semperis

2024

# Ransomware Holiday Risk Report

- Expert guidance for strengthening ransomware defense, especially during high-risk periods such as holidays, weekends, and corporate transitions
- Insights into ransomware attack patterns from a survey of 900 IT and security leaders, revealing that many organizations lack adequate defenses against attacks that strike during times of distraction
- New evidence that organizations routinely overestimate their ability to defend against identity-based attacks

"Threat actors ... are calculated and persistent in their attack methods. Security awareness and functionality don't wax and wane. If anything, organizations should increase their security persistence on holidays and weekends, knowing that threat actors aren't taking time off."

**Chris Inglis**

Strategic Advisor, Semperis

First US National Cyber Director

# Executive Summary

**Ransomware attacks don't observe business hours, and attacks often move too quickly for human intervention alone. Therefore, automated identity playbooks are required to mitigate risk.**

**Threat actors strike during periods of absence or distraction, such as holidays, weekends, and corporate events, including mergers and acquisitions.**

Organizations across the globe are locked in a battle against ransomware and cyberattacks. As the stakes increase, so does the evidence that Microsoft Active Directory is a top target for threat actors and that identity threat detection and response (ITDR) is a key aspect of both cyber and operational resilience.

To examine trends in ransomware's frequency, severity, and impact, Semperis partnered with international research firm Censuswide to conduct a comprehensive study spanning multiple industries across the United States, the United Kingdom, France, and Germany. The first report of our findings—*2024 Ransomware Risk Report*—revealed that ransomware attacks are incessant and costly. Now, our second report—*2024 Ransomware Holiday Risk Report*—examines the timing of attacks that occur during periods of corporate distraction (including holidays, weekends, and material events such as mergers, IPOs, and layoffs) and potential gaps in organizations' cybersecurity defenses.

## Ransomware groups frequently strike outside of business hours.

Ransomware attackers often strike when defenses are weakest—**86% of study participants who experienced a ransomware attack were targeted on a weekend or holiday,** when staffing is most likely to be reduced.

## Organizations typically reduce security staffing during the most likely times of attack.

Even though 96% of surveyed organizations maintained a security operations center (SOC), **85% reduced SOC staffing by as much as 50% on holidays and weekends.**

## Material corporate events present attractive opportunities for ransomware attackers.

From an attacker's perspective, mergers, acquisitions, IPOs, and workforce restructuring provide useful distractions as business and technology leaders focus on event requirements rather than cyber defenses. Mergers and acquisitions are also notorious for providing opportunities to breach Active Directory, and **63% of respondents experienced a ransomware attack following a material corporate event.**

## Business leaders must prioritize strengthening identity system defense.

With Active Directory as the core of organizations' access to systems and resources, identity-based attacks are a growing threat. Yet **40% of companies do not have—or are uncertain that they have—sufficient budget to defend core identity systems such as Active Directory.** Without sufficient budget to address identity system defense, many organizations are missing key parts of an effective ITDR strategy.

# CONTRIBUTING EXPERTS

**Mickey Bresman**
Semperis CEO

**Sean Deuby**
Semperis Principal Technologist (North America)

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

**Simon Hodgkinson**
Semperis Strategic Advisor, former bp CISO

**Chris Inglis**
Semperis Strategic Advisor, former US National Cyber Director

**Ciaran Martin, CB**
Paladin Capital Group Managing Director, founding Chief Executive of the UK's National Cyber Security Centre

**Kemba Walden**
Paladin Global Institute President, former Acting US National Cyber Director

**Jeff Wichman**
Semperis Director of Incident Response

# TABLE OF Contents

# Effective Operational Resilience Is a 24/7/365 Initiative

## Study of global IT and security leaders reveals a striking gap in ransomware defenses.

> "Threat actors want to make as much money as possible with the least hassle. They look for events that give them more leverage, and they try to catch organizations unprepared."
>
> **Sean Deuby**
> Principal Technologist
> (North America), Semperis

Ransomware attackers are adept at hiding their activities. Whether masquerading as legitimate users to breach Zero Trust defenses or using an attack like DCShadow to bypass detection mechanisms, stealth is a key part of the cyberattack playbook. And, as our new global study reveals, this tactic extends beyond the method of attack.

