SOPHOS

THE STATE OF RANSOMWARE IN THE UNITED ARAB EMIRATES 2025

Findings from an independent, vendor-agnostic survey of 118 organizations in the United Arab Emirates that were hit by ransomware in the last year.

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 118 from the United Arab Emirates.

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

118

IT/cybersecurity leaders in the United Arab Emirates working in organizations that were hit by ransomware in the last year

55%

Percentage of attacks that resulted in data being encypted.

$1.33M

Median UAE ransom payment in the last year.

$1.41M

Average cost to recover from a ransomware attack.

Why UAE organizations fall victim to ransomware

▶ **Exploited vulnerabilities were the most common technical root cause of attack, used in 42% of attacks**. They are followed by malicious emails, which were the start of 23% of attacks. Compromised credentials were used in 18% of attacks.

▶ **An unknown security gap was the most common operational root cause**, cited by 49% of UAE respondents. This was followed by a lack of protection and poor quality protection, both cited by 36% of organizations.

What happens to the data

▶ **55% of attacks resulted in data being encrypted** – above the global average.

▶ **Data was also stolen in 43% of attacks where data was encrypted**, significantly above the 28% global average.

▶ **98% of UAE organizations that had data encrypted** were able to get it back.

▶ **43% of UAE organizations paid the ransom and got data back**.

▶ **68% of UAE organizations used backups to recover encrypted data**.

Ransoms: Demands and payments

▶ **The median UAE ransom demand** in the last year was $1.33 million, in line with the $1.32 million global average.

$1.33M

Median UAE ransom demand in the last year.

▶ 59% of **ransom demands were for $1 million or more**.

▶ 28 respondents from the United Arab Emirates whose organization paid the ransom shared the amount, revealing a **median ransom payment of $1.33 million** - above the $1 million global average.

▶ **UAE organizations typically paid 92% of the ransom demand**, above the global average of 85%.

  ▪ 30% **paid LESS THAN the initial ransom** demand (global average: 53%)

  ▪ 52% **paid THE SAME as the initial ransom** demand (global average: 29%)

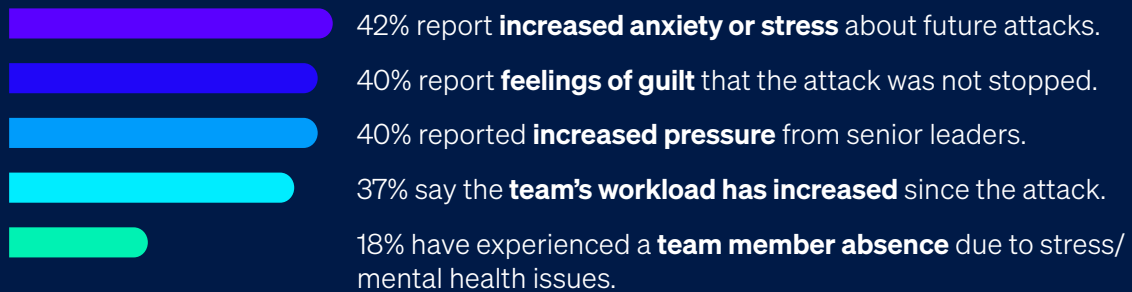 ▪ 19% **paid MORE THAN the initial ransom** demand (global average: 18%)

Business impact of ransomware

▶ Excluding any ransom payments, the **average (mean) bill incurred by UAE organizations to recover from a ransomware attack in the last year came in at $1.41 million**, below the $1.53 million global average. This includes costs of downtime, people time, device cost, network cost, lost opportunity, etc.

▶ **UAE organizations recover swiftly from ransomware attacks**, with 63% fully recovered in up to a week, notably above the 53% global average. 15% took between one and six months to recover, below the 18% global average.

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

42% report **increased anxiety or stress** about future attacks.

40% report **feelings of guilt** that the attack was not stopped.

40% reported **increased pressure** from senior leaders.

37% say the **team's workload has increased** since the attack.

18% have experienced a **team member absence** due to stress/mental health issues.

Recommendations

Ransomware remains a major threat to UAE 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.