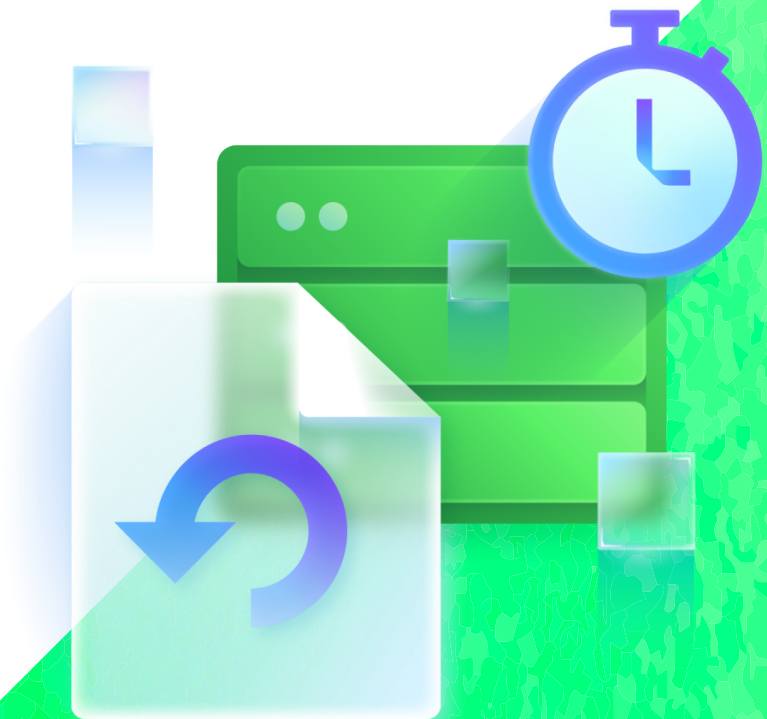




Strategies to Counter the Ransomware Threat in Malaysia

August 2025



Contents

What Ransomware Looks Like Today	4
The Latest Regulatory Requirements in Malaysia	5
Responding to a Ransomware Incident in Malaysia	7
Work with Veeam to Fight the Ransomware Scourge	10
What Makes You Better Prepared?	12

© 2025 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

NOTE:

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Introduction

In the face of a rapidly evolving cyberthreat landscape, ransomware remains one of the most persistent and devastating risks for enterprises worldwide. In 2025, it continues to plague organizations big and small, as these attacks originate from both established groups and a growing number of “lone wolf” attackers.

Failing to prepare thoroughly can cost an organization significant time and money, as well as trust among stakeholders, Veeam 2025 Ransomware Trends and Proactive Strategies Report revealed this year.

The study captured insights from 900 enterprise respondents across 1,300 organizations in key industries and geographies, all of whom experienced a ransomware incident in the past year.

High-profile attacks in the past have forced organizations to be better prepared – and while the proportion of companies impacted by ransomware attacks has fallen from 75% to 69% today - ransomware is no less destructive.

From costly ransoms to data exposure, victims often take years to recover from the monetary, reputational and operational impact. The challenge will be greater as ransomware and extortion threats morph to include multiple attacks and threaten data backups.

One of the most striking ransomware attacks in Malaysia occurred in March 2025, when an airport was hit by a cyberattack that set back operations temporarily. The criminals’ demand for US\$10 million in ransom was refused.

Indeed, Malaysia has seen ransomware threats multiply in the past year. Digital Minister Gobind Singh Deo has told [local media](#) that the country faced a staggering 78 per cent increase in ransomware cases in the fourth quarter of 2024.

Recent ransomware attacks in Malaysia show the drastic impact they can have on everyday life, from disrupting crucial infrastructure to causing heavy business losses. The Cyber Security Act and related regulations will help align the defensive strategies for organizations by ensuring more stringent requirements are met to better counter future threats.

For organizations in Malaysia, this whitepaper explores the readiness, impact, and response strategies that they should employ to better defend against the persistent ransomware threat.

It analyzes the updated regulatory landscape in the country and provides guidance for best-practice adoption to ensure compliance with regulations such as the Cyber Security Act 2024 and requirements for organizations to adopt a more structured and resilient approach to cyber risk management.

