



**TOP SECRET
CONFIDENTIAL**

บทนำสู่การจัดการความมั่นคงปลอดภัย

Introduction to Security Management



แฟ้มข้อมูลลับ:
ปรับแนวคิดจาก "การเฝ้ายาม"
สู่ "การบริหารความเสี่ยงเชิงกลยุทธ์"
(เอกสารสำหรับอ่านและศึกษาด้วยตนเอง)



ภาพลวงตาแห่งความปลอดภัย (The Illusion of Safety)

บทเรียนจากภาพยนตร์ Die Hard (1988):
อาคารที่ทันสมัยที่สุด ล็อกอิเล็กทรอนิกส์ และ รปภ.
ในเครื่องแบบ ไม่สามารถหยุดยั้งผู้ก่อการร้ายได้

สาเหตุความล้มเหลว:

- การบุกรุกผ่านจุดที่หละหลวมที่สุด (จุดโหลดสินค้า)
- รปภ. ขาดทักษะการคัดกรองบุคคล
- ผู้บุกรุกใช้ระบบของอาคารเป็นอาวุธย้อนกลับ

ความมั่นคงปลอดภัยไม่ใช่ผลิตภัณฑ์ แต่เป็นกระบวนการ (Security is a process, not a product)

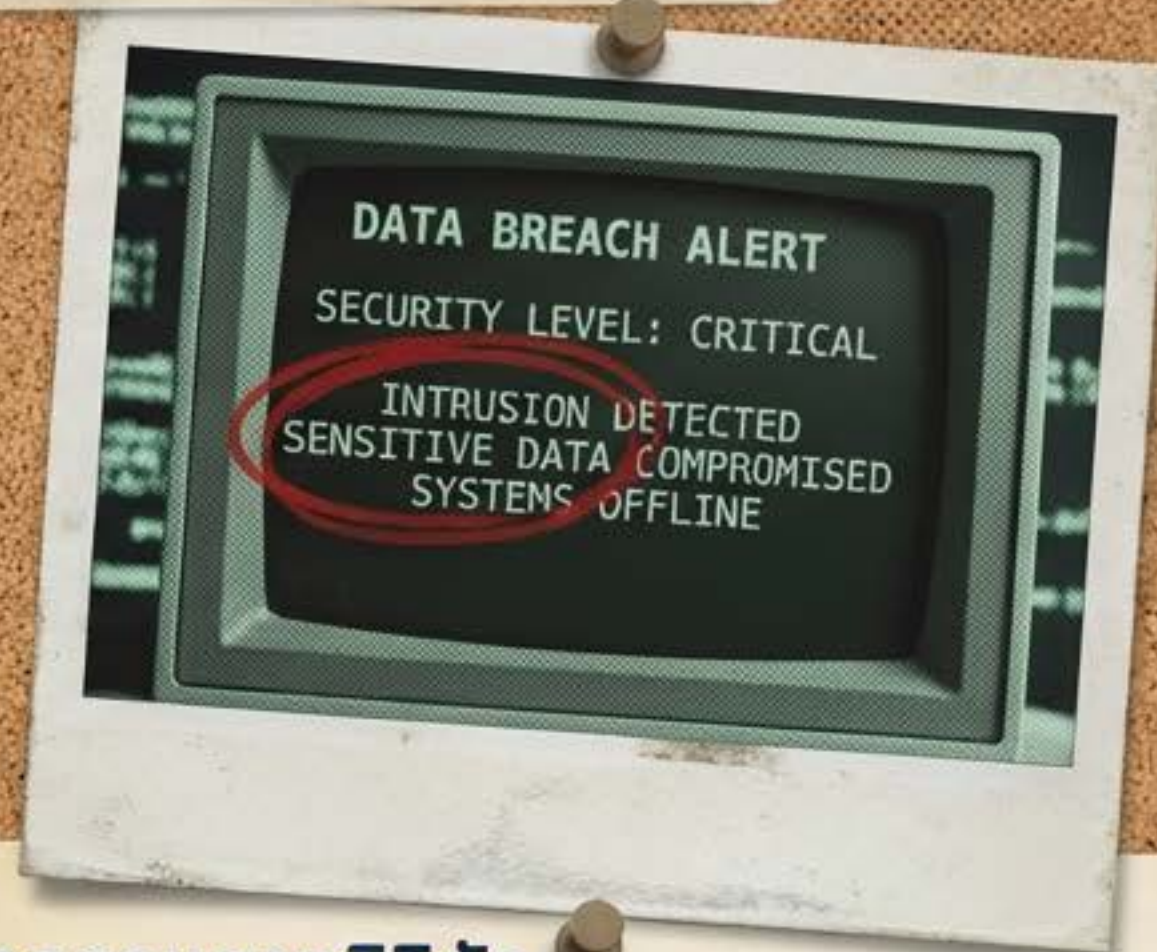
บทเรียนจากเรื่องจริงในสังคมไทย



ภัยคุกคามทางกายภาพ

กรณีศึกษา: สยามพารากอน (2023)

- มาตรการคัดกรองเน้นเพียง "พิธีกรรม" (Ritualistic Screening)
- ขาดแผนเผชิญเหตุและการสื่อสารที่ชัดเจน
- ผลลัพธ์: ความเสียหายระดับมหภาคต่ออุตสาหกรรมท่องเที่ยว



ภัยคุกคามทางดิจิทัล

