เมื่อจุดอ่อนเพียงจุดเดียวเปลี่ยนแปลงทุกสิ่ง

Jurassic Park (1993): สวนสนุกที่ดูเหมือนสมบูรณ์แบบด้วยเทคโนโลยีล้ำสมัยและรั้วไฟฟ้า 10,000 โวลต์

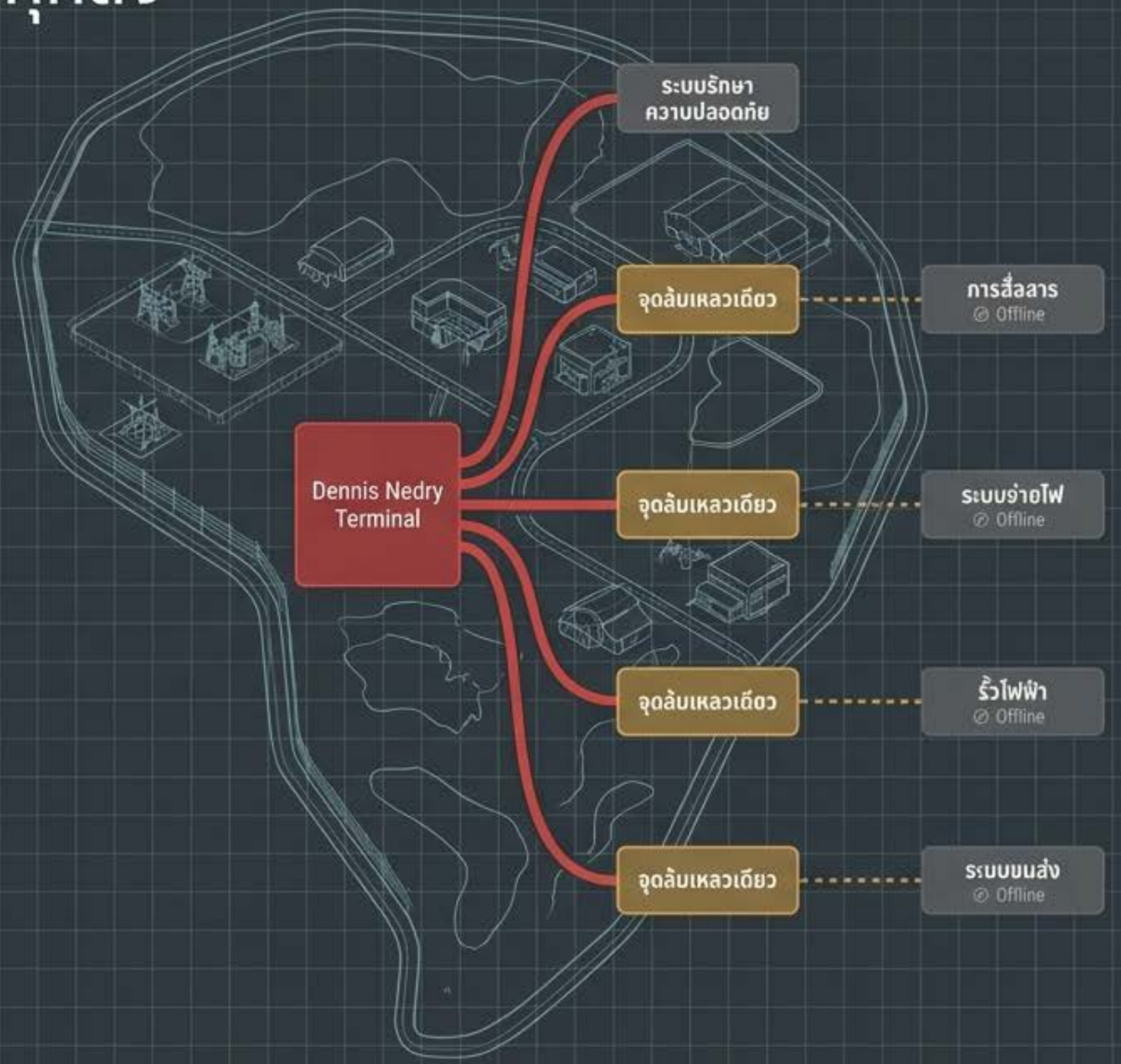
ภัยคุกคามจากคนใน (Insider Threat): Dennis Nedry โปรแกรมเมอร์หลัก ใช้สิทธิ์การเข้าถึงโดยชอบธรรมปิดระบบเพื่อขโมยตัวอ่อนไดโนเสาร์

ความล้มเหลวที่ไหลล้นต่อเนื่อง (Cascading Failure): ตัวแปรที่ไม่คาดคิด (พายุโซนร้อน, อุบัติเหตุรถชน) ทำให้แผน 18 นาทีกลายเป็นหายนะ

