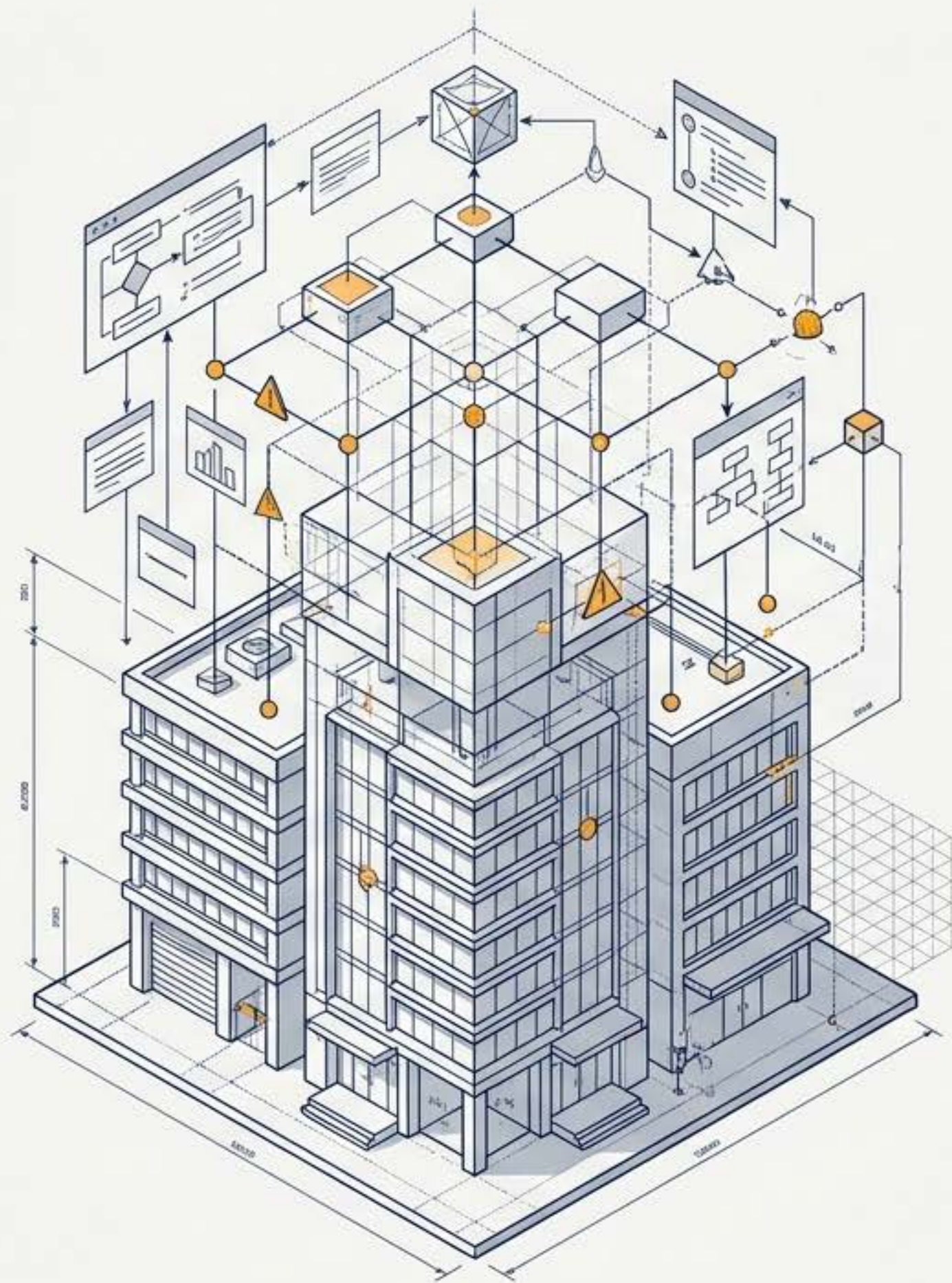




บทที่ 1 บทนำสู่การจัดการ ความมั่นคงปลอดภัย

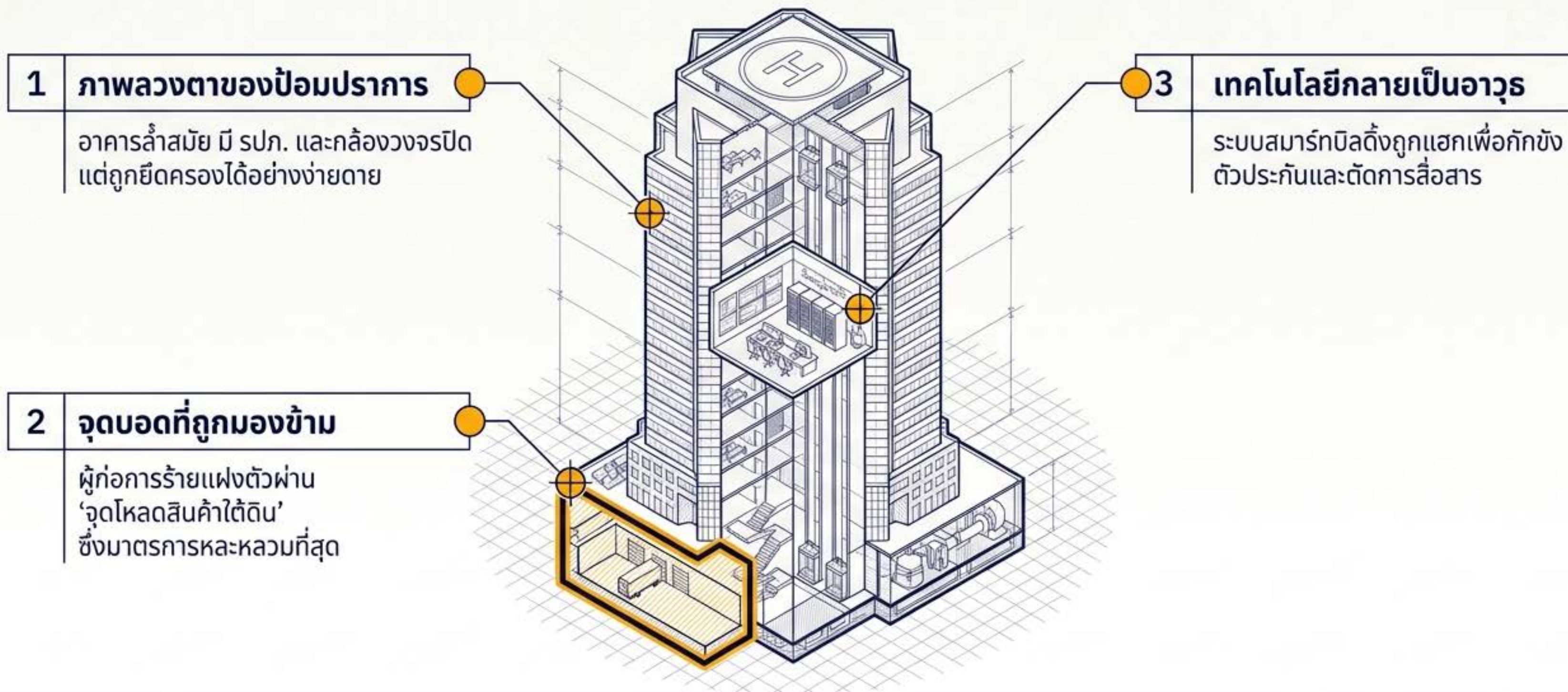
(Introduction to Security Management)

จากผู้เฝ้าระวัง สู่สถาปนิกผู้บริหารความเสี่ยง

- เรียนรู้ความล้มเหลวเชิงระบบและภาพลองตาแห่งความปลอดภัย
- ทำความเข้าใจระบบนิเวศความมั่นคงและวิวัฒนาการของวิชาชีพ
- เจาะลึกบริบทความมั่นคงปลอดภัยในสังคมและวัฒนธรรมไทย