กรณีศึกษา: แฮกเกอร์ 9Near (2023)

- การเจาะผ่านช่องโหว่ของการบริหารจัดการข้อมูล (Data Governance)
- ข้อมูลคนไทย 55 ล้านคนรั่วไหล
- ผลลัพธ์: การนำไปสู่การสวมรอยและอาชญากรรมไซเบอร์

ความล้มเหลวเพียงจุดเดียว = ความพินาศเชิงระบบ

เส้นแบ่งที่ชัดเจน: Safety vs. Security



Safety (ความปลอดภัย)



การป้องกันอันตรายจาก “อุบัติเหตุ” หรือภัยธรรมชาติ

- ไม่มีเจตนามุ่งร้าย (Unintentional)
- ตัวอย่าง: อาชีวอนามัย, ทัศนภัย, สารเคมีรั่วไหล
- อุปกรณ์: หมวกนิรภัย, รองเท้าเซฟตี้



Security (ความมั่นคงปลอดภัย)



การปกป้องสินทรัพย์จาก “เจตนาประสงค์ร้าย” ของมนุษย์

- มีเจตนามุ่งร้าย (Malicious Acts)
- ตัวอย่าง: อาชญากรรม, การก่อการร้าย, จารกรรมข้อมูล
- อุปกรณ์: กล้องวงจรปิด, ระบบ Access Control, การเข้ารหัสข้อมูล

กับดัก "ละครรักษาความปลอดภัย" (Security Theater)

การแยกระหว่างความรู้สึกกับความเป็นจริง:



1. ความมั่นคงปลอดภัยเชิงจิตวิสัย (Subjective Security):

- การสร้าง "ความรู้สึก" ว่าปลอดภัย
- ตัวอย่าง: สปก. ยื่นทำความเคารพรถทุกคัน แต่ไม่เคยตรวจสอบท้ายรถหรือขอบัตรประชาชน