Despite widespread cybersecurity efforts, many organizations are unintentionally opening a door to ransomware by reducing their defenses during weekends and holidays. Attackers clearly expect this behavior and target these periods—as well as other material corporate events that might signal distracted or reduced defenses—to strike.

Organizations that aim to strengthen their cyber defenses can use this information to their advantage. Implementing robust, automated protection and recovery solutions for the identity infrastructure can help to foil ransomware attempts, even during times of corporate upheaval or when human resources are scarce.

Cybersecurity experts and the consortium of national cybersecurity agencies from the US, UK, Australia, New Zealand, and Canada known as the Five Eyes alliance are increasingly focused on the value of effective identity threat detection and response (ITDR). An unprecedented report released by the alliance in September 2024 is a warning that identity systems—especially Active Directory—are often referred to as "the keys to the kingdom" because of their pivotal role in identity and access management (IAM). On-premises Active Directory and related cloud-based identity systems, such as Entra ID and Okta, form the basis of Zero Trust capabilities and are a primary target for cyberattackers, who use these systems to move laterally, escalate privilege, and gain access to sensitive resources.

As part of Semperis' mission to be a force for good, we are dedicated to helping organizations understand the business implications of ransomware and improve their ITDR capabilities. Toward these goals, Semperis recently conducted a detailed study of 900 IT and security professionals from global organizations across the United States, the United Kingdom, France, and Germany.

We surveyed global enterprise IT, security, and risk-management professionals across multiple industries, including education, finance, healthcare, manufacturing and utilities, IT and telecommunications, and travel and transportation. The first Semperis report based on these study responses, ***2024 Ransomware Risk Report***, discussed the prevalence and effects of ransomware. Our new report expands on this research, providing expert insights into common ransomware attack timing and revealing how business and cybersecurity leaders can improve their organization's cyber and operational resilience.

We encourage you to share this information not just with your IT and security teams but also with business leadership. Expanding your organization's ITDR strategy to provide sufficient defense during high-threat periods and to enable fast, secure recovery of the hybrid Active Directory environment is a top business imperative to reduce downtime risk.

# Key Findings

Ransomware attackers strike when security coverage is lighter or when companies are distracted.

**Ransomware strikes when it's least expected—and most damaging.**

72% of survey respondents (**86% of those targeted** by ransomware) were attacked on a **holiday or weekend,** and **63%** of respondents (**76% of targeted organizations**) suffered a ransomware attack during a **major corporate event,** such as a merger, acquisition, or IPO.

**Security staffing is a widespread challenge.**

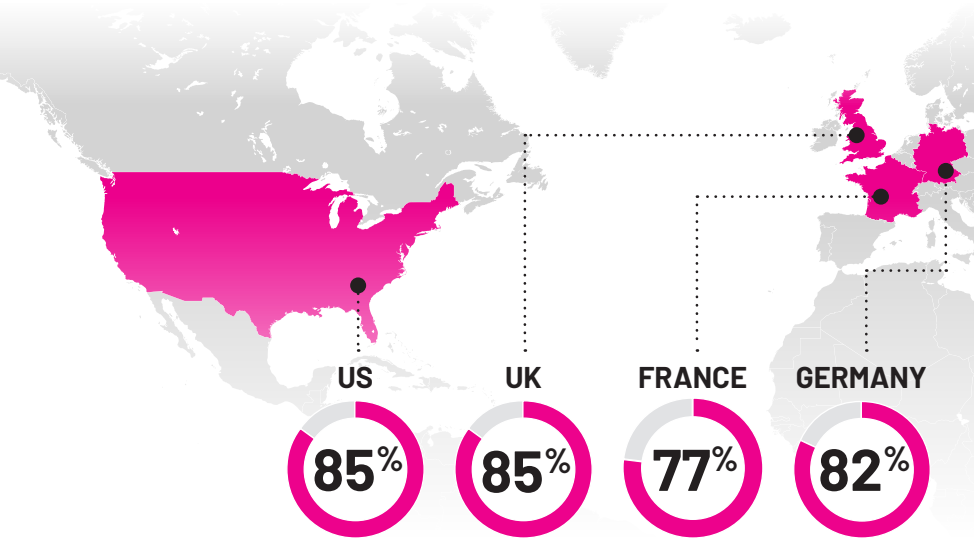
85% of organizations that maintain a year-round, 24-hour SOC—whether outsourced or operated in-house—**reduce staffing on holidays and weekends by up to 50%,** due to staffing challenges and difficulty justifying higher overtime costs when most employees are out of the office.

