PCI Security Standards Council

# Evolution of Payment Landscape in Asia and its Implications Globally


*Dharshan Shanthamurthy*
*Founder and CEO,*
**SISA**

# Vanguard of Digital Payments: Asia's Cashless Revolution in Numbers

**By 2025, Asia is set to lead the digital payments landscape with the strongest surge in transaction volumes.**

Digital payments to grow **19.8%** annually across the Asia Pacific by 2027.

The volume of non-cash transactions is forecast to reach the **1.3 trillion** mark by 2023.

Real-time payments (RTP) transaction volumes to grow at a **CAGR of 14.1%** from 2022 to 2027.

B2B payments revenue will double to **US$1.4 trillion** by 2025, at a CAGR of 10.5%.

Government promotions, regulatory changes, shifting consumer preferences, smartphone-led M-commerce, and growing internet access will be key catalysts driving the surge.

Sources: Capgemini, “WORLD PAYMENTS REPORT 2023”; ACI, IT’S PRIME TIME FOR REAL-TIME 2023; FROST AND SULLIVAN,” B2B payments revenue will double to **US$1.4 trillion** by 2025, at a CAGR of 10.5%

PCI Security Standards Council

# Macro Trends Shaping the Digital Payments Industry

## 1 Rapid adoption of Mobile Payments

- 2X jump in **Digital wallets'** share in e-commerce transactions in 5 years.
- Rapid adoption of **Unified QR codes**, like Singapore's PayNow and Thailand's PromptPay.
- **Embedded financing** to grow at a CAGR of 24.4% from 2022 to 2029 to US$358 billion.

## 2 The growth of Central Bank Digital Currencies (CBDCs)

- Countries evaluating use cases for **cross-border payments**, securities settlement and retail CBDCs.
- In China, **5.6 million+** merchants now accept digital yuan (e-CNY).

## 3 The rise of Payments-as-a-Service and API models

- The adoption of PaaS and **cloud-based platforms** to accelerate.
- **48%** businesses using payments APIs in some form.
- **Majority (80%)** using APIs to increase operational efficiency.

Source: MAS, “Singapore and Thailand Launch World's First Linkage of Real-time Payment Systems”, April 2021; Fintechnews.sg,” Real-time Digital Payments Fuels Growth Across APAC”, July 2023; Reuters, “China's digital currency passes 100 bln yuan in spending – PBOC”; October 2022

PCI Security Standards Council

# Macro Trends Shaping the Digital Payments Industry

## 4 Launch of New Services

- Australia, Hong Kong, Malaysia etc. plan to roll out **Request to Pay** services.
- Indonesia will be rolling out the new **Instant Payment** service (launched BI-FAST RTP system in 2022).

## 5 Laser focus on innovations in Digital Payment Security

- Adoption of newer standards such **EMV 3-DS 2.0** and payment tokenization.
- Use of **biometrics** by merchants for payments authentication.
- **Project Bakong**, a blockchain-based system from the Central Bank of Cambodia uses digital tokens.

Source: Temenos, “Payments in 2023 and Beyond Key trends for Asia Pacific”

PCI Security Standards Council

# Breaking Borders - The Rise in Cross-border Transactions

**APAC leads in real-time payment (RTP) initiatives among ASEAN nations, with key states uniting for a QR code payment system across member countries.**

In 2022 Malaysia, Singapore, Indonesia, Thailand, and the Philippines signed a deal to integrate their **QR Code payment** systems.

Cambodia & Malaysia launched Bakong, a blockchain-based remittance service.

Thailand, China, Hong Kong, & UAE successfully tested a **cross-border digital currency** trial backed by the Bank for International Settlements.

In March 2023, Bank for International Settlements (BIS), Monetary Authority of Singapore (MAS) and Bank Negara Malaysia (BNM) announced successful tests of **Project Nexus**, on cross-border instant transfer among the EU, Singapore and Malaysia.

Source: Temenos, “Payments in 2023 and Beyond Key trends for Asia Pacific”; Reuters, “China trials cross-border settlement involving cenbank digital currencies”, September 2022; MAS, “BIS’s Project Nexus prototype successfully links Eurosystem, Malaysia and Singapore payment systems; partners in Indonesia, Malaysia, the Philippines, Singapore and Thailand to work towards wider payment connectivity”; NIUM, “How APAC is Winning the Real-Time Payments Race”

PCI Security Standards Council

# The Flip Side: The Rising Cybersecurity and Data Privacy Risks

The rapid expansion of digital payments landscape has widened the attack surface, leading to a rise in cyberattacks, payment frauds and financial crimes.

APAC was the most attacked region in 2022: it accounted for **31% of attacks** globally.

**49% of successful attacks** on organizations resulted in compromise of sensitive information.

Rapid uptake of real-time payments (78% adoption) driving **Authorized Push Payment** (APP) fraud.

Cyberattacks on APAC's **payment segment** grew 50% in 2022.

The most common ads on the **Dark Web forums** in the region are for the sale of network access credentials to organizations in China, Thailand, and India.

Source: Checkpoint, "Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year"; IBM, "X-Force Threat Intelligence Index 2023"; Cyber Security Hub, "Toyota's data breach resulted from an access key from their T-Connect app source code mistakenly posted on GitHub, and impacted up to 296,019 customers"

PCI Security Standards Council

# Commonly Observed Intruder Trends and Tactics

With adversaries evolving rapidly, the threat landscape is increasingly getting complex and treacherous. SISA's forensic  investigations reveal key insights into novel methods adopted by intruders.

