

หลักสูตรออนไลน์ · สำหรับ จป. และผู้ที่ต้องดูแลความปลอดภัยในองค์กร

ความเสี่ยงไซเบอร์ ในภาษาของ จป.

CYBER RISK FOR SAFETY PROFESSIONALS

บุญญภัทร พงษ์เก่า · **CISSP · CISM**

ความเสี่ยงและธรรมาภิบาลความปลอดภัยไซเบอร์ · ธุรกิจยานยนต์



มิถุนายน 2560

โรงงานปิโตรเคมี ประเทศซาอุดีอาระเบีย

ระบบ Safety Instrumented System (SIS) สั่ง shutdown กะทันหัน

สิงหาคม 2560

เกิดขึ้นอีกครั้ง

คราวนี้เขาเรียกทีมสืบสวนเข้ามา — และสิ่งที่เจอ ไม่ใช่ปัญหาเชิงกล

TRITON

หรือที่รู้จักในชื่อ TRISIS / HatMan

เป้าหมาย

ระบบ Safety Instrumented System (Schneider Electric Triconex)

ไม่ได้ขโมย

ข้อมูลลูกค้า · เงิน · ความลับทางการค้า

ที่มา

FireEye ชี้ไปที่สถาบันวิจัยของรัฐบาลรัสเซีย · ปี 2563 สหรัฐคว่ำบาตร
สถาบันนั้น



SIS คืออะไร

ระบบที่ทำหน้าที่สั่งหยุดเครื่องเมื่อ process ผิดปกติ — คือระบบที่ จป. ตรวจสอบและเซ็นรับรอง

มัลแวร์ตัวแรกในประวัติศาสตร์ ที่ถูกออกแบบมาเพื่อทำให้คนตาย

นักวิจัยหลายสำนักเรียกมันแบบนั้น ' ในเคสนี้ไม่มีใครบาดเจ็บ เพราะโรงงาน trip ไป safe state ก่อน — โชคดี ไม่ใช่เพราะ
ป้องกันได้

วันนั้น ระบบ SIS ที่มีคนเซ็นรับรองไว้ว่าปลอดภัย
ถูกโจมตีจากคีย์บอร์ดที่อยู่คนละทวีป

และไม่มี PPE ขึ้นไหนในโลกป้องกันมันได้

และมันเริ่มเกิดใกล้ตัวแล้ว

ประเทศไทย • ก.พ. 2562

โรงงาน HOYA ในไทย
กำลังผลิตหาย 60% นาน 3 วัน

มัลแวร์ติดคอมพิวเตอร์ราว 100 เครื่อง
ฝัง IT โดน สายการผลิตหยุดตาม

ที่มา: BleepingComputer

ประเทศไทย • ก.ย. 2563

แรนซัมแวร์ล็อกระบบ รพ.สระบุรี

ผู้ป่วยต้องถือประวัติการรักษามาเอง
สธ. ตั้งงบ 1.9 พันล้านยกกระดืบ รพ.รัฐ

ที่มา: Bangkok Post

ไทย-กัมพูชา • ก.ค.-ส.ค. 2568

ปะทะชายแดนลามสู่ไซเบอร์
139 การโจมตีในสองสัปดาห์

19 กลุ่มแฮกทวิสต์

เป้าคือหน่วยงานรัฐ การศึกษา สาธารณสุข

ที่มา: Group-IB

ญี่ปุ่น • มี.ค. 2565

ซัพพลายเออร์ชิ้นส่วนโดนโจมตี
ผู้ผลิตรายใหญ่หยุด 14 โรงงาน

28 สายการผลิตหยุด 1 วัน
เพราะระบบสั่งชิ้นส่วนของคู่ค้าล้ม

ที่มา: BleepingComputer

ยูเครน • ธ.ค. 2558

แฮกเกอร์สั่งตัดไฟผ่านระบบ
ควบคุม ไฟดับราว 225,000 ราย

หนึ่งในเคสแรกที่ยืนยันได้ว่า
ไซเบอร์ทำให้ไฟดับได้จริง

ที่มา: SANS ICS / E-ISAC

โปแลนด์ • ธ.ค. 2568

ผู้โจมตีสั่งหยุดกังหันไอน้ำ
ตั้ง PLC โรงไฟฟ้าเป็น STOP

ช่องทาง VPN ของฟาร์มลมที่ไม่มี MFA
CERT Polska เปิดเผย ส.ค. 2569

ที่มา: CERT Polska

ทุกเคสเป็นข่าวสาธารณะ • จุดร่วมคือของที่หยุดไม่ได้ — สายการผลิต ระบบไฟ โรงพยาบาล
นี่คือเหตุผลที่เราต้องถอดบทเรียนไซเบอร์ แบบเดียวกับที่เราถอดบทเรียนอุบัติเหตุ

บุญญภัทร พงษ์เก่า, CISSP

ขอบเขตงาน

ความเสี่ยงและธรรมาภิบาลความปลอดภัยไซเบอร์
(Cybersecurity Risk & Governance)

โฟกัสหลัก

ความเสี่ยงไซเบอร์จากคู่ค้า (TPCRM)
ดีลเลอร์ · ซัพพลายเออร์ · ผู้ให้บริการ

และ

ข้อกำหนดไซเบอร์ของยานยนต์ UN R155

สภาพแวดล้อมที่ดูแล

ธุรกิจยานยนต์ ทั้งผลิต วิจัย และขาย
ระบบ IT และ OT · 10 กว่าปีในสายนี้

พูดง่าย ๆ ฝั่งผม
เทียบได้กับ “จป.วิชาชีพ”
ของโลกไซเบอร์

งานของเราสองฝั่งใช้วิธีคิดเดียวกัน —
ต่างกันที่อันตรายฝั่งผมมองไม่เห็น และมัน
คิดเองได้



