2025 Ransomware Risk Report

- A modest decrease in ransomware success is encouraging, but attack-related business disruptions continue
- Increased frequency and sophistication of attacks, identity system compromise, and legacy vulnerabilities top the list of cybersecurity challenges
- To build business resilience, organizations must balance cybersecurity efforts across people, processes, and technology

"I do believe that we can make ransomware a shocking anomaly. And that is the world I want to live in: a world where software vulnerabilities are so rare that they make the nightly news, not the morning meeting. A world where cyber-attacks are as infrequent as plane collisions. I do believe we can get there."

Jen Easterly

Former Director of the Cybersecurity and Infrastructure Agency (CISA)

semperis

A World Without Ransomware? We Aren't There Yet.

Business leaders are catching up with the business benefits of cyber resilience … but challenges persist.

The spread of generative AI, an increasing concern about agentic AI attacks, rising geopolitical tensions, global regulatory shifts … many new developments have occurred since we released the *2024 Ransomware Risk Report*. Has the ransomware landscape shifted as a result? And how well are organizations adapting to today's threats?

There's good news in this year's findings: Ransomware attack frequency and success saw modest decreases. But as former US National Cyber Director and Semperis Strategic Advisor Chris Inglis told us, "Now is not the time for complacency. True regret isn't not knowing what you should have done; it's not having done what you knew was needed and had the means to do."

Organizations across the globe still see cyberattacks as the biggest threat to business resilience, and an increase in the frequency and sophistication of those attacks is their top cybersecurity concern. Fortunately, business leaders now seem to agree; lack of Board support for cybersecurity initiatives—the top challenge cited by respondents last year—dropped to last place in the list of this year's concerns.

What can organizations do to prepare for the new generation of AI-driven attacks? Our panel of experts weighs in on steps you can take today to reduce ransomware threats that exploit legacy vulnerabilities and the identity infrastructure—organizations' other two top cybersecurity concerns—while managing business resilience challenges, including regulatory compliance. We hope you find these tips useful in the continued fight against ransomware and other cyber threats.

For this report, we partnered with international research firm Censuswide, expanding the scope of our study to include **10 countries** and **8 industry sectors** across **North America, Europe, the United Kingdom, and Asia Pacific.** The ***2025 Ransomware Risk Report*** offers a more extensive view into the activity and business impact of ransomware around the world.

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.

"Paying ransoms should never be the default option. While some circumstances might leave the company in a no-choice situation, we should acknowledge that it's a downpayment on the next attack. Every dollar handed to ransomware gangs fuels their criminal economy, incentivizing them to strike again. The only real way to break the ransomware scourge is to invest in resilience, creating an option to not pay ransom."

Mickey Bresman
Semperis CEO

semperis

Key Findings

Adopting an assume breach mindset is still necessary.

78% of respondents were targeted by ransomware within the past 12 months. Of companies that were successfully attacked, 73% were attacked multiple times—31% three or more times.

Ransom payment and business disruptions are still cause for concern.

69% of successful attacks resulted in ransom payment; 55% paid multiple times. Ransom payments in the US increased over last year, with **81%** of organizations paying up. In addition, victims experienced **job and data losses** as well as **cybersecurity cancellation** or premium increases.

Identity infrastructure represents an area of opportunity for enhanced defense.

83% of attacks compromised the identity infrastructure. Yet many organizations still lack AD recovery plans and dedicated, AD-specific backup systems.

Attack sophistication and legacy vulnerabilities threaten cyber—and business—resilience.

50% of organizations cited cybersecurity threats as the top threat to business resilience. Despite a drop this year in ransomware attack frequency and success, increased frequency and sophistication of attacks were the top cybersecurity challenge for **37%** of respondents, followed closely by attacks against the identity infrastructure for **32%** of organizations.

Bad actors are finding new ways to force victims' hands.

47% of attacks leveraged threats to file regulatory complaints against the victims, while **40%** involved physical threats against staff.

Ransom payments do not guarantee recovery.

15% of ransomware victims that paid either did not receive decryption keys or received corrupted keys. An additional **3%** received usable keys but discovered that the attackers had published or otherwise illegally used their stolen data.

Note: Percentages represent average of responses

semperis

TABLE OF Contents

CONTRIBUTING EXPERTS

Jen Easterly
Former Director of the Cybersecurity and Infrastructure Agency (CISA)

Chris Inglis
Former US National Cyber Director
Semperis Strategic Advisor

Sanjay Poonen
Cohesity CEO

Malcolm Turnbull
Former Australian Prime Minister
Semperis Strategic Advisor

Mickey Bresman
Semperis CEO

Sean Deuby
Semperis Principal Technologist (Americas)

Guido Grillenmeier
Semperis Principal Technologist (EMEA)

Courtney Guss
Semperis Director of Crisis Management

Yossi Rachman
Semperis Director of Security Research

Jeff Wichman
Semperis Director of Incident Response

Are We Gaining Ground Against Ransomware?

Optimistic? Yes. Off the hook? Not even close.

Let's start with some (cautionary) good news: Globally, study respondents reported *slightly* fewer ransomware attacks than in the previous year. Still, a clear majority (**78%**) said they were targeted by ransomware during the past 12 months.

Clearly, an assume breach mindset is still necessary.

More mixed news: *Successful* attacks dropped to just over half (**56%**) of targeted organizations. However, **73%** of those victims suffered multiple attacks; **31%** were attacked three or more times. At least those organizations gained a little breathing space. Fewer respondents this year reported simultaneous or same-day attacks.

"If attackers start getting less money, they will adapt and pivot to something that can increase their profit margins. When ransom payments start going down, cyber criminals are going to adapt and figure out what will force companies to pay them."

Jeff Wichman
Semperis Director of Incident Response

This year's study also revealed a modest reduction in the number of organizations that paid ransom globally (**69%**) over the past year. But don't pop the champagne just yet: More than half (**55%**) of organizations that paid did so multiple times, with over one-quarter (**29%**) of those paying three or more times.

"Nation-state actors are often after intel. They aren't demanding ransom, they're learning your systems, your operation; they're monitoring data transactions. They're looking for your weak spots and ways to create the biggest impact. Intelligence-gathering missions are meant to go unnoticed."

