

PCI SSC 2026
ASIA-PACIFIC COMMUNITY MEETING

Mind the Gap: Bridging Compliance Requirements and Real-World Security

From meeting requirements to surviving real-world attacks

Speaker

Mr. Fong Choong Fook

Founder & Managing Director, LGMS Group

Agenda

01	**Recognising the Gap**	*Where control presence and control effectiveness diverge*
02	**The Attacker's Path**	*Where PCI DSS cycles and attacker clocks diverge*
03	**Outcome-Driven Security**	*From minimum cadence to demonstrated resilience*
04	**The Boardroom Takeaway**	*Four leadership actions, and three questions to carry home*

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

About Us

Speaker & Company Introduction





Mr. Fong Choong Fook

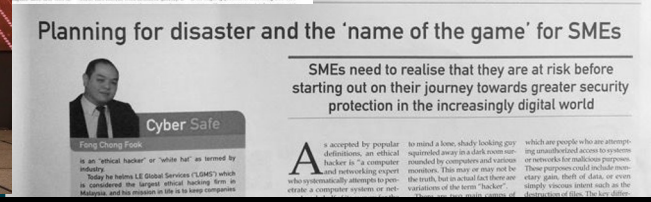
Founder and Managing Director of LGMS Berhad











PIKOM Digital Excellence Awards – Tech Entrepreneur (Cybersecurity) of The Year 2024

Author of Certified Lead Forensic Examiner Program (PECB, USA)

Cyber Security Malaysia – Cyber Security Professional of The Year 2022

IDC ASEAN Chief Security Officer of The Year 2013

Qualifications:

- Bachelor of Information Technology (CSU, Australia)
- PCI ASV (International)
- GIAC Forensic Examiner (GCFE – SANS), USA
- Certified Information Systems Security Professional (CISSP) – International
- Certified Fraud Examiner (CFE) – USA
- Certified Cellebrite Logical Analyst (CCLA)
- Certified Cellebrite Physical Analyst (CCPA)
- Certified Penetration Testing Specialist (CPTS) – USA
- Certified Information Security Manager (CISM) – International
- Certified in Risk and Information System Control (CRISC) – International
- PECB Certified ISO 27001 Master – USA
- Certified Information Systems Auditor (CISA) – International
- Sun Certified Information System Administrator (SCSA) – USA
- Microsoft Certified Systems Engineer (MCSE) – USA
- Certificate of Cloud Security Knowledge (CCSK) – International
- Certified in COBIT Foundation – International
- PRINCE2 – UK

20 YEARS OF SECURING PAYMENT DATA

ABOUT LGMS









A leading cyber security expert in Asia Pacific – trusted by multinational corporations around the world.

Since 2005
21 Years
Of Experience

Independent
Product Agnostic
Security Assessors

More than **1,000**
Satisfied Local and Global Clients

FROST & SULLIVAN
Malaysian Professional Security Services
Customer Value Leadership
2026

Gartner
Market Guide
Representative Vendor
CCIR Retainer Services
2026

Gartner
Market Guide
Representative Vendor
DFIR Retainer Services
2025

PIKOM
DIGITAL EXCELLENCE AWARDS 2025

ASOCIO
Tech Excellence Awards
2025

Top Employer
of the Year
Public Listed Sector
2025

Top Employer
of Best Workplace
Public Listed Sector
2025

Top Employer
of Best Workplace
Private Sector
2025

PIKOM
DIGITAL EXCELLENCE AWARDS 2024

Internet Alliance
Gold Winner in
Digital Intelligence
2024

Cyber Security
Product Innovation
of the Year
2023

isg
Leader in Strategic
Security Services
2022, 2023

isg
Leader in Technical
Security Services
2022, 2023

Cyber Security
Company
of the Year
2022

ASOCIO
Tech Excellence
Awards
2022

IDC
IoT Key Penetration
Testing Vendors
2018

Cyber Security
Company
of the Year
2017

ISO 27001:2022
9001:2015

ISO 17025:2017
Accredited
Laboratory

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

01

Recognising the Gap

Where control presence and control effectiveness diverge.



