THAILAND CLOUD SECURITY ASSURANCE PROGRAM (TCSAP)

ตำแหน่งปัจจุบัน

- เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประสบการณ์ทำงาน

- ผู้อำนวยการกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
- Director of Cyber Warfare Division Department of Information and Communication Technology, Royal Thai Air Force
- Electronics Warfare Manager, F-16 MLU, Gripen
- คณะทำงาน Tactical Data Link (TDL) (F-16, Gripen)
- ริเริ่มการนำอินเทอร์เน็ตมาใช้งานใน ทอ.
- ริเริ่มการจัดแข่งทักษะทางไซเบอร์
- ร่างระเบียบการรักษาความปลอดภัยระบบสารสนเทศ ทอ. ปี 43
- ริเริ่มการตั้งหน่วยงานด้านไซเบอร์ ใน ทอ.

การศึกษา

- หลักสูตรผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ (Executive Chief Information Security Officer: Executive CISO) รุ่นที่ 1
- หลักสูตรพัฒนาเครือข่ายและศักยภาพผู้บริหารระดับสูงของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม WiNS รุ่นที่ 2
- วิทยาลัยการทัพอากาศ รุ่นที่ 51
- วท.บ. วิทยาการคอมพิวเตอร์ United States Air Force Academy
- วท.ม. เทคโนโลยีสารสนเทศ มหาวิทยาลัยเกษตรศาสตร์
- นักเรียนนายเรืออากาศรุ่นที่ 35

เกียรติคุณเพิ่มเติม

- บุคคลดีเด่นกองทัพอากาศปี 49, 62
- (ISC)² Government Professional Award 2021
- อาจารย์พิเศษ จุฬาลงกรณ์มหาวิทยาลัย
- วิทยากรรับเชิญงาน US-Thailand Cybersecurity Standards and Data Protection Workshop, OpenGov Insider
- ศิษย์เก่าดีเด่นนักศึกษาวิทยาลัยกองทัพอากาศ รุ่น 51 ปี 60
- บุคคลดีเด่นชุมนุมนายเรืออากาศ ประจำปี 2566
- ศิษย์เก่าดีเด่นโรงเรียนเสนาธิการทหารอากาศ ประจำปี 2566
- สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) 2566
- CSO 30 ASEAN AWARD
- รับรางวัลเกียรติยศจักรดาว ประจำปี 2567

CERTIFICATES

พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โครงสร้าง

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์

2.2 การจัดการทรัพย์สิน

2.3 การควบคุมการเข้าถึง

2.4 การเข้ารหัส

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม

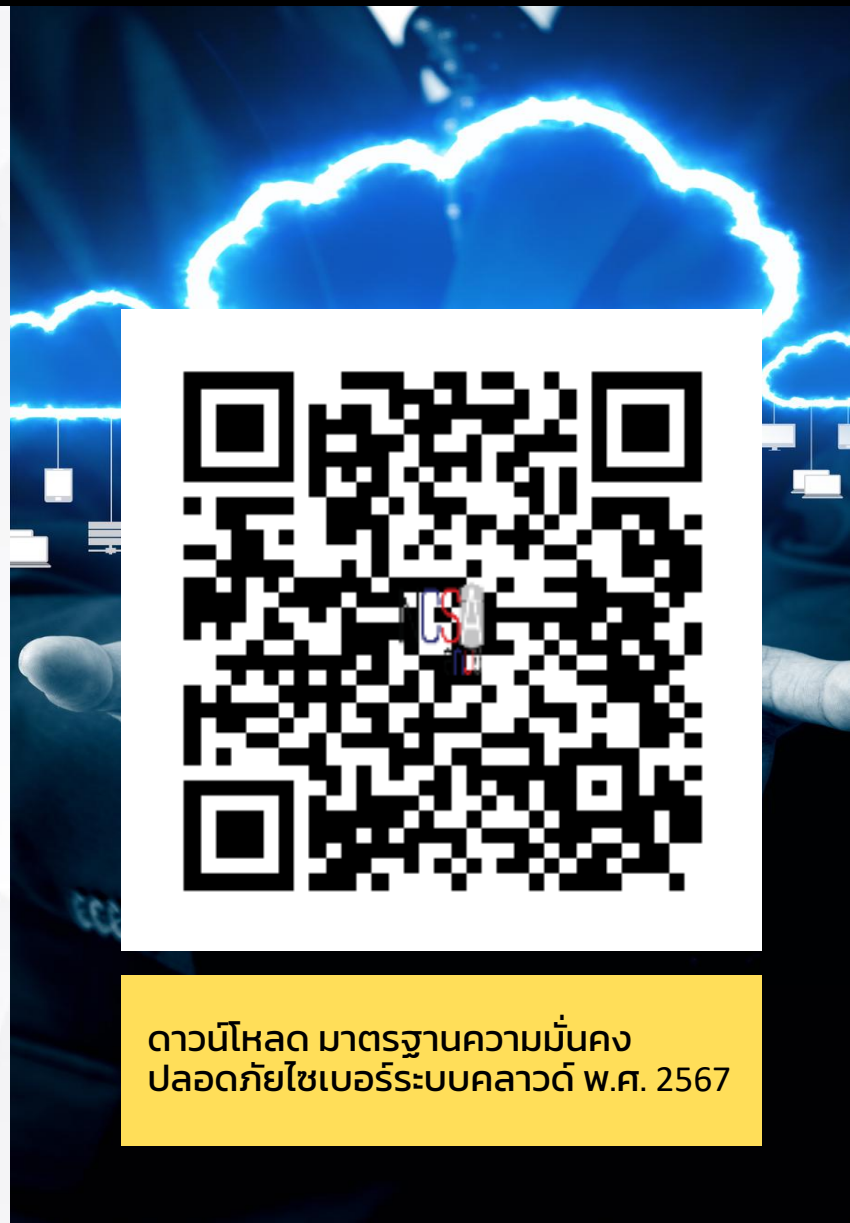
2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย

