2025 Ransomware Holiday Risk Report

- The majority of ransomware attacks continue to occur over weekends or holidays; an even larger share occurs following an M&A.
- In-house SOCs surge, but most organizations still slash staffing by 50% or more during high-risk periods.
- ITDR strategies and identity vulnerability detection see wide adoption, but remediation and recovery capabilities are often lacking.

"If you are not thinking about your infrastructure and protecting your infrastructure, which includes identity systems ... I don't know what to say. There's no other starting point."

Heather Costa

Mayo Clinic Director of Technology Resilience

semperis

The Balancing Act: Risk vs Resilience

A proactive approach to identity threats can help leaders weigh ransomware risk against staffing and resource concerns.

Building business resilience requires an often complex calculation of cyber threat risk and a balance between mitigating that risk, conserving resources, and retaining security personnel. Understanding when ransomware is most likely to strike and how attackers seek to infiltrate your environment is an important factor in the success of these efforts.

The ***2025 Ransomware Holiday Risk Report*** analyzes responses from **10 countries** and **8 industry sectors** across **North America, Europe, the United Kingdom, and Asia Pacific**, gathered in partnership with international research firm Censuswide. The report offers insight into ransomware attack behavior and defense trends and recommends steps that organizations can take to strengthen their cybersecurity preparedness. Share these findings **with your IT, security, and business stakeholders, and leverage the expert insights to improve your cyber crisis response planning.**

"We need to focus on resilience and how to keep the business running while we're being attacked. We need to proceed in the assumption that we've been compromised ... how do we keep the business resilient?"

Sean Deuby
Semperis Principal Technologist (Americas)

KEY FINDINGS

Most attacks occur during times of distraction or disruption

of reported ransomware attacks within the past 12 months occurred on a weekend or holiday; **60%** of attacks followed a material event such as a merger, acquisition, or round of layoffs.

SOCs move in-house but continue to slash off-hours staffing

of surveyed organizations that maintain a security operations center (SOC) say they now do so internally; **78%** of respondents with a SOC cut staffing by **50% or more** during weekends and holidays.

Identity security plans lack remediation and recovery capabilities

of respondents say they have solutions and procedures in place to detect identity system vulnerabilities, but only **45%** have vulnerability remediation procedures and only **63%** automate identity system recovery.

TABLE OF Contents

CONTRIBUTING EXPERTS

Heather Costa
Mayo Clinic Director of Technology Resilience

Simon Hodgkinson
Former bp CISO | Semperis Strategic Advisor

Chris Inglis
Former US National Cyber Director | Semperis Strategic Advisor

Malcolm Turnbull
Former Australian Prime Minister | Semperis Strategic Advisor

Sean Deuby
Semperis Principal Technologist (Americas)

James Doggett
Semperis CISO

Courtney Guss
Semperis Director of Crisis Management

Jeff Wichman
Semperis Director of Incident Response

No Time Off for Ransomware

Attackers continue to target periods of distraction and disruption.

As noted in the *Semperis 2025 Ransomware Risk Report*, this year's study showed an overall drop in the frequency of ransomware attacks.* Still, more than half (**52%**) of global study respondents who reported being targeted said that the attack occurred during a weekend or holiday.

"While attacks on holidays and weekends have dropped, they still make up the majority," notes Chris Inglis, former US National Cyber Director. "Staying alert is imperative because persistent and patient attackers will strike again if our vigilance fades."

In addition, **60%** of ransomware attacks reportedly took place after a material corporate event, making such times the period of highest risk. Of those attacked after such an event, the majority (**54%**) reported being targeted following a merger or acquisition.

"When you go into a merger or acquisition, cyber due diligence tends to be an afterthought. By the time IT or security identifies necessary fixes, your attack surface has already grown by what you've acquired."

Simon Hodgkinson
Former bp CISO | Semperis Strategic Advisor

"Corporate material events such as mergers and acquisitions often create distractions and ambiguity in governance and accountability—exactly the environment ransomware groups thrive on," says Inglis. "Worse, organizations are under intense pressure to sustain operations while transforming their form and protocols during an IPO or merger and cannot afford downtime, making them more likely to pay quickly to restore operations.

"During these times," Inglis advises, "it is critical to remain vigilant and situationally aware that bad actors may be lurking, looking to plant ransomware."

**Note: Fewer ransomware attacks do not necessarily equate with fewer attacks overall. Intrusions that are designed to "live off the land" aim to stay undetected, enabling attackers to establish persistence or exfiltrate sensitive data rather than demand ransom. We caution readers to remain vigilant against all types of cyberattack.*

52% of ransomware attacks occurred **on a weekend or holiday**

HIGHEST

SINGAPORE 59%

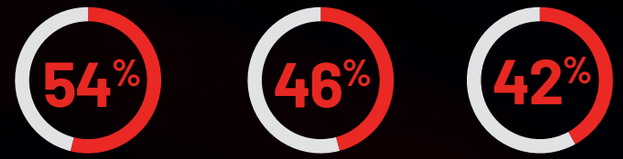
IT/TELECOM 60%

LOWEST

CANADA 41%

ENERGY 36%

60% of ransomware attacks occurred **after a material corporate event**



after a merger or acquisition

after layoffs/ redundancies

after an IPO

Attacks most frequently followed an IPO in Spain (47%) and in the Travel/Transportation industry (55%).