What Ransomware Looks Like Today

To ward off ransomware attacks, organizations must understand how they are evolving. The Veeam 2025 Ransomware Trends and Proactive Strategies Report provides a snapshot of the biggest threats today, revealing that many organizations across the world are ill-prepared for such attacks:



Multiple attacks are the norm

Defending simultaneously against many attacks is not easy. In the past year, 69% of impacted organizations suffered multiple ransomware attacks, averaging 2.2 attacks per organization.



Preparation is often illusory

While 69% felt prepared prior to the attack, only 55% believed they were once the attack occurred. The number of respondents who felt unprepared rose by over 160% post-incident.



Backup systems under siege

A staggering 90% reported that attackers attempted to impact backups, with 66% confirming backup compromise. On average, 34% of repositories were modified or deleted.



Playbooks lack critical components

Despite 98% of organizations claiming to have a ransomware playbook, none of the 11 critical response elements were implemented by a majority. Most had only 3–4 elements in place.



Server recovery expectations often missed

Fewer than 1 in 5 organizations recovered more than 80% of servers as expected, with average recovery from backups sitting at 64%.



Budgetary shifts reflect awareness

Organizations are increasing their 2025 budgets by 15% for prevention and 13% for recovery, reflecting a growing awareness of the need for comprehensive cyber resilience strategies.

The Latest Regulatory Requirements in Malaysia

In recent years, Malaysia has taken significant steps to strengthen its cybersecurity and data governance posture. With the introduction of the Cyber Security Act 2024 and various supporting regulations, organizations across all industries—especially in financial services, healthcare, and the public sector—must adopt a more structured and resilient approach to cyber risk management. The country's cybersecurity ecosystem is shaped by both cross-industry laws that apply broadly, and sector-specific frameworks designed to address the unique risks of regulated sectors.

Cross-Industry Cybersecurity Frameworks and Acts

The Cyber Security Act 2024, which came into force on [Aug. 26, 2024](#), serves as Malaysia's core cybersecurity legislation. It introduces a national framework applicable to both public and private sector entities, especially those designated as National Critical Information Infrastructure (NCII). These entities operate in vital sectors such as finance, energy, telecommunications, and healthcare.

Under the Cyber Security Act, NCII entities are required to conduct annual cybersecurity risk assessments and undergo audits at least once every two years. Organizations must also report any significant cybersecurity incidents promptly to the National Cyber Security Agency (NACSA). Oversight of national cybersecurity policy is led by the National Cyber Security Committee, chaired by the Prime Minister.

In addition, companies providing cybersecurity services, such as managed detection and response (MDR), penetration testing, or vulnerability scanning, must be licensed by NACSA. Operating without such a license may result in penalties of up to RM500,000 and imprisonment of up to 10 years.

To support the Cyber Security Act, several subsidiary regulations have also been introduced:

- The Cyber Security (Risk Assessment & Audit) Regulations 2024 mandate annual and biennial reviews for NCII entities.
- The Cyber Security (Incident Notification) Regulations 2024 specify how and when incidents must be reported.
- The Cyber Security (Compounding of Offences) Regulations 2024 outline offences that can be resolved without criminal proceedings.

Besides the Cyber Security Act, Malaysia's Personal Data Protection Act remains important for organizations operating in the country. In 2024, it was amended to provide more clarity and scope, such as expanding the definition of sensitive personal data to include biometric data. At the same time, [penalties](#) for non-compliance with data principles under the law have also been increased to fines of up to MYR1,000,000 and/or imprisonment up to three years.

Together, these laws and regulations form a baseline cybersecurity compliance framework for all Malaysian organizations, particularly those that support national infrastructure or provide security services.

Sector-Specific Cybersecurity Regulations

Financial Services Sector

Entities in the financial sector, such as banks, insurers, and capital market participants, must comply not only with the Cyber Security Act 2024 but also with sectoral guidelines from Bank Negara Malaysia (BNM) and the Securities Commission (SC).

[BNM's Risk Management in Technology \(RMiT\)](#) policy framework requires financial institutions to maintain secure IT infrastructure, conduct regular risk assessments, implement incident response protocols, and ensure resilience against cyberthreats. These obligations align closely with NACSA's expectations, creating a dual-regulatory compliance environment.