2.8 การจัดหา การพัฒนา และการบำรุงรักษา

2.9 การจัดการผู้ให้บริการภายนอก

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ



ดาวน์โหลด มาตรฐานความมั่นคง
ปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

โครงสร้างของมาตรฐาน

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

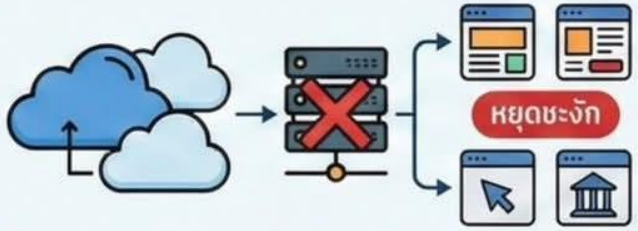
ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์	ต้องเพิ่มนโนบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อจัดการกับการจัดหา และใช้บริการคลาวด์
นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการคลาวด์ ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ กับผู้ใช้บริการคลาวด์	

NCSA สกมช | ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

การรับมือสถานการณ์ความไม่พร้อมใช้งาน จากผู้ให้บริการ CDN และ บริการคลาวด์

ความเปราะบางของโครงสร้างพื้นฐานดิจิทัลและการเตรียมความพร้อม

สถานการณ์และความเสี่ยง

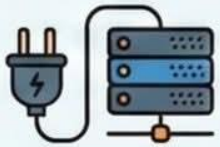


การพึ่งพาผู้ให้บริการรายใหญ่เพียงไม่กี่ราย ทำให้เกิดความเสี่ยงเชิงระบบ

เมื่อโครงสร้างพื้นฐานส่วนกลางสะดุด ผลกระทบขยายวงกว้างสู่ผู้ใช้จำนวนมหาศาลในเวลาอันสั้น

สาเหตุหลักของเหตุขัดข้อง

การตั้งค่าระบบผิดพลาด, การปรับปรุงที่ไม่เพียงพอ



ปัญหาไฟฟ้า หรือศูนย์ข้อมูล

ปัญหาเครือข่าย และระบบ DNS

ปัจจัยภายในของผู้ให้บริการเอง ไม่ใช่แค่การโจมตีทางไซเบอร์

9 แนวทางป้องกันและลดผลกระทบ (สำหรับองค์กร)

คำแนะนำสำหรับประชาชน

เตรียมช่องทางสำรองในการติดต่อ

ไม่เก็บข้อมูลสำคัญไว้ที่เดียว

ติดตามประกาศจากเจ้าของระบบ

แจ้งเหตุภัยคุกคามทางไซเบอร์ ThaiCERT @thaicert thaicert@ncsa.or.th 02-114-3531

อ่านเพิ่มเติม

ประกาศ กมช. เรื่อง

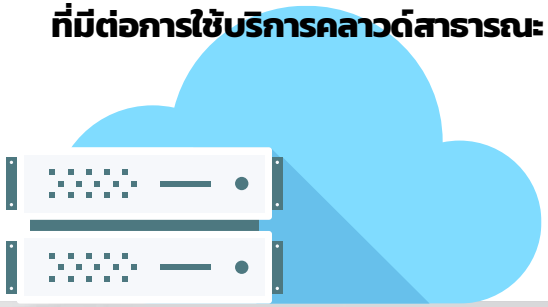
มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 69 เป็นต้นไป

