

resilience

WHITEPAPER

The Ransom Dilemma

Driving loss control in the age of extortion-only attacks

Jud Dressler
Director, Risk Operations Center

The Ransom Dilemma

Driving loss control in the age of extortion-only attacks

Introduction

Attackers no longer need to encrypt a single file to get paid. Across Resilience's claims portfolio, data theft without encryption accelerated from 49% of extortion claims in the first half of 2025 to 65% in the second half. By year end, only 13% of attacks relied on encryption alone, while data theft—either on its own or combined with encryption—accounted for 87%. Those numbers shift slightly in the first half of 2026 with just over half of attacks featuring data theft solely and 84% of attacks including encryption and data theft. The decisive shift from operational disruption to reputational leverage is no longer a forecast. It is the current operating environment.

To understand the change, it helps to recognize how extortion tactics have layered over time. Single extortion is the original model: attackers encrypt a victim's systems and demand payment for the decryption key. Double extortion added data theft to that equation, giving attackers a second source of leverage—pay to restore access, and pay again to keep the stolen data quiet. Triple extortion added a third pressure point, typically distributed denial-of-service attacks or direct harassment of the victim's employees, customers, or partners.

The newest model strips the equation back down. Attackers skip encryption entirely and rely on stolen data as the sole point of leverage. There is nothing to decrypt, nothing to restore, and no operational outage to remediate. The threat is exposure, and backup-centric defenses do nothing to stop it.

This shift fundamentally changes the calculus around payment. Paying a ransom for a decryption key is a transaction with a verifiable outcome: either the key works or it does not. Paying for data suppression is something else entirely—a payment for a promise from a criminal that a digital copy has been deleted, with no way to confirm the claim. As suppression payments have become the central financial objective of modern cybercrime, the decision to pay or refuse has moved from a technical question about recovery to a strategic question about risk, reputation, and legal exposure. This paper examines the factors that drive that decision, the real-world outcomes of each path, the trends shaping how negotiations unfold, and the role of experienced incident response partners throughout.

Three numbers worth remembering

84%

of Resilience portfolio extortion claims in H2 2025 and H1 2026 involved data theft, over half involved no encryption.

83%

of organizations that paid a ransom in 2025 were attacked again, often by the same threat actor

30–40%

of suppression payments fail to prevent the data from being leaked, sold, or shared anyway

To pay or not to pay

There is no single business case model for when to pay a ransom. It is a complex, high-stakes decision that requires a thorough risk assessment based on the victim's specific circumstances. While authorities such as the FBI advise against paying, some organizations feel they have no alternative.

The decision hinges on weighing the potential costs of payment against the costs of refusal. This is why organizations almost always rely on support from specialized negotiators, forensic investigators, and legal counsel to navigate the decision. And Resilience clients get the additional support of the Resilience Risk Operations Center sitting alongside them.

The case for paying

► Buying time

Paying is often less about trust and more about friction. It can stall the immediate public release of data, giving legal and communications teams more time to notify affected parties and prepare a response.

► Preventing reputational damage

If the exfiltrated data contains highly sensitive information—trade secrets, embarrassing internal communications, or other material that could be characterized as a 'smoking gun'—paying is a gamble to keep that information out of the public eye and out of the hands of competitors.

► Protecting third parties

If the data includes sensitive information about clients, patients, or employees (such as Social Security numbers or medical records), some organizations pay out of a sense of moral or legal obligation to minimize the risk of those individuals being exposed or suffering identity theft. However, as demonstrated by the 2024 PowerSchool breach, payment for this kind of promise can easily backfire, creating new extortion targets based on a dataset the victim has effectively confirmed as valuable.¹

► Cost-benefit analysis

In some cases, the ransom amount is significantly lower than the projected costs of lawsuits, regulatory fines (such as GDPR or CCPA violations), and the total loss of customer trust that would follow a public leak. From a legal standpoint, suppression payments are sometimes viewed as a preemptive defense posture: if a class-action lawsuit or regulatory enforcement action follows a breach, the organization can argue it took all reasonable steps to mitigate harm, including paying to recover or delete the data.

This line of reasoning, however, is inherently flawed. The actions of criminal actors are neither verifiable nor enforceable. Threat actors understand this dynamic. They now tailor their ransom communications to emphasize proof of deletion or quasi-legal indemnification language designed to give victims plausible deniability or courtroom

leverage. These promises are hollow, but they exploit the legal system's preference for documented mitigation efforts and transform ransomware from a technological problem into a legal one. If attackers know an organization will pay purely for legal optics, the ransom ecosystem becomes self-reinforcing.