งานฝังผมก็แยกหลายเรื่อง เหมือนงานความปลอดภัย



CISSP

ออกแบบและบริหารทั้งระบบ



CEH

มองจากมุมผู้โจมตี



CC

พื้นฐานความปลอดภัยไซเบอร์



CISM

บริหารจัดการความเสี่ยง



Security+

พื้นฐานความปลอดภัย



CySA+

เฝ้าระวังและวิเคราะห์



CSAP

วิเคราะห์เหตุการณ์ระดับมืออาชีพ

เรื่องทำงานฝังนี้ต้องดู

ความต่อเนื่องทางธุรกิจ · รับมือเหตุการณ์ · จัดการช่องโหว่ · ประเมินความเสี่ยง · ธรรมาภิบาล

ใบรับรองบอกได้แค่ว่าผมสอบผ่าน · อันตรายงานของท่าน ท่านรู้ดีกว่าผม

สิ่งที่ท่านจะได้กลับไป

วันนี้ผมไม่สอนให้ท่านเป็นคนไอที — และไม่ต้องเป็น จป. ก็ฟัง รู้เรื่อง



แปลเองได้

ท่านจะแปลศัพท์ไอเบอร์เป็นภาษาความ
ปลอดภัยได้ด้วยตัวเอง



ใช้ของเดิมได้

ท่านจะรู้ว่าเครื่องมือที่ใช้อยู่ทุกวัน ใช้กับ
ความเสี่ยงไอเบอร์ตรงไหนบ้าง



ทำได้ทันที

3 อย่างที่กลับไปทำได้ทันที โดยไม่ต้อง
ขออนุมัติงบประมาณ

ความเสี่ยง คำนวณอย่างไร

ท่านมีข้อสงสัยแล้ว

สูตรเดียวกัน แต่ “โอกาสเกิด” ไม่เหมือนกัน

$$\text{RISK} = \text{LIKELIHOOD} \times \text{IMPACT}$$

โลกความปลอดภัย

ความเสี่ยง = โอกาสเกิด × ความรุนแรง

โลกไซเบอร์

Risk = Likelihood × Impact

ประเด็น

ฝั่งท่าน โอกาสเกิดมาจากสถิติและสภาพอุปกรณ์ — ฝั่งไซเบอร์ มาจากคนที่ตั้งใจหาช่อง และเปลี่ยนวิธีได้ทุกสัปดาห์

ท่านเรียกว่า	ผมเรียกว่า	จริง ๆ แล้วคือ
Hazard — สิ่งนี้อาจก่ออันตราย	Threat	สิ่งที่ทำให้เจ็บได้
JSA — ชีบ่งอันตรายก่อนเริ่มงาน	Threat Modeling	ถามว่า “งานนี้มีอะไรทำให้เจ็บได้บ้าง”
การประเมินความเสี่ยง	Risk Assessment	จัดลำดับว่าอันไหนต้องแก้ก่อน

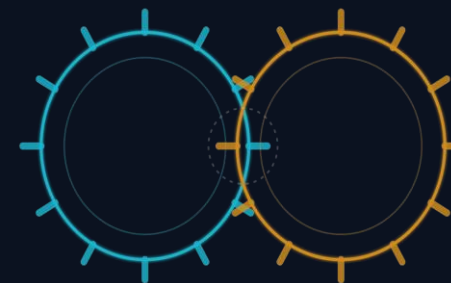
[illegible]

