacturing and Production	58%	12%	40%	25%
Retail, Distribution, and Transport	53%	21%	44%	29%
Healthcare	52%	23%	40%	35%
Financial Services	52%	38%	37%	26%
IT and Telecom	43%	28%	36%	18%



Common Ransomware Attack Vectors

Phishing was cited by 45% of victims as the initial point of compromise, making it the leading access vector for ransomware. Despite 92% of organizations believing their employees are well trained to spot phishing emails, many incidents began when staff members clicked malicious links or opened infected files.

Other frequently cited entry points include vulnerability exploits (40%), supply chain compromise (35%), compromised credentials (33%), malicious downloads (32%), misuse of remote monitoring and management (RMM) tools (31%), and insider threats (27%). Though human error is the most visible weakness, these attacks reveal a broader pattern: Technical gaps, outdated defenses, and inconsistent preparedness combine to create multiple opportunities for adversaries to succeed.

Adversaries are increasingly exploiting RMM tools such as RDP and AnyDesk to gain covert access, maintain persistence, and deploy ransomware without raising immediate suspicion. Nearly one in three organizations (31%) that suffered a ransomware attack reported RMM tools as the attacker's entry point, underscoring how often legitimate IT utilities are turned against their operators.

CrowdStrike has also observed adversaries, including PUNK SPIDER and BLOCKADE SPIDER, using ransomware variants that remotely encrypt files over Windows Server Message Block (SMB) network shares from unmanaged systems, allowing them to encrypt remote targets without transferring the ransomware binary.[1] It's a scenario most defenders recognize as a serious gap: 76% of organizations reported being concerned about their ability to stop ransomware spreading from an unmanaged host over SMB today.

45%

Reported a phishing email allowed the attacker access during their latest ransomware attack

84%

Have seen a measurable increase in phishing and/or credential theft incidents they suspect were AI-assisted

[1] CrowdStrike 2025 Threat Hunting Report https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/

The AI Arms Race

Most organizations (76%) agree it's increasingly difficult to prepare as attackers use AI to adapt and evade defenses. AI has altered the ransomware landscape, creating an arms race where attackers and defenders deploy increasingly sophisticated tools. The emergence of AI-powered attacks challenges traditional security models built around predictable threat patterns and human-driven response times.

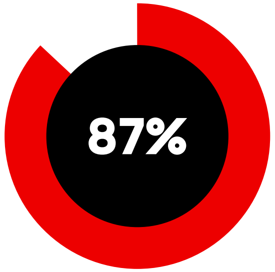
The Social Engineering Evolution

AI-generated social engineering is a concerning development in the threat landscape: 82% of organizations believe generative AI (GenAI) makes phishing emails more difficult to identify, even for well-trained employees. This challenge further undermines traditional security awareness training programs.

82% **Believe that generative AI is making phishing emails more difficult to identify, even for well-trained employees**

Most organizations (87%) consider AI-generated social engineering tactics more convincing than traditional methods. The sophistication of these attacks creates new challenges for human detection, as AI can craft contextually appropriate messages that exploit specific organizational or individual security gaps.

The threat extends beyond current capabilities: 87% of organizations expect deepfakes to become major attack vectors in future ransomware campaigns, with healthcare organizations (89%) and C-level executives (90%) expressing the greatest concern. This evolution suggests social engineering will become increasingly difficult to counter through training alone.



Believe deepfake audio and video will become major vectors for social engineering in future ransomware attacks

SECTOR	SENIORITY
Healthcare 89%	C-level executives 90%
Financial services 88%	Senior management 86%
Public sector 83%	Mid-level management 88%

The Detection Challenge

A critical speed differential exists between AI-powered attacks and human-driven defenses: 45% of organizations reported worrying they cannot detect and respond to threats as quickly as AI-automated attacks can execute. This gap creates a disadvantage for security operations centers that rely on human analysis and decision-making.

Most security teams (85%) acknowledge traditional detection methods are not keeping pace with modern threats. Yet defenders' AI adoption lags behind, with only 53% implementing AI-powered threat detection. This gap leaves organizations vulnerable to increasingly faster attacks.