**Organizations seem to overestimate their identity defenses.**

81% of respondents **believe they have the necessary expertise** to protect against identity-related attacks, yet **83% suffered a successful ransomware attack** within the past 12 months.

**Many identity recovery plans show concerning gaps.**

40% of respondents either have **no budget or are unsure whether they have budget** dedicated to **defending core identity systems** such as Active Directory.




**86%**

**of organizations that experienced ransomware attacks were targeted on a holiday or weekend**

# Attackers Don't Take Holidays

For cyber criminals, office closures offer huge opportunities.

Imagine returning from a relaxing weekend only to discover that Active Directory is down and your critical IT systems are being held for ransom. This was the reality for nearly three-quarters (72%) of the 900 companies included in our study. In fact, **86% of those who experienced a ransomware attack were targeted on a weekend or holiday.**

What makes these periods a threat-actor favorite? Organizations tend to reduce both general and security operations center (SOC) staffing during holidays and weekends, which can also be times of distraction for employees preparing to be away from the office. Cyber criminals see these lowered defenses as an opening for attack.

Ciaran Martin, CB, Managing Director at Paladin Capital Group and founding Chief Executive of the UK's National Cyber Security Centre, notes: "It is human nature for services not to be as strong on the weekends, as many [organizations maintain] the mindset of the workweek. ... And when staffing levels decrease, naturally the fallout could be systems that are more vulnerable to breach."

"Sophisticated criminal organizations exercise patience," says Chris Inglis, Semperis Strategic Advisor and first US National Cyber Director. "They'll compromise a network and lay low for long periods—scouting, normalizing their presence, and creating a foothold inside your system, where they will wait for an advantageous time to extract data and then deploy their ransomware payload during a holiday, weekend, or material event. Suddenly, you're being attacked literally from the inside."

Yet for many respondents, the timing of the attacks came as a surprise.

"When fewer people are in the office, there's less demand for that help-desk role, and internal risks are lower," says Guido Grillenmeier, Principal Technologist (EMEA) at Semperis. "So, it's understandable that companies with a hybrid SOC—one that fulfills both cybersecurity and help-desk roles—might ask, 'Why do I need to have so many people here?'"

"When attackers get inside a company's systems, especially if it's on a holiday weekend when staff is diminished, they may not be noticed right away. Companies are less careful and more vulnerable during those periods, and attackers know that."

**Guido Grillenmeier**
Principal Technologist (EMEA), Semperis

# KEY TAKEAWAYS

Most ransomware attacks took place during a **holiday or weekend.**

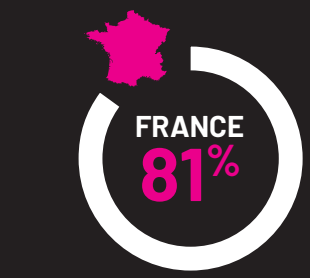
Organizations in **France** were **10% more likely** than organizations in other countries to be targeted during these periods.

**IT/telecom companies** companies were **6%–11% less likely** to be attacked during weekends and holidays.

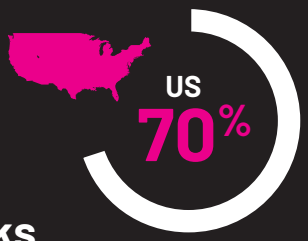
# BY THE NUMBERS

**72%**

**of companies on average have been hit with ransomware attacks on holidays or weekends**









**EDUCATION** 79%

**MANUFACTURING** 75%

**FINANCE** 78%

**IT/TELECOM** 68%

**HEALTHCARE** 74%

**TRAVEL/TRANSPORTATION** 75%

# Attackers Strike When SOC Staffing Is Reduced

Ransomware threats demand 24/7/365 attention.

