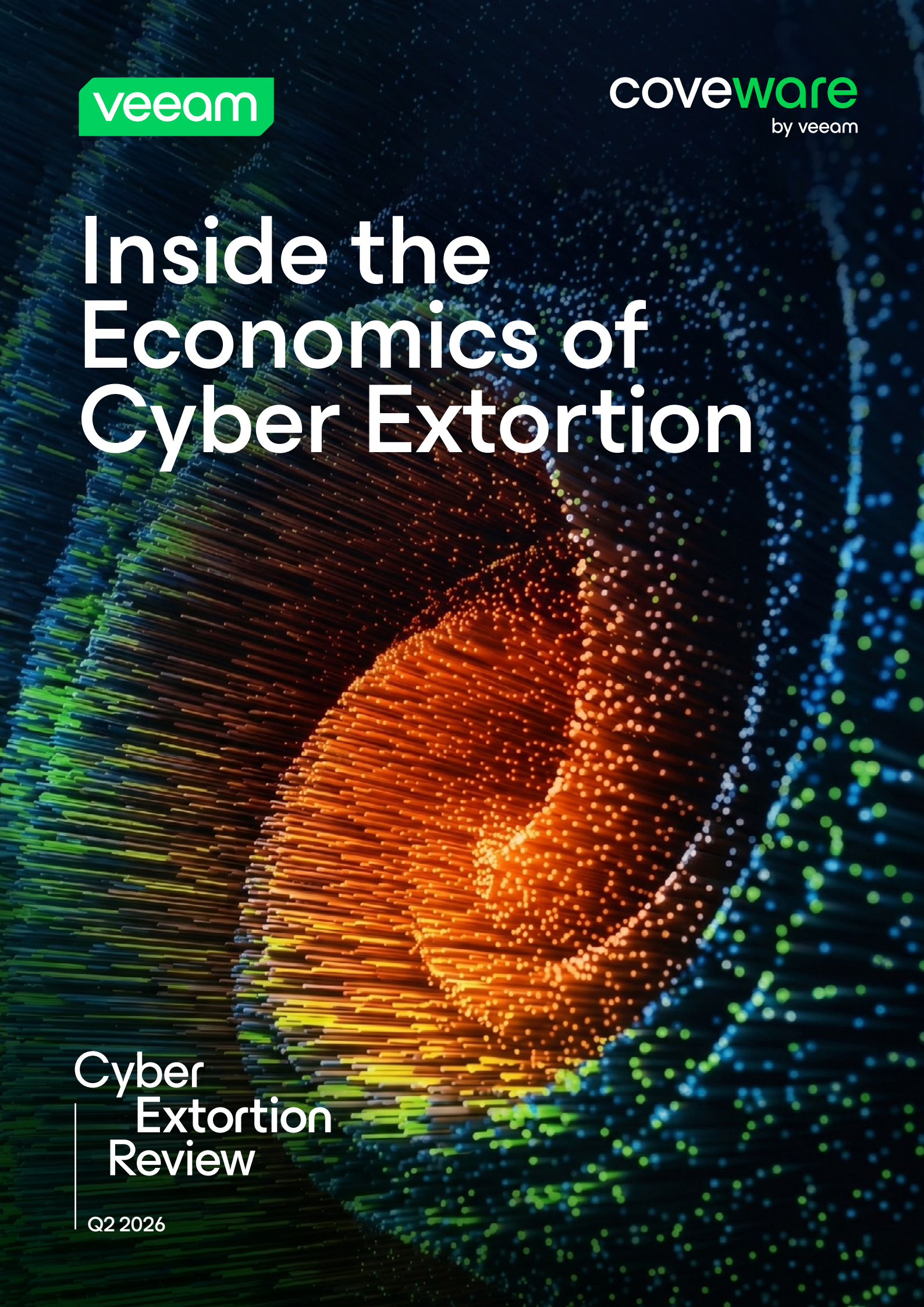
veeam

coveware by veeam

Inside the Economics of Cyber Extortion



Cyber Extortion Review

Q2 2026

Cyber extortion is a fast-changing threat, and key attack vectors have changed substantially in just six months. Businesses should reconsider whether annual planning is still enough.

Foreword

Does your cyber extortion planning reflect the realities of today's threats?

This question is particularly vital given the rapid changes to the threat landscape over the last six months.

This quarter's data shows a sharp rise in the use of phishing/social engineering as attack vectors, making them the most common route into victims' systems. At the same time, compromised credentials have continued to rise as a standalone vector, while third-party and supply-chain access remain a lower-volume but increasingly complex threat.

Cyber extortion is a business. And like all businesses, it adapts quickly when new opportunities open and old ones close.