The case against paying

► No guarantee of deletion

You are paying for a promise from a criminal. Nothing prevents the threat actor from retaining a copy of the data and extorting the organization again months later. While the data may not immediately appear on the dark web, threat actors increasingly leverage stolen data for follow-on attacks—either directly or by selling it to another group. In one case from Resilience's claims portfolio, an organization paid for data suppression and was promised protection from reattack. Less than 90 days later, the same threat actor returned using data that had supposedly been deleted.

The 'mark' factor. Paying signals that an organization is a paying customer. This can make it a more attractive target for future attacks by the same group or others in the broader criminal ecosystem. [CrowdStrike's 2025 State of Ransomware Survey](#) found that 83% of organizations that paid were attacked again, often by the same threat actor—a re-extortion rate nearly four times higher than for organizations that refused payment.

► Legal and sanctions risk

Depending on the organization's jurisdiction and the identity of the hackers, paying the ransom could be illegal, particularly if the group is on a government sanctions list such as the U.S. Treasury's OFAC designations.

► Funding the criminal enterprise

Payment fuels the broader extortion ecosystem, encouraging and financing criminal activity. A single organization's decision to pay may address its own legal exposure in the short term, but it increases the threat surface for others in its sector and supply chain. This is not just a compliance issue or a boardroom dilemma; it is a systemic cyber risk multiplier.

► Reputational exposure

Paying a ransom often requires disclosing the attack, which can itself damage reputation and erode customer trust.

The legal reality regardless of payment

The decision to pay or not to pay does not affect notification requirements. Regardless of the payment decision, the path carries legal consequences. The baseline for almost all litigation is the negligence claim: plaintiffs—customers, employees, or shareholders—will argue that the organization failed to maintain reasonable security measures.

It becomes a difficult position in either direction. If an organization pays to prevent a leak, the threat actor may leak the data anyway, or a plaintiff's attorney may argue the company paid a criminal rather than taking care of the victims. If the organization does not pay, opposing counsel may argue the company had an opportunity to limit the damage and chose not to, thereby failing its duty to minimize impact on affected individuals.

Negotiation trends

Negotiating with cyber extortion groups has evolved from ad hoc email exchanges into a highly structured, professionalized process. Modern ransomware groups often operate with the organizational hallmarks of legitimate businesses, complete with help desks, communications staff, and tiered management.

Threat actor personas

Attackers generally adopt one of two primary personas depending on their group's brand and level of sophistication. Some groups employ a calm, businesslike tone, framing the ransom as a 'security audit fee' and referring to the victim as a 'client.' Others rely on intimidation, ridicule, and emotional volatility to induce panic—mocking the organization's security team, using profanity, or dismissing counter-offers as insulting.

Common pressure tactics

Regardless of persona, negotiations typically revolve around several recurring themes.

► Omniscience

Attackers frequently demonstrate knowledge of the victim's financial health to justify their demands. They often exfiltrate insurance policies, bank statements, or executive communications, then reference that material directly—citing a specific cyber insurance policy limit, for instance, to undercut any claim that the organization cannot afford payment.

► The product guarantee

Threat actors emphasize their reputation, asserting that if the victim pays, the data will be deleted and no reattack will follow. They frame this as a business interest: if word spreads that a group does not honor its commitments, future victims will be less willing to pay.

► Legal and regulatory pressure

Attackers increasingly use automated tools to scan stolen data for personally identifiable information, protected health information, or financial records. They then theme their communications around the fines, lawsuits, and reputational consequences the victim will face if the data is released.

► The ticking clock

Nearly every negotiation features a countdown.

Professional counter-tactics

Experienced negotiators deploy a range of strategies to reduce urgency, buy time for the forensic investigation, and maintain a controlled dialogue.

► Buying time

Negotiators ask detailed technical questions about the exfiltrated data, request additional proof of claims, or slow the conversation through deliberate procedural complexity. Across our incident response partner network, data suggests that when negotiations extend beyond 14 days, the likelihood of a payment being made drops to less than 10%.

► Tactical empathy

Skilled negotiators acknowledge the attacker's 'business' in order to keep the conversation civil and reduce the risk of impulsive data releases.

► **The limited authority play**

The negotiator positions themselves as having only a constrained budget approved by leadership, making it harder for the attacker to anchor demands to the full insurance policy limit.

