veeam Insights

PRIVAL.

From Risk to Resilience

2025 Ransomware Trends and Proactive Strategies

Executive Summary:

Assessing Ransomware Threats and Defenses in 2025

Ransomware attacks are evolving, growing faster and more sophisticated than ever. One thing is certain: **The pervasive threat of ransomware will continue to plague organizations throughout 2025 and beyond.** Whether these attacks come from established groups or the increasing number of "lone wolf" threat actors, failing to prepare thoroughly can cost an organization significant time and money, as well as trust among stakeholders.

To help address these persistent cyber threats, our Our 2025 Risk to Resilience Report shows several actionable steps organizations can take to mitigate risk and recover more quickly from an attack. **We surveyed 1,300 organizations globally** to gauge how Chief Information Security Officers (CISOs), security professionals, and IT leaders are recovering from cyber threats.

The field-tested strategies from companies that recovered faster from attacks reflect a set of best practices for cyber resilience that all organizations should consider implementing.

There is some good news. Compared to our 2024 survey,[1] **the percentage of companies impacted by at least one ransomware attack resulting in encryption or data exfiltration declined slightly from 75% to 69%.** This decrease likely stems from organizations continuing to improve their preparation and resilience practices, as well as increased collaboration between IT and security teams. Governments have also teamed up to take down major ransomware groups, leading threat actors to adapt and change broader attack dynamics.

Our analysis reveals **six key trends shaping the ransomware threat landscape in 2025** and the data-backed insights that can help companies enhance resilience. From cat-and-mouse tactics and the growth of exfiltration to a decline in ransom payments and increasing collaboration among stakeholders, we examine the persistent threat landscape and how successful organizations reduce ransomware risks and impacts.

1,300

organizations globally were surveyed by Veeam

6%

fewer companies impacted by at least one ransomware attack

Organizations must shift from reactive security to proactive **cyber resilience strategies** to meet the challenges of ransomware, leveraging preparedness, rapid response, and secure recovery measures to reduce risk.

Top 6 Ransomware Trends To Watch in 2025

1. Law Enforcement Forces Threat Actors To Adapt
2. Data Exfiltration Attacks Grow
3. Ransomware Payments Are Decreasing
4. Emerging Legal Consequences Of Ransom Payments
5. Collaboration Reinforces Resilience Against Ransomware
6. Budgets Rise For Security And Recovery, But More Is Needed

Law Enforcement Forces Threat Actors To Adapt

TREND# 1

2024 saw authorities launch several successful operations to take down prominent cyber threat groups. The elimination of these larger groups is obviously a positive development for threat defense. However, **the number of smaller groups and "lone wolf" threat actors propagating attacks has increased.** Some groups have also shifted their aim downstream, avoiding critical infrastructure to reduce scrutiny by law enforcement and targeting small and medium-sized enterprises (SMEs) that often have weaker cyber defenses.

Some of the larger groups that either been shut down, disappeared or ceased operation include:

- **LockBit**, a ransomware-as-a-service (RaaS) group, eliminated by law enforcement efforts led by the UK's National Crime Agency in conjunction with the FBI and Europol.[2]
- **BlackCat**, a RaaS group, that the FBI previously disrupted in 2023,[3] ended operations in March 2024 following their successful attack targeting Change Healthcare — and a ransom payout reportedly worth over 22 million U.S. dollars.[4]
- **Black Basta**, which appeared to stop operations in 2025 after leaked chat logs revealed concerns about law enforcement scrutiny after an attack on US Health System Acension, which included 140 hospitals across 19 states.[5]

Data Exfiltration Attacks Grow

TREND# 2

As the threat landscape evolves, threat actors continue to shift their tactics. Notably, while exfiltration tactics are typically used in conjunction with data encryption, the number of exfiltration-only victims that paid a ransom rose during Q4.[6]

Exfiltration reflects a "smash and grab" approach that is common in traditional ransomware attacks prior to encryption. It also occurs with poorly secured cloud-based applications and cloud infrastructure. Along with this shift toward data exfiltration — as well as toward double extortion that combines both encryption to restrict access and publication of sensitive exfiltrated data — **there has also been a reduction in dwell time, the time between compromise and launching the attack, with many attacks occurring in just a matter of hours.**

In Q2 of 2024, Coveware by Veeam noted that two of the top three ransomware adversaries in that quarter had an average dwell time of less than 24 hours.[7] That's a marked decrease compared to previous quarters, and the trend continued through Q4 as well.