ท่านทำ JSA ก่อนเริ่มงาน ผมทำ Threat Modeling ก่อนขึ้นระบบ — เหมือนกันทุกประการ



แปลภาษา

เครื่องมือที่ท่านใช้อยู่ทุกวัน
ใช้กับความเสี่ยงไซเบอร์ได้ตรงไหนบ้าง



1

ทำไมเรื่องนี้เป็นงานของท่าน

2

แปลภาษา

3

เจาะลึก 2 เครื่องมือ

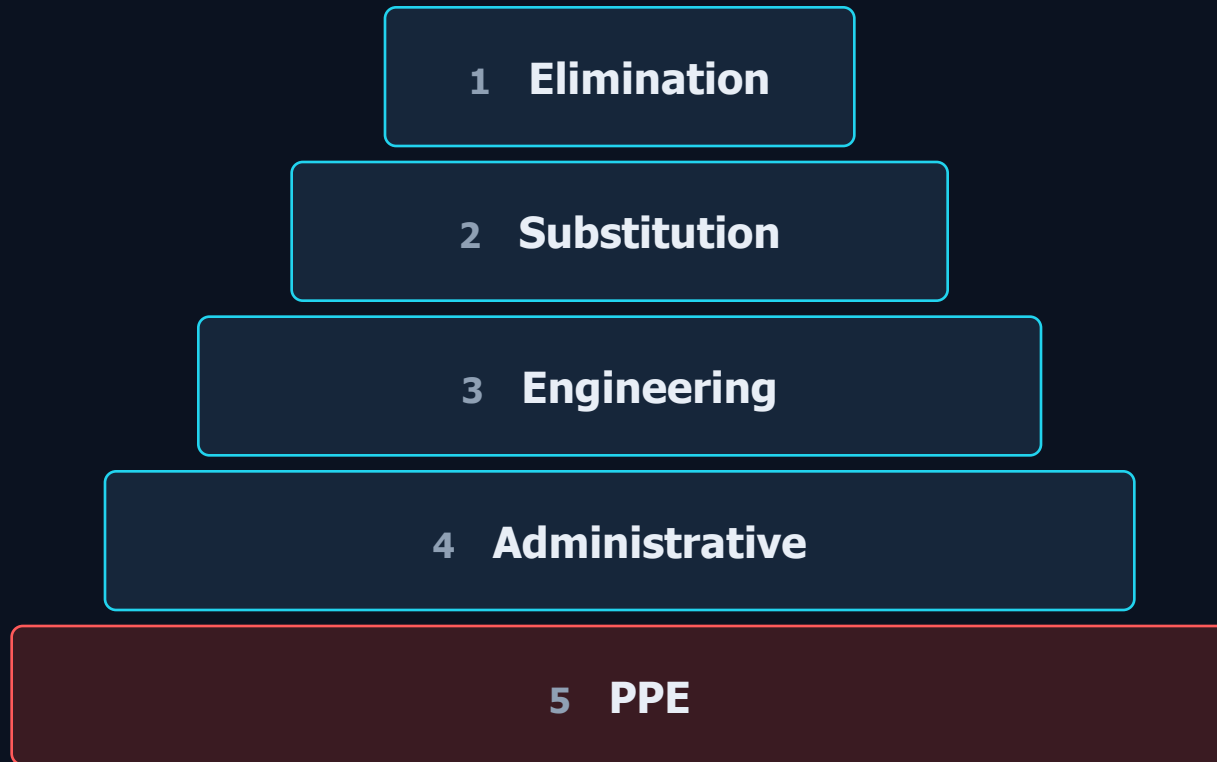
4

อุปมาพ้อง 4 จุด

5

ลงมือ

Hierarchy of Controls



Elimination

เอาอันตรายออกจากงานไปเลย ไม่ให้มืออยู่ตั้งแต่ต้น

Substitution

เปลี่ยนไปใช้สิ่งที่อันตรายน้อยกว่าแทนของเดิม

Engineering

ออกแบบให้อันตรายเข้าไม่ถึงคน โดยไม่ต้องพึ่งการตัดสินใจของใคร

Administrative

กำหนดวิธีทำงานและกฎ แล้วให้คนปฏิบัติตาม

PPE

ป้องกันที่ตัวคนเป็นขั้นสุดท้าย ตอนที่อันตรายยังอยู่ครบ

ชั้นไหนอ่อนแอที่สุด และทำไม

พีระมิดเดียวกัน คนละหน้างาน

ชั้น	โลกความปลอดภัย	โลกไซเบอร์
Elimination	ไม่ใช่สารเคมีตัวนั้นเลย	ไม่เก็บข้อมูลที่ไม่จำเป็น
Substitution	เปลี่ยนไปใช้สารที่อันตรายน้อยกว่า	ใช้ Passkey แทนรหัสผ่าน / Tokenization
Engineering	การ์ดเครื่องจักร ระบบระบายอากาศ	MFA, Network Segmentation, EDR, บล็อกมาโคร
Administrative	SOP, Permit to Work, ป้ายเตือน	นโยบาย, สิทธิ์การเข้าถึง, Change Management
PPE	หมวก แวน ถุงมือ	การอบรม Security Awareness

การอบรมแบบที่ท่านกำลังนั่งอยู่ตอนนี้ อยู่ชั้นล่างสุดของพีระมิด

มันคือ PPE ของโลกไซเบอร์ — จำเป็น แต่อ่อนแอที่สุด และไม่ควรเป็นมาตรการหลัก

ไม่ใช่ผมคิดเอง

งานวิจัย: การอบรมประจำปีไม่ลดการคลิกฟิชชิ่ง

19,500

พนักงานที่ถูกติดตาม
เป็นเวลา 8 เดือน

UC San Diego Health, 2025

ผลการศึกษา

การอบรมประจำปีแบบมาตรฐาน ไม่ได้ลดอัตราการคลิก
ฟิชชิ่งอย่างมีนัยสำคัญ

ตีพิมพ์ปี 2025 · เก็บข้อมูลจริงจากองค์กรเดียว ไม่ใช่แบบสอบถาม

คำถามที่ควรถามกลับองค์กร

ไม่ใช่ “เราอบรมพอหรือยัง” แต่คือ “เรามีมาตรการขั้น Engineering หรือยัง”

พจนานุกรม Safety → Security

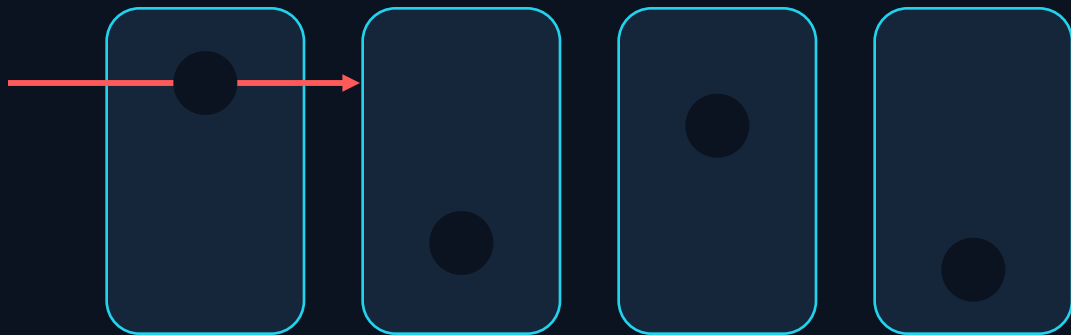
โลก Safety ที่ท่านรู้อยู่แล้ว	โลก Security
Hazard — สิ่งที่น่าจะก่ออันตราย	Threat
สอบสวนอุบัติเหตุ / หาสาเหตุราก	Incident Response / Post-Incident Review
JSA / ชี้บ่งอันตรายก่อนเริ่มงาน	Threat Modeling
Swiss Cheese Model	Defense in Depth
บัญชีเครื่องจักร / ทะเบียนสารเคมี	Asset Inventory