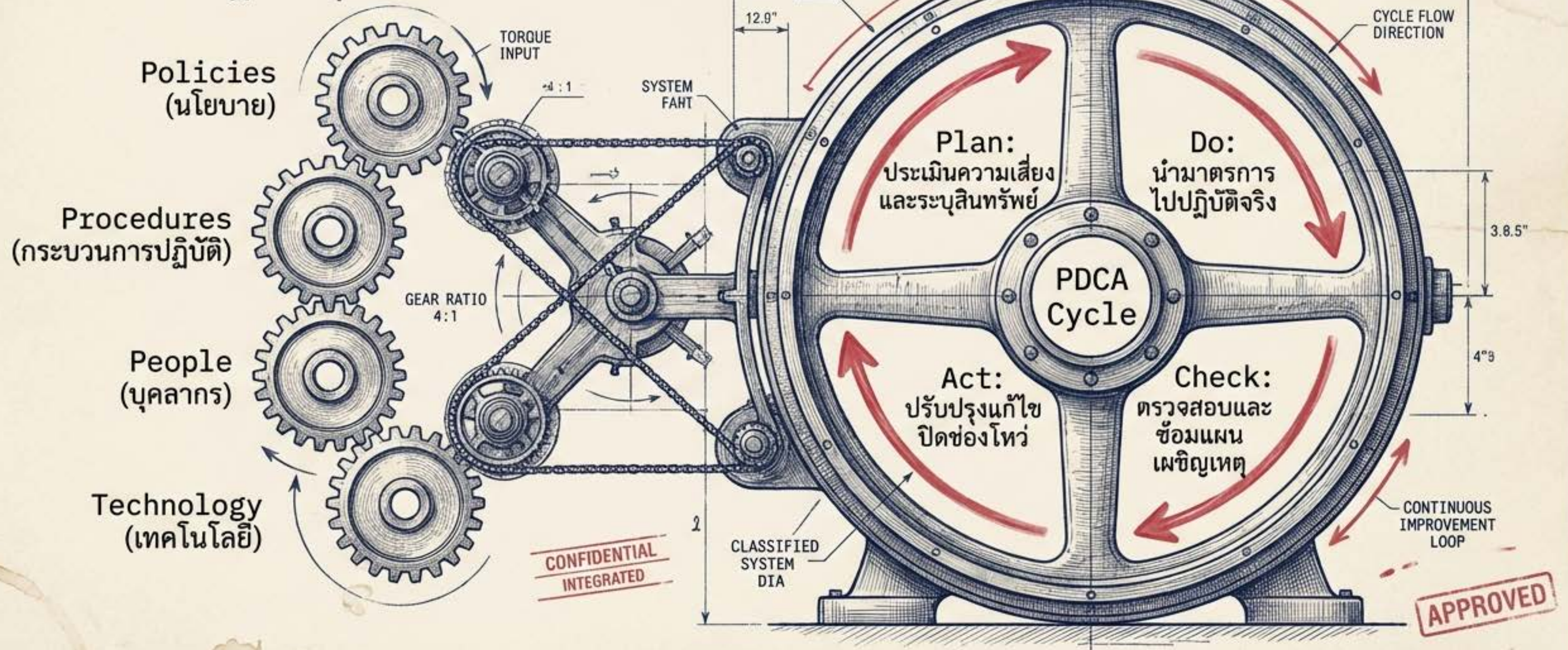
2. ความมั่นคงปลอดภัยเชิงวัตถุวิสัย (Objective Security):

- สถานะที่ "วัดผลและจับต้องได้จริง"
- ตัวอย่าง: ความละเอียดของกล้อง 4K, มาตรฐานการเข้ารหัสข้อมูล, จำนวนเจ้าหน้าที่ต่อพลัด

หน้าที่ของผู้จัดการคือการขจัด "ปาหี่" ที่ไร้ประโยชน์ และแทนที่ด้วยมาตรการที่ป้องกันได้จริง!

กลไกการจัดการความมั่นคงปลอดภัย

การบูรณาการองค์ประกอบ 4 ประการ (4Ps)
ขับเคลื่อนด้วยวัฏจักรคุณภาพ:



ระบบนิเวศความมั่นคงปลอดภัย (The Security Ecosystem)

สินทรัพย์ 4 ประเภทที่ต้องได้รับการปกป้องอย่างบูรณาการ:

2. สินทรัพย์ทางกายภาพ (Physical Assets):
อาคาร, เครื่องจักร, เว้นสค
ใช้หลักการป้องกันคนร้าย

1. คน (Human Assets):
สินทรัพย์ที่มีค่าและบางที่สุด
(พนักงาน, ลูกค้า, ผู้บริหาร)
เน้นป้องกันภัยคุกคามจาก
และการตรวจสอบประวัติ

3. ข้อมูล (Information/Data):
ฐานข้อมูล, ความลับทางการค้า
เป้าหมายหลักในเศรษฐกิจดิจิทัล

4. ชื่อเสียง (Reputation):
สินทรัพย์ที่สร้างมูลค่าหลายต่อได้
เชื่อมโยงกับการบริหารวิกฤต
(Crisis Management)

Organizational
Survival

STRUCTURAL
INTEGRITY
ANALYSIS

STRUCTURAL
INTEGRITY
ANALYSIS

INTEGRATED ECOSYSTEM

CONFIDENTIAL

INTERCONNECTED FOUNDATION

INTERCONNECTED FOUNDATION

SYSTEM
REUNDANCY
CHECK

ASSET

C:\>■

SYSTEM READY...