Financial institutions must prioritize data protection, ransomware preparedness, secure backup systems, third-party risk assessments, and incident response drills to remain compliant and resilient.

Healthcare Sector

Healthcare organizations, particularly those handling electronic medical records or delivering public healthcare services, are considered critical infrastructure under the Cyber Security Act 2024. As NCII entities, they must fulfill annual cyber risk assessments, incident reporting requirements, and NACSA-led audits.

Additionally, the Personal Data Protection Act enacted in 2010 also applies to the sector, which oversees and manages a large amount of sensitive personal data, which is often the target of ransomware gangs.

Government & Public Sector

Government ministries, agencies, and national service platforms are automatically covered under the Cyber Security Act 2024 and must adhere to all reporting and security audit obligations. These entities are also expected to implement internal cyber teams, maintain annual compliance plans, and align with NACSA's response protocols.

Responding to a Ransomware Incident in Malaysia

As ransomware threats continue to escalate in complexity and frequency, organizations in Malaysia — especially those classified as NCII or offering cybersecurity services — must adopt a structured, proactive, and compliant incident response strategy. The following guidelines align with the Cyber Security Act 2024, its supporting regulations, and NACSA's expectations for cyber incident management:

1. Preparation (Pre-Incident Readiness)



Establish a Cybersecurity Incident Response Team (CSIRT), including IT, legal, compliance, and communications representatives.



Create and regularly update a ransomware-specific incident response plan, integrated with national reporting requirements under CSA 2024.



Conduct annual cyber risk assessments and biennial audits as required for NCII entities.



Implement immutable and air-gapped backup systems and conduct recovery drills regularly.



Deliver cyber awareness and phishing training to all employees and service vendors.

2. Detection and Triage



Utilize EDR, SIEM, and intrusion detection tools to monitor systems for ransomware signatures, encryption behavior, or external command-and-control traffic.



Identify and isolate infected systems immediately to prevent further spread.



Begin incident classification and logging, determining the severity and impact on critical assets or personal data.



Activate the incident response team and prepare containment actions within the first hour.

3. Containment and Analysis



Quarantine affected endpoints, disable compromised credentials, and preserve forensic evidence (logs, encrypted files, traffic captures).



Engage internal or external cybersecurity experts to determine root cause, attack vector, and scope of data impact.



Initiate internal communications and legal briefings to support decision-making around disclosure, escalation, and recovery options.

4. Reporting Obligations



Notify NACSA promptly if the ransomware attack affects NCII systems or threatens national infrastructure, per the Cyber Security (Incident Notification) Regulations 2024.



If applicable, report the incident to sector leads (e.g., Bank Negara Malaysia for financial institutions, MOH for healthcare).



Ensure logs, evidence, and communications are retained in a regulator-ready format, including recovery timelines, breach indicators, and containment summaries.

5. Recovery and Restoration



Scan and validate backup files using tools like Veeam Secure Restore to ensure malware-free recovery.



Restore affected systems from clean, verified backups stored in immutable repositories or offline media.



Gradually reintroduce systems to the network, while monitoring for persistence or reinfection attempts.



Prioritize restoration of essential business services and customer-facing applications.

6. Post-Incident Review and Mitigation



Conduct a formal post-incident review within 7-10 days to evaluate response effectiveness, data exposure, and gaps in procedures.



Update the incident response plan based on lessons learned, and submit final audit and closure reports to NACSA if required.



Reassess third-party risks and adjust access controls and segmentation to prevent future breaches.



Communicate results and action plans to stakeholders, regulators, and (where applicable) affected customers or individuals.

Regulatory Alignment

Requirement	Applies To	Response Action
Cybersecurity Risk Assessment	All NCII entities	Annual assessments; included in IRP planning
Cybersecurity Audit	All NCII entities	Conducted every two years; integrated into post-incident recovery
Ransomware Incident Reporting	All NCII and licensed cybersecurity providers	Report to NACSA and sector regulators as per CSA 2024 guidelines
Evidence Preservation & Forensics	All entities	Mandatory for regulatory reporting and RCA

Work with Veeam to Fight the Ransomware Scourge

The Cyber Security Act 2024 has introduced a robust regulatory foundation for managing cyber risk in Malaysia, particularly for organizations designated as NCII and those offering Cybersecurity Services. These entities must now demonstrate stronger operational readiness, maintain regulatory-aligned recovery procedures, and meet new mandates for incident reporting, risk assessment, and audit cycles.

