Company Visit 6/2026

BEYOND THE FIREWALL: INSIDE SCBX'S CYBER DEFENSE & TECH OPERATIONS

28 ตุลาคม 2569

14.00 - 16.30 น.
(เริ่มลงทะเบียนเวลา 13.30 น.)



คุณตริยรัตน์ สุวรรณประทีป
Chief Technology Officer, SCB

คุณพศวัชร์ วงศ์วานิช
Head of Security Strategy & Advisory, SCBX

คุณสุรชัย ฉัตรเฉลิมพันธุ์
Head of Group Security Operations, SCBX

สนับสนุนกิจกรรมโดย

Today's Agenda

28 October 2026 · SCBX TownHall ชั้น 9

14:00 — **Welcome & Introduction: Overall Cyber Security**
คุณตรัยรัตน์ สุวรรณประทีป – Chief Technology Officer, SCB

14:30 — **Cyber Threat Landscape: Emerging Risks & Key Trends**
คุณพศวัชร์ วงศ์วานิช – Head of Security Strategy & Advisory, SCBX

14:45 — **SCBX Cyber Defense Strategy: Cybersecurity, AI & Unknown Threats**
คุณสุรชัย ฉัตรเฉลิมพันธุ์ – Head of Group Security Operations, SCBX

15:00 — **Q&A**
ถาม–ตอบกับทีมวิทยากร

15:15 — **Coffee Break**
พักรับประทานอาหารว่าง

15:30 — **Site Tour: Security Operations Center (SOC) & Tech Nerve Center**
เยี่ยมชมศูนย์ปฏิบัติการ SOC และ Tech Nerve Center

Welcome & Introduction



K. Trirat Suwanprateeb
Chief Technology Officer, SCB

IOD COMPANY VISIT 6/2026

Cyber Threat Landscape: Emerging Risks & Key Trends

K. Pasawat Wongwanich (Tony)
Head of Security Strategy & Advisory, SCBX
SCBX Public Company Limited

Why Security Matters

From Risk to Resilience, Enabling Sustainable Growth



The Values

PROTECT TRUST
Customers, data, reputation and confidence

PRESERVE VALUE
Financial loss, disruption and enterprise exposure

ENABLE GROWTH
Secure digital, cloud, AI and ecosystem innovation

ASSURE RESILIENCE
Ability to respond, recover, continue critical services & sustainability

Today's Threat Landscape

More Complex, More Targeted, Higher Impact

AI-POWERED THREATS
Attacks become faster, smarter, and more scalable

- AI-enabled phishing and deepfake fraud
- Autonomous and agentic AI attacks
- Shadow AI and AI data leakage
- AI-assisted vulnerability exploitation

IDENTITY & TRUST EXPLOITATION
Attackers increasingly log in rather than break in.

- Credential theft and account takeover
- Session and token hijacking
- Third-party and supply-chain compromise
- Privileged and machine identity abuse

EXPANDING DIGITAL EXPOSURE
Cloud, APIs, and new technologies expand exposure.

- Cloud and API exploitation
- Zero-day and rapidly weaponized vulnerabilities
- SaaS and interconnected platform risks
- Quantum-era cryptographic exposure

SYSTEMIC & DISRUPTIVE THREATS
Cyberattacks increasingly threaten business continuity.

- State sponsor cyber attack
- Ransomware and data extortion
- Critical infrastructure and DDoS attacks
- Cascading outages from ecosystem dependencies

+89%
AI-enabled attack activity

29Min
verage attacker breakout time

8Hours
Quantum decryption time compare to billion of years current

Ref. Mandiant | CrowdStrike

Copyright © 2026 SCBx All Rights Reserved

From Threats to a Security Roadmap

The security roadmap is driven by the threat landscape, business priorities and regulatory requirements, translated into clear capabilities and outcomes.

THREAT LANDSCAPE
- Evolving threats and attack trends
- Industry and peer insights
- Real incidents and lessons learned

BUSINESS PRIORITIES
- Strategic growth initiatives
- Digital transformation
- Customer experience and trust

REGULATORY & STAKEHOLDER REQUIREMENTS
- PQC and financial regulations
- Industry standards (e.g. DORA, NIST2)
- Board and stakeholder expectations

From these insights, we translate risk into a clear and executable Security Roadmap with measurable outcomes.

Security Roadmap
A prioritized, multi-year plan to build the right capabilities, reduce key risks and enable the business strategy.