When threat actors do gain access to victims' networks, they tend to use lateral movement techniques. They look for ease of exfiltration or a specific objective, such as compromising VMware ESXi hypervisors, to coerce victims into paying the ransom. These efficient and well-rehearsed strategies often result in faster attacks that can be difficult to detect and contain.

All too often, organizations that have a weak cybersecurity posture and complex network architectures are particularly vulnerable to data exfiltration and related cyber threats.

Ransomware Payments Are Decreasing

TREND# 3

Fortunately, the total value of ransomware payments decreased during 2024 compared to 2023.[8] More than one-third of organizations affected by a ransomware attack (36%) didn't pay a ransom, and 25% didn't pay but were able to recover their data anyway.

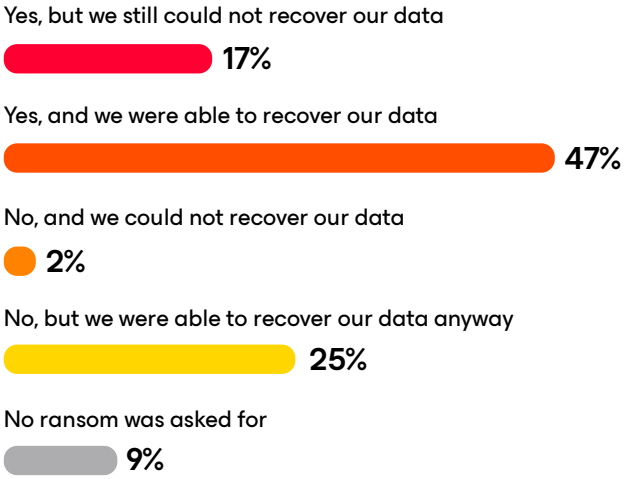
Among those that did pay, 82% paid less than the initial ransom and 60% paid less than half that sum. This data also aligns with what Coveware by Veeam saw first-hand during its work with impacted companies during 2024, when the **median payment decreased by 45% in Q4** to approximately $110k, an all-time low.

Only 25% of companies working with expert incident response from Coveware by Veeam paid a ransom, marking a "significant milestone in the fight against ransomware."[9]

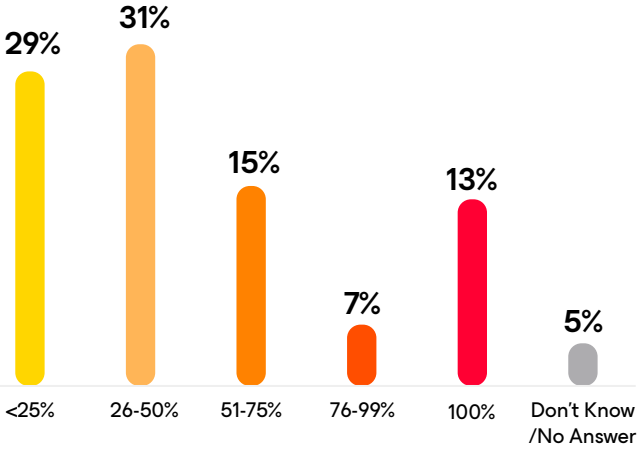
Compared to the companies that leveraged Coveware by Veeam's incident response services, other organizations were 156% more likely to pay a ransom. That suggests **working with experienced third parties for incident response correlates with fewer ransom payments, lower ransom payments, and more resilient practices overall.**

Victims are increasingly hesitant to pay ransoms because they can't trust attackers to release their data. Organizations have also proactively improved their own incident response plans, including through the use of immutable backups.

Did your organization pay a ransom to recover its data?



Percentage of ransom paid



Emerging Legal Consequences of Ransom Payments

TREND#4

Paying a ransom can prove very costly, as it incentivizes attackers and confirms that a vulnerable organization is willing to pay. In fact, **among those that paid a ransom, 69% were attacked more than once.** Organizations that don't take steps to bolster their capacity for defense and response leave themselves with fewer options when an attack does occur.

