SOPHOS
Cybersecurity delivered.

The State of Ransomware in Mexico 2022

Findings from an independent, vendor-agnostic survey of 200 IT professionals in mid-sized organizations in Mexico.

A Sophos Whitepaper. April 2022

About the survey

Sophos commissioned research agency Vanson Bourne to conduct an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations (100-5,000 employees) across 31 countries, including 200 in Mexico. The survey was conducted during January and February 2022, and respondents were asked to answer based on their experiences over the previous year.

Key findings

- **74% of Mexican organizations were hit by ransomware in the last year,** a three-fold increase from the 25% that reported an attack in 2020. By comparison, globally, 66% of respondents experienced a ransomware attack in 2021.
- **57% of attacks resulted in data being encrypted.** This is slightly lower than the global average of 65%, and a considerable increase from the 22% that was reported by respondents in Mexico in 2020.
- **100% of Mexican respondents whose data was encrypted got some of their data back.** This aligns with the global results where 99% reported getting at least some of their data back.
- **Backups were the #1 method used for restoring data,** with 79% of Mexican respondents whose data was encrypted using this approach. 44% paid the ransom. It's clear that using multiple recovery methods in parallel is now common. By comparison, globally 73% of respondents used backups and 46% paid the ransom to restore data.
- **Mexican organizations that paid the ransom got back on average 58% of their data.** Globally, 61% of encrypted data was restored by those that paid the ransom, a slight reduction on the 2020 figure of 65%.
- 37 respondents from Mexico that paid the ransom shared the amount paid, with **the average payment coming in at US$482,446.** 16% paid less than US$10,000 while 16% paid US$1M or more. Globally, the average ransom payment was US$812,360, and there was an almost threefold increase in the percentage paying US$1M or more (up from 4% in 2020 to 11% in 2021).
- **The average Mexican bill to recover from a ransomware attack in 2021 was US$0.88M.** This is a considerable decrease from the US$2.03M reported in 2020.
- **88% of respondents in Mexico said the ransomware attack impacted their ability to operate.** This is in line with the global figure of 90%.
- **79% reported that the ransomware attack caused their organization to lose business/revenue.** Again, this is in line with the global figure of 86%.
- **Mexican organizations took on average one month to recover from the attack.**
- **85% of Mexican respondents said their organization has cyber insurance that covers it if hit by ransomware.** Globally this figure stands at 83%.
- **95% reported that it got harder to secure cyber insurance over the last year.** 59% said the level of cybersecurity needed to qualify for insurance is higher, 53% said cybersecurity policies are now more complex, 29% said the process takes longer, and 32% reported it is more expensive. Given that the major cyber insurance price rise began in the second and third quarters of 2021, it is likely that many organizations will experience a considerable price increase at their next renewal.
- **99% of Mexican organizations have made changes to their cyber defenses over the last year to improve their insurance position.** Globally, 97% made changes with 64% implementing new technology/services, 56% increasing staff training and education activities, and 52% changing their processes and behaviors.

- **The cyber insurance paid out in 100% of Mexican ransomware claims.** Of those hit by ransomware and that had cyber insurance cover against ransomware, 69% reported that the insurance paid the costs to get them up and running again, 40% said it paid the ransom, and 29% said it paid other costs.

Conclusion

The ransomware challenge facing Mexican organizations continues to grow.
Optimizing your cybersecurity is an imperative for all organizations. Our five top tips are:

- Ensure high-quality defenses at all points in your environment. Review your security controls and make sure they continue to meet your needs.
- Proactively hunt for threats so you can stop adversaries before they can execute their attack – if you don't have the time or skills in house, outsource to a MDR specialist.
- Harden your environment by searching for and closing down security gaps: unpatched devices, unprotected machines, open RDP ports, etc. Extended Detection and Response (XDR) is ideal for this purpose.
- Prepare for the worst. Know what to do if a cyber incident occurs and who you need to contact.
- Make backups, and practice restoring from them. Your goal is to get back up and running quickly, with minimum disruption.

Further information

Read The State of Ransomware 2022 report for the full global findings and data by sector.

For detailed information on individual ransomware groups, see the Sophos Ransomware Threat Intelligence Center.

Learn more about ransomware and how Sophos can help you defend your organization.

2022-04-25 (WP-PS)

SOPHOS