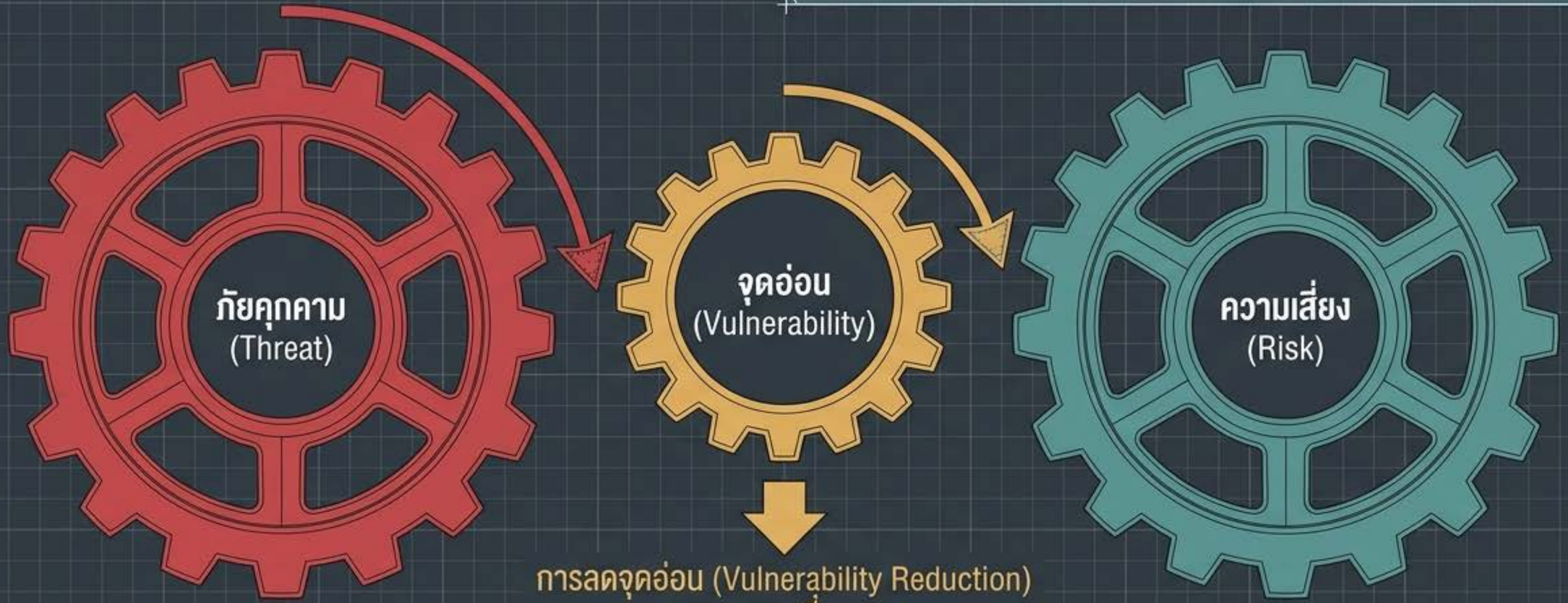
จุดล้มเหลวเดียว (Single Point of Failure): ระบบพังทลายเพราะขาดระบบสำรองและพึ่งพาบุคคลเพียงคนเดียว

บทเรียนสำคัญ: ภัยคุกคามไม่ได้กลายเป็นหายนะด้วยตัวมันเอง แต่มันต้องอาศัยการเจาะผ่านจุดอ่อนของระบบ

Think About It: ภัยคุกคามที่ร้ายแรงที่สุดของสวนสนุกแห่งนี้คือ T-Rex หรือความไว้วางใจที่มอบให้พนักงานเพียงคนเดียวโดยไม่มีการตรวจสอบ?



เป้าหมายหลัก: ผู้จัดการไม่สามารถกำจัดภัยคุกคามได้ทั้งหมด ต้องเน้นการลดจุดอ่อน



การลดจุดอ่อน (Vulnerability Reduction)
= ลดความเสี่ยงรวม

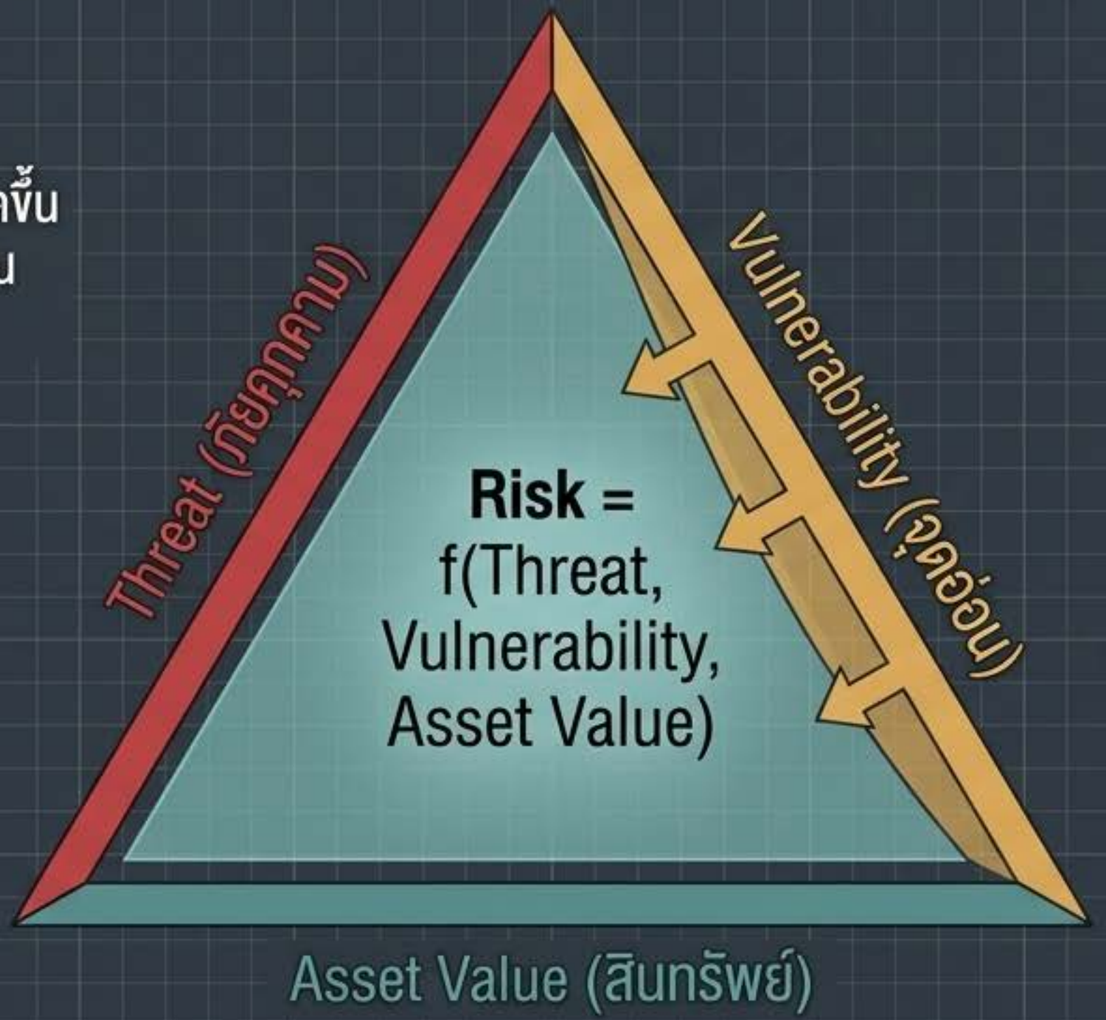
แหล่งกำเนิดของอันตรายที่อาจเกิดขึ้น (เป็นพลวัต ควบคุมไม่ได้โดยตรง เช่น พายุ หรือ แฮกเกอร์)	ช่องโหว่หรือความบกพร่องทางระบบ กายภาพ หรือมนุษย์ ที่ภัยคุกคามสามารถใช้ประโยชน์ได้	โอกาส (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้นเมื่อภัยคุกคาม เจาะผ่านจุดอ่อนได้สำเร็จ

Think About It: ทำไมฝนตกหนักที่สุดในรอบ 300 ปีจึงถูกมองว่าเป็น ‘ภัยคุกคาม’ แต่ระบบท่อระบายน้ำที่ล้าสมัยกลับถูกมองว่าเป็น ‘จุดอ่อน’?