► **Data-driven valuation**

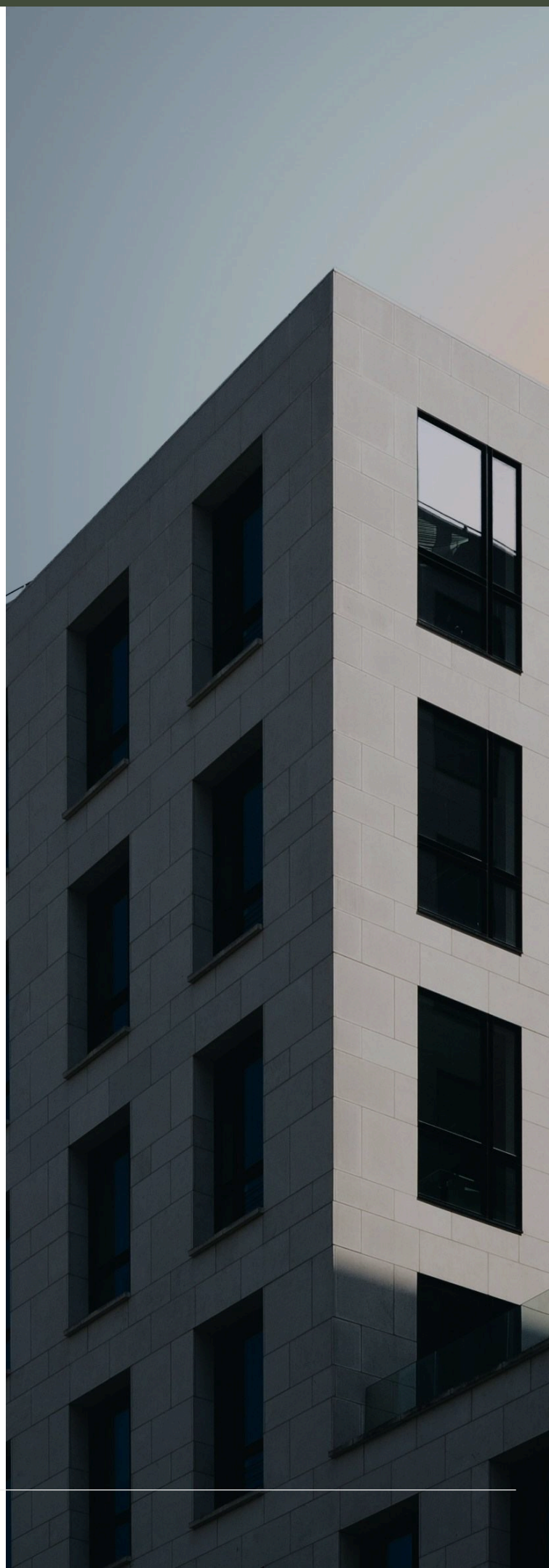
The victim's team conducts a thorough, independent valuation of the exfiltrated data and holds that number firmly throughout the process, removing leverage from the threat actor.

Threat actor discount behavior

For data extortion-only events—where no decryption key is at stake—organizations can generally expect a significant discount from the initial demand, often in the range of 50-70%. If the negotiation team can extend the timeline and tie the discussion to a defensible, independent valuation of the data, even greater reductions are achievable.

Threat actors treat extortion as a business and generally follow a 'something is better than nothing' calculus. Once a group has successfully exfiltrated data, it has already expended resources. If the victim demonstrates convincingly that it cannot or will not pay the full amount, the attacker will frequently reduce the price substantially to avoid a total loss on its investment.

One critical variable: if the threat actor has obtained a copy of the victim's cyber insurance policy, significant negotiation leverage is lost. This is an increasingly common scenario and one that organizations should plan for by limiting internal access to policy documents and implementing controls to prevent their exfiltration.



Payment vs. non-payment outcomes at a glance

	Payment refused	Payment made
Leak rate	40–50% of stolen data eventually surfaces on the dark web	30–40% of data is leaked, sold privately, or made available to affiliated groups regardless of payment
Re-extortion rate	20–25% re-attacked within one year; typically because the original vulnerability remained unpatched	83% attacked again, often by the same threat actor (CrowdStrike, 2025)
Harassment	25–30% of groups harass individuals as standard procedure via direct emails, calls, or mass SMS	Less common post-payment, but threat actors may use confirmed data value to target the organization's clients or partners
Release timeline	Name on leak site within 1–3 days; data sample within a week; full dataset within 14 days	No fixed timeline; leaks may surface months later through private sales or affiliated groups
Legal exposure	Plaintiff's counsel may argue the organization had a chance to limit damage and chose not to	Courts have ruled theft of data constitutes the harm; plaintiff's counsel have used payment as evidence the company prioritized concealment over victim protection
Regulatory risk	Standard breach notification obligations apply	Regulators are increasingly aggressive toward organizations that attempt to pay their way out of disclosure; <u>nearly all 50 U.S. states impose strict liability for breaches involving PII</u>

Outcomes when payment is refused

When a victim refuses to pay, the threat actor's response is no longer limited to a simple data leak. Attackers now auction stolen data to competitors, harass the victim's employees or clients directly, and deploy increasingly aggressive public pressure campaigns.

