semperis

2026 Ransomware Risk Report

AI complicates an evolving threat environment, with attackers implementing AI-driven attacks and exploiting companies' internal AI agents and systems.

Bad actors increasingly turn to personal threats, including doxxing and swatting, to turn up the pressure on their targets.

The identity infrastructure continues to be a top target, but a lack of procedures and tools for identity system recovery may hamstring ransomware response.

"The attack surface is enormous and continues to grow. The security and IT communities must work together to try to defend this surface, which is getting ever broader with AI being used by adversaries as well as the increasing occurrence of shadow AI in the workplace. One thing that hasn't changed is the high prevalence of attacks that target the identity system.

SIMON HODGKINSON | Former bp CISO and Semperis Strategic Advisor

Executive Summary

The ransomware threat landscape continues to evolve, with AI taking a pivotal role and attackers expanding the scope of their threats beyond the business and into the personal realm. However, one core truth is unchanged: Identity is still a top attack target, and too few organizations are prepared to quickly recover the identity infrastructure to a secure state.

Semperis' *2026 Ransomware Risk Report* studies organizations that experienced at least one successful ransomware attack. This year's report provides visibility into the state of ransomware and related risks to both business continuity and employee well-being. We synthesize responses to provide a candid and detailed exploration of interconnected factors including AI's involvement in threat escalation and attack timing, frequency, and payment trends; attacker tactics; operational resilience levels; and crisis management challenges. Drawing on this data and insights and experiences from real-world engagements, our experts provide insights and recommendations for strengthening ransomware preparedness.

For this report, we partnered with international research firm Censuswide to survey organizations in **9 countries** and **8 industry sectors** across **North America, Europe, the United Kingdom, and Asia-Pacific.** The ***2026 Ransomware Risk Report*** offers an extensive view into the activity and business impact of ransomware around the world.

> Collective resilience — that 'we're all in it together' spirit — is really important. Collectively, we need to understand both the upstream and downstream impacts of every attack and what we can do to protect not just ourselves but also one another.
>
> – **Sarah Armstrong-Smith** | UK Government Cyber Advisory Board Member and Author

We encourage you to share this information with your IT and security teams. Most important, share these findings with your organization's business leadership — and build alignment around the actions your organization must take to ensure operational resilience in the face of ransomware's never-ending threat.

Key Findings

69%

Multiple attacks (and multiple payments) continue.

69% of surveyed ransomware victims were targeted multiple times within the past 12 months;

31% made multiple payments to attackers.

84%

AI is changing the ransomware landscape.

84% of attacks weaponized artificial intelligence in some way.

37%

Attackers increasingly threaten victimized companies' staff and their families.

37% of attacks involved threats not just against operations or company staff but against employees' friends or family members. In addition,

41% of respondents said they had been the target of physical or psychological intimidation.

87%

Identity infrastructure continues to be a prime target as identity recovery preparation lags.

87% of ransomware attacks targeted identity systems like Active Directory (AD), Entra ID, and Okta. But only about half the companies we surveyed have dedicated identity backups, automated identity recovery solutions, and identity-specific crisis response procedures.

Contents

01	Ransomware = Big Business	05
02	Evolving Tactics and Escalating Threats	10
03	Real People, Real Consequences	15
04	The Identity Crisis Continues	19
05	Achieving Resilience	23
06	Appendix	29
07	Methodology	47

Contributing Experts

Sarah Armstrong-Smith
UK Government Cyber Advisory Board Member and Author

Tomer Bar
Semperis AVP of Security Research

Tim Beasley
Semperis Senior Incident Response Consultant

Mickey Bresman
Semperis CEO

Sarah Gosler
Cyber Resiliency and Human Defense Expert

Guido Grillenmeier
Semperis Principal Technologist (EMEA)

Courtney Guss
Semperis AVP of Crisis Management

Simon Hodgkinson
Former bp CISO and Semperis Strategic Advisor

Chris Inglis
Former US National Cyber Director and Semperis Strategic Advisor

01

Ransomware = Big Business

Attackers continue to hit hard, fast, and frequently; most organizations continue to pay up.

> Ransomware has proven to be a great cash-generating activity for criminal syndicates, which have no hesitation about inflicting both cyber and physical harm.
>
> – **Mickey Bresman** | Semperis CEO

For the past several years, we've encouraged global organizations of all sizes to adopt an "assume breach" position. Ransomware (and other types of cyberattacks) have become endemic, and although maintaining a strong security posture is vital, there's no such thing as a foolproof defense.

KEY TAKEAWAYS

More than two thirds of victims were successfully attacked multiple times.

Nearly one third of attacks occurred on the same day; another one third occurred within the same week.

Most attackers had a dwell time of 2–6 days; less than one third attacked within 1 day; and more than one tenth were in the victim's environment for a week or more.

Most organizations are still paying ransom at least once, with nearly one third paying multiple times.

With that in mind, **this year's report surveyed only organizations that were successfully attacked** — that is, at least one ransomware attack caused some level of disruption to the business. Our goal with this change from previous studies is to focus more deeply on the behaviors and responses that might lead to or result from a successful breach.

In our analysis, we call out commonalities, anomalies, and trendsetters that fell outside the norms. Let's dive in.

Threat actors are always true to their mission. So, you must determine: Are they financially motivated or politically motivated? Because the latter is more likely to wipe your data no matter how much you pay.

– **Sarah Armstrong-Smith** | UK Government Cyber Advisory Board Member and Author

Tried and True: Attackers Continue to Focus on Times of Distraction

As we've noted in previous years, bad actors strike when companies are most likely to miss their initial entry into the environment. Although **38%** of attacks occurred during regular operating hours, evenings and weekends were by far the most dangerous times, with **79%** of respondents noting attacks then. And **14%** happened during the chaos that often accompanies material corporate events: mergers or acquisitions, IPOs, or mass staffing changes.

Attackers evaluate how they can attack most effectively. One of the most promising methods is to hit targets when their security operations staffing is lower than usual, which is typically outside normal business hours.

– **Guido Grillenmeier** | Semperis Principal Technologist (EMEA)

When were you attacked?

TRENDSETTERS

AUSTRALIA
41% attacked during a holiday; 34% attacked after a material event

ITALY
100% attacked during an evening or weekend

SPAIN
68% attacked during regular hours

CRITICAL INFRASTRUCTURE
27% attacked during a holiday

FEDERAL
48% attacked during regular hours

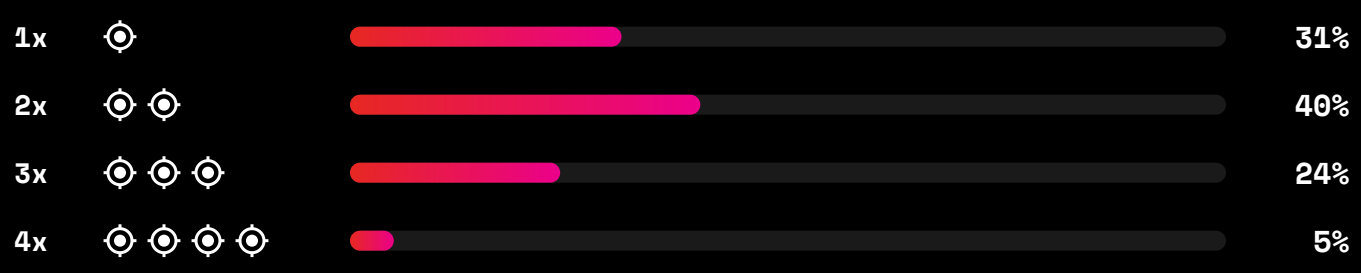
MANUFACTURING
84% attacked during an evening or weekend; 25% attacked after a material event

Multiple Attacks, Multiple Payouts

Another risk factor that remains consistent year over year is that once attackers breach a company's defenses, the flood gates for additional attacks open wide. More than two thirds of respondents (69%) told us they'd been successfully attacked multiple times.