สามเหลี่ยมความเสี่ยงด้านความปลอดภัย

เหตุการณ์ด้านความปลอดภัยจะเกิดขึ้นเมื่อองค์ประกอบทั้งสามบรรจบกันในเวลาและสถานที่เดียวกัน

ภัยคุกคามเดียวกันสร้างความเสี่ยงต่างกัน ขึ้นอยู่กับความพร้อมขององค์กร



แรนซัมแวร์โจมตีโรงพยาบาลที่ไม่มีข้อมูลสำรอง = ความเสี่ยงสูง

แรนซัมแวร์โจมตีโรงพยาบาลที่มีระบบสำรองออฟไลน์ = ความเสี่ยงต่ำ

การจัดสรรทรัพยากรต้องอิงตามความสำคัญและมูลค่าของสินทรัพย์ที่ถูกคุกคาม

Think About It: หากสินทรัพย์ไม่มีมูลค่าเลย ภัยคุกคามที่ร้ายแรงต่อสินทรัพย์นั้นจะยังถือว่าเป็นความเสี่ยงด้านความปลอดภัยหรือไม่?

การจัดประเภทของภัยคุกคาม

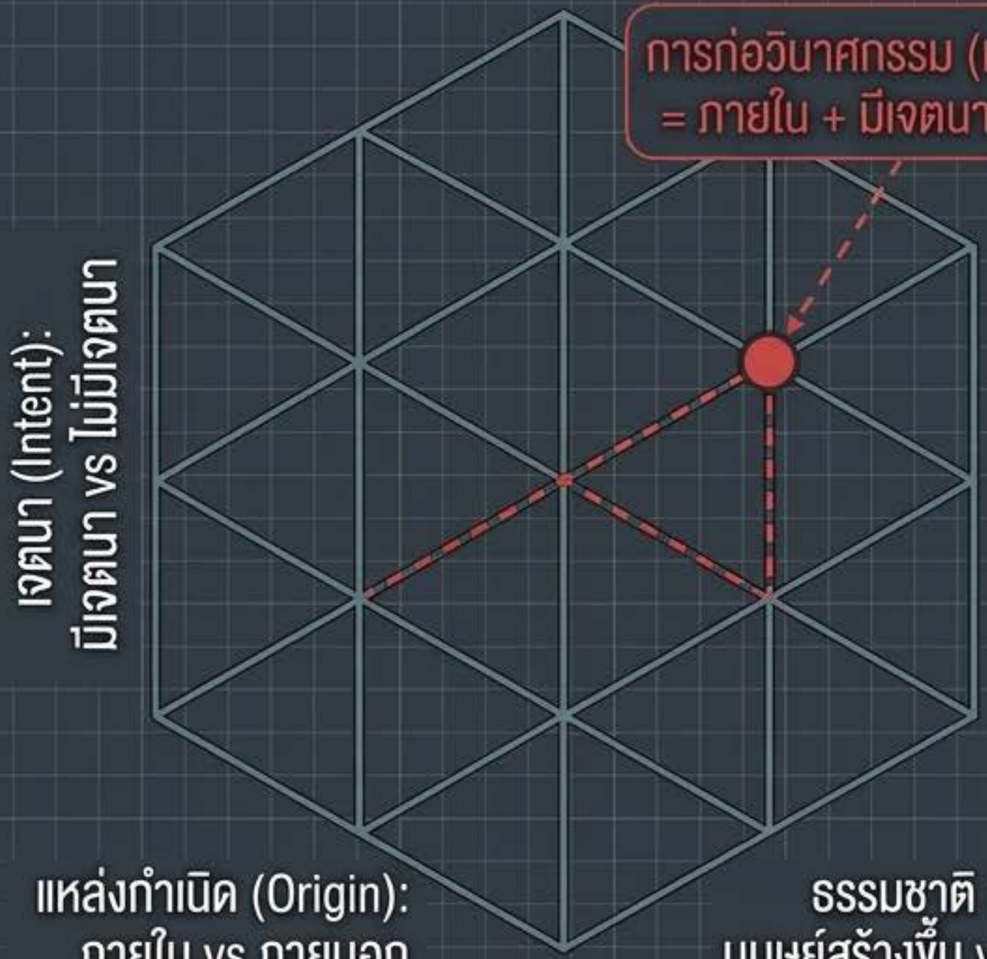
การประเมินความเสี่ยงที่ครอบคลุมต้องเริ่มจากการจัดหมวดหมู่ภัยคุกคามอย่างเป็นระบบ

Origin: พนักงาน, ผู้รับเหมา (ภายใน) หรือ แฮกเกอร์, พายุ (ภายนอก)

Intent: การก่อวินาศกรรม, โจรกรรม (มีเจตนา) หรือ อุบัติเหตุ, ความผิดพลาดของมนุษย์ (ไม่มีเจตนา)

Nature: การก่อการร้าย, ฉ้อโกง (มนุษย์สร้างขึ้น) หรือ น้ำท่วม, แผ่นดินไหว (ภัยธรรมชาติ)

ภูมิทัศน์ภัยคุกคามขึ้นอยู่กับบริบท (Context-dependent) เช่น ภัยของธนาคารย่อมต่างจากภัยของชาวประมงพื้นบ้าน



Think About It: คุณจะจัดประเภทของพนักงานที่เผลอเอาของหนีบประตูห้องเซิร์ฟเวอร์ทิ้งไว้ให้อยู่ในหมวดหมู่ใด?