Veeam empowers Malaysian organizations to fulfill these obligations with secure, immutable backups, orchestrated disaster recovery, and automated compliance reporting. Meanwhile, Veeam supports the critical breach response phase—offering ransomware negotiation (when permissible), root-cause forensics, and post-incident reporting aligned with NACSA expectations.

Together, Veeam + Veeam help regulated entities in Malaysia meet CSA 2024 mandates while maintaining operational resilience and minimizing recovery time in the face of ransomware attacks.

Framework Layer	Description	Veeam and Veeam Support
Governance	Ensure board-level accountability and compliance with CSA 2024 and licensing obligations	Veeam provides audit trails and backup policy governance as well as delivers post-incident summaries for NACSA reporting
Risk Management	Conduct annual cyber risk assessments and define impact-based recovery goals	Veeam enables simulated recovery testing and provides ransomware trend intelligence as well as breach insights
Incident Response	Respond to ransomware incidents and fulfill mandatory NACSA reporting requirements	Veeam assists with forensic triage, negotiation support, and regulator-ready incident summaries
Backup & Immutability	Maintain tamper-proof, verifiable backups to enable recovery in compliance with NCII standards	Veeam offers Hardened Repositories, Object Lock (S3), and air-gapped backup configurations
Data Protection	Secure personal and business data with traceability, access control, and recovery transparency	Veeam enforces encryption, RBAC, and secure recovery workflows; in addition to identifying exposed data for regulatory disclosures
Monitoring & Alerts	Detect early signs of compromise and backup anomalies	Veeam offers anomaly detection within backup chains and tracks attacker tactics as well as common compromise indicators
Recovery & Restoration	Rapidly restore from clean, malware-free backups and minimize downtime	Veeam delivers SureBackup and Orchestrated Restore as well as validates recovery process against malware persistence
Regulatory Reporting	Generate compliance documentation for audits and breach notifications	Veeam logs backup and restore actions in addition to compiling formal reports required by NACSA and sector regulators

This solution is ideal for:

- * NCII-classified organizations under the CSA 2024
- * Financial, healthcare, telecom, and public sector operators
- * Licensed cybersecurity service providers requiring resilient internal controls

What Makes You Better Prepared?

Veeam's study of organizations impacted by ransomware shows that some were better prepared than others. These were the ones with resilient, proactive data protection strategies and best practices in place.

They also conducted regular penetration testing and invested in post-attack improvements such as cybersecurity training and enforcing multi-factor authentication (MFA). They also had more complete and tested ransomware playbooks, including backup verification and communication planning. Notably, they were less dependent on third-party services during recovery.

These findings highlight the need to treat ransomware not as a one-off crisis, but as an ongoing operational threat. Organizations need to prepare with a structured, long-term approach that strengthens prevention, response and recovery capabilities.