The timings of subsequent attacks varied. Although 11% occurred simultaneously and 15% occurred more than a month apart, most organizations experienced two or more attacks on the same day (30%) or within the same week (29%); 15% occurred within the same month.

How often were you attacked?



TRENDSETTERS

AUSTRALIA

42%

experienced multiple attacks within the same week

CANADA

47%

went 1 month or more between attacks

FRANCE

51%

experienced multiple attacks during the same week

SINGAPORE

39%

went 1 month or more between attacks

SPAIN

39%

went 1 month or more between attacks

FEDERAL

53%

went 1 month or more between attacks

SLED
(State and Local Government and Education)

36%

went 1 month or more between attacks

"People don't think they'll be attacked twice," notes Sarah Armstrong-Smith, UK Government Cyber Advisory Board Member and Author. "But once you've been breached, you're an open target. After an attack, most companies focus on how to recover as quickly as possible, not how to evict the attacker and regain control of the operating system.

"But you can never trust that operating system again, because you don't know what the bad actors have done to it," she explains. "They put in malware, they put in backdoors, so regardless of whether you pay the ransom and get the encryption key, you're going to have to rebuild your environment to a known good state."

Unfortunately, this barrage of attacks is still having the desired effect, from the attackers' perspective. Most organizations paid a ransom, with most of those that paid doing so multiple times.

Yet as we've previously reported, payment offers no guarantee of recovering data or system access. In fact, Armstrong-Smith points out, receiving a decryption key from the cyber criminals can create as many problems as it solves.

"I think there's a misconception about what that key is," she says. "People think it's a magic wand that suddenly restores all their data. But those keys are typically also full of bugs and malicious code. And sometimes old, large, or complex files might never be recoverable because the decryption keys are such low quality."

Did you pay the ransom?

TRENDSETTERS

FRANCE

86%

of those that paid did so multiple times

US

87%

paid ransom

HEALTHCARE

77%

of those that paid did so multiple times

MANUFACTURING

73%

paid at least once

Paying can also be counterproductive, signaling to criminals that you're an attractive target, explains Cyber Resiliency and Human Defense expert Sarah Gosler.

"So, you pay, you exercise the deductible in your cyber insurance, and you figure you're done," says Gosler. "But if you pay but don't fix the hole in your cybersecurity dam, you're likely to be hit by another threat actor — sometimes within the same week or month — because now you have a record of payment."

So, why do companies continue to pay? Unsurprisingly, a desire to minimize damage to the business, its reputation, and its customers are leading reasons. However, nearly one quarter (23%) of respondents paid because they could not remove the attackers from their environment.

Why did you pay ransom?

TRENDSETTERS

AUSTRALIA

41%

paid because they couldn't eject attackers

FRANCE

60%

paid because they couldn't eject attackers

In addition, changing attack tactics are raising the stakes and making the threat landscape more treacherous than ever.

02

Evolving Tactics and Escalating Threats

AI enters the attack chat, and bad actors are expanding their threats beyond the business environment.

> We're starting to see more attacks with more rapid development, and attribution of these attacks will be more difficult for law enforcement. We'll also be less likely to see mistakes in attack encryption algorithms because attackers can test their code with LLMs.
>
> – **Tomer Bar** | Semperis AVP of Security Research

The majority (**51%**) of respondents in this year's survey are concerned with the rapid evolution of the threat landscape. Between the potential exploitation of AI and attackers' increasing willingness to escalate threats beyond the theft or encryption of data and operational systems, things are getting scary out there.

KEY TAKEAWAYS

AI was exploited in some way in more than four fifths of attacks.

Data destruction, business extortion, and system lockouts continue to be the most prevalent threats.

Attack tactics are becoming more personal, extending beyond the business to include threats against staff members' families or friends in more than one third of cases.

Attackers followed through on their threats in more than half of reported cases.

Here's what we learned about the tactics that are dominating the ransomware landscape … and the very personal consequences to victims' staff and their families.

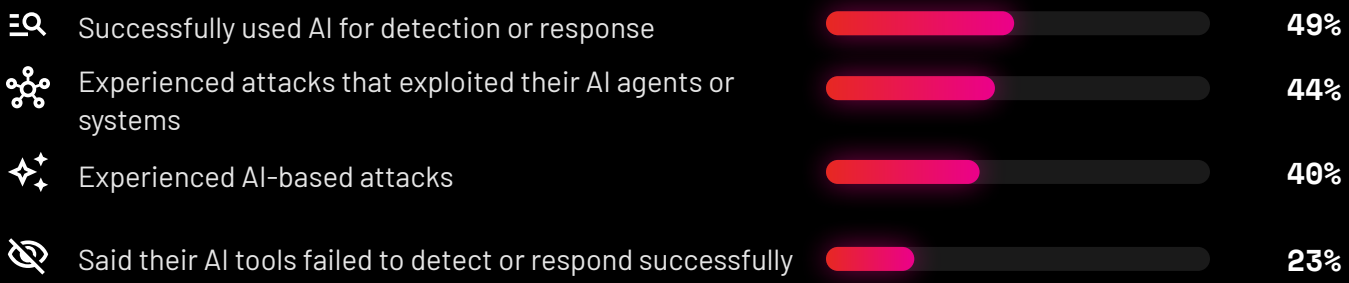
> An attacker has one goal in mind: They want to extract something from you. And the only way they're going to do that is to make the cost of resisting their demands greater than the cost of giving in. Holding you at physical risk is the latest phenomenon because we've covered most of the other risks.
>
> – **Chris Inglis** | Former US National Cyber Director and Semperis Strategic Advisor

AI: The Good, the Bad, and the Ugly

Earlier this year, we reported that **74%** of companies we surveyed were concerned that AI would make identity attacks more common. In addition, **73%** were concerned that bad actors would use AI to attack their networks.

These concerns proved prescient. Most respondents (**84%**) experienced attacks that exploited AI in some way, either via an AI-based attack (**40%**) or through manipulation of their own AI agents or systems (**44%**).

Was AI involved in the attack?



TRENDSETTERS

FRANCE

95%

successfully used AI for detection or response

GERMANY

46%

experienced defensive AI tool failure

ITALY

72%

experienced AI-based attacks; 83% experienced attacks that exploited their AI

FEDERAL

63%

experienced AI-based attacks

MANUFACTURING

52%

experienced attacks that exploited their own AI

SLED

35%

experienced defensive AI tool failure

"AI is increasing not only the speed, scope, and scale of cyberattacks, but also their sophistication," says former US National Cyber Director and Semperis Strategic Advisor Chris Inglis. "Many attacks are not perceived as being aided and abetted by AI because they're just too slick, too sophisticated."

Semperis AVP of Crisis Management Courtney Guss points out that rapid adoption of AI is complicating the defense posture for many organizations.

"If your company is adopting AI agents, you should consider that at some point, those agents will try to compromise your identity systems — even if that action isn't meant to be malicious," Guss says. "That's just how they operate. AI agents typically try to accomplish their assigned tasks by any means they can. One way they can gain more ability to operate in the environment is by getting permissions to other systems. The fastest path to get those permissions is to compromise your identity system, which effectively puts the agent into 'god mode,' enabling it to grant itself whichever permissions it needs to accomplish its task. Unfortunately, the agent then becomes a ticking time bomb."