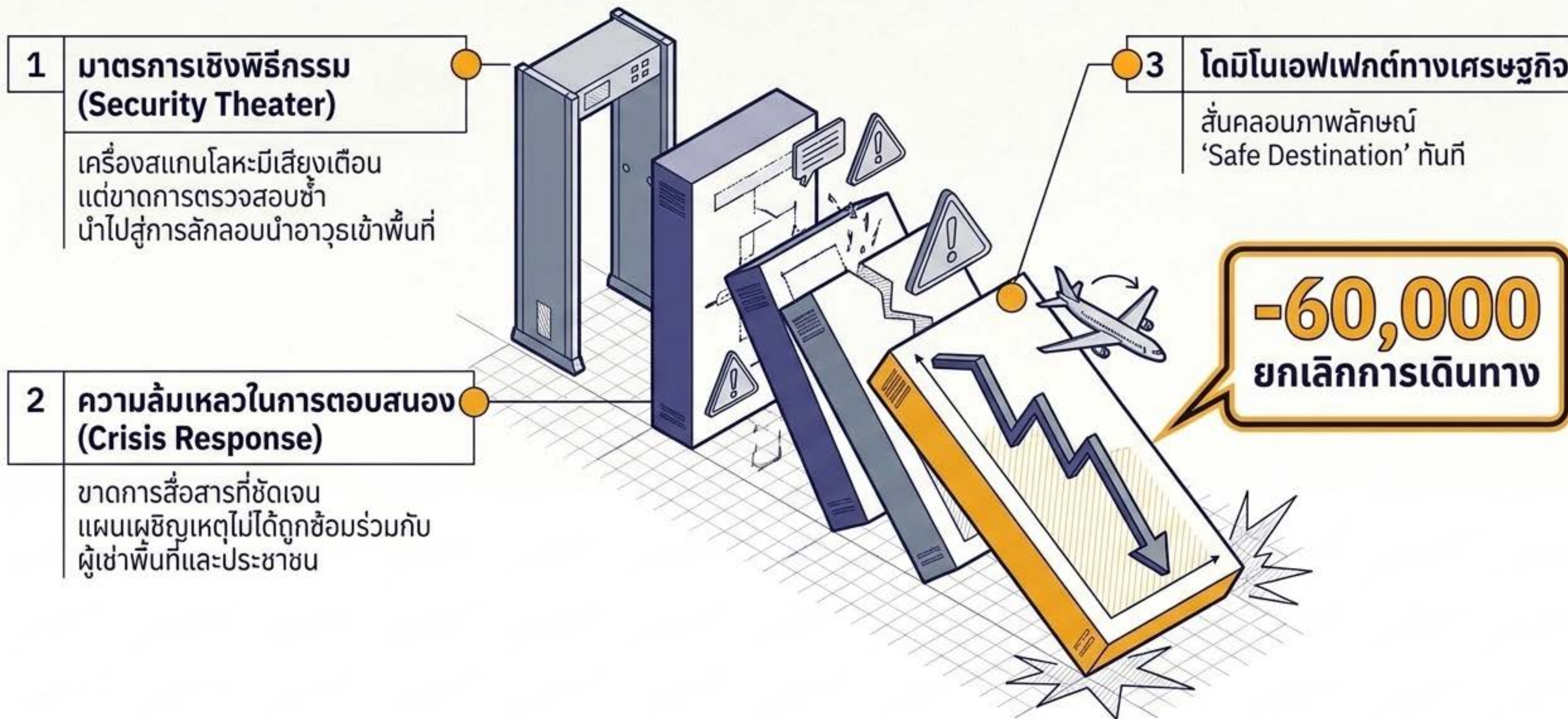
ผู้บรรยาย: พศ.ดร.กัณฑ์พันธ์์ สุนทรพิพิธ

ความล้มเหลวเชิงระบบ: บทเรียนจากนาฬิกาโตมิ พลาซ่า (Die Hard 1988)



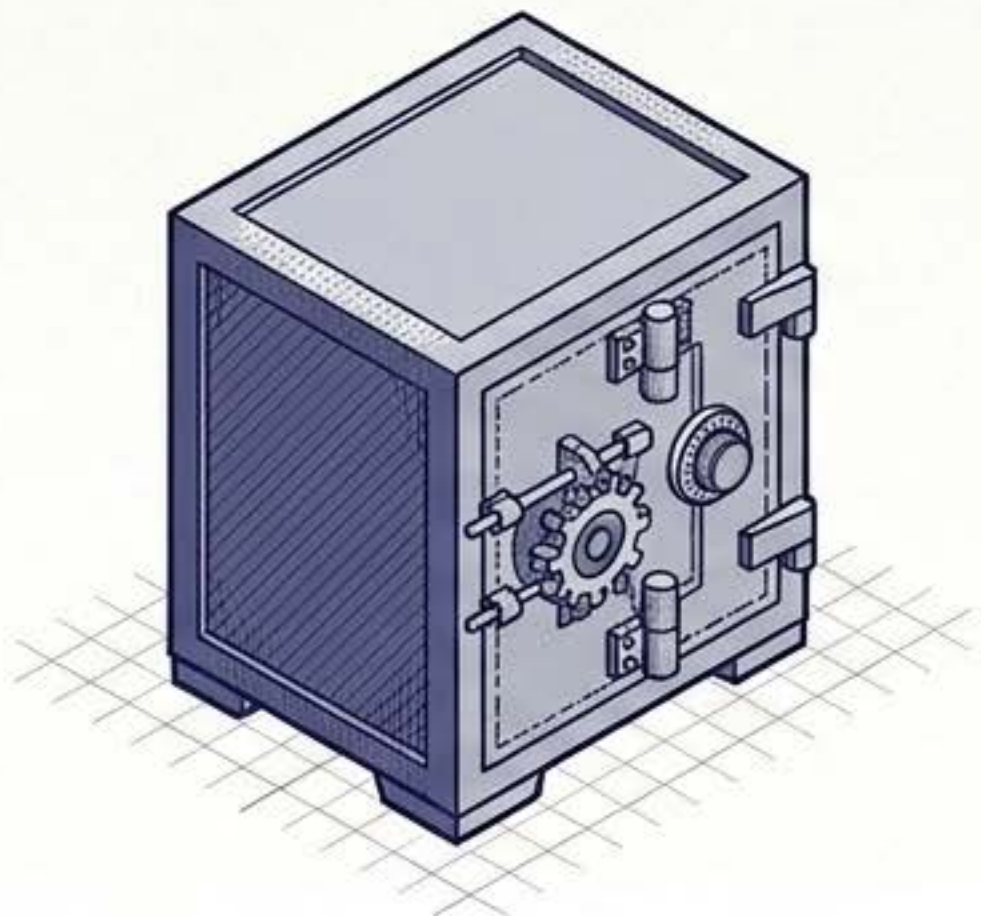
บทเรียนสำคัญ: Security is a process, not a product. (ความมั่นคงคือกระบวนการ ไม่ใช่แค่ตัวผลิตภัณฑ์)