พจนานุกรม Safety → Security

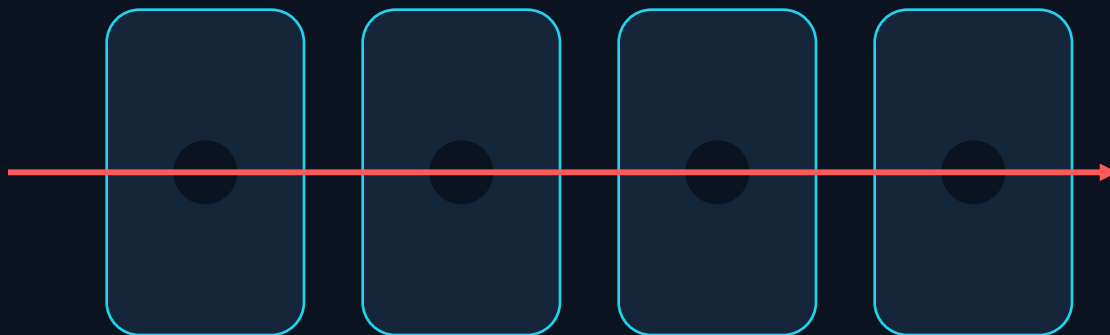
โลก Safety ที่ท่านรู้อยู่แล้ว	โลก Security
ซ้อมหนีไฟ / ซ้อมแผนฉุกเฉิน	IR Drill / DR Test — ซ้อมกู้ระบบจริง (Tabletop = ซ้อมบนโต๊ะ ขั้นต่ำสุด)
Just Culture — ไม่ลงโทษคนรายงาน	Blameless Culture
SDS / จำแนกสารเคมีตามอันตราย	Data Classification
Permit to Work	Change Management / Privileged Access
Lockout / Tagout	เดี่ยวเจาะล็อกช่วงถัดไป

Swiss Cheese Model = Defense in Depth

ปกติ — รู้ไม่ตรงกัน อันตรายผ่านไม่ได้



วันที่รู้เรียงตรงกันหมด — คือวันที่เกิดเหตุ



Firewall
รั้วและประตู

MFA
บัตรผ่าน

EDR
การตรวจตรา

Backup
แผนฉุกเฉิน

ไม่มีมาตรการไหน
ที่ไม่มีรู

งานของเราคือทำให้รูไม่เรียงกัน

และในรูปแบบนี้ ไม่มีแผ่นไหนชื่อ
"การอบรมพนักงาน"

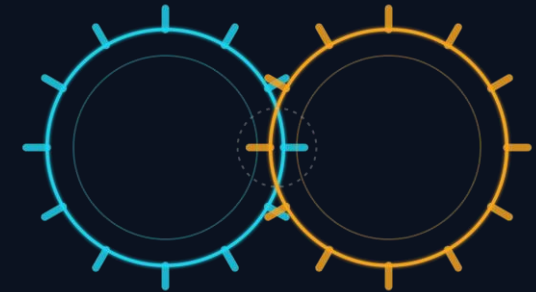
ISO 45001 กับ ISO 27001

ISO 45001

ระบบการจัดการอาชีวอนามัยและความปลอดภัย

ISO 27001

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ



โครงสร้างเดียวกัน



เข้าใจบริบทองค์กร



ประเมินความเสี่ยง



กำหนดมาตรการ



ตรวจติดตาม



ทบทวนโดยฝ่ายบริหาร

ลองแปลเองครับ



Backup

แปลเป็นภาษาความปลอดภัยว่าอะไร



Patch (การอัปเดตแพตช์)

แปลเป็นภาษาความปลอดภัยว่าอะไร

เฉลย Checkpoint

ศัพท์ไอที	แปลเป็นภาษาความปลอดภัย	ประเด็นที่ตามมา
Backup	แผนฉุกเฉิน / อุปกรณ์สำรอง	Backup ที่ไม่เคยทดสอบ restore = ถังดับเพลิงที่ไม่เคยตรวจ
Patch	การบำรุงรักษาเชิงป้องกัน (PM)	ระบบที่ไม่ patch = เครื่องจักรที่ไม่เคย PM

สรุปช่วงแปลภาษา

ทุกศัพท์ไอทีมีคู่ในภาษาความปลอดภัย — และเมื่อแปลเป็นภาษาของท่านได้ ท่านก็ตรวจมันได้



เจาะลึก 2 เครื่องมือ

Lockout/Tagout

การรายงานเหตุการณ์เกือบเกิด



1

ทำไมเรื่องนี้เป็นงานของท่าน

2

แปลภาษา

3

เจาะลึก 2 เครื่องมือ

4

อุปมาพ้อง 4 จุด

5

ลงมือ

5 ขั้นตอนของ LOTO

- 1 ประกาศ / แจ้งผู้เกี่ยวข้อง
- 2 ชีบปลั๊กแหล่งพลังงาน ทุกแหล่ง
- 3 ตัดแยกทุกแหล่ง
- 4 ใส่ล็อก + ป้าย
- 5 พิสูจน์ว่าตัดได้ผลจริง — ลองกดสตาร์ท / วัดด้วยมิเตอร์



