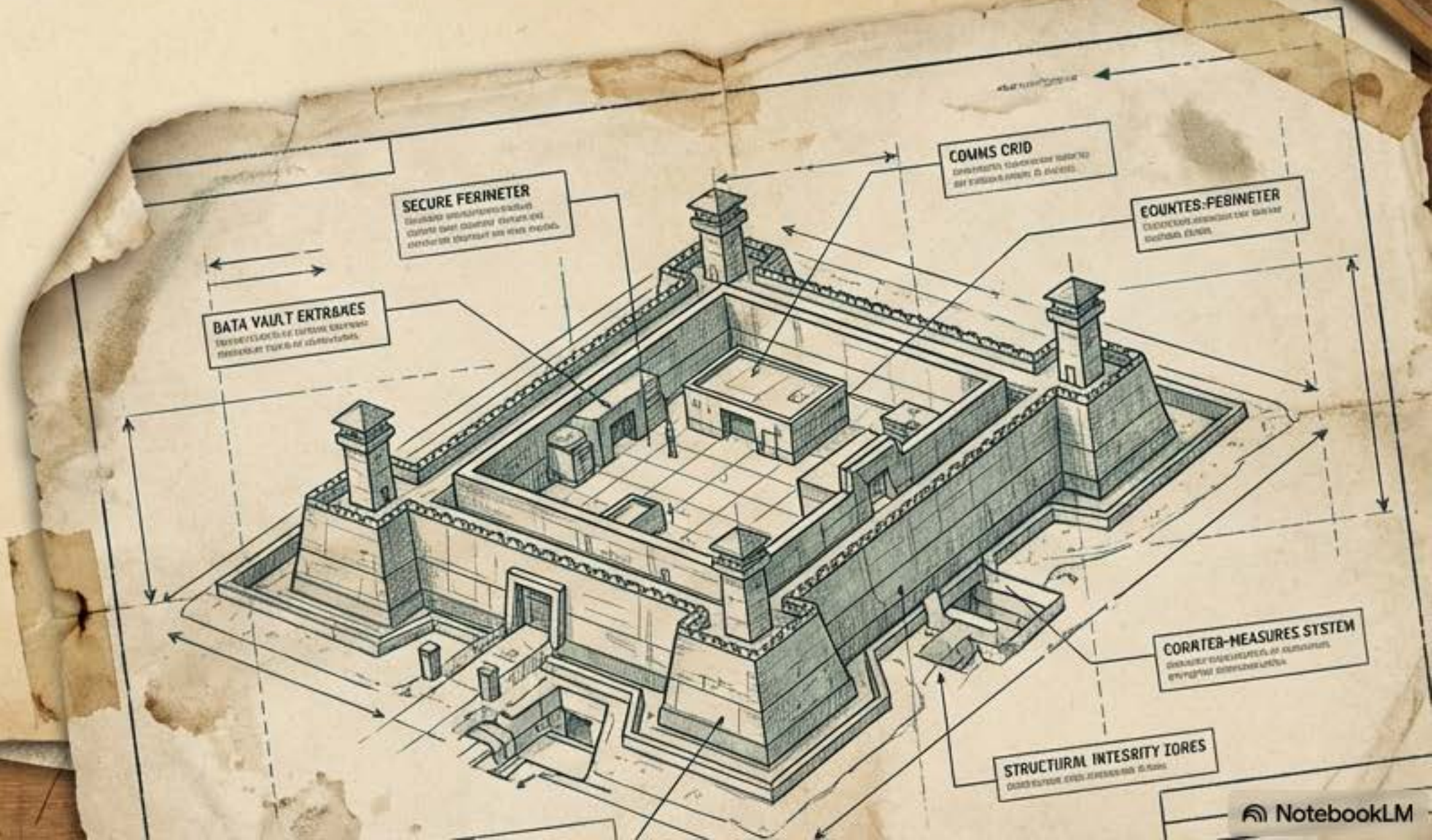




สถาปัตยกรรมแห่งความมั่นคงปลอดภัย

รากฐานและทฤษฎี (The Architecture of Security: Foundations & Theories)

จากความโกลาหลสู่ความเป็นระเบียบ
(From Chaos to Order)



ภัยคุกคามคือการฉวยโอกาสจาก "ระบบ"

CASE FILE: The Agent of Chaos

"ไม่มีใครขึ้นตระหนกตราบเท่าที่ทุกอย่างเป็นไปตามแผน
แม้ว่าแผนนั้นจะน่าสยดสยองเพียงใดก็ตาม"