Most of the organizations included in our study (**96%**) said their **SOC operates 24/7/365,** through some combination of internal and external resources. Even so, **the majority of global companies (85%) scale back on their after-hours SOC staffing levels by up to 50%.** And alarmingly, **nearly 5% of respondents indicated that their SOC is not staffed at all during holidays or weekends.**

> "Cybersecurity cannot wax and wane. It must be steady and ever-present."
>
> **Chris Inglis**
> Semperis Strategic Advisor, former US National Cyber Director

Organizations that scaled back SOC staffing during holidays and weekends did so for multiple reasons:

- They did not think it was necessary, considering most employees work only during weekdays or their business was open only Monday through Friday.
- Their business had never been targeted by ransomware, or they did not believe that it would be targeted.
- They were attempting to maintain a work-life balance for staff.

In addition, many countries mandate higher rates of pay for holiday, overnight, or weekend hours. Fully staffing a SOC during these periods can incur significant costs; reducing staffing levels to offset those expenses, especially for hybrid SOCs that might see fewer help-desk requests, can be tempting.

**Semperis CEO Mickey Bresman advises against skimping on cybersecurity coverage, regardless of the reasoning. "24/7/365 coverage is a necessity, as are automated identity playbooks that serve to reduce risk and improve operational resilience," he cautions.**

Jeff Wichman, Semperis Director of Incident Response, also notes that even when a SOC operates around the clock, staff reductions can be risky. "If you're big enough to have a SOC, it should be staffed at all times—and not by a skeleton crew," he warns. "It should be at least 75 percent staffed, and SOC teams should have effective automated threat detection and response solution in place as well."

# KEY TAKEAWAYS

Despite the high incidence of holiday and weekend cyberattacks, most organizations **reduce SOC staffing over holidays and weekends.**

Organizations in the US were most likely to **maintain 24-hour, year-round SOC coverage** but also most likely to reduce staffing to less than 50% during weekends and holidays.

Conversely, **German companies** were the most likely to maintain staffing of 50% or more during office closures.

Organizations in the **travel/transportation industry** were most likely to maintain staffing of 50% or more during weekends and holidays.

# BY THE NUMBERS

**Does your company maintain a 24/7/365 SOC?**

| | ALL | US | UK | FRANCE | GERMANY |
|---|---|---|---|---|---|
| **Yes (total)*** | **96%** | **97%** | **98%** | **95%** | **91%** |
| Yes *(outsource/hybrid)* | 48% | 47% | 49% | 47% | 50% |
| Yes *(in-house)* | 48% | 50% | 49% | 48% | 41% |
| No | 4% | 3% | 2% | 5% | 9% |

| | EDUCATION | FINANCE | HEALTHCARE | IT/TELECOM | MANUFACTURING | TRAVEL/ TRANSPORTATION |
|---|---|---|---|---|---|---|
| **Yes (total)*** | **95%** | **98%** | **94%** | **96%** | **97%** | **96%** |
| Yes *(outsource/hybrid)* | 44% | 48% | 54% | 39% | 44% | 45% |
| Yes *(in-house)* | 51% | 50% | 41% | 57% | 52% | 51% |
| No | 4% | 2% | 6% | 4% | 3% | 4% |

**We asked companies that maintained a 24/7/365 SOC whether they reduced staffing on holidays and weekends, and if so, by how much.**

**85%**

of respondents **reduced** their staffing by **as much as 50%**

UK **82%**

US **90%**

FRANCE **85%**

GERMANY **75%**

EDUCATION **86%**

IT/TELECOM **82%**

FINANCE **87%**

MANUFACTURING **87%**

HEALTHCARE **81%**

TRAVEL/TRANSPORTATION **77%**

# Attacks Occur During Times of Corporate Distraction

## Leadership and staff changes, system integrations, and mergers create vulnerabilities.

> "I am not at all surprised by the percentage of organizations that are attacked after a corporate event. ... During material events, the business priority is to complete the event—not security."
>
> **Simon Hodgkinson**
> Strategic Advisor, Semperis
> Former bp CISO

Times of corporate upheaval—whether a merger, acquisition, IPO, or reduction in workforce—are also magnets for ransomware attackers. Semperis survey data show that the majority (**63%**) of respondents also **experienced a ransomware attack following a material corporate event.**

Not only do these situations create the distractions that bad actors love to exploit, but attackers can often extract large ransoms from companies desperate to regain access to critical systems or prove operational competence ahead of a major transaction. In addition, such events create inherent identity security challenges.

