R0Cyber

CYBER LAW & STANDARDS · 2.2 ตอนที่ 1

พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

ใครกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหน้าที่อะไร และองค์กรทั่วไปเกี่ยวข้องอย่างไร

สกมช. | CII | ภัยคุกคาม 3 ระดับ

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	ทำไมต้องมีกฎหมายนี้	ที่มา · ช่วงเวลา · กฎหมายลำดับรอง
02	โครงสร้างหน่วยงาน	กมช. · กกม. · สกมช. · หน่วยงานควบคุม
03	หน่วยงาน CII	ด้านที่กำหนด · หน้าที่ · มาตรฐานขั้นต่ำ
04	ภัยคุกคามและแนวโน้ม	3 ระดับ · องค์กรทั่วไป · ร่างแก้ไข
05	ทบทวนและสรุป	Quick check · สรุปตอน

R0Cyber

ทำไมต้องมี พ.ร.บ.ไซเบอร์

ปกป้องบริการสำคัญ

ไฟฟ้า ประปา ธนาคาร โรงพยาบาล โทรคมนาคม — ถ้าหยุด ทั้งประเทศได้รับผลกระทบ

ประสานงานระดับชาติ

มีศูนย์กลางรับแจ้ง วิเคราะห์ และช่วยรับมือเหตุ

มาตรฐานขั้นต่ำร่วมกัน

หน่วยงานสำคัญต้องมีมาตรการและซ้อมรับมือ

27 พ.ค. 2562 — ประกาศใช้ (วันเดียวกับ PDPA)

2564 — ประมวลแนวทางปฏิบัติ + มาตรฐานขั้นต่ำ

2565 — มาตรฐานขั้นต่ำมีผลใช้

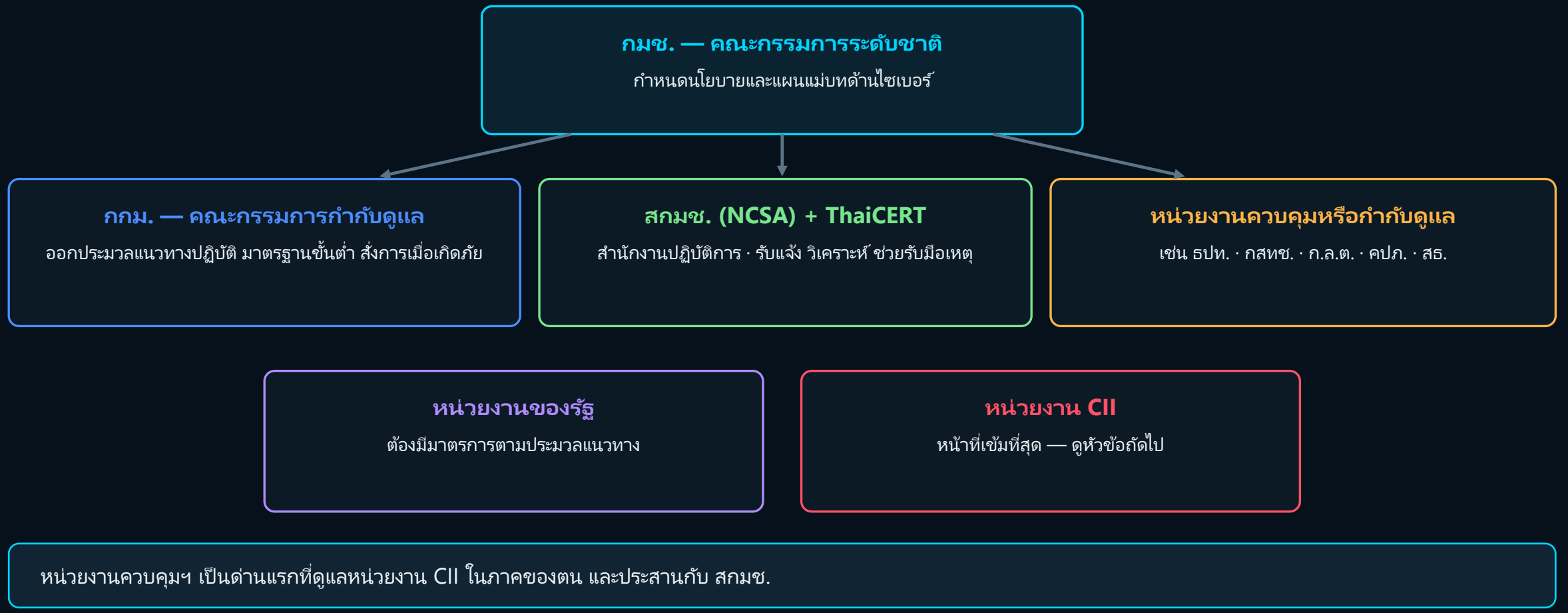
10 ก.ย. 2569 — มาตรฐานความปลอดภัยคลาวด์มีผล