69%

of organizations that paid a ransom, were attacked more than once

Evolving regulatory and reporting initiatives, as well as coordinated enforcement by authorities across jurisdictions, have also contributed to the decline in ransom payments. Notably, the International Counter Ransomware Initiative (CRI), launched by the U.S. government in 2021, and its affiliated task force bring together 68 countries with the aim of disrupting the ransomware ecosystem and developing common policy approaches.[10]

In 2023, 40 CRI members signed a joint governmental pledge to "strongly discourage anyone from paying a ransomware demand."[11] Some countries have also proposed legislation barring public sector organizations from paying ransoms — such as the UK in January 2025[12] — and two U.S. states (Florida and North Carolina) have passed such laws.[13]

The FBI discourages organizations from paying ransoms,[14] and the U.S. Treasury Department advises there may be sanctions risks associated with payments made to entities blocked by the Office of Foreign Asset Control (OFAC).[15] Global organizations must consider other payment risks and compliance requirements as well.

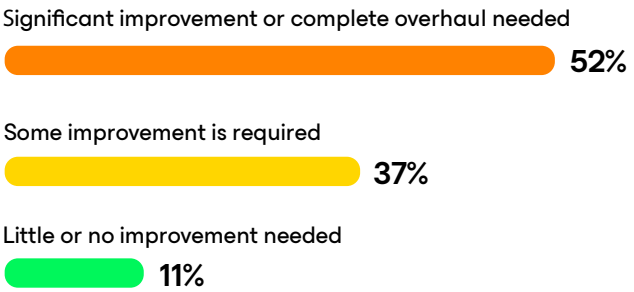
Collaboration Reinforces Resilience Against Ransomware

TREND# 5

Enhancing collaboration and communication between IT operations and security teams also helped organizations increase their cyber resilience. However, the majority of respondents (52%) said significant improvement or a complete overhaul is required to align those teams. And just 11% said little improvement or no improvement is required.

At the same time, platform and technology players are partnering to aggregate ransomware intelligence, and to provide services to help organizations boost defenses. Reporting ransomware and other cyberattacks to law enforcement and regulatory authorities, as well as to those emerging partner networks and industry information sharing exchanges, strengthens collective defenses.

Alignment of IT Operations & Security Teams



> "We are in a shared purpose of security, and we have to do that together. So, I don't think there's any way that we get to a future that is cyber secure without both the public and private entities, and their value propositions, coming together to find some solutions."[16]

Sue Gordon

former Principal Deputy Director of U.S. National Intelligence

Watch the full interview with Sue Gordon Veeam CISO Gil Vega here

Budgets Rise for Security and Recovery, but More Is Needed

TREND# 6

Critically, it enables vendors and agencies to provide indicators of compromise and mitigation strategies to others in the ecosystem.

While many ransomware defense techniques have shown signs of improvement, **some organizations aren't increasing security and recovery budgets fast enough** to keep pace with the growing threat landscape. Security teams are also spread thin due to the wide range of ransomware and other attack vectors they face.

Overall, organizations tend to devote slightly more resources to security (31% of IT budget on average) rather than recovery (28% on average), which suggests a potential vulnerability in building up proactive resilience. Chief Information Officers (CIOs) and CISOs should strike the appropriate balance based on their organization's needs when allocating budget for each area. The survey results indicate that **underinvestment in either security or recovery can weaken organizations' capacities to guard against and respond to ransomware attacks.** The lack of focus on recovery in particular can cost precious time and resources, particularly when threat actors target backup repositories.

On the plus side, **94% of organizations increased the recovery budget for 2025 and 95% increased it for prevention,** indicating a growing priority to boost cyber resilience.

94%

of organizations increased the recovery budget for 2025

95%

of organizations increased the recovery budget for prevention

Questions Your Board of Directors Will Ask After a Ransomware Attack

How did the attack occur?

Detail the attack's cause, scope, and impact.

What has been done to eliminate the threat?

Describe whether a ransom was paid (if so, how) and the steps taken to remove the threat and recover.

Which systems, data, and business operations were affected?

Outline the impacts of the attack, including any financial and reputational consequences.

What has been done to improve cyber resilience and prevent future attacks?

Identify steps taken to strengthen security and recovery, such as changes in governance measures or cybersecurity investment priorities.

Key Success Factors:

What Organizations With Better Outcomes Have in Common

When suddenly facing a ransomware attack, organizations need to act immediately and with coordination. Time is of the essence, so it's critical to assess the scope of the breach, contain the threat, and launch your incident response within a matter of minutes.