หัวใจของความปลอดภัยข้อมูล: CIA Triad

ในยุคที่ข้อมูลมีค่ามากกว่าทองคำ การปกป้องต้องยึดหลัก 3 ประการ:



C - Confidentiality (ความลับ):
ข้อมูลต้องเข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น
(เช่น การเข้ารหัส, PDPA)

I - Integrity (ความถูกต้องครบถ้วน):
ข้อมูลต้องไม่ถูกแก้ไข เปลี่ยนแปลง
หรือทำลายโดยไม่ได้รับอนุญาต
(เช่น ยอดเงินในบัญชี)

A - Availability (ความพร้อมใช้):
ระบบต้องพร้อมใช้งานเสมอ ไม่ล่ม
ไม่ถูกปิดกั้น
(เช่น ระบบจ่ายไฟโรงพยาบาล)

ACCESSING_

DATA SECURE.

วิวัฒนาการของวิชาชีพ (Evolution of the Profession)



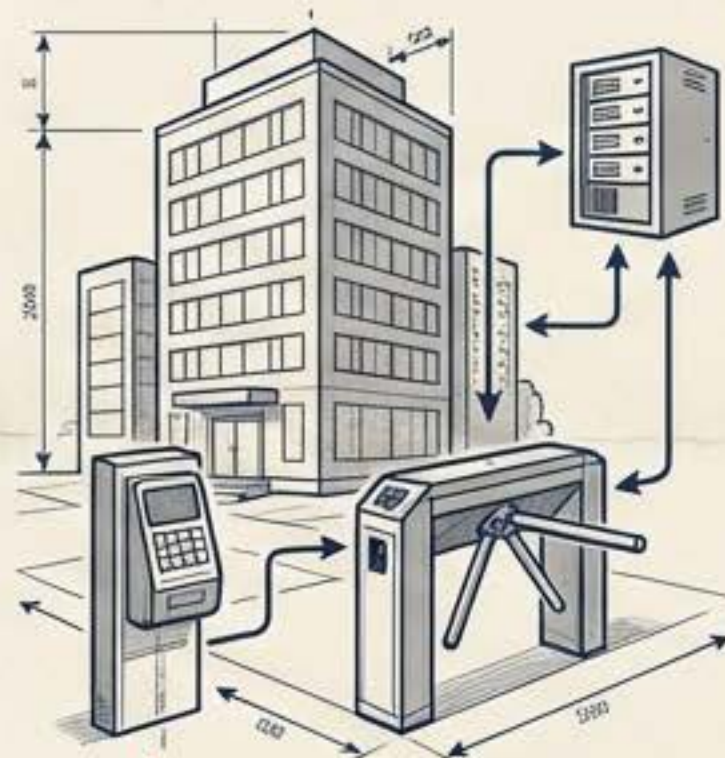
HUMAN-CENTRIC SECURITY

ยุคโบราณ - เฝ้ายาม (Watchmen):
พึ่งพากำลังคนและความกล้าหาญ
เน้นการเฝ้าระวังและการต่อสู้ด้วย
อาวุธพื้นฐาน



EARLY PRIVATE SECURITY & BASIC TECH

ศตวรรษที่ 19 - ยุคอุตสาหกรรม
(Pinkertons):
จุดกำเนิดบริษัทรักษาความปลอดภัย
เอกชน เริ่มมีการใช้เทคโนโลยีเบื้องต้น



INTEGRATED RISK & CORPORATE SECURITY

หลัง 9/11 - ยุคจัดการความเสี่ยง
(Risk Era):
บูรณาการการต่อต้านการก่อการร้าย
และการรักษาความปลอดภัยระดับ
องค์กร



CYBER-PHYSICAL CONVERGENCE & AI

ปัจจุบัน - การรวมศูนย์ไซเบอร์และ
กายภาพ:
ผู้จัดการต้องบริหารความเสี่ยงแบบ
องค์รวม (CISO) ผสมผสาน AI
และเทคโนโลยี

