



CYBER SECURITY AWARENESS

By
Mr. Suchaya Sanghan
EVP of SCP SYSTEMS CO.,LTD.
Cyber Security and Telecom Department

AGENDA

- ประวัติวิทยากร
- ความเสี่ยงในการถูกโจมตีไซเบอร์
- การป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์
- ความเสี่ยงในการถูกโจมตีไซเบอร์ การป้องกันและแก้ไขปัญหาจากภัยคุกคามไซเบอร์





คุณวุฒิการศึกษา

- **Primary School and Secondary school : Saint Gabriel College**
- **ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมศาสตร์ไฟฟ้า (ไฟฟ้าสื่อสาร , TELECOMM)
จุฬาลงกรณ์มหาวิทยาลัย / เกียรตินิยมอันดับ 1 (Top 5)**
- **ปริญญาโท วิทยาศาสตร์มหาบัณฑิต สาขา เทคโนโลยีสารสนเทศ
SIU International University / Full Scholarship / 1st in Class**

****ปริญญาเอก ได้รับทุนศึกษาต่อที่ USA จาก ศ.ดร. ปรีดา วัฒนยศสวัสดิ์*

International Publication

- **Intelligent P2P VoIP through Extension of Existing Protocols : IEEE in 2007**

ประกาศนียบัตรและใบรับรอง

- ๑) Certified Cybersecurity Expert (CCE) by Institute of Information Security
- ๒) CISCO Certified Network Associate (CCNA)
- ๓) Computer Language Programming: Pascal, Java, Visual Basic, PHP, HTML, MathLab, Maple
- ๔) Database: MySQL, Oracle, MS Access
- ๕) Computer Operating System: MS Windows XP, MS Window2003 Server, Linux, Unix
- ๖) VoIP System Design and Implementation on both Software and Hardware base
- ๗) Telecommunication and IP & Computer network Test & Measurement
- ๘) Network Synchronization Design and Implementation
- ๙) Fiber Optic Network Design and Implementation
- ๑๐) IT & Telecom Project Management



- ၁၁) Certificate of Microwave Design and Implementation from Nera Telecommunication (Thailand)
- ၁၂) Certificate of Fiber Optic Test Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
- ၁၃) Certificate of Data Monitoring Solution (DA-3400) from JDSU/ACTERNA (Singapore)
- ၁၄) Certificate of SDH Monitoring Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
- ၁၅) Certificate of DWDM Monitoring Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
- ၁၆) Certificate of Ethernet Technology and Ethernet Testing including the Hand-On Testing
- ၁၇) Certificate of Ethernet Testing Solution (HST-3000) from JDSU/ACTERNA (Singapore)
- ၁၈) Certificate of IPTV Technology and IPTV Testing including the Hand-On Testing
- ၁၉) Certificate of VoIP Technology and VoIP Testing including the Hand-On Testing
- ၂၀) Certificate of DWDM Technology and DWDM Testing including the Hand-On Testing
- ၂၁) Certificate of Fiber Optic Technology and Fiber Optic Testing including the Hand-On Testing
- ၂၂) Certificate of Copper Link Technology and Copper Link Testing including the Hand-On Testing
- ၂၃) Certificate of Circuit Switching Technology and Circuit Switching Testing including the Hand-On Testing
- ၂၄) Certificate of Mobile Wireless Technology and Mobile Wireless Testing including the Hand-On Testing
- ၂၅) Certificate of Communication Signaling Technology and Communication Signaling Testing including the Hand-On Testing
- ၂၆) Certified Cybersecurity Expert (CCE) by Institute of Information Security



ประวัติการเป็นอาจารย์ และ วิทยากร

- วิทยากรพิเศษ : MBA Class at Mahidol International Management School of Mahidol University
- อาจารย์พิเศษ : Information Technology Class at SIU International University
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", การสื่อสารแห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", องค์การโทรศัพท์แห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", กระทรวงมหาดไทย, มกราคม ๒๕๕๒
- วิทยากรอบรม "Traffic Testing and Optimization using IP Traffic Generator", การสื่อสารแห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", การสื่อสารแห่งประเทศไทย, ธันวาคม ๒๕๕๒
- วิทยากรอบรม "Traffic Testing and Optimization using IP Traffic Generator", การสื่อสารแห่งประเทศไทย, ธันวาคม ๒๕๕๒
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", กรมการสื่อสารทหารอากาศ, ธันวาคม ๒๕๕๒
- วิทยากรอบรม "Data Network Analysis using IP Analyzer", การสื่อสารแห่งประเทศไทย, มีนาคม ๒๕๕๓
- วิทยากรอบรม "Traffic Testing and Optimization using IP Traffic Generator", การสื่อสารแห่งประเทศไทย, มีนาคม ๒๕๕๓
- วิทยากรอบรม "Optical Network Monitoring using Optical Network management system", การสื่อสารแห่งประเทศไทย, มิถุนายน ๒๕๕๒