สาระสำคัญ

เพื่อกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ให้แก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะ**



ดาวน์โหลดเอกสารมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

ประกาศ กมช. เรื่อง

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

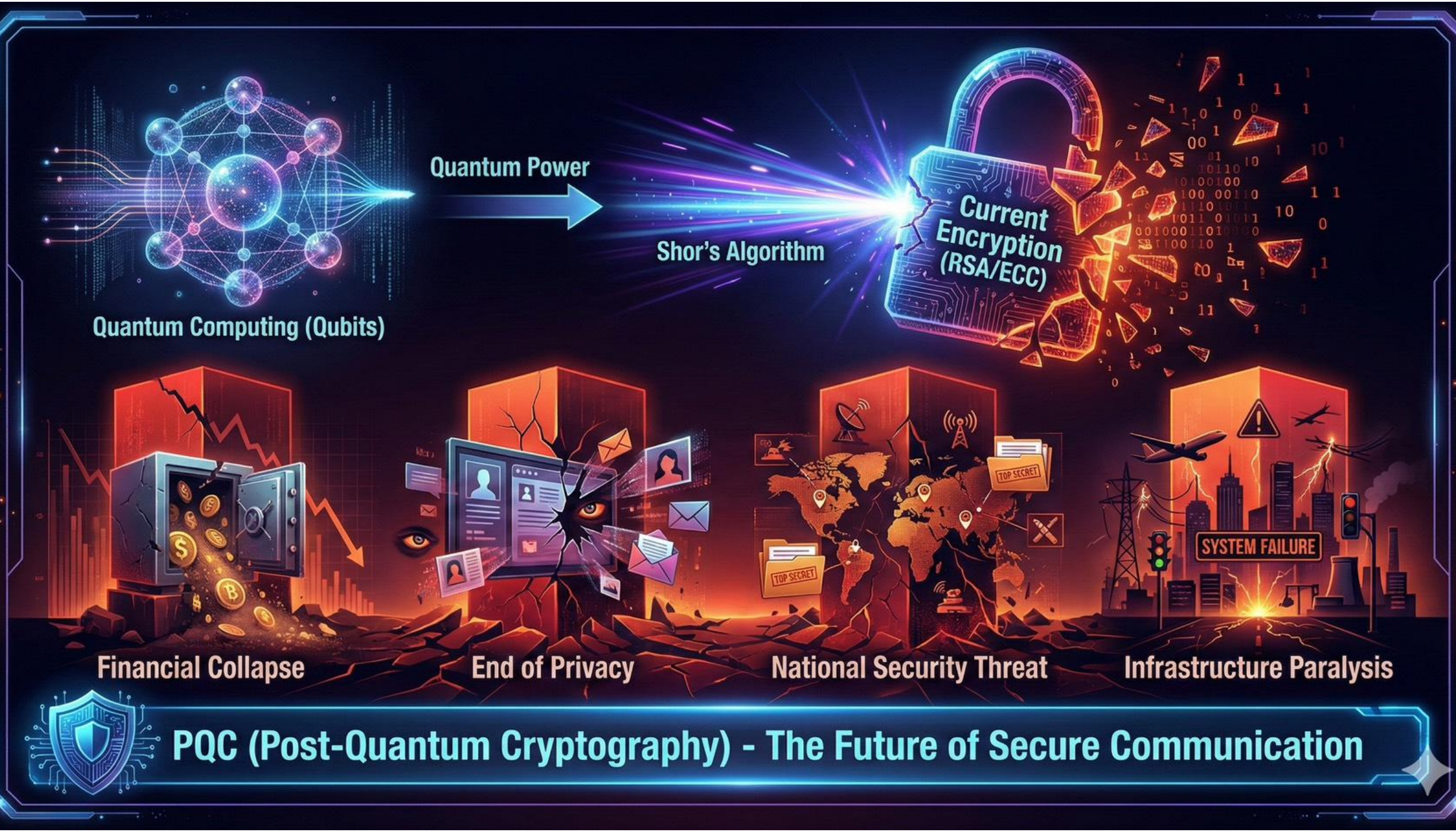
พ.ศ. 2568

อยู่ระหว่างประกาศในราชกิจจานุเบกษา

สาระสำคัญ

เพื่อเป็นการกำหนดและส่งเสริมให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน **มีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ของตน เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และให้บริการได้อย่างต่อเนื่อง**