That makes annual planning too slow for the threat model. Ray Umerley, CISO of Coveware by Veeam, argues that companies do not need to rewrite their entire plan every quarter. However, they should revisit their ransomware and extortion strategy at least quarterly at the executive level, and immediately after major changes such as a vendor incident, a material SaaS change, a new third-party dependency, or a meaningful shift in attacker behavior.

There is another reason to keep those plans under review: new evidence continues to emerge about how criminal enterprises actually operate, and it undermines many common assumptions.

Businesses that hope to move on from their attack by paying their attacker to delete stolen data may be paying for little more than an empty promise. We consider the issue of "load-bearing assumptions" later in this report—particularly the assumptions that may shape the boardroom response after a breach. Errors here can be particularly costly.

Coveware by Veeam's data reflects observed casework, not a representative market sample.

"If we were hit today, would our plan still match how these incidents are actually happening?"

Ray Umerley

CISO, Coveware by Veeam

REFLECTION

A Quarter in Review: Q2 Data at a Glance

The average ransom payment rose 176% to $1.9 million in Q2, in part because of some very high payments involving data exfiltration (data removal) rather than the encryption that was more common at the start of the year. Although mid-market companies (11 to 10,000 employees) represented 75% of cases, larger companies made up 19% of cases, up from 14%, pushing up median victim size.