กฎเหล็ก: คนที่ใส่ล็อกเท่านั้นที่ปลดได้ • หลายคนทำงาน = Group Lockout

หัวใจของ LOTO ไม่ใช่กุญแจ

**แต่คือ การทำให้อันตรายอยู่ในสภาวะ
ที่ “พิสูจน์ได้” ว่าเป็นศูนย์
และคนที่เสี่ยงเป็นคนคุมสวิตช์เอง**

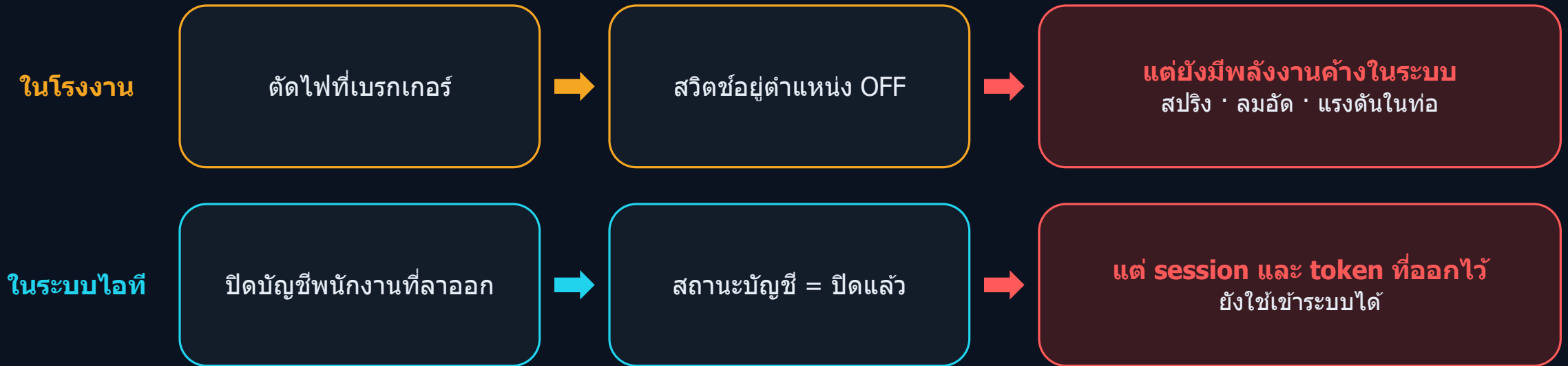
ทำไมแปลตรงตัวไม่ได้

ชั้นส่วนของ LOTO	คู่ในโลกไซเบอร์
ตัดพลังงาน ทุกแหล่ง	ปิดสิทธิ์ตอนพนักงานลาออก — AD, VPN, SaaS, SSH key, API token, etc.
พลังงานสะสม	Session / Token ที่ยังไม่หมดอายุ
ล็อก + ป้าย	Change Ticket + Audit Log
พิสูจน์ (Verify)	Access Review / ลอง login ด้วยบัญชีที่เพิ่งปิด



สองแถวสีเหลืองคือแถวที่วงการไอทีทำตกบ่อยที่สุด

พลังงานสะสม = Session ที่ยังเปิดค้าง



บัญชีถูกปิดแล้ว แต่คนนั้นยังใช้งานต่อได้ — นั่นคือสปริงที่ยังอัดอยู่

ในโรงงานของท่าน ห้ามใครเข้าไปในเครื่อง
จนกว่าจะลองกดสตาร์ทแล้วเครื่องไม่ติด

แต่ในระบบไอที เราปิดบัญชีคนที่ลาออก
แล้วเดินจากไปแล้ว — โดยไม่เคยลองกดสตาร์ท

วันนี้ผมไม่ได้มาสอนท่าน ผมมายืมมาตรฐานของท่าน ไปวัดวงการผมเอง

อันไหนคือ Near-miss ทางไซเบอร์



Firewall บล็อกการเชื่อมต่อ 2 ล้านครั้งเมื่อวาน



พนักงานคลิกฟิชชิ่งและกรอกรหัสผ่านไปแล้ว แต่ MFA หยุดไว้



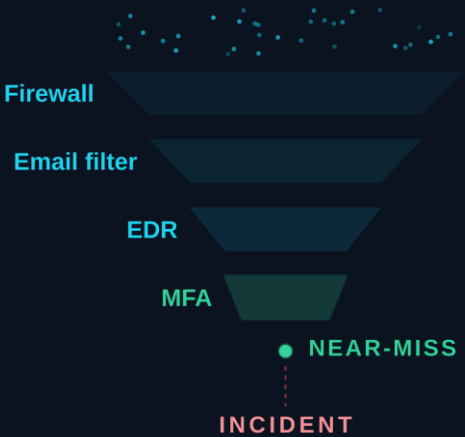
เกือบโอนเงินตามอีเมลปลอม แต่บังเอิญโทรถามหัวหน้าก่อน



ระบบล่ม 3 ชั่วโมงจากแรนซัมแวร์

Near-miss = รอดเพราะชั้นสุดท้าย หรือรอดเพราะโชค

ข้อ	คำตอบ	เหตุผล
ก) Firewall บล็อก 2 ล้านครั้ง	ไม่ใช่	มาตรการทำงานตามปกติ
ข) MFA หยุดไว้ทัน	ใช่	รอดเพราะชั้นสุดท้าย
ค) บังเอิญโทรทรมก่อนโอน	ใช่	รอดเพราะโชค
ง) ระบบล่มจากแรนซัมแวร์	ไม่ใช่	อุบัติเหตุแล้ว