ประวัติการเป็นอาจารย์ และ วิทยากร

- วิทยากรอบรม “Wi-Fi เทคโนโลยี”, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, มิถุนายน ๒๕๕๖
- วิทยากรอบรม “Mobile Technology Evolution 2G 3G & 4G”, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, พฤศจิกายน ๒๕๕๖
- วิทยากรอบรม “Cyber Security Awareness” ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย, เมษายน ๒๕๖๒
- วิทยากรอบรม “Cyber Security Awareness” หลักสูตร มหาบัณฑิต เทคโนโลยีป้องกันประเทศ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, กุมภาพันธ์ ๒๕๖๓
- วิทยากรอบรม “Cyber Security Awareness” หลักสูตร ผู้บริหาร การทำเรื่องแห่งประเทศไทย, ตุลาคม ๒๕๖๓
- Project Manager และวิทยากร โครงการตรวจประเมิน และ พัฒนาความมั่นคงปลอดภัยทางไซเบอร์ รไฟฟ้าส่วนภูมิภาค
- วิทยากรอบรม “Cyber Security Awareness” หลักสูตร ผู้บริหาร กรมทรัพยากรน้ำ
- Project Manager โครงการตรวจประเมิน และ พัฒนาความมั่นคงปลอดภัยทางไซเบอร์ กรมทรัพยากรน้ำ
- วิทยากรอบรม “Cyber Security Awareness” หลักสูตร ผู้บริหาร กรมขนส่งทางราง
- Team Lead : ISO27001 and ISMS การรถไฟแห่งประเทศไทย
- Project Head : National Cyber Exercise (NCX) 2022, 2023, 2024 และ 2025 สกมช.



ความเสี่ยงในการถูกโจมตีไซเบอร์



ความเสี่ยงในการถูกโจมตีไซเบอร์

- ความตระหนักถึงความเสี่ยงในการถูกโจมตีไซเบอร์ เป็นสิ่งสำคัญมากในโลกยุคดิจิทัล ทั้งในระดับบุคคลและองค์กร เพื่อป้องกันข้อมูลส่วนตัว ทรัพย์สินดิจิทัล และชื่อเสียงจากการถูกละเมิดหรือโจมตีทางไซเบอร์ต่อไป



- Phishing (ฟิชชิง): การหลอกล่อให้กรอกข้อมูลสำคัญผ่านอีเมล/เว็บปลอม
- Malware (มัลแวร์): โปรแกรมที่มุ่งร้าย เช่น ไวรัส, Ransomware
- Social Engineering: การหลอกล่อหรือใช้จิตวิทยาเพื่อเข้าถึงข้อมูล
- DDoS: การโจมตีให้ระบบล่มด้วยการส่งคำร้องขอจำนวนมาก
- การเจาะระบบ (Hacking): เช่น การใช้ช่องโหว่ของซอฟต์แวร์

- Confidentiality (การรักษาความลับ): ข้อมูลต้องเข้าถึงได้เฉพาะผู้ที่มีสิทธิ
- Integrity (ความถูกต้องครบถ้วน): ข้อมูลต้องไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต
- Availability (ความพร้อมใช้งาน): ระบบ/ข้อมูลต้องใช้งานได้เมื่อจำเป็น



ความเสี่ยงในการถูกโจมตีไซเบอร์

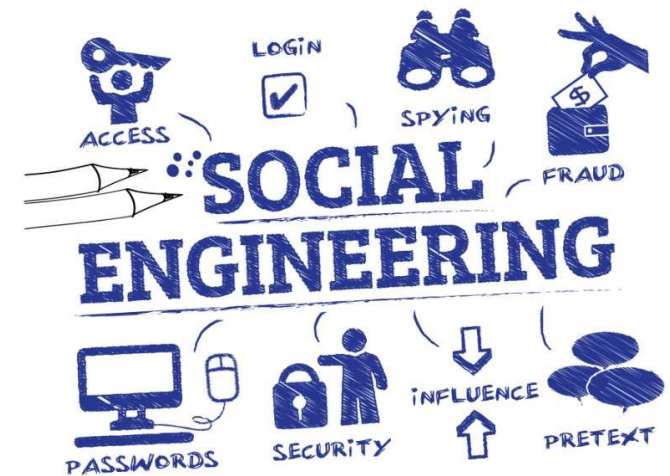


3. ความรู้พื้นฐานสำหรับบุคคลทั่วไป

- ใช้รหัสผ่านที่รัดกุม และเปิดใช้งาน Two-Factor Authentication (2FA)
- ไม่คลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่น่าเชื่อถือ
- อัปเดตระบบปฏิบัติการและแอปพลิเคชันอย่างสม่ำเสมอ
- ใช้แอนตี้ไวรัส/ไฟร์วอลล์ที่เชื่อถือได้