The Patch Load Is Growing

Microsoft October Patch Tuesday: 2025 versus 2026.

Metric	October 2025	October 2026	Change
Flaws Fixed	172	1,411	+720% *(about 8x)*
Critical Flaws	8	70	+775% *(about 9x)*

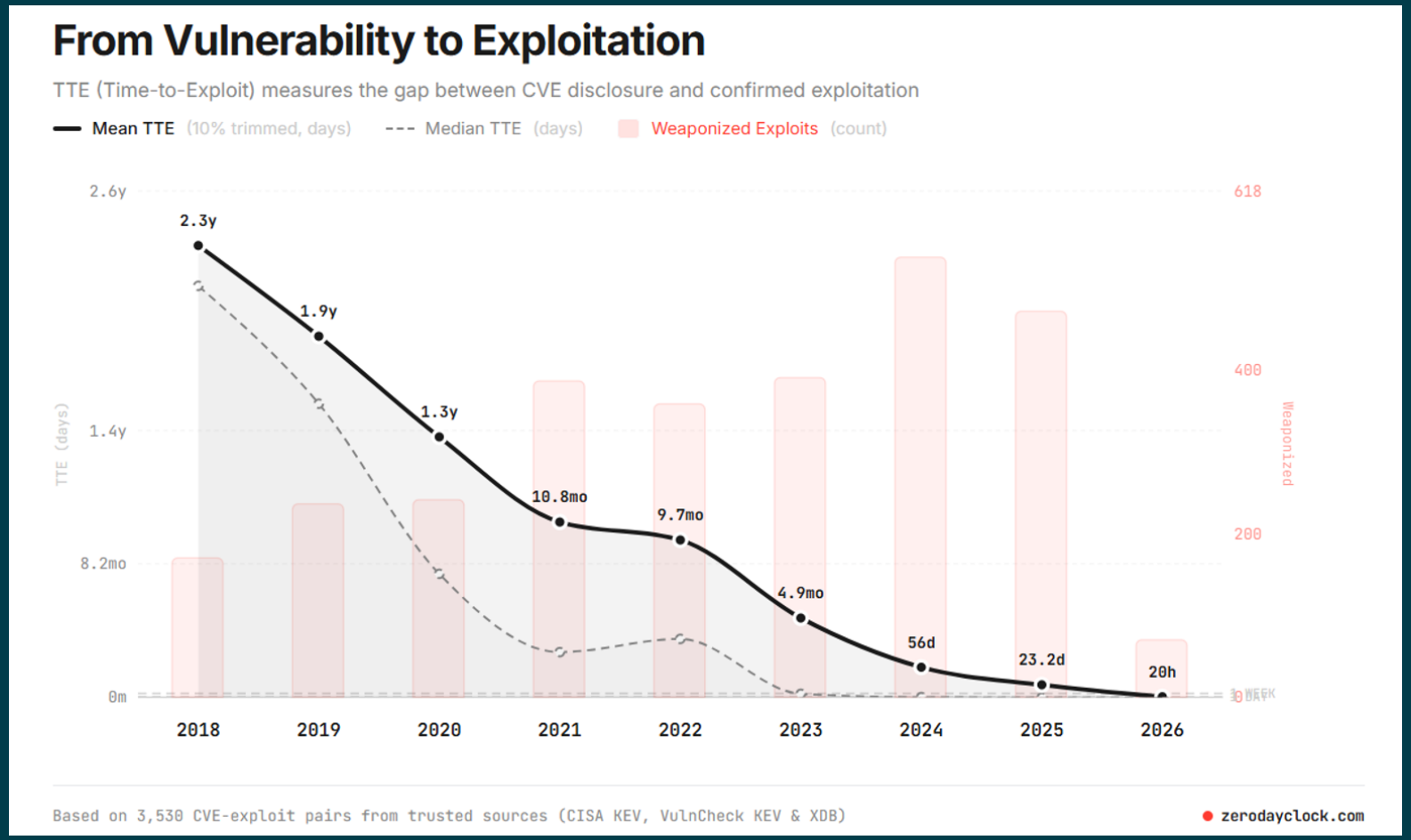
More flaws to triage.
Critical patches are still due within one month.