- The Joker (The Dark Knight)

ภัยคุกคามไม่ได้เกิดจากความบังเอิญ

อาชญากรที่แท้จริงโจมตีโดยอาศัย:

- กิจกรรมประจำวันที่สามารถคาดเดาได้ (Predictable Routines)
- การเฝ้าระวังที่หละหลวม (Weak Guardianship)
- จุดบอดขององค์กร (Organizational Blind Spots)



การรักษาความปลอดภัยที่มีประสิทธิภาพไม่ใช่เรื่องบังเอิญ แต่มันคือเรื่องของทฤษฎี

ก้าวข้าม "ละครแห่งการรักษาความปลอดภัย"

ทำไมทฤษฎีจึงสำคัญ? (Why Theory Matters)

การพึ่งพาสัญชาตญาณเพียงอย่างเดียว นำไปสู่มาตรการที่ดูดีแต่ไร้ผล (Security Theater)
ทฤษฎีให้รากฐานที่มั่นคง 3 ประการ:



WARNING

สังคมแห่งความเสี่ยง (Risk Society)

ภัยคุกคามในศตวรรษที่ 21 คือสิ่งที่มนุษย์สร้างขึ้น

เราอยู่ในยุคที่ความเสี่ยงไม่ได้มาจากธรรมชาติ
แต่มาจากเทคโนโลยีและระบบที่ซับซ้อนของเราเอง
(Manufactured Risks):

- Incalculable: คำนวณความเสียหาย
ล่วงหน้าไม่ได้
- Transboundary: ไร้พรมแดน ลุกลาม
อย่างรวดเร็ว
- Irreversible: ความเสียหายมักแก้ไขให้
กลับเป็นเหมือนเดิมไม่ได้

[INTELLIGENCE REPORT]

Alert: ประเทศไทยเผชิญการโจมตี
ไซเบอร์เฉลี่ย 3,180 ครั้ง/สัปดาห์
(สูงกว่าค่าเฉลี่ยโลกถึง 70%)

ทฤษฎีหน้าต่างแตก

ความไม่เป็นระเบียบ คือจุดเริ่มต้นของอาชญากรรม
(Broken Windows Theory)

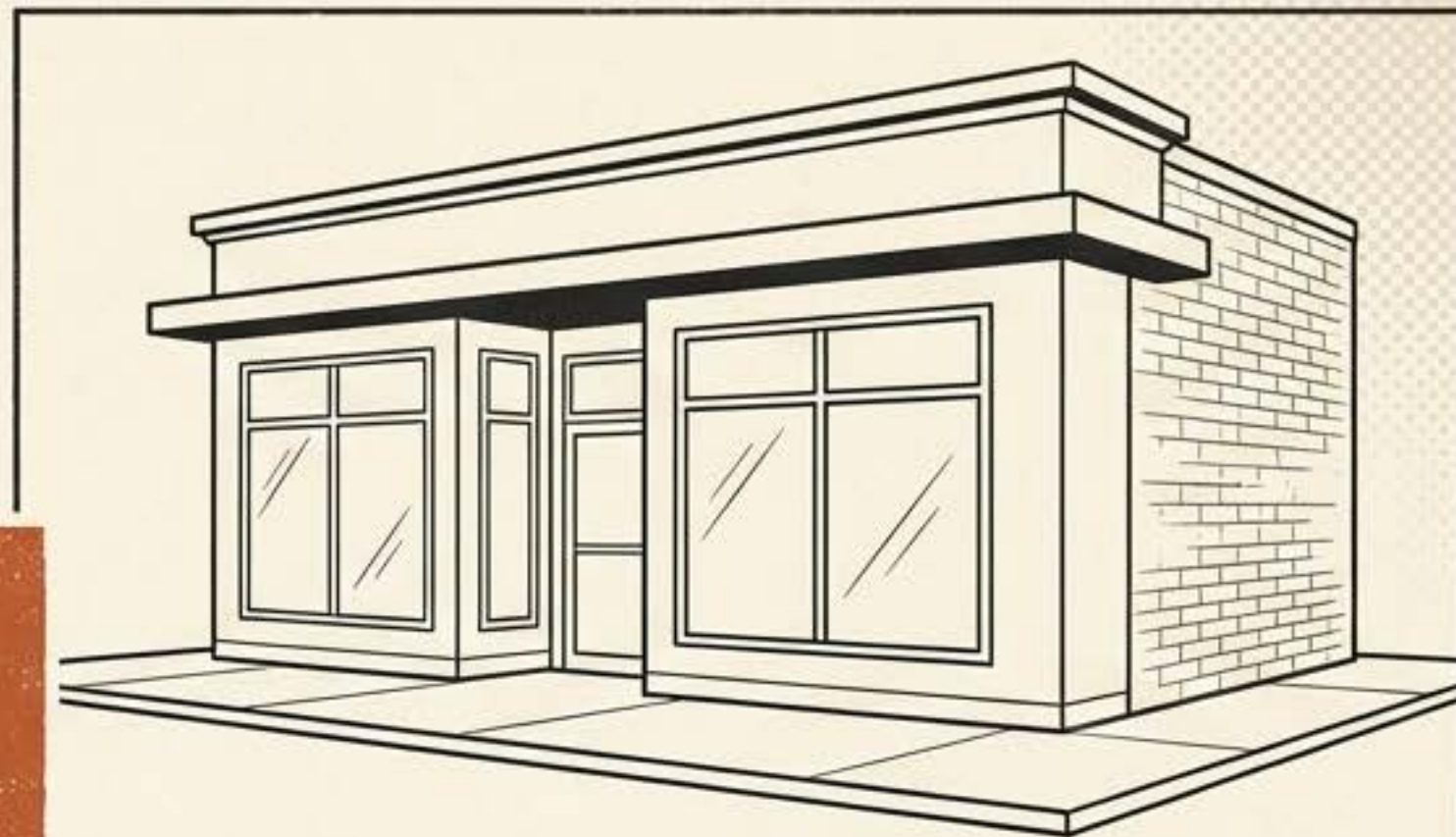
การทดลองของ Zimbardo (1969):