จากนาคาโตมิ สู่สยามพารากอน (2023): ผลกระทบระดับมหภาค



ภัยคุกคามยุคดิจิทัล: กรณีศึกษาแฮกเกอร์ 9Near

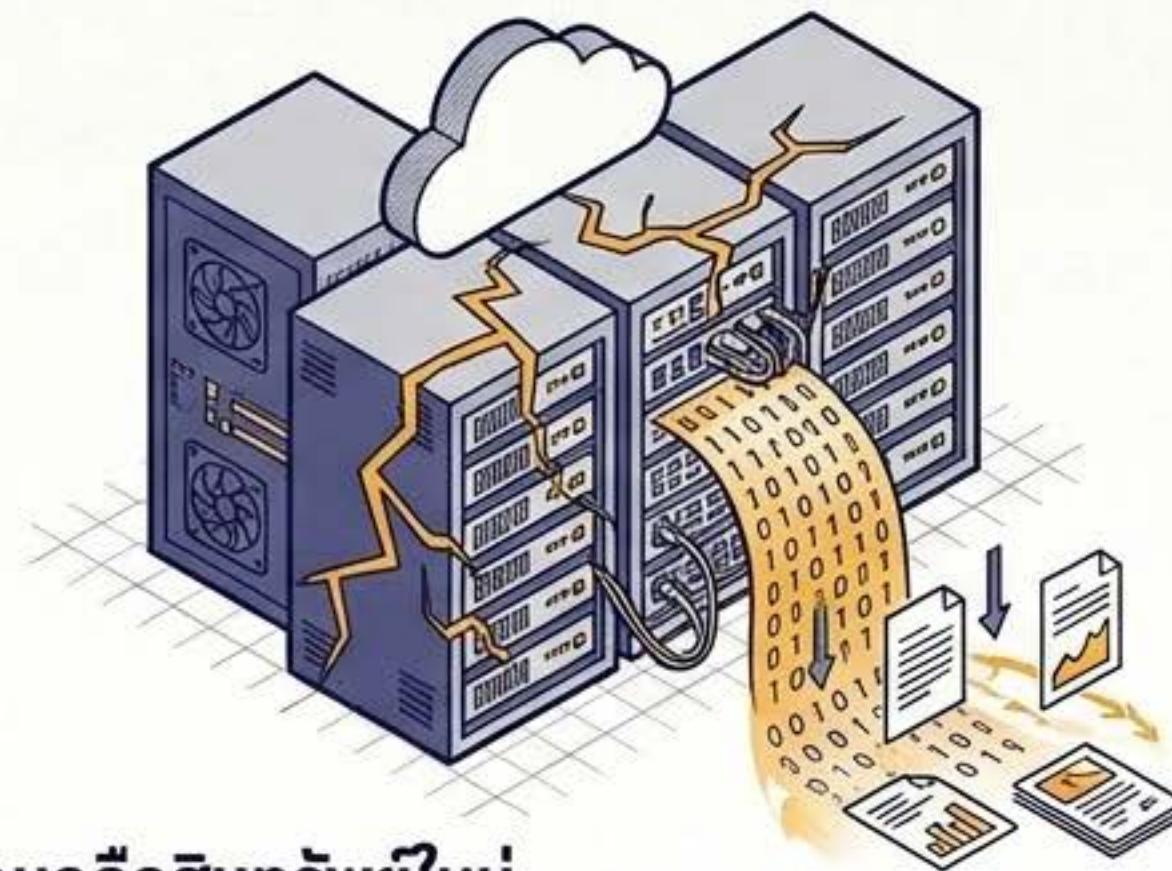
การปล้นในอดีต



ต้องใช้ระเบิด อาวุธ หรือการเดินทางมาสถานที่จริงเพื่อโจรกรรมสินทรัพย์ทางกายภาพ

ผลกระทบ: ชื่อ, เลขบัตร ปชช., เบอร์โทร ถูกนำไปใช้หลอกลวง (Scam) และสวมรอย (Identity Theft)

การปล้นที่ไร้ร่องรอย



ข้อมูลคือสินทรัพย์ใหม่
ข้อมูลคนไทย 55 ล้านรายชื่อรั่วไหลผ่านช่องโหว่การบริหารจัดการ (Data Governance) ของหน่วยงาน

สถิติวิกฤต: ไทยเผชิญการโจมตีไซเบอร์สูงกว่าค่าเฉลี่ยโลกถึง 70% (2024-2025)

นิยามทวิลักษณ์: ความต่างของ Safety และ Security



ความมั่นคงเชิงวัตถุวิสัย vs จิตวิสัย และอันตรายของ Security Theater



Objective Security (เชิงวัตถุวิสัย)

วัดผลได้จริง กายภาพจับต้องได้
(ความหนาของประตู, กล้อง 4K, มาตรฐานเข้ารหัสข้อมูล)

Subjective Security (เชิงจิตวิสัย)

ความรู้สึกปลอดภัยของผู้คน
ซึ่งอาจไม่ตรงกับความเป็นจริง

อันตรายของ Security Theater

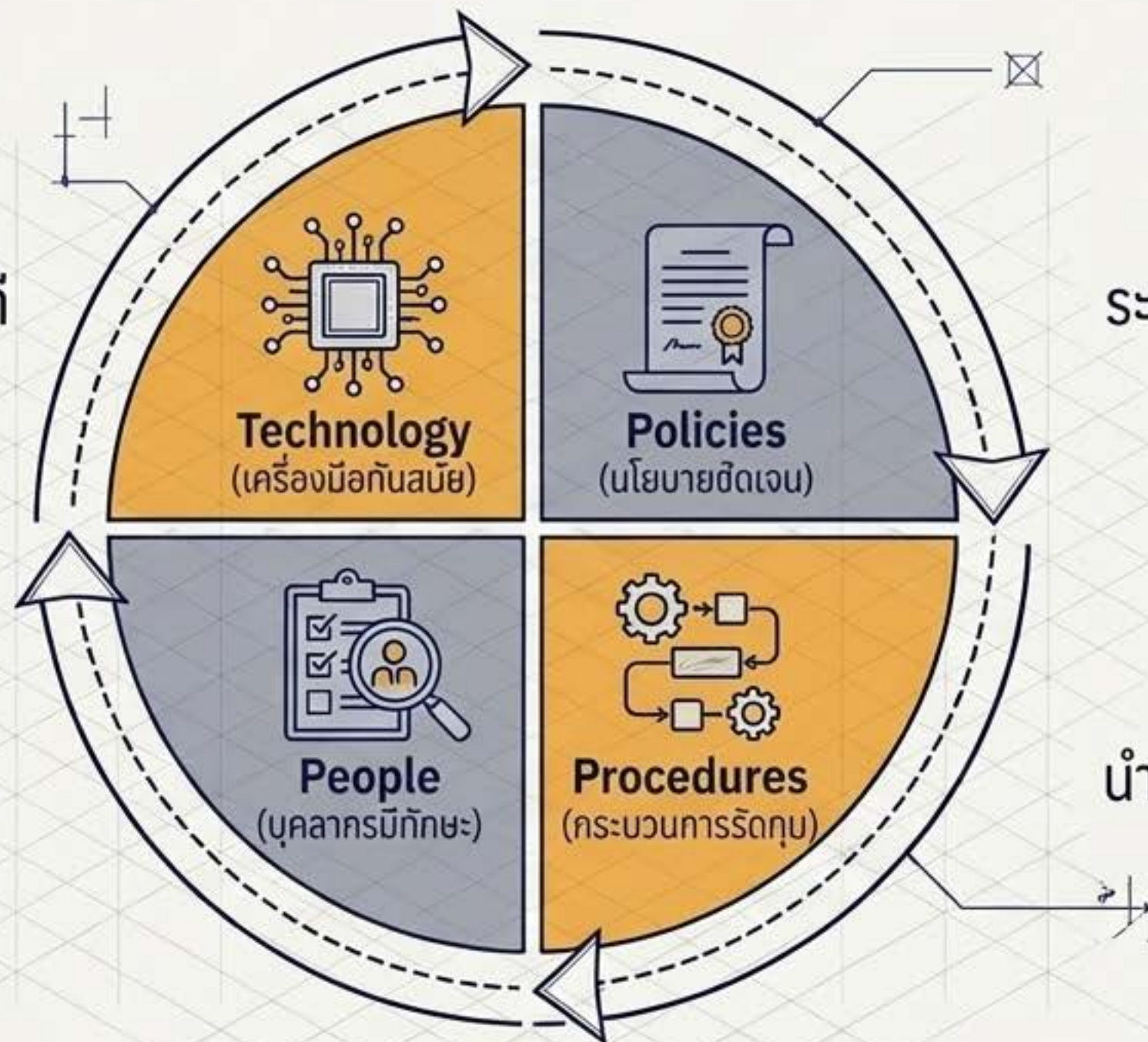
เน้นสร้างความรู้สึก แต่ไม่ป้องกันภัยจริง

ตัวอย่างในไทย: รปภ. ยืนตะเบ๊ะรถทุกคันหน้าหมู่บ้าน
แต่ไม่เคยขอแลกบัตรหรือตรวจสอบท้ายรถ