Defenders' AI Adoption

Organizations deploy AI across multiple security use cases, but adoption remains uneven:

AI-powered threat detection leads adoption at 53% among surveyed organizations, followed by automated incident response at 51% and AI-enhanced phishing detection at 48%. GenAI-assisted investigation, AI-based threat hunting, and other advanced capabilities were reported to have moderately lower adoption rates, suggesting organizations are still exploring how to integrate AI into their security operations.

Public sector organizations lag significantly in AI adoption, with only 41% implementing AI-powered threat detection compared to 54% of healthcare organizations and 50% of financial services organizations. This gap is concerning given the sensitive nature of government data and the sector's critical importance to society.

85%

believe traditional detection methods are becoming obsolete in the face of AI-enhanced attack strategies

Variations Span Geographies and Industries

The concern of AI-enabled threats varies significantly across regions and industries, suggesting different risk profiles and preparedness levels:

42% of U.S. respondents cited AI-generated phishing emails as a top concern; 37% cited GenAI-enabled malware. French organizations showed the greatest concern about AI-enabled threats overall (57% vs. 45% on average across geographies) and GenAI-enabled malware (53% vs. 40% average), potentially reflecting recent experience with sophisticated attacks. U.K. and Singapore organizations expressed the most concern about social engineering tactics (57% each), suggesting that these threats are already materializing in their environments.

Senior decision-makers showed more concern about AI-generated phishing emails (50%) compared to junior management (40%), possibly reflecting their higher profile as social engineering targets. Industry variations suggest sector-specific threat patterns, with healthcare, financial services, and public sector organizations facing different AI-enhanced attack profiles.

The Economics of Ransomware: When Payments Don't Pay Off

The ransomware economy has evolved from opportunistic attacks to sophisticated business operations. However, paying a ransom does not guarantee threat actors will not leak the victim's data or strike again, fundamentally altering the risk-benefit calculation for targeted organizations.

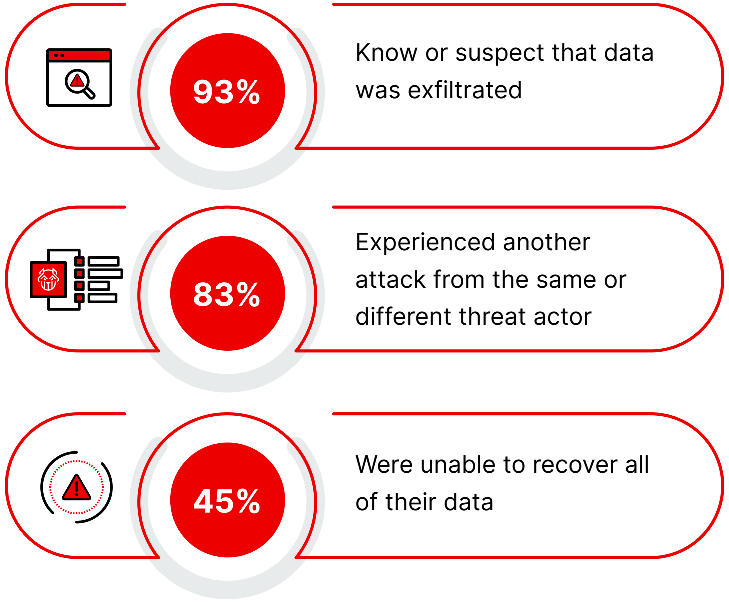
Ransom Payment Realities

Organizations that pay ransoms face significant ongoing risks that challenge their perceived value of complying with attacker demands. Most paying victims (83%) said they experienced another attack from the same or different threat actor, demonstrating that payment marks organizations as profitable targets rather than providing security. Even more paying victims (93%) learned that data was exfiltrated despite payment. And 45% could not recover all of their data even after paying.

Backups and rollback features aren't a safety net. 39% of organizations couldn't fully recover from backups after their last ransomware incident, and in 93% of cases, data was stolen anyway, proving data recovery alone no longer ends the crisis. Though 61% did successfully restore from backups after their most recent incident, 82% acknowledge that despite their ability to fully restore, they are not equipped to weather the reputational fallout from sensitive data leaks.

These statistics demonstrate that ransom payments provide neither security nor complete data recovery. The economics favor attackers that can collect payment while retaining stolen data for future exploitation, additional extortion attempts, or sale to other criminal groups.