รถยนต์ที่จอดทิ้งไว้ในสภาพดีจะไม่ถูกขโมย
จนกว่าจะมีร่องรอยความเสียหายแรกเกิดขึ้น

สมการความเสี่ยง: ความไม่เป็นระเบียบ (Disorder)
+ การละเลย (Neglect) = การเชิญชวนอาชญากร

ยุทธศาสตร์: การซ่อมแซมและดูแลรักษาสภาพ
แวดล้อม (Maintenance) คือการป้องกันที่มีต้นทุน
ต่ำแต่ได้ผลสูงสุด

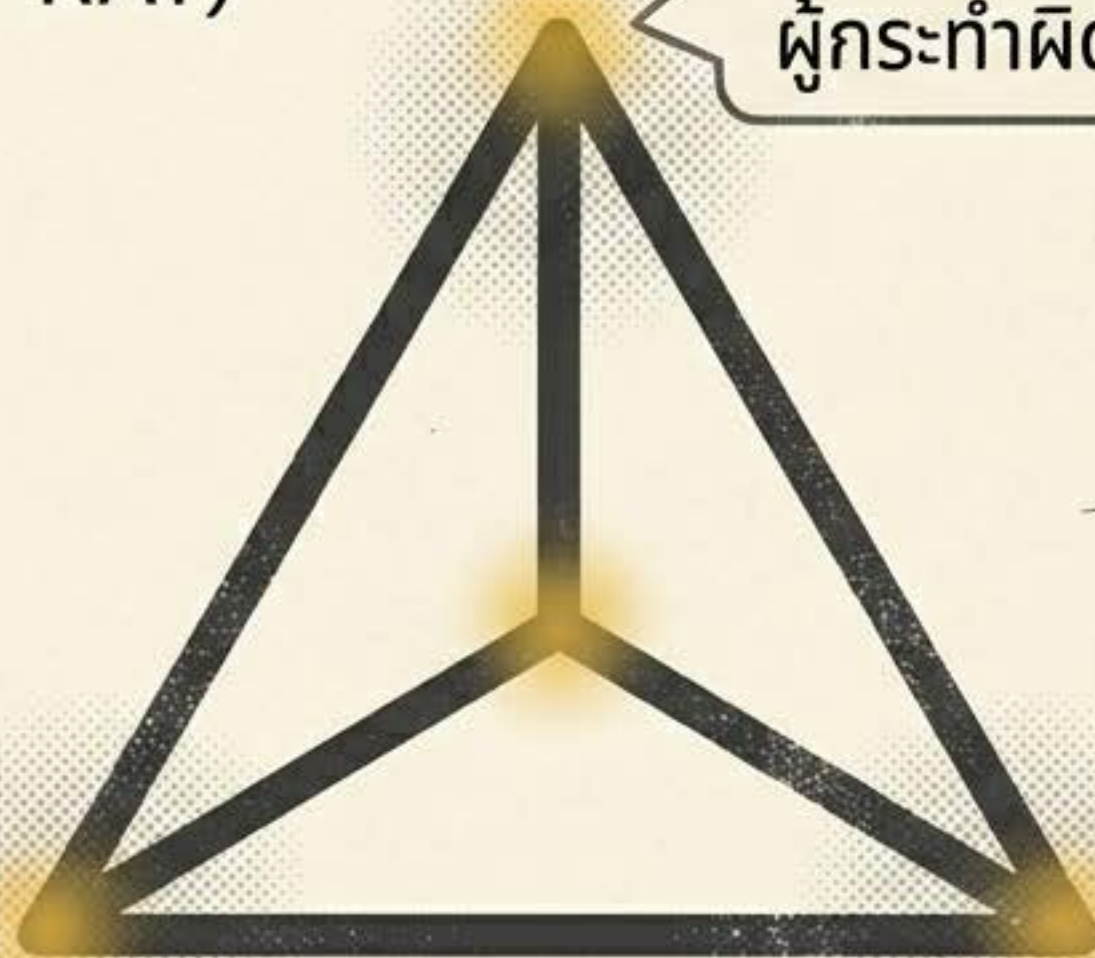
INTELLIGENCE
BRIEF



โครงสร้างของโอกาส (The Crime Triangle)

ทฤษฎีกิจวัตรประจำวัน
(Routine Activity Theory - RAT)

อาชญากรรมไม่ได้เกิดจากความ
ยากจนเพียงอย่างเดียว
แต่เกิดจาก 3 องค์ประกอบ
ที่บรรจบกันในเวลาและสถานที่:



1. Motivated Offender:
ผู้กระทำความผิดที่มีแรงจูงใจ

3. Absence of Guardian:
การขาดผู้พิทักษ์
(ไม่มีเจ้าหน้าที่, มุมอับ)

2. Suitable Target:
เป้าหมายที่เหมาะสม
(มีค่า, เข้าถึงง่าย)

ทำไมการล้วงกระเป๋าจึง
สูงในรถไฟฟ้าช่วงเร่งด่วน?
เป้าหมายหนาแน่น + ผู้พิทักษ์
ถูกลบบังทัศนวิสัยด้วยฝูงชน

CLASSIFIED
CLASSIFIED
CLASSIFIED



[TRANSIT CASE STUDY]

สถาปัตยกรรมป้องกันภัย (CPTED)

