R0Cyber

CYBER LAW & STANDARDS · 2.2 ตอนที่ 4

Workshop Data Flow ถึง Tabletop Exercise

ลงมือวิเคราะห์ data flow จัดทำ compliance checklist และ incident reporting flow แล้วฝึกตัดสินใจกับเหตุจำลอง

Data flow | Checklist | Tabletop

CYBER ACT	พ.ร.บ.ไซเบอร์ 2562 · CII	สกมช.
COMPUTER	พ.ร.บ.คอมพิวเตอร์	ม.5–14, 26
PDPA	คุ้มครองข้อมูลส่วนบุคคล	สคส.
POLICY	นโยบายความปลอดภัยองค์กร	ISO 27001
REPORT	รายงานเหตุ · ประสานงาน	72 ชม.
EXERCISE	Tabletop · ซ้อมตัดสินใจ	Workshop

CYBER LAW · POLICY · RESPONSE

อ้างอิง พ.ร.บ.ไซเบอร์ 2562 · พ.ร.บ.คอมพิวเตอร์ 2550/2560 · PDPA 2562 · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

R0Cyber

ตอนนี้มี 5 หัวข้อ

01	โจทย์บริษัทจำลอง	ธุรกิจ · ระบบ · ข้อมูลที่ใช้
02	กิจกรรม 1–2	วิเคราะห์ Data flow · Compliance checklist
03	กิจกรรม 3	เหตุจำลอง · Incident reporting flow
04	กิจกรรม 4	Tabletop exercise · ประเมินผล
05	สรุปและส่งงาน	สิ่งที่ต้องส่ง · แบบทดสอบหลังเรียน

R0Cyber

บริษัทจำลอง: เฮลธ์พลัส (บริษัทสมมติ)

ธุรกิจ

- แอปร้านยาออนไลน์ + ปรึกษาเภสัชกรผ่านวิดีโอ
- ลูกค้า 200,000 ราย · คำสั่งซื้อวันละ 3,000 รายการ
- เป็นผู้ให้บริการระบบจ่ายยาให้โรงพยาบาลรัฐแห่งหนึ่ง (คู่สัญญา)

ข้อมูลที่ใช้

- ชื่อ ที่อยู่ เบอร์โทร เลขบัตรประชาชน
- ใบสั่งยาและประวัติการใช้ยา (ข้อมูลสุขภาพ = อ่อนไหว)
- ข้อมูลชำระเงินผ่านผู้ให้บริการชำระเงิน

แอป/เว็บ

API บนคลาวด์ (สิงคโปร์)