ภัยคุกคามภายนอก

เกิดจากภายนอกขอบเขตการควบคุมขององค์กร และผู้กระทำไม่มีสิทธิ์เข้าถึงตั้งแต่แรก

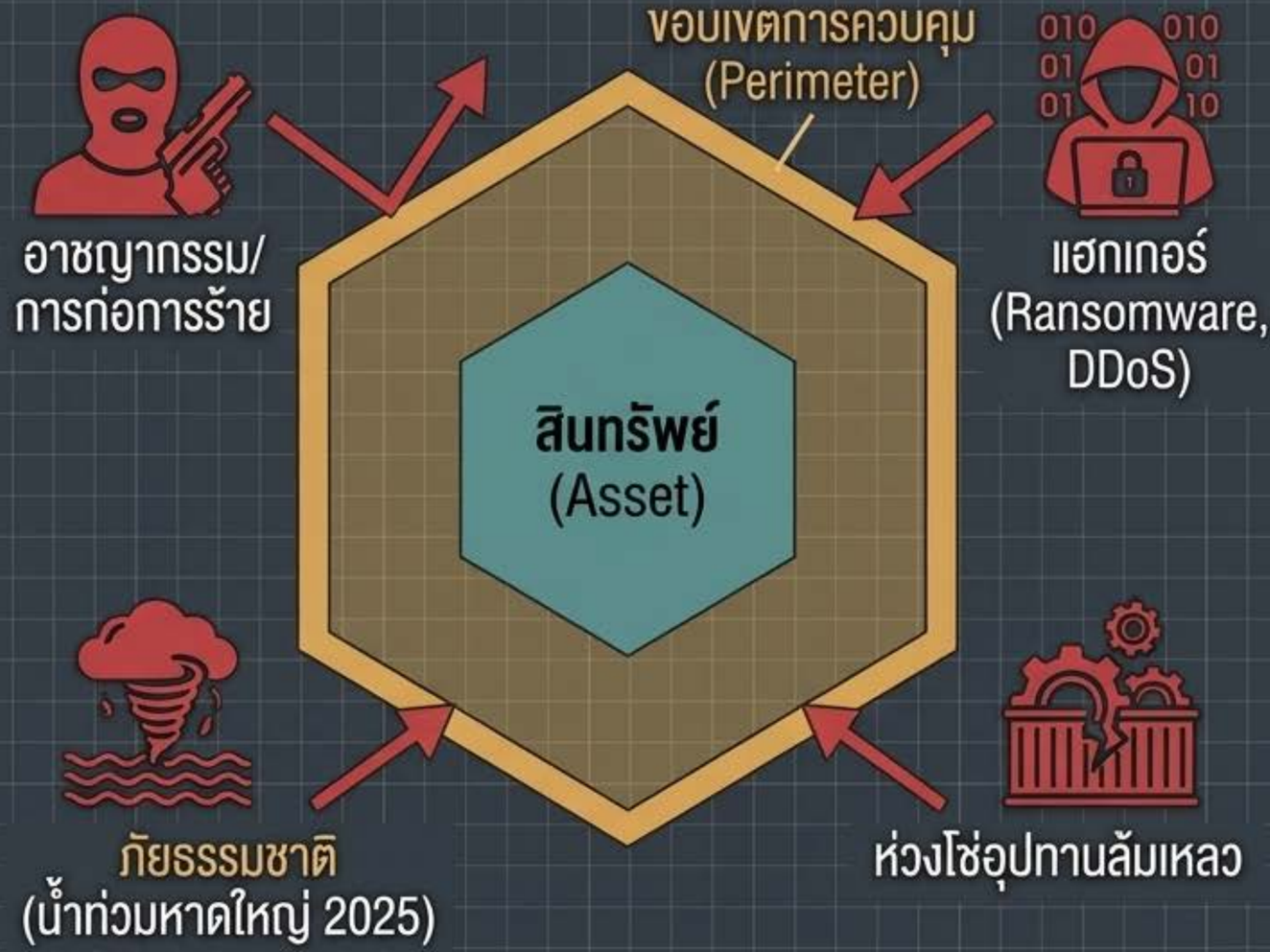
อาชญากรรม/การก่อการร้าย: โจรกรรม, การบุกรุก, หรือความรุนแรงเชิงอุดมการณ์

ภัยคุกคามไซเบอร์: มัลแวร์เรียกค่าไถ่ (Ransomware), ฟิชชิ่ง, และ DDoS จากภายนอก

ภัยธรรมชาติ: เช่น เหตุการณ์น้ำท่วมใหญ่หาดใหญ่ (พ.ย. 2025) ที่กระทบ 1.2 ล้านครัวเรือน

การหยุดชะงักของห่วงโซ่อุปทาน: ความล้มเหลวในเครือข่ายผู้ผลิตหรือระบบโลจิสติกส์

ภัยภายนอกคาดการณ์ได้ง่ายกว่าแต่ป้องกันได้ยาก เนื่องจากความไม่แน่นอนของเวลาและเป้าหมาย



Think About It: ทำไมภัยคุกคามภายนอกมักจะมองเห็นและคาดการณ์ได้ง่ายกว่า แต่กลับป้องกันให้เบ็ดเสร็จได้ยากกว่าภัยคุกคามภายใน?

