

# **The State of Ransomware in Japan 2023**

Findings from an independent, vendor-agnostic survey of 300 IT professionals in mid-sized organizations in Japan.

## About the survey

Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in mid-sized organizations (100-5,000 employees) across 14 countries, including 300 respondents in Japan. The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences in the previous 12 months.

## Key findings

- ▶ **58% of Japanese organizations were hit by ransomware in the last year**, a slight drop from the 61% that reported an attack in our 2022 survey. By comparison, globally, 66% of respondents said their organization had experienced a ransomware attack in the last twelve months.
- ▶ **Exploited vulnerabilities were the most common root cause of attack** for Japanese organizations, used in 37% of incidents. Compromised credentials were the second most frequent attack vector, used in 26% of attacks.
- ▶ **72% of attacks resulted in data being encrypted.** This is slightly lower than the global average of 76%, but slightly higher than the 69% reported by Japanese respondents in last year's survey.
- ▶ **Data was also stolen in 34% of attacks where data was encrypted,** slightly higher than the global average of 30%.
- ▶ **95% of Japanese organizations whose data was encrypted got data back,** slightly below the global average of 97%.
- ▶ **Backups remain the most common method used for restoring data,** with 60% of Japanese respondents whose data was encrypted using this approach. This is a sizeable drop on the 72% that used backups in our 2022 survey.
- ▶ **52% of those that had data encrypted in Japan paid the ransom,** slightly up from last year's rate of 50%. As in our 2022 survey, Japanese respondents reported an above average propensity to pay the ransom (global average 2023: 47%, 2022: 46%)
- ▶ **22% of Japanese organizations that had data encrypted used multiple recovery methods** in parallel.
- ▶ 20 respondents from Japan whose organization paid the ransom shared the exact amount, with both the mean and median **ransom payments coming in considerably lower than the global average:**
  - Mean ransom payment: Japan \$113,048; global average \$1,542,330
  - Median ransom payment: Japan \$45,038; global average \$400,00055% paid between \$5,000 and \$99,999 and 35% paid between \$100,000 and \$499,999.
- ▶ Excluding any ransom payments, **the average (mean) bill incurred by Japanese organizations to recover from a ransomware attack was reported at \$1.31 million,** including costs of downtime, people time, device cost, network cost, lost opportunity, et cetera. This is below the global average cost of \$1.82 million.
- ▶ **91% of private sector Japanese organizations hit by ransomware said the attack caused them to lose business/revenue,** higher than the global average of 84%.
- ▶ **49% of Japanese organizations took up to a week to recover from the attack.** 24% took up to a month while 28% took between one and six months.

- **82% of Japanese organizations say they have some form of cyber insurance** with 47% having a standalone cyber policy and 34% having cyber as part of a wider business policy. By comparison, globally, 91% have cyber coverage with 47% having a standalone policy and 43% a wider business policy that covers cyber.
- **93% of Japanese respondents** whose organization had purchased cyber insurance in the last year **said the quality of their defenses had a direct impact on their insurance position.**
  - 62% said it impacted the cost of their coverage (the premium)
  - 58% said it impacted their ability to get coverage
  - 29% said it impacted the terms of their policy, for example the total amount of coverage or sub-limits

## Conclusion

Ransomware continues to be a major threat facing Japanese organizations. With the growth of the ransomware-as-a-service business model, we do not anticipate a drop in attacks in the coming year. In this light, organizations should focus on:

- Further strengthening their defensive shields with:
  - Security tools that defend against the most common attack vectors, including endpoint protection with strong anti-exploit capabilities to prevent exploitation of vulnerabilities, and zero trust network access [ZTNA] to thwart the abuse of compromised credentials
  - Adaptive technologies that respond automatically to attacks, disrupting adversaries and buying defenders time to respond
  - 24/7 threat detection, investigation, and response, whether delivered in-house or in partnership with a specialist Managed Detection and Response (MDR) service provider
- Optimizing attack preparation, including making regular backups, practicing recovering data from backups, and maintaining an up-to-date incident response plan
- Maintaining good security hygiene, including timely patching and regularly reviewing security tool configurations

## Further information

Read [The State of Ransomware 2023](#) report for the full global findings and data by sector.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.