CONFIDENTIAL

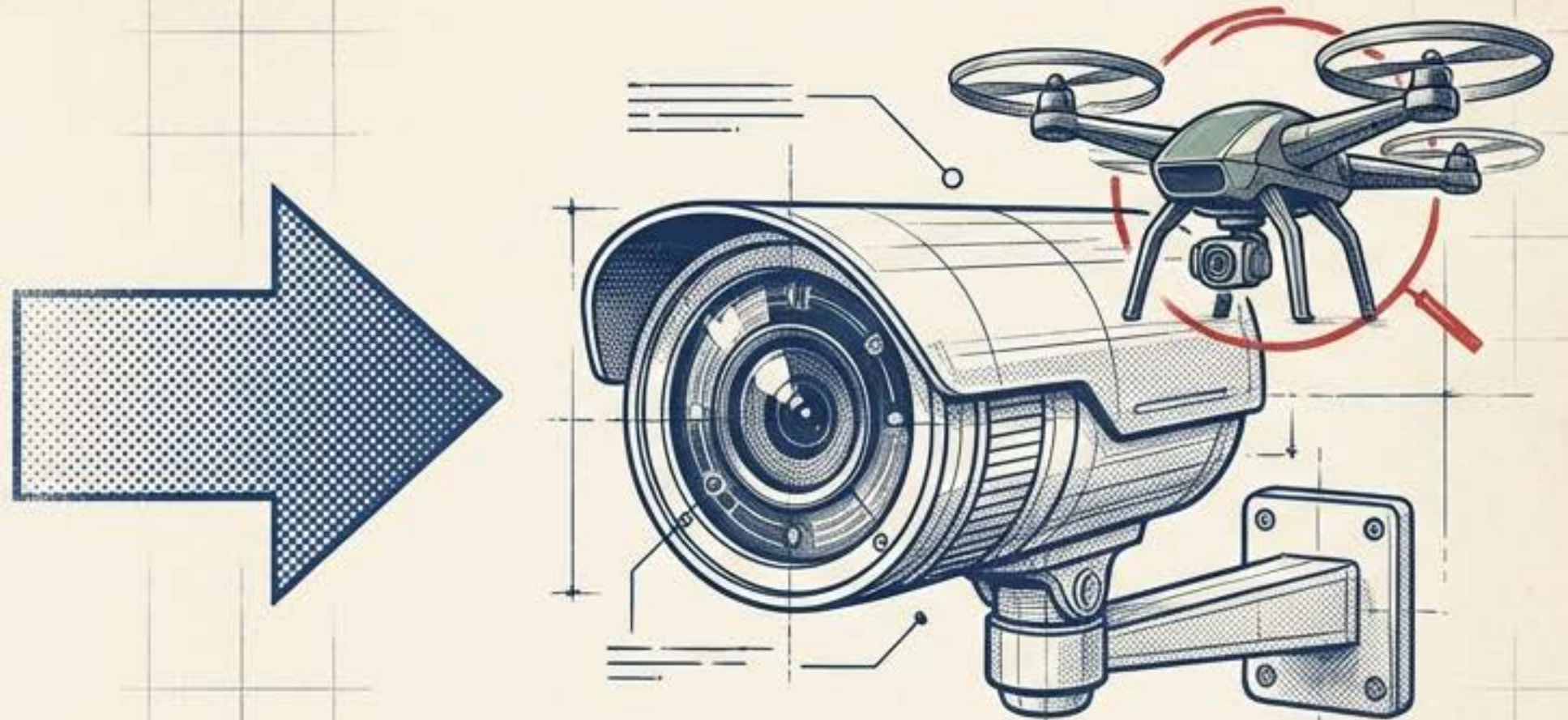
จุดเปลี่ยนของอุตสาหกรรมในประเทศไทย

[แรงกดดันทางกฎหมายและเศรษฐกิจ]



- พ.ร.บ. อนุรักษ์ความปลอดภัย 2558: ยกระดับมาตรฐาน รปภ. นำไปสู่ภาวะ “ขาดแคลนแรงงาน”
- ค่าแรงขั้นต่ำและสังคมผู้สูงอายุ: ต้นทุนแรงงานพุ่งสูง (400 บาท/วัน) และคนหนุ่มสาวลดลง

[การปรับตัว: Manpower Substitution]



การใช้เทคโนโลยีทดแทนคน:

- กล้อง AI CCTV ตรวจจับผู้บุกรุกอัตโนมัติ
- โดรน (Drones) ลาดตระเวนพื้นที่กว้าง
- ระบบ Access Control และ Facial Recognition