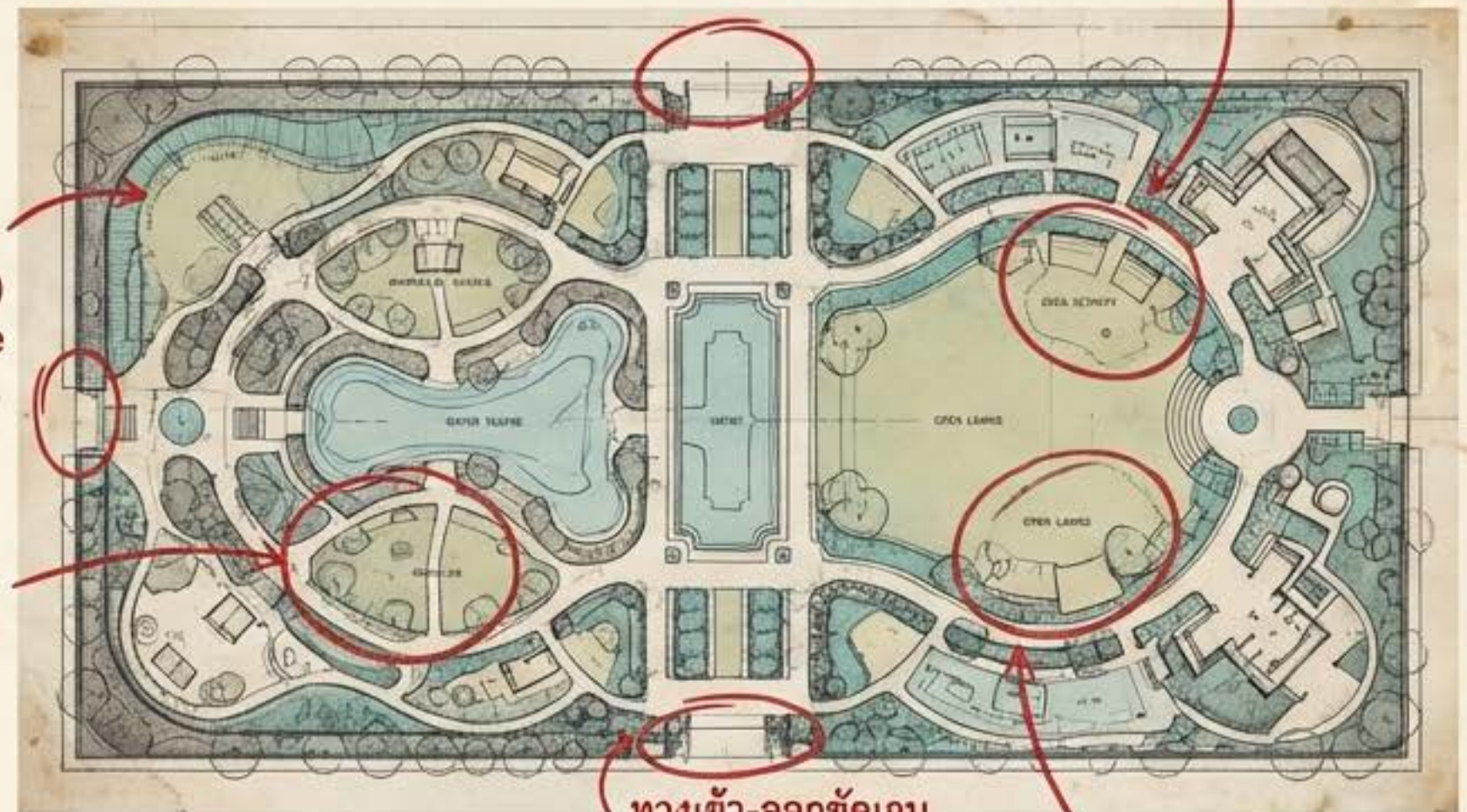
การป้องกันอาชญากรรมด้วยการออกแบบสภาพแวดล้อม

หลักการออกแบบพื้นที่เพื่อตัดโอกาสอาชญากร:

- Territoriality (อาณาเขต): แบ่งโซนชัดเจน สร้างความรู้สึกเป็นเจ้าของ
- Natural Surveillance (การเฝ้าสังเกต): ไม่มีจุดอับสายตา มองเห็นได้จากภายนอก
- Image & Milieu (ภาพลักษณ์และบริบท): สะอาด สว่าง ปลอดภัย

รั้วโปร่ง
(Transparent Fence)
- Natural Surveillance

พื้นที่กิจกรรมกระจาย
(Activity Support)



ทางเข้า-ออกชัดเจน
(Clear Entrances/Exits)
- Territoriality

ทางเข้า-ออกชัดเจน
(Clear Entrances/Exits)
- Territoriality

ไม่มีจุดอับสายตา
(No Blind Spots)
- Image & Milieu

[BLUEPRINT: อุทยาน 100 ปี จุฬาฯ]

ใช้รั้วโปร่งเพื่อให้มองเห็นจากภายนอก และกระจายพื้นที่กิจกรรมเพื่อสร้างความเคลื่อนไหว (Activity Support) ลงจุดบอดในสวน

5 กลไกควบคุมสถานการณ์

การป้องกันอาชญากรรมตามสถานการณ์ (SCP)

การเปลี่ยนพฤติกรรมคนนั้นยาก
การเปลี่ยน 'สถานการณ์' ง่ายกว่า
ทำให้การก่อเหตุ 'ไม่คุ้มค่า'
ผ่าน 5 กลยุทธ์:



จิตวิทยาของการป้องปราม

ทฤษฎีการป้องปราม (Deterrence Theory)

อาชญากรที่เป็นมนุษย์เศรษฐกิจ (Rational Actor) จะคำนวณความเสี่ยงเสมอ การป้องปรามต้องอาศัย 3 องค์ประกอบ (3 C's):