เหมือนราวกันตกที่กันคนไม่ให้ตก — ไม่มี จป. คนไหนเรียกสิ่งนั้นว่า near-miss

คนที่โดน Near-miss ไซเบอร์ มักไม่รู้ตัว

โลกความปลอดภัย

คนที่เกือบตกนั้งร้าน รู้ตัวว่าเกือบตาย เขาจึงรายงานได้

โลกไซเบอร์

คนที่โดน near-miss ส่วนใหญ่ ไม่รู้ตัวเลยว่าเกิดอะไรขึ้น

ผลที่ตามมา

ระบบรายงานแบบสมัครใจเก็บได้แค่เศษเสี้ยว — ฟังไซเบอร์ต้องฟังระบบตรวจจับเป็นหลัก แล้วใช้คนรายงานเป็นส่วนเสริม

โลกไซเบอร์

เวลาที่ผู้โจมตีอยู่ในระบบก่อนถูกตรวจพบ

ยอดที่โผล่น้ำ = ที่เราตรวจพบ

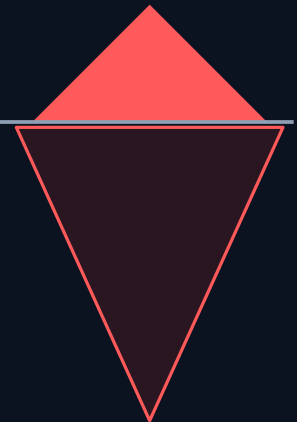
ค่ากลางทั่วโลก

14 วัน

เคสจرائم และคนในปลอมตัว

122 วัน

ที่มา: Mandiant M-Trends 2026 (ข้อมูลปี 2025)



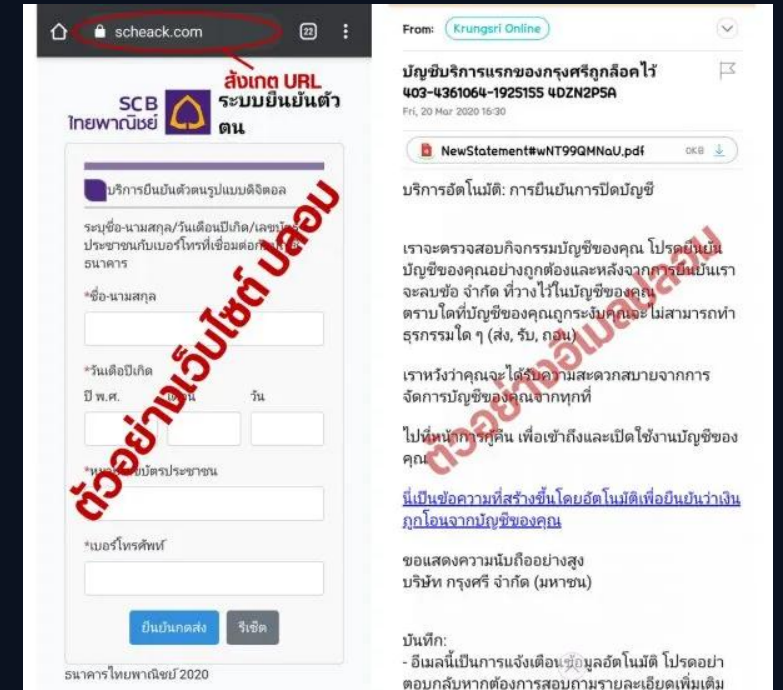
เรื่องที่ท่านสอนวงการผมได้

Just Culture

ท่านรู้ดีว่าถ้าลงโทษคนที่รายงาน
ระบบรายงานตายภายในเดือนเดียว

แล้วองค์กรที่ประจานพนักงานที่คลิก phishing test ล่ะครับ

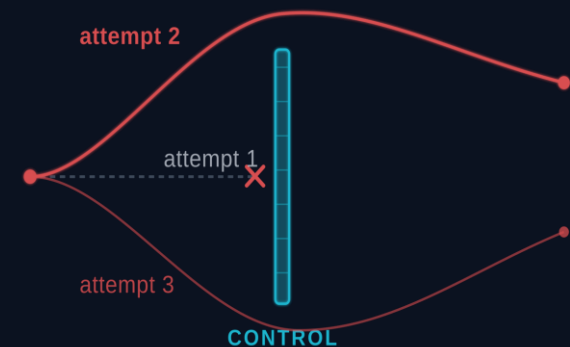
คนจะซื่อ → ไม่มีใครรายงาน → เวลาที่ผู้โจมตีอยู่ในระบบโดยไม่มีใครรู้ ก็ยาวขึ้น



4

อุปมาพัง 4 จุด

ก่อนหน้านี้ผมบอกว่างานเราเหมือนกัน
ตอนนี้ผมจะบอกว่ามันไม่เหมือนตรงไหน



1

ทำไมเรื่องนี้เป็นงานของท่าน

2

แปลภาษา

3

เจาะลึก 2 เครื่องมือ

4

อุปมาพัง 4 จุด

5

ลงมือ

ศัตรูปรับตัวได้

โลกความปลอดภัย

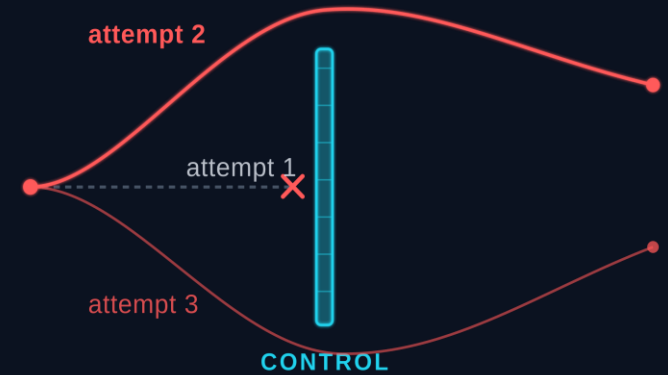
แรงโน้มถ่วงไม่เคยเรียนรู้จากความล้มเหลวของมัน