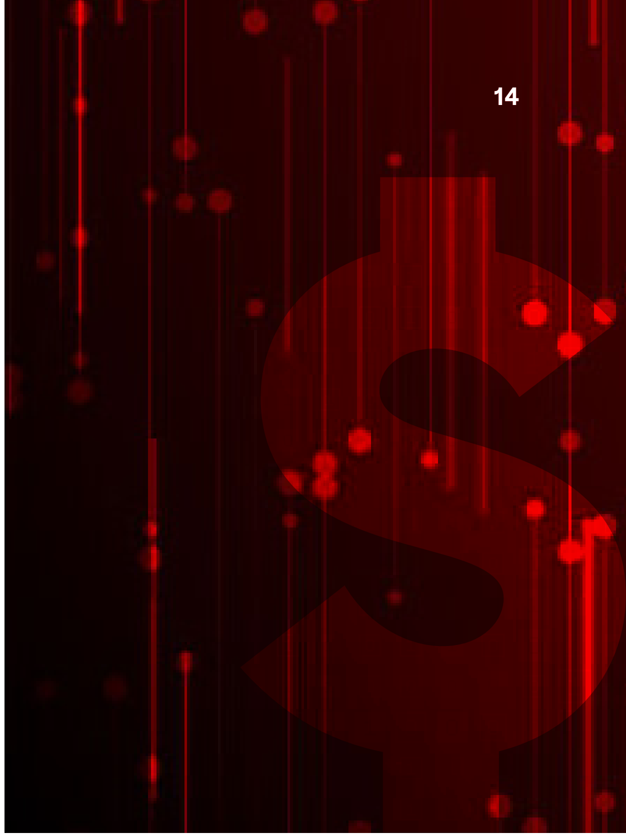
Consequences experienced by those who paid the ransom



93% Know or suspect that data was exfiltrated

83% Experienced another attack from the same or different threat actor

45% Were unable to recover all of their data



The True Cost of Ransomware

The financial impact of ransomware extends far beyond immediate downtime costs. Organizations reported an average downtime cost of $1.7 million USD per incident, but additional impacts create lasting damage:

- **Reputational damage** affected 34% of victim organizations, undermining customer and partner trust
- **Legal and regulatory penalties** impacted 24% of organizations
- **Publicly released or stolen data** affected 24% of victims, creating ongoing competitive and compliance risks

Cost variations by sector reflect different operational dependencies and regulatory environments. Public sector organizations faced the highest average downtime costs at $2.5 million USD, while healthcare organizations averaged $1.5 million USD and financial services organizations averaged $1.3 million USD.

$1.7M

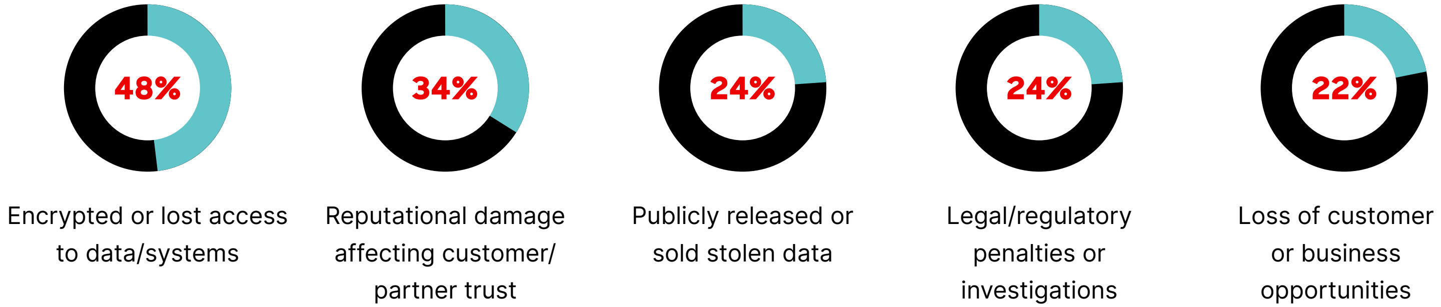
Average cost of downtime from most recent ransomware incident

Public sector: $2.5M

Healthcare: $1.5M

Financial services: $1.3M

Additional costs/impacts experienced (beyond downtime)



These costs compound over time. Reputational damage can affect customer acquisition and retention for years. Stolen data creates ongoing blackmail opportunities for attackers and competitive intelligence for adversaries. Regulatory penalties may trigger increased oversight and compliance costs that persist long after initial recovery.

