SOPHOS

THE STATE OF RANSOMWARE IN THE UK 2026

Findings from an independent, vendor-agnostic survey of 120 organizations in the UK that were hit by ransomware in the last year.

A SOPHOS WHITEPAPER - JULY 2026

About the report

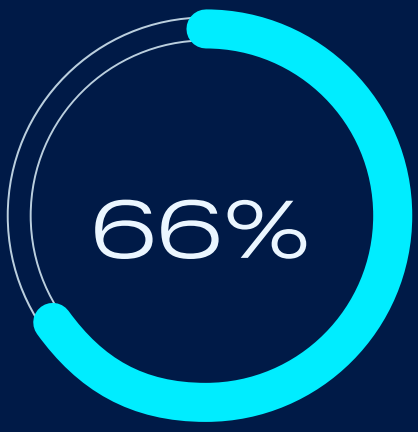
Now in its seventh year, the State of Ransomware report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. This year's global report is based on the experiences of 2,158 IT/cybersecurity leaders working in organizations that were hit by ransomware in the last year, including 120 from the UK.

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.

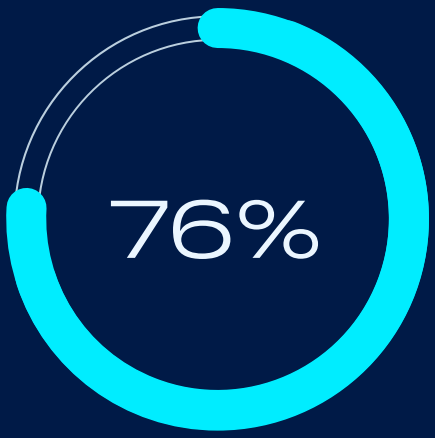
Survey of

120

IT/cybersecurity leaders in the UK 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 UK organizations fall victim to ransomware

- **Compromised credentials were the most common technical root cause of attack, used in 28% of attacks,** followed by malicious email (25%) and phishing (22%). Exploited vulnerabilities fell to 18% from 36% in the 2025 report.
- **Human error (42%) was the most common operational root cause,** followed by an unknown security gap (35%) and a known security gap (33%).
- **(NEW) Firewalls were the most common attack entry point (37%)** for non-email, non-phishing attacks, followed by user devices (32%) and exposed applications and systems (22%).
- **(NEW) 76% 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 a verage of 56% and a drop from the 70% reported by UK respondents in the 2025 report.
- **Data was also stolen in 30% of attacks where data was encrypted,** up from the 26% in 2025.
- **97% of UK organizations that had data encrypted were able to get it back,** in line with the global average.
- **18% of UK organizations paid the ransom and got data back,** a big drop from the 54% in last year's report.
- **78% of UK organizations used backups to recover encrypted data,** a considerable jump from the 39% reported in 2025.

Ransoms demands

- **The median UK ransom demand was $2.5 million — the highest demand recorded for any country** and a 53% drop from the $5.37 million reported in the 2025 report.
  - **65% of ransom demands were for $1 million or more,** down from 89% in the 2025 report.

Median UK ransom demand.

Business impact of ransomware

- Excluding any ransom payments, **the average (mean) cost incurred by UK organizations to recover from a ransomware attack in this year's report came in at $1.49 million**, a significant drop from the $2.58 mean reported in the 2025 report. This includes the costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **55% of UK organizations recovered from a ransomware attack in up to a week**, a slight drop from the 59% reported in the 2025 report. 16% took between one and six months to recover, a small increase from 13% in the 2025 report.

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

47% report increased pressure from senior leaders. Up from 39% in 2025.

47% report increased recognition from senior leaders. Up from 25% in 2025.

41% report increased anxiety or stress about future attacks**.**

25% experienced changes to team/organizational structure.

19% report that the team's leadership has been replaced.

Recommendations

Strengthen identity security as a ransomware defense. More than three-quarters of UK 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 just under half of ransomware root causes in the UK, 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.

2026-08-04 UK-WP (NP)