Courtney Guss
Semperis Director of Crisis Management

Are ransomware attacks really decreasing?

"Improvements in procedures and tools that enable faster patching or that automate containment—including newly minted AI-based defense solutions—are making a positive impact," explains Yossi Rachman, Semperis Director of Security Research. "So, too, are large, successful law-enforcement campaigns against cybercrime rings. For example, Operation Cronos drastically disrupted LockBit operations. But even with financially motivated groups, we're also seeing attackers shift from a 'spray and pray' approach to high-value targets and deeper reconnaissance."

Even small reductions in ransomware frequency and success are encouraging. But now is not the time for complacency, warns Inglis.

"Organizational leadership has become more aware of their dependence on digital infrastructure," Inglis says. "That makes them more committed to inherent resilience, recovery, and response than they might have been before. That's good news. But I think that the people they rely on—the IT and cyber staff—would say that the environment is just as challenging. The attackers have not backed off. If we believe that we've whistled past the graveyard, we'll be in trouble."

In addition, we caution readers that fewer *ransomware* attacks do not necessarily equate with fewer attacks overall. As our experts noted in Semperis' report ***The State of Critical Infrastructure Resilience***, many cyberattacks—especially geopolitically motivated ones—aim to infiltrate rather than extort.

"Different attack groups are motivated by different goals," says Rachman. "Certain nation states, primarily those that are under international sanctions, see ransomware as a means to obtain funds. Others aim to create persistent access, taking a 'low and slow' approach to bide their time and create bridgeheads that enable them to disrupt the target's operations. And certain crime rings are motivated by financial gain but sponsored, or at least tacitly approved, by nation states that allow them to operate independently with the understanding that the attackers will also serve as an extension of their military operations if needed."

Ransomware, by its nature, is designed to make itself known to victims. After all, you need to know where and how to pay off the bad guys. In contrast, attacks that are designed to "live off the land" and establish persistence or exfiltrate sensitive data can be devilishly difficult to detect. Without sophisticated tools that provide extensive visibility and root out indicators of attack and compromise, such threats can lie in wait for many months.

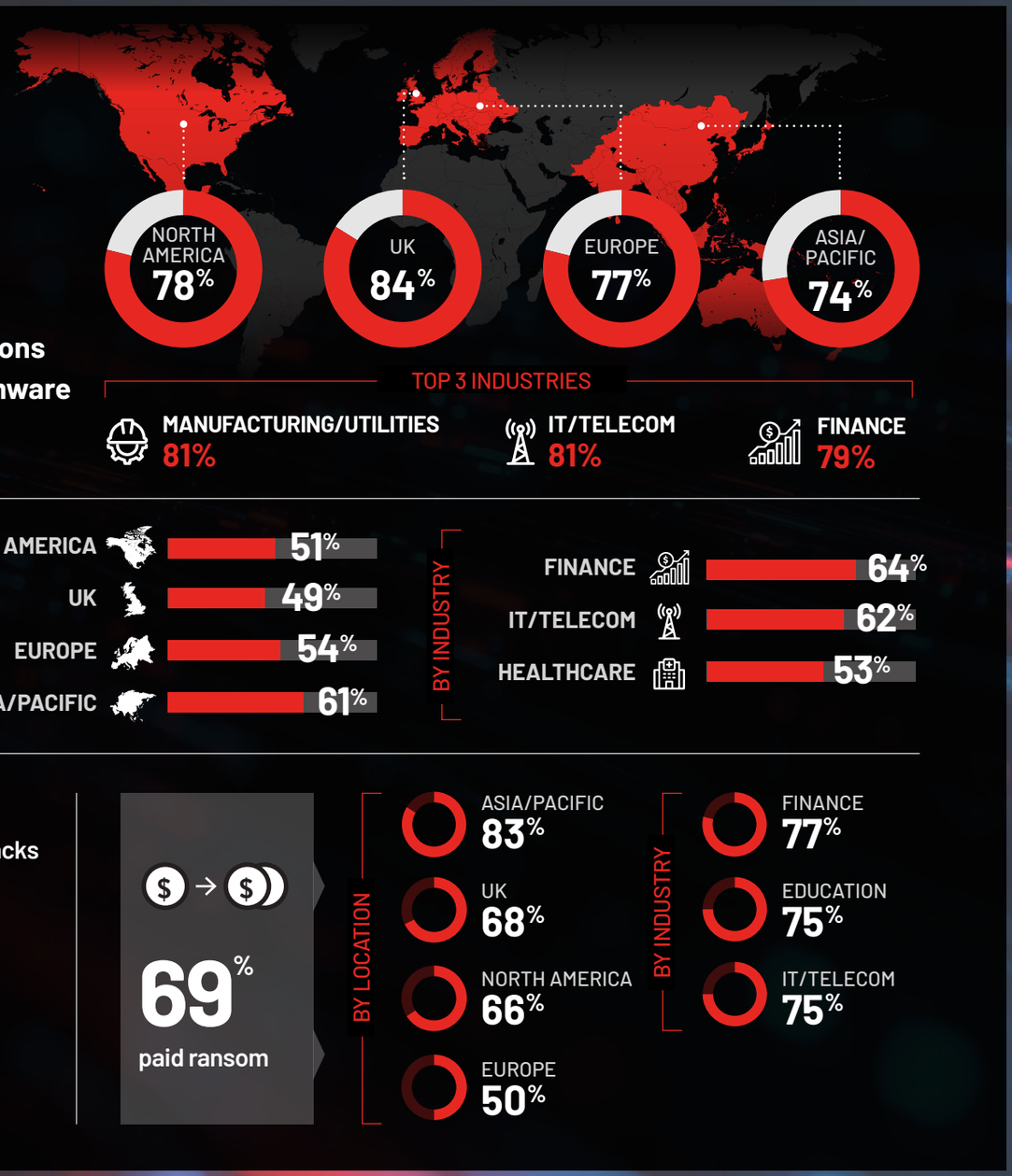
KEY TAKEAWAYS

Organizations in **Australia/New Zealand**, **Italy**, **Germany**, the **UK**, and the **US** **reported the highest rates of attack** (all over **81%**). A whopping **90%** of **German** respondents were targeted—an 8 percentage-point increase over last year. Among industries, **Manufacturing/Utilities** and **IT/Telecom** companies were most targeted (over **81%**).