The Enterprising Adversary

By operating ransomware as an enterprise and turning cybercrime into a business, adversaries create new pressures that complicate payment decisions. Nearly half (48%) of organizations identified faster and more automated attack chains as the greatest threat from ransomware, reducing the time available for incident response and increasing pressure for rapid payment decisions.

The evolution of multi-extortion tactics increases payment complexity as attackers combine data encryption, data theft, distributed denial-of-service (DDoS) attacks, and supply chain threats into coordinated campaigns. Organizations face multiple simultaneous demands rather than simple encryption recovery, making payment negotiations more complex and outcomes less predictable.

Ransomware as a service (RaaS) has professionalized cybercrime. In the Asia Pacific and Japan (APJ) region, adversaries like OCULAR SPIDER, BITWISE SPIDER, BRAIN SPIDER, TRAVELING SPIDER, and PUNK SPIDER, alongside RaaS operators *FunkLocker* and *KillSec*, run ransomware extortion campaigns with assembly-line efficiency. *FunkLocker* acknowledged in an interview that they target "high-value organizations with weak defenses."[2] These are not faceless hackers but calculated business operators, with targeted organizations as entries in a revenue pipeline.

> ***"Budget cuts created gaps in our defenses. We saved money on security tools, but the ransom cost far more. Now we view cybersecurity as insurance: Pay a little now or a lot later."***
>
> **— Board member/C-level executive, Australian financial services firm**

[2] Foresiet: Inside FunkSec: An Exclusive Interview with a Ransomware Architect https://foresiet.com/blog/funksec-ransomware-architect-exclusive-interview/

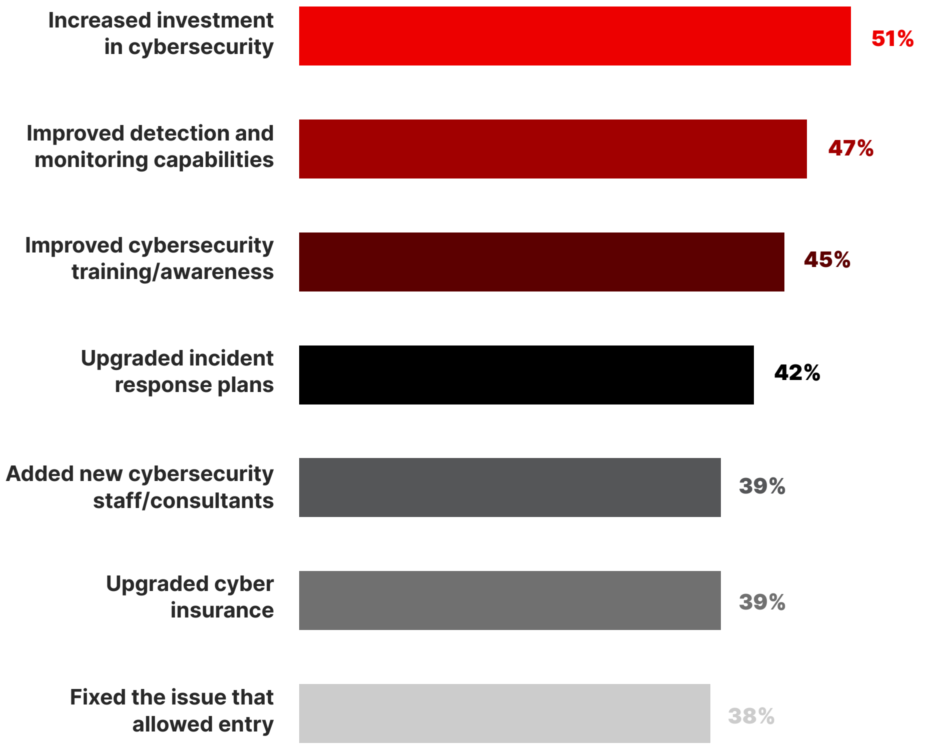
Post-Attack Improvements

Organizations typically react to ransomware attacks by improving processes or their security stack, but survey data suggests these responses often lack a strategic approach.