Ransomware most frequently followed layoffs in Australia/ New Zealand (54%) and in the Energy sector (54%).

SOC Staffing Challenges

Work/life balance takes priority as organizations bring security operations in-house.

We are encouraged to see a slight rise in the share of companies that say they staff their SOC at more than half-capacity during weekend and holiday periods. Unfortunately, more than three-quarters (**78%**) still cut SOC staffing by **50% or more** at those times … and **6%** do not staff their SOC at all outside of the regular workweek.

The No. 1 reason given for staffing reductions this year was an effort to provide work/life balance for employees. This rationale is up **30 percentage points** over last year—perhaps because this year's study saw a significant shift (**+28** percentage points) toward organizations bringing their SOCs in-house. **More than 75%** of respondents said they now operate their SOC internally.

Although determining the reasons for this shift is beyond the scope of this study, Courtney Guss, Semperis Director of Crisis Management, thinks several factors could be at play, including a desire for increased visibility and ownership.

"Being able to see what's happening might enable organizations to pivot and adapt faster based on changing operations, business needs, and regulatory reporting requirements," Guss says. "The ROI of outsourcing also seems to be shifting as AI begins to handle some Tier 1 work, leaving the more complex work for SOC analysts."

Slightly fewer respondents than last year said they reduced staffing out of the belief that they wouldn't be targeted or because they had escaped attack to date. That's a good sign that companies are adopting an "assume breach" mindset, a foundational step in any effective cybersecurity strategy.

Smaller organizations (fewer than 1,000 employees), **younger respondents** (under age 34), and **business owners** were **most likely to cut SOC staffing** because they believed they had never been or wouldn't be attacked. Organizations with **more than 5,000** employees and respondents over age 55 **were least likely to cite this reason.**

"If you want your employees to be out for the holiday, you need to plan and prepare. You need to have some type of monitoring, even if it's third-party monitoring with extra diligence over that period. There is no time off."

Jeff Wichman
Semperis Director of Incident Response

96%
of organizations maintain a SOC

78% reduce SOC staffing by **50% or more** on weekends and holidays

6% eliminate SOC staffing on weekends and holidays

Why do you reduce SOC staffing on weekends and holidays?

62% to provide work/life balance

47% we are closed at those times

29% didn't think we'd be attacked

Readiness, Response … and Recovery

Most identity security strategies focus on threat detection over response.

For more than a decade, Semperis has worked to educate global enterprises about the important role of identity system defense in overall cyber resilience. So, we were happy to learn that **90%** of the respondents in this year's study said that they have an ITDR strategy—a slight increase from last year. Nearly all those who said they have an ITDR plan said that they also have procedures in place to scan for identity system vulnerabilities. That's great news.

"One of the most effective ways to defend against ransomware attacks is by tightening identity systems, most commonly Active Directory, Entra ID, and Okta," says former Australian Prime Minister Malcolm Turnbull. "These are the digital keys that determine who can access what within an organization. In nearly every major ransomware incident, weak or compromised credentials have been the initial entry point. Strengthening identity systems is therefore not just good practice but a critical line of defense."

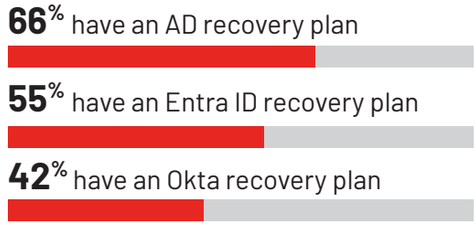
On a less encouraging note, only half as many respondents (**45%**) said they have procedures to remediate the vulnerabilities that an identity system scan detects. Inclusion of identity systems in disaster recovery plans ranges from **66%** for Active Directory to just **42%** for Okta, with Entra ID recovery included in **55%** of plans. And only **63%** of respondents automate identity system recovery, a crucial factor in overall resilience and one that too many ITDR plans leave out.

"Recovery—the ability to restore your identity platform at speed—is the most critical thing from an operational resilience perspective," says Simon Hodgkinson, former bp CISO. "And to be resilient, you've not only got to have identity threat detection and threat response, you need the ability to restore quickly to a trustworthy state."