ศาสตร์แห่งการบริหารจัดการ: 4Ps และวงจร PDCA

ACT
ปรับปรุงและอุดช่องโหว่ทันที

CHECK
ตรวจสอบ (Audit),
ซ้อมแผน, ทำ Pen-Test

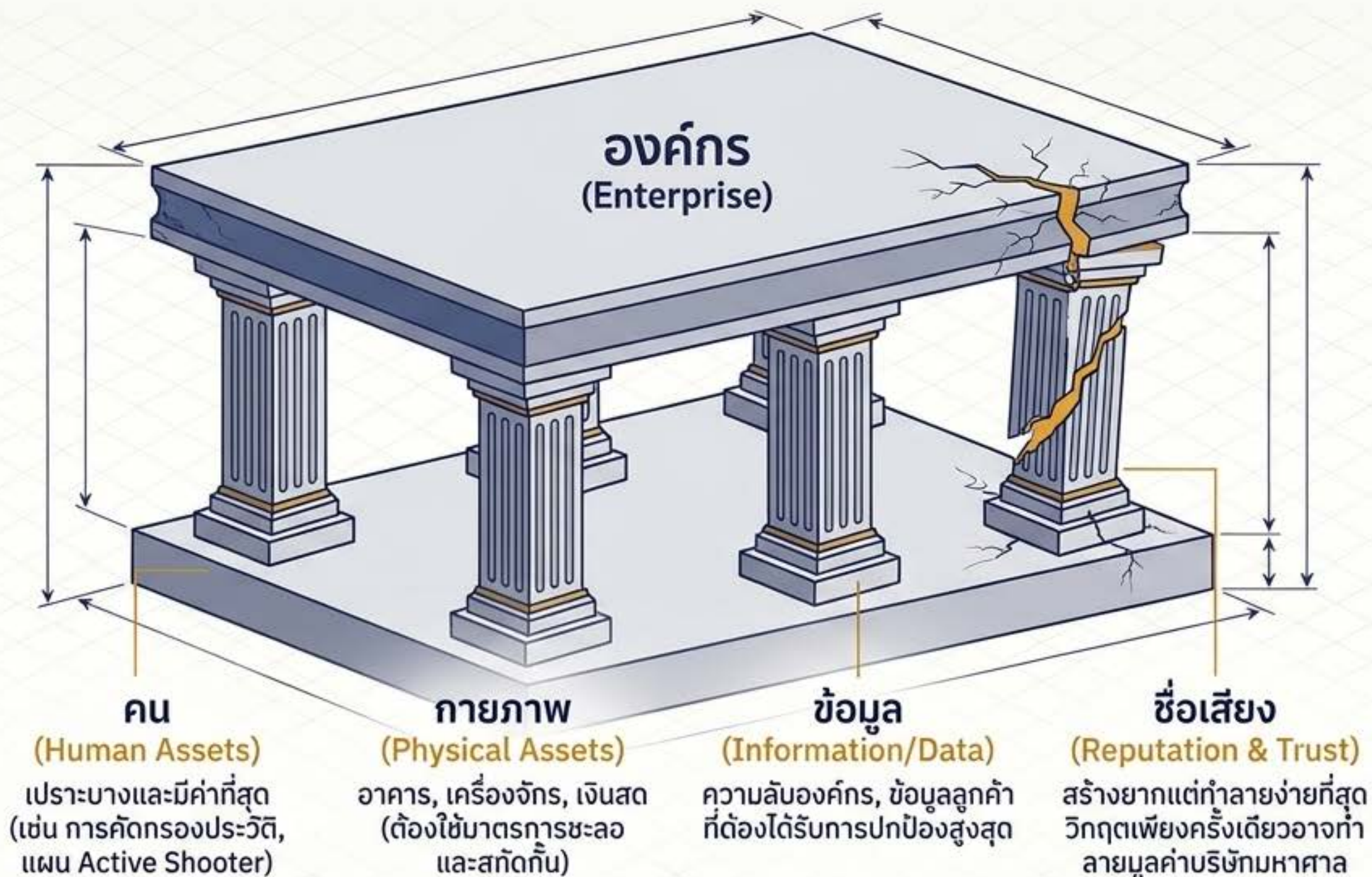


PLAN
ระบุสินทรัพย์และประเมิน
ความเสี่ยง

DO
นำมาตรการไปปฏิบัติจริง

การจัดการความมั่นคงปลอดภัย คือระบบนิเวศน์ที่หมุนเวียนเพื่อการพัฒนาอย่างไม่หยุดนิ่ง
ไม่ใช่แค่การซื้อเครื่องมือ

ระบบนิเวศความมั่นคงปลอดภัย (The Security Ecosystem)



วัตถุประสงค์หลักของการจัดการความมั่นคงปลอดภัย



Risk Meter Dashboard

เป้าหมายไม่ใช่ 'ความเสี่ยงเป็นศูนย์' (Zero Risk)
แต่เป็นการบริหารให้อยู่ในระดับที่ยอมรับได้



1. ป้องกันความสูญเสีย (Loss Prevention)

สกัดกั้นอาชญากรรมและอุบัติเหตุ



3. การปฏิบัติตามกฎหมาย (Compliance)

ป้องกันการถูกฟ้องร้อง (PDPA, กฎหมายแรงงาน)



2. ความต่อเนื่องทางธุรกิจ (Business Continuity)

องค์กรต้องฟื้นตัวเร็วเมื่อเกิดวิกฤต
(เช่น มหาอุทกภัยปี 2011)



4. สร้างความเชื่อมั่น (Confidence Building)

ให้กับพนักงาน ผู้ถือหุ้น และสังคม

ความมั่นคงสารสนเทศกับกฎแห่ง CIA Triad



1 Confidentiality (ความลับ)

เข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น (ป้องกันข้อมูลรั่วไหล)

2 Integrity (ความถูกต้องครบถ้วน)

ข้อมูลต้องไม่ถูกดัดแปลง (ป้องกันแฮกเกอร์แก้ไขตัวเลข)

3 Availability (ความพร้อมใช้)

ระบบใช้งานได้เสมอเมื่อต้องการ (ป้องกันระบบล่ม/DDoS)

บริบทไทยกับความอยู่รอดทางกฎหมาย: ความล้มเหลวของ CIA Triad นำไปสู่บทลงโทษรุนแรง
(กรณีศึกษา: บริษัท JIB ถูกปรับ 7 ล้านบาท ฐานมาตรการหละหลวม)

วิวัฒนาการวิชาชีพความมั่นคงโลก: จากเผ่ายามสู่ผู้จัดการความเสี่ยง

ยุคเริ่มต้น (Ancient/Medieval)

ยามเฝ้าระวัง
ใช้กำลังกายและความ
กล้าหาญ



ยุคอุตสาหกรรม (18th-19th C.)

บริษัท สปก. เอกชนแรก
(Pinkerton) คุ่มกันเส้น
ทางรถไฟและโรงงาน



ยุคการจัดการ (20th C.)

เกิดองค์กร ASIS และ
มาตรฐานวิชาชีพ (CPP)
มองความปลอดภัยเป็น
กลยุทธ์ธุรกิจ



ยุคหลัง 9/11 (21st C.)