Analyzing the common attributes of organizations with more successful and less successful outcomes from a ransomware attack can provide insights to boost your cyber defenses.

That wide gap in success raises the question:

Why did so many organizations struggle to address such a widespread cyber threat?

Examining the survey results, several areas of deficiency correlate with lower ransomware resilience. What's more, by looking at which lessons organizations said they learned in the past year after being attacked, several patterns come into focus that can be applied for better ransomware defense and recovery.

An organization was considered more successful if five of the nine of the following criteria were met.

- A ransom wasn't paid by the organization, and they were able to recover their data.
- The organization wasn't attacked multiple times.
- The organization didn't experience significant impacts.
- The organization didn't have production data encrypted.
- The organization was rated as prepared or completely prepared post-attack.
- The organization recovered functionality for more than 80% of its servers.
- More than 90% of the organization's affected data was recovered.
- Less than 20% of the organization's production platforms were affected.
- Less than 10% of the backup repositories were modified or deleted when the threat actor tried.

Ransomware Playbooks Boost Attack Preparation

Pre-attack confidence doesn't always match reality: **69% of ransomware victims said they thought they were prepared before being attacked, but that confidence dropped by more than 20% post-attack,** highlighting critical gaps in planning.

The gap in perception of preparedness vs. reality was also wider for certain roles. In particular, CIOs' preparedness rating declined 30% post-attack compared to a 15% decline for CISOs, indicating CISOs have a more accurate understanding of their organization's security posture.

Overall, it's critical to foster organizational alignment around cyber resilience, preparation measures, and incident response procedures. This should include trainings and exercises across all applicable groups to support a consistent, coordinated response during and after an attack.

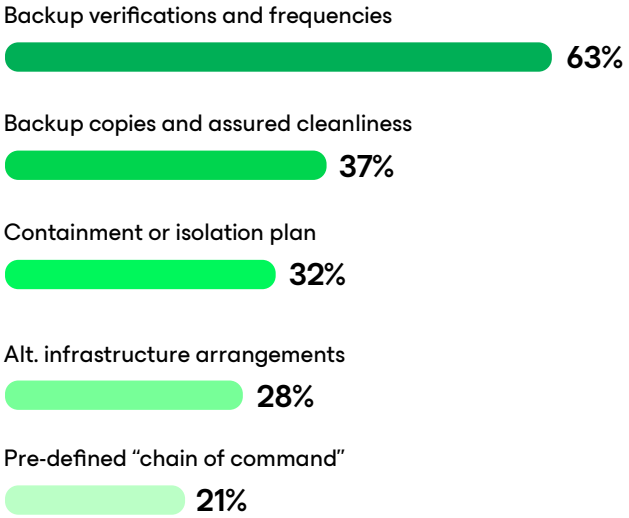
While 98% of respondents had a ransomware playbook, **less than half of organizations had key technical elements,** such as backup verifications and frequencies (44%), backup copies and assured cleanliness (44%), alternative infrastructure arrangements (37%), containment or isolation plans (32%), and a pre-defined "chain of command" (30%).

Organizations with **more successful outcomes had a much higher instance of including those five key technical elements in their playbooks.**

were confident in their preparations before a ransomware attack

drop in confidence in their organization's preparations after an attack

Key playbook elements for more successful organizations



Proactive Backup Recovery Builds Resilience

Secure backup recovery is critical, but it's more challenging than many anticipate. In fact, **89% of organizations had their backup repositories targeted by the threat actor.**

Worse still, they had an average of 34% of backup repositories modified or deleted. Less than 10% managed to recover more than 90% of their servers within expectations, and just 51% recovered the majority of their servers.

Planning for recovery is critical and involves multiple stages. Security and IT teams must contain or remove the cyber threat, then remediate access with tools such as identity and access management and other cybersecurity solutions, before finally restoring data to a secure environment.