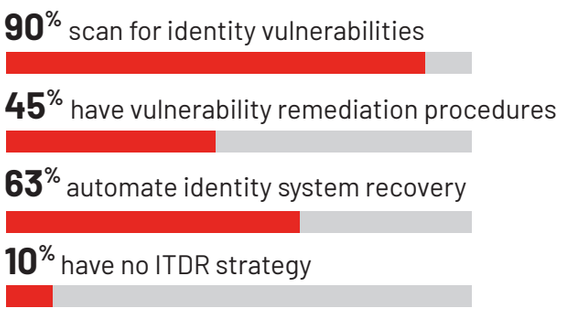
Semperis CISO James Doggett notes that "you can work to prevent and detect intruders, but you must also ask, 'How do I recover from an attack quickly?'"

And the technical aspect of recovery is "just the tip of the iceberg" when it comes to effective ransomware response, says Doggett. "How do you communicate with people, your customers, your vendors, the regulatory people during a crisis? Who makes decisions on what to turn off and turn on or bring back up? In what order do you do all of that?"

Does your disaster recovery plan specifically include identity system recovery?



How are you protecting identity systems?



"Adversaries are always after the identity system because that's where they can create the maximum blast radius. Therefore, you must have the ability to recover the identity system quickly and—most critically—with integrity. Without that integrity, organizations often end up restoring the adversary into the environment."

Simon Hodgkinson
Former bp CISO | Semperis Strategic Advisor

Crunching the Numbers: A Proactive Plan for Resilience

Take steps now to prioritize business continuity.

What can security, IT, and SOC leaders learn from these insights? Cybersecurity and identity resilience experts offer the following suggestions.

Plan for identity system defense, especially during times of disruption

Knowing that attackers frequently target organizations during the chaos of merging identity systems, IT leaders should prioritize Active Directory review and, potentially, modernization *before* a merger or acquisition. "Cyber should be a strategic business capability that is involved in any early-stage transactions," says Hodgkinson.

"The idea of integrating technologies can be overwhelming," says Guss. "When you do merger and acquisition valuations or even divestiture valuations, consider what you are inheriting or offloading and what any integration might look like. Asking these questions in advance could slow things down tremendously and change valuations, which is probably why it isn't often done. But that means that organizations are inheriting risk, inheriting gaps. And truly integrating post-merger or post-acquisition is both difficult and expensive."

Evaluate technology's role in risk mitigation

New AI-powered monitoring and detection capabilities might offer methods for reducing pressure on SOC staff. Still, SOC and security leaders should be realistic about what this technology can—and can't—provide.

"You have to be smart about the resources you have on staff and how you're trying to protect the business because you are taking on some level of risk," says Guss. "Take steps to mitigate or reduce that risk. It could be prioritizing alerting, logging, and monitoring of specific operations that are the most critical to the business."

In addition, be aware that agentic AI can increase your identity attack surface by creating nonhuman identities that must also be secured against threat actors.

Include identity system recovery in crisis response planning

Acknowledging the role of identity security in overall business resilience and taking steps to detect and mitigate identity system vulnerabilities is an excellent start. But security leaders should also include response and recovery in their ITDR and overall crisis response strategies.

"Security officers are good at detecting and preventing, but when something goes wrong, suddenly you're in incident response crisis management—something that most security professionals are not trained in," notes Doggett. "CISOs are going to need to become resilience officers as much as security officers."

> "As ransomware campaigns grow more sophisticated, one truth has become clear: Cyber resilience is not the sole responsibility of the IT department; it is a collective obligation across the entire organization."
>
> **Malcolm Turnbull**
> Former Australian Prime Minister
> Semperis Strategic Advisor

Make resilience your top priority

Whatever your industry, Heather Costa, Mayo Clinic's Director of Technology Resilience, notes that resilience should be the top goal across the organization.

"Disaster recovery has historically been an all-or-nothing approach to physical disruption. Technology resilience is focused on any disruption and ensures that we are looking at things granularly enough to be effective and add value to the organization. Whether it's catastrophic or daily business operation disruptions that happen, how can we mitigate the impacts?"

Focusing on the critical infrastructure that enables day-to-day operations is a crucial step in evaluating and mitigating ransomware risk.

APPENDIX

Ransomware Risk

by Country and Industry

US Ransomware Response Readiness

56%
of ransomware attacks occurred on **a weekend or holiday**

64%
of ransomware attacks occurred **after a material corporate event**

- **43%** after layoffs/redundancies
- **62%** after a merger or acquisition
- **43%** after an IPO

98%
of organizations **maintain a SOC**

- **23%** outsourced
- **77%** in-house

OF THOSE:

- **71%** reduce SOC staffing by **50% or more** on weekends and holidays
- **4%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **93%** scan for identity vulnerabilities
- **45%** have vulnerability remediation procedures
- **67%** automate identity recovery
- **7%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

Why do you reduce SOC staffing on weekends and holidays?