จุดเปลี่ยนสู่ยุค Risk
Management
บูรณาการต่อต้านก่อการ
ร้ายและภัยไซเบอร์



วิวัฒนาการวิชาชีพในไทย: การปรับตัวสู่มาตรฐานสากล

อดีต: ยุคเฝ้ายามแบบดั้งเดิม
(ก่อน 2520)



- **จ้างคนรู้จัก** หรือแรงงานสูงอายุ
- **ขาดมาตรฐาน**
- เครื่องมือมีเพียงไฟฉายและกระบอง

ยุคกลาง: ยุคอุตสาหกรรม
(2520-2550)



- บริษัทข้ามชาติเข้าตั้งฐานทัพ (Eastern Seaboard)
- เกิดบริษัท **สปก. สากล** นำระบบตะวันตกมาใช้
- ตลาดล่างยังเน้น **ตัดราคา**

ปัจจุบัน: จุดเปลี่ยนผ่าน
(2558 - ปัจจุบัน)

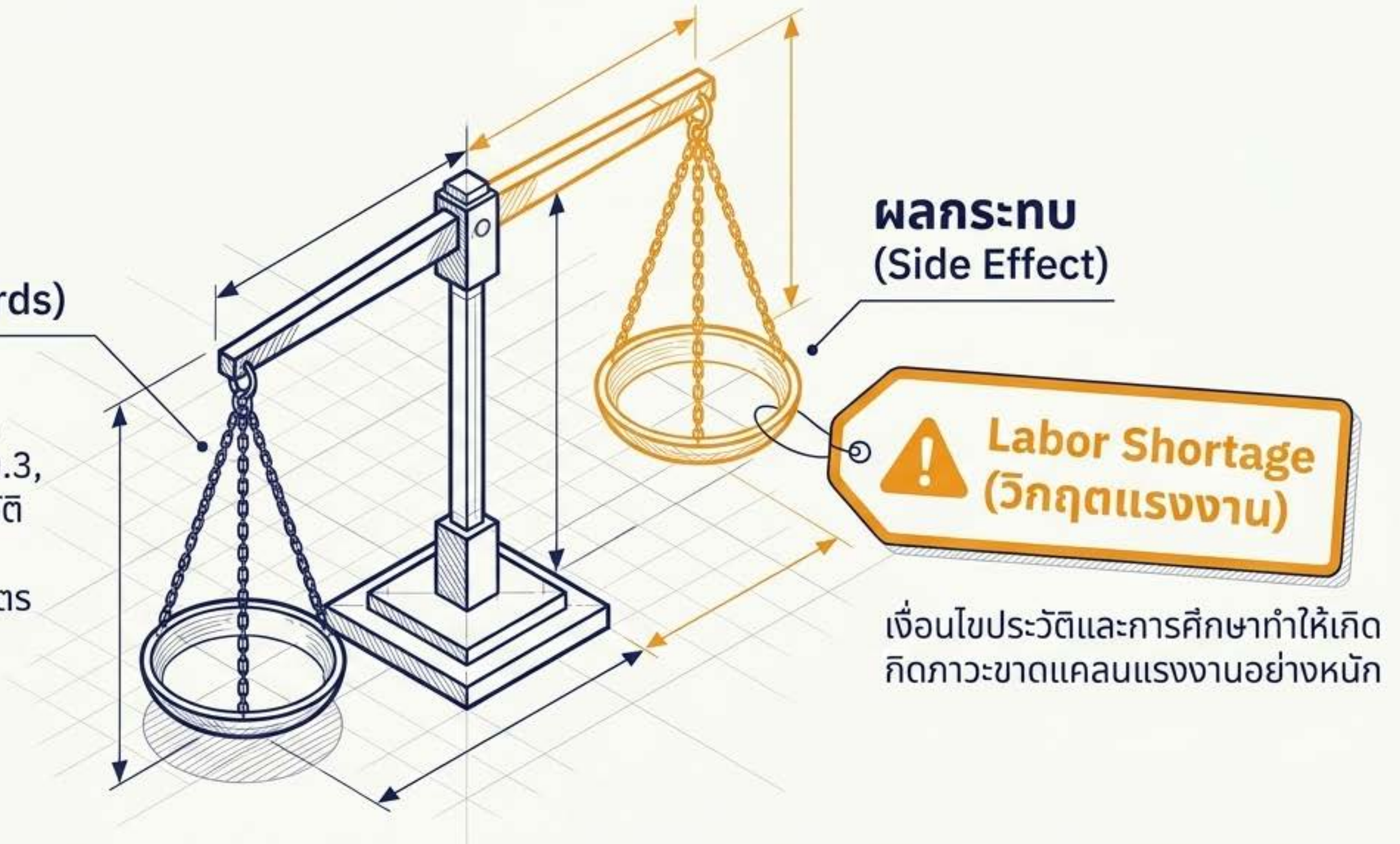


- **กฎหมาย** เข้ามาจัดระเบียบวิชาชีพ
- ยกระดับคุณภาพสู่ยุค **Hybrid Security**
- เผชิญปัญหา **ขาดแคลนแรงงาน**

พ.ร.บ. รุรกิจรักษาความปลอดภัย 2558: จุดเปลี่ยนสำคัญ

มาตรฐานวิชาชีพ (Professional Standards)

- **ระดับบริษัท:**
ต้องรับใบอนุญาตจาก สตช.
- **ระดับพนักงาน:** วุฒิขั้นต่ำ ม.3,
ต้องผ่านการตรวจสอบประวัติ
อาชญากรรม
- **การฝึกอบรม:** บังคับหลักสูตร
มาตรฐาน 40 ชั่วโมง



การจัดระเบียบครั้งใหญ่ (Regulatory Overhaul): ยกระดับ 'รปภ.' สู่ 'วิชาชีพ' ที่ควบคุมโดยกฎหมาย

ขอบเขตอำนาจ: ตำรวจ vs ความมั่นคงปลอดภัยเอกชน (สปก.)

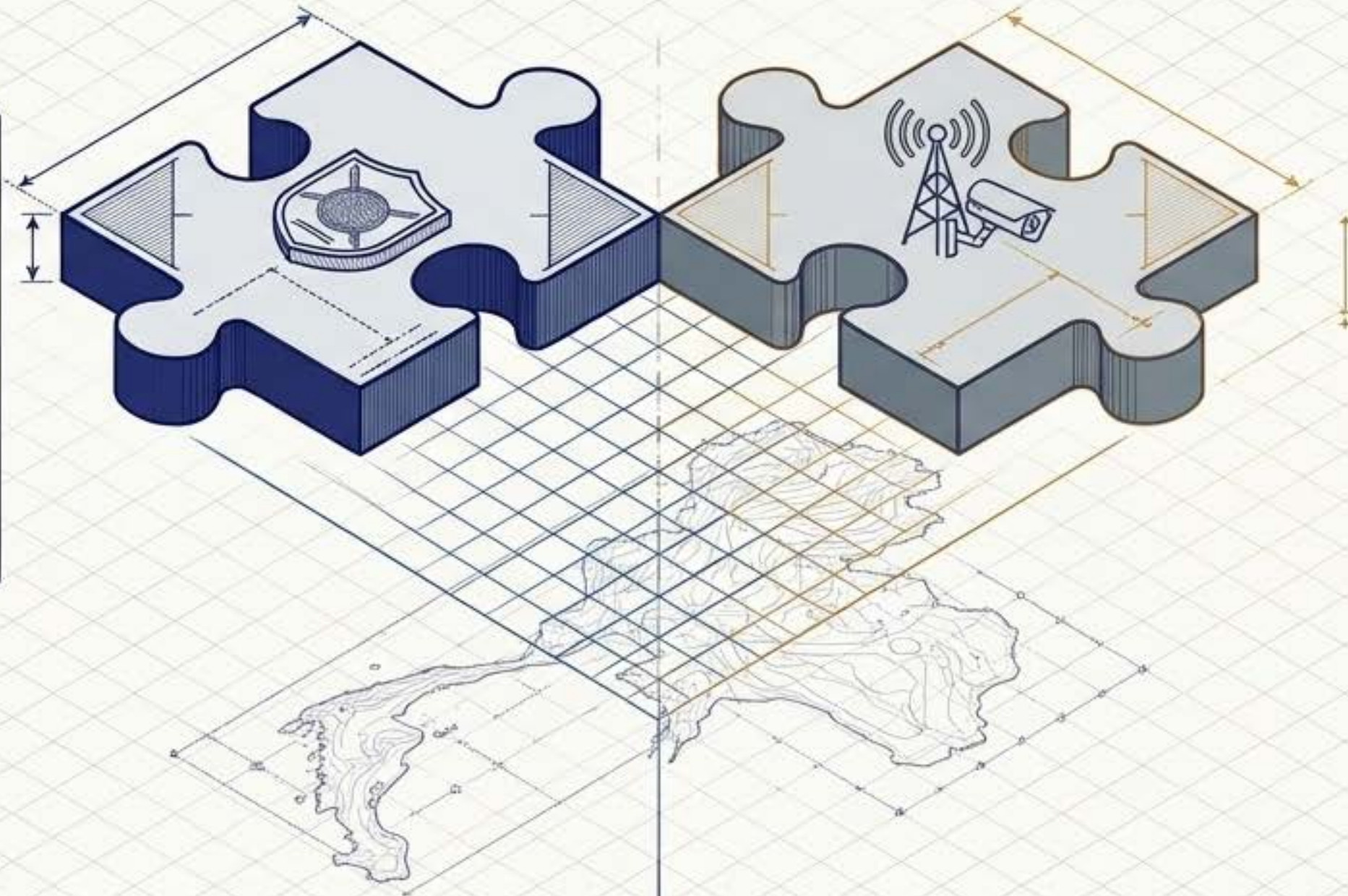
ประเด็น (Domain)	 ตำรวจ (Public Security)	 สปก. (Private Security)
พันธกิจหลัก	ดูแลความสงบเรียบร้อยส่วนรวม	ป้องกันความสูญเสียให้ผู้ว่าจ้าง
การจับกุม	มีอำนาจสืบสวน สอบสวน จับกุม ☒	จับได้เฉพาะ 'ความผิดซึ่งหน้า' (Citizen's Arrest) ☐
การค้นตัว/สัมภาระ	มีอำนาจค้นตามกฎหมาย ☒	อาศัยหลัก 'เงื่อนไขการเข้าพื้นที่' (Condition of Entry) ไม่มีสิทธิค้นโดยพลการ ☐
อาวุธ	พกพาปืนได้ตามหน้าที่ราชการ ☒	ห้ามพกพาปืน (ยกเว้นหน่วยพิเศษเช่น รถชนเงิน) ☐