Organizations in **Germany** (**66%**) and in the **Asia/Pacific region** (**61%**) were **most likely to be successfully attacked at least once.** Companies in the **US** and **Singapore**, as well as those in the **IT/Telecom** sector, were most likely to be successfully attacked 3+ times.

50% of multiple-attack victims in **Spain** were **attacked simultaneously or on the same day.** Companies in the **IT/Telecom** industry were more likely than other industries to experience the same.

Ransom payment rates *increased* in the US companies, hitting **81%**. Organizations in **Australia/New Zealand** and **Singapore** also reported higher than average payment rates, at **80%** and **85%**, respectively.



Getting Back to Business … Eventually

Despite gains in fending off attacks, business disruptions are continuous, persistent, and potentially life-threatening.

Although the global decrease in attack success is encouraging, it had a negligible effect on business disruption for our study respondents.

Even for those who paid ransom, those losses—**between $500,000 and $1,000,000 annually for 50%** and **over $1,000,000 for 8%** of study participants who paid—were just the tip of the iceberg. On average, **15%** of victims failed to receive usable decryption keys, even after paying ransom. Another **3%** discovered that attackers had published or illegally used their stolen data.

And as in last year's study, ransomware victims suffered a range of collateral damages. For many industries, those disruptions can be catastrophic. Recent attacks on healthcare organizations have resulted in patient deaths. And attacks that disrupt critical infrastructure could cause widespread chaos, damage, and human casualties.

Collateral expense, in the form of job losses, data compromise, and cyber insurance cancellation or price hikes topped respondents' concerns. For CISOs and other executives, the fallout from a successful (and expensive) attack often results in firing or retirement. For others, the cost of ransom payments can result in belt-tightening that forces staff layoffs.

Many companies suffered data loss or compromise, troubling given ransomware attackers' known tendency to use stolen data to launch additional exploits.

As for cyber insurance, "If you don't properly secure your environment, you're going to pay more for your insurance—or you're going to become uninsurable," warns Jeff Wichman, Semperis Director of Incident Response. To protect your investment, he says, "You need to determine what your weak spots are, think of different tactics that an attacker might throw at you, start building from there—and then test, test, test."

> "The most important thing that you can do to prevent yourself from falling victim to a ransomware attack is … to prepare your business for disruption: to have backups in place, to ensure that your technology is as secure as possible, that you've implemented multi-factor authentication, that you've patched your internet-facing devices."
>
> **Jen Easterly**
> Former Director of CISA

Another worrying bit of news: Organizations were slower to recover from attacks this year. Less than one quarter (**23%**) were able to recover within a day, compared with 39% last year. And **18%** needed between one week and one month, compared with just 11% in 2024.

"Protection does have an impact at reducing the likelihood of ransomware success," says Guido Grillenmeier, Semperis Principal Technologist (EMEA), "but being well-prepared for recovery is necessary to maintain business continuity and resilience. And during recovery, until you get your identities back, you can't get anything else back."

"Once attackers access your data, the trust is broken. You can't be sure it won't be misused later, through extortion, resale, or strategic leaks. That's why prevention is key. Organizations must prioritize tools and controls that stop attackers from moving laterally, escalating privileges after an initial breach. Protecting sensitive data at every level is essential to maintaining business continuity, reputation, and customer trust."

Sanjay Poonen
Cohesity CEO

KEY TAKEAWAYS

Brand damage was a top disruption for organizations in **North America**, **Italy**, **Spain**, and **Singapore**, as well as those in **Government** and **Healthcare**.

Organizations in **Germany** and the **UK** and in the **Education**, **Energy**, **Manufacturing/Utilities**, and **Travel/Transportation** sectors all rated **revenue loss** as a top ransomware-related disruption.

30% of UK organizations needed between 1 week and 1 month to resume normal business operations. This region also saw the biggest drop (28 percentage points) in same-day recovery. Organizations in **Government** and **Healthcare** took the longest to resume operations. **Healthcare** also saw a 28-percentage-point drop in same-day recovery.

Over 20% of ransomware victims **failed to receive usable decryption keys** in **Germany**, **Canada**, and **Australia/New Zealand**, as well as in the **Manufacturing/Utilities** sector.

Total annual ransom paid

42% paid **$500,000** or less

50% paid **$500,000-$1M**

8% paid more than **$1M**

BY COUNTRY
- SINGAPORE 21%
- US 11%

BY INDUSTRY
- IT/TELECOM 14%
- GOVERNMENT 12%

Top 3 ransomware-related business disruptions

62% Job losses

61% Data breach

46% Cyber coverage disruption

Time needed to return to normal operations

23% less than 1 day

58% 1 day-1 week

18% 1 week-1 month

BY COUNTRY
- UK 30%
- FRANCE 26%

BY INDUSTRY
- GOVERNMENT 43%
- HEALTHCARE 31%

Identity at the Heart of Defense—and Recovery

Ready or not? ITDR efforts are widespread, but gaps remain.

More than three-quarters (**83%**) of study participants told us that attacks—regardless of entry point or level of success—compromised their identity systems. No surprises here; infiltrating Active Directory (AD), Entra ID, or Okta enables attackers to establish persistence, move laterally, and elevate privileges for greater reach once in the environment. With threat actors targeting the identity and access management (IAM) infrastructure itself, and credential abuse ranking as a top attack vector, organizations must strengthen their IAM defenses to stay ahead of attackers.

"Identity is a core, foundational piece of your infrastructure that underpins every other function," explains Cohesity CEO Sanjay Poonen. "The ability to recover identity to a trustworthy state is paramount, and every other piece of recovery builds from there—including data security and the ability to keep attackers from gaining a stronger foothold and accessing not just data but other Tier 0 resources."

Many organizations now understand that identity security and resilience are foundational to cyber and business resilience. Yet despite **90%** of respondents telling us that they have implemented an Identity Threat Detection and Response (ITDR) strategy, a much smaller percentage (just **66%**) include AD recovery procedures in their disaster recovery plan, and only **60%** maintain dedicated, AD-specific backup systems—both key parts of effective ITDR. That's a gap that attackers will be more than happy to exploit.