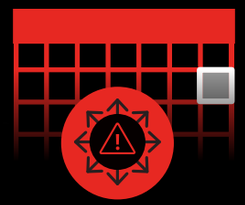
- to provide work/life balance **68%**
- organization is closed at those times **43%**
- don't expect an attack **26%**

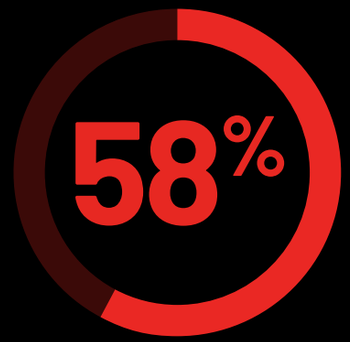
Note: Percentages represent average of responses

CANADA Ransomware Response Readiness

41%

of ransomware attacks occurred on a weekend or holiday





of ransomware attacks occurred after a material corporate event

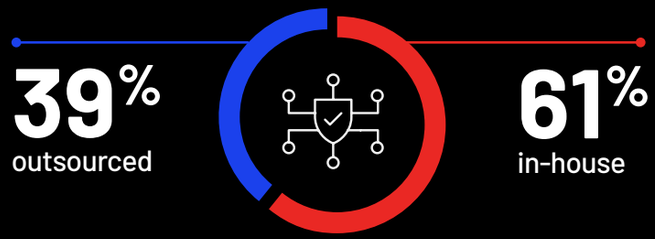
41% after layoffs/redundancies

49% after a merger or acquisition

41% after an IPO

97%

of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

90% scan for identity vulnerabilities

47% have vulnerability remediation procedures

57% automate identity recovery

10% have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

Why do you reduce SOC staffing on weekends and holidays?

to provide work/life balance **60%**

organization is closed at those times **44%**

don't expect an attack **34%**

Note: Percentages represent average of responses

UK Ransomware Response Readiness

50%

of ransomware attacks occurred on a weekend or holiday

46%

of ransomware attacks occurred after a material corporate event

- **46%** after layoffs/redundancies
- **49%** after a merger or acquisition
- **40%** after an IPO

97%

of organizations **maintain a SOC**

21% outsourced

79% in-house

OF THOSE:

78% reduce SOC staffing by **50% or more** on weekends and holidays

7% eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **89%** scan for identity vulnerabilities
- **46%** have vulnerability remediation procedures
- **60%** automate identity recovery
- **11%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **62%**
- organization is closed at those times **41%**
- don't expect an attack **23%**

Note: Percentages represent average of responses

FRANCE Ransomware Response Readiness

53%

of ransomware attacks occurred on a weekend or holiday

53%

of ransomware attacks occurred after a material corporate event

- **49%** after layoffs/redundancies
- **61%** after a merger or acquisition
- **57%** after an IPO

94% of organizations **maintain a SOC**

- **18%** outsourced
- **82%** in-house

OF THOSE:

- **87%** reduce SOC staffing by **50% or more** on weekends and holidays
- **10%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **86%** scan for identity vulnerabilities
- **41%** have vulnerability remediation procedures
- **66%** automate identity recovery
- **14%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

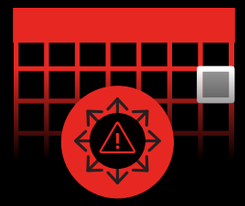
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **58%**
- organization is closed at those times **54%**
- don't expect an attack **33%**

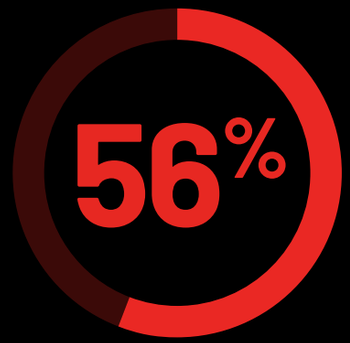
Note: Percentages represent average of responses

GERMANY Ransomware Response Readiness

50%



of ransomware attacks occurred on a weekend or holiday



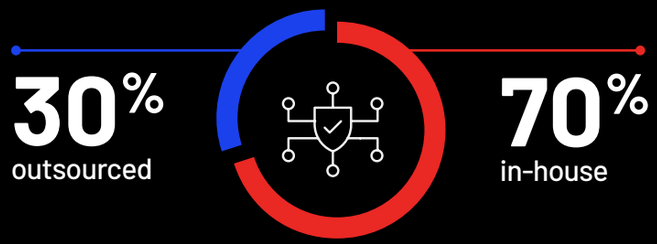
of ransomware attacks occurred after a material corporate event

41% after layoffs/redundancies

60% after a merger or acquisition

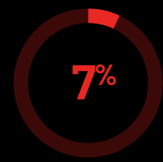
41% after an IPO

98%
of organizations **maintain a SOC**



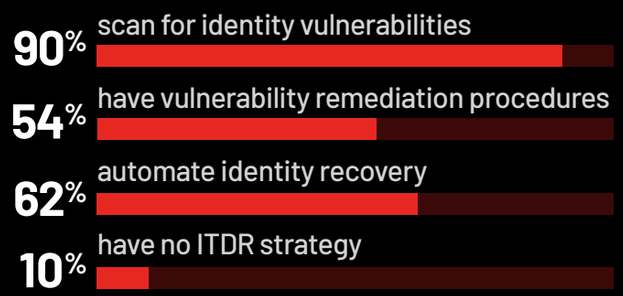
OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