Average ransom payment in Q2 was

$1.9M

up

176%

Median victim size was

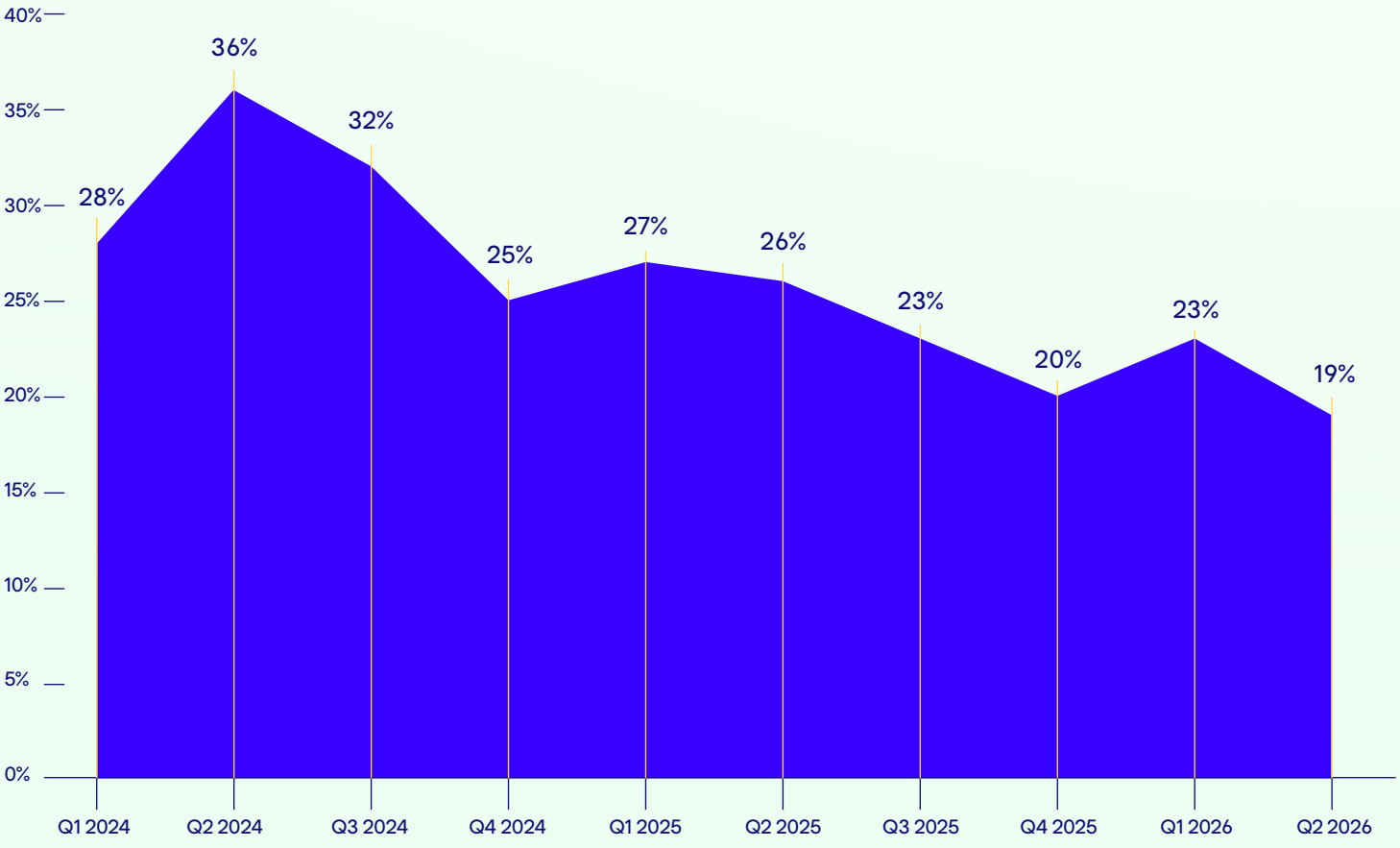
750

employees, a rise of

50%

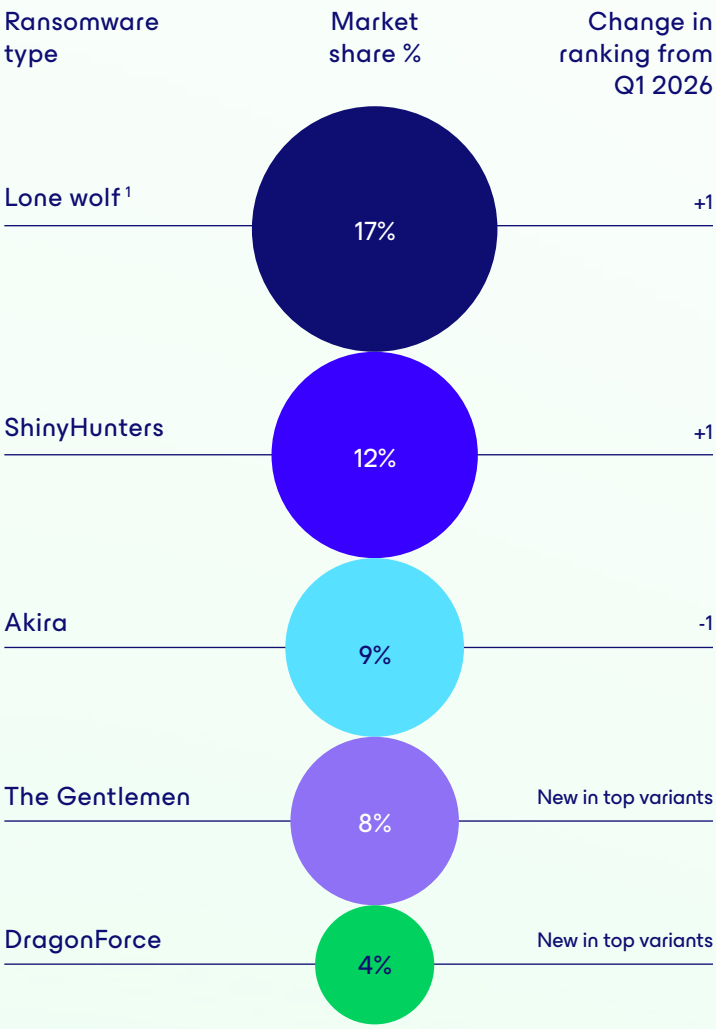
All ransomware payment rates, Q1 2024–Q2 2026

Payment rate is at a record low



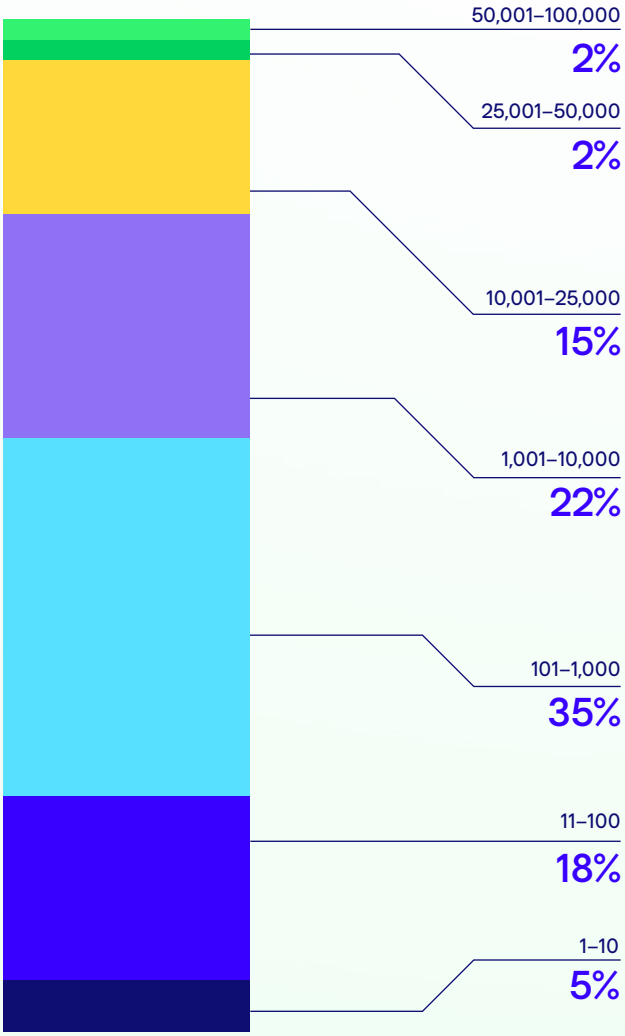
Most common ransomware variants, Q2 2026