- **ความแน่นอน (Certainty):** เชื่อมั่นว่าทำผิดแล้วต้องถูกจับแน่ๆ (สำคัญที่สุด)
- **ความรุนแรง (Severity):** โทษหนักพอที่จะกลบผลประโยชน์
- **ความรวดเร็ว (Celerity):** การลงโทษต้องเกิดขึ้นทันที



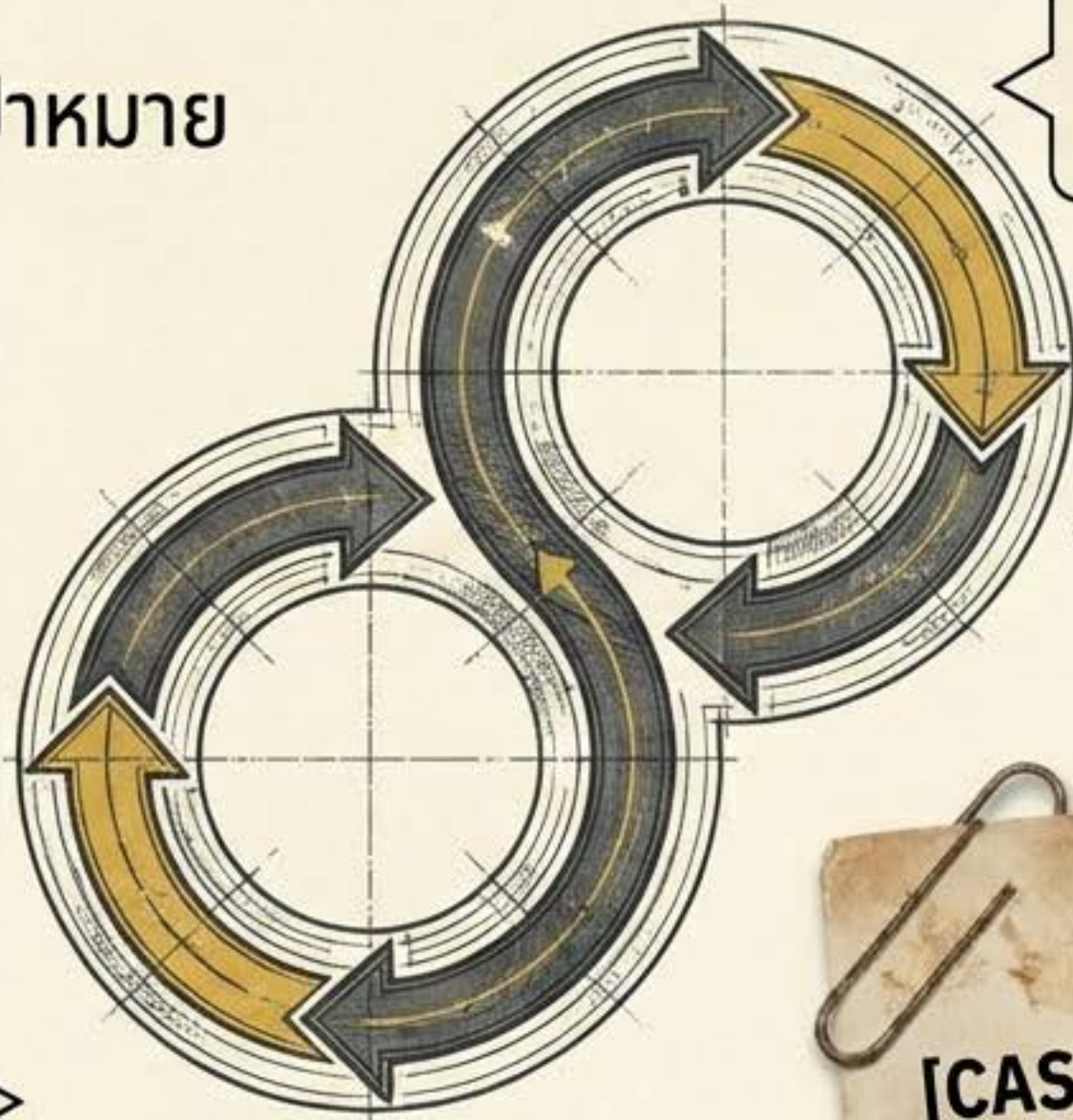
ยืดหยุ่นและฟื้นตัว (Resilience)

เมื่อการป้องกัน 100% เป็นไปไม่ได้

ความมั่นคงยุคใหม่เปลี่ยนจากเป้าหมาย
"ไม่ให้เกิดเหตุเลย" ใดๆเลย"
เป็น "ความยืดหยุ่น"
(Organizational Resilience):