สปก. เอกชน **ไม่มีอำนาจ**ตามกฎหมายมากกว่า **พลเมือง**ดีทั่วไป

ความร่วมมือรัฐและเอกชน (Public-Private Partnerships - PPP)

Smart Safety Zone 4.0

- เชื่อมต่อกล้อง CCTV เอกชน (โรงแรม, 7-11) เข้าศูนย์บัญชาการตำรวจ
- ใช้ AI วิเคราะห์ความเสี่ยง ช่วยลดดัชนีความหวาดกลัวภัย (Fear of Crime)

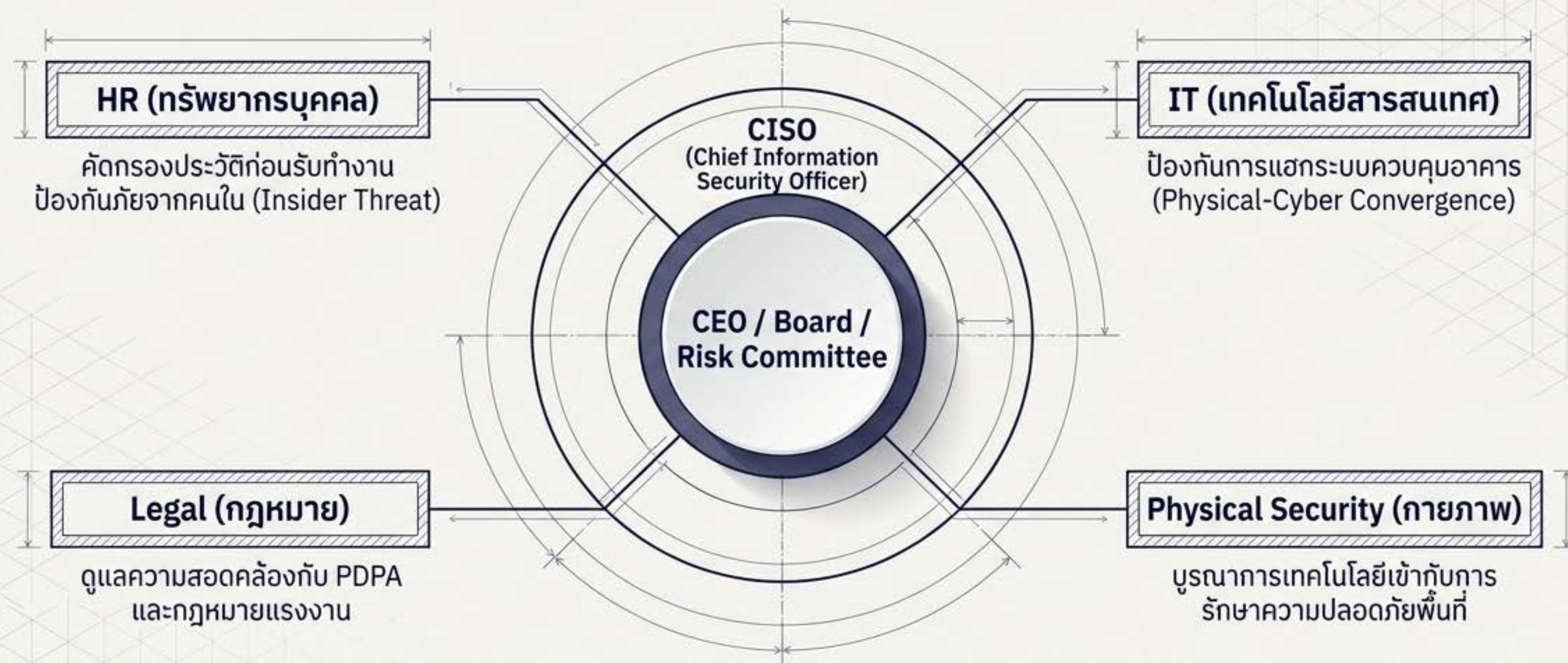


Cyber Vaccine

- เอกชน (ธนาคาร, ผู้ให้บริการเครือข่าย) ส่ง SMS แจ้งเตือน และระงับบัญชีม้า
- ตำรวจรับหน้าที่บังคับใช้กฎหมายและปราบปรามเครือข่าย