4. ความเข้าใจสำหรับระดับองค์กร

- การประเมินความเสี่ยงไซเบอร์: วิเคราะห์ว่ามีช่องโหว่ตรงไหนบ้าง
- นโยบายความปลอดภัย IT (IT Security Policy): จัดทำนโยบายชัดเจน
- การฝึกอบรมพนักงาน: สร้างความตระหนักและสอนแนวทางป้องกัน
- แผนตอบสนองต่อเหตุการณ์ (Incident Response Plan): หากเกิดเหตุแล้วจะอย่างไร



ความเสี่ยงในการถูกโจรกรรมไซเบอร์



5. ความตระหนักรู้เชิงจิตวิทยาเข้าใจว่า “ภัยไซเบอร์ไม่ได้เกิดจากเทคโนโลยีอย่างเดียว แต่คนคือจุดอ่อนหลัก” เช่น พนักงานหลงเชื่ออีเมลปลอมความมั่นใจเกินไป หรือการคิดว่า “เราไม่น่าสนใจพอให้ถูกโจมตี” คือกับดักที่อันตราย

“ภัยไซเบอร์ไม่ได้เกิดจากเทคโนโลยีอย่างเดียว แต่คนคือจุดอ่อนหลัก”

เพื่อมี ความตระหนักถึงความเสี่ยงไซเบอร์ อย่างแท้จริง ควรมี

- พื้นฐานความรู้ทางไซเบอร์
- เข้าใจว่าทุกคน ทุกองค์กรคือเป้าหมายได้
- มีพฤติกรรมดิจิทัลที่ปลอดภัย
- วางแผนป้องกันและตอบโต้ภัยอย่างรอบคอบ



การป้องกันตนเองและหน่วยงาน จากภัยคุกคามไซเบอร์

การป้องกันตนเองและหน่วยงานจากภัยคุกคาม ไซเบอร์



ในฐานะที่คุณเป็น บุคลากรของหน่วยงาน (ไม่ว่าจะเป็นภาครัฐหรือเอกชน) คุณมีบทบาทสำคัญในการ ป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์ เนื่องจากบุคคลคือจุดอ่อนที่ถูกโจมตีได้ง่ายที่สุดในระบบความมั่นคงปลอดภัยทางไซเบอร์ที่มี ความตระหนักถึงความเสี่ยงไซเบอร์ อย่างแท้จริง

- ปฏิบัติตามนโยบายความปลอดภัยขององค์กรเข้าใจว่าทุกคน ทุกองค์กรคือเป้าหมายได้
- ปกป้องบัญชีผู้ใช้ของคุณวางแผนป้องกันและตอบโต้ภัยอย่างรอบคอบ
- ระวังระวังกับอีเมลและลิงก์
- ใช้เครื่องคอมพิวเตอร์และเครือข่ายอย่างปลอดภัย
- สำรองข้อมูลและปฏิบัติตามแนวทางของ IT
- เพิ่มพูนความรู้และตระหนักภัยไซเบอร์ อย่างต่อเนื่อง
- เมื่อเกิดเหตุผิดปกติ ควรรู้ว่าจะทำอย่างไร (Incident Response Plan)

"บุคลากรที่มีความตระหนัก + พฤติกรรมที่ปลอดภัย = หน่วยงานที่มั่นคงจากภัยไซเบอร์" การป้องกันไม่ใช่หน้าที่ของฝ่าย IT เท่านั้น แต่เป็น ความรับผิดชอบร่วมกันของทุกคนในองค์กร"