What about AI-powered defensive tools? The good news is that nearly half (**49%**) of surveyed companies used the technology to detect or defend against ransomware. Less encouraging: Nearly one quarter (**23%**) of our respondents said their defensive AI tools failed to detect or stop the attack.

49%

of surveyed companies used the technology to detect or defend against ransomware

23%

of our respondents said their defensive AI tools failed to detect or stop the attack

Threats Extend Beyond Cyber

When it comes to ransomware leverage, data erasure, destruction, or release is still the most popular threat (**56%**), followed closely by blackmail or extortion (**41%**) and system lockouts or sabotage (**40%**). But cyber criminals aren't stopping at the digital ecosystem.

Bad actors are also threatening psychological intimidation (**23%**), physical threats (**17%**), and legal exposure (**10%**) to guarantee payment. They are targeting executives, staff, and even the families of their victims. Although criminals in some regions are still focused on "traditional" ransomware, more-personal threats are quickly gaining traction.

What threats did attackers leverage?

TRENDSETTERS

FRANCE

83%

experienced system lockout or operational sabotage

ITALY

41%

were psychologically intimidated

SPAIN

25%

were physically threatened

Semperis CEO Mickey Bresman sees expanding tactics as the natural evolution of an activity that has increasingly become the domain of terrorists and crime syndicates.

"The bad guys are always evolving their tactics," says Bresman. "When the initial wave of ransomware attacks began, most focused on data encryption. Then, after data backup and recovery systems started gaining traction and enabling companies to resist ransom demands, we saw the double extraction: encryption coupled with data theft and threats to expose or sell that data. So, it makes sense that we'll continue to see attackers trying to find more ways to make victims pay."

Threats against staff and their families take a variety of forms. Last year, we reported that attackers were turning to physical intimidation. This year's survey saw a continuation of that alarming trend.

With more than half (**53%**) of respondents reporting that ransomware attackers carried through on threats in the past year, these tactics are especially troubling.

What personal threats did staff experience?

TRENDSETTERS

AUSTRALIA

47%

were threatened with physical intrusion

ITALY

32%

were threatened with abduction; 22% with bodily harm; 74% saw threats carried out

UK

18%

were stalked; 34% saw threats carried out

CRITICAL INFRASTRUCTURE

66%

saw threats carried out

IT/TELECOMMUNICATIONS

13%

were stalked

TRANSPORTATION

38%

saw threats carried out

03

Real People, Real Consequences

Ransomware causes significant business disruption, but fallout from ransomware now extends far beyond company boundaries.

> Threats that target corporate employees beyond corporate borders are an unusual new phenomenon that distracts employees from being laser-focused while at work on the job at hand. Now you're trying to figure out how to protect yourself and loved ones against a threat that has crossed the boundary from work to personal life.

– **Chris Inglis** | Former US National Cyber Director and Semperis Strategic Advisor

KEY TAKEAWAYS

Victims or their families were doxxed, swatted, or subject to public shaming in more than half of attacks.

Business disruption, revenue loss, and cyber insurance cancellation or rate hikes overtook data loss or compromise as the top business disruptions following an attack.

More than one quarter of respondents saw staff or executive layoffs, dismissals, or resignations following an attack.

Cybersecurity leaders now know that completely preventing ransomware attacks is a near impossibility. Evaluating and balancing the risk of ransomware against the cost of defense, response, and recovery is a primary chore for IT, security, and business leaders.

The first step is a realistic understanding of the repercussions of a successful attack.

Top Ransomware Risks: Data, Revenue, and Insurability

As in previous years, the top disruptions experienced by ransomware victims were revenue loss and business disruptions (**42%**). Victimized organizations also experienced cyber insurance cancellation or rate hikes **42%** of the time — about the same as last year, but now tied with operational disruption as the leading disruption.

"Insurers want to ensure a reasonable risk," explains Inglis. "If you show through your behavior that you've not actually moderated and mitigated that risk, then you're no longer insurable to the extent that they thought you were."

Overall, data theft or destruction (**36%**) was also a prevalent concern. However, only about half as many companies experienced this consequence compared with last year.

Job losses following ransomware attacks were dramatically lower this year — **28%** overall, compared with **62%** last year. Still, this disruption was present in more than one quarter of organizations.

What disruptions or losses did your organization experience?

TRENDSETTERS

FRANCE

71%

experienced revenue loss or temporary business disruption; 65% experienced data theft or destruction

ITALY

60%

needed up to a month to recover regular operations

SLED

73%

experienced revenue loss or temporary business disruption; 49% experienced data theft or destruction

"IT and cybersecurity staff are already dealing with high levels of stress," says Tim Beasley, Semperis Senior Incident Response Consultant. "A ransomware attack takes that to a whole new level. I've seen CISOs literally say, 'I'm out, I'm done, I can't do this. It isn't worth it.' I've seen people walk out the door because leadership thought they mismanaged something that caused the breach to occur. It all takes a mental toll."

One bright spot is that overall, more organizations were able to quickly return to a normal operating state, with **28%** requiring less than a day (compared with **17%** last year) and only **17%** requiring more than a week (compared with **31%** last year). Still, half of all respondents required up to a week to return to regular business.

28%

requiring less than a day
(compared with 17% last year)

17%

requiring more than a week
(compared with 31% last year)

The Personal Cost of Ransomware

Organizations are used to weighing the business risks of a ransomware attack. Some of these risks, such as staff reductions, obviously affect the real people behind the corporate entity. Those negative effects are now spreading to people outside the company, including not just staff but their families.

About one quarter of ransomware targets reported that their employees and employees' family members were doxxed, meaning their identities were revealed online without their consent (**25%**); swatted, meaning that they were harassed by fabricated emergency reports that resulted in law enforcement being dispatched to their location (**23%**); or required medical or psychological treatment (**25%**) or extra security details (**24%**) because of ransomware threats. Some (**14%**) were even forced to change jobs or office locations or move to a new home.

What impact did the attack have on staff and their families?

TRENDSETTERS

AUSTRALIA

51%

of employees hired security; 47% required medical or psychological intervention

ITALY

63%

were doxxed; 38% were swatted

SPAIN

33%

had staff that were forced to change jobs, offices, or residences

"People are becoming almost desensitized to their data being stolen or shared," says Guss. "That's where the growth of psychological and physical threats is coming from: Other levers just aren't as effective anymore for threat actors, so they're adopting even more nefarious tactics."

"Attackers play as dirty as they need to get what they want," says Sarah Gosler. "That's why they're taking it beyond just a company's operation and making it personal. We need to start thinking about cyber attackers as the criminals that they are. Would it surprise you if a criminal physically intimidated somebody? No. As companies, we have rules, compliance, lawyers, regulators ... all these rules that we must follow. Attackers don't follow any rules. You're basically going to a gunfight, and you're equipped with a spork."

04

The Identity Crisis Continues

Despite being a top attack target, the identity infrastructure remains at risk in most organizations.

> *Identity is the coin of the realm. If an attacker can steal an identity, they're off to the races. Insider threats are not always a literal insider, a physical person who's abusing their authority. Often, it's an internal persona acting on an external attacker's behalf to abuse an insider's privileges. Sometimes it's a process that just runs amok. In every case, identity is the core issue.*
>
> – **Chris Inglis** | Former US National Cyber Director and Semperis Strategic Advisor

KEY TAKEAWAYS

In nearly four fifths of organizations, ransomware targeted or exploited the identity infrastructure.