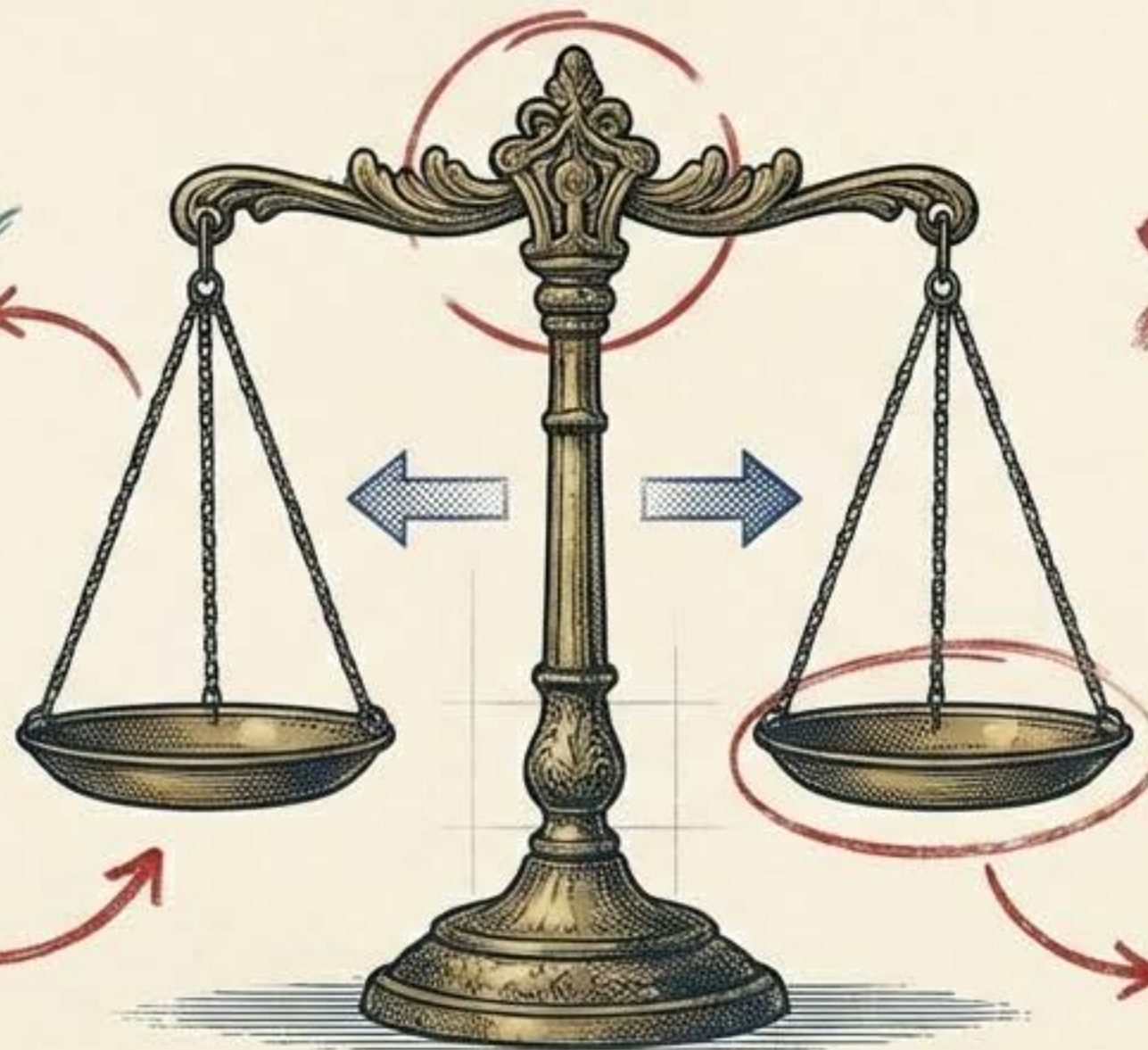
SYSTEM READY...