Lone wolf operators enjoy increased success



Ransomware-impacted companies by employee size, Q2 2026

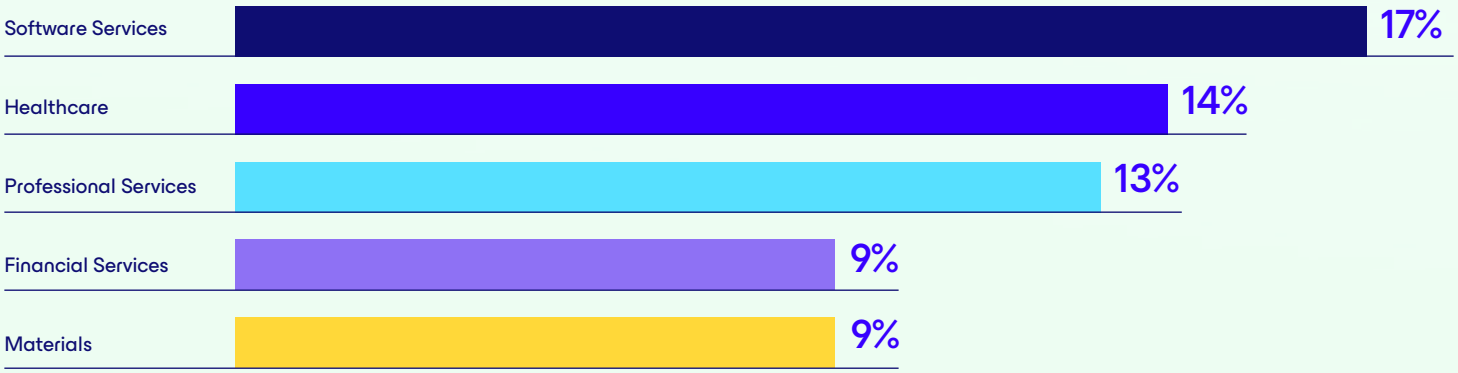
Mid-market companies account for 75% of cases



1. Lone wolf category aggregates one-person/small group attacks

Industries impacted by ransomware, Q2 2026

The Software Services sector was in the crosshairs in Q2, while Healthcare and Professional Services are still under pressure



Ransomware attackers are returning to decades-old tactics that exploit human, not technical, weaknesses. Businesses need to react.

ARTICLE ONE

The New Golden Age of Social Engineering and Phishing

For years, businesses have reinforced their front door. They may have failed to secure the side entrance—and ransomware attackers have noticed.

Until recently, data from Coveware by Veeam showed that the most successful attack vector was remote access—exploiting weaknesses in VPN gateways, RDP (remote desktop protocol), and other tools that have proliferated as employees have grown more mobile.

However, this quarter's data shows that remote access has declined from its late-2025 peak. It has been overtaken by phishing/social engineering, a vector that dominated ransomware's first boom in the early-to-mid 2010s.

Part of the shift traces to Silent Ransom Group (SRG), also known as Luna Moth. SRG has targeted high-profile law firms—a premium target given the damage from exposing client data—as well as sectors such as healthcare.

SRG and others have augmented their attack vectors, traditionally phishing emails, to include voice phishing ("vishing") calls, where they pose as IT support to manipulate helpdesk employees into handing over credentials or remote access. In bolder operations, attackers impersonating IT staff have walked into law offices and gained hands-on workstation access. Once inside the perimeter, they use ordinary tools such as WinSCP—which mimics routine admin activity and rarely triggers alerts—to send client data to a flash drive or external location.

AI compounds the threat. The technology has already been used to convincingly clone a senior executive's voice, enabling a fraudulent transfer.

Attackers are also targeting the human layer from a different angle entirely. In 2025, a member of the Medusa ransomware gang approached an employee of UK broadcaster the BBC, offering him a 15% cut—later raised to 25%—of a ransom payment in exchange for network access through the employee's work computer.

Also significant is the move from encryption—demanding a ransom to unscramble data—to exfiltration, where data is transferred out. Exfiltration accelerates an attack's pace, putting immense pressure on the victim: attackers may go first to clients with a sample of stolen data, pressuring them to push the victim into payment.

> **"Stop treating trusted access workflows as administrative plumbing. They are security controls now."**
>
> Ray Umerley
>
> CISO, Coveware by Veeam

This featured in 76% of cases Coveware by Veeam saw in the quarter. Fewer cases reached the point of encryption, service disruption or recovery impairment.

The immediate lesson is to update plans to match today's threat landscape. Human processes need to be hardened against phishing and social engineering. As Bill Siegel, CEO of Coveware by Veeam, has said: "Organizations must prioritize employee awareness, harden identity controls, and treat data exfiltration as an urgent risk, not an afterthought."