Only half of the victimized organizations maintained dedicated identity backup systems, and less than half had solutions that automate identity system recovery.

Crisis management and disaster recovery plans lacked consideration of the identity infrastructure (primarily Active Directory, Entra ID, and Okta).

The identity infrastructure continues to be a primary target for ransomware attackers, who targeted Active Directory, Entra ID, or Okta in **87%** of the cases in our survey. Active Directory (AD) was the target in more than half (**51%**) of these cases, followed closely by Entra ID (**48%**). More than one quarter (**27%**) of respondents also experienced Okta breaches.

The threats against identity are not new. For years, multiple studies from global experts have reported that AD, especially, is a top target. Yet the rate of preparation to recover identity systems — the first step in successful operational recovery after an attack — continues to be a missing link for nearly half the companies in our study.

"We've known for a long time that identity is always a target for attackers, whether nation states or criminal gangs," says Simon Hodgkinson, Former bp CISO and Semperis Strategic Advisor. "You wouldn't build a house without firm foundations, but people are building their digital ecosystems without laying those foundations."

Did attackers exploit or target your identity infrastructure?

TRENDSETTERS

AUSTRALIA

98%

experienced an identity attack

ITALY

75%

of attacks targeted Entra ID

SPAIN

57%

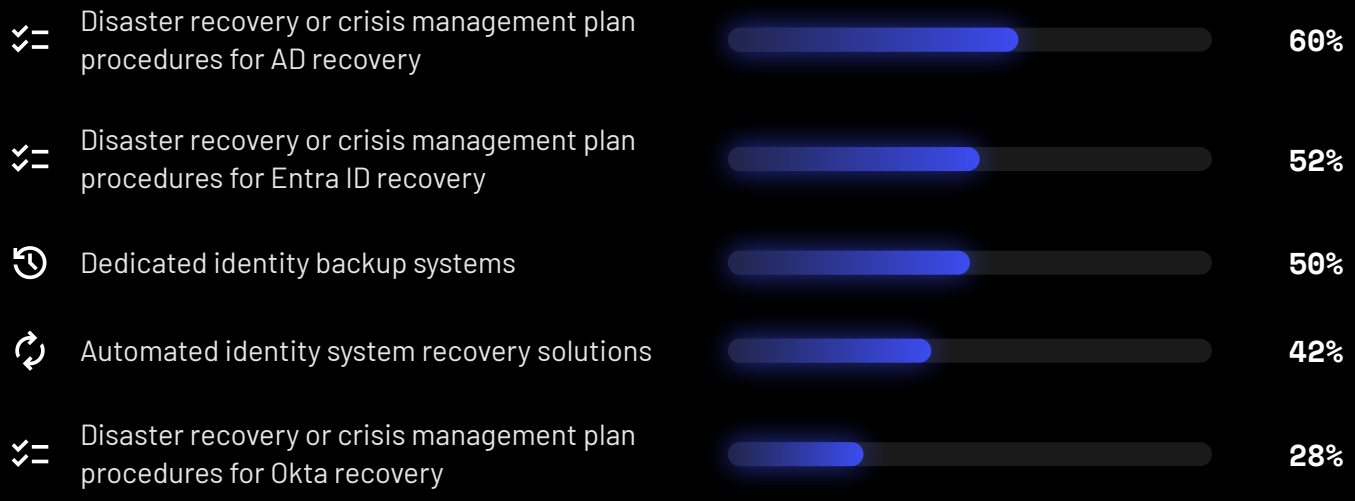
of attacks targeted Okta

FEDERAL

96%

experienced an identity attack

What steps have you taken to defend and recover your identity infrastructure?



Where Identity Defense Falls Short

For the past several years, identity threat detection and response (ITDR) solutions have proliferated across the cybersecurity market. Yet based on our study, the adoption gap remains significant.

Only half (50%) of the companies we studied had dedicated identity backup systems, an important factor in the ability to recover identity to a secure state. Without such backups, identity systems are vulnerable to hidden malware and backdoors, reintroducing bad actors into the recovered environment.

Less than half (42%) of respondents had automated identity recovery solutions, another necessity for identity recovery, especially as AI speeds the rate of attacks. Such tools reduce a time-consuming manual process with dozens of steps to a matter of hours.

Only about half the organizations in our study reported having documented recovery procedures for their AD (**60%**) or Entra ID (**52%**) systems. Even fewer (**28%**) had documented the steps to recover Okta. Even — or perhaps especially — without identity-recovery automation, the inclusion of identity attack response procedures in crisis response and disaster recovery plans is crucial to identity and operational resilience.

The lack of preparation for identity recovery is especially concerning in the face of rapid AI adoption by both attackers and their potential victims, as discussed in our previous report on AI-related identity risks and as evidenced in the rate of attacks that exploited victims' own AI agents and systems.

"Organizations have no way of predicting what an AI agent will decide to do and what unexpected effect its actions might have," explains Bresman. "An attacker that exploits that agent gains that same level of access. So, putting up guardrails around your identity systems as quickly as you can is critical."

TRENDSETTERS

FRANCE

31%

maintained dedicated identity backups; 23% included AD recovery procedures in their crisis response plans

UK

75%

included AD recovery procedures in their crisis response plans

US

20%

had automated identity recovery tools; 33% included Entra ID recovery procedures in their crisis response plans

ITALY

76%

included Entra ID recovery procedures in their crisis response plans

FEDERAL

37%

maintained dedicated identity backups

05

Achieving Resilience

The rapidly changing attack landscape demands more of your crisis management plans. Here's how you can prepare for what's ahead.

> Organizations constantly need to reevaluate their response and recovery plans to ensure that they're aligned on the scenarios in which they are willing to pay a ransom and how to handle communications with customers, suppliers, partners, and the public. The more aligned you are before an incident, the easier it is to make those calls under pressure.
>
> – **Courtney Guss** | Semperis AVP of Crisis Management

Crisis management planning is a key factor in organizations' ability to respond to ransomware and to recover compromised systems, increasing their ability to resist criminal demands.

So, what do companies say is blocking effective response?

KEY TAKEAWAYS

Nearly half of respondents pointed to a lack of defined roles and responsibilities as their top blocker to effective cyber crisis response.

Cross-team communication and outdated plans were also major concerns.

Evolving threats, including AI, are the biggest challenge to operational resilience for half the organizations we studied.

Organizations can better prepare for evolving attacks by updating crisis management plans and closing communication gaps.

> The power in this industry is community: collaboration between the public and private sector, big business, small business. All of us must work together. Even from a critical infrastructure perspective, it's finance, healthcare, energy, all working in partnership with the government. We have to create a mission-oriented community. It's like that adage: We're safer together.