Based on data from Resilience's 2024–2025 claims portfolio and incident response partner network, the following patterns emerge when payment is refused

► Leak rates

Approximately 40–50% of stolen data eventually surfaces on the dark web. Stolen credentials from these breaches in turn fuel the broader cybercriminal marketplace.

► Harassment

An estimated 25–30% of extortion groups have made direct harassment of individuals a standard operating procedure—through direct emails, phone calls to personal devices, or mass SMS campaigns targeting employees or clients.

► Release timelines

Once a ransom deadline passes, threat groups typically post the victim's name to a leak site within one to three days, release a data sample within a week, and publish the full dataset within 14 days. Modern tactics increasingly include the creation of searchable, indexed web portals of stolen data, making it easier for journalists and other threat actors to locate specific records.

► Re-extortion

For organizations that do not pay, the re-attack rate within a year sits at roughly 20–25%. These follow-up attacks are rarely retaliation for non-payment. Instead, they occur because the original vulnerability remained unpatched and was discovered by a different threat actor.

Outcomes when payment is made

Paying to recover a decryption key and paying to suppress stolen data are not the same decision. The first has a verifiable outcome. The second does not.

Based on available data from Resilience's claims portfolio and third-party research, the following outcomes are observed.

► Leak rates

In approximately 30–40% of cases, data is either leaked anyway, sold privately, or made available to affiliated groups—regardless of the suppression payment.

► Re-extortion

Once identified as a paying customer, organizations face significantly elevated re-extortion risk. CrowdStrike's 2025 State of Ransomware Survey found that 83% of organizations that paid a ransom were subsequently attacked again.²

► Regulatory exposure

Regulators are becoming more aggressive toward organizations that attempt to pay their way out of public disclosure. Nearly all 50 U.S. states now impose notification obligations for data breaches. If personally identifiable information was exfiltrated, the organization is legally required to notify affected individuals regardless of whether it paid the attacker.

► Follow-on litigation

Class-action lawsuits are now commonplace regardless of whether a ransom was paid. Courts have increasingly found that confirmed data theft constitutes cognizable harm, and plaintiff's attorneys will argue the stolen data remains permanently at risk regardless of whether it surfaces publicly. In some cases, attorneys have used the fact of payment itself against the organization, arguing the company was willing to pay a criminal to conceal the breach but unwilling to compensate the actual victims.

Recommendations

The data above points to several strategic priorities for organizations seeking to reduce their exposure to extortion-only attacks and manage the consequences when they occur.

► Shift from recovery to prevention

The extortion-only model renders backup-centric resilience strategies insufficient. Organizations should prioritize data loss prevention capabilities designed to intercept exfiltration before it occurs. A zero trust architecture is essential to contain the blast radius of identity compromises, as stolen credentials and session hijacking remain the primary precursors to breaches in this category.

► Prepare for the ransom decision before a crisis occurs

The worst time to evaluate whether to pay a ransom is during an active incident. Organizations should develop a decision framework in advance that accounts for threat actor behavior, their industry's regulatory environment, and the types of data they hold. This framework should include pre-identified legal counsel, an incident response retainer with experienced forensic and negotiation firms, and a clear chain of authority for payment decisions.

► Protect insurance policy information

When a threat actor obtains a copy of an organization's cyber insurance policy, negotiation leverage shifts dramatically. Organizations should treat policy documents as sensitive material: restrict internal access, store them outside the primary network where possible, and implement monitoring controls to detect unauthorized access or exfiltration.

► Test preparedness rigorously

Tabletop exercises and breach simulations should replicate the fog of war that characterizes a real crisis. Generic scenarios are insufficient. Exercises should incorporate extortion-specific decision points—including the ransom payment question itself—and involve legal counsel, communications, and executive leadership alongside security teams.

► Track the long tail of financial impact

One area where the industry's understanding remains incomplete is the full financial lifecycle of a ransomware or extortion event. Organizations and their insurers should invest in tracking long-tail costs—regulatory fines, litigation outcomes, customer churn, and reputational recovery—to build a more complete picture of the true cost of both paying and refusing to pay.

Endnotes

¹ In the 2024 PowerSchool breach, the company paid a ransom to prevent disclosure of student and teacher data. The threat actor subsequently re-extorted individual school districts using the same dataset, demonstrating how suppression payments can validate the value of stolen data and create new extortion targets.

² CrowdStrike, 2025 State of Ransomware Survey