STRENGTHEN CORE DEFENSES
Figh AI with AI and rethinking new way to handle emerging threats

INCREASE VISIBILITY AND DETECTION
Policies as code, automate policies enforce and detection

ENHANCE RESPONSE AND RECOVERY
Minimize impact and recover faster

BUILD A SECURITY-AWARE ORGANIZATION
People, culture and governance

DELIVER MEASURABLE BUSINESS VALUE
Track progress with clear metrics (risk reduction, resilience, compliance, ROI)

Outcome: A more secure, resilient and trusted, enabling sustainable growth.



What the Board Should Consider and Ask

Board oversight of technology governance requires evaluating both immediate operational risks and long-term strategic readiness. By asking targeted questions around resilience, alignment, compliance, and emerging technologies like AI, board members can validate security execution and ensure organizational trust.

Security Strategy & Operational Execution



ARE WE FOCUSED ON THE RIGHT RISKS?

Ensure strategy addresses the most relevant threats to the business.

ARE WE SUFFICIENTLY RESILIENT?

Validate capabilities to prevent, detect, respond to, and recover from incidents.





ARE OUR INVESTMENTS ALIGNED AND EFFECTIVE?

Target high-impact areas with measurable outcomes to optimize security spending.

Stakeholder Governance & Future Readiness



ARE WE MEETING REGULATORY AND STAKEHOLDER EXPECTATIONS?

Maintain regulatory compliance and build long-term trust with key stakeholders.

ARE WE PREPARED FOR FUTURE RISKS?

Address emerging technology threats including AI and broader ecosystem vulnerabilities.



IOD COMPANY VISIT 6/2026

SCBX Cyber Defense Strategy into Actions

Responding to Cybersecurity, AI and Unknown Threats

K. Surachai Chatchalermpun (Pok)
Head of Group Security Operations
SCBX Public Company Limited

IOD DCP 329, NCSA Executive CISO #1
Security cert: CISSP, CISA, CISM, CSSLP, CEH, ECSA, ISO27001
Privacy cert: DPO-CEPAS-GDPR, FIP, CIPM, CIPP/E, CPDSE

GROUP MODEL | CYBER CENTER OF EXCELLENCE

One Group. Shared strength.

Shared capabilities. Clear company accountability.



STANDARDS

Common minimum controls

EXPERTS

Specialists shared across the Group

PLATFORMS

Scale without duplicating investment

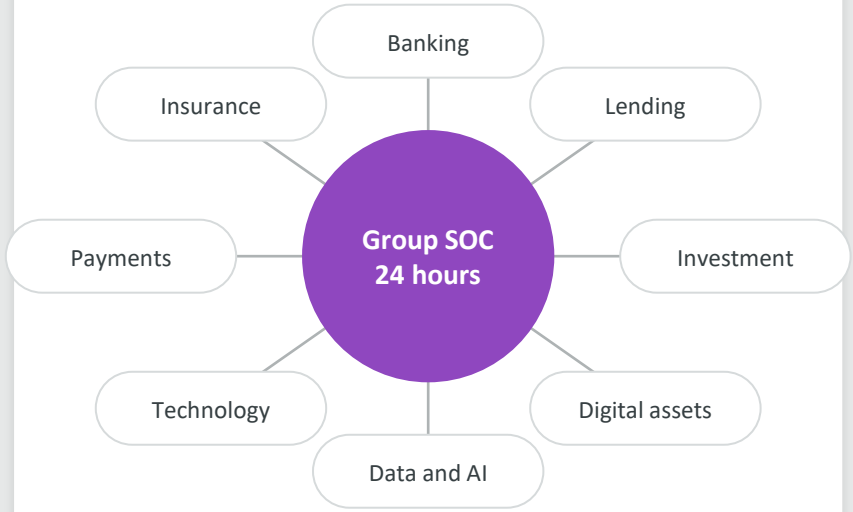
INTELLIGENCE

Learn once, strengthen many

Unified standards and economies of scale, with business ownership in each company.

Responding to cyber threats: One team, find early, stop fast, learn.

One shared Security Operations Center (SOC) watches every company in the Group, real-time for 24 x 7.



Machines filter **very large volume of security signals** down to the **cases that expert need to investigate**, so analysts spend their time on what business matters.

Find early Cyber Threat intelligence

We track all Threat actor groups, **vulnerabilities, leaked passwords and PII data.**
We also scan everything we expose any **misconfiguration** to the internet/Darkweb the way an attacker would.

Stop fast, contain the business damage first

A 24 hour team investigates anything unusual and follows a Group IR playbook with promised SLA containment time. **Access is cut first**, questions come after.

Learn every time with Preventive approach

Every case ends with a root cause and a fix pushed to all subsidiaries. Lessons are shared at a monthly Group **Cyber Forum** with all key stakeholders and **reported to the top management & BoD committees on time.**

Attack Surface Management

We scan every internet-facing system across the Group the way an attacker would, and close exposures first.