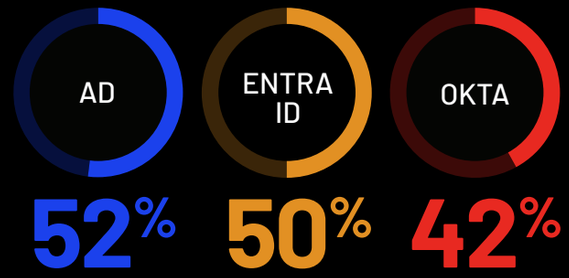


eliminate SOC staffing on weekends and holidays

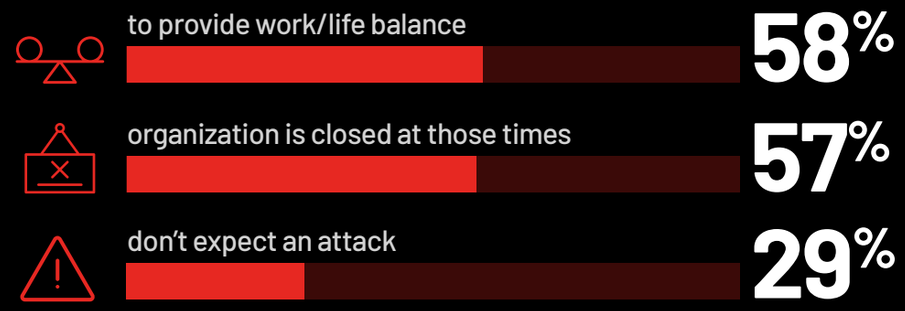
How are you protecting your identity infrastructure?



Does your disaster recovery plan include identity system recovery?



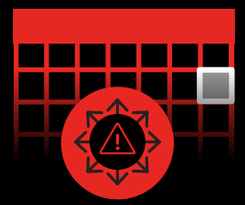
Why do you reduce SOC staffing on weekends and holidays?



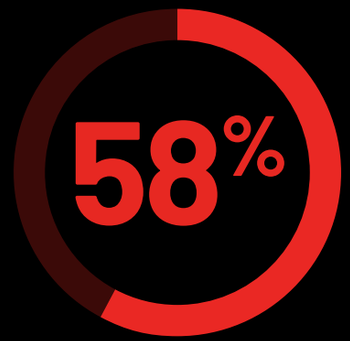
Note: Percentages represent average of responses

SPAIN Ransomware Response Readiness

41%



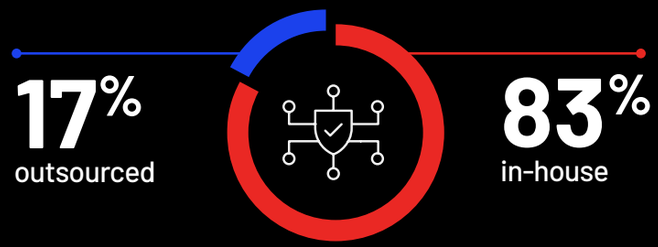
of ransomware attacks occurred on a weekend or holiday



of ransomware attacks occurred after a material corporate event

- **38%** after layoffs/redundancies
- **44%** after a merger or acquisition
- **47%** after an IPO

93%
of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **88%** scan for identity vulnerabilities
- **43%** have vulnerability remediation procedures
- **66%** automate identity recovery
- **12%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **59%**
- organization is closed at those times **50%**
- don't expect an attack **33%**

Note: Percentages represent average of responses

ITALY Ransomware Response Readiness

49%
of ransomware attacks occurred on **a weekend or holiday**

38%
of ransomware attacks occurred **after a material corporate event**

- **32%** after layoffs/redundancies
- **32%** after a merger or acquisition
- **32%** after an IPO

87%
of organizations **maintain a SOC**

- **28%** outsourced
- **72%** in-house

OF THOSE:

- **57%** reduce SOC staffing by **50% or more** on weekends and holidays
- **3%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **79%** scan for identity vulnerabilities
- **42%** have vulnerability remediation procedures
- **53%** automate identity recovery
- **21%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **50%**
- organization is closed at those times **47%**
- don't expect an attack **18%**

Note: Percentages represent average of responses

SINGAPORE Ransomware Response Readiness

59% of ransomware attacks occurred on **a weekend or holiday**

79% of ransomware attacks occurred **after a material corporate event**

- **57%** after layoffs/redundancies
- **63%** after a merger or acquisition
- **53%** after an IPO