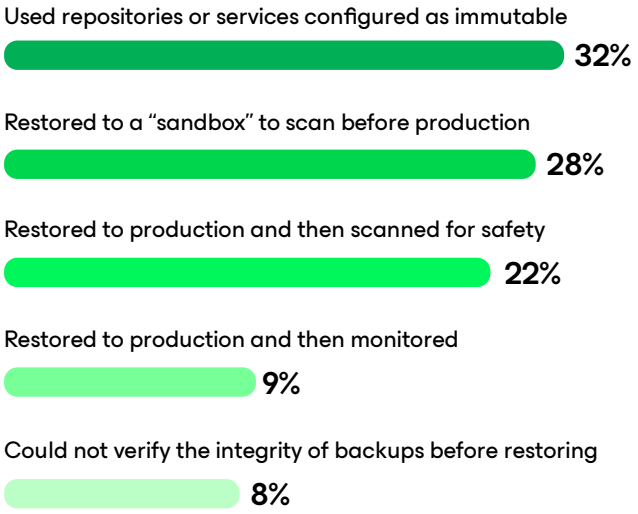
Secure backups were also underutilized as a proactive measure. **Only 32% of respondents used repositories or services configured as immutable,** while just 28% restored data to a "sandbox" environment and scanned for integrity. **A whopping 39% of respondents had to restore data directly to the production environment, and 8% couldn't verify backup integrity before restoring.**

Business and IT leaders need to ensure that data and backups are scanned and free of malware before restoring to production to help mitigate enterprise risk. Otherwise, they may face a range of serious consequences, including: rapid reinfection, lateral movement, persistence mechanisms, delayed detonation, sustained business interruption, compliance violations and more.

89%

of organizations had their backup repositories targeted by the threat actor

Backup Integrity Verification Method



The Power of "People" in Ransomware Resilience

While these technical aspects of recovery are vital, too many organizations neglect the crucial "people" elements in their ransomware playbooks.

Just 26% of organizations had a ransom payment decision process in place to guide a rapid response to payment demands based on potential impact. Many also lack procedures for informing law enforcement, which could aid in recovery and compliance.

26%

of organizations had a ransom payment decision process

Over a third of organizations used internal team members to communicate with threat actors. The rest relied on third parties to assist them, including incident response specialists and ransom negotiation specialists. These specialists are indispensable for guiding engagement based on a detailed understanding of threat actor behavior, which helps support more successful outcomes. Having internal team members communicate with threat actors can also inadvertently expose an organization to additional risks and threats.

Finally, just 30% of organizations had a pre-defined chain of command for dealing with attacks. The chain of command helps ensure proper authorization ladders and approvals for critical decisions during incident response, up to and including engaging with threat actors or paying a ransom.

No matter the day or time, it's always a bad time to experience a ransomware attack, which is why it's so important to have a roadmap for responding to such stressful and time-sensitive threats.

Bringing It All Together

When viewed together, these measures point to a core difference in mindset between organizations that demonstrated resilience against ransomware attacks in the past year and those that didn't:

Successful organizations make cyber resilience part of their daily discipline. They embed proactive strategies across their daily IT operations.

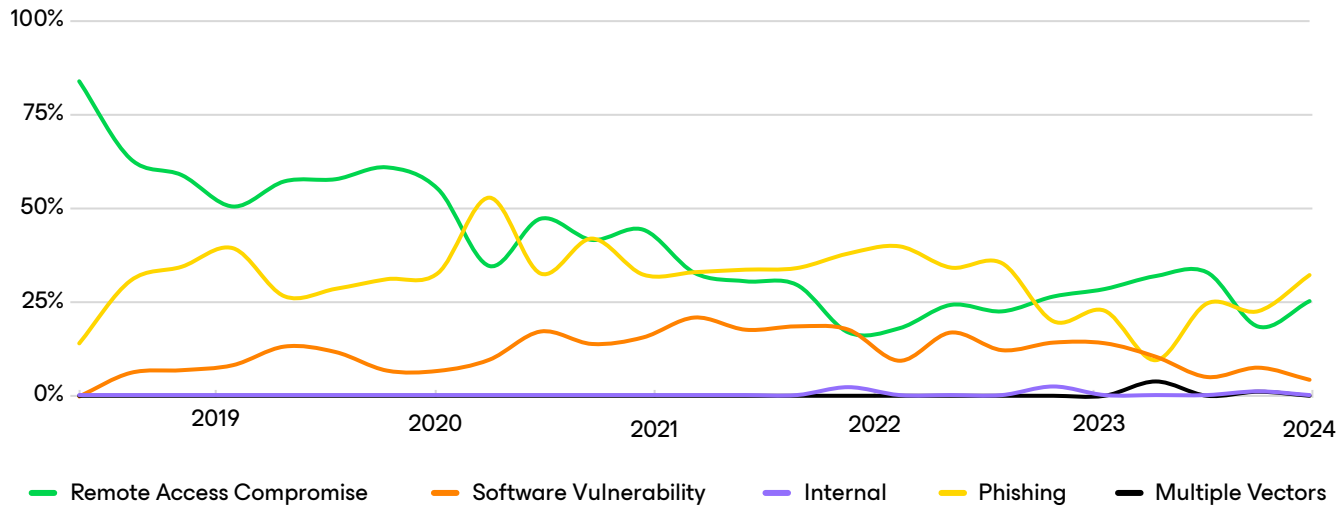
Post-attack, more successful organizations were also more likely to bolster employee training and awareness programs, which can help mitigate social engineering attacks like phishing. Software update policies are also commonly strengthened post-attack to guard against exploitation of software vulnerabilities on an ongoing basis. In particular, **many companies implemented newer backup and recovery solutions and transitioned to cloud or managed services post-attack.** Using these measures helps guard against common attack vectors and enhances resilience.