Detection and response SLA

We met our SLA for detection and response every month, even as the number of cases grew.

Bug Bounty program

Most of the significant weaknesses we fixed last quarter were reported by ethical hackers through our Bug Bounty program.

Unknown threats: you cannot block what you have never seen

Standard defenses stop the attacks they recognise. Most of the danger sits below the surface, so we design for finding it fast.



WHAT WE DO ABOUT EACH ONE

Attacks with no signature

We detect behavior, not signatures: identity and anomaly monitoring across all subsidiaries, with cyber with cyber threat intelligence on who targets us.

Intruders who stay quiet

We hunt proactively for outliers hiding in normal activity, and keep evidence central logs management management and protected so an intruder cannot erase the trail.

Blind spots we do not know we have

We let outsiders find them first: Attack Surface Management, red teaming, a public bug bounty, and bounty, and cyber crisis exercises with role-play top executives for end-to-end process.

Sources: CrowdStrike Global Threat Report 2026 (malware-free intrusions, 2025 data). Google Threat Intelligence Group, 2025 Zero-Days in Review, March 2026. Mandiant (Google Cloud), M-Trends 2026, March 2026: median dwell time, 2026: median dwell time, espionage dwell time, mean time to exploit.

From Cyber Defense to Cyber Resilience: outside in, as one Group

OUTSIDE IN: WHAT AN ATTACKER MEETS FIRST, AND WHAT A CUSTOMER CAN TRUST

Attack Surface Management

See what attackers see, close it first, before sec incident happened

Breach and Attack Attack Simulation Simulation

Simulate real attacks on ourselves, continuously improvement

Bug Bounty Program

Global and local of ethical hackers reported for our double assurance

24x7 Detection and Response

One Group SOC with promised response times

Recover and Learn

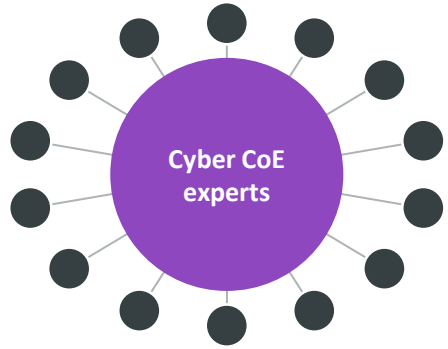
Crisis exercises, monthly Cyber Forum, committee oversight

PROACTIVE: FIND THE BLIND SPOTS BEFORE ATTACKERS DO

RESPOND, RECOVER, IMPROVE

Every layer is tested by outsiders, not only by ourselves. That is what customers can trust.

ONE GROUP, ONE STANDARD



All subsidiaries, one COE expert team

- **Same standard for every subsidiary**
- **Shared expert team, shared tools**
- **Economy of scale**

The shift: Customer trust is built from the outside in: tested by outsiders, watched around the clock, and run as one Group with one standard.

Cyber CoE: SCBX Cyber Center of Excellence, the Group's shared security expert team serving all subsidiaries.

AI threats: AI attacks us, our own AI is protected, and AI defends us

Three different things that are often mixed up. We manage each one on purpose.

AI used against us

THE THREAT

Phishing in perfect Thai, fake sites that copy our brands, probing around the clock

WHAT WE DO

Verify every urgent request on a second channel, train staff with real examples, take down VIP C-level impersonation

Our own AI protected

THE THREAT

Chatbots tricked with words (prompt injection), injection), poisoned data, shadow AI

WHAT WE DO

AI Inventory with a project owner, penetration testing the Guardrail and keep monitoring on the Group SOC.

AI as our defender

Machines filter,
people investigate

An AI assistant drafts each investigation. Hours become minutes

AI agents do the routine steps,
every action approved by our team

Our rule: AI proposes, people decide.

Why the board owns this: The Bank of Thailand's AI risk guideline (September 2025) makes the board accountable for decisions made by the institution's AI.

Source: Bank of Thailand, Policy Guideline on AI Risk Management for financial service providers, 12 September 2025.

Top 3 questions a BoD can ask management next day

You do not need to be technical to oversee cyber risk. These questions have clear answers, and the answers tell you a lot.

1	**How fast can we detect and contain an intruder?**	The attacker benchmark is under hour. If the answer is days, or nobody knows, that is the key gap finding.
2	**Who is testing our cyber defenses from the outside, and how often?**	Not rely on only the yearly penetration testing.
3	**When did the executive team last rehearse a cyber crisis?**	A plan that has never been practised is a just document. The Cyber exercise shows who decides, and how fast to manage/escalate.

Q & A



Thank You

