SOPHOS

The State of Ransomware in the UK 2024

Findings from an independent, vendor-agnostic, survey of 330 IT professionals in mid-sized organizations in the United Kingdom.

A Sophos Whitepaper. April 2024

About the survey

Sophos commissioned an independent, vendor-agnostic survey of 5,000 IT/cybersecurity leaders in mid-sized organizations (100-5,000 employees) across 14 countries, including 330 respondents in the UK. The survey was conducted between January and February 2024, and respondents were asked to respond based on their experiences in the previous 12 months. All financial data points are in U.S. dollars.

Key findings

- **58% of UK organizations were hit by ransomware in the last year**, a considerable increase from the 44% reported in our 2023 survey and just above the 57% reported in 2022. By comparison, globally, 59% of respondents said their organization had experienced a ransomware attack in the last twelve months.
- **46% of computers were impacted, on average, in the attack**, slightly below the global average of 49%.
- **Compromised credentials were the most common root cause of attack** for UK organizations, used in 33% of incidents. Exploited vulnerabilities were the second most frequent attack vector, used in 24% of attacks.
- **46% of attacks resulted in data being encrypted**. This is considerably below the global average of 70%, and a notable drop from the 75% reported by UK respondents in last year's survey.
- **Data was also stolen in 49% of attacks where data was encrypted**, above the global average of 32% and an increase from the 44% reported by UK respondents in our 2023 study.
- **In 84% of UK ransomware attacks, cybercriminals tried to compromise the organization's backups**, below the global average of 94%.
- **58% of UK backup compromise attempts were successful**, just above the global average of 57%.
- **98% of UK organizations whose data was encrypted got data back**, in line with the global average of 98% but a welcome increase on last year's figure of 94%.
- **For the first time in our five-year study, UK organizations are more likely to recover data by paying the ransom (51%) than using backups (48%)**. Globally, backups are the most common method used for restoring data, used in 68% of encryption events, while 56% paid the ransom.
- **19% of UK organizations that had data encrypted used multiple recovery methods to get data back**, considerably below the global average of 47%.
- 72 respondents from the UK whose organization had data encrypted shared the initial ransom demand:
  - **Mean UK ransom demand: $5,193,258**; global average $4,321,880
  - Median UK ransom demand: $2,540,000; global average $2 million
  - 71% of demands were for $1 million or more
- 42 respondents from the UK whose organization paid the ransom shared the amount:
  - **Mean UK ransom payment: $4,370,395**; global average $3,960,917
  - Median UK ransom payment: $2,540,000; global average $2 million
- **UK organizations paid on average 102% of the initial demand**. In comparison, globally, organizations paid 94% of the initial demand.
- **91% of UK ransom payments are funded from multiple sources**, above the global average of 82%.
- **Cyber insurance providers contributed to the ransom in 93% of incidents**, but only paid the whole ransom in 2% of cases.

- Excluding any ransom payments, **the average (mean) bill incurred by UK organizations to recover from a ransomware attack was reported at $2.07 million, a very slight decrease from the $2.09 million** reported in 2023. This includes costs of downtime, people time, device cost, network cost, lost opportunity, et cetera.
- **UK organizations are getting slower at recovering from attacks** with 38% fully recovered in up to a week, down from 45% in 2023. 31% took between one and six months, a significant increase from the 20% last year.
- **95% of UK ransomware victims reported the attack** to law enforcement and/or an official government body.
  - 64% received advice on dealing with the attack
  - 58% got help investigating the attack
  - 26% received assistance in recovering data encrypted in the attack
- **55% of those that reported the attack found it easy to engage with law enforcement and/or official bodies**. 31% found it somewhat difficult while 14% said it was very difficult to engage.

Recommendations

Ransomware remains a major threat to UK organizations of all sizes around the globe. Both the overall attack rate and the impact of an attack on those that fall victim has increased over the last year. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace.

Prevention. The best ransomware attack is the one that didn't happen because the adversaries couldn't get into your organization.

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. Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypt your data will considerably improve your outcomes.

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.

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

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.

2024-04-24 (WP-MP)

SOPHOS