ภัยคุกคามภายใน

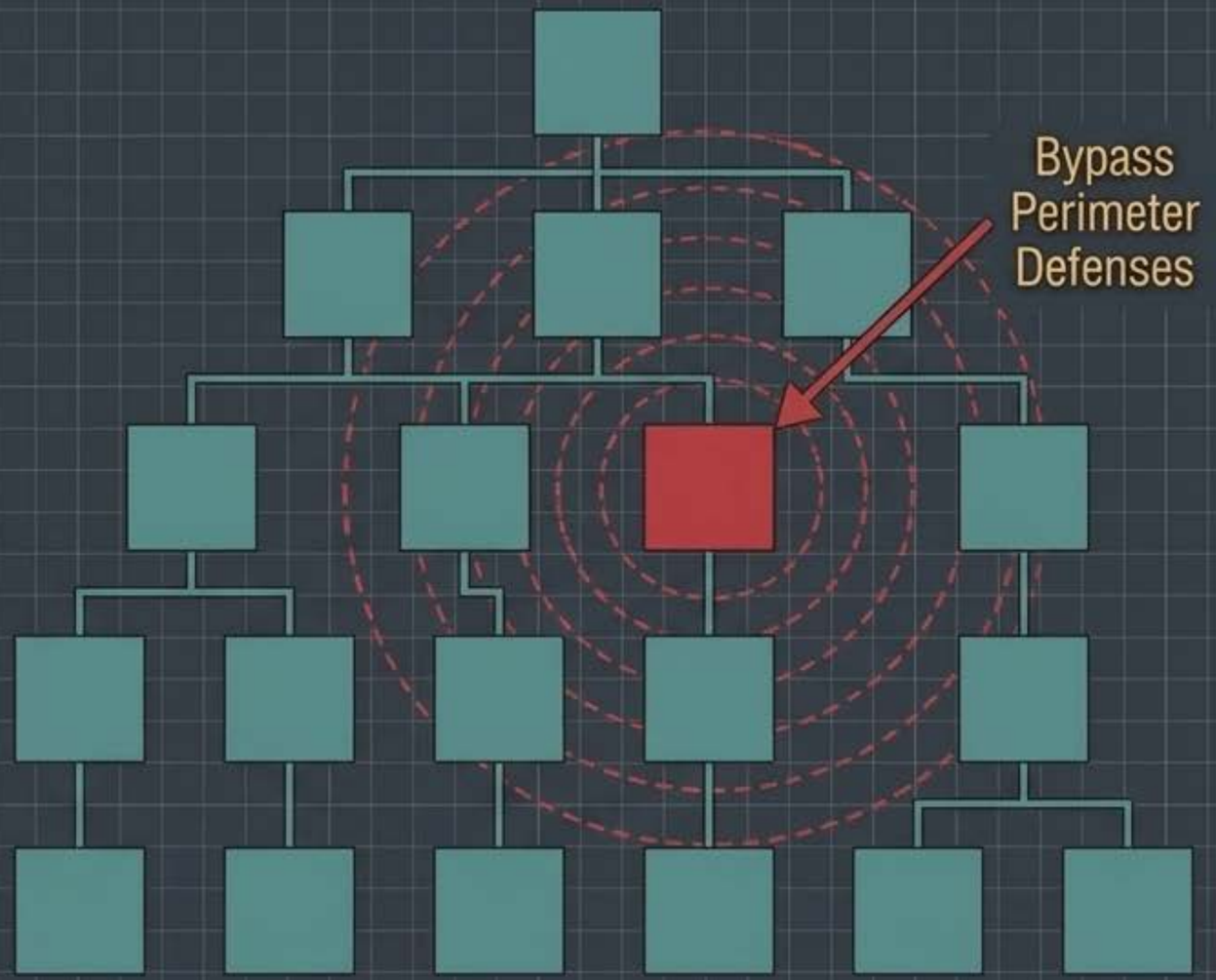
เกิดจากบุคคลที่มี “สิทธิ์ในการเข้าถึง” (Authorized Access) และมีความรู้ในระบบ

การกระทำโดยมุ่งร้าย (Malicious): การก่อวินาศกรรม, ขโมยทรัพย์สินทางปัญญา, ทุจริตโดยพนักงาน

ความประมาท (Negligence): 90% ของการละเมิดความปลอดภัยไซเบอร์เกิดจากความผิดพลาดของมนุษย์

การละเมิดนโยบาย (Policy Violations): การหาทางลัดเพื่อความสะดวก เช่น Shadow IT หรือการแชร์รหัสผ่าน

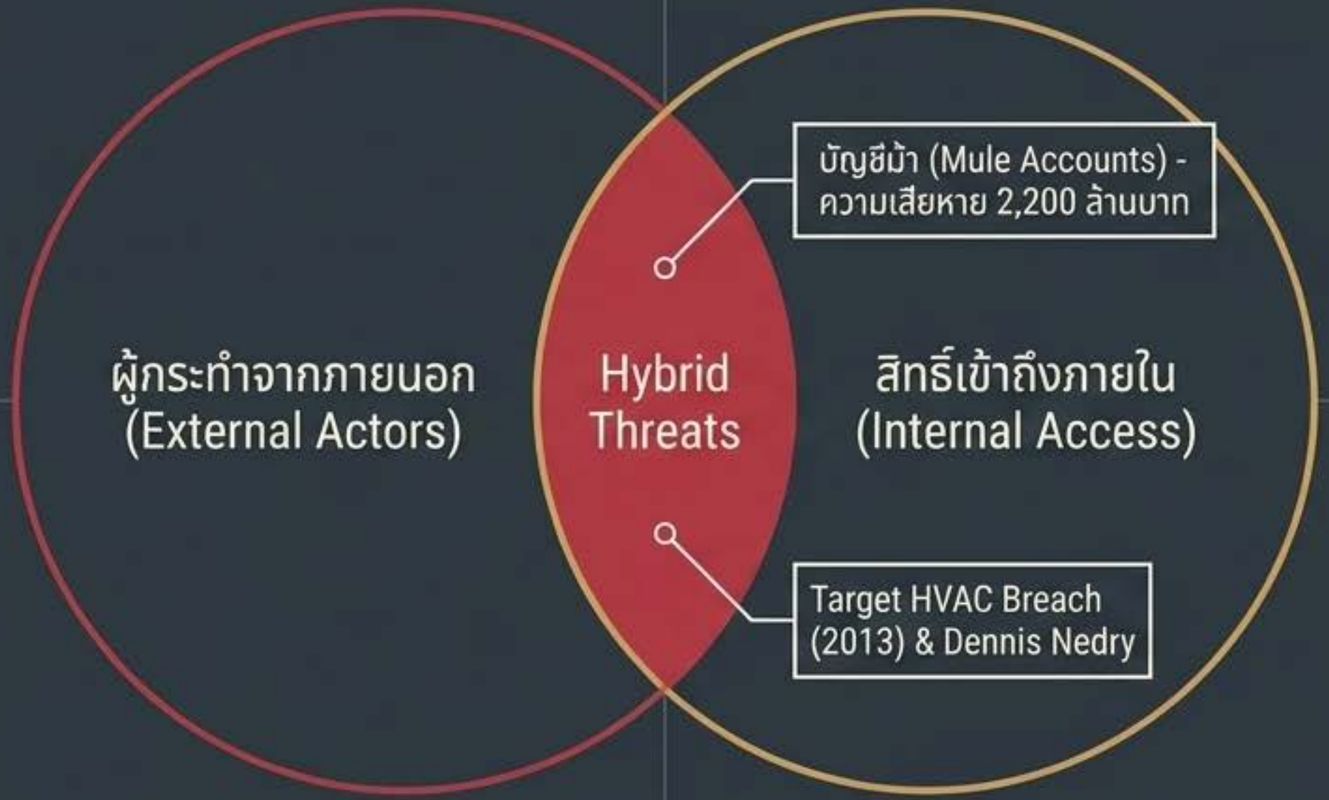
ภัยคุกคามภายในอันตรายที่สุดเพราะไม่ต้องเจาะระบบป้องกันจากภายนอก



Think About It: การออกแบบระบบของ Jurassic Park ละเลยความเป็นจริงเกี่ยวกับความอันตรายของภัยคุกคามภายในอย่างไร?