4. เรียนรู้และปรับตัว (Adapt):
นำบทเรียนมาอุดช่องโหว่

3. ฟื้นฟู (Recover):
กลับสู่สถานะปกติอย่างรวดเร็ว



1. เตรียมพร้อม (Prepare):
ซ้อมแผน สำรองทรัพยากร

2. ดูดซับแรงกระแทก (Absorb):
รักษาการทำงานหลักแม้ระบบจะพัง

[CASE FILE: อุทกภัยปี 2554]
องค์กรที่มีศูนย์สำรองข้อมูล (DR Site) นอกพื้นที่
สามารถดำเนินกิจการต่อได้แม้สำนักงานใหญ่จมน้ำ

ดีเอ็นเอขององค์กรไร้รอยต่อ

องค์กรที่มีความน่าเชื่อถือสูง (High-Reliability Organizations)

อุตสาหกรรมที่มีความเสี่ยงสูง (เช่น การบิน, พลังงาน) รักษาความปลอดภัยระดับสูงสุดด้วย 5 วัฒนธรรม:

1

- หมกมุ่นกับความล้มเหลว: ไม่ปล่อยผ่านเหตุการณ์ “เกือบเกิดปัญหา” (Near-misses)

2

- ไม่ไว้ใจคำอธิบายง่ายๆ: มองหาความซับซ้อนที่ซ่อนอยู่เสมอ

3

- ตั้งตัวต่อหน้างานจริง: รับฟังสัญญาณเตือนจากพนักงานระดับปฏิบัติการ

4

- มุ่งมั่นสู่ความยืดหยุ่น: พร้อมแก้ปัญหาเฉพาะหน้าอย่างสร้างสรรค์

5

- เชื่อฟังผู้เชี่ยวชาญ: ให้อำนาจตัดสินใจแก่ผู้รู้จริง ไม่ใช่แค่ตามลำดับชั้น

CLASSIFIED

ระบบสังคม-เทคนิค

ความล้มเหลวไม่ได้เกิดจากเครื่องจักรเพียงอย่างเดียว

ความมั่นคงที่แท้จริงเกิดจาก 4 ส่วนที่สอดคล้องกัน (Socio-Technical Systems):

1. คน (People):

พฤติกรรมและวัฒนธรรม

2. เทคโนโลยี (Technology):