Phishing/ social engineering

was the leading initial access vector in Q2 2026

But the bigger picture is more challenging. Cyber extortion is a business—and an agile one. Businesses need regular and ad hoc reviews updating defenses and worst-case response plans. This is a higher-level governance decision that typically sits above IT and tech teams, linking back to business-level decisions about acceptable risk. Reinforcing the front door is vital, but senior executives must build a plan that ensures every entrance is firmly shut.

Umerley's first move for any business: harden the processes that create or restore access. "Attackers are increasingly trying to look like legitimate users, admins, vendors, or support personnel, rather than relying only on noisy technical exploits," he says. That puts help desk verification, password resets, MFA resets, device enrollment, account recovery, OAuth approvals, service accounts, vendor access, and remote administration tools in scope as security controls, deserving the same rigor as any perimeter defense.

Hardening these trusted workflows is where technical and human countermeasures meet. If an attacker can socially engineer a user, the help desk, or a vendor session, stronger perimeter controls alone are not enough. "The risk has moved into the trust layer," says Umerley.

What This Means for Defenders: Five Key Questions for CEOs/Boards

If an attacker calls our help desk impersonating an executive, what stops them?
Ransomware attackers often exploit perceived seniority to create pressure. Don't assume MFA and other protocols will hold firm during a call from a time-poor executive who seems locked out of their email. Businesses should test existing protocols to find weaknesses. Senior executives may have to follow stricter verification processes, but in doing so will gain resilience.

If a threat actor accesses our office and physically plugs in, would we notice?
Could a lanyard bypass years of expensive systems hardening? Physical and digital infrastructure need to be planned as a single attack surface. Reception, facilities, and floor staff are now security controls.

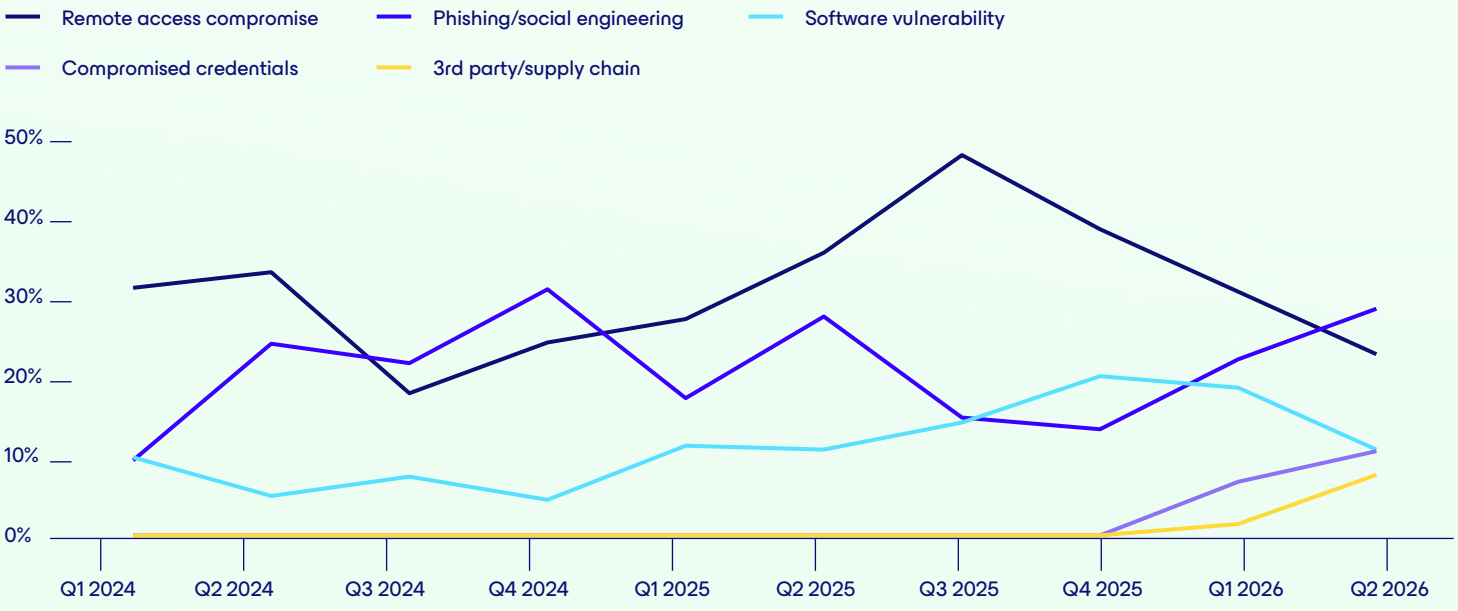
If one of our partners suffers a breach, could it become our problem?
IT providers and suppliers are your super-extended attack surface. Businesses should ensure they have mapped this risk landscape fully. Have you planned for their failure?