More than half (51%) of organizations increased general cybersecurity investment following attacks, and 47% improved detection and monitoring capabilities, suggesting previous blind spots in threat visibility. Nearly half (45%) enhanced training and awareness programs, acknowledging human factors in successful attacks.

However, only 38% addressed the specific issue they identified as enabling the attack, suggesting a preference for more general security posture improvements over targeted hardening. Leaving those root causes unresolved could help explain why 83% of organizations that pay ransoms were hit again. Generalized investments may create the impression of stronger defenses, but without closing the specific entry points used, organizations may remain vulnerable to repeat attacks.

Reasons for improved confidence since last attack



Building True Ransomware Readiness

Moving beyond the confidence illusion requires organizations to change how they approach ransomware preparedness. Success demands honest assessment of current capabilities, strategic investment in modern technologies, and recognition that well-trained humans remain essential in the fight against ransomware.

Testing Assumptions vs. Confidence

Organizations must challenge their preparedness assumptions through rigorous testing, readiness assessments, and tabletop exercises. Incident response simulations replicate real-world attack conditions, including system failures, communication disruptions, and decision-making under pressure. Red team exercises pressure-test defenses and can reveal blind spots in detection capabilities and response procedures that may not emerge during routine operations.

Measuring actual recovery times provides more accurate preparedness metrics than estimated capabilities. Organizations should track restoration timelines for different attack scenarios and identify bottlenecks that could extend downtime during real incidents.

Bridging leadership and operational perspectives requires shared metrics and regular communication about security realities. Executive dashboards should include meaningful security metrics that reflect actual threat trends and defensive capabilities rather than compliance checkboxes.

Comprehensive Defense: AI-Powered Endpoint Protection

Traditional security approaches cannot keep up with the speed and sophistication of modern ransomware attacks. AI-powered detection technologies have emerged as a critical countermeasure to quickly analyze behavioral patterns and identify threats that evade traditional tools and point products. These systems become more effective when integrated across endpoint, identity, and cloud to provide comprehensive visibility. Over 40% of organizations reported using AI or automation to support threat detection and alerting to respond to a ransomware incident.

Advanced endpoint protection with real-time threat hunting capabilities can proactively identify and contain threats before they spread. According to survey responses, organizations using legacy antivirus (AV) at the time of their last ransomware attack were more likely to have suffered significant impact compared to those without legacy AV. Conversely, organizations with endpoint detection and response (EDR), identity threat detection and response (ITDR), or threat intelligence were more likely to report minimal impact.

Updated Training and Culture Building

Security awareness programs must evolve to address AI-enhanced social engineering tactics. Traditional phishing training becomes insufficient when attackers use AI to craft contextually appropriate and personally targeted messages. Training should include recognition of deepfakes, voice cloning, and other emerging deception techniques.

Fostering a security culture extends beyond periodic training to create ongoing awareness and responsibility across employees. Organizations should encourage reporting of suspicious activities and maintain open communication channels between security teams and business units.

Empowering security teams with AI tools for threat analysis and response helps human analysts focus on complex decision-making while automating routine tasks. The goal is augmentation rather than replacement, enhancing human capabilities through technology.

> ***“We underestimated how quickly hackers could move. Our security investments failed to keep pace with growing threats.”***
>
> **— Board member/C-level executive, Australian financial services firm**

Conclusion

The ransomware landscape is evolving with unprecedented speed and sophistication. Adversaries now wield AI, operate with business-like efficiency, and target the most critical aspects of modern operations.