ฐานข้อมูลคำสั่งซื้อ

บริษัทขนส่ง

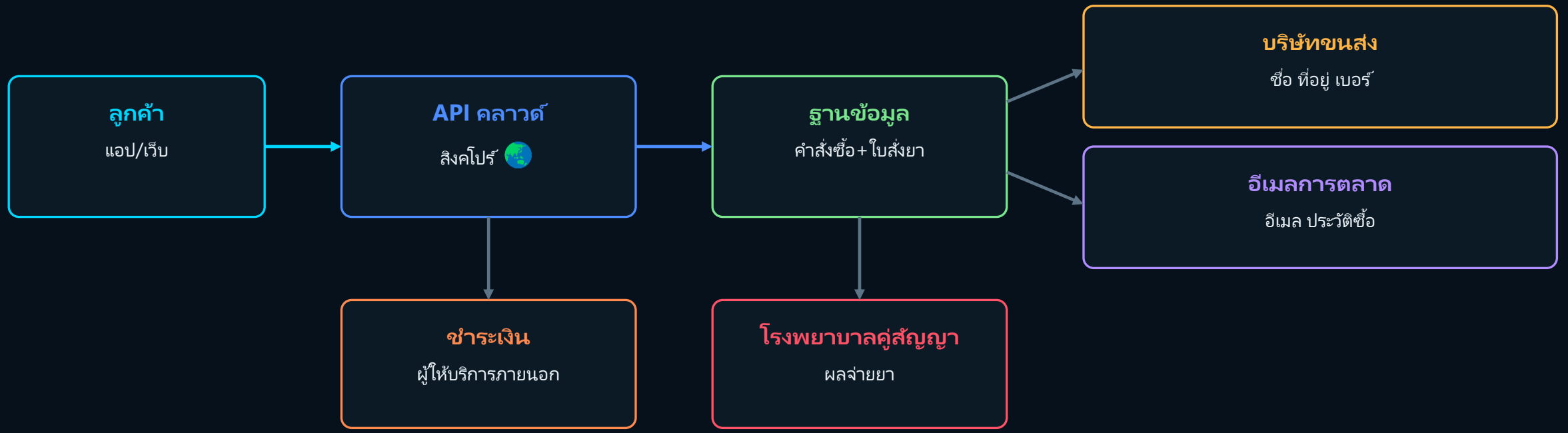
ระบบอีเมลการตลาด

Wi-Fi สาขา 12 แห่ง

ทุกชื่อและตัวเลขในโจทย์เป็นข้อมูลสมมติเพื่อการฝึก

R0Cyber

กิจกรรม 1: วาดเส้นทางข้อมูล



ถามกับทุกลูกศร: ข้อมูลอะไร · อ่อนไหวไหม · ฐานทางกฎหมายใด · เข้ารหัสไหม · ข้ามประเทศไหม · มีสัญญา (DPA) ไหม · เก็บนานเท่าไร

ใช้ Worksheet 1 ในชุดเอกสาร Workshop (ดาวน์โหลดได้จากหน้าตอนนี้)

R0Cyber

ตัวอย่างผลวิเคราะห์ (เฉลยบางส่วน)

เส้นทาง	ประเด็นที่พบ	กฎหมาย/ข้อกำหนด	สิ่งที่ต้องทำ
แอป ⟶ คลาวด์สิงคโปร์	ข้อมูลสุขภาพข้ามประเทศ	PDPA ม.26, 28–29	ประเมินเกณฑ์ส่งต่างประเทศ + DPA
ฐานข้อมูล ⟶ อีเมลการตลาด	ส่งประวัติซื้อยาไปทำการตลาด	PDPA ม.21, 24, 26	ตัดข้อมูลยา · ขอความยินยอมแยก
ฐานข้อมูล ⟶ ขนส่ง	ส่งข้อมูลเกินจำเป็น?	PDPA ม.22, 40	ส่งเฉพาะชื่อ ที่อยู่ เบอร์ + DPA
ระบบ ⟷ โรงพยาบาลรัฐ	เป็นผู้ให้บริการของหน่วยงานรัฐ/CII	พ.ร.บ.ไซเบอร์ · สัญญา	มาตรฐานตามสัญญา · ผู้ประสานงาน
Wi-Fi สาขา	ให้ลูกค้าใช้อินเทอร์เน็ต	พ.ร.บ.คอมพิวเตอร์ ม.26	เก็บ log ≥ 90 วัน

หมายเหตุ: ไม่มีเฉลยเดียว — ให้ใส่เหตุผลทางกฎหมายประกอบทุกข้อ และระบุผู้รับผิดชอบกับกำหนดเสร็จ

R0Cyber

กิจกรรม 2: จัดทำ Compliance Checklist

PDPA

- ROPA ครบทุกกิจกรรม
- ฐานทางกฎหมาย + consent ข้อมูลสุขภาพ
- Privacy notice ในแอป
- DPA กับขนส่ง คลาวด์ ชำระเงิน
- DPO (ข้อมูลอ่อนไหวเป็นหลัก)
- แผนแจ้งเหตุ 72 ชม.

พ.ร.บ.ไซเบอร์ + สัญญา

- มาตรฐานความปลอดภัยตามสัญญากับโรงพยาบาล
- ผู้ประสานงานด้านไซเบอร์ 24 ชม.
- ประเมินความเสี่ยงปีละครั้ง
- ช่องทางแจ้งเหตุถึงคู่สัญญา
- ซ้อมแผนร่วมกัน

พ.ร.บ.คอมพิวเตอร์ + นโยบาย

- log Wi-Fi/ระบบ ≥ 90 วัน
- ซิงก์เวลา · log แก้ไขไม่ได้
- นโยบายการใช้งานที่ยอมรับได้
- ขั้นตอนเก็บหลักฐาน
- ขั้นตอนแจ้งความ