โลกไซเบอร์

ผู้โจมตีดูมาตรการที่เราคิด แล้วเปลี่ยนวิธีในสัปดาห์ถัดไป

ทำไมถึงสำคัญ

นี่คือรอยแตกที่ใหญ่ที่สุด และมันเปลี่ยนวิธีออกแบบมาตรการทั้งหมด



ต้องถูกทุกครั้ง VS ผิดครั้งเดียว

โลกความปลอดภัย

ควบคุมได้ 99% ถือว่าดีมาก

โลกไซเบอร์

ผู้โจมตีต้องการแค่ 1% — เขาลองหมื่นครั้งได้ ผมพลาดครั้งเดียวไม่ได้

ทำไมถึงสำคัญ

มาตรการที่ “ส่วนใหญ่ได้ผล” ในโลกไซเบอร์ แปลว่าไม่ได้ผล



มองไม่เห็น

โลกความปลอดภัย

เห็นสายไฟเปลือย เห็นน้ำมันหก เห็นคนไม่ใส่หมวก

โลกไซเบอร์

ข้อมูลรั่วมาแล้ว 6 เดือนโดยไม่มีใครรู้ — ยังเป็นเรื่องปกติ

ทำไมถึงสำคัญ

นี่คือเหตุผลที่ฝั่งเราลงทุนกับ “การมองเห็น” มากกว่าที่ท่านคิด



จุดฟังที่ 4 จาก 4



ฝั่งท่าน “Zero Accident” เป็นเป้าที่ชอบธรรม

ฝั่งผม “Zero Breach” เป็นเป้าที่ผิด — หลักของเราคือ Assume Breach

สมมติไว้ก่อนว่าเขาเข้ามาแล้ว

ทำไม KPI “Cyber Incident = 0” ถึงอันตราย

ถ้าองค์กรตั้ง KPI ว่าศูนย์ ระบบรายงาน near-miss ที่เราเพิ่งคุยกัน จะตายภายในไตรมาสเดียว

คนจะไม่รายงาน

ตัวเลขสวยขึ้น

ความเสี่ยงจริงเพิ่มขึ้น

แยกตามความรุนแรง เหมือนตัวชี้วัดอุบัติเหตุ LTIFR / TRIR

แทนที่จะตั้งเป้าว่า

Cyber Incident = 0

ให้ตั้งเป้าแบบนี้แทน

กู้ระบบคืนได้เร็วแค่ไหน

RTO ไม่เกิน 4 ชั่วโมง

RPO ไม่เกิน 15 นาที

ผลกระทบต่อธุรกิจ

ไม่มีเหตุที่ทำให้

สายการผลิตหยุดเกิน 2 ชั่วโมง

เส้นแบ่งที่ **PDPA** ชี้ให้เห็น

**ทุกเหตุที่เข้าเกณฑ์
แจ้ง สคส. ทันภายใน 72 ชม.
(นับแต่ทราบเหตุ)**



ลงมือ

Scenario 3 ข้อ

ทุกตัวเลือกฟังดูมีเหตุผล แต่มีตัวเดียวที่ดีที่สุด



1

ทำไมเรื่องนี้เป็นงานของท่าน

2

แปลภาษา

3

เจาะลึก 2 เครื่องมือ

4

อุปมาฟัง 4 จุด

5

ลงมือ

พนักงานฝ่ายผลิตแจ้งว่าเปิดไฟล์แนบแปลก ๆ เมื่อ 20 นาทีที่แล้ว
ตอนนี้เครื่องเข้าผิดปกติ — ท่านควรทำอะไรเป็นอย่างแรก



สั่งปิดเครื่องทันที



แจ้งผู้รับผิดชอบ และแยกเครื่องออกจากเครือข่าย (ถอดสาย LAN / ปิด Wi-Fi) โดยยังไม่ปิดเครื่อง



สแกนไวรัสด้วยโปรแกรมที่มีอยู่



รายงานผู้บริหารเพื่อขอ งบ จัดซื้อระบบป้องกัน

เฉลย SCENARIO 1

พนักงานฝ่ายผลิตแจ้งว่าเปิดไฟล์แนบแปลก ๆ เมื่อ 20 นาทีที่แล้ว ตอนนี้เครื่องชำรุดปกติ — ท่านควรทำอะไรเป็นอย่างแรก



สั่งปิดเครื่องทันที



แจ้งผู้รับผิดชอบ และแยกเครื่องออกจากเครือข่าย (ถอดสาย LAN / ปิด Wi-Fi) โดยยังไม่ปิดเครื่อง

คำตอบที่ดีที่สุด



สแกนไวรัสด้วยโปรแกรมที่มีอยู่



รายงานผู้บริหารเพื่อขอ งบ จัดซื้อระบบป้องกัน

ทำไมไม่ปิดเครื่อง

การปิดเครื่อง = การล้างที่เกิดเหตุ หลักฐานสำคัญอยู่ในหน่วยความจำ ปิดปั๊บหายหมด

ส่วนการถอดสาย LAN = การกันพื้นที่ — หยุดการแพร่ แต่รักษาที่เกิดเหตุไว้

ผู้รับเหมาภายนอกขอ Remote Access เข้าระบบควบคุมการผลิต
เพื่อซ่อมบำรุงดาวน์คีนี่ — ท่านควรเสนออะไร