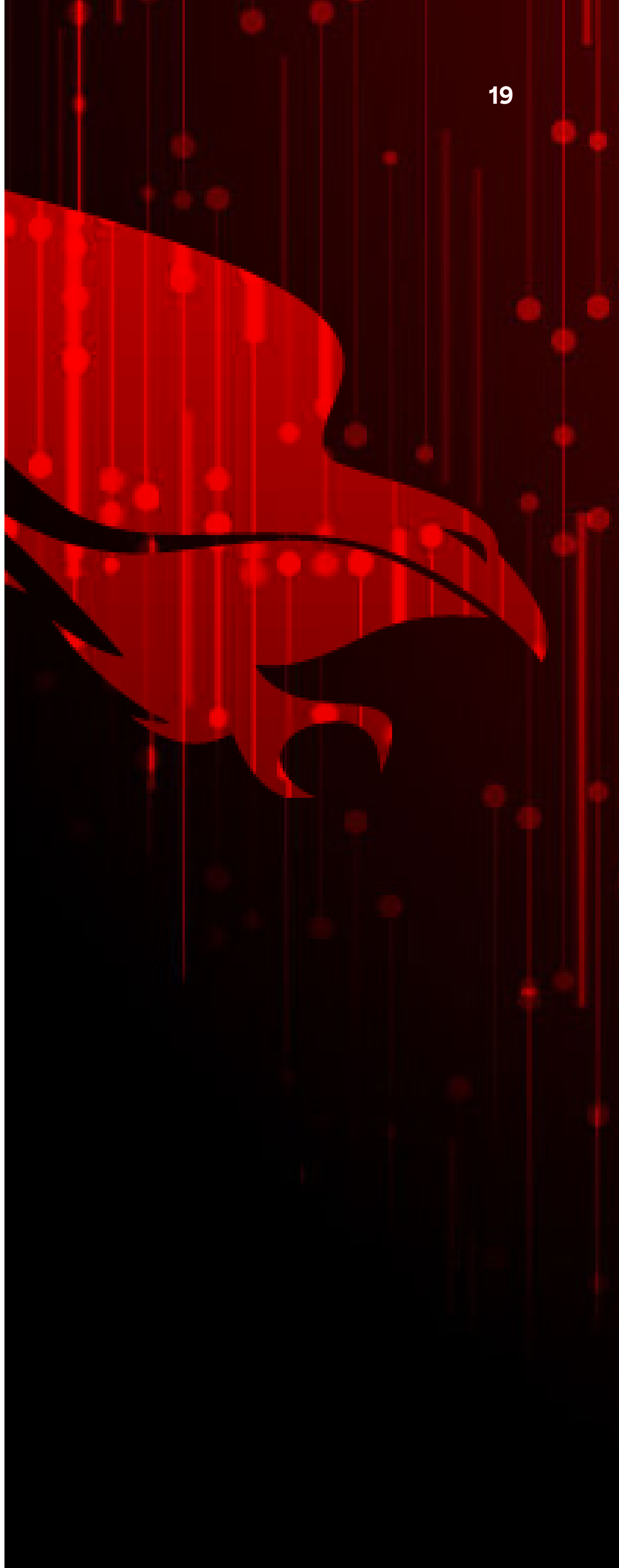
This survey exposes a dangerous confidence gap: Half of organizations believed they were very well prepared before their most recent attack, yet only 22% achieved rapid recovery. Overconfidence creates a false sense of security that inhibits critical investments in defense.

Additionally, the economics of ransomware have shifted — ransom payments offer no guarantees. Attackers are accelerating their use of AI, forcing defenders to match their speed with intelligence-led, automated defense.

But organizations do have options to improve their security posture. Achieving this requires:

- Testing assumptions
- Integrating AI-powered detection across endpoint, identity, and cloud
- Evolving employee training to counter AI-generated social engineering
- Embedding threat intelligence to stay ahead of evolving tradecraft
- Closing the leadership disconnect through shared metrics and honest communication between executives and security teams

Ransomware is a persistent threat. The future of stopping breaches will be decided by who holds the AI advantage, adversaries or defenders.



Appendix: Survey Methodology

CrowdStrike worked with Vanson Bourne to conduct this research between June 19, 2025, and July 17, 2025, surveying 1,100 senior IT and cybersecurity decision-makers across seven countries: the United States (600 respondents), the United Kingdom (100), Australia (100), France (75), Germany (75), India (75), and Singapore (75).

All respondents represent organizations with a minimum of 250 employees across both the public and private sectors, including healthcare, financial services, manufacturing, IT and telecommunications, and many other industries.

All respondents self-identified as either having a deep understanding of the cybersecurity systems, policies, tools, and strategies in place across their organization or as being familiar with key cybersecurity tools and policies, with a solid grasp of the overall ecosystem.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: www.crowdstrike.com/free-trial-guide