รัฐและตำรวจไม่สามารถดูแลได้ครอบคลุม การบูรณาการร่วมกับเอกชนคือทางออกระดับชาติ

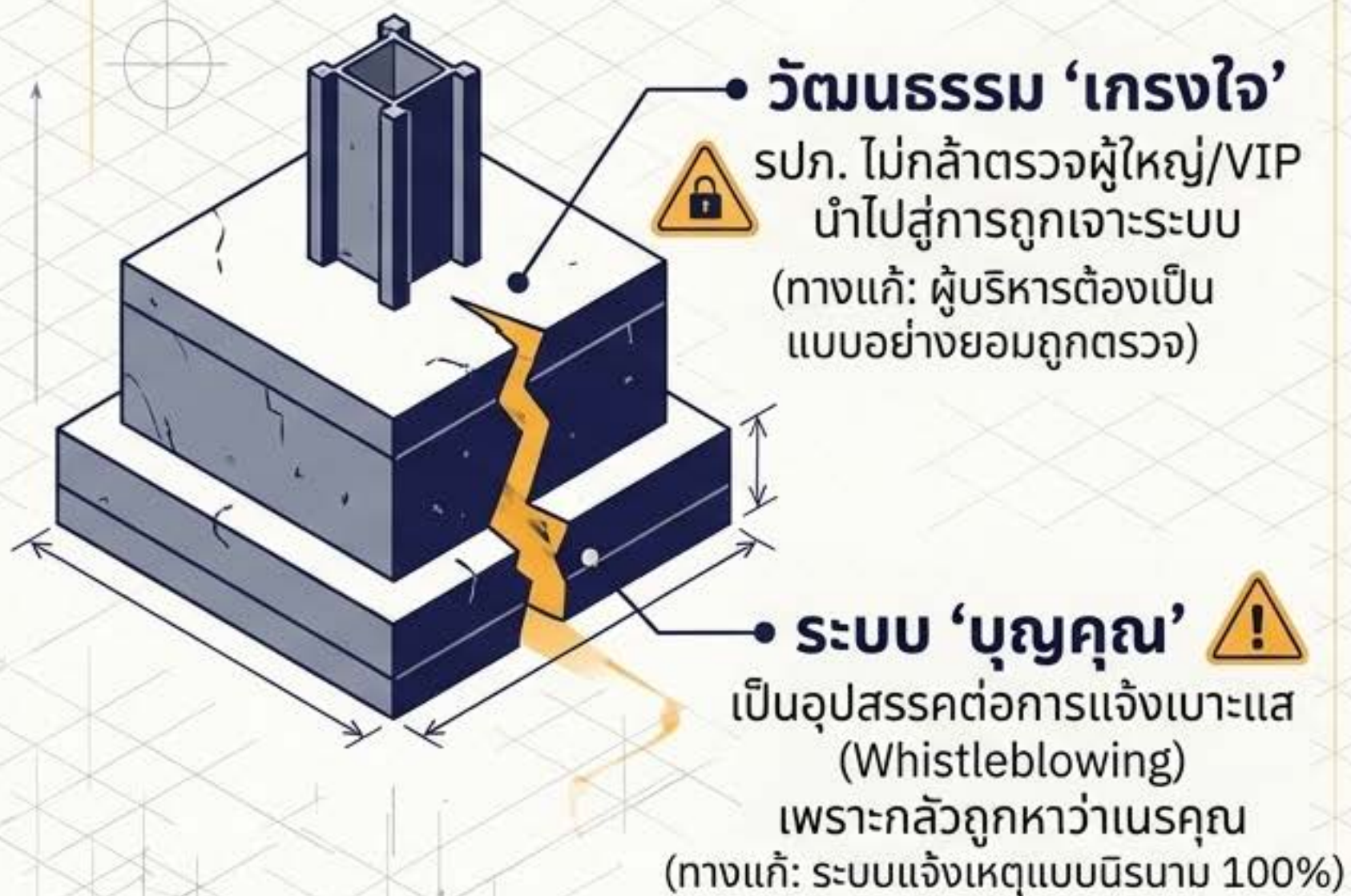
การจัดการความมั่นคงในองค์กรสมัยใหม่และบทบาท CISO



ความมั่นคงไม่ใช่แผนกที่แยกตัวโดดเดี่ยว (Silo) แต่ต้องบูรณาการข้ามสายงาน (Cross-Functional) และรายงานตรงต่อระดับบริหารเพื่อกำหนดกลยุทธ์สูงสุด

บริบทวัฒนธรรมไทย: ช่องโหว่และจุดแข็งที่ซ่อนอยู่

ช่องโหว่ทางวัฒนธรรม (Vulnerabilities)



จุดแข็งที่ตะวันตกไม่มี (Strengths)



การประยุกต์ทฤษฎีอาชญาวิทยากับสถานการณ์ไทย

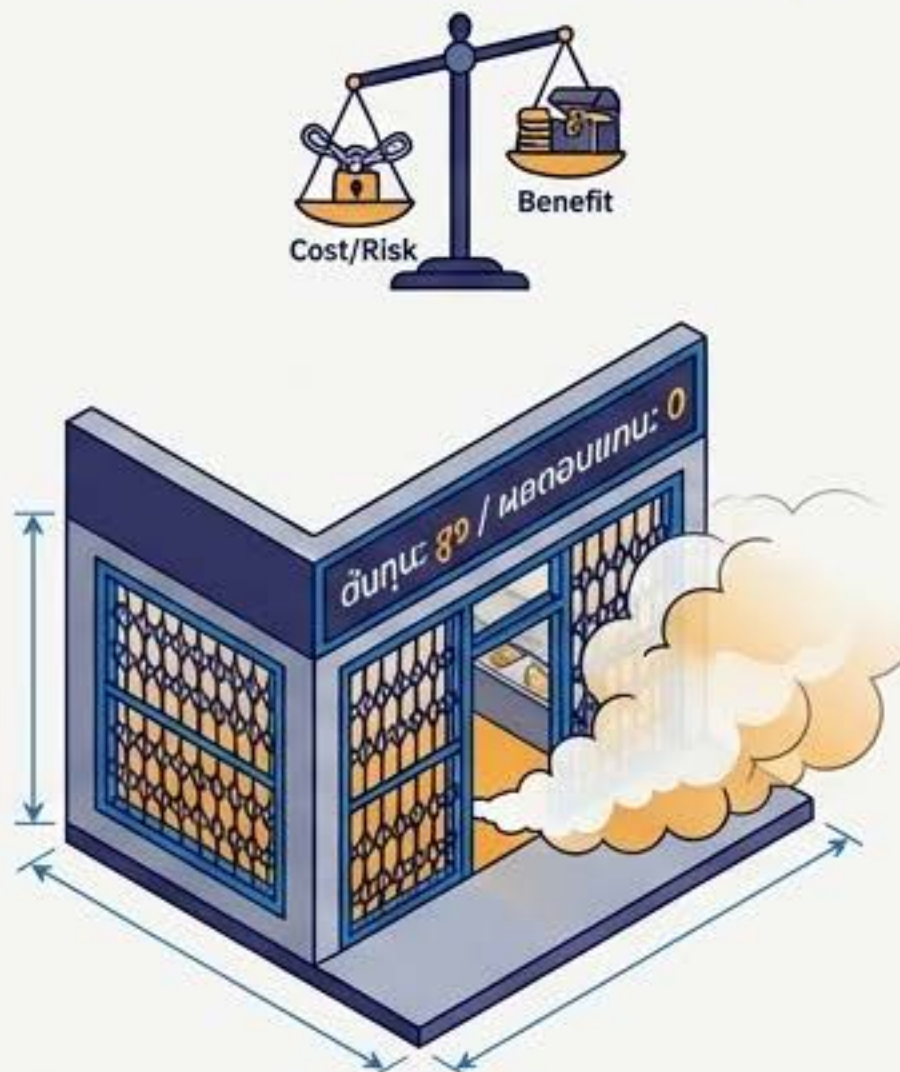
Routine Activity Theory (RAT)



อาชญากรรมเกิดเมื่อ:
คนร้าย + เป้าหมาย + ขาดผู้ดูแล

การประยุกต์: เสา SOS และกล้อง AI
ใน Smart Safety Zone
ทำหน้าที่เป็น 'ผู้ดูแล' แทนตำรวจ

Rational Choice Theory



อาชญากรคำนวณ:
ต้นทุน/ความเสี่ยง vs ผลตอบแทน

การประยุกต์: ร้านทองติดลูกกรง 2 ชั้น
และ Fog Cannon พ่นควันทึบ
เพื่อให้โจรคำนวณว่า 'ทำไปก็ไม่คุ้ม'