Source: BleepingComputer, Microsoft Patch Tuesday reports, October 2025 and October 2026 (Patch Tuesday releases only); PCI DSS v4.0.1, Req. 6.3.3.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Automation Outpaces Human Response

Exploits arrive in hours. The patch deadline is still one month.



Automated reconnaissance bots scan the entire public internet in **minutes**, not weeks.

Manual triage, approval and patch cycles cannot compress at the same rate.

Net effect:
The human-led defence window is collapsing from **years to hours**.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Compliant on Paper. Exposed in Practice.

What compliance confirms

1. **Policies are defined**
2. **Controls are implemented**
3. **Evidence is available**

A point-in-time view of control presence

THE GAP

Controls exist. Do they hold?

What an attacker tests

01	02	03	04
EXPOSURE	IDENTITY	MOVEMENT	IMPACT
What is open?	Whose access can I use?	How far can I go?	What can I disrupt?

A connected path to business impact

The gap often exists between control presence and control effectiveness.

Context: 61% of organisations identify the rapidly evolving threat landscape and emerging technologies as a leading challenge to strengthening cyber resilience. Source: World Economic Forum, Global Cybersecurity Outlook 2026.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

02

The Attacker’s Path

Where PCI DSS cycles and attacker clocks diverge.



The Cadence Gap

PCI DSS Minimum Cadence

- **Daily** — Log review · 10.4.1
- **Weekly** — Payment-page checks · 11.6.1
- **Within a month** — Critical patches · 6.3.3
- **Every 3 months** — Scans · 11.3.1 · 11.3.2
- **Six-monthly** — Access reviews · 7.2.4
- **Annually** — Segmentation · 11.4.5

Attacker Clock

29 min
Average time to move laterally

−7 days
Mean time to exploit (pre-patch)

247 days
To detect and contain a breach

> **The gap sits between the cycles.**

Source: PCI DSS v4.0.1; CrowdStrike 2026; Mandiant M-Trends 2026; IBM 2026.

20 YEARS OF SECURING PAYMENT DATA

REGIONAL INCIDENT

Case Study

One Trusted Path. Enterprise-Wide Consequences.

(October 2025)

ONE ORGANISATION. SHARED CONSEQUENCES.

Industry

B2B commerce & logistics

Country

Japan

Summary of Incident

- **Company estimate:** entry via compromised credentials for a partner's administrator account that lacked MFA.
- **Order processing and logistics** operations were affected.
- Downstream business customers and partners experienced knock-on disruption.

Source: Company statements, as reported by BleepingComputer; The Record.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

A Breach May Take Minutes. Recovery Can Take Months.

The impact of an incident extends far beyond initial compromise.

- Compromise
- Detection
- Containment
- Investigation
- Recovery
- Regulatory & customer response
- Trust rebuilding

USD 4.99m

Global average total cost of a data breach in 2026 — a record, up 12% year on year.

247 days average time to identify and contain a breach — reversing five consecutive years of improvement

Cyber resilience is as much about limiting consequences as preventing entry.

Source: IBM, Cost of a Data Breach Report 2026 — 602 breaches analysed, March 2025 to February 2026.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Identity and Third-Party Access

Same requirements. A harder test.

8.4.2 · 8.4.3

MFA on Every Path In

REALITY

MFA stops the login. A stolen session skips it.

8.2.7 · 12.8

Partner Access

REALITY

A breached vendor logs in with valid credentials and looks normal.

7.2.4

Access Reviews

REALITY

Reviews run every 6 months. Attackers need hours.