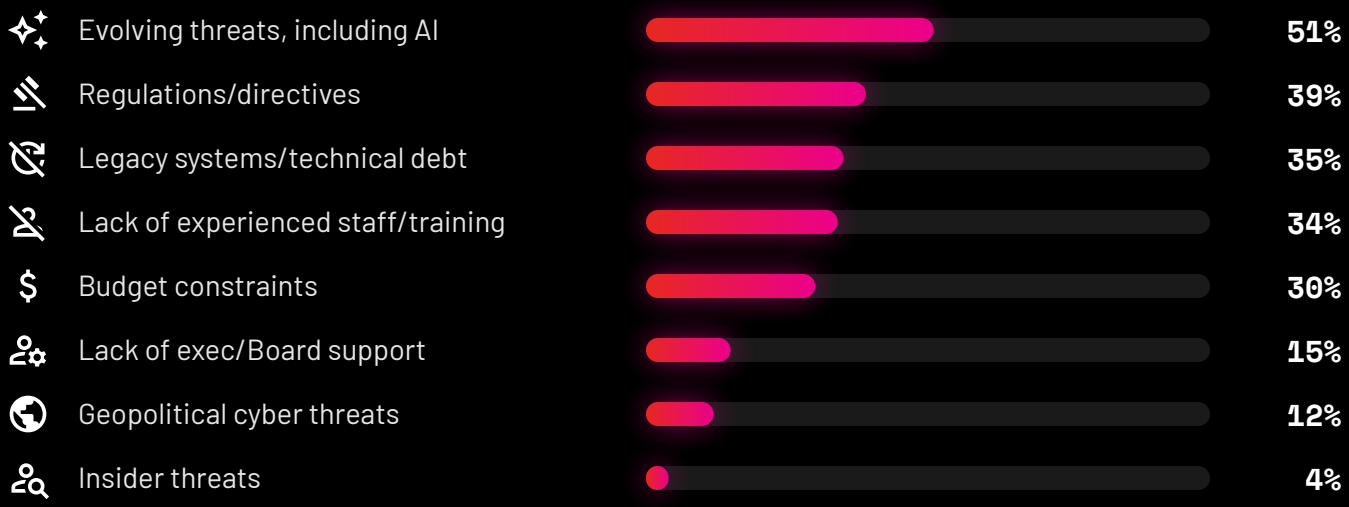
– **Sarah Gosler** | Cyber Resiliency and Human Defense Expert

What's Blocking Operational Resilience?

When organizations adopt an "assume breach" mindset, resilience — the ability to maintain or recover operations even when the worst happens — takes priority. So, we asked the companies in our study to tell us what's getting in the way of resilience.

Unsurprisingly, the threat landscape was the biggest challenge for **51%** of respondents. Many organizations also struggled with outdated systems and the technical debt that accompanies them (**35%**).

What are your biggest challenges to operational resilience?



TRENDSETTERS

FRANCE

72%

were concerned with the threat landscape; 79% worried about lack of experienced and trained staff

FEDERAL

48%

were concerned with legacy systems and technical debt

SLED

43%

were concerned with legacy systems and technical debt

"Legacy systems, usually in combination with specialized hardware, often require less secure protocols to connect and authenticate to the identity plane," says Grillenmeier. "This introduces unwanted attack vectors that are nevertheless necessary to keep the business-critical systems operational."

This year, **39%** of respondents also reported a challenge meeting regulatory demands (up from **24%** last year). Grillenmeier notes that changing cybersecurity laws are likely the cause.

"Regulated environments often need to prove their ability to respond to various cyberattack situations," he says. "For years, regulating bodies have not focused on identity resilience, but recent updates — such as NIS2 for European companies — now demand proper identity resilience by companies that fall under their purview."

Budget constraints were a concern for about one third of our study participants (**30%**) but took a back seat to a lack of experienced staff, cited by **34%** of respondents overall.

39%

reported a challenge meeting regulatory demands (up from 24% last year)

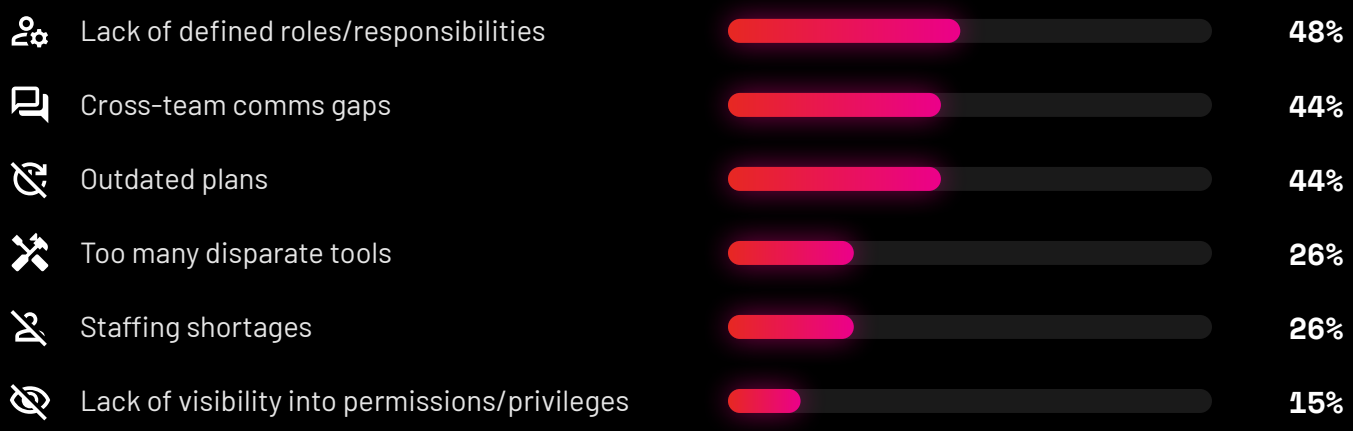
34%

a lack of experienced staff

What's Blocking Effective Cyber Crisis Response?

Considering worries about the threat landscape, effective crisis response becomes more vital than ever. This year, the biggest challenges to effective response were related to companies' crisis plans themselves. About half of all respondents said they struggle with outdated plans (**44%**), a lack of defined roles and responsibilities during crisis response (**48%**), and gaps in communication across teams (**44%**).

What are your biggest blockers to effective cyber crisis management and response?



> Many organizations struggle with cross-team communication gaps. We often see this issue when a company uses separate tools for different teams — rather than one out-of-band communication tool that can serve all teams — or hasn't made sure that everyone involved in response knows how to use the organization's tools and processes in a crisis.
>
> – **Mickey Bresman** | Semperis CEO

Defined roles are especially important for organizations that aim to stay in favor with their cyber insurance companies. Many policies have stringent requirements about who carries out certain responsibilities and in which order.

"As soon as you know that you have an adversary in your network, you need to respond at light speed and you need to be able to make decisions even without all the information at hand," says Hodgkinson. "You need to have those roles and responsibilities already defined so that decisions can be made whilst you're spinning up the rest of your crisis management capability to manage the business impact and so on."

He sees the problem as a common one for companies that fail to run their plans through realistic attack scenarios.

"To me, having spent years in crisis management, this concern suggests that people aren't doing tabletop exercises," he says. "Such exercises should be foundational."

Communication issues also catch many organizations by surprise when ransomware locks down phones or email or when attackers breach those systems.

How to Improve Ransomware Resilience

What can organizations do to better prepare for evolving threats? Our experts suggest beginning with three priority steps.

01 Prepare for modern threat tactics.

If you haven't updated your crisis management plan lately, now is the time. Make sure that you've documented roles not just within the cybersecurity team, but across the entire enterprise.

Establish out-of-band communications for use when standard tools are unavailable or untrustworthy. Make sure that all stakeholders have access to these tools and know how to access and use them.

Include procedures for how to respond to incidents that involve places and people outside the organization, such as threats against family members. For example, reach out to local and federal law enforcement in advance to establish proper channels.

"I've spoken with CISOs that had strong relationships with law enforcement," says Guss. "They've found it to be a much faster route to information and resources than they would otherwise have found on their own, which can often help them recover more quickly. So, knowing those contacts and building those relationships in advance should be part of your crisis management plan."

02 Strengthen identity resilience.

Prepare for identity system breaches. Strengthening identity defense — for example, by locking down agentic AI access to the identity fabric — is an important step, but preparing for identity system recovery is even more critical.

