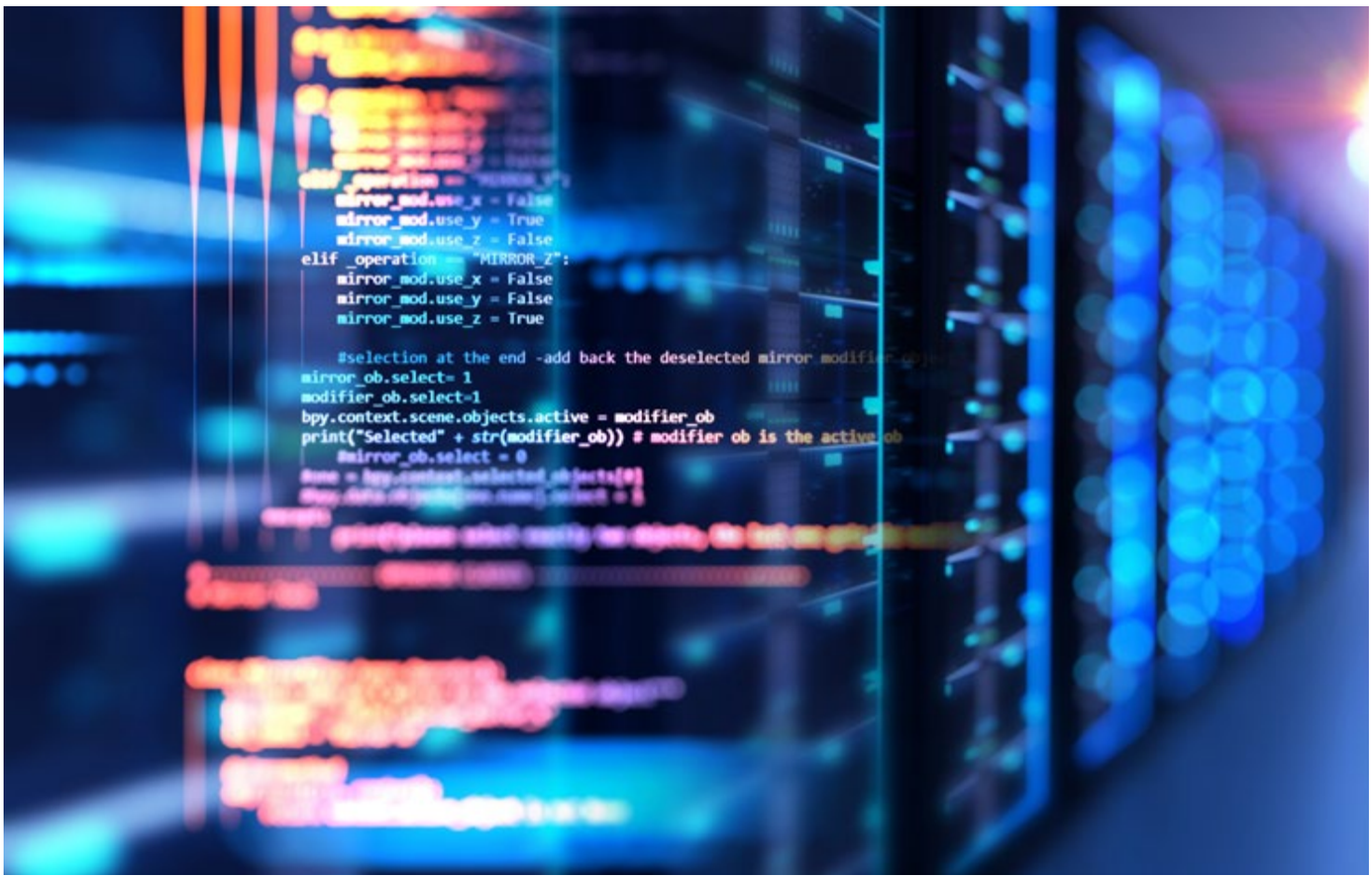
CYBER SECURITY



WHY WE CARE

Given the nature of our business as a digital enabler, we face various cyber security risks and threats that can have severe consequences for our society, businesses and the Government. A cyber attack on our network infrastructure can force us to shut down critical services, disrupt socio-economic well-being and cause major losses for TM. Protecting our digital landscape is crucial to avoid such consequences.

