SOPHOS

The State of Ransomware in India 2024

Findings from an independent, vendor-agnostic, survey of 500 IT professionals in mid-sized organizations in India.

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 500 respondents in India. 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

- **64% of Indian organizations were hit by ransomware in the last year**. This is a decrease on the 73% reported in our 2023 survey but an increase on the 57% reported in 2022. By comparison, globally, 59% of respondents said their organization had experienced a ransomware attack in the last twelve months.
- **44% of computers were impacted, on average, in the attack**, below the global average of 49%.
- **Malicious emails were the most common root cause of attack** for Indian organizations, used in 42% of incidents. Exploited vulnerabilities were the second most frequent attack vector, used in 23% of attacks.
- **62% of attacks resulted in data being encrypted**. This is below both the global average of 70%, and the 77% reported by Indian respondents in last year's survey.
- **Data was also stolen in 34% of attacks where data was encrypted**, above the global average of 32% but below the 38% reported by Indian respondents in our 2023 study.
- **In 96% of Indian ransomware attacks, cybercriminals tried to compromise the organization's backups**, slightly above the global average of 94%.
- **52% of backup compromise attempts were successful**, below the global average of 57%.
- **98% of Indian organizations whose data was encrypted got data back**, in line with both the global average and last year's figure of 98%.
- **For the first time in our five-year study, Indian organizations are more likely recover data by paying the ransom (65%) than using backups (52%)**. Globally, backups are the most common method used for restoring data, used in 68% of encryption events, while 56% paid the ransom.
- **34% of Indian organizations that had data encrypted used multiple recovery methods to get data back**, below the global average of 47%.
- 170 respondents from India whose organization had data encrypted shared the initial ransom demand:
  - **Mean Indian ransom demand: $4,778,746**; global average $4,321,880
  - Median Indian ransom demand: $2,000,000; global average $2 million
  - 62% of demands were for $1,000,000 or more
- 116 respondents from India whose organization paid the ransom shared the amount:
  - **Mean Indian ransom payment: $2,674,239**; global average $3,960,917
  - Median Indian ransom payment: $2,000,000; global average $2 million
- **The eventual ransom paid by Indian organizations, was on average, 86% of the initial demand**. In comparison, globally, organizations paid 94% of the initial demand.
- **95% of Indian ransom payments are funded from multiple sources**, above the global average of 82%.
- **Cyber insurance providers contributed to the ransom in 94% of incidents**, but never paid the full ransom.

- Excluding any ransom payments, **the average (mean) bill incurred by Indian organizations to recover from a ransomware attack was reported at $1.35 million**. This is an increase on the $1.03 million reported in 2023. This includes costs of downtime, people time, device cost, network cost, lost opportunity, et cetera.
- **Indian organizations are getting faster at recovering from attacks** with 61% fully recovered in up to a week, up from 59% in 2023. 14% took between one and six months, a decrease from the 16% last year.
- **96% of Indian ransomware victims reported the attack** to law enforcement and/or an official government body.
  - 71% received advice on dealing with the attack
  - 70% got help investigating the attack
  - 44% received assistance in recovering data encrypted in the attack
- **59% of those that reported the attack found it easy to engage with law enforcement and/or official bodies**. 33% found it somewhat difficult while 7% said it was very difficult to engage.

Recommendations

Ransomware remains a major threat to Indian organizations of all sizes around the globe. While the overall attack rate has dropped over the last year, the impact of an attack on those that fall victim has increased. 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.

2024-04-22 (WP-PC)

SOPHOS