Controls cover the accounts you know about.
Attackers use the ones you missed.

Source: PCI DSS v4.0.1, Req. 7.2.4, 8.2.7, 8.4.2, 8.4.3, 12.8.

20 YEARS OF SECURING PAYMENT DATA

Scope Moves Faster Than Assessments

Annual checks describe one day. Attackers use every day.

1.2.3

Know the Network

REALITY

The diagram shows what was approved. Attackers map what exists.

12.5.2

Confirm the Scope

REALITY

Scope is confirmed on one day. The estate changes every day.

11.4.5

Test the Segmentation

REALITY

Testers get a scope. Attackers don't.

Can a compromised endpoint reach the cardholder data environment today?

Source: PCI DSS v4.0.1, Req. 1.2.3, 11.4.5, 12.5.2.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

0 3

Outcome-Driven Security

From minimum cadence to demonstrated resilience.



Stop Asking Only: “Are We Compliant?”

INSTEAD OF

“Do we have network segmentation?”

ASK

“Can a compromised endpoint reach our critical systems?”

PCI DSS 11.4.5

INSTEAD OF

“Do we have MFA?”

ASK

“Can stolen or compromised credentials alone grant privileged access?”

PCI DSS 8.4.2 · 8.4.3

INSTEAD OF

“Do we have backups?”

ASK

“Can critical operations recover within an acceptable timeframe?”

PCI DSS 12.10.1

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Resilience Equation



COMPLIANCE

Defines the baseline

+



CONTINUOUS VALIDATION

Proves effectiveness

+



RECOVERY READINESS

Limits consequences

=



Cyber Resilience

The objective is not to replace compliance.
It is to make security controls perform in the real world.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Minimum Cadence Versus Resilient Practice

Same requirement. A different burden of proof.

Requirement	Minimum	Resilient Practice
Scanning · 11.3.1 · 11.3.2	At least once every 3 months	*Threat-triggered scans*
Patching · 6.3.3	Critical within one month	*Exploited flaws first*
MFA · 8.4.2 · 8.4.3	CDE and remote access	*Test bypass, partners included*
Log Review · 10.4.1	Reviewed daily	*Alert on behaviour, not events*
Payment Pages · 6.4.3 · 11.6.1	Scripts authorised, checked weekly	*Monitor scripts at runtime*
Recovery · 12.10.1	Plan includes recovery	*Rehearse and time the restore*

> **Compliance sets the floor. Validation shows it holds.**

Source: PCI DSS v4.0.1, Req. 6.3.3, 6.4.3, 8.4.2, 8.4.3, 10.4.1, 11.3.1, 11.3.2, 11.6.1, 12.10.1.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council



Compliance Is the Floor.
Resilience Is the Standard.

Compliance establishes the baseline.
Continuous validation proves whether it holds.
Resilience is the outcome.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

04

The Boardroom Takeaway

Four leadership actions, and three questions to carry home.



Four Actions Leaders Can Take

01

Validate continuously

Evidence between assessments, not only at them.

02

Secure identity & third-party access

Review privileged and partner accounts continuously.

03

Test beyond minimum scope

Test how weaknesses connect.

04

Report resilience outcomes

Attack paths remaining. Time to detect, contain, recover.

Large Companies Naming Third-Party and Supply-Chain Vulnerabilities Their Greatest Challenge



Only 27%

of organisations simulate cyber incidents or run recovery exercises.

Measure security by demonstrated capability, not only completed controls.

Source: World Economic Forum, Global Cybersecurity Outlook 2026.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Three Key Questions

1. Which security control do we trust today but have never realistically challenged?
2. If an attacker obtained one legitimate identity tomorrow, how far could they go?
3. If a critical system went offline tonight, could we prove how quickly the business would recover?

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You!

Scan to stay connected with us.

+603-8605 0155

info@lgms.global

www.lgms.global

Follow Us
https://lgms.global/follow/

20 YEARS OF SECURING PAYMENT DATA