ภัยคุกคามแบบผสมผสาน

ภัยคุกคามสมัยใหม่มักทำให้เส้นแบ่งระหว่างภายในและภายนอกเลือนลางลง



วิศวกรรมสังคม (Social Engineering): แฮกเกอร์ภายนอกหลอกลวงพนักงานภายในเพื่อให้ได้สิทธิ์เข้าถึง

การโจมตีห่วงโซ่อุปทาน (Supply Chain Attacks): การเจาะระบบผ่านผู้รับเหมาที่องค์กรไว้วางใจ

การสมรู้ร่วมคิด (Collusion): คนในร่วมมือกับอาชญากรภายนอก (เช่น พนักงานธนาคารเปิดบัญชีม้าให้แก๊งคอลเซ็นเตอร์)

องค์กรต้องบูรณาการการป้องกันรอบนอกเข้ากับการตรวจสอบพฤติกรรมภายในอย่างแนบเนียน

Think About It: หากพนักงานถูกหลอกให้บอกรหัสผ่านผ่านอีเมลฟิชชิ่ง เหตุการณ์นี้ถือเป็นภัยคุกคามจากภายในหรือภายนอก?

ภัยคุกคามโดยเจตนาและไม่เจตนา

ภัยคุกคามโดยเจตนา (Intentional) 	**ภัยคุกคามโดยไม่เจตนา (Unintentional)** 
มีเป้าหมายชัดเจน ปรับตัวได้ และพยายามหลบหลีกระบบป้องกัน	เกิดจากอุบัติเหตุ ความล้มเหลวของระบบ หรือภัยธรรมชาติ
เช่น อาชญากรรมไซเบอร์ 3,180 ครั้ง/สัปดาห์ในไทย	บ่อยครั้งสร้างความเสียหายรวมมากกว่าการก่อวินาศกรรม (เช่น น้ำท่วมหาดใหญ่)
กลยุทธ์รับมือ: เน้นข่าวกรองเชิงรุก การป้องปราม และการควบคุมการเข้าถึง	**กลยุทธ์รับมือ:** เน้นความซ้ำซ้อน (Redundancy) ป้องกันความผิดพลาด (Poka-yoke) และแผนฟื้นฟู

Think About It: ระบบเซิร์ฟเวอร์ล่มเพราะขาดการบำรุงรักษาอย่างต่อเนื่อง ควรนับเป็นอุบัติเหตุทางธรรมชาติหรือความประมาทของมนุษย์?

อาชญากรรมในฐานะภัยคุกคาม

- อาชญากรรมพื้นฐานรบกวนการดำเนินงานและส่งผลกระทบโดยตรงต่อผลกำไรขององค์กร
- **ประเภท**: ลักทรัพย์, บุกรุก, ปล้นทรัพย์, ฉ้อโกง, และการทำลายทรัพย์สิน
- อาชญากรรมมักเกิดขึ้นตาม 'กิจวัตรประจำวัน' ที่คาดเดาได้ (เช่น เวลาเปลี่ยนกะ, วันนำเงินสดฝากธนาคาร)
- **ทฤษฎีกิจวัตรประจำวัน** (Routine Activity Theory): ผู้กระทำผิดที่มีแรงจูงใจ + เป้าหมายที่เหมาะสม - ผู้พิทักษ์ที่เพียงพอ
- **เป้าหมายผู้จัดการความปลอดภัย:** ต้องขัดจังหวะกิจวัตรเหล่านี้เพื่อลบโอกาสในการก่ออาชญากรรม

Think About It: กิจวัตรขององค์กร (เช่น การเปลี่ยนกะ รปภ. เวลา 18:00 น. ตรงทุกวัน) สร้างหน้าต่างแห่งโอกาสให้ช่องโหว่อย่างไร?