"During a merger or acquisition, cybersecurity best practices, which are difficult to fully achieve under normal circumstances, become far more difficult," notes Sean Deuby, Principal Technologist (North America) at Semperis.

Merging entities must integrate their identity infrastructures—typically Active Directory environments. Ideally, both organizations will audit each other's systems to identify potential vulnerabilities before such integration begins.

**"If an adversary can get hold of a company that has a weak security posture when two companies merge, they gain a beachhead that can be used to bounce into the more secure environment," says Bresman.**

More often, however, cyber due diligence is sacrificed in favor of financial concerns and operational expedience. Even when IT teams are consulted about cybersecurity vulnerabilities, business leaders might pressure them to move forward despite identified risks. As Deuby notes, "The CEO is not going to delay a merger date because of a security vulnerability. They want to get the merger done and worry about it afterwards."

During the chaos of system integration, what's considered "normal behavior" is in flux. Because threat detection often depends on behavioral analytics, suspicious activity becomes much more difficult to define and, therefore, detect. Threat actors thrive on such confusion.

Legacy systems also pose an opportunity for threat actors. Transition teams are often reluctant to disturb older, potentially fragile systems.

"Legacy applications remain prime targets for a long time, increasing the attack surface," Deuby says. "And yet, rebuilding them is typically not cost effective. So, the long tail of an acquisition can be really dangerous."

Lastly, the restructuring that often accompanies corporate events can provoke malicious actions. As Simon Hodgkinson, Semperis Strategic Advisor and former bp CISO, points out, "When you have disgruntled employees or former employees, the risk of an insider threat goes through the roof."

# KEY TAKEAWAYS

A majority (**63%**) of respondents experienced a **ransomware attack following a material corporate event.**

In **Germany,** organizations were **significantly less likely to suffer** an attack during these periods.

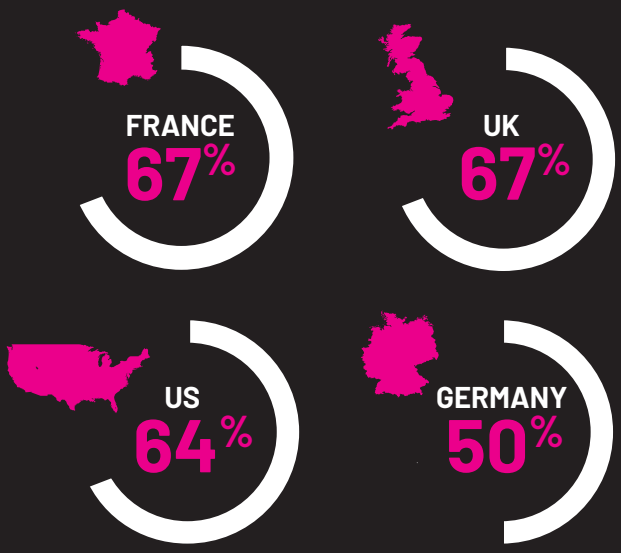
Organizations in the **finance sector** were **most likely to be targeted** by ransomware after such events.

Corporate events create **distractions** and pressure to overlook cyber due diligence. **Technical debt, legacy systems,** and **the potential for disgruntled employees** present additional risks.

# BY THE NUMBERS

**63%**

**of companies were victimized by a ransomware attack after a material corporate event**




**EDUCATION**
60%

**MANUFACTURING**
61%

**FINANCE**
75%

**IT/TELECOM**
66%

**HEALTHCARE**
62%

**TRAVEL/TRANSPORTATION**
63%

# Identity Protection Is Pivotal to Business Resilience

Operational resilience depends on strong Active Directory security and a dedicated identity system recovery plan.

Whether for financial or cultural reasons, organizations are facing a clear gap in their cyber defenses. Fully staffing a 24/7/365 SOC might help to close this gap, as would increasing IT and security resources immediately before, during, and after material corporate events.

Realistically, such an increase in staffing might be difficult to achieve. Yet organizations must take steps to strengthen their ransomware defenses during these critical periods.