How can organizations successfully combat identity-related ransomware threats to build operational resilience?

"As with any cybersecurity effort, it boils down to a combination of people, processes, and technology," says Sean Deuby, Semperis Principal Technologist (Americas). "In terms of people, you need cybersecurity training at every level and in every department. Everybody needs to know their part and what to do. And in terms of processes, you can start by calculating your *minimum viable company*, establishing isolated recovery environments, network segmentation, identity recovery, and having a customized, documented, and practiced crisis response plan."

Courtney Guss, Semperis Director of Crisis Management, notes the importance of identifying your core digital capabilities. "When you have identified your minimum viable services—the things needed to keep the business operational, the lights on, and the doors open—you can focus on restoring and recovering those systems, then spend time fixing the rest. Not everything needs to be fixed in the first 24 hours."

But during recovery, until you get your identities back, you can't get anything else back.

"Too often, organizations miss bad actors within the environment because it just looks like normal activity," says Guss. "Managing critical vulnerabilities or known vulnerabilities can be time-consuming, but you wouldn't leave your car unlocked. Too often, critical operating systems and applications aren't just left unlocked, the key is left in the ignition. That's where identity and access control come in."

"Active Directory is obviously a key vector for attack. If you have been breached, the ability to restore the integrity of your Active Directory, very quickly, is paramount."

Malcolm Turnbull
Former Australian Prime Minister and Semperis Strategic Advisor

KEY TAKEAWAYS

93% of organizations in **Asia/Pacific** experienced **identity-infrastructure compromise**, as did **89%** of **Canadian** organizations and **87%** of companies in the **IT/Telecom** sector.

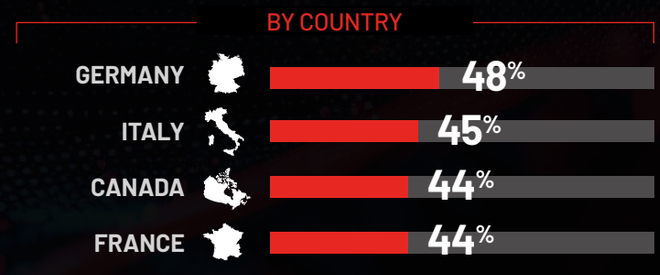
Organizations in **Germany**—**most likely to be attacked and to be attacked successfully**—had the smallest increase (just 2 percentage points) in dedicated, AD-specific backup systems and were least likely of all countries (**52%**) to maintain such systems. Only **52%** have an AD recovery plan—again, the least of all countries. Companies in the **IT/Telecom**, **Travel/Transportation**, and **Finance** sectors were least likely to maintain dedicated, AD-specific backup systems. In **Singapore** and in the **Energy** sector, **69%** of organizations maintain such systems—the most of any country or industry.

76% of **UK** organizations and **71%** of **Spanish** **organizations have an AD recovery plan.** So do **77%** of **Government** organizations and **74%** of companies in the **Energy** sector.

of organizations experienced identity-infrastructure compromise

Only 66% of organizations maintain an AD recovery plan

40% of organizations still do not maintain dedicated, AD-specific backup systems



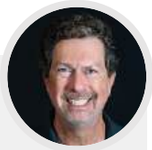
Meeting the Moment

Where Do We Go from Here?

Cybersecurity experts offer advice for meeting top challenges to resilience.

Despite the positive trends we see in this year's study, organizations still view cyberattacks as the biggest threat to their business and operational resilience. And they view the frequency and complexity of those attacks, along with threats to the identity infrastructure and vulnerabilities posed by legacy systems and years of technological debt, as their biggest cybersecurity challenges.

So, what can organizations do over the coming year to build on successes and increase their resilience against ransomware?



"Successful cyber defense, response, and recovery depends on a combination of people, processes, and technology. The *people* part of that equation is just as critical as the other parts."

Sean Deuby
Semperis Principal Technologist (Americas)

"With the introduction of generative AI and the fast development of agentic AI attacks, creating more advanced tools with more destructive impact is easier, so threat actors no longer need a lot of money and resources to create those tools. As a result, even a drop in ransom payments will not necessarily stop attack groups from proliferating and conducting more effective and frequent attacks."

Yossi Rachman
Semperis Director of Security Research

Commit to a culture of resilience

Long-term reductions in ransomware risk demand a proactive dedication to resilience, not just once or within the IT or cybersecurity departments, but continuously and throughout the organization.

"Whatever advantage transgressors might have, you can take away," says Inglis. "If they form syndicates and come at you from all sides, become part of a coalition of defense. If they take advantage of weaknesses in your security skills, processes, or technical architecture, bolster those areas. If they use generative AI to come at you faster, implement automation in recovery or defense. If they can lock down your primary store, maintain effective backup and recovery solutions.

"Make the necessary investments to have appropriate resilience. Vigorously understand how your architecture is used so that you can detect a transgression at the earliest possible moment, bring a coalition to bear, and have backups so that you can respond and recover.

"Take away attackers' advantages. Any number of companies do. They're the ones that you don't hear about in the news."

MEETING THE MOMENT: WHERE DO WE GO FROM HERE?

1. Prepare for changing tactics in ransomware development and deployment.

Ransomware (and other cyber threats) clearly aren't going away. Tightening defenses by addressing vulnerabilities and improving the ability to recover your environment are key steps in being able to say "no" to ransom demands.

But as attack success and companies' willingness to pay ransom decreases, bad actors are finding new ways to force victims' hands. Aside from receiving traditional threats such as system lockouts (**52%**) and data destruction (**63%**), nearly half (**47%**) the organizations in this year's study reported that attackers threatened to file regulatory complaints against them; **40%** received physical threats. Rachman notes that some ransomware gangs might also be changing tactics to "take their time to map out and compromise the most critical business assets, so the chances of their targets paying up will be maximized when they finally decide to shut things down."

Ensuring that your organization is meeting regulatory cybersecurity requirements can help to defang complaints. And implementing solutions that are adept at identifying back doors and intruder perseverance can help you locate and evict hidden attackers.