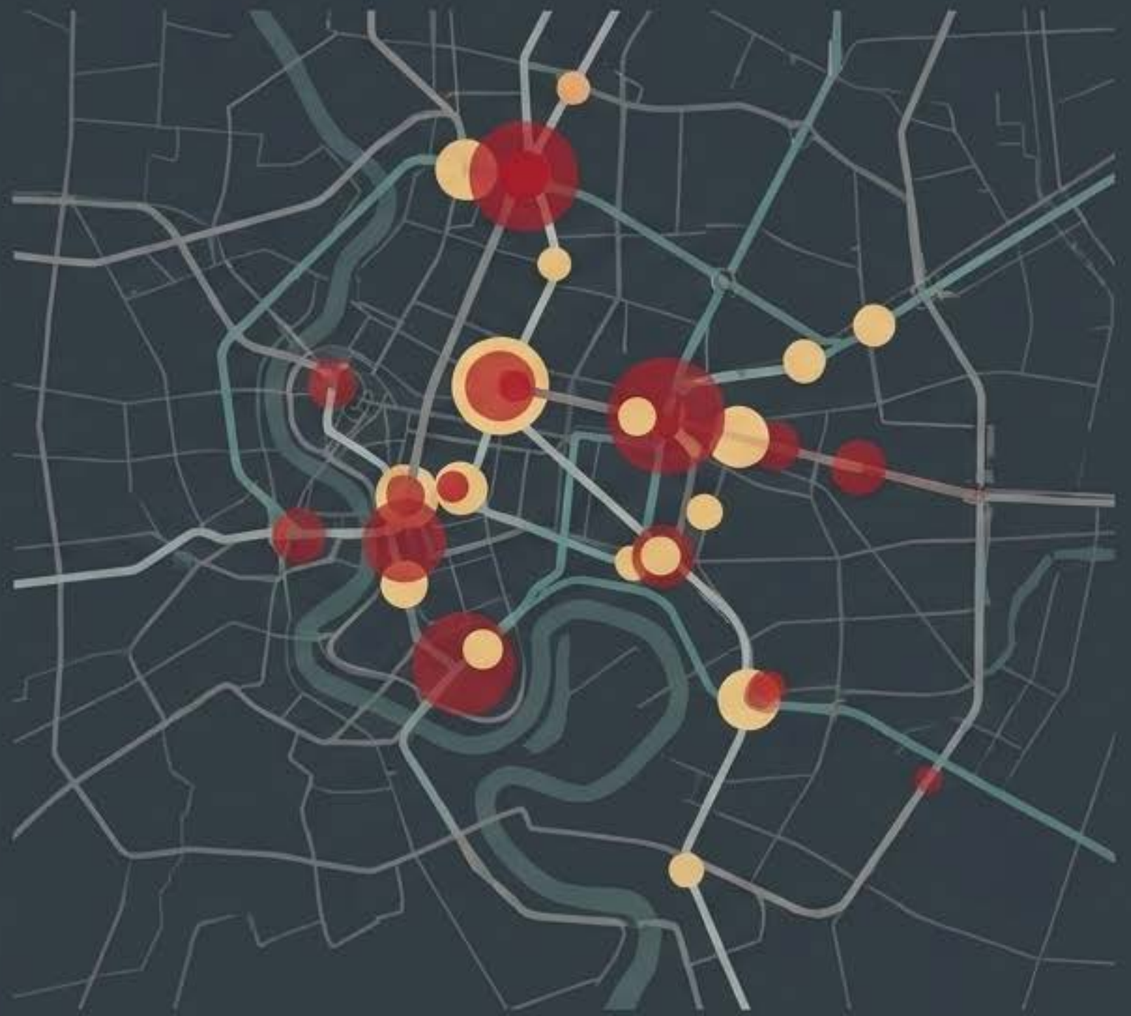
The Routine Activity Theory Triangle

การวิเคราะห์อาชญากรรม

เปลี่ยนข้อมูลดิบ (Raw Data) ให้กลายเป็นข่าวกรอง (Actionable Intelligence)

- **รูปแบบและแนวโน้ม** (Patterns & Trends): ระบุลักษณะที่เกิดขึ้นซ้ำและการเปลี่ยนแปลงตามเวลา
- **จุดเสี่ยง** (Hot Spots): การกระจุกตัวทางภูมิศาสตร์ (เช่น การล้วงกระเป๋าตามสถานีรถไฟฟ้าที่มีนักท่องเที่ยวหนาแน่น)
- **พฤติการณ์กระทำผิด** (Modus Operandi - MO): เชื่อมโยงอาชญากรรมหลายเหตุการณ์เข้ากับผู้ก่อเหตุคนเดียวกันผ่านเอกลักษณ์การลงมือ
- **ผลลัพธ์:** ช่วยให้ผู้จัดการจัดสรรทรัพยากรที่มีจำกัดได้อย่างแม่นยำ แทนที่จะใช้การคาดเดา

Think About It: ทำไมการสร้างแผนที่ระบุ ‘เวลา’ และ ‘สถานที่’ ที่เกิดเหตุ จึงมีประสิทธิภาพกว่าการแค่นับจำนวน ‘สถิติ’ อาชญากรรมทั้งหมด?



3 ระดับของการวิเคราะห์อาชญากรรม

แผนคความปลอดภัยที่มีประสิทธิภาพสูงสุด
จะต้องใช้การวิเคราะห์ทั้งสามระดับควบคู่กัน

	กรอบเวลา (Time Horizon)	**วัตถุประสงค์** (Purpose)	**ผู้รับสารหลัก** (Audience)
เชิงยุทธวิธี (Tactical)	ระยะสั้น (วัน/สัปดาห์)	หยุดยั้งซีรีส์อาชญากรรมเฉพาะหน้า (เช่น จัด รปภ. นอกเครื่องแบบลงพื้นที่ Hot spot ทันที)	ทีมปฏิบัติการ, รปภ.
เชิงกลยุทธ์ (Strategic)	ระยะยาว (เดือน/ปี)	ค้นหาสาเหตุรากฐานและกำหนดนโยบาย (เช่น วิเคราะห์เทรนด์จักรยานหายช่วงเปิดเทอม)	ผู้จัดการความปลอดภัย, ผู้วางนโยบาย
เชิงบริหารงาน (Administrative)	รอบการรายงาน (ไตรมาส/ปี)	เน้นการรายงาน การปฏิบัติตามกฎหมาย และการขออนุมัติงบประมาณ	ผู้บริหารระดับสูง, บอร์ดบริหาร, CEO

Think About It: หากคุณต้องนำเสนอ CEO เพื่อขอเพิ่มงบประมาณความปลอดภัยประจำปีอีก 2 เท่า คุณจะใช้การวิเคราะห์ประเภทใด?

การก่อการร้ายและความรุนแรงทางการเมือง

ขับเคลื่อนด้วยอุดมการณ์การเมือง หรือศาสนามากกว่าผลประโยชน์ทางการเงิน

บริบทประเทศไทย: ความไม่สงบในชายแดนภาคใต้หลอมรวมเข้ากับเครือข่ายธุรกิจมืด (การค้ายา, การลักลอบขนส่ง) ทำให้เส้นแบ่งอาชญากรเลือนลาง

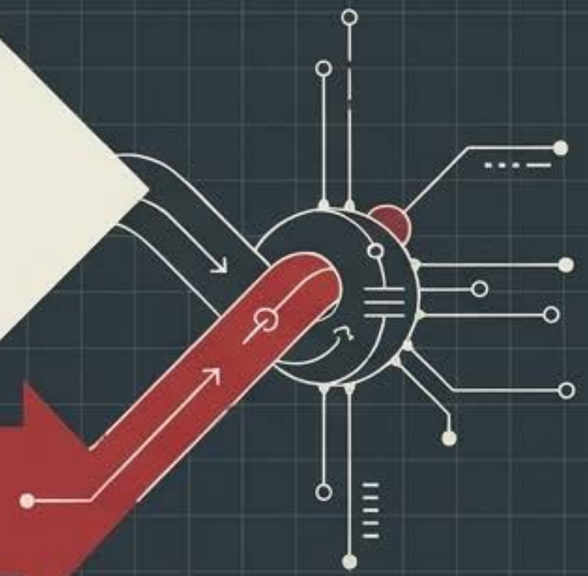
เป้าหมายปัจจุบันคือระบบขนส่งมวลชน โครงสร้างพื้นฐาน และหน่วยงานรัฐ ต้องการการบูรณาการระหว่างข่าวกรองเชิงรุกและการควบคุมการเข้าถึงทางกายภาพอย่างเข้มงวด

Think About It: การหลอมรวมระหว่างความรุนแรงทางการเมืองกับเครือข่ายอาชญากรรมผิดกฎหมาย ทำให้การวิเคราะห์ความปลอดภัยซับซ้อนขึ้นอย่างไร?