**[Active Directory's] pivotal role in authentication and authorisation makes it a valuable target for malicious actors.**

*– Five Eyes alliance*

For most organizations, strengthening operational resilience means improving their ability to defend and recover Active Directory.

In September 2024, the **Five Eyes alliance**—a cybersecurity advisory group comprising the Australian Signals Directorate (ASD), the US Cybersecurity and Infrastructure Security Agency (CISA), the US National Security Agency (NSA), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the UK National Cyber Security Centre (NCSC-UK)—published a report encouraging organizations to "better protect Active Directory from malicious actors."[1]

"Microsoft's Active Directory is the most widely used authentication and authorisation solution in enterprise information technology (IT) networks globally [and its] pivotal role in authentication and

1 Detecting and Mitigating Microsoft Active Directory Compromises, September 2024.

"Cyberattacks, including ransomware, often happen in the cracks—during mergers, acquisitions, layoffs, and in the seams of supplier-vendor relationships. ... To combat never-ending ransomware attacks, organizations should focus on building resilience into their networks."

**Kemba Walden**
Paladin Global Institute President, former Acting US National Cyber Director

authorisation makes it a valuable target for malicious actors," according to the Five Eyes' advisory, which also notes that Active Directory security is pivotal to "overall network security."

A truly effective ransomware and cyber-threat defense strategy, then, must include strong identity protection. Organizations are aware of the importance of ITDR, as **70% of our study respondents** claimed to **have an identity recovery plan** and **81%** believe they **have the necessary identity security expertise** to protect against identity-related attacks.

Yet, as illustrated in this report and the *2024 Ransomware Recovery Report*, organizations might be overestimating their ransomware defense capabilities, including Active Directory–specific backup systems and solutions to enable fast recovery of the identity system.


**of responding organizations that have an identity recovery plan DO NOT take cyber-specific use cases into account.**


**DO NOT include measures to test for identity vulnerabilities.**


**TEST their identity backups and identity recovery plan ONLY QUARTERLY—or less frequently.**


**DO NOT include dedicated, Active Directory–specific backup systems, which are crucial to ensuring a fast, malware-free recovery of the identity system.**

Wichman emphasizes that the ransomware threat—specifically, the threat to a company's critical identity systems—needs to be considered separately from other technology risks, such as outages or disasters.

"I've seen organizations put a war room together during a cyber incident," he says. "That can work from an outage perspective, but it's useless in a ransomware attack. For those situations, that approach to recovery is simply too little, too late."

# Aligning Business Priorities

Elevating cybersecurity to a business priority and implementing automated monitoring solutions will help organizations protect themselves against ransomware risk.

**Ransomware attacks can, and do, strike when least expected. No company—regardless of region, sector, or SOC status—should underestimate the need for constant vigilance. Furthermore, cybersecurity leaders are increasingly insistent that successful ransomware defense efforts must include a clear plan to defend and recover Active Directory.**

**So, what steps can business, technology, and security leaders take to reduce the likelihood of a successful ransomware attack and increase their ability to say "no" to threat actors? Our experts suggest three initial actions.**

## STEP 1 C-level leadership must acknowledge ransomware defense and identity security as business priorities.

The time has come for members of the C-suite to take a more active interest in cybersecurity and ITDR strategy.

"A lot of corporate leaders tend to say, 'Let the tech guys deal with this,'" says Hodgkinson. "But they need to think about security risk like any other operational risk: as part of their business resilience plan. It isn't just a technology priority; it's a business priority, just like safety, financial, or reputational risk."

Inglis agrees. "Asset protection will improve when organizations begin framing cybersecurity not as a technology issue," he says, "but as a business or mission assurance issue."

Bresman suggests that corporate leaders begin by reevaluating risk from an operational resilience perspective.

"Every company's leadership should want to understand the exposure of their IT infrastructure," he says. "Every corporate board should be asking their CISO two questions. One: What is our level of risk?

"It is critical to thwart identity-based attacks as that takes care of an important part of the problem. As time goes by, due to new regulations, organizations are going to have to be able to recover more quickly from ransomware. And recovering an identity system will be increasingly important."

**Ciaran Martin**
CB, Paladin Capital Group Managing Director and founding Chief Executive of the UK's National Cyber Security Centre

And two: What are the systems that would completely cripple our organization if they were taken out?"