ขอบเขตอำนาจ: รัฐ vs เอกชน

ความเข้าใจผิดที่อันตราย: “รปภ. ไม่ใช่ตำรวจเอกชน”

[ความมั่นคงปลอดภัยสาธารณะ
(ตำรวจ/รัฐ)]

- เป้าหมาย: บังคับใช้กฎหมาย อาญาและดูแลความสงบ
- อำนาจ: มีอำนาจตาม ป.วิอาญา ในการสืบสวน, จับกุม, ค้น, ยึด ทรัพย์สิน และพกพาอาวุธปืน



[ความมั่นคงปลอดภัยเอกชน
(รปภ./องค์กร)]

- เป้าหมาย: ป้องกันความสูญเสีย (Loss Prevention)
- ข้อจำกัด: ไม่มีอำนาจจับกุม (เว้นแต่ความผิดซึ่งหน้า)
- การค้น: ไม่มีอำนาจค้นโดยพลการ ต้องอาศัยหลัก “เงื่อนไขการเข้าพื้นที่” (Condition of Entry) สิทธิในการปฏิเสธไม่ให้เข้าพื้นที่ หากไม่ยินยอมให้ตรวจค้น

CONFIDENTIAL

SYSTEM READY...

การบูรณาการร่วมกัน (Public-Private Synergy)

รัฐและเอกชนต้องพึ่งพากันเพื่ออุดช่องโหว่ของระบบ โครงการความร่วมมือที่ประสบความสำเร็จในไทย:



- **Smart Safety Zone 4.0:**

การเชื่อมโยงเครือข่ายกล้อง CCTV ของภาคเอกชน เข้ากับศูนย์บัญชาการตำรวจ ใช้ AI วิเคราะห์ภาพ เพิ่ม “ตา” นับแสนดวงช่วยลดอาชญากรรม

- **Cyber Vaccine:**

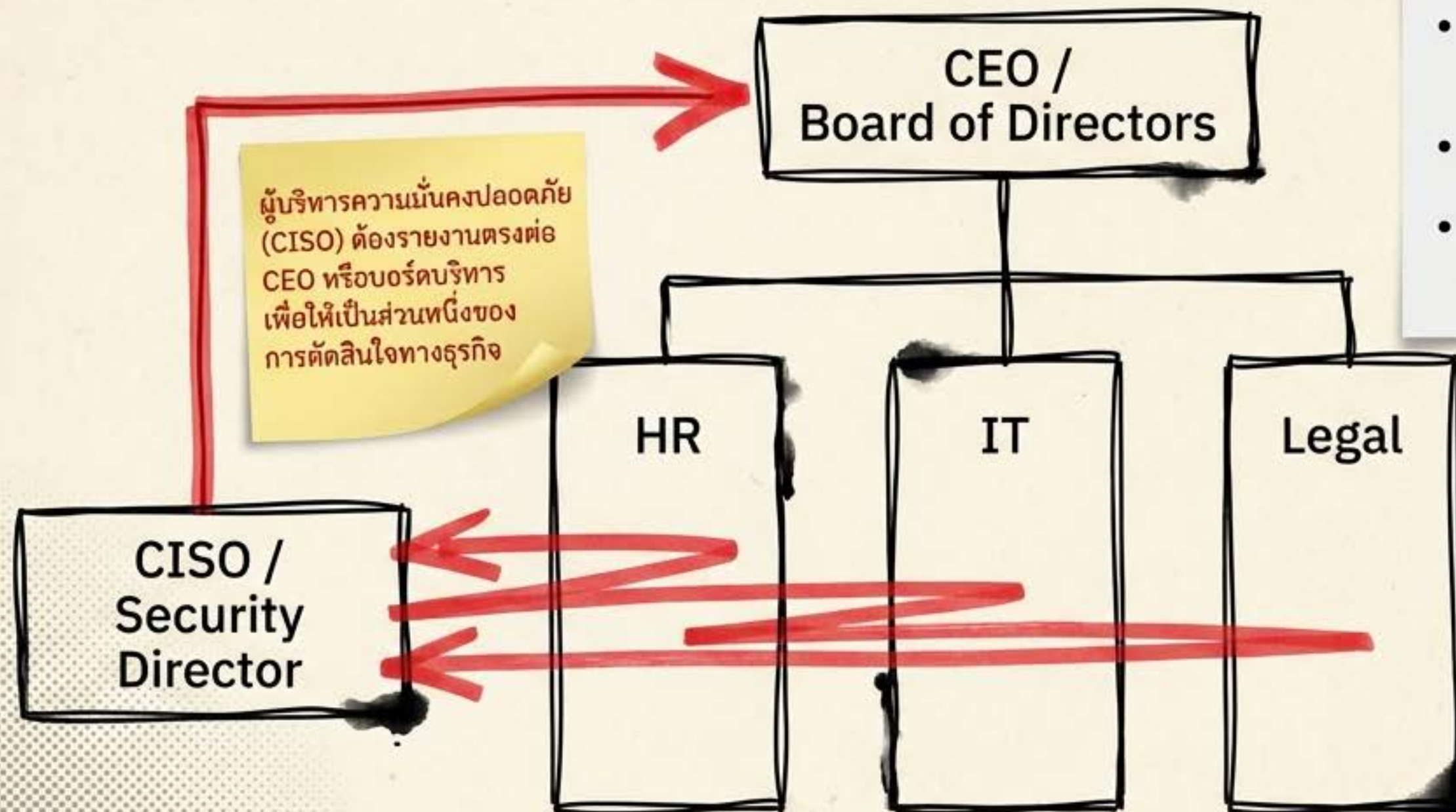
รัฐร่วมมือกับเอกชนเพื่อ “ฉีดวัคซีนทางปัญญา” แจกเตือนหลอกลวง และพัฒนาระบบตรวจสอบ บัญชีม้า ตัดวงจรอาชญากรรมไซเบอร์