ดาวน์โหลดเอกสารมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์


Quantum Computing (Qubits)
Quantum Power
Shor's Algorithm
Current Encryption (RSA/ECC)
TOP SECRET
TOP SECRET
SYSTEM FAILURE
Financial Collapse
End of Privacy
National Security Threat
Infrastructure Paralysis
PQC (Post-Quantum Cryptography) - The Future of Secure Communication

Steps to Quantum Readiness

- Roadmap
- Awareness
- Role & Responsibility
- Assets Inventory
- Solutions Evaluation
- Experiment & Testing
- Monitoring & Evaluation

(2023)

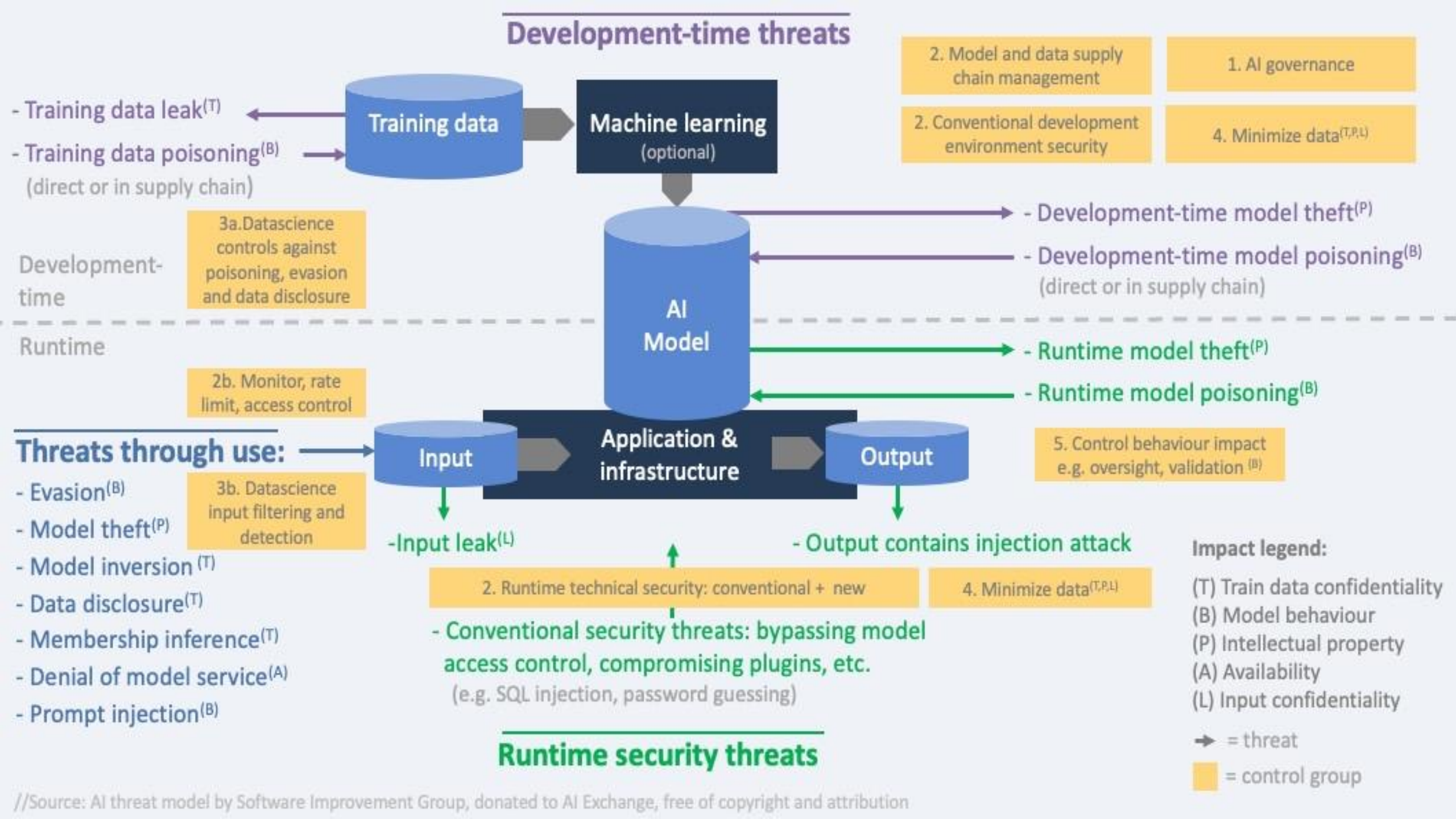
https://www.ncsa.or.th/ncsa_book/5004a6893034327c56000029