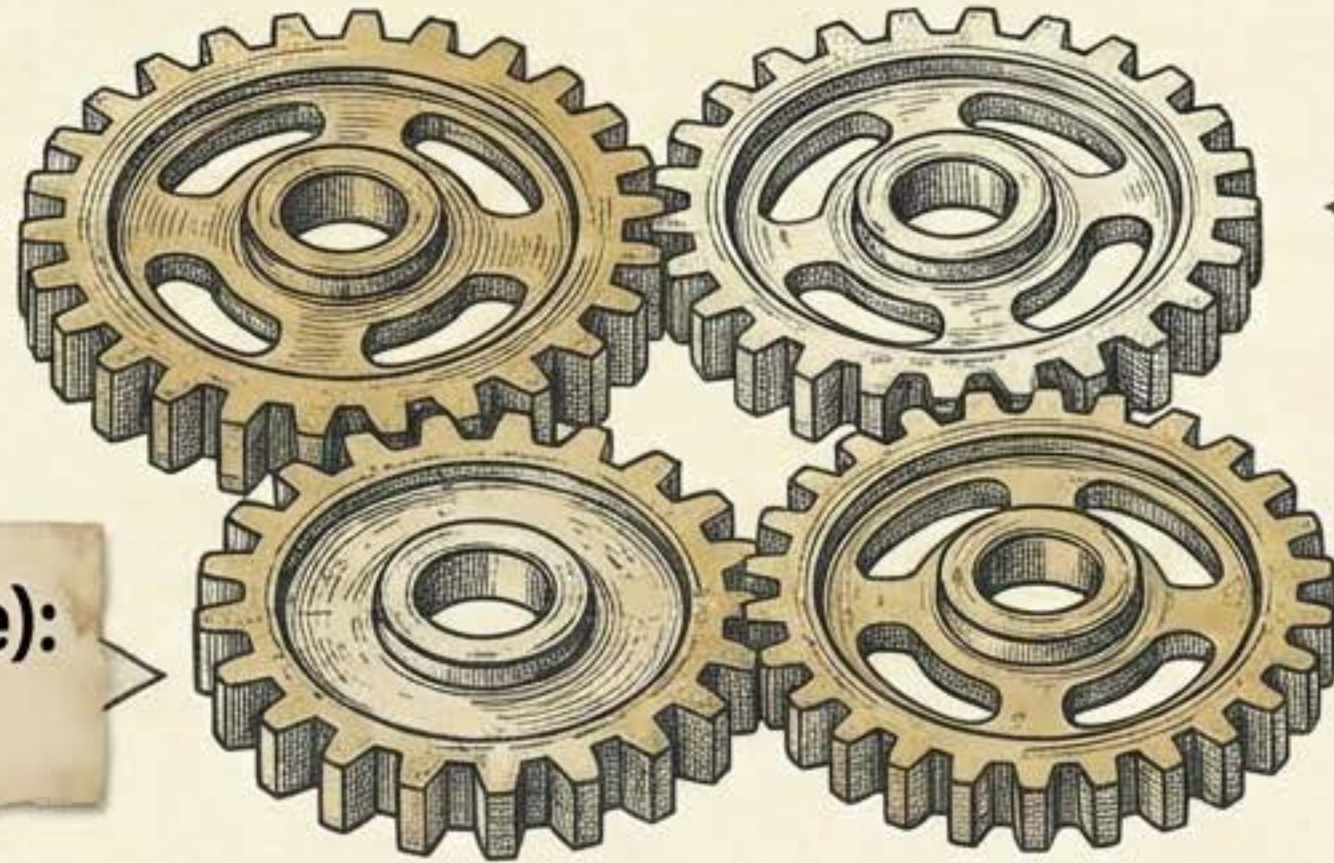
อุปกรณ์และซอฟต์แวร์

4. ธรรมาภิบาล (Governance):

การกำกับดูแลจากผู้บริหาร

3. กระบวนการ (Procedures):

นโยบายและแผนปฏิบัติการ



[DATA ALERT] ไตรมาสเดียวในปี 2024 ไทยถูกโจมตีไซเบอร์ 196,078 ครั้ง – สาเหตุหลักไม่ได้มาจากระบบล้ำสมัย แต่มาจากการตั้งรหัสผ่านที่อ่อนแอและพฤติกรรมของผู้ใช้

CLASSIFIED

เส้นแบ่งจริยธรรม

ความชอบธรรมในการรักษาความมั่นคงปลอดภัย

CONFIDENTIAL

การควบคุมที่เข้มงวดเกินไป (Over-securitization) จะทำลายความไว้วางใจขององค์กร
การจัดการต้องรักษาสมดุล 3 ด้าน:

- ความเป็นส่วนตัว (Privacy): เคารพกฎหมาย (เช่น PDPA) จัดเก็บข้อมูลที่จำเป็น
- ความได้สัดส่วน (Proportionality): มาตรการต้องไม่รุนแรงเกินกว่าภัยคุกคามจริง