Successful organizations implemented more proactive recovery elements post-attack than less successful organizations.

These proactive defense practices also help address the most common initial access vectors that Coveware by Veeam saw in its work during Q4, including remote access compromise, phishing, software vulnerabilities, and more.

Strong defense against ransomware attacks cannot simply be conjured up when an attack occurs. They must be a fundamental part of an organization's daily operations.

Ransomware Attack Vectors



Source: Coveware by Veeam, "Will Law Enforcement Success Against Ransomware Continue in 2025?"

Taking Stock and Taking Action

Ransomware attacks can damage an organization's reputation and erode trust among its customers and end users. There can also be severe financial impacts from the costs of dealing with an attack, including operational downtime, lost productivity, and potential fines or lawsuits.

When an attack does take place, organizations should focus on teamwork, collaboration, and communication, remaining calm and composed while implementing the response strategies from their ransomware attack playbook. In the aftermath of an attack, organizations need to take stock, address the root causes of why it happened, and take steps to build resilience so they prevent it from happening again.

Organizations that had more successful recoveries followed these best practices:

- Develop robust incident response plans with clear roles and responsibilities.
- Create a backup and recovery strategy. Follow the 3-2-1-1-0 data resilience rule to configure repositories as immutable or otherwise protected and ensure backups are free from malware prior to restoration.[17]
- Implement proactive security measures and processes, such as zero-trust architecture, identity and access management, software update policies, newer detection and response solutions, and cloud or managed services.
- Increase spending on threat detection tools for prevention and backup solutions for recovery. Platforms for data resilience that are integrated with security tools and have features to prevent or detect threats — such as the Veeam Data Platform[18] — significantly help enhance cybersecurity and resilience.
- Organize security training programs and raise awareness amongst all employees.

About the Report

This year's ransomware report surveyed 1,300 organizations, 900 of which had experienced at least one ransomware attack resulting in encryption or exfiltration in the past 12 months. The respondents were comprised of Chief Information Security Officers (CISOs) or executives with similar responsibilities, as well as security professionals and IT leaders from across the Americas, Europe, and Australia.

Visit our homepage to learn more about security solutions that can enhance your cybersecurity posture to help accelerate recovery or to speak with one of our Veeam experts.

Cyber defense strategies are a board-level issue. Don't wait for a cyberattack to happen. Take the steps needed to minimize risk and maintain resilience.

Endnotes

1 https://go.veeam.com/ransomware-trends-executive-summary-2024-us

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

4 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

5 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

6 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

7 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

8 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

9 https://www.coveware.com/blog/2025/1/31/q4-report

10 https://counter-ransomware.org/aboutus

11 https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

12 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

13 https://www.databreachtoday.com/blogs/as-states-ban-ransom-payments-what-could-possibly-go-wrong-p-3273

14 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

15 https://ofac.treasury.gov/media/912981/download?inline

16 https://www.youtube.com/watch?v=Fs2xq0pb7YQ

17 https://www.veeam.com/blog/321-backup-rule.html

18 https://www.veeam.com/products/veeam-data-platform.html

veeam Insights