"A ransomware operation can use Active Directory to encrypt your entire organization," says Semperis AVP of Security Research Tomer Bar. "With the right permissions, they can move laterally from machine to machine. You must harden the system, verify your security posture, and prepare for fast recovery to a trusted state."

Effective identity resilience is a combination of people, processes, and technology. Certainly, tech solutions like automated AD, Entra ID, or Okta recovery are incredibly useful. But equally important is making sure that your crisis response plan clearly documents identity recovery procedures so that you are fully prepared to reclaim a secure identity ecosystem and recover your minimum viable company (MVC) as quickly as possible.

03 Practice, then practice again.

As you develop your plan, be sure to run it through its paces against realistic scenarios, not just on paper. This type of tabletop exercise will reveal where the plan falls apart and help your crisis response team react quickly and calmly to ransomware and other attacks.

"You need to be testing all the people on your incident response and recovery processes to make sure that you understand and can overcome any blockers to effective response," says Hodgkinson. "This type of practice is important to clarify things like roles and responsibilities, such as who has the delegated authority to make certain decisions during a cyber incident. Who decides when to take the network offline? Who decides whether to isolate the internet?"

"You need to figure out what you would do in advance," says Gosler, "so that the first time you're having that conversation is not in the middle of a ransomware attack. Not everyone reacts calmly under pressure. Things move quickly, and that's where mistakes happen. Some people want to go in this direction, other people want to go in that direction, and trying to contain things and keep people all moving in the same direction is vital. Focusing on humans and on training them to handle cyber crises can become one of your greatest assets."

Plan for a Stronger Ransomware Response

Companies can prepare for ransomware attacks by addressing emerging AI-related risks and by proactively modernizing their crisis response plans to address criminal tactics — both long-standing ones, such as identity attacks, and new threats that extend into the physical space. Although cyberattacks are now endemic, effective response is both possible and necessary.

"Cybersecurity is everyone's problem," says Gosler. "No individual or organization is immune from it. In a world of next-frontier AI, companies must invest in cybersecurity. It is no longer something that can take a backseat in budget discussions. And within cybersecurity, we're starting to see a shift from cybersecurity to cyber resilience. As much as focusing on detection and prevention is important, you have to focus on resilience and recovery."

06

Appendix

Full response breakdown by country and industry.

COUNTRIES

- AUSTRALIA
- CANADA
- FRANCE
- GERMANY
- ITALY
- SINGAPORE
- SPAIN
- UNITED KINGDOM
- UNITED STATES

INDUSTRIES

- BANKING & FINANCE
- CRITICAL INFRASTRUCTURE
- FEDERAL GOVERNMENT
- HEALTHCARE
- IT & TELECOMS
- MANUFACTURING
- SLED
- TRANSPORTATION

AUSTRALIA

Ransomware attack statistics, full response breakdown

semperis

84% were successfully attacked multiple times

79% paid ransom

When were you attacked?

on an evening or weekend	74%
during a holiday	41%
after a material event	34%

Was AI involved in the attack?

attacks used AI	37%
attacks exploited the victim's AI agents or system	50%
defenders successfully used AI to detect or respond	65%
defenders' AI detection or response tools failed	35%

19% of attacks involved physical threats

41% of attacks involved threats against family members or friends

Staff impacts

were doxxed	24%
were swatted	35%
required medical/psychological treatment	47%
were forced to move from job, office, or home	26%

Business impact

temporary disruption	58%
cyberinsurance cancellation/price hike	50%
data theft/destruction	27%
reputational damage	36%
layoffs, resignations, or dismissals	50%
fines or lawsuits	25%

98% of attacks targeted the identity infrastructure

63% maintained dedicated identity backup systems

59% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	64%
Entra ID recovery	65%
Okta recovery	46%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Outdated/legacy systems or technical debt

CANADA

Ransomware attack statistics, full response breakdown

semperis

48% were successfully attacked multiple times

31% paid ransom

When were you attacked?

on an evening or weekend	53%
during a holiday	27%
after a material event	12%

Was AI involved in the attack?

attacks used AI	47%
attacks exploited the victim's AI agents or system	36%
defenders successfully used AI to detect or respond	47%
defenders' AI detection or response tools failed	23%

12% of attacks involved physical threats

42% of attacks involved threats against family members or friends

Staff impacts

were doxxed	6%
were swatted	14%
required medical/psychological treatment	8%
were forced to move from job, office, or home	20%

Business impact

temporary disruption	53%
cyberinsurance cancellation/price hike	25%
data theft/destruction	32%
reputational damage	45%
layoffs, resignations, or dismissals	19%
fines or lawsuits	16%

91% of attacks targeted the identity infrastructure

55% maintained dedicated identity backup systems

57% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	45%
Entra ID recovery	57%
Okta recovery	49%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Outdated response plans

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

FRANCE

Ransomware attack statistics, full response breakdown

semperis

100% were successfully attacked multiple times

35% paid ransom

When were you attacked?

on an evening or weekend	95%
during a holiday	10%
after a material event	21%

Was AI involved in the attack?

attacks used AI	1%
attacks exploited the victim's AI agents or system	20%
defenders successfully used AI to detect or respond	95%
defenders' AI detection or response tools failed	19%

6% of attacks involved physical threats

17% of attacks involved threats against family members or friends

Staff impacts

were doxxed	14%
were swatted	32%
required medical/psychological treatment	27%
were forced to move from job, office, or home	3%

Business impact

temporary disruption	71%
cyberinsurance cancellation/price hike	18%
data theft/destruction	65%
reputational damage	16%
layoffs, resignations, or dismissals	32%
fines or lawsuits	16%

40% of attacks targeted the identity infrastructure

31% maintained dedicated identity backup systems

30% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	23%
Entra ID recovery	33%
Okta recovery	19%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Outdated response plans

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Lack of experienced personnel/ employee training

GERMANY

Ransomware attack statistics, full response breakdown

semperis

74% were successfully attacked multiple times

51% paid ransom

When were you attacked?

on an evening or weekend	77%
during a holiday	29%
after a material event	18%

Was AI involved in the attack?

attacks used AI	42%
attacks exploited the victim's AI agents or system	43%
defenders successfully used AI to detect or respond	59%
defenders' AI detection or response tools failed	46%

24% of attacks involved physical threats

48% of attacks involved threats against family members or friends

Staff impacts

were doxxed	20%
were swatted	32%
required medical/psychological treatment	37%
were forced to move from job, office, or home	22%

Business impact

temporary disruption	47%
cyberinsurance cancellation/price hike	39%
data theft/destruction	31%
reputational damage	42%
layoffs, resignations, or dismissals	36%
fines or lawsuits	33%

87% of attacks targeted the identity infrastructure

57% maintained dedicated identity backup systems

59% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	57%
Entra ID recovery	63%
Okta recovery	41%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Outdated response plans

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

ITALY

Ransomware attack statistics, full response breakdown

semperis

81% were successfully attacked multiple times

76% paid ransom

When were you attacked?

on an evening or weekend	100%
during a holiday	19%
after a material event	11%

Was AI involved in the attack?

attacks used AI	72%
attacks exploited the victim's AI agents or system	83%
defenders successfully used AI to detect or respond	48%
defenders' AI detection or response tools failed	13%

8% of attacks involved physical threats

43% of attacks involved threats against family members or friends

Staff impacts

were doxxed	63%
were swatted	38%
required medical/psychological treatment	34%
were forced to move from job, office, or home	9%

Business impact

temporary disruption	15%
cyberinsurance cancellation/price hike	61%
data theft/destruction	24%
reputational damage	43%
layoffs, resignations, or dismissals	37%
fines or lawsuits	16%