- ความรับผิดชอบ (Accountability): ผู้คุมกฎต้องโปร่งใสและตรวจสอบได้

COMPLIANT

ความมั่นคงที่ปราศจากความชอบธรรม จะนำไปสู่การต่อต้านจากภายใน

แผนแม่บท (The Master Plan)

บูรณาการทุกขงูสู่การปฏิบัติ (Integrated Security Strategy)

กรณีศึกษา:

การวางระบบความปลอดภัย
ในพื้นที่มหาวิทยาลัย

• **RAT:** ตัดโอกาสโจรฉวยโอกาส
ด้วยตู้ล็อกเกอร์และเจ้าหน้าที่ตรวจตรา

• **SCP & CPTED:** ออกแบบพื้นที่สว่าง
ติดตั้ง CCTV และใช้ระบบคีย์การ์ด

• **Deterrence:** บังคับใช้กฎอย่าง
รวดเร็วและเด็ดขาดเพื่อป้องปราม

• **Resilience:** มีแผนฉุกเฉิน
และฝึกซ้อมอยู่เสมอ

• **Socio-Technical:** ผสานเทคโนโลยีเข้า
กับวัฒนธรรมการระงับภัยของนักศึกษา

ทุกขงูเปลี่ยนการดับเพลิงเฉพาะหน้า
ให้เป็นการบริหารความเสี่ยงเชิงยุทธศาสตร์