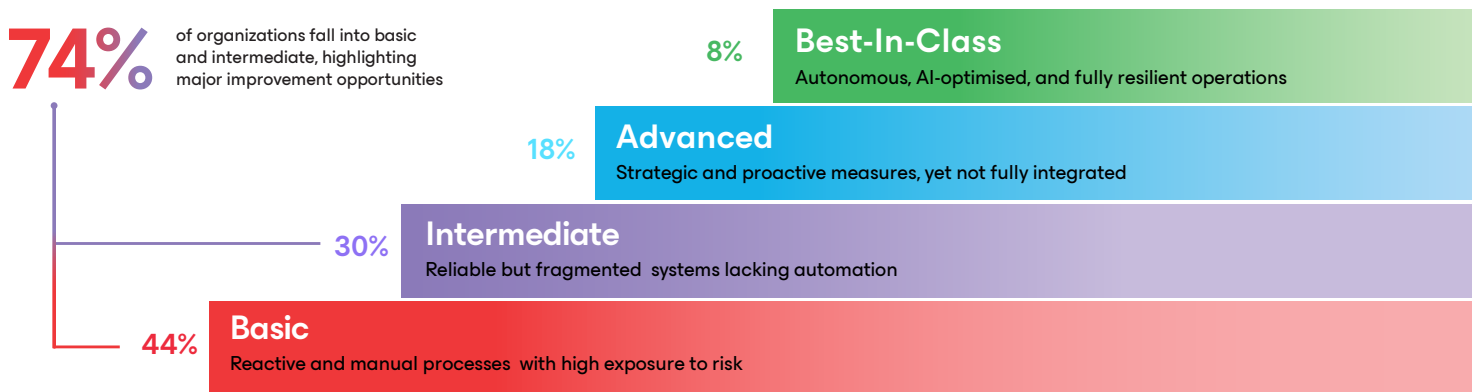
Building Resilience with the Veeam DRMM

To help organizations take the next step, Veeam developed the DRMM in collaboration with McKinsey & Company and other industry experts.

The DRMM is a structured framework that allows organizations to assess and benchmark their current data resilience posture, identify areas for improvement, and implement targeted changes to demonstrate quantitative improvements. It brings together strategy, people, processes, and technology to improve an organization's ability to withstand and recover from disruption.

Four Horizons of Data Resilience Maturity

Organizations at the Best-in-Class level recover from outages faster, experience less downtime, and suffer less data loss compared to others.

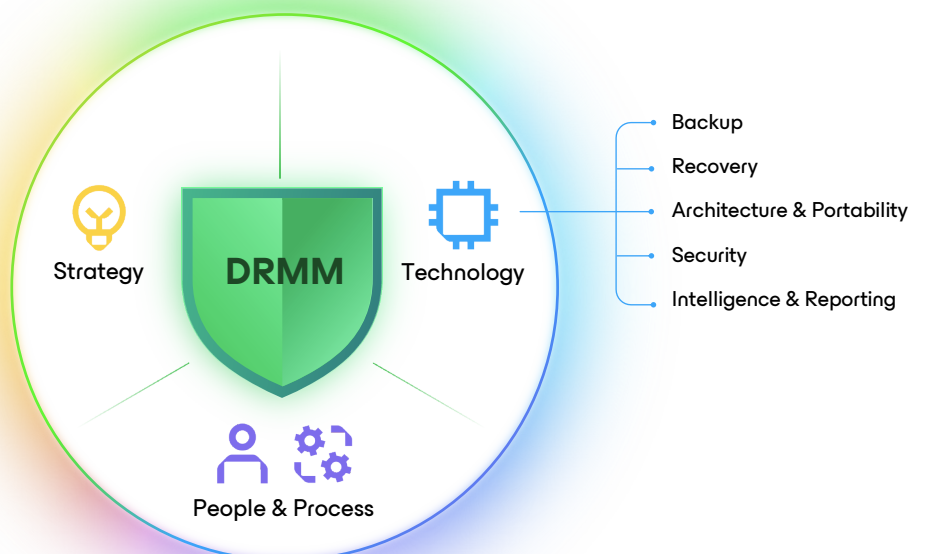


Assess and Improve Your Data Resilience

The DRMM serves as a practical tool to help organizations:

By adopting the DRMM framework, organizations can move from reactive incident response to proactive resilience improvement. This ensures that data remains protected, integrous, recoverable, and available in the face of evolving cyberthreats.

[Download this e-book](#) to learn more about the Veeam DRRM and how it can help you strengthen your ransomware defense strategy.



Veeam: A Trusted Leader In Data Resilience

As organizations continue to navigate rising ransomware threats and evolving compliance requirements, trusted solutions are critical to maintaining data availability, integrity, and recoverability.

Veeam has consistently been recognised for its leadership in this space. According to the IDC Semi-Annual Software Tracker 2H2024, Veeam holds the number one market share position in the data protection software market across the Asia Pacific and Japan (APJ) region, with an 11.4 percent share.

This recognition reflects the growing confidence that organizations place in Veeam's ability to deliver reliable, secure, and modern data resilience solutions. By combining advanced protection capabilities with trusted expertise, Veeam enables enterprises to strengthen ransomware defense, simplify recovery, and meet regulatory demands with confidence.

→ Learn more at www.veeam.com

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 67% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) and X [@veeam](https://twitter.com/veeam).