ความเสี่ยงในการถูกโจมตีไซเบอร์

ความเสี่ยงในการถูกโจมตีไซเบอร์



ความเสี่ยงในการถูกโจมตีไซเบอร์มีอยู่หลายด้าน ทั้งในระดับบุคคลและองค์กร ซึ่งหากไม่เข้าใจหรือไม่เตรียมการรับมืออย่างเหมาะสม อาจนำไปสู่การรั่วไหลของข้อมูล, การสูญเสียทรัพย์สิน, ความเสียหายทางชื่อเสียง, หรือการหยุดชะงักของระบบงานต่อไปนี้คือ ความเสี่ยงหลัก ๆ ในแต่ละด้าน พร้อมแนวทางป้องกันหรือการลดความเสี่ยง



ความเสี่ยงในระดับบุคคล

ความเสี่ยง	ตัวอย่าง	วิธีป้องกัน / ลดความเสี่ยง
1. การถูกหลอกลวง (Phishing / Social Engineering)	อีเมลปลอม, โทรหลอก, ลิงก์หลอก	- ตรวจสอบอีเมลและลิงก์ก่อนคลิก- อย่าเปิดเผยข้อมูลส่วนตัวกับบุคคลแปลกหน้า- หมั่นฝึกสังเกตพฤติกรรมต้องสงสัย
2. รหัสผ่านไม่ปลอดภัย	ใช้รหัสผ่านง่าย ๆ ซ้ำ ๆ หลายที่	- ใช้รหัสผ่านซับซ้อน- เปิดใช้ 2FA- ใช้ Password Manager
3. การใช้อุปกรณ์หรือเครือข่ายไม่ปลอดภัย	ใช้ Wi-Fi สาธารณะ, ไม่อัปเดตเครื่อง	- หลีกเลี่ยง Wi-Fi สาธารณะหรือใช้ VPN- อัปเดตซอฟต์แวร์เสมอ
4. การดาวน์โหลดไฟล์หรือแอปพลิเคชันอันตราย	ไฟล์แนบจากอีเมล, แอปเถื่อน	- ดาวน์โหลดเฉพาะจากแหล่งที่เชื่อถือได้- สแกนไวรัสก่อนเปิดไฟล์

ความเสี่ยงในระดับองค์กร

ความเสี่ยง

ตัวอย่าง

วิธีป้องกัน / ลดความเสี่ยง

1. ช่องโหว่ระบบหรือซอฟต์แวร์ (Vulnerabilities)

ซอฟต์แวร์ไม่ได้อัปเดต

- ติดตาม Patch / Update ระบบ- ใช้เครื่องมือสแกนหาช่องโหว่

2. พนักงานขาดความรู้ความเข้าใจ

คลิกลิงก์ฟิชซิง, ส่งข้อมูลให้แฮกเกอร์

- จัดอบรม Security Awareness เป็นประจำ- จำลองเหตุการณ์โจมตีเพื่อฝึกซ้อม

3. การจัดการสิทธิ์ไม่เหมาะสม

พนักงานเข้าถึงข้อมูลเกินสิทธิ์

- ใช้หลักการ Least Privilege- ตรวจสอบสิทธิ์เป็นประจำ

4. ขาดการสำรองข้อมูล (Backup)

โดน Ransomware แล้วข้อมูลหาย

- สำรองข้อมูลอย่างสม่ำเสมอ- ทดสอบการกู้คืนข้อมูล

5. ไม่มีแผนรับมือเหตุการณ์ (Incident Response Plan)

ไม่รู้ว่าควรทำอะไรเมื่อระบบโดนโจมตี

- จัดทำและทดสอบแผน IR- มีทีมรับมือเหตุฉุกเฉินชัดเจน

6. ระบบหรือบุคคลภายนอก (Third-party Risk)

Vendor ที่เชื่อมต่อเข้าระบบถูกแฮก

- ตรวจสอบความปลอดภัยของผู้ให้บริการ- ทำข้อตกลงด้านความปลอดภัย (Security SLA)

แผนการลดความเสี่ยงไซเบอร์ของ กรม ทรัพยากรน้ำ

วัตถุประสงค์ของแผน



- ลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจส่งผลกระทบต่อข้อมูล น้ำ ระบบเครือข่าย และบริการภาครัฐ
- ปกป้องความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ทั้งข้อมูลภายใน และข้อมูลสาธารณะ
- เสริมสร้างความรู้ ความเข้าใจ และวินัยด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่เจ้าหน้าที่



การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน



ความเสี่ยงด้านข้อมูล (Data Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
A1	ข้อมูลเชิงพื้นที่ (GIS, น้ำท่วม, เชื้อน ฯลฯ) รั่วไหล	- จัดการสิทธิ์การเข้าถึงข้อมูล (Role-based Access Control)- เข้ารหัสข้อมูลสำคัญ ทั้งที่เก็บและส่งผ่าน (Encryption)- ตรวจสอบ log การเข้าถึงเป็นประจำ
A2	การจัดเก็บข้อมูลประชาชนหรือผู้ใช้งานระบบร้องเรียน	- ปรับให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)- ลบ/ทำลายข้อมูลเมื่อ หมดอายุการใช้งาน- ใช้นโยบายการรักษาความลับภายในหน่วยงาน

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน



ความเสี่ยงด้านระบบและเทคโนโลยี (System/Network Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
B1	ระบบบริการเว็บไซต์ถูกรุมโจมตี (เช่น DDoS)	- ติดตั้งระบบ Firewall / Web Application Firewall - จัดทำ Backup ข้อมูลเว็บทุกวัน- ใช้บริการ CDN (เช่น Cloudflare) ป้องกันการโจมตี
B2	ช่องโหว่จากซอฟต์แวร์ หรือแอปพลิเคชันที่ล้าสมัย	- อัปเดตระบบและ Patch ทันทีที่มีเวอร์ชันใหม่ - สแกนหาช่องโหว่เป็นประจำ (Vulnerability Assessment)
B3	การเจาะระบบจากภายนอก (เช่น การแฮกระบบน้ำอัจฉริยะ)	- แยกระบบสำคัญออกจากระบบอินเทอร์เน็ต - ใช้ VPN สำหรับการเข้าระบบภายในจากภายนอก - บังคับใช้การยืนยันตัวตนหลายชั้น (MFA)

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน



ความเสี่ยงจากบุคลากร (Human Risk)

รายการ ความเสี่ยง

C1	เจ้าหน้าที่คลิกลิงกฟิชชิ่ง / เปิดไฟล์แนบอันตราย
C2	พนักงานลาออกแต่ยังเข้าระบบได้
C3	เจ้าหน้าที่นำแฟลชไดรฟ์หรืออุปกรณ์ส่วนตัวมาเสียบในระบบ

แนวทางลดความเสี่ยง

- อบรมภัยคุกคามไซเบอร์อย่างน้อยปีละ 2 ครั้ง
- จัดอบรมจำลองสถานการณ์ (Phishing Simulation)
- จัดทำคู่มือ/โปสเตอร์เตือนภัยติดตามพื้นที่ทำงาน
- จัดให้มีขั้นตอน “ถอนสิทธิ์การเข้าระบบ” ภายใน 24 ชั่วโมงหลังลาออก-ตรวจสอบบัญชีผู้ใช้งานประจำเดือน
- ติดตั้งระบบป้องกัน USB อัตโนมัติ
- ใช้นโยบาย BYOD พร้อมตรวจสอบอุปกรณ์ก่อนเชื่อมต่อ

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน



ความเสี่ยงจากการไม่มีแผนรับมือ (Operational Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
D1	ไม่มีแผนรับมือเมื่อเกิดเหตุไซเบอร์	- จัดทำ Incident Response Plan - แต่งตั้งทีม CSIRT (Computer Security Incident Response Team) - ซ้อมแผนทุก 6 เดือน
D2	ข้อมูลสูญหายโดยไม่ได้สำรอง	- สำรองข้อมูลระบบสำคัญทุกวัน และแยกเก็บบนระบบหลัก- ทดสอบการกู้คืนข้อมูล (Restore) อย่างน้อยเดือนละครั้ง

กำหนดนโยบายและการกำกับติดตาม

จัดตั้ง คณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Committee)	ระยะเวลา	แผนปฏิบัติ
แต่งตั้ง เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) ระดับกรม	ระยะสั้น (0-3 เดือน)	- อบรมบุคลากรเรื่องฟิชซิงและพฤติกรรมปลอดภัย - อัปเดตระบบและตรวจสอบบัญชีผู้ใช้งาน
มีการ ประเมินความเสี่ยงไซเบอร์ประจำปี และรายงานผลต่อผู้บริหาร	ระยะกลาง (3-6 เดือน)	- จัดทำ Incident Response Plan และทดสอบ - เริ่มใช้ VPN และ MFA สำหรับงานภายใน
ปรับปรุงแผนตามภัยคุกคามที่เปลี่ยนแปลง และตามแนวทางของ พรบ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	ระยะยาว (6-12 เดือน)	ตรวจสอบช่องโหว่ระบบและรายงานความเสี่ยง-จัดทำรายงานประเมินผลด้านไซเบอร์ต่อผู้บริหาร



THANK YOU

Suchaya Sanghan
EVP, SCP SYSTEMS CO.,LTD.