In addition, the proliferation of generative AI has lowered the bar of entry for new attackers.

"The introduction of generative AI is a boon for bad actors as well as defenders," explains Rachman, "enabling them to create and evolve attack tools at a far greater velocity than ever before. Nowadays, even a technical beginner can write and improve their own string of ransomware. That has created a sort of democratization of ransomware-development capability, which will likely translate to many more incidents than we've seen in the past."

To combat these new capabilities, look for opportunities to automate defense, response, and recovery functions. AI- and ML-powered automation can help speed the process of identifying indicators of compromise or exposure, detecting intruders, notifying security staff of suspicious activity, and even recovering compromised systems.

2. Implement the right technology to protect IAM infrastructure—the #1 target.

Simplifying and consolidating technology deployments are understandable goals for most companies. So are cost savings. But as ITDR becomes widely adopted and vendors roll out new offerings, determining which tools are the most effective—and balancing that efficacy with legitimate cost and complexity concerns—is critical.

"You can't simply bolt on identity security," warns Inglis, "because it is core to business operations and critical to sustain defense against sophisticated and motivated nation state-backed threat groups. Like business resilience, identity resilience must be addressed at the core."

To ensure the integrity of your IAM infrastructure, Gartner emphasizes the need for a granular "govern, identify, detect, respond, and recover loop."[1] As you evaluate your ITDR maturity and ransomware readiness, ask questions like:

- Do I know if my hybrid AD is compromised?
- How quickly can I detect and contain an identity-based attack?
- Can I recover AD and Entra ID—quickly, cleanly, and confidently?
- Can I get my IAM infrastructure back to a **trustworthy** state?

1 Gartner. "Hype Cycle for Security Operations, 2025." June 23, 2025.

3. Document, train, and test to improve ransomware response.

Identifying the right technology is only one part of a successful equation for business resilience. Organizations from several countries and industries in this year's study listed a lack of experienced personnel or employee training as top challenges. And as discussed in Semperis' report *The State of Enterprise Cyber Crisis Readiness*, truly effective crisis response and recovery processes are customized, well-documented, clearly communicated, and practiced in test scenarios that mirror the real world.

"Train for the day you are attacked," advises Rachman. "See that everybody knows exactly what they should do, which systems, processes, and tools need to be involved, and do that every six months. Focus on different stakeholders each time. Do an exercise for the executive level, an exercise for the managers, an exercise for the security practitioners and other technical practitioners."

4. Evaluate the security of partners and supply chain vendors.

Confident that you've done everything you can to lock down cybersecurity and improve ransomware resilience? You must still consider potential vulnerabilities in your supply chain, partners, or vendors that have access to sensitive systems and assets—even potential merger or acquisition targets.

"You might have very good security," notes Malcolm Turnbull, former Australian Prime Minister and Semperis Strategic Advisor. "But what about the law firms you deal with? The accounting firms? There are a whole number of trusted consultants that have got access to things that can make you vulnerable."

Depending on your industry, managing such third-party risk might also be a required part of regulatory compliance. For example, certain organizations working within or for the financial sector in the European Union (EU) must comply with the EU's Digital Operational Resilience Act (DORA) requirements for third-party risk management.

Require partners, suppliers, and any third party that has access to your environment to meet the same standards of defense and resilience as your organization.

KEY TAKEAWAYS

Organizations in **Canada** and **France** and in the **Energy** sector all cited **lack of experienced personnel** as a top challenge to business resilience; in the **Government** sector, it was a top cybersecurity concern. Organizations in **Australia/New Zealand** and in the **Travel/Transportation** sector cited **lack of employee training** as a primary threat to business resilience as well as a top cybersecurity challenge in the **Energy** sector.

Outdated/legacy systems were noted as a top threat to business resilience by organizations in **Canada** and **Germany** and in the **Education**, **Energy**, **Government**, **Healthcare**, and **Manufacturing/Utilities** sectors.

Regulatory compliance was cited as a top cybersecurity challenge by organizations in the **UK** and **France** and in the **Finance** and **Healthcare** sectors.

Organizations in **Singapore** and in the **Education**, **Government**, and **Travel/Transportation** sectors noted cybersecurity challenges related to **budget cuts.**

Organizations in **Italy** listed **geopolitical threats** as top cybersecurity challenges.

Top three challenges

	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1	Cybersecurity threats	Sophisticated and frequent threats
2	Cybersecurity regulations	Identity system attacks
3	Budget constraints	Legacy systems and technical debt

APPENDIX

Ransomware Risk

by Country and Industry

US Ransomware Risk

81% were targeted by ransomware in the **past 12 months**

59% of attacks succeeded

- 1X 17%
- 2X 43%
- 3X 25%
- 4+X 15%

Average time between attacks

- 23% simultaneous
- 14% less than 1 day
- 38% 1-6 days
- 23% 7-29 days
- 3% 1+ month

81% paid ransom

- 1X 42%
- 2X 35%
- 3X 15%
- 4+X 8%

Total annual ransom paid

- **38%** paid **$500,000** or less
- **51%** paid **$500,000-$1M**
- **11%** paid more than **$1M**

83% said the attack **compromised their identity infrastructure**

62% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 67%
- ENTRA ID 55%
- OKTA 42%

Time to return to normal operations

- 19% less than 1 day
- 62% 1 day-1 week
- 20% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Job losses	2 Cybersecurity regulations	2 Identity system attacks
3 Brand damage	3 Budget constraints	3 Legacy systems and technical debt

Note: Percentages represent average of responses

CANADA Ransomware Risk

64% were targeted by ransomware in the **past 12 months**

44% of attacks succeeded

- 1X 32%
- 2X 50%
- 3X 14%
- 4+X 4%

Average time between attacks

- 21% simultaneous
- 21% less than 1 day
- 32% 1-6 days
- 11% 7-29 days
- 16% 1+ month

50% paid ransom

- 1X 71%
- 2X 21%
- 3X 7%
- 4+X 0%

Total annual ransom paid

- **36%** paid **$500,000** or less
- **57%** paid **$500,000-$1M**
- **7%** paid more than **$1M**