2568–2569 — ร่างแก้ไข พ.ร.บ. รับฟังความเห็น

แยกให้ออก: พ.ร.บ.ไซเบอร์ ดูแล "ระบบ" จากภัยคุกคาม · PDPA ดูแล "ข้อมูลส่วนบุคคล" · พ.ร.บ.คอมพิวเตอร์ เอาผิด "ผู้กระทำ"

R0Cyber

โครงสร้างหน่วยงานตาม พ.ร.บ.ไซเบอร์



R0Cyber

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

- ความมั่นคงของรัฐ
- บริการภาครัฐที่สำคัญ
- การเงินการธนาคาร
- ไอทีและโทรคมนาคม
- ขนส่งและโลจิสติกส์
- พลังงานและสาธารณูปโภค
- สาธารณสุข
- ด้านอื่นที่ ครม. ประกาศ

เกณฑ์: ภารกิจหรือบริการที่ถ้าถูกโจมตีหรือหยุดชะงัก จะกระทบความมั่นคง เศรษฐกิจ สาธารณสุข หรือความสงบเรียบร้อยของประเทศ

ไม่ใช่ทุกองค์กรในภาคเหล่านี้เป็น CII — ต้องดูประกาศของ กกม. และหน่วยงานควบคุมฯ ที่ระบุรายชื่อ

R0Cyber

หน้าที่ของหน่วยงาน CII

ปฏิบัติตามมาตรฐานขั้นต่ำ	ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานที่ กกม. ประกาศ (2564)
แจ้งผู้ประสานงาน	รายชื่อผู้บริหารและผู้ปฏิบัติงานด้านไซเบอร์ เพื่อการติดต่อเมื่อเกิดเหตุ
ประเมินความเสี่ยง + ตรวจสอบ	โดยผู้ตรวจประเมิน/ผู้ตรวจสอบภายในหรือภายนอก อย่างน้อยปีละครั้ง
ซ้อมและทดสอบความพร้อม	มีแผนรับมือ และเข้าร่วมการทดสอบที่ สกมช. หรือหน่วยงานควบคุมจัด
แจ้งเหตุภัยคุกคาม	แจ้ง สกมช. และหน่วยงานควบคุมฯ เมื่อเกิดภัยคุกคามที่มีนัยสำคัญ และร่วมรับมือ

ไม่ปฏิบัติตาม: หน่วยงานควบคุมฯ และ กกม. สั่งให้แก้ไขได้ และมีบทลงโทษตามกฎหมาย — อ่านตัวบทและประกาศฉบับล่าสุดของภาคตนเสมอ

R0Cyber

มาตรฐานขั้นต่ำ: ครบวงจร 5 ด้าน

ระบุ
Identify
ทรัพย์สิน · ความเสี่ยง · ผู้รับผิดชอบ

→

ป้องกัน
Protect
สิทธิ์ · แพตช์ · สำรอง · อบรม

→

ตรวจจับ
Detect
log · เฝ้าระวัง · แจ้งเตือน

→

ตอบสนอง
Respond
แผนรับมือ · แจ้งเหตุ · ประสานงาน

→

กู้คืน
Recover
BCP/DR · บทเรียน · ปรับปรุง

สอดคล้องสากล: โครงเดียวกับ NIST Cybersecurity Framework — องค์กรที่ทำ ISO 27001 อยู่แล้ว ต่อยอดได้ง่าย

มาตรฐานความปลอดภัยคลาวด์ (มีผล 10 ก.ย. 2569) ใช้กับหน่วยงานรัฐ CII และผู้ให้บริการคลาวด์ที่ให้บริการหน่วยงานเหล่านี้

R0Cyber

ภัยคุกคามไซเบอร์ 3 ระดับ

ระดับ	ลักษณะ	การดำเนินการ
ไม่ร้ายแรง	ระบบคอมพิวเตอร์สำคัญมีประสิทธิภาพลดลง	หน่วยงานรับมือเอง ร่วมกับหน่วยงานควบคุมฯ
ร้ายแรง	ระบบ CII ถูกโจมตีจนเสียหายหรือให้บริการไม่ได้	กกม. สั่งการได้มากขึ้น · การเข้าถึงระบบบางอย่างต้องขอศาล
วิกฤติ	กระทบวงกว้าง ชีวิตประชาชน หรือความมั่นคงของประเทศ	สภาความมั่นคงแห่งชาติเข้ามาดำเนินการ