Who holds credentials that would be catastrophic in the wrong hands, and what would we lose if they failed?
The issue here is leverage. Are there a small number of credentials with extended access that, accessed via social engineering, could cause disproportionate damage? If one set of credentials creates such a risk, the solution is not training, but architecture.

How does our incident response plan change if customers/suppliers are contacted first?
This tactic by ransomware attackers gives zero time for strategic planning—which is why they do it. Does everyone know their role if this happens? Have you thought through how disclosure requirements change if your response window, normally measured in hours, is telescoped down to minutes?

Attack vector distribution, Q2 2026

Phishing and social engineering overtake remote access in Q2



ARTICLE TWO

The Lie About Deleted Data

Ransomware attackers are shifting tactics from data encryption to data theft. This creates new opportunities to deceive victims.

76%

of cases in Q2 involved data exfiltration

Just

15%

of data exfiltration-only victims paid a ransom in Q2, a record low

The attack on market intelligence platform Klue in June 2026 underlined an important message: companies that pay a ransom after being attacked may not get what they pay for. Indeed, they may get nothing at all.

Klue's data was breached after attackers compromised an integration credential and harvested OAuth tokens from its Salesforce environment. The attackers stole CRM data Klue was managing on behalf of customers, most notably commercially sensitive information such as pricing quotes and sales notes. A group named Icarus claimed responsibility. Although the intermediate steps are unclear, on June 24 Klue told customers it was in communication with Icarus, which had said it was taking steps to delete the stolen data. When companies pay a ransom, this is the outcome they hope to purchase.

But reports soon emerged that Icarus, a relative newcomer to the ransomware ecosystem, had itself been compromised. Another group posted data online that appeared to come from Klue customers with the message: "Pay the ransom or we will leak everything if you no pay us."

As with many ransomware cases, the full narrative is uncertain. However, the take-home message is very clear: ransomware groups are criminal enterprises. Nothing they say can be trusted.

For example, when the UK's National Crime Agency, working with the FBI and international partners, raided LockBit in Operation Cronos in February 2024, it discovered that data that had been "deleted" following ransom payments was not, in fact, deleted at all.

The issue has become even more important as the tactics of ransomware attackers have pivoted. Previously, many groups encrypted their victims' data in place, offering to send decryption keys if payment was made. But this is a processor-intensive process that can trigger alerts. Even if data is scrambled, companies with a backup program can simply restore.

> **"Be very careful with the word 'delete.' In most extortion cases, deletion cannot be independently proven."**
>
> Ray Umerley
>
> CISO, Coveware by Veeam

In contrast, exfiltration can use ordinary file transfer tools that blend in with normal network traffic. Backups are irrelevant. It is no surprise that Coveware by Veeam saw exfiltration in 76% of cases in Q2. Of course, cases can involve both encryption and exfiltration.

Critically, this means the promises made by attackers are becoming increasingly non-verifiable. A victim of data encryption who pays a ransom receives crypto keys which can be verified immediately. However, a victim of data exfiltration who pays a ransom may only receive a chat message with a promise.

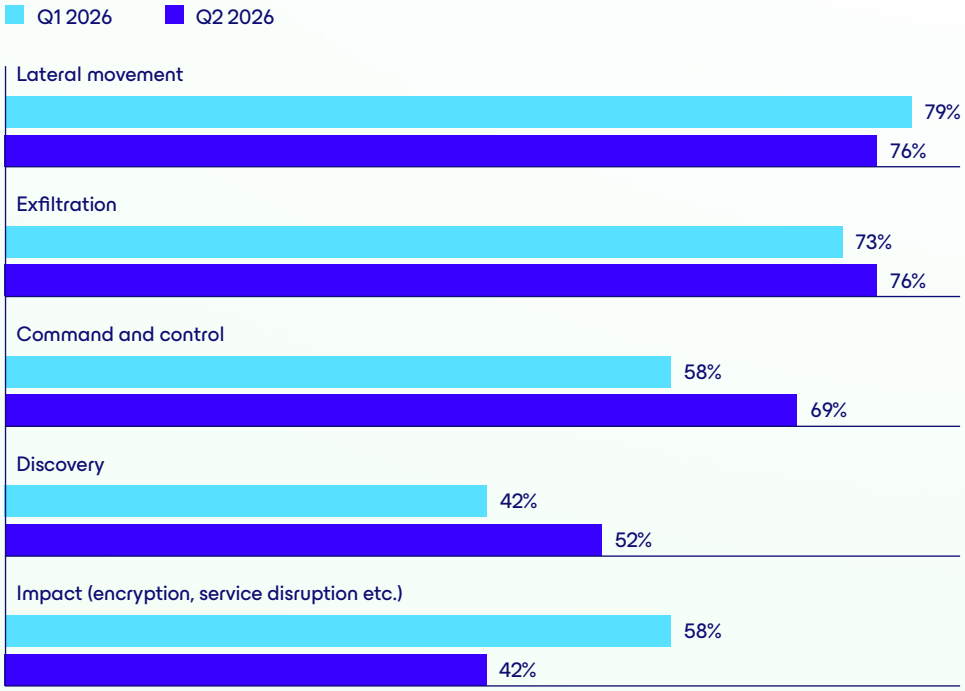
Umerley tells clients to "be very careful with the word 'delete.'" The victim does not control the attacker's infrastructure or how they use the data. Instead, he pushes boards to ask: "Does payment meaningfully change the probability, timing, or severity of future harm, knowing deletion cannot be independently verified?"

