SOPHOS

THE STATE OF RANSOMWARE IN THE UK 2025

Findings from an independent, vendor-agnostic survey of 201 organizations in the UK 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 201 from the UK.

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

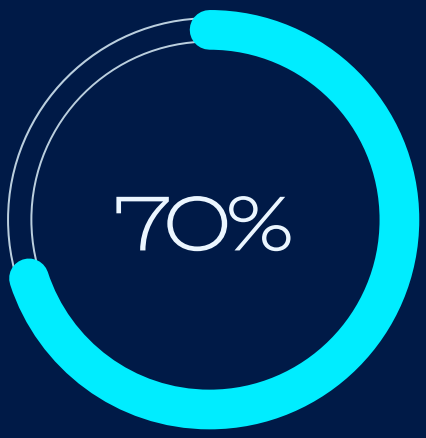
All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

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

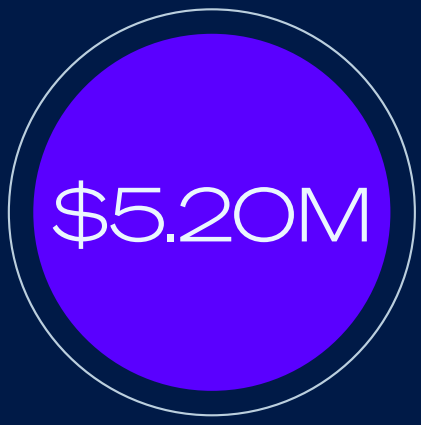
Survey of

201

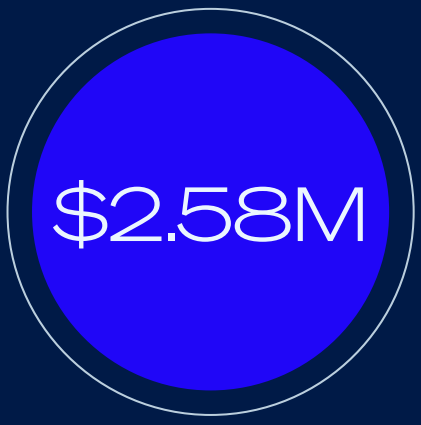
IT/cybersecurity leaders in the UK working in organizations that were hit by ransomware in the last year



Percentage of attacks that resulted in data being encypted.



Median UK ransom payment in the last year.



Average cost to recover from a ransomware attack.

Why UK organizations fall victim to ransomware

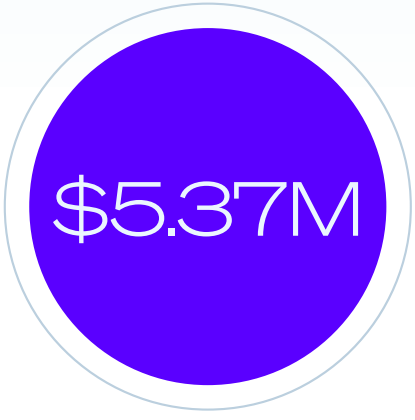
- **Exploited vulnerabilities were the most common technical root cause of attack, used in 36% of attacks**. They are followed by malicious emails, which were the root cause of 20% of attacks. Compromised credentials were used in 19% of attacks.
- **A lack of expertise was the most common operational root cause**, cited by 42% of the UK respondents. This was followed by an unknown security gap reported by 40% of organizations. 38% said that not having the necessary cybersecurity products and services in place played a factor in their organization falling victim to ransomware.

What happens to the data

- **70% of attacks resulted in data being encrypted**. This is well above the global average of 50% and the 46% reported by UK respondents in 2024.
- **Data was also stolen in 26% of attacks where data was encrypted**, a significant drop from the 49% reported last year.
- **99% of UK organizations that had data encrypted** were able to get it back, just above the global average.
- **54% of UK organizations paid the ransom and got data back**, a marginal increase from the 51% reported last year.
- **39% of UK organizations used backups to recover encrypted data**, a notable drop from the 48% reported last year.

Ransoms: Demands and payments

- **The median UK ransom demand** in the last year was $5.37 million, which is more than double the $2.54 million reported in our 2024 survey.



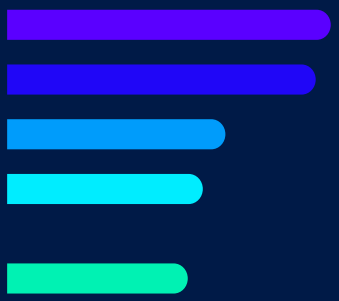
Median UK ransom demand in the last year.

- 89% of **ransom demands were for $1 million or more**, up from 71% in 2024.
- The **median UK ransom payment in the last year was $5.20 million**, significantly above the $2.54 million reported last year.
- **UK organizations typically paid** 103% of the ransom demand, notably higher than the global average of 85%.
  - 49% **paid LESS THAN the initial ransom** demand (global average: 53%)
  - 23% **paid THE SAME as the initial ransom** demand (global average: 29%)
  - 28% **paid MORE THAN the initial ransom** demand (global average: 18%)

Business impact of ransomware

- Excluding any ransom payments, the **average (mean) bill incurred by UK organizations to recover from a ransomware attack in the last year came in at a staggering $2.58 million**, an increase from the $2.07 million reported by UK respondents in 2024. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.
- **UK organizations are getting faster at recovering from a ransomware attack**, with 59% fully recovered in up to a week, a significant increase from the 38% reported last year. Just 13% took between one and six months to recover, a notable drop from last year's 31%.

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



43% reported an **increase in workload**.

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

29% report **feelings of guilt** that the attack was not stopped.

26% have experienced a **team member absence** due to stress/ mental health issues.

24% report that the **team's leadership has been replaced**.

Recommendations

Ransomware remains a major threat to UK 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 **sophos.com/ransomware2025**

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 UK-WP (DD)