98% of organizations **maintain a SOC**

- **14%** outsourced
- **86%** in-house

OF THOSE:

- **78%** reduce SOC staffing by **50% or more** on weekends and holidays
- **3%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **96%** scan for identity vulnerabilities
- **39%** have vulnerability remediation procedures
- **71%** automate identity recovery
- **4%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **67%**
- organization is closed at those times **49%**
- don't expect an attack **30%**

Note: Percentages represent average of responses

AUSTRALIA/NEW ZEALAND Ransomware Response Readiness

52%
of ransomware attacks occurred on **a weekend or holiday**

81%
of ransomware attacks occurred **after a material corporate event**

- **54%** after layoffs/redundancies
- **45%** after a merger or acquisition
- **32%** after an IPO

99%
of organizations **maintain a SOC**

- **28%** outsourced
- **72%** in-house

OF THOSE:

- **85%** reduce SOC staffing by **50% or more** on weekends and holidays
- **7%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **92%** scan for identity vulnerabilities
- **47%** have vulnerability remediation procedures
- **62%** automate identity recovery
- **9%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

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

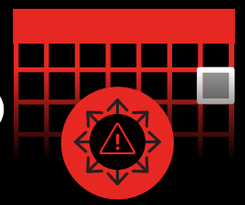
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **63%**
- organization is closed at those times **47%**
- don't expect an attack **35%**

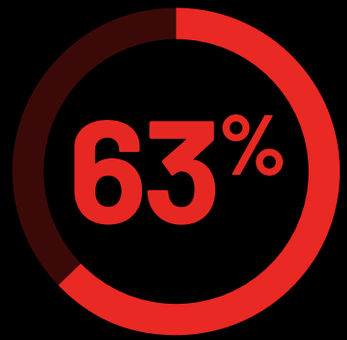
Note: Percentages represent average of responses

EDUCATION Ransomware Response Readiness

48%



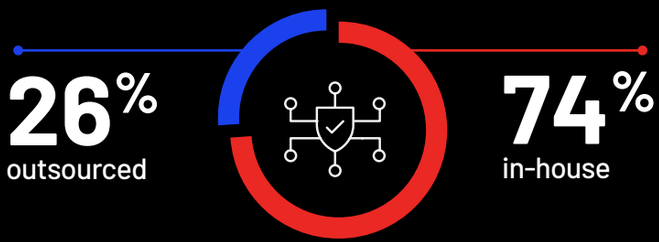
of ransomware attacks occurred on a weekend or holiday



of ransomware attacks occurred after a material corporate event

- **49%** after layoffs/redundancies
- **56%** after a merger or acquisition
- **51%** after an IPO

97% of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **85%** scan for identity vulnerabilities
- **45%** have vulnerability remediation procedures
- **68%** automate identity recovery
- **15%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

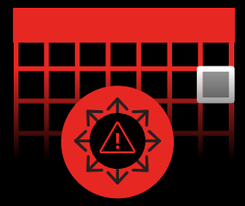
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **51%**
- organization is closed at those times **60%**
- don't expect an attack **33%**

Note: Percentages represent average of responses

ENERGY Ransomware Response Readiness

36%



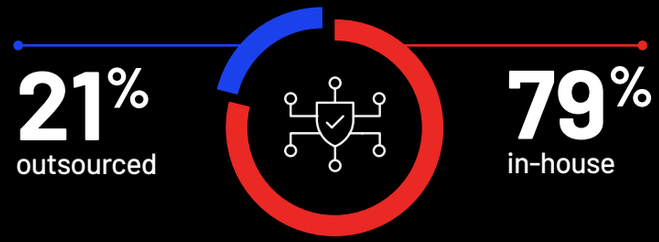
of ransomware attacks occurred on a weekend or holiday

62%

of ransomware attacks occurred after a material corporate event

- **54%** after layoffs/redundancies
- **46%** after a merger or acquisition
- **42%** after an IPO

98%
of organizations **maintain a SOC**



OF THOSE:

- **85%** reduce SOC staffing by **50% or more** on weekends and holidays
- **2%** eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **89%** scan for identity vulnerabilities
- **28%** have vulnerability remediation procedures
- **74%** automate identity recovery
- **11%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

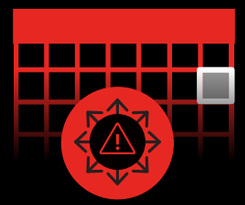
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **68%**
- organization is closed at those times **36%**
- don't expect an attack **28%**

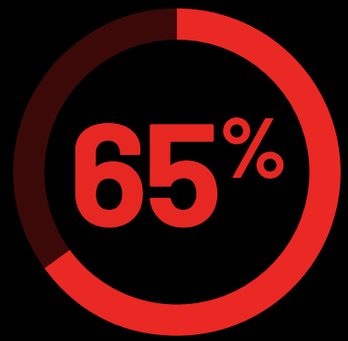
Note: Percentages represent average of responses

