semperis

AUSTRALIA/NEW ZEALAND SUPPLEMENT

2024

Ransomware Holiday Risk Report

- Expert guidance for strengthening ransomware defence, especially during high-risk periods such as holidays, weekends, and corporate transitions
- Insights into ransomware attack patterns revealing that many organisations lack adequate defences against attacks that strike during times of distraction
- New evidence that organisations routinely overestimate their ability to defend against identity-based attacks

"Companies should not lower their guard against cyberattacks during holidays and weekends. Instead, they should bolster their defences against ransomware attacks during these times. The most effective protection against threats during the holidays is maintaining awareness and having a robust backup and recovery plan ready to deploy when needed. "

Malcolm Turnbull

Strategic Advisor, Semperis
Former Australian Prime Minister

Understanding the **Ransomware Risk**

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.

Organisations 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. A second report—*2024 Ransomware Holiday Risk Report*—examined 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 organisations' cybersecurity defences.

This supplement expands our research. We asked 250 organisations in Australia and New Zealand to respond to a subset of our study questions to determine their experience with the topics discussed in the previous reports.

CONTRIBUTING EXPERTS

Mickey Bresman
Semperis CEO

Malcolm Turnbull
Semperis Strategic Advisor, former Australian Prime Minister

Guido Grillenmeier
Semperis Principal Technologist (EMEA)

Simon Hodgkinson
Semperis Strategic Advisor, former bp CISO

Chris Inglis
Semperis Strategic Advisor, former US National Cyber Director

Attackers Don't Take Holidays

"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

69%

of organisations that were targeted by ransomware were attacked on a weekend or holiday

EDUCATION
50%

MANUFACTURING
44%

FINANCE
57%

IT/TELECOM
72%

HEALTHCARE
71%

TRAVEL/TRANSPORTATION
100%

Attackers Strike When SOC Staffing Is Reduced

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

99%

YES

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

	ALL	EDUCATION	FINANCE	HEALTHCARE	MANUFACTURING	IT/TELECOM	TRAVEL/ TRANSPORTATION
Yes (total)*	**99%**	**100%**	**100%**	**100%**	**100%**	**99%**	**100%**
Yes *(outsource/hybrid)*	**27%**	50%	29%	29%	36%	25%	67%
Yes *(in-house)*	**72%**	50%	71%	71%	64%	74%	33%

Do you reduce SOC staffing on weekends and holidays, and if so, by how much?

78% of respondents **reduced** their staffing by **as much as 50%**

Organisations in the healthcare industry were most likely to **maintain staffing** of

50% **OR MORE** during weekends and holidays.

60% of organisations that **scaled back** SOC staffing during holidays and weekends did so to **protect work/life balance**

Attacks Occur During Times of Corporate Distraction

"I am not at all surprised by the percentage of organisations 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

50%

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

EDUCATION 50%

MANUFACTURING 30%

FINANCE 43%

IT/TELECOM 54%

HEALTHCARE 29%

Identity Protection Is Pivotal to Business Resilience

"Attackers often bypass endpoint defences and target the identity system—the backbone of your network. Breach it, and they control your entire infrastructure. Without a resilient identity system, all other defences fail."

Malcolm Turnbull
Strategic Advisor, Semperis
former Australian Prime Minister

83%

HAVE BUDGET SPECIFICALLY FOR THE DEFENCE OF CORE IDENTITY SYSTEMS SUCH AS ACTIVE DIRECTORY

How long did companies take to recover minimal IT functionality?

- **18%** UNDER 5 HOURS
- **30%** 1-7 HOURS
- **49%** 5 HOURS - 1 DAY
- **2%** 7+ DAYS

83%

of respondents say they had an **identity recovery plan in place**

- **EDUCATION** 50%
- **FINANCE** 100%
- **HEALTHCARE** 86%
- **MANUFACTURING** 78%
- **IT/TELECOM** 84%
- **TRAVEL/ TRANSPORTATION** 67%

Aligning Business Priorities

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, successful ransomware defence 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 defence** and **identity security** as **business priorities.**

STEP 2

Robust ITDR solutions and **expert partners** can help security leaders **offset staffing challenges.**

STEP 3

Active Directory security should be a **core aspect** of every merger or acquisition.

"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

METHODOLOGY

To conduct this study, we partnered with experts at Censuswide, an international market research consultancy headquartered in London. Censuswide surveyed 250 IT and security professionals in Australia and New Zealand, across the education, finance, healthcare, manufacturing and utilities, IT and telecommunications, and travel and transportation industries.

HOW TO CITE INFORMATION IN THIS REPORT

The data in this report are provided as an information source for the cybersecurity community and the organisations it serves. Semperis encourages you to share our findings. To cite statistics or insights, reference *Semperis 2024 Ransomware Holiday Report*: *Australia/New Zealand Supplement* and link to the full report, downloadable at https://www.semperis.com/resources/australia-new-zealand-ransomware-risk. 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 organisations 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

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