The answers can help leaders identify the most critical business infrastructure components, which typically include the identity system.

## STEP 2 Robust ITDR solutions and expert partners can help security leaders offset staffing challenges.

SOCs are indispensable cyber defense tools, but their effectiveness fluctuates. Plus, financial and cultural pressures make adequate security staffing, especially outside of business hours, a universal challenge.

"Clearly, your security posture will be stronger on holidays and weekends if your SOC is staffed to proper levels," says Martin. "Here's where operational resilience becomes so important, as that level of staffing might not be possible. How quickly can you mobilize if things go wrong?"

To fill the gaps, organizations can deploy dedicated ITDR solutions and cultivate relationships with trusted partners. Automated auditing and alerting, attack pattern detection, rollback or suspension of unusual changes to Active Directory, and automated Active Directory forest recovery can all help organizations detect and respond to threats as rapidly as possible—with minimal demands for human intervention.

"You can replace some human monitoring with good automation," suggests Grillenmeier. "For intruders to persist once they're in, they often need to change settings that are otherwise static. So, you can set alarms to go off when these settings are changed."

Organizations with an outsourced SOC should ensure that the provider has dedicated backup systems for Active Directory and a documented identity recovery plan. Organizations that maintain in-house security operations should also have such resources. Those that do not or that are unsure of the efficacy of their disaster recovery plan should consult with a trusted ITDR expert with experience defending, detecting, and recovering from ransomware.

A combination of staff, automated solutions, and trusted partners can help companies **detect threats** and **mobilize quickly.**

## STEP 3 Active Directory security should be a core aspect of every merger or acquisition.

Business and technology leaders must make Active Directory security a priority rather than an afterthought when planning for material corporate events. Planning should include an evaluation of the identity infrastructure health as part of their financial due diligence ahead of any possible merger or acquisition.

"Nothing in the other entity's network should touch yours until you've had a chance to assess their cyber assets," says Wichman. "Have a third-party review done, see what controls are really in place, and start negotiations from there. The cost of that service is a drop in the bucket compared to the risk."

Hodgkinson agrees. "Whether it's obsolete technology or security risks, those are things they'll need to remediate post-deal, and you're talking about millions of dollars," he says, adding that organizations should specifically audit potential partners' identity systems before inking any deals. "If their Active Directory isn't locked down, that's a sign that there are other security holes in the rest of the organization."

As our study shows, organizations simply cannot afford to take their attention off cyber and identity defense, no matter the circumstances.

"Cyberattacks, including ransomware, often happen in the cracks—during mergers, acquisitions, layoffs, and in the seams of supplier-vendor relationships," says Kemba Walden, Paladin Global Institute President and former Acting US National Cyber Director. "We need to ensure these cracks are seamless to prevent vulnerabilities."

"Understanding of the critical role that identity plays within the security story has increased significantly over the past few years. While ITDR is finally getting the attention that it deserves, there is still a lot to do for the protection and security of identity systems."

**Mickey Bresman**
CEO, Semperis

# KEY TAKEAWAYS

Ransomware and identity defense are no longer simply IT challenges; they are **business priorities.**

**Expert ITDR solutions** can help to automate ransomware detection and defense in the face of staffing challenges.

Active Directory security auditing is a **necessary part of due diligence** in advance of material corporate events.

"Improving operational resilience during material events takes patience and diligence. It is essential that the CISOs at both organizations involved in the material event connect prior to any deal and discuss 'must haves' from a security standpoint before the integration of networks begins. They should also identify vulnerabilities and weak spots and make sure both organizations have the best resources available to reduce risks."

**Kemba Walden**
Paladin Global Institute President,
former Acting US National Cyber Director

## METHODOLOGY

In the first half of 2024, global organizations across the United States, the United Kingdom, France, and Germany participated in a detailed study 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 900 IT and security professionals across multiple industries, including education, finance, healthcare, 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 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 2024 Ransomware Holiday 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 the topic of ransomware and resilience. Find Semperis on LinkedIn.

## ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series and built the community hybrid Active Directory cyber defender tools, Purple Knight and Forest Druid. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2024 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and is a member of the Microsoft Intelligent Security Association (MISA).

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

semperis

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