91% of attacks targeted the identity infrastructure

65% maintained dedicated identity backup systems

51% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	71%
Entra ID recovery	76%
Okta recovery	25%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Budget constraints

SINGAPORE

Ransomware attack statistics, full response breakdown

semperis

57% were successfully attacked multiple times

26% paid ransom

When were you attacked?

on an evening or weekend	65%
during a holiday	16%
after a material event	7%

Was AI involved in the attack?

attacks used AI	60%
attacks exploited the victim's AI agents or system	42%
defenders successfully used AI to detect or respond	49%
defenders' AI detection or response tools failed	28%

24% of attacks involved physical threats

41% of attacks involved threats against family members or friends

Staff impacts

were doxxed	15%
were swatted	15%
required medical/psychological treatment	8%
were forced to move from job, office, or home	16%

Business impact

temporary disruption	52%
cyberinsurance cancellation/price hike	47%
data theft/destruction	25%
reputational damage	28%
layoffs, resignations, or dismissals	18%
fines or lawsuits	18%

92% of attacks targeted the identity infrastructure

54% maintained dedicated identity backup systems

49% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	59%
Entra ID recovery	53%
Okta recovery	39%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Cross-team communication gaps

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

SPAIN

Ransomware attack statistics, full response breakdown

semperis

81% were successfully attacked multiple times

29% paid ransom

When were you attacked?

on an evening or weekend	75%
during a holiday	28%
after a material event	13%

Was AI involved in the attack?

attacks used AI	49%
attacks exploited the victim's AI agents or system	47%
defenders successfully used AI to detect or respond	52%
defenders' AI detection or response tools failed	43%

25% of attacks involved physical threats

53% of attacks involved threats against family members or friends

Staff impacts

were doxxed	22%
were swatted	16%
required medical/psychological treatment	18%
were forced to move from job, office, or home	33%

Business impact

temporary disruption	61%
cyberinsurance cancellation/price hike	48%
data theft/destruction	41%
reputational damage	29%
layoffs, resignations, or dismissals	41%
fines or lawsuits	16%

97% of attacks targeted the identity infrastructure

56% maintained dedicated identity backup systems

55% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	53%
Entra ID recovery	63%
Okta recovery	56%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities, too many disparate tools

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Cybersecurity regulations/directives

UNITED KINGDOM

Ransomware attack statistics, full response breakdown

semperis

70% were successfully attacked multiple times

51% paid ransom

When were you attacked?

on an evening or weekend	88%
during a holiday	16%
after a material event	10%

Was AI involved in the attack?

attacks used AI	40%
attacks exploited the victim's AI agents or system	47%
defenders successfully used AI to detect or respond	48%
defenders' AI detection or response tools failed	23%

17% of attacks involved physical threats

28% of attacks involved threats against family members or friends

Staff impacts

were doxxed	28%
were swatted	14%
required medical/psychological treatment	25%
were forced to move from job, office, or home	15%

Business impact

temporary disruption	52%
cyberinsurance cancellation/price hike	37%
data theft/destruction	50%
reputational damage	29%
layoffs, resignations, or dismissals	27%
fines or lawsuits	16%

84% of attacks targeted the identity infrastructure

50% maintained dedicated identity backup systems

49% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	75%
Entra ID recovery	65%
Okta recovery	24%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Cross-team communication gaps

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

UNITED STATES

Ransomware attack statistics, full response breakdown

semperis

57% were successfully attacked multiple times

87% paid ransom

When were you attacked?

on an evening or weekend	72%
during a holiday	7%
after a material event	11%

Was AI involved in the attack?

attacks used AI	35%
attacks exploited the victim's AI agents or system	40%
defenders successfully used AI to detect or respond	28%
defenders' AI detection or response tools failed	9%

18% of attacks involved physical threats

40% of attacks involved threats against family members or friends

Staff impacts

were doxxed	28%
were swatted	24%
required medical/psychological treatment	23%
were forced to move from job, office, or home	6%

Business impact

temporary disruption	18%
cyberinsurance cancellation/price hike	46%
data theft/destruction	28%
reputational damage	33%
layoffs, resignations, or dismissals	17%
fines or lawsuits	11%

94% of attacks targeted the identity infrastructure

41% maintained dedicated identity backup systems

20% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	63%
Entra ID recovery	33%
Okta recovery	13%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Cross-team communication gaps

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

BANKING & FINANCE

Ransomware attack statistics, full response breakdown

semperis

58% were successfully attacked multiple times

59% paid ransom

When were you attacked?

on an evening or weekend	67%
during a holiday	19%
after a material event	12%

Was AI involved in the attack?

attacks used AI	40%
attacks exploited the victim's AI agents or system	39%
defenders successfully used AI to detect or respond	47%
defenders' AI detection or response tools failed	17%

17% of attacks involved physical threats

31% of attacks involved threats against family members or friends

Staff impacts

were doxxed	19%
were swatted	19%
required medical/psychological treatment	24%
were forced to move from job, office, or home	7%

Business impact

temporary disruption	37%
cyberinsurance cancellation/price hike	42%
data theft/destruction	30%
reputational damage	34%
layoffs, resignations, or dismissals	24%
fines or lawsuits	7%

85% of attacks targeted the identity infrastructure

50% maintained dedicated identity backup systems

32% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	55%
Entra ID recovery	51%
Okta recovery	26%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

CRITICAL INFRASTRUCTURE

Ransomware attack statistics, full response breakdown

semperis

69% were successfully attacked multiple times

42% paid ransom

When were you attacked?

on an evening or weekend	73%
during a holiday	27%
after a material event	12%

Was AI involved in the attack?

attacks used AI	48%
attacks exploited the victim's AI agents or system	42%
defenders successfully used AI to detect or respond	54%
defenders' AI detection or response tools failed	25%

19% of attacks involved physical threats

35% of attacks involved threats against family members or friends

Staff impacts

were doxxed	23%
were swatted	16%
required medical/psychological treatment	19%
were forced to move from job, office, or home	20%

Business impact

temporary disruption	60%
cyberinsurance cancellation/price hike	40%
data theft/destruction	34%
reputational damage	30%
layoffs, resignations, or dismissals	24%
fines or lawsuits	17%

77% of attacks targeted the identity infrastructure

45% maintained dedicated identity backup systems

55% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	47%
Entra ID recovery	43%
Okta recovery	39%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

FEDERAL GOVERNMENT

Ransomware attack statistics, full response breakdown

semperis

63% were successfully attacked multiple times

37% paid ransom

When were you attacked?

on an evening or weekend	74%
during a holiday	22%
after a material event	19%

Was AI involved in the attack?

attacks used AI	63%
attacks exploited the victim's AI agents or system	44%
defenders successfully used AI to detect or respond	41%
defenders' AI detection or response tools failed	15%

7% of attacks involved physical threats

50% of attacks involved threats against family members or friends

Staff impacts

were doxxed	13%
were swatted	17%
required medical/psychological treatment	17%
were forced to move from job, office, or home	17%

Business impact

temporary disruption	56%
cyberinsurance cancellation/price hike	26%
data theft/destruction	33%
reputational damage	26%
layoffs, resignations, or dismissals	41%
fines or lawsuits	26%

96% of attacks targeted the identity infrastructure

37% maintained dedicated identity backup systems

48% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	63%
Entra ID recovery	56%
Okta recovery	41%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Outdated response plans

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Cybersecurity regulations/directives

HEALTHCARE

Ransomware attack statistics, full response breakdown

semperis

82% were successfully attacked multiple times

65% paid ransom

When were you attacked?