In the first days of an extortion event, the attacker is trying to shape the narrative, forensics are incomplete, and executives are under pressure to decide fast. That is when assumptions start sounding like facts. Umerley recommends focusing on four key questions: What have we verified? What is the attacker claiming? What are we assuming for now? What would change our decision?

Ultimately, the goal is defensible decision-making under conditions of uncertainty.

Observed tactics as a percentage of cases

Lateral movement and exfiltration are the most common ransomware tactics



What This Means for Defenders - Payout Rates Hit a Record Low

The five-year trend is clear: companies are increasingly standing firm and refusing to pay up.

In Q2, the payout rate of the cases handled by Coveware by Veeam was 19%, the lowest on record. For those whose data was only exfiltrated, without any encryption, the rate was still lower, at 15%. Victims of cyber extortion are becoming increasingly uncertain that their payment will deliver the outcome they want.

Yet average payments have surged 176% in the quarter to $1.9M. Silent Ransom Group's ongoing campaign against high-profile law firms was a key factor: by threatening public exposure of sensitive legal records exfiltrated through targeted social engineering, the group secured large payments that skewed the quarterly average dramatically upward.

The reduced rate at which companies give in to ransom demands shows increasing acceptance of our longstanding general advice: the base scenario should be non-payment.

Paying for that claim does not purchase safety. It purchases silence, for as long as the attacker chooses to keep it.

But non-payment only answers half the question. The other is whether the business can independently establish what data left its environment, rather than relying on the attacker's account.

This is the real argument for commanding data rather than simply controlling the systems it sits on. Control stops an attacker's access. Command is what lets a company answer, on its own authority, exactly what was touched, when, and in what form. The base scenario should be non-payment. Increasingly, it should also be independence: a company's own verified answer to "what did they take?", whether the attacker ever tells the truth.

With ransomware changing every month, decisions should be based on today's realities, not yesterday's averages.

ARTICLE THREE

Your Breach Is Not Average

The academic and author Nassim Nicholas Taleb warns against using averages for decision-making, saying: "Never cross a river if it is on average four feet deep." This principle has important implications for companies that have been victims of ransomware.

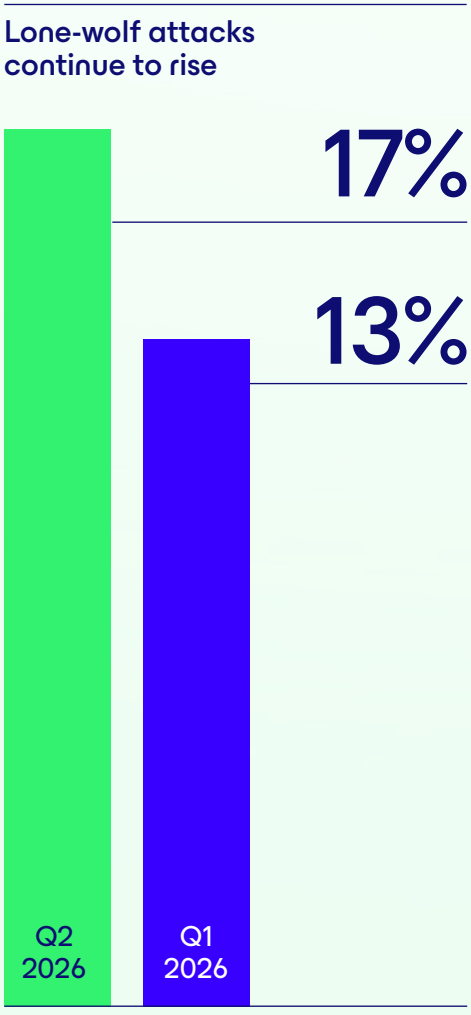
Our experience with clients shows that rare or low-probability outcomes occur far more often than decision-makers tend to expect, while "average" outcomes occur less often than their name implies. Ransomware is a business, but the groups that perpetrate it cannot be relied upon to act in a business-like way. Indeed, they sometimes do not even act in their own self-interest.