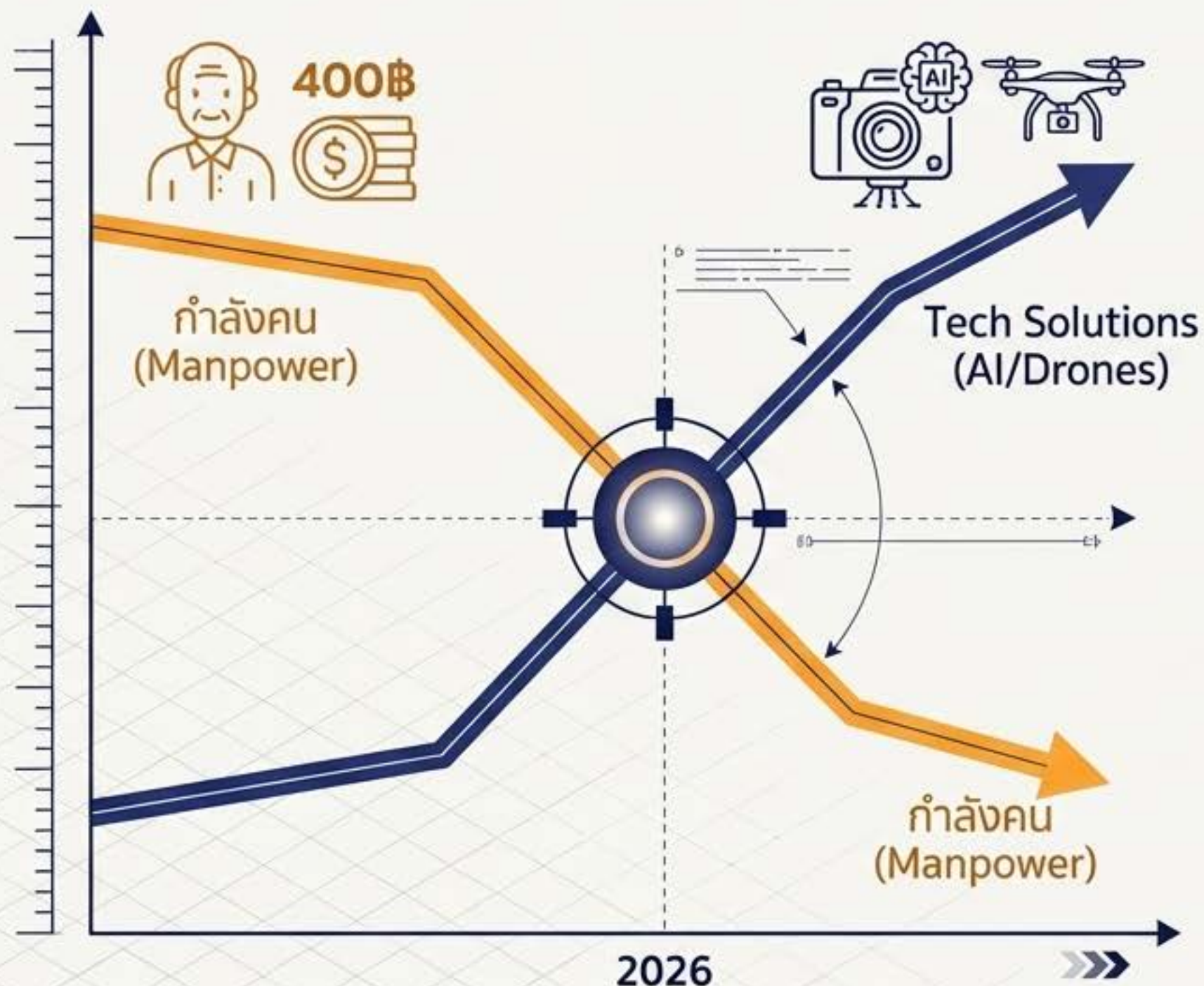
Broken Windows Theory



ความไร้ระเบียบเล็กน้อย
นำไปสู่อาชญากรรมรุนแรง

การประยุกต์: หลอดไฟลานจอดรถเสียหรือขยะล้น
เชื้อเชิญมิจฉาชีพ ต้องเน้นการบำรุงรักษา
(Maintenance) ให้ดูมีคนดูแล

ความท้าทายและแนวโน้มอนาคต (2026+)



วิกฤตแรงงานและค่าแรง

สังคม Super-Aged และค่าแรง 400 บาท
ทำให้แรงงาน สปก. หายากและมีต้นทุนแพงมหาศาล



Tech Substitution (เทคโนโลยีทดแทนคน)

เปลี่ยนจาก Man-guarding สู่ Security Solutions
(กล้อง AI, โดรน, IoT) ทดแทนงานซ้ำซ้อน



ภัยคุกคามไซเบอร์ระดับสูง

การใช้ AI สร้าง Deepfake (ปลอมหน้า/เสียง
ผู้บริหาร) เพื่อหลอกลวงทางการเงิน

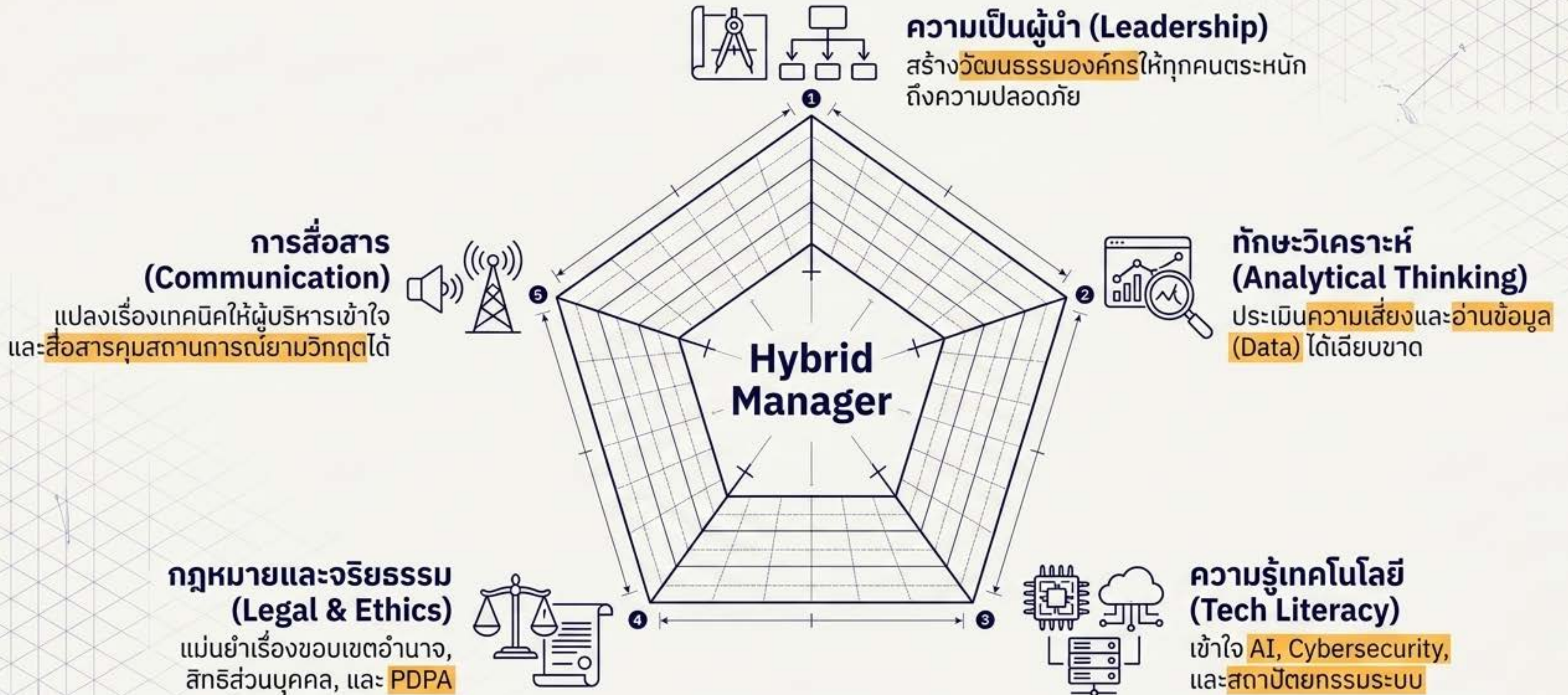


ความเข้มข้นของ Data Privacy

PDPA จะบังคับใช้เคร่งครัดขึ้น ผู้จัดการต้อง
ทำงานคู่กับ DPO อย่างใกล้ชิด



ทักษะหลักของผู้จัดการความมั่นคงยุคใหม่ (Hybrid Manager)



บทสรุป: จาก ‘หัวหน้ายาม’ สู่ ‘Strategic Risk Manager’

อดีต: การใช้กำลังกาย (Force) และเฝ้าประตู



ปัจจุบัน: การใช้สติปัญญา (Intelligence & Management)



- ภัยคุกคามเปลี่ยนแปลงตลอดเวลา การยึดติดวิธีเดิมคือจุดอ่อนที่สุด
- หน้าทีของคุณไม่ใช่การเฝ้าประตู แต่คือการสร้าง ‘ความยืดหยุ่นและการฟื้นตัว’ (Resilience) ให้กับองค์กร

คำถามทบทวน: องค์กรของคุณยังมี Security Theater อยู่หรือไม่? และคุณพร้อมรับมือภัยคุกคามแบบ Hybrid หรือยัง?