89% said the attack **compromised their identity infrastructure**

56% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 53%
- ENTRA ID 54%
- OKTA 47%

Time to return to normal operations

- 27% less than 1 day
- 73% 1 day-1 week
- 0% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Brand damage	2 Outdated systems	2 Legacy systems and technical debt
3 Cyber insurance cost/ cancellation	3 Cybersecurity regulations and talent shortage	3 Identity system attacks

Note: Percentages represent average of responses

UK Ransomware Risk

84% were targeted by ransomware in the **past 12 months**

49% of attacks succeeded

- 1X 18%
- 2X 51%
- 3X 22%
- 4+X 10%

Average time between attacks

- 20% simultaneous
- 12% less than 1 day
- 37% 1-6 days
- 24% 7-29 days
- 8% 1+ month

68% paid ransom

- 1X 43%
- 2X 49%
- 3X 5%
- 4+X 3%

Total annual ransom paid

- **41%** paid **$500,000** or less
- **56%** paid **$500,000-$1M**
- **3%** paid more than **$1M**

79% said the attack **compromised their identity infrastructure**

60% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 76%
- ENTRA ID 56%
- OKTA 33%

Time to return to normal operations

- 9% less than 1 day
- 61% 1 day-1 week
- 30% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Loss of revenue	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Cyber insurance cost/ cancellation	2 Cybersecurity regulations	2 Identity system attacks
3 Data breach	3 Budget constraints	3 Legacy systems, technical debt, and regulatory compliance

Note: Percentages represent average of responses

FRANCE Ransomware Risk

74% were targeted by ransomware in the **past 12 months**

52% of attacks succeeded

- 1X — 52%
- 2X — 31%
- 3X — 8%
- 4+X — 8%

Average time between attacks

- 9% simultaneous
- 26% less than 1 day
- 48% 1-6 days
- 17% 7-29 days
- 0% 1+ month

54% paid ransom

- 1X — 46%
- 2X — 38%
- 3X — 8%
- 4+X — 8%

Total annual ransom paid

- **42%** paid **$500,000** or less
- **50%** paid **$500,000-$1M**
- **8%** paid more than **$1M**

78% said the attack **compromised their identity infrastructure**

56% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD — 70%
- ENTRA ID — 57%
- OKTA — 35%

Time to return to normal operations

- 24% less than 1 day
- 50% 1 day-1 week
- 26% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Data breach	2 Budget constraints	2 Identity system attacks
3 Cyber insurance cost/ cancellation	3 Talent shortage	3 Regulatory compliance

Note: Percentages represent average of responses

GERMANY Ransomware Risk

90% were targeted by ransomware in the **past 12 months**

66% of attacks succeeded

- 1X 44%
- 2X 39%
- 3X 13%
- 4+X 4%

Average time between attacks

- 5% simultaneous
- 26% less than 1 day
- 31% 1-6 days
- 36% 7-29 days
- 2% 1+ month

53% paid ransom

- 1X 73%
- 2X 25%
- 3X 3%
- 4+X 0%

Total annual ransom paid

- **53%** paid **$500,000** or less
- **45%** paid **$500,000-$1M**
- **3%** paid more than **$1M**

84% said the attack **compromised their identity infrastructure**

52% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 52%
- ENTRA ID 50%
- OKTA 42%

Time to return to normal operations

- 34% less than 1 day
- 50% 1 day-1 week
- 16% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Cyber insurance cost/ cancellation	1 Cybersecurity threats	1 Identity system attacks
2 Loss of revenue	2 Cybersecurity regulations	2 Sophisticated and frequent threats
3 Data breach	3 Outdated systems	3 Legacy systems and technical debt

Note: Percentages represent average of responses

SPAIN Ransomware Risk

59% were targeted by ransomware in the **past 12 months**

56% of attacks succeeded

- 1X 39%
- 2X 52%
- 3X 6%
- 4+X 3%

Average time between attacks

- 20% simultaneous
- 30% less than 1 day
- 35% 1-6 days
- 15% 7-29 days
- 0% 1+ month

52% paid ransom

- 1X 47%
- 2X 47%
- 3X 6%
- 4+X 0%

Total annual ransom paid

- **53%** paid **$500,000** or less
- **47%** paid **$500,000-$1M**
- **0%** paid more than **$1M**

85% said the attack **compromised their identity infrastructure**

59% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 71%
- ENTRA ID 55%
- OKTA 50%

Time to return to normal operations

- 16% less than 1 day
- 68% 1 day-1 week
- 16% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Identity system attacks
2 Cyber insurance cost/ cancellation	2 Talent shortage	2 Sophisticated and frequent attacks
3 Brand damage	3 Budget constraints	3 Legacy systems and technical debt

Note: Percentages represent average of responses

ITALY Ransomware Risk

82% were targeted by ransomware in the **past 12 months**

42% of attacks succeeded

- 1X 50%
- 2X 32%
- 3X 15%
- 4+X 3%

Average time between attacks

- 12% simultaneous
- 18% less than 1 day
- 29% between 1-6 days
- 41% between 7-29 days
- 0% 1+ month

41% paid ransom

- 1X 79%
- 2X 21%
- 3X 0%
- 4+X 0%

Total annual ransom paid

- **36%** paid **$500,000** or less
- **64%** paid **$500,000-$1M**
- **0%** paid more than **$1M**

56% said the attack **compromised their identity infrastructure**

55% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 59%
- ENTRA ID 47%
- OKTA 26%

Time to return to normal operations

- 45% less than 1 day
- 55% 1 day-1 week
- 0% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Brand damage	2 Cybersecurity regulations	2 Geopolitical threats
3 Data breach	3 Budget constraints	3 Legacy systems and technical debt

Note: Percentages represent average of responses

SINGAPORE Ransomware Risk

61% were targeted by ransomware in the **past 12 months**

61% of attacks succeeded

- 1X 22%
- 2X 35%
- 3X 26%
- 4+X 17%

Average time between attacks

- 14% simultaneous
- 17% less than 1 day
- 50% 1-6 days
- 19% 7-29 days
- 0% 1+ month