The LockBit case mentioned earlier is one example. Commercial logic would suggest that LockBit delete the data after a ransom is paid, as part of a strategy to maximize future income. It did not do so.

A more striking example was a small extortion case we handled in 2020. The group, which appeared to be based in China, was using Dharma ransomware, known to be fairly reliable in terms of the outcomes that could be forecasted and achieved. Dharma was sold to criminal groups as a ransomware franchise that promised a consistent, reliable product. Yet a week or two into the case, the threat actors completely disappeared from our conversations. Some weeks later, they re-emerged with the strange explanation that their entire team had fallen ill from a virus.

At the time, we thought that the group was lazy and sloppy. A few months later, as the COVID-19 pandemic enveloped the world, we rethought the incident. Our revised verdict was that the threat actors were likely among the first victims of the highly virulent disease, long before it was well known internationally. An analysis of average outcomes would have assigned this near-zero probability. Nevertheless, it became a reality.

Lone-wolf operators raise the stakes further: one-person and small-group attackers accounted for 17% of Q2 cases, up from 13% in Q1. They arrive with far less history than established groups, which usually leave a record: pricing, communication style, leak behavior, decryptor reliability, payment logistics, and so on.



“Success cannot always be measured at the moment the negotiation ends.”

Ray Umerley

CISO, Coveware by Veeam

“None of that makes them trustworthy, but it can give responders some basis for forecasting,” says Umerley.

A lone wolf may be improvising, overstating what they hold, misunderstanding the value of the data, or unable to deliver what they promise. Their motivations can run beyond money to clout or hacktivism. Umerley’s posture for these cases is slower and more evidence-driven: validate samples, test claims, avoid overreacting to deadlines, and make sure leadership understands there is less historical signal to rely on.

Even historical data can have multiple perspectives: although average payments in Q2 rose 176% due to a small number of big payouts, the median payment halved. What, then, is the yardstick?

Yes, historical outcome data is still relevant and important for developing a recovery strategy, but it is not the only data that matters. Law enforcement activity, economic conditions, sanctions, even global health crises and other “black swan” events can make any case distinctly non-average.

As ransomware has industrialized, established groups have developed more repeatable ways of operating—from pricing and negotiation to leak behavior and payment logistics. That gives responders more historical signals to work with. But repeatability is not certainty: past behavior should inform the decision, not determine it.

That distinction matters in the boardroom. Advisors will present scenarios and likely outcomes. Under-pressure executives want certainty and swift resolution. Yet executives should still ask tough questions and weigh multiple options. They should ask for worst-case scenarios, not likely ones, then build a resilient plan around the more pessimistic outcomes.

Any probability-based claim needs to be challenged, especially the reassuring ones. And executives must ask what makes their breach one-of-a-kind.

What This Means for Defenders - Five Assumptions That May Not Be True

Assumption	Can it be evidenced?
We know which attacker holds our data	Attribution is contested. Brand names can be borrowed. The original attacker may themselves have been compromised.
Only one attacker holds our data	The ransomware-as-a-service business model implies distribution of access with tech creators, operators, affiliates, and brokers. Anyone could have a copy on a flash drive.
Payment will end the risk	Testable only in hindsight, and only negatively. Payment may, however, reduce the risk of release in the short- or medium-term.
Deletion proof closes the case	It only proves one copy was deleted. Many others may exist.
Deletion will satisfy the regulator	Regulators have seen these deletion promises before. They know that they don’t hold.

Conclusion

Ransomware is a fast-evolving business. Six months ago, almost half the cases we recorded exploited remote access. Today, we see a pivot to phishing, vishing, and even instances of criminals walking into receptions with a lanyard and a cover story. By next quarter's report, it will have changed again. After all, even successfully blocked attacks don't guarantee that threat actors will lose interest in your data. They are just as likely, if not more so, to instead pursue a new way to get the information they are after.

And that is the point. Cyber extortion is agile, and those who want to combat it must show the same agility. An annual review will analyze a threat landscape that no longer exists by the time the review is complete. Boards should press beyond the plan itself: every load-bearing assumption within it needs to be backed up with evidence, not historical probabilities.

In the unfortunate circumstance that your company becomes a victim, the same clarity of thought is needed. Your incident is a sample of one, and your opponent has an incentive to be unpredictable. Coveware by Veeam's own casework has shown that the rare, implausible outcome arrives far more often than averages suggest. The organizations best prepared will be those that plan not only for the likely outcome, but for the unexpected one.

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk.

Veeam delivers deep contextual intelligence across every data asset, identity, and AI model. The company governs access for both humans and AI agents, automates privacy, compliance, and remediation processes, and protects and recovers organizations from modern threats – including ransomware, disasters, AI errors, and ensuring the restoration of clean, trusted data. Veeam empowers organizations to move beyond simply protecting data, enabling them to activate and unlock its full potential.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.