## Ingress Trends

- In **48% cases**, intruders utilized stolen credentials to access networks via remote services.
- In **55% of cases, intruders used weak** credentials to authenticate to API requests.

## Lateral Movement Trends

- **Web shells** were the most common backdoors observed.
- **Creating registry keys** that execute malicious code was mainly observed in user systems.

## Action on Objective Trends

- In **73% of cases**, clients experienced ransomware attacks, locking or encrypting their systems.
- In **14% of cases** payment brands identified the client's environment as a 'Common Purchase Point'.

PCI Security Standards Council

# Navigating the Regulatory Waters

## Challenges

- **Diverse jurisdictions**: APAC comprises distinct governments, each with unique agendas, leading to fragmented approaches.
- **Multiple regulators**: Within some jurisdictions, several regulators oversee different facets of e-payments, adding to regulatory complexity.

## Advances Made

- **Dialogues and DEAs**: Governments are adopting DEAs to align digital rules, set standards, and enhance data exchange for smart regulations.
- **Supportive sand-box environment** targeted at fintechs and paytechs for pilots and tests.

## Future Focus

- **Coherent cross-border policies**: As the region aims for economic integration, a harmonized approach to cross-border payment policies is vital.
- Non-bank financial newcomers pose risks. **Quick regulatory alignment** and technologies like biometrics are crucial.
- **Holistic financial crime management**: Payment organizations should integrate prevention and detection technologies to comprehensively address financial crime.

PCI Security Standards Council

# Best Practices for Securing Digital Payments Infrastructure

SISA recommends implementing a forensics-driven approach that uses Top 5 preventive and detective controls to secure payments data and infrastructure.

## SISA Top 5 Learnings

### 1 Faster vulnerability mitigation

- Implement an automated, cloud-based **patch management** solution for all user systems.
- Ensure that all vulnerabilities with a **CVSS score of 6.5 and higher** are mitigated immediately.

### 2 Endpoint protection

- Implement **DNS security solutions** to route traffic, particularly for remote systems, can prevent command and control communications.
- Deploy an **endpoint response solution** to enable the IT/Infosec/IR team to respond to a suspicious event in the in the endpoint systems.

PCI Security Standards Council

# Best Practices for Securing Digital Payments Infrastructure

SISA Top 5 Learnings

## 3 Intelligent detection and response

- Ensure the **log monitoring** activity covers the organization's entire technology infrastructure and not just the production environment.
- Integrate open source and commercial **threat intelligence** including Indicators of compromise (IoCs), into existing SIEM solutions.

## 4 MFA everywhere

- Implement **MFA for all access points**, including remote access, VPN, email, SaaS applications, code repository, and systems requiring authentication.
- Ensure that it's an **out-of-band** authentication and covers all applications and system components.

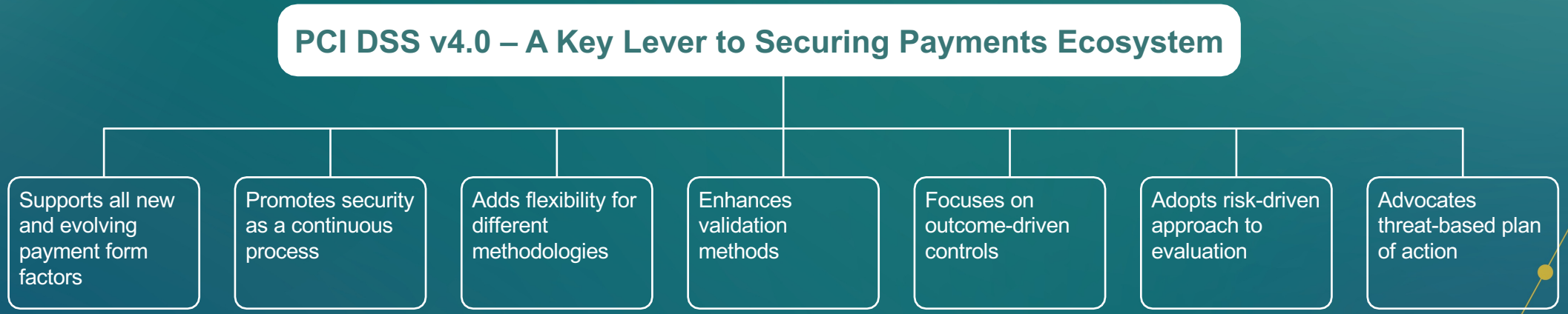
## 5 Attack surface reduction

- Use open-source **API discovery tools** to identify various API calls within the network.
- Route all web-based traffic through a **web application firewall**, which can protect against web application-based attacks.

PCI Security Standards Council

# Importance of PCI DSS Controls in Securing Payments Data

PCI DSS v4.0 is the next evolution of the payment security standard that is expansive in scope, futuristic in approach and sharper in focus.




***Organizations must prioritize transitioning to PCI DSS v4.0, not just as a compliance mandate, but as a critical security measure.***

PCI Security Standards Council

PCI Security Standards Council

# Thank you.