ทุกข้อต้องมี: สถานะ (มี/บางส่วน/ไม่มี) · หลักฐาน · ผู้รับผิดชอบ · กำหนดเสร็จ — แล้วจัดลำดับตามความเสี่ยง

R0Cyber

กิจกรรม 3: เหตุจำลอง — ข้อมูลรั่วและระบบถูกเข้ารหัส

timeline.log

ศ. 22:10 SOC แจ้งเตือน: ส่งออกข้อมูลจำนวนมากจาก order-db
ศ. 22:40 ไฟล์บน file-server ถูกเข้ารหัส · พบข้อความเรียกค่าไถ่
ศ. 23:05 ตัดการเชื่อมต่อเครือข่ายเซิร์ฟเวอร์ที่ได้รับผล
ส. 08:00 ผู้โจมตีส่งตัวอย่างข้อมูลลูกค้า 100 ราย (มีใบสั่งยา)
ส. 10:00 ระบบจ่ายยาของโรงพยาบาลคู่สัญญาเชื่อมต่อไม่ได้
ส. 14:00 นักข่าวสอบถามผ่านเพจบริษัท

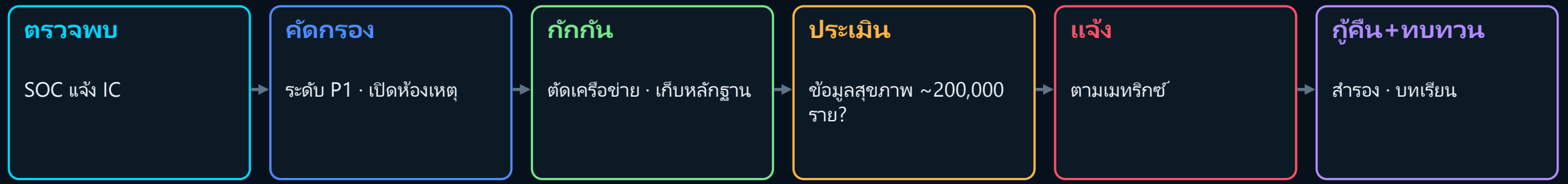
ให้ทีมตอบ

- "ทราบเหตุ" เมื่อไร ⟶ นาฬิกา 72 ชม.
- ข้อมูลอะไร กี่ราย อ่อนไหวไหม
- ต้องแจ้งใครบ้าง ตามกฎหมาย/สัญญา
- ใครตัดสินใจ ใครสื่อสาร
- หลักฐานอะไรต้องเก็บก่อนกู้คืน

ตัวอย่างนี้เป็นสถานการณ์สมมติเพื่อฝึกการตัดสินใจและการประสานงาน

R0Cyber

ผลงาน: Incident Reporting Flow ของเฮลธ์พลัส



แจ้ง	เหตุผล	ภายใน	ผู้แจ้ง
สคส.	ข้อมูลสุขภาพรั่ว — มีความเสี่ยง	72 ชม. นับจาก ศ. 22:10	DPO
ลูกค้าที่ได้รับผลกระทบ	ความเสี่ยงสูง (สุขภาพ + ถูกหลอกลวง)	โดยไม่ชักช้า + แนวทางเยียวยา	DPO + สื่อสาร
โรงพยาบาลคู่สัญญา	บริการจ่ายยากระทบ · ตามสัญญา	ตามสัญญา (เร็วที่สุด)	ผู้บริหาร
ตำรวจไซเบอร์	มีการกระทำผิด ม.5, 7, 9, 10	หลังเก็บหลักฐาน	กฎหมาย
ThaiCERT / สกมช.	ขอความช่วยเหลือ · ภัยกระทบคู่สัญญาภาครัฐ	โดยเร็ว	CISO

