# Ransomware attacks persist despite rising cybersecurity budgets and law enforcement successes



Research conducted by Veeam has highlighted ongoing challenges in cybersecurity, particularly in combating ransomware, despite an increase in budgets allocated for such measures. The study, which surveyed 1,300 Chief Information Security Officers (CISOs), IT leaders, and security professionals from the Americas, Europe, and Australia, indicated that nearly three-quarters of surveyed businesses had encountered ransomware attacks within the past year.

While there has been a slight improvement, with the rate of businesses affected by ransomware decreasing from 75% to 69%, the study reveals a complex landscape of evolving threats. Notably, the financial response to such attacks has also changed. In 2024, 36% of organisations that were targeted opted not to pay ransoms, and among those that did, 60% paid less than half of the original demands. This shift suggests a growing willingness among businesses to resist extortion, although the overall threat remains significant.

Anand Eswaran, CEO of Veeam, stated, "Organizations are improving their defenses against cyber-attacks, yet 7 out of 10 still experienced an attack in the past year. And of those attacked, only 10% recovered more than 90% of their data, while 57% recovered less than 50%." This underscores the notion that diminished attack rates do not equate to a resolution of the ransomware crisis.

Despite successful law enforcement initiatives targeting prominent ransomware groups like LockBit and BlackCat, these actions have inadvertently led to an uptick in independent attackers, showcasing the constantly shifting nature of cyber threats. As such, Eswaran emphasised the need for a proactive rather than reactive approach to cybersecurity. He urged organisations to adopt resilient data protection strategies, implement strong recovery solutions, and enhance interdepartmental collaboration to mitigate the impacts of ransomware.

The emergence of data exfiltration-only attacks, wherein hackers bypass encryption to access sensitive information directly, further complicates the cybersecurity landscape. Veeam’s findings suggested that while 69% of companies believe they are prepared for an attack, confidence diminishes significantly post-incident, dropping to 44% for those that have tested their backup plans and just 30% having established a formal chain of command.

Investment in strong recovery frameworks, comprehensive training, and cooperation across teams are deemed essential for enhancing resilience against cyber threats. Despite a noted increase in cybersecurity budgets, the study concluded that these investments remain insufficient to effectively counter the sophisticated tactics employed by cybercriminals. Veeam recommends the adoption of stringent procedures, such as the 3-2-1-1-0 data rule, to maintain multiple immutable backups free from malware before any restoration efforts are undertaken.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.veeam.com/blog/announcing-rw24.html> - Veeam's 2024 Ransomware Trends Report surveyed 1,200 IT leaders and implementers, revealing that 76% of organizations experienced at least one ransomware attack in the past year, highlighting the ongoing challenges in combating ransomware despite increased cybersecurity budgets.
2. <https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html> - The report indicates that 41% of data is compromised during a cyberattack, and only 57% of the compromised data is recoverable, underscoring the significant data loss and business impact resulting from ransomware attacks.
3. <https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html> - Veeam's findings suggest that while 69% of companies believe they are prepared for an attack, confidence diminishes post-incident, with only 44% for those that have tested their backup plans and just 30% having established a formal chain of command.
4. <https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html> - The report highlights that 63% of organizations are at risk of reintroducing infections while recovering from ransomware attacks, emphasizing the need for comprehensive recovery strategies to prevent reinfection.
5. <https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html> - Veeam recommends the adoption of stringent procedures, such as the 3-2-1-1-0 data rule, to maintain multiple immutable backups free from malware before any restoration efforts are undertaken, enhancing resilience against cyber threats.
6. <https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html> - The report underscores the importance of proactive cybersecurity measures, including resilient data protection strategies, strong recovery solutions, and enhanced interdepartmental collaboration to mitigate the impacts of ransomware.
7. <https://www.techradar.com/pro/more-than-7-out-of-10-businesses-worldwide-have-sustained-a-ransomware-attack-in-2024-heres-what-you-need-to-know-about-this-epidemic> - Please view link - unable to able to access data