

Ransomware attacks are escalating.

According to Veeam's 2024 Ransomware Trends report, it was found that...



Bad actors will now target your backup.

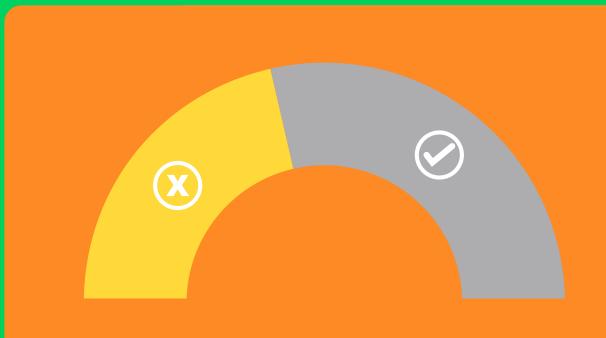
of attacks targeted backups and

were successful.

Paying ransom ≠ solution

The ransom is only

of the financial impact organizations will experience.



affected data won't be recoverable.



Where does Malaysia stand?

Malaysia's new Cyber Security Act emphasises prevention, urging agencies to implement multi-layered security measures, with backups as crucial defense. The 4 key requirements of the Act are:



Act 1

Provide information on critical infrastructure.



Act 2

Implement code of practice.



Act 3

Conduct cyber security risk assessment and audit.



Act 4

Give notification on cyber security incident.

Malaysia's cybersecurity authorities advise companies hit by ransomware to refuse paying cyber criminals and seek assistance from the Cyber999 service, filing reports online.

Fortifying Against Ransomware: Veeam's Alignment with Malausian Cuber Securitu Act Strateaies

Prevent Attacks



Application Control



Patch **Applications**



Configure Microsoft Office Macro Settings



Application Hardening

Limit Impact of Cyber Attacks



Restrict Admin Access



Patch Operating System **Vulnerabilities**



Implement Multi Factor Authentication

Data Recovery and System Availability



Daily Backups

Download the full whitepaper: Comprehensive Ransomware Mitigation Strategies for Malaysia