SOPHOS

THE STATE OF RANSOMWARE IN SWITZERLAND 2026

Findings from an independent, vendor-agnostic survey of 79 organizations in Switzerland that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

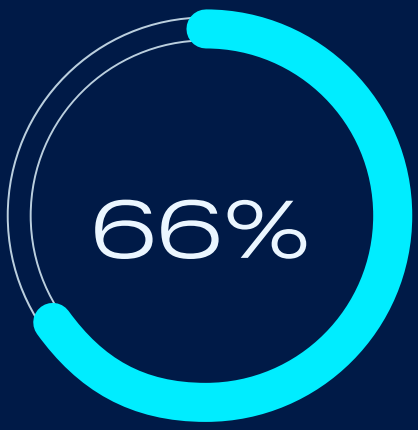
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 79 from Switzerland.

The survey was conducted between January and March 2026. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months. All financial data points are in U.S. dollars. Outlier ransoms of $40 million or more were removed from this data.

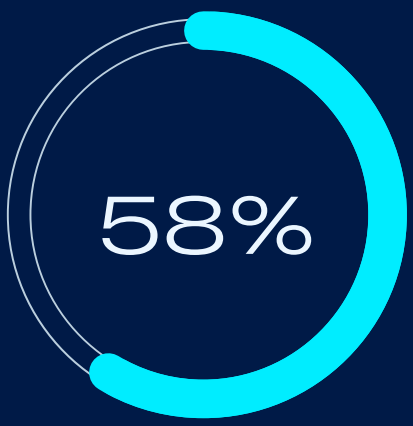
Survey of

79

IT/cybersecurity leaders in Switzerland working in organizations that were hit by ransomware in the last year.



Percentage of attacks that resulted in data being encrypted.



Confirmed that this past year's ransomware incident was the same event as their most significant identity attack.

Average cost to recover from a ransomware attack.

Why Swiss organizations fall victim to ransomware

- **Malicious email was the most common technical root cause of attack,** used in 29% of attacks, followed by compromised credentials (24%) and exploited vulnerabilities (22%). Exploited vulnerabilities dropped sharply, falling to 22% from 31% in the 2025 report.
- **A known security gap (44%) was the most common operational root cause,** the highest of any country surveyed, followed by a lack of people/capacity (43%) and a lack of protection (38%).
- **(NEW) Exposed applications and systems were the most common attack entry point (40%)** for non-email, non-phishing root causes, followed by user devices (30%) and firewalls (28%).
- **(NEW) 58% confirmed that this past year's ransomware incident was the same event as their most significant identity attack.**

What happens to the data

- **66% of attacks resulted in data being encrypted.** This is above the global average of 56% and an increase from the 53% reported by Swiss respondents in the 2025 report.
- **60% of Swiss organizations paid the ransom and got data back,** up from the 54% in the 2025 report, the highest rate of any country surveyed.
- **100% of Swiss organizations that had data encrypted were able to get it back,** in line with the global average.
- **Data was also stolen in 23% of attacks where data was encrypted,** up from the 10% in the 2025 report.
- **77% of Swiss organizations used backups to recover encrypted data,** a considerable increase from the 56% in the 2025 report.

Ransom demands

- **The median Swiss ransom demand was $1.29 million,** a very large increase from the $328,748 in the 2025 report.
- **63% of ransom demands were for $1 million or more,** up from the 46% in the 2025 report.

Median Swiss ransom demand.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) recovery cost for Swiss organizations after their ransomware attack was $2.21 million,** a significant increase from the $1.04 million mean in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **59% of Swiss organizations recovered from a ransomware attack in up to a week,** a slight increase from the 58% in the 2025 report. 24% took between one and six months to recover, a considerable increase from the 9% in the 2025 report, the highest of any country surveyed.

Human impact of ransomware on IT/cybersecurity teams in organizations where data was encrypted

44% report increased anxiety or stress about future attacks. Up from 28% in 2025.

37% report increased recognition from senior leaders.

37% report feelings of guilt that the attack was not stopped.

37% have experienced staff absence due to stress/mental health issues.

13% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. More than half of Swiss ransomware victims confirmed their ransomware incident was the same event as their most significant identity attack. Organizations should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Strengthen endpoint protection for AI frontier models. Frontier AI is accelerating vulnerability discovery and exploitability. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Prioritize email security. With phishing and malicious email accounting for nearly half of ransomware root causes in Switzerland, organizations should deploy advanced email filtering, implement DMARC/DKIM/SPF protocols, and invest in regular phishing awareness training.

Invest in backup and recovery infrastructure. Organizations that maintained robust backup systems recovered encrypted data at nearly record rates in the past year. Backups should be tested regularly, stored offline or in immutable formats, and integrated into a documented incident response plan that can be executed under pressure.

SOPHOS

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor or visit **sophos.com/ransomware2026**

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.

2026-08-05 SW-WP (TA) CRE-6104