กิจกรรม 4: Tabletop — ซ้อมตัดสินใจบนโต๊ะ

เวลา	สถานการณ์แทรก (inject)	ต้องตัดสินใจ
T+0	SOC แจ้งเตือนการส่งออกข้อมูลผิดปกติ	เปิดเหตุระดับใด · ใครเป็น IC
T+1 ชม.	ไฟล์ถูกเข้ารหัส พบข้อความเรียกค่าไถ่	กักกันอย่างไรโดยไม่ทำลายหลักฐาน
T+10 ชม.	ผู้โจมตีปล่อยตัวอย่างข้อมูลลูกค้า	ยืนยันข้อมูลรั่ว · เริ่มร่างรายงาน สคส.
T+16 ชม.	นักข่าวถาม · ลูกค้าโพสต์ในโซเชียล	ข้อความสื่อสาร · ใครเป็นโฆษก
T+40 ชม.	ผู้บริหารถามว่าจะจ่ายค่าไถ่ไหม	ข้อพิจารณาทางกฎหมาย ความเสี่ยง และทางเลือกกู้คืน
T+70 ชม.	ข้อมูลบางส่วนยังไม่ครบ	แจ้ง สคส. เท่าที่ทราบ + อัปเดตภายหลัง

วิธีเล่น: แบ่งบทบาท IC · ไอที · DPO/กฎหมาย · สื่อสาร · ผู้บริหาร · ผู้ดำเนินเกมเปิด inject ทีละใบ · 90–120 นาที · ห้ามใช้ระบบจริง

R0Cyber

ประเมินผลการซ้อม และทบทวนหลังการซ้อม

เกณฑ์	ดี (3)	พอใช้ (2)	ต้องปรับ (1)
ความครบถ้วนทางกฎหมาย	ระบุทุกหน่วยงาน + เหตุผล	ขาด 1 หน่วยงาน	ขาดหลายหน่วยงาน
ความทันเวลา	แจ้ง สคส. < 72 ชม. พร้อมบันทึก	ทันแต่ไม่มีบันทึก	เกิน 72 ชม.
การตัดสินใจและบทบาท	IC ชัด ตัดสินใจเป็นลำดับ	บางจุดสับสน	ไม่มีผู้ตัดสินใจ
การสื่อสาร	ข้อความถูกต้อง สอดคล้องทุกช่องทาง	ช้าหรือไม่สอดคล้อง	ขัดกันเอง
หลักฐาน	เก็บก่อนกู้คืน มี hash	เก็บบางส่วน	ล้างระบบก่อนเก็บ

ทบทวนหลังการซ้อม: 3 อย่างที่ได้ผล · 3 อย่างที่ต้องแก้ · ใครแก้ เสร็จเมื่อไร — แล้วปรับนโยบายและเมทริกซ์การรายงาน

DELIVERABLES

R0Cyber

ผลงานที่ได้จาก Workshop

1. Data flow + ผลวิเคราะห์

แผนภาพเส้นทางข้อมูล และประเด็นกฎหมายรายเส้นทาง

2. Compliance checklist

PDPA · พ.ร.บ.ไซเบอร์ · พ.ร.บ.คอมพิวเตอร์ พร้อมสถานะและผู้รับผิดชอบ

3. Incident reporting flow

ขั้นตอนภายใน + เมทริกซ์แจ้งหน่วยงานภายนอก

4. ผล Tabletop + แผนปรับปรุง

คะแนนตามเกณฑ์ และรายการสิ่งที่ต้องแก้

ดาวน์โหลด: ชุดเอกสาร Workshop (Worksheet 1–5 + แนวเฉลยสำหรับผู้สอน) จากหน้าตอนนี้บน learn.r0cyber.com

SUMMARY · ตอนที่ 4

สรุป: Workshop

- ✓ Data flow ช่วยเห็นประเด็นกฎหมายรายเส้นทาง
- ✓ Checklist ต้องมีสถานะ หลักฐาน ผู้รับผิดชอบ
- ✓ Reporting flow + เมทริกซ์ = รู้ว่าต้องแจ้งใคร เมื่อไร
- ✓ Tabletop ซ้อมตัดสินใจก่อนเกิดเหตุจริง
- ✓ ทบทวนหลังซ้อม แล้วปรับนโยบาย

ทำแบบทดสอบหลังเรียน เพื่อรับใบรับรอง

ขั้นต่อไป

สอบหลังเรียน

ทดสอบความรู้ทั้งหลักสูตร

- 15 ข้อ · ผ่าน 75%
- คะแนนต้องไม่ต่ำกว่าก่อนเรียน
- รับใบรับรองที่มีรหัสตรวจสอบ