on an evening or weekend	81%
during a holiday	21%
after a material event	13%

Was AI involved in the attack?

attacks used AI	38%
attacks exploited the victim's AI agents or system	48%
defenders successfully used AI to detect or respond	48%
defenders' AI detection or response tools failed	26%

15% of attacks involved physical threats

43% of attacks involved threats against family members or friends

Staff impacts

were doxxed	26%
were swatted	24%
required medical/psychological treatment	26%
were forced to move from job, office, or home	13%

Business impact

temporary disruption	34%
cyberinsurance cancellation/price hike	48%
data theft/destruction	31%
reputational damage	30%
layoffs, resignations, or dismissals	31%
fines or lawsuits	16%

89% of attacks targeted the identity infrastructure

51% maintained dedicated identity backup systems

45% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	60%
Entra ID recovery	51%
Okta recovery	29%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

IT & TELECOMS

Ransomware attack statistics, full response breakdown

semperis

67% were successfully attacked multiple times

62% paid ransom

When were you attacked?

on an evening or weekend	83%
during a holiday	13%
after a material event	8%

Was AI involved in the attack?

attacks used AI	33%
attacks exploited the victim's AI agents or system	42%
defenders successfully used AI to detect or respond	44%
defenders' AI detection or response tools failed	18%

22% of attacks involved physical threats

34% of attacks involved threats against family members or friends

Staff impacts

were doxxed	28%
were swatted	28%
required medical/psychological treatment	26%
were forced to move from job, office, or home	15%

Business impact

temporary disruption	39%
cyberinsurance cancellation/price hike	38%
data theft/destruction	42%
reputational damage	33%
layoffs, resignations, or dismissals	25%
fines or lawsuits	21%

89% of attacks targeted the identity infrastructure

47% maintained dedicated identity backup systems

37% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	70%
Entra ID recovery	55%
Okta recovery	20%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Cross-team communication gaps

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

MANUFACTURING

Ransomware attack statistics, full response breakdown

semperis

72% were successfully attacked multiple times

73% paid ransom

When were you attacked?

on an evening or weekend	84%
during a holiday	19%
after a material event	25%

Was AI involved in the attack?

attacks used AI	45%
attacks exploited the victim's AI agents or system	52%
defenders successfully used AI to detect or respond	53%
defenders' AI detection or response tools failed	26%

16% of attacks involved physical threats

42% of attacks involved threats against family members or friends

Staff impacts

were doxxed	36%
were swatted	27%
required medical/psychological treatment	33%
were forced to move from job, office, or home	14%

Business impact

temporary disruption	36%
cyberinsurance cancellation/price hike	47%
data theft/destruction	33%
reputational damage	37%
layoffs, resignations, or dismissals	33%
fines or lawsuits	23%

90% of attacks targeted the identity infrastructure

54% maintained dedicated identity backup systems

47% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	60%
Entra ID recovery	54%
Okta recovery	31%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

STATE, LOCAL GOVERNMENT & EDUCATION

Ransomware attack statistics, full response breakdown

semperis

67% were successfully attacked multiple times

27% paid ransom

When were you attacked?

on an evening or weekend	76%
during a holiday	10%
after a material event	8%

Was AI involved in the attack?

attacks used AI	29%
attacks exploited the victim's AI agents or system	31%
defenders successfully used AI to detect or respond	53%
defenders' AI detection or response tools failed	35%

12% of attacks involved physical threats

41% of attacks involved threats against family members or friends

Staff impacts

were doxxed	10%
were swatted	14%
required medical/psychological treatment	6%
were forced to move from job, office, or home	18%

Business impact

temporary disruption	73%
cyberinsurance cancellation/price hike	24%
data theft/destruction	49%
reputational damage	16%
layoffs, resignations, or dismissals	22%
fines or lawsuits	6%

78% of attacks targeted the identity infrastructure

53% maintained dedicated identity backup systems

43% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	51%
Entra ID recovery	35%
Okta recovery	41%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Cross-team communication gaps

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Evolving cybersecurity threats, including AI-based threats

TRANSPORTATION

Ransomware attack statistics, full response breakdown

semperis

77% were successfully attacked multiple times

35% paid ransom

When were you attacked?

on an evening or weekend	83%
during a holiday	15%
after a material event	10%

Was AI involved in the attack?

attacks used AI	43%
attacks exploited the victim's AI agents or system	37%
defenders successfully used AI to detect or respond	48%
defenders' AI detection or response tools failed	30%

13% of attacks involved physical threats

40% of attacks involved threats against family members or friends

Staff impacts

were doxxed	15%
were swatted	18%
required medical/psychological treatment	13%
were forced to move from job, office, or home	23%

Business impact

temporary disruption	65%
cyberinsurance cancellation/price hike	38%
data theft/destruction	48%
reputational damage	32%
layoffs, resignations, or dismissals	22%
fines or lawsuits	17%

87% of attacks targeted the identity infrastructure

43% maintained dedicated identity backup systems

40% automated identity system recovery

Did your disaster recovery or crisis management plan include identity recovery procedures?

AD recovery	52%
Entra ID recovery	57%
Okta recovery	30%

TOP BLOCKER TO EFFECTIVE CRISIS MANAGEMENT & RESPONSE

Lack of defined roles & responsibilities

TOP CHALLENGE TO OPERATIONAL RESILIENCE

Cybersecurity regulations/directives

Methodology

1,200
IT AND SECURITY PROFESSIONALS

9
COUNTRIES

8
INDUSTRY SECTORS

In the first half of 2026, global organizations across North America, the United Kingdom, Europe, and the Asia-Pacific region participated in a detailed survey on their experience with ransomware. To conduct this study, we partnered with experts at Censuswide, an international market research consultancy headquartered in London. Censuswide surveyed 1,200 IT and security professionals across multiple industries, including finance, critical infrastructure, federal government, healthcare, IT and telecommunications, manufacturing, transportation, and state and local government and education (SLED).

How to cite information in this report

The data in this report are provided as an information source for the cybersecurity community and the organizations it serves. Semperis encourages you to share our findings. To cite statistics or insights, reference *Semperis 2026 Ransomware Risk Report* and link to the full report, downloadable at https://www.semperis.com/ransomware-risk-report. To interview Semperis experts, contact Bill Keeler at billk@semperis.com. We'd love to hear your questions or thoughts on the topic of ransomware and resilience. To join the conversation, find Semperis on LinkedIn.

About Semperis

Semperis is the identity-driven cyber resilience and crisis management company trusted by the world's largest enterprises and government agencies to protect critical identity systems. Purpose-built for multi-cloud and hybrid identity environments — including Active Directory, Entra ID, Okta, and Ping Identity — Semperis helps organizations prevent, detect, respond to, and recover from identity-based cyberattacks.

Modern cyberattacks are won or lost at the identity layer, where failures now escalate into full-scale business crises. Semperis' AI-powered platform unifies identity lifecycle defense and crisis management — hardening identity infrastructure, detecting and containing active threats, enabling rapid, trusted recovery, and supporting secure, out-of-band coordination when core systems are disrupted — all reinforced by a world-class identity forensics and incident response team.

As part of its mission to help organizations achieve true cyber resilience, Semperis supports the broader cyber community through the award-winning Hybrid Identity Protection (HIP) Conference and Podcast and free identity security tools including Purple Knight and Forest Druid. More than 1,200 organizations — including over 25% of the 100 largest US companies — rely on Semperis. The company is privately held, headquartered in Hoboken, New Jersey, and serves customers in more than 40 countries.

semperis

2026 RANSOMWARE RISK REPORT

semperis.com