FINANCE Ransomware Response Readiness

51%



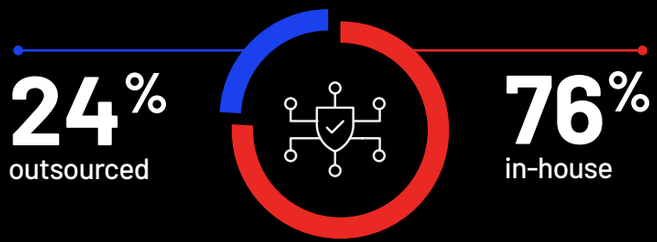
of ransomware attacks occurred on a weekend or holiday



of ransomware attacks occurred after a material corporate event

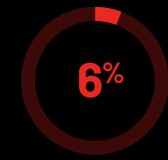
- **47%** after layoffs/redundancies
- **56%** after a merger or acquisition
- **36%** after an IPO

98% of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

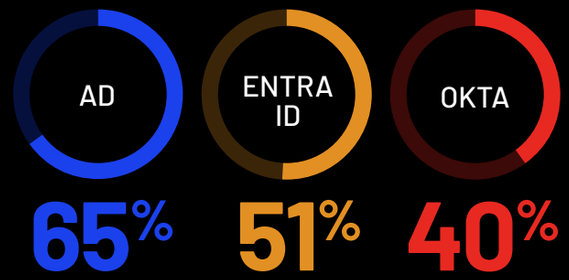


eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **92%** scan for identity vulnerabilities
- **49%** have vulnerability remediation procedures
- **62%** automate identity recovery
- **8%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?



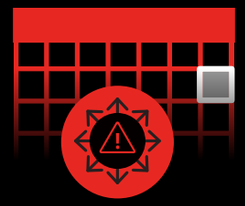
Why do you reduce SOC staffing on weekends and holidays?

- **64%** to provide work/life balance
- **50%** organization is closed at those times
- **26%** don't expect an attack

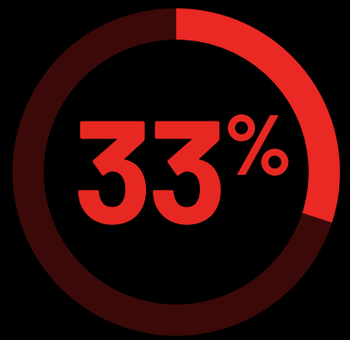
Note: Percentages represent average of responses

GOVERNMENT Ransomware Response Readiness

56%



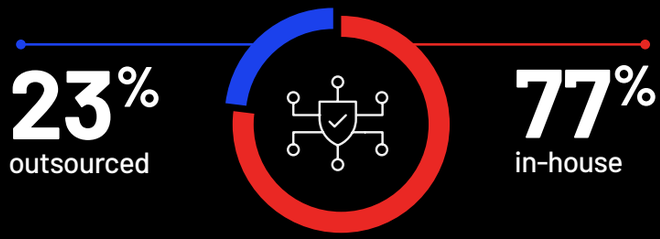
of ransomware attacks occurred on a weekend or holiday



of ransomware attacks occurred after a material corporate event

- **50%** after layoffs/redundancies
- **64%** after a merger or acquisition
- **36%** after an IPO

97% of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **88%** scan for identity vulnerabilities
- **47%** have vulnerability remediation procedures
- **59%** automate identity recovery
- **13%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

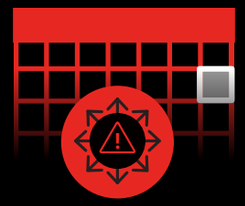
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **50%**
- organization is closed at those times **56%**
- don't expect an attack **15%**

Note: Percentages represent average of responses

HEALTHCARE Ransomware Response Readiness

47%



of ransomware attacks occurred on a weekend or holiday

of ransomware attacks occurred after a material corporate event

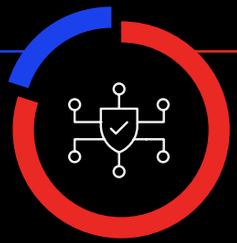
50% after layoffs/redundancies

60% after a merger or acquisition

40% after an IPO

96%
of organizations **maintain a SOC**

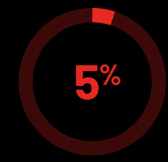
20% outsourced



80% in-house

OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays



eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

90% scan for identity vulnerabilities

38% have vulnerability remediation procedures

66% automate identity recovery

10% have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

67% **58%** **50%**

Why do you reduce SOC staffing on weekends and holidays?