Moreover, cyber breaches can lead to the loss of critical stakeholder information. Successful attacks can result in severe impacts on both individual and business customers, including credit card and identity theft, sensitive information leaks and reputational damage. Therefore, we have a responsibility to protect and manage the data entrusted to us.

What Our Stakeholders Expect

- Protection against cyber crime and threats
- Responsible use of stakeholder data
- High-quality and continuous network service

WHAT IS OUR APPROACH

TM's cyber security is overseen by the Group Information Security (GIS). Our goal is to continuously improve our cyber security governance, compliance, risk management and operations management throughout our business. Through these programmes, we are able to build infrastructure protection against cyber threats, protect stakeholder data and ensure the high availability of our critical services at all times. The GIS team is critical to our business continuity and ensuring a secure experience for our customers and stakeholders as we advance our digital objectives.

Our cyber security efforts are governed by the following policies, frameworks and certifications to ensure we deliver world-class protection at all times:

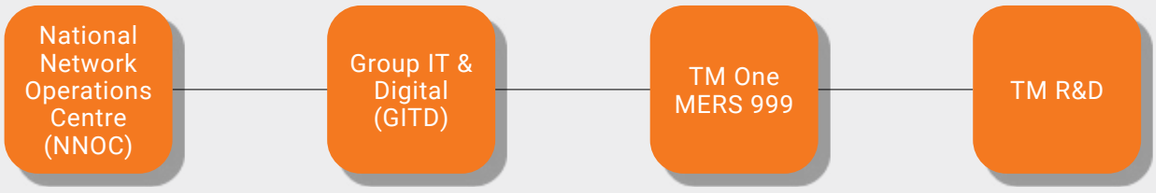
- TM's Information Security Policy
- Information Security Management System (ISO/IEC27001, ISO/IEC27017, ISO/IEC27018)
- Payment Card Industry Data Security Standards (PCI DSS)
- BCMS

Deployed Capitals: *Met Strategic Aspirations:* *Stakeholders Affected:* *Sustainability Impact:*

HOW WE CREATED VALUE IN 2022

1 Enhancing Our Security Policies & Standards

Our GIS team regularly reviews and updates our Information Security Policy and TM's cyber security standards based on evolving risks and threats to our business assets. We also maintain ISO/IEC 27001 certifications to manage and govern information in various operational areas:



We also received certifications for our various systems and platforms, particularly for those that customers regularly utilise.

TM One Cloud Alpha Edge	Achieved certifications in: • ISO/IEC 27001 ISO/IEC 27017 & ISO/IEC 27018 • PCI DSS Certification
TM Payment Gateway (PG) System	Sustained PCI DSS Certification
Business Continuity Management System (BCMS)	Included GIS Security Operation Centre (SOC) within the scope of BCMS Operation of TM NOC Gallery certification.

2 Strengthening Security Measures

Cyber security needs to evolve constantly with the dynamic digital landscape. It requires continuous improvements in our fundamentals and systems. Therefore, we continue to strengthen our cyber security measures to ensure they remain resilient and robust.