เข้าร่วมการเตรียมความพร้อมระบบสารสนเทศของหน่วยงาน เพื่อเข้าสู่ยุคควอนตัม (PQC)

https://dg.th/8x6heca1f4

สิ่งที่ท่านจะได้รับ

- เห็นตัวอย่างการดำเนินการจริง ตั้งแต่การสำรวจสินทรัพย์ระบบรหัสลับ การจัดลำดับความสำคัญ และการวางแผนการเปลี่ยนผ่าน
- มีแนวทางในการจัดทำแผนการเปลี่ยนผ่านระบบสารสนเทศ
- สิทธิ์สำหรับการใช้ระบบติดตามการดำเนินการเปลี่ยนผ่านระบบสารสนเทศ
- สิทธิ์ในการเข้าใช้ศูนย์ข้อมูลและสาธิต PQC และรับคำแนะนำจากผู้เชี่ยวชาญ



//Source: AI threat model by Software Improvement Group, donated to AI Exchange, free of copyright and attribution

เริ่มต้นด้วยการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัยตั้งแต่วันนี้

AI SecurityGuidelines

TEMPLATE นโยบายการใช้เทคโนโลยี
Generative AI ที่ยอมรับได้

https://dg.th/tn4pza5orb
https://www.ncsa.or.th/docpdf/view/ba37afc6636334401e000142

กลยุทธ์ความมั่นคงใหม่: เชื่อมช่องว่าง "Cyber Elite" กับสังคมด้วย "Empathy"

หอคอยงาช้าง (The Ivory Tower) - กลุ่ม Cyber Elites

"Users are the Weakest Link"
(ผู้ใช้คือจุดอ่อนที่สุด)

- ใช้ภาษา Jargon (ศัพท์เทคนิค)
- เน้นการตำหนิ (Blaming)
- มองว่าผู้ใช้ "โง่" หรือ "ขี้เกียจ"

สนามรบที่วุ่นวาย (The Chaotic Battlefield) - สังคมทั่วไป

- เหนื่อยหน่าย (Fatigue)
- ไม่กล้ารายงาน เพราะกลัวโดนด่า

Empathy ไม่ใช่ Soft Skill แต่คือ Critical Infrastructure ของระบบรักษาความปลอดภัย
(Creating Psychological Safety for Early Detection)

เหวแห่งความกลัว
(The Chasm of Fear):
ภัยคุกคามถูกซ่อนเร้น = ความเสี่ยงระดับองค์กร/ระดับชาติ

สะพานเชื่อม "Empathy" (The Empathy Bridge)

1. **เปลี่ยนภาษาให้เข้าใจง่าย (Analogy-based Communication)**
   เช่น เปรียบเทียบ 2FA กับกุญแจบ้าน
2. **ออกแบบโดยเข้าใจมนุษย์ (Secure by "Human" Design)**
   เช่น ใช้ Passkeys แทนรหัสผ่านซับซ้อน
3. **เปลี่ยนจากการตำหนิ เป็นการเสริมพลัง (Shift blame to empower)**
   เช่น จัด "Cyber Clinic" ช่วยเหลือโดยไม่ตัดสิน
4. **ทำให้ภัยคุกคามดูเป็นเรื่องปกติ (Humanize Threats)**
   อธิบายว่าเป็นธุรกิจผิดกฎหมาย ไม่ใช่เวทมนตร์

เป้าหมายสุดท้าย: แนวร่วมที่แข็งแกร่ง
(United Resilient Front)
"Users คือ ปราการด่านแรกที่สำคัญที่สุด เมื่อได้รับความเข้าใจ"

Contact us

National Cyber Security Agency - NCSA

NCSA Thailand

Line ID : NCSA Thailand

E-Mail: saraban@ncsa.or.th

02-142-6885

4loTus (สี่ แอล โอ ทีใหญ่ ยู เอส)