85% paid ransom

- 1X 41%
- 2X 31%
- 3X 18%
- 4+X 10%

Total annual ransom paid

- **49%** paid **$500,000** or less
- **31%** paid **$500,000-$1M**
- **21%** paid more than **$1M**

93% said the attack **compromised their identity infrastructure**

69% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 70%
- ENTRA ID 62%
- OKTA 58%

Time to return to normal operations

- 30% less than 1 day
- 48% 1 day-1 week
- 22% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Budget cuts
2 Data breach	2 Cybersecurity regulations	2 Sophisticated and frequent threats
3 Brand damage	3 Budget constraints	3 Identity system attacks

Note: Percentages represent average of responses

AUSTRALIA/NEW ZEALAND Ransomware Risk

83% were targeted by ransomware in the **past 12 months**

62% of attacks succeeded

- 1X 19%
- 2X 41%
- 3X 28%
- 4+X 12%

Average time between attacks

- 12% simultaneous
- 13% less than 1 day
- 34% 1-6 days
- 40% 7-29 days
- 1% 1+ month

80% paid ransom

- 1X 28%
- 2X 56%
- 3X 13%
- 4+X 2%

Total annual ransom paid

- **41%** paid **$500,000** or less
- **55%** paid **$500,000-$1M**
- **4%** paid more than **$1M**

93% said the attack **compromised their identity infrastructure**

62% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 64%
- ENTRA ID 59%
- OKTA 50%

Time to return to normal operations

- 30% less than 1 day
- 58% 1 day-1 week
- 11% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Data breach	2 Cybersecurity regulations	2 Legacy systems and technical debt
3 Cyber insurance cost/ cancellation	3 Employee training gap	3 Identity system attacks

Note: Percentages represent average of responses

EDUCATION Ransomware Risk

61% were targeted by ransomware in the **past 12 months**

49% of attacks succeeded

- 1X 38%
- 2X 44%
- 3X 13%
- 4+X 6%

Average time between attacks

- 5% simultaneous
- 25% less than 1 day
- 30% 1-6 days
- 40% 7-29 days
- 0% 1+ month

59% paid ransom

- 1X 47%
- 2X 42%
- 3X 11%
- 4+X 0%

Total annual ransom paid

- **63%** paid **$500,000** or less
- **37%** paid **$500,000-$1M**
- **0%** paid more than **$1M**

82% said the attack **compromised their identity infrastructure**

60% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 72%
- ENTRA ID 60%
- OKTA 45%

Time to return to normal operations

- 31% less than 1 day
- 50% 1 day-1 week
- 19% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Outdated systems	1 Sophisticated and frequent threats
2 Cyber insurance cost/ cancellation	2 Budget constraints	2 Budget cuts
3 Loss of revenue	3 Cybersecurity threats	3 Identity system attacks

Note: Percentages represent average of responses

ENERGY Ransomware Risk

78% were targeted by ransomware in the **past 12 months**

48% of attacks succeeded

- 1X — 40%
- 2X — 45%
- 3X — 10%
- 4+X — 5%

Average time between attacks

- 8% simultaneous
- 25% less than 1 day
- 50% 1-6 days
- 17% 7-29 days
- 0% 1+ month

75% paid ransom

- 1X — 53%
- 2X — 47%
- 3X — 0%
- 4+X — 0%

Total annual ransom paid

- 40% paid **$500,000** or less
- 60% paid **$500,000-$1M**
- 0% paid more than **$1M**

81% said the attack **compromised their identity infrastructure**

69% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD — 74%
- ENTRA ID — 69%
- OKTA — 59%

Time to return to normal operations

- 29% less than 1 day
- 65% 1 day-1 week
- 6% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Loss of revenue	2 Talent shortage	2 Legacy systems and technical debt
3 Job losses	3 Outdated systems	3 Employee training gap

Note: Percentages represent average of responses

FINANCE Ransomware Risk

79% were targeted by ransomware in the **past 12 months**

64% of attacks succeeded

- 1X 26%
- 2X 50%
- 3X 18%
- 4+X 6%

Average time between attacks

- 11% simultaneous
- 15% less than 1 day
- 45% 1-6 days
- 26% 7-29 days
- 3% 1+ month

77% paid ransom

- 1X 48%
- 2X 43%
- 3X 6%
- 4+X 4%

Total annual ransom paid

- **43%** paid **$500,000** or less
- **54%** paid **$500,000-$1M**
- **4%** paid more than **$1M**

85% said the attack **compromised their identity infrastructure**

59% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 65%
- ENTRA ID 51%
- OKTA 40%

Time to return to normal operations

- 23% less than 1 day
- 59% 1 day-1 week
- 18% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Data breach	2 Cybersecurity regulations	2 Identity system attacks
3 Cyber insurance cost/ cancellation	3 Budget constraints	3 Legacy systems, technical debt, and regulatory compliance

Note: Percentages represent average of responses

GOVERNMENT Ransomware Risk

67% were targeted by ransomware in the **past 12 months**

33% of attacks succeeded

- 1X 43%
- 2X 29%
- 3X 14%
- 4+X 14%

Average time between attacks

- 13% simultaneous
- 0% less than 1 day
- 50% 1-6 days
- 25% 7-29 days
- 13% 1+ month

57% paid ransom

- 1X 50%
- 2X 38%
- 3X 0%
- 4+X 13%

Total annual ransom paid

- **38%** paid **$500,000** or less
- **50%** paid **$500,000-$1M**
- **13%** paid more than **$1M**

58% said the attack **compromised their identity infrastructure**

67% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 77%
- ENTRA ID 44%
- OKTA 27%

Time to return to normal operations

- 0% less than 1 day
- 57% 1 day-1 week
- 43% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Brand damage	2 Budget constraints	2 Budget cuts
3 Cyber insurance cost/ cancellation	3 Outdated systems	3 Talent shortage

Note: Percentages represent average of responses

HEALTHCARE Ransomware Risk

77% were targeted by ransomware in the **past 12 months**

53% of attacks succeeded

- 1X 40%
- 2X 42%
- 3X 13%
- 4+X 5%

Average time between attacks

- 12% simultaneous
- 14% less than 1 day
- 35% 1-6 days
- 30% 7-29 days
- 9% 1+ month