อนุมัติ เพราะดาวน์และเป็นคู่ค้าประจำ



ปฏิเสธทั้งหมด ห้าม Remote Access เด็ดขาด



ใช้กระบวนการเดียวกับ Permit to Work: ระบุขอบเขต เวลาเริ่ม-จบ ผู้รับผิดชอบ บันทึก session และปิดสิทธิ์ทันทีเมื่อจบงาน พร้อมตรวจสอบว่าปิดจริง



ให้บัญชี admin ถาวรไว้เลย จะได้ไม่ต้องขบอย

เฉลย SCENARIO 2

ผู้รับเหมาภายนอกขอ Remote Access เข้าระบบควบคุมการผลิต เพื่อซ่อมบำรุงตัวเดินนี้ — ท่านควรเสนออะไร



อนุมัติ เพราะตัวเดินและเป็นผู้ค้าประจำ



ปฏิเสธทั้งหมด ห้าม Remote Access เด็ดขาด



ใช้กระบวนการเดียวกับ Permit to Work: ระบุขอบเขต เวลาเริ่ม-จบ ผู้รับผิดชอบ บันทึก session และปิดสิทธิ์ทันทีเมื่อจบงาน พร้อมตรวจสอบว่าปิดจริง

คำตอบที่ดีที่สุด



ให้บัญชี admin ถาวรไว้เลย จะได้ไม่ต้องขบ่อย

ทำไมไม่ใช่ ข

ข ฟังดูปลอดภัยแต่จริงก็เดินไม่ได้ — ท่านไม่เคยห้ามงานตัวเดินเด็ดขาด แต่ท่านออกเกณฑ์ในการออกใบอนุญาตทำงาน

ค คือ Permit to Work + LOTO ขั้นที่ 5 รวมกัน

ฝ่ายบริหารตั้ง KPI ปีนหน้าว่า “Cyber Incident = 0”
ท่านควรทำอย่างไร



เห็นด้วย เป็นเป้าที่ท้าทายดี



ท้วงที่จะทำให้คนไม่รายงานเหตุ และเสนอเป็นเป้าแยกตามความรุนแรงแทน



เสนอลดเป็น “ไม่เกิน 5 ครั้งต่อปี”



ไม่ยุ่ง เป็นเรื่องของ IT

เฉลย SCENARIO 3

ฝ่ายบริหารตั้ง KPI ปีหน้าว่า "Cyber Incident = 0" ท่านควรทำอย่างไร



เห็นด้วย เป็นเป้าที่ท้าทายดี



ท้วงที่จะทำให้คนไม่รายงานเหตุ และเสนอเป็นเป้าแยกตามความรุนแรงแทน

คำตอบที่ดีที่สุด



เสนอลดเป็น "ไม่เกิน 5 ครั้งต่อปี"



ไม่ยุ่ง เป็นเรื่องของ IT

เหตุผลที่ท่านใช้ท้วงได้ทันที

คือเหตุผลเดียวกับที่ท่านใช้ปกป้องระบบรายงาน near-miss มาตลอด

เสนอแทนด้วย RTO/RPO และเกณฑ์การแจ้งตาม PDPA

ไม่ต้องขอ งบ ไม่ต้องซื้ออะไร ไม่ต้องรอ IT

1

เพิ่ม 1 บรรทัดใน JSA

“งานนี้เกี่ยวข้องกับระบบควบคุมหรือ
ข้อมูลสำคัญหรือไม่”

ใช้แบบฟอร์มเดิมที่มีอยู่

2

ถามคำถามเดียว

ขอดูขั้นตอนปิดสิทธิ์พนักงานลาออก
แล้วถามว่า

“เคยลองกดสตาร์ทไหม”

3

เข้าวาระ คปอ.

เสนอความเสี่ยงไซเบอร์เข้าที่ประชุม
คปอ.

กลไกตามกฎหมาย : “ไม่มี คปอ. ใช้
ประชุมประจำเดือนของทีมแทนได้”

ท่านไม่ได้กำลังเรียนเรื่องใหม่
ท่านกำลังขยายขอบเขตของสิ่งที่ท่านเก่งอยู่แล้ว

เพราะวันที่ระบบความปลอดภัยถูกโจมตีจากคีย์บอร์ด — คนที่ต้องรู้ว่ามันแปลว่าอะไร คือท่าน ไม่ใช่แผนกไอที

ขอบคุณครับ

บุญญภัทร พงษ์เก่า · CISSP · CISM

theybertalk.net · เช็กलिस्टทั้งหมดโหลดได้ ไม่ต้องลงทะเบียน
แบบทดสอบ 10 ข้อ → ลิงก์ในแชท · ทำผ่านรับ E-Certificate

แหล่งอ้างอิง

- TRITON/TRISIS — MIT Technology Review (2019); FBI Private Industry Notification (2022)
- NIOSH Hierarchy of Controls — CDC / OSHA
- Lockout/Tagout — OSHA 29 CFR 1910.147
- “Understanding the Efficacy of Phishing Training in Practice” — UC San Diego Health, 2025
- Swiss Cheese Model — James Reason
- ประกาศ กคส. เรื่องหลักเกณฑ์และวิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
- ISO 45001 / ISO 27001
- BleepingComputer (2019, 2022) · Bangkok Post (2020) · Group-IB (2025) · SANS ICS/E-ISAC (2016) · CERT Polska (2026)

เอกสารนี้เป็นข้อมูลประกอบการอบรม ไม่ใช่คำแนะนำทางกฎหมาย



สแกนรับเช็กलिस्ट