SOPHOS

THE STATE OF RANSOMWARE IN SWITZERLAND 2025

Findings from an independent, vendor-agnostic survey of 74 organizations in Switzerland that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JUNE 2025

About the report

This report is based on the findings of an independent, vendor-agnostic survey of 3,400 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 74 from Switzerland.

The survey was commissioned by Sophos and conducted by a third-party specialist between January and March 2025.

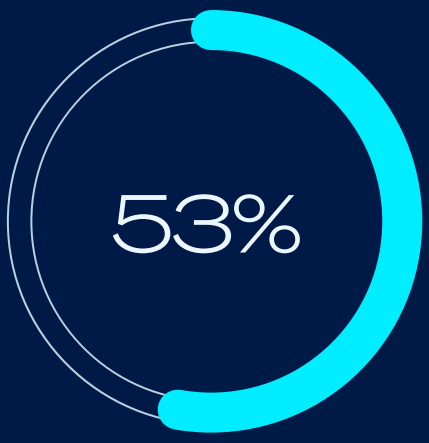
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The report includes comparisons with the findings from our 2024 survey. All financial data points are in U.S. dollars.

Survey of

74

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 encypted.

The most common technical root cause of attacks.

Average cost to recover from a ransomware attack.

Why Swiss organizations fall victim to ransomware

- **Compromised credentials were the most common technical root cause of attack**, used in 32% of attacks. They are followed by exploited vulnerabilities, which were the start of 31% of attacks. Malicious emails were used in 14% of attacks.
- **A lack of people/capacity was the most common operational root cause**, cited by 55% of Swiss respondents. This was followed by a known security gap reported by 49% of organizations. 45% said that a mistake/failure to follow proper processes by their teams played a factor in their organization falling victim to ransomware.

What happens to the data

- **53% of attacks resulted in data being encrypted**. This is just above the global average of 50% but a significant drop from the 68% reported by Swiss respondents in 2024.
- **Data was also stolen in just 10% of attacks where data was encrypted**, a significant drop from the 29% reported last year.
- **97% of Swiss organizations that had data encrypted were able to get it back**, in line with the global average.
- **54% of Swiss organizations paid the ransom and got data back**, a marginal increase from the 50% reported last year.
- **56% of Swiss organizations used backups to recover encrypted data**, a notable drop from the 65% reported last year.

Ransoms: Demands and payments

- The **median Swiss ransom demand in the last year was $328,748,** which is a substantial drop from the $3.97 million reported in our 2024 survey.

Median Swiss ransom demand in the last year.

- 46% of **ransom demands were for $1 million or more**, down from 81% in 2024.
- 22 respondents from Switzerland whose organization paid the ransom shared the amount, revealing a **median ransom payment of $1.1 million**.
- **Swiss organizations typically paid** 76% of the ransom demand, notably below the global average of 85%.
  - 65% **paid LESS THAN the initial ransom** demand (global average: 53%).
  - 15% **paid THE SAME as the initial ransom** demand (global average: 29%).
  - 20% **paid MORE THAN the initial ransom** demand (global average: 18%).

Business impact of ransomware

- Excluding any ransom payments, the **average (mean) bill incurred by Swiss organizations to recover from a ransomware attack in the last year came in at $1.04 million**, a substantial drop from the $3.11 million reported by Swiss respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **Swiss organizations are getting faster at recovering from a ransomware attack**, with 58% fully recovered in up to a week, a significant increase from the 26% reported last year. Just 9% took between one and six months to recover, a notable drop from last year's 41%.

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

64% have experienced a **team member absence** due to stress/ mental health issues.

38% report **feelings of guilt** that the attack was not stopped.

31% report **increased pressure** from senior leaders.

28% report **increased anxiety or stress** about future attacks.

26% report that the **team's leadership has been replaced**.

Recommendations

Ransomware remains a major threat to Swiss organizations. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace. The learnings from this report indicate key areas for focus in 2025 and beyond.

- **Prevention.** The best ransomware attack is the one that didn't happen because adversaries couldn't get into your organization. Look to reduce both the technical root causes of attack and the operational ones highlighted in this report.
- **Protection.** Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- **Detection and response.** The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in house, look to work with a trusted managed detection and response (MDR) provider.
- **Planning and preparation.** Having an incident response plan that you are well versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to take good backups and regularly practice recovering from them.

SOPHOS

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

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.

2025-06-19 CH-WP (DD)