หลักคิด: ยิ่งร้ายแรง อำนาจรัฐยิ่งมาก — องค์กรต้องรู้ล่วงหน้าว่าจะถูกขอข้อมูล ขอเข้าตรวจ หรือสั่งแก้ไขอะไรได้บ้าง

ร่างแก้ไขปี 2568–2569 เสนอเกณฑ์จัดระดับเหตุและกรอบเวลารายงานที่ชัดขึ้น — ติดตามประกาศฉบับใหม่

R0Cyber

องค์กรที่ไม่ใช่ CII เกี่ยวข้องอย่างไร

เป็นผู้ให้บริการของ CII

คลาวด์ · ซอฟต์แวร์ · ดูแลระบบ — ถูกกำหนดมาตรฐานผ่านสัญญาและการตรวจสอบ

อาจถูกขอข้อมูลเมื่อเกิดเหตุ

หน่วยงานรัฐขอข้อมูลเพื่อวิเคราะห์ภัยคุกคามได้ ต้องเตรียม log และผู้ประสาน

ขอความช่วยเหลือได้

แจ้งและขอคำแนะนำจาก ThaiCERT / สกมช. ได้แม้ไม่ใช่ CII

กฎหมายอื่นยังบังคับ

PDPA · พ.ร.บ.คอมพิวเตอร์ · เกณฑ์ของหน่วยงานกำกับในธุรกิจตน

แนวโน้ม: ร่างแก้ไขเสนอให้ CII ต้องกำกับผู้ให้บริการภายนอก และขยายไปยังผู้ให้บริการคลาวด์และดาต้าเซ็นเตอร์ — ห่วงโซ่อุปทานคือความเสี่ยงร่วม

R0Cyber

สิ่งที่องค์กรควรทำตอนนี้

1. ตรวจสถานะ	เราเป็นหน่วยงานรัฐ CII หรือผู้ให้บริการของ CII หรือไม่ · หน่วยงานควบคุมของเราคือใคร
2. Gap assessment	เทียบมาตรการปัจจุบันกับมาตรฐานขั้นต่ำ 5 ด้าน
3. ผู้ประสานงานและช่องทาง	รายชื่อ เบอร์ติดต่อนอกเวลา · ช่องทางแจ้ง สกมช./ThaiCERT
4. แผนรับมือ + ซ้อม	อย่างน้อยปีละครั้ง · รวมผู้ให้บริการภายนอก
5. ติดตามกฎหมาย	ร่างแก้ไข พ.ร.บ. · ประกาศ กกม. · มาตรฐานคลาวด์

ขั้นที่ 3–4 จะลงรายละเอียดในตอนที่ 3 (นโยบายและการรายงานเหตุ) และฝึกจริงใน Workshop ตอนที่ 4

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. พ.ร.บ.ไซเบอร์ เน้นปกป้องระบบจากภัยคุกคาม	✓ จริง	ส่วนข้อมูลบุคคลคือ PDPA
2. ทุกบริษัทในภาคการเงินเป็น CII อัตโนมัติ	✗ ไม่จริง	ดูประกาศรายชื่อ
3. หน่วยงาน CII ต้องประเมินความเสี่ยงอย่างน้อยปีละครั้ง	✓ จริง	โดยผู้ตรวจประเมิน
4. ภัยคุกคามระดับวิกฤติ อยู่ในอำนาจสภาความมั่นคงแห่งชาติ	✓ จริง	ระดับสูงสุด

SUMMARY · ตอนที่ 1

สรุป: พ.ร.บ.ไซเบอร์ 2562

- ✓ ปกป้องระบบและบริการสำคัญของประเทศ
- ✓ กมช. · กกม. · สกมช. · หน่วยงานควบคุมฯ
- ✓ CII: มาตรฐานขั้นต่ำ · ประเมินปีละครั้ง · ซ้อม · แจ้งเหตุ
- ✓ ภัยคุกคาม 3 ระดับ: ไม่ร้ายแรง · ร้ายแรง · วิกฤติ
- ✓ องค์กรทั่วไปเกี่ยวข้องผ่านห่วงโซ่อุปทาน

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

ตอนถัดไป

ตอนที่ 2

พ.ร.บ.คอมพิวเตอร์ และขอบเขตทางกฎหมาย

- ความผิด ม.5–14
- log 90 วัน (ม.26)
- งานไซเบอร์ที่ถูกกฎหมาย
- เก็บหลักฐานและแจ้งความ