PCI Security Standards Council

Charting the Course: Assessing 2024's Payment Security Scene, Predicting 2025's Trends

Insights & Forecasts for Payment Security Professionals

Speaker
Mr. Gilbert Chu Kim Foong
Chief Operating Officer of LGMS

Content

1. About Us
2. 2024’s Payment Security Landscape
3. Data Breach Cases and Impact
4. Emerging Trends in Payment Security
5. Actionable Strategies for Businesses

PCI Security Standards Council®

PCI Security Standards Council

About Us

Speaker &
Company Introduction

Mr. Gilbert Chu Kim Foong

Chief Operating Officer of LGMS | PCI QSA

Qualifications:

He is leading the cybersecurity consultants in LGMS primarily in the cyber security management and compliance segments of LGMS. Gilbert is also a guest speaker for various public events held locally and internationally. Gilbert is qualified in his field in that he holds both academic and professional qualifications.

He provided consultation and training to various government and multinational clients across Asia, Europe and Africa on information system security, enterprise risk design, policy review and implementation assurance, penetration testing, and other technical risk assessment.

Qualifications:

- Bachelor Degree in Business Information System (UCSI, Malaysia)
- ISACA Certified Information Security Manager (CISM) - International
- Payment Card Industry Data Security Standard Qualified Security Assessor (PCI QSA) - International
- Mile2 Certified Penetration Testing Engineer (CPTE) - International
- PECB ISO27032 Senior Lead Cybersecurity Manager (LCM) - International
- PECB ISO27001 Senior Lead Auditor (LA) - International
- PECB Certified Trainer (CT) - International
- PECB ISO9001 Lead Auditor - International
- Malaysia Common Criteria (MyCC) Scheme Foundation Evaluator

PCI Security Standards Council

About LGMS

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

Since 2005
19 Years
Of Experience

Independent
Product Agnostic
Security Assessors

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

PCI Security Standards Council
APPROVED SCANNING VENDOR™

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR™

PCI Security Standards Council
3DS ASSESSOR

ISO 27001:2022 9001:2015

ISO 17025:2017 Accredited Laboratory

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

PCI Security Standards Council®

PCI Security Standards Council®

2024's Payment Security Landscape

Payment Security Landscape

Payment Industry Growth

Global digital payment transactions are expected to grow to 1.84 billion by 2024

Shift to Cashless

Rising adoption of mobile payments, contactless systems

Evolving Fraud Tactics

Fraudsters are continuously adapting their methods, making it essential for the payment industry to stay ahead.

PCI Security Standards Council

PCI Security Standards Council

Key Cybersecurity Threats in 2024: A Closer Look

Key Cybersecurity Threats in 2024

Phishing Attacks

Malware and Ransomware

Data Breaches

PCI Security Standards Council

PCI Security Standards Council®

Data Breach Cases and Impact

Data Breach Cases and Impact

2013

- **An American retail corporation.**
- Data breach that affected over **40 million** payment card accounts.
- The settlement with respective regulator costs **$67 million.**

2017

- **A multinational consumer credit reporting agency.**
- Data breach that affected **143 million** people in the US.
- The company settled with respective regulator for **$1.25 million** in 2020.

2017

- **One of the largest multinational fast-fashion retailer.**
- Data breach for customers who shopped between **April and November 2017.**
- The company paid **$1.1 million** in penalties to the respective regulators.

2018

- **One of the largest airlines based in Europe.**
- Data breach that affected over 400,000 customers.
- The company was **fined $27 million** by the respective regulator.

2018

- **One of the largest hospitality companies.**
- Data breach that affected **500 million** customers.
- The company was fined **$23.8 million.**

PCI Security Standards Council®

Data Breach Cases and Impact (Cont.)

2018

- **A well-known fast-food chain in the Philippines.**
- A data breach compromised over 80,000 customer and job applicant records.
- The respective regulator issued a **72-hour rehabilitation plan** for the company to address website vulnerabilities.

2019

- **One of the largest multinational automotive manufacturers.**
- A series of data breaches affected **3.1 million customers** across Australia, Thailand, Vietnam, and Japan.

2020

- **A major public-listed banking group in Malaysia.**
- A data breach exposed the personal information of the bank's customers due to inadequate security measures.
- The bank was **fined** by the respective regulator for failing to implement sufficient security measures to protect customer data.

2022

- **A payment gateway in Malaysia.**
- A data breach compromised the personal information of up to **3.3 million** customers.

PCI Security Standards Council®

2023 Data Breach Incident Case Study

Airline Data Breach Case Study | October 2023

Breach

A major airline in Spain discovered a data breach that compromised customer payment card information.

Customer Data Exposed

Unauthorized access to customer data, potentially exposing credit card details like numbers, expiration dates, and CVV codes.

Impact

- The exact number of affected customers remains undisclosed by the airline.
- Customers who used credit cards for flight purchases were advised to cancel their cards to prevent fraudulent use.
- This incident damaged customer trust and potentially resulted in financial losses for affected individuals.

PCI Security Standards Council®

Lessons Learned

Prioritize Robust Security

- Strong Password Policies
- Strong Data Encryption for all payment information
- Multi-Factor Authentication
- Regular Security Audits

Implement Secure Systems and Processes

- Strict Access controls to limit access into sensitive data
- Employee Awareness Training
- Third-Party Risk management

Incident Response and Customer Communication

- Incident Response Plan
- Prompt Notification to affected customers

PCI Security Standards Council®

PCI Security Standards Council®

Emerging Trends in Payment Security

Emerging Trends in Payment Security

Increased Adoption of Buy Now, Pay Later

Enhanced Payment Security Technologies

Regulatory Changes and Compliance Challenges

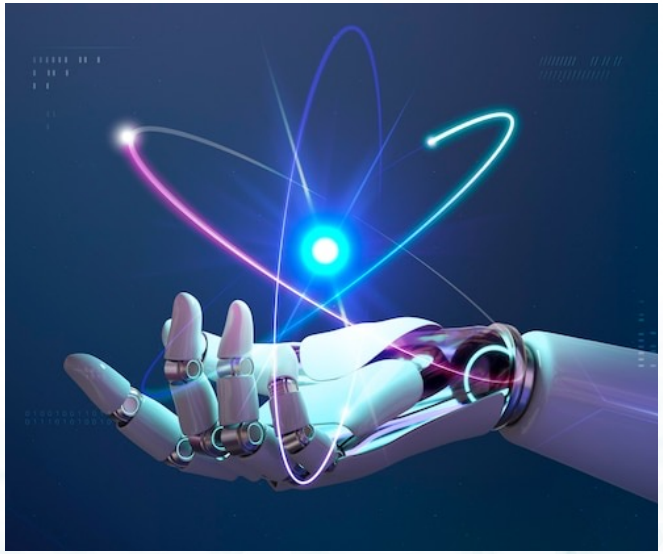
PCI Security Standards Council

PCI Security Standards Council

Strategies for Businesses

Strategies for Businesses

Focus on Compliance with PCI DSS v4.0



Leverage Advanced Technologies

Continuous Awareness Training

PCI Security Standards Council®

PCI Security Standards Council

Thank You!

Scan to stay connect with us.

+603-8605 0155 info@lgms.global www.lgms.global

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


PCi
Security
Standards Council
®