CONFIDENTIAL

SYSTEM READY...

บทบาทในองค์กรยุคใหม่ (The Modern Organization)

ความมั่นคงปลอดภัยไม่ใช่แผนกที่โดดเดี่ยว (Silo) อีกต่อไป แต่เป็นฟังก์ชันเชิงกลยุทธ์:



ผู้บริหารความมั่นคงปลอดภัย (CISO) ต้องรายงานตรงต่อ CEO หรือบอร์ดบริหาร เพื่อให้เป็นส่วนหนึ่งของการตัดสินใจทางธุรกิจ

- HR & Security: คัดกรองประวัติพนักงาน ป้องกันภัยคุกคามจากคนใน
- IT & Security: ปกป้องระบบ ภายภาพที่เชื่อมต่อเน็ตเวิร์ก
- Legal & Security: ตรวจสอบการปฏิบัติตาม PDPA และกฎหมายแรงงาน

CONFIDENTIAL

ความท้าทายในบริบทวัฒนธรรมไทย

ทฤษฎีสากลต้องปรับใช้ให้เข้ากับพฤติกรรมท้องถิ่น
(Localization):



[ภัยเงียบ: วัฒนธรรม "เกรงใจ"]

- ปัญหา: รปภ. ไม่กล้าตรวจค้นผู้ใหญ่หรือ VIP (วิศวกรรมสังคม)
- ทางแก้: ผู้บริหารระดับสูงต้องเป็น Role Model ยอมรับการตรวจค้นเพื่อสร้างบรรทัดฐาน "ไม่มีใครอยู่เหนือกฎ"



[เครือข่ายลับ: "วินมอเตอร์ไซด์"]

- ข้อได้เปรียบ: หน่วยข่าวกรองชุมชน (Community Intelligence) ที่ดีที่สุด
- การประยุกต์ใช้: ผู้จัดการต้องสร้างพันธมิตรกับ วินหน้าอาคาร เพื่อช่วยแจ้งเบาะแสบุคคลแปลกหน้า หรือสังเกตการณ์ความผิดปกติที่กล้องมองไม่เห็น

CONFIDENTIAL



CONFIDENTIAL

บทสรุป: นักบริหารความเสี่ยงเชิงกลยุทธ์

การจัดการความมั่นคงปลอดภัยในศตวรรษที่ 21 ไม่ใช่เรื่องของการใช้กำลัง
แต่เป็นเรื่องของ "สติปัญญาและการบริหารจัดการ"

ผู้บริหารความมั่นคงปลอดภัยที่แท้จริงต้อง:

- มองทะลุภาพลวงตาของ "ละครรักษาความปลอดภัย" 
- บุคลากร คน เทคโนโลยี และกฎหมาย อย่างแนบเนียน
- เปลี่ยนบทบาทจาก "ผู้บังคับใช้กฎ" เป็น "ผู้สนับสนุนธุรกิจ" (Business Enabler) 

SYSTEM
APPROVED

"หน้าที่ของคุณคือการทำให้นั่นใจว่าองค์กรจะไม่ล่มสลายเพราะความล้มเหลวเชิงระบบ ไม่ว่าจะเป็นในโลกกายภาพหรือโลกดิจิทัล"