What We Did in 2022	Achievements
Expanded our Centralised Vulnerability Assessment System (CVAS) to continuously scan and identify security issues on TM information assets	261 systems/applications on boarded onto CVAS for 5,109 assets
Conducted regular security assessments and penetration testing by internal and external teams	>5000 IP addresses security assessment and penetration testing by internal and external teams
Enhanced Endpoint Security Management to protect against security incidents	18,238 corporate devices have been installed with End Point Protections
Fortified Identity and Access Control Management	Enablement of Multifactor Authentication (MFA) at network gateways for remote working personnel and vendors, as well as corporate email access
Enabled data protection at Microsoft O365 cloud and endpoint for devices with TM data	Enabling data protection email and endpoint devices (MDM/ MAM) where TM business data resides
Adopted Security by Design to ensure security control standardisation across assets and effectiveness is measurable	Enhance existing security baseline, incorporating security requirements from design architecture and contractual terms, until implementation of digitalisation initiatives

3 Elevating Our Cyber Security Culture

The responsibility to protect our business and customers from cyber threats, does not solely rest with the GIS team. It requires groupwide effort and awareness to ensure all employees and related stakeholders uphold the highest standards of cyber security practices. Therefore, throughout 2022, we implemented various programmes and awareness sessions designed to enhance our cyber security culture across the Group.

CYBER SECURITY AWARENESS PROGRAMMES 2022

TM's Cyber Security Response Drills

Objective:
To increase our employee's awareness and preparedness against potential cyber attacks.

What We Did:
We organised a drill exercise that exposed network, system, application, cloud administrators and engineers, as well as security analysts to multiple cyber attack scenarios. This enabled us to understand their preparedness to managing potential cyber related crises and close any gaps.

Impact:
70 cyber technical employees across ten (10) lines of business

Cyber Security Webinars

Objective:
To fortify our employee's awareness on the cyber secure culture at workplace, strengthening TM against cyber attacks as 'Human Firewall'.

What We Did:
To introduce our employees to the current state of the cyber security threat landscape and workplace cyber security best practises, we hosted a cyber security webinar session. This is to enable interactive engagements of employees with subject matter experts in security, for greater understanding and appreciation of cyber security best practices in their daily activities, which will significantly strengthen TM's defences against cyber attacks.

Impact:
524 employees across the Group (including subsidiaries)

Security Awareness Packs

Objective:
To ensure that employees understand and are aware of their potential contribution to continuous effort in strengthening and enforcing the organisation's cyber security policies and posture.

What We Did:
We delivered continuous fortnightly security awareness and advisory information via email to all employees to keep them updated on development of cyber attacks and countermeasures.

Impact:
100% of employees reached

Email Phishing Simulation Campaign

Objective:
To strengthen employees use of the best practices for protecting themselves against potential phishing scams.

What We Did:
We conducted an email phishing simulation exercise, in which we sent out simulation phishing emails to nearly 18,000 mailboxes as part of simulation exercises in TM to gauge and promote cyber security awareness in Q1 and Q4, 2022.

Impact:
100% of employees reached

Positive reduction in employees compromised:
Phase 1: 23% **Phase 2: 7%**

External Engagements for Best Practices

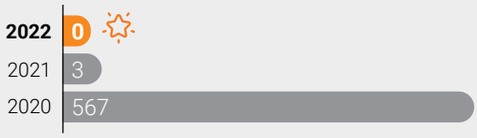
Objective:
To engage with external stakeholders and experts to shape and encourage cyber security culture and awareness across industry and across sectors in Malaysia.

What We Did:
We participated and contributed to the Communication & Digital industry technical code development with Malaysia Technical Standard Forum Berhad (MTSFB), as well as organised a knowledge-sharing session on cyber security with educational institutions, that is Universiti Kuala Lumpur (UniKL) and Universiti Malaya (UM).

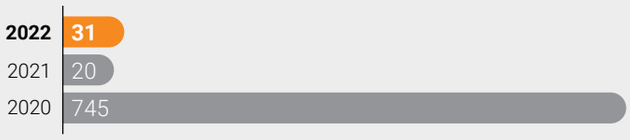
4 Overall Performance

We are pleased to report zero cases of data loss in 2022, despite an increase in online breaches and data-related incidents. Increase of incidence ticket was due to the improvement of security tools, controls and resources resulting in greater threat visibility and early detection. This reflects the robustness of our system, which is prepared to counteract the rising trend in cyber attacks in the market.

Number of data loss



Number of online breaches



Number of cyber security incidents resolved/handled

Number of data-related incidents