to provide work/life balance **63%**

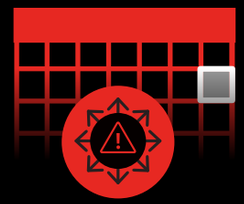
organization is closed at those times **43%**

don't expect an attack **36%**

Note: Percentages represent average of responses

IT/TELECOMMUNICATIONS Ransomware Response Readiness

60%



of ransomware attacks occurred on a weekend or holiday

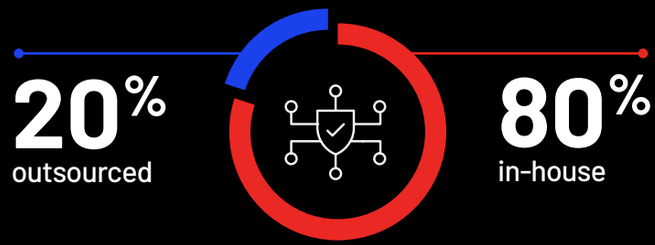
of ransomware attacks occurred after a material corporate event

46% after layoffs/redundancies

53% after a merger or acquisition

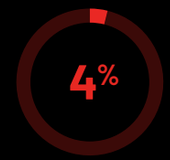
43% after an IPO

96%
of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays



eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

91% scan for identity vulnerabilities

48% have vulnerability remediation procedures

63% automate identity recovery

9% have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

63% **51%** **39%**

Why do you reduce SOC staffing on weekends and holidays?

to provide work/life balance **65%**

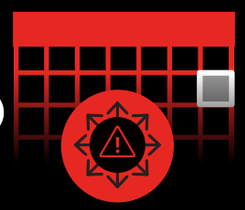
organization is closed at those times **42%**

don't expect an attack **30%**

Note: Percentages represent average of responses

MANUFACTURING/UTILITIES Ransomware Response Readiness

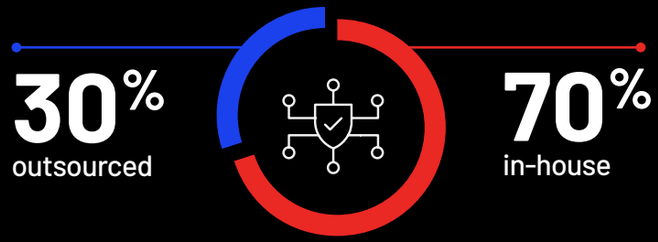
48%
of ransomware attacks occurred on **a weekend or holiday**



54%
of ransomware attacks occurred **after a material corporate event**

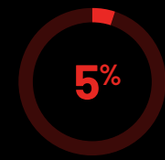
- **41%** after layoffs/redundancies
- **51%** after a merger or acquisition
- **43%** after an IPO

95%
of organizations **maintain a SOC**



OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays



eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

- **90%** scan for identity vulnerabilities
- **44%** have vulnerability remediation procedures
- **63%** automate identity recovery
- **10%** have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

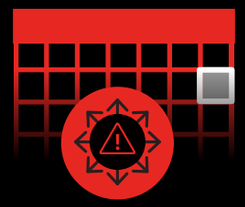
Why do you reduce SOC staffing on weekends and holidays?

- to provide work/life balance **63%**
- organization is closed at those times **50%**
- don't expect an attack **26%**

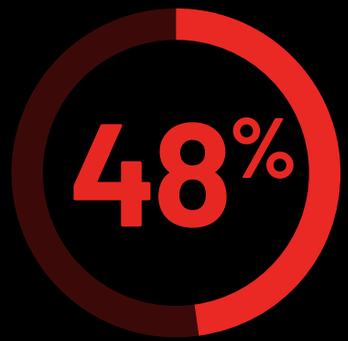
Note: Percentages represent average of responses

TRAVEL/TRANSPORTATION Ransomware Response Readiness

41%



of ransomware attacks occurred on a weekend or holiday



of ransomware attacks occurred after a material corporate event

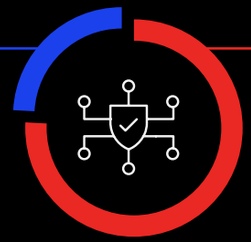
50% after layoffs/redundancies

50% after a merger or acquisition

55% after an IPO

97%
of organizations **maintain a SOC**

24% outsourced



76% in-house

OF THOSE:

reduce SOC staffing by **50% or more** on weekends and holidays

eliminate SOC staffing on weekends and holidays

How are you protecting your identity infrastructure?

90% scan for identity vulnerabilities

51% have vulnerability remediation procedures

57% automate identity recovery

11% have no ITDR strategy

Does your disaster recovery plan include identity system recovery?

66% **57%** **43%**

Why do you reduce SOC staffing on weekends and holidays?

to provide work/life balance **65%**

organization is closed at those times **31%**

don't expect an attack **30%**

Note: Percentages represent average of responses

METHODOLOGY

In the first half of 2025, global organizations across the 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. Global and regional statistics represent an average of responses.

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 2025 Ransomware Holiday Risk Report* and link to the full report, downloadable at https://www.semperis.com/ransomware-holiday-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