53% paid ransom

- 1X 61%
- 2X 24%
- 3X 11%
- 4+X 5%

Total annual ransom paid

- **55%** paid **$500,000** or less
- **39%** paid **$500,000-$1M**
- **5%** paid more than **$1M**

78% said the attack **compromised their identity infrastructure**

61% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 67%
- ENTRA ID 58%
- OKTA 50%

Time to return to normal operations

- 17% less than 1 day
- 52% 1 day-1 week
- 31% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Brand damage	2 Cybersecurity regulations	2 Identity system attacks
3 Job losses	3 Outdated systems	3 Regulatory compliance

Note: Percentages represent average of responses

IT/TELECOMMUNICATIONS Ransomware Risk

81% were targeted by ransomware in the **past 12 months**

62% of attacks succeeded

- 1X 18%
- 2X 40%
- 3X 24%
- 4+X 18%

Average time between attacks

- 28% simultaneous
- 16% less than 1 day
- 33% 1-6 days
- 21% 7-29 days
- 3% 1+ month

75% paid ransom

- 1X 43%
- 2X 38%
- 3X 12%
- 4+X 6%

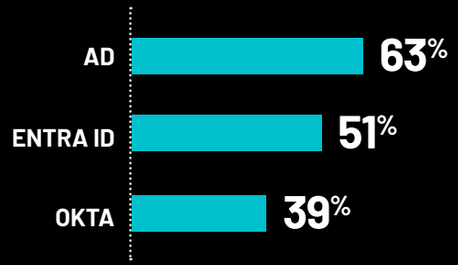
Total annual ransom paid

- **39%** paid **$500,000** or less
- **48%** paid **$500,000-$1M**
- **14%** paid more than **$1M**

87% said the attack **compromised their identity infrastructure**

57% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan



Time to return to normal operations

- 26% less than 1 day
- 56% 1 day-1 week
- 18% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Identity system attacks
2 Data breach	2 Cybersecurity regulations	2 Sophisticated and frequent threats
3 Cyber insurance cost/ cancellation	3 Budget constraints	3 Legacy systems and technical debt

Note: Percentages represent average of responses

MANUFACTURING/UTILITIES Ransomware Risk

81% were targeted by ransomware in the **past 12 months**

50% of attacks succeeded

- 1X 29%
- 2X 39%
- 3X 25%
- 4+X 8%

Average time between attacks

- 11% simultaneous
- 18% less than 1 day
- 38% 1-6 days
- 31% 7-29 days
- 2% 1+ month

63% paid ransom

- 1X 35%
- 2X 41%
- 3X 18%
- 4+X 6%

Total annual ransom paid

- **34%** paid **$500,000** or less
- **61%** paid **$500,000-$1M**
- **5%** paid more than **$1M**

83% said the attack **compromised their identity infrastructure**

61% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 65%
- ENTRA ID 61%
- OKTA 42%

Time to return to normal operations

- 21% less than 1 day
- 63% 1 day-1 week
- 16% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Data breach	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Loss of revenue	2 Cybersecurity regulations	2 Legacy systems and technical debt
3 Job losses	3 Outdated systems	3 Identity system attacks

Note: Percentages represent average of responses

TRAVEL/TRANSPORTATION Ransomware Risk

71% were targeted by ransomware in the **past 12 months**

50% of attacks succeeded

- 1X 39%
- 2X 31%
- 3X 26%
- 4+X 4%

Average time between attacks

- 7% simultaneous
- 21% less than 1 day
- 21% 1-6 days
- 50% 7-29 days
- 0% 1+ month

65% paid ransom

- 1X 33%
- 2X 53%
- 3X 13%
- 4+X 0%

Total annual ransom paid

- **60%** paid **$500,000** or less
- **33%** paid **$500,000-$1M**
- **7%** paid more than **$1M**

80% said the attack **compromised their identity infrastructure**

57% maintain dedicated, **AD-specific backup systems**

Have an identity system recovery plan

- AD 66%
- ENTRA ID 57%
- OKTA 43%

Time to return to normal operations

- 15% less than 1 day
- 69% 1 day-1 week
- 15% 1 week-1 month

Top concerns and challenges

DISRUPTIONS EXPERIENCED	BUSINESS RESILIENCE CHALLENGES	CYBERSECURITY CHALLENGES
1 Job losses	1 Cybersecurity threats	1 Sophisticated and frequent threats
2 Data breach	2 Cybersecurity regulations	2 Identity system attacks
3 Loss of revenue	3 Budget constraints and talent shortage	3 Budget cuts and talent shortage

Note: Percentages represent average of responses

METHODOLOGY

In the first half of 2025, global organizations across North America, the United Kingdom, Europe, and the Asia Pacific region participated in the 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 1,500 IT and security professionals across multiple industries, including education, finance, healthcare, government, energy, manufacturing and utilities, IT and telecommunications, and travel and transportation.

HOW TO CITE INFORMATION IN THIS REPORT

The data in this report are provided as a resource for the cybersecurity community and the organizations it serves. Semperis encourages you to share our findings. To cite statistics or insights, refer to *Semperis 2025 Ransomware Risk Report* and include a link to the full report, which is available for download at https://www.semperis.com/ransomware-risk-report. To interview Semperis experts, contact Bill Keeler at billk@semperis.com. Lastly, we'd love to hear your questions or thoughts on ransomware and resilience. Find Semperis on LinkedIn.

ABOUT SEMPERIS

Semperis protects critical enterprise identity services for security teams charged with defending hybrid and multi-cloud environments. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' AI-powered technology protects over 100 million identities from cyberattacks, data breaches, and operational errors.

As part of its mission to be a force for good, Semperis offers a variety of cyber community resources, including the award-winning Hybrid Identity Protection (HIP) Conference, HIP Podcast, and free identity security tools Purple Knight and Forest Druid. Semperis is a privately owned, international company headquartered in Hoboken, New Jersey, supporting the world's biggest brands and government agencies, with customers in more than 40 countries.

Learn more: https://www.semperis.com

+1-703-918-4884 | info@semperis.com | www.semperis.com
5 Marine View Plaza, Suite 102, Hoboken, NJ 07030