อดีต: Broad Mass Casualty
(การสร้างความเสียหายวงกว้าง)

ปัจจุบัน/อนาคต: Precision, Symbolic & Cyber Disruption
(ความแม่นยำสูงและเป้าหมายเชิงสัญลักษณ์)

เครือข่ายธุรกิจมืด
(Illicit Networks)



ภูมิทัศน์ภัยคุกคามทางไซเบอร์

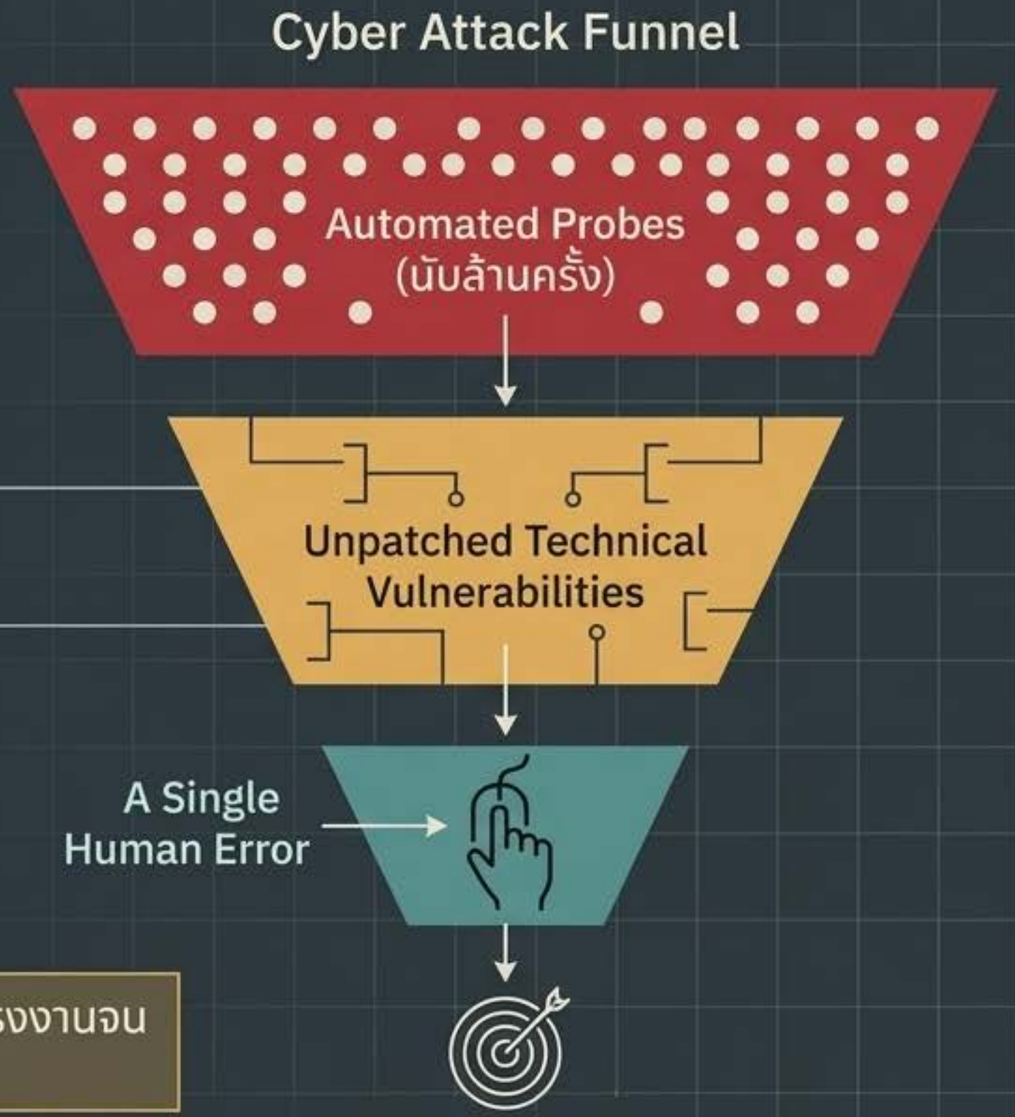
ภัยคุกคามทางไซเบอร์ไร้พรมแดน ขยายผลได้รวดเร็ว (Scalable) และปรับตัวได้ตลอดเวลา

รูปแบบหลัก: ฟิชชิ่ง, แรนซัมแวร์ (Ransomware), DDoS, และช่องโหว่ของ API/Cloud

สถานการณ์ในไทย: เผชิญการโจมตี 3,180 ครั้ง/สัปดาห์ (สูงกว่าค่าเฉลี่ยโลก 70%) พุ่งเป้าไปที่ระบบเก่าและ SME

การผสาน IT และ OT: การโจมตีไซเบอร์สามารถสร้างความเสียหายทางกายภาพได้แล้ว (เช่น สั่งดับโครงข่ายไฟฟ้า)

ความจริงที่สำคัญ: มากกว่า 90% ของการเจาะระบบสำเร็จเริ่มต้นที่ความผิดพลาดของมนุษย์ (วิศวกรรมสังคม)



Think About It: หากแฮกเกอร์เจาะระบบเพื่อปิดพัดลมระบายอากาศของโรงงานจนเครื่องจักรพัง ถือเป็นภัยคุกคามไซเบอร์หรือภัยคุกคามทางกายภาพ?

ภัยคุกคามจากคนใน

กุญแจ 3 ดอกของคนใน: ถือครอง สิทธิ์การเข้าถึง (Access), ความไว้วางใจ (Trust), และความรู้ในระบบ (System Knowledge)

ประเภท: ผู้มุ่งร้าย (Sabotage), ผู้ประมาท (Negligent), และผู้ถูกเจาะบัญชี (Compromised)

Jurassic Park ล่มสลายเพราะ Nedry มีสิทธิ์แบบ God Mode โดยปราศจากการตรวจสอบซ้ำซ้อน (Redundancy)

บริบทวัฒนธรรมไทย: ระบบอาวุโส ความ 'เกรงใจ' และวัฒนธรรมอุปถัมภ์ มักทำให้พนักงานไม่กล้าตรวจสอบผู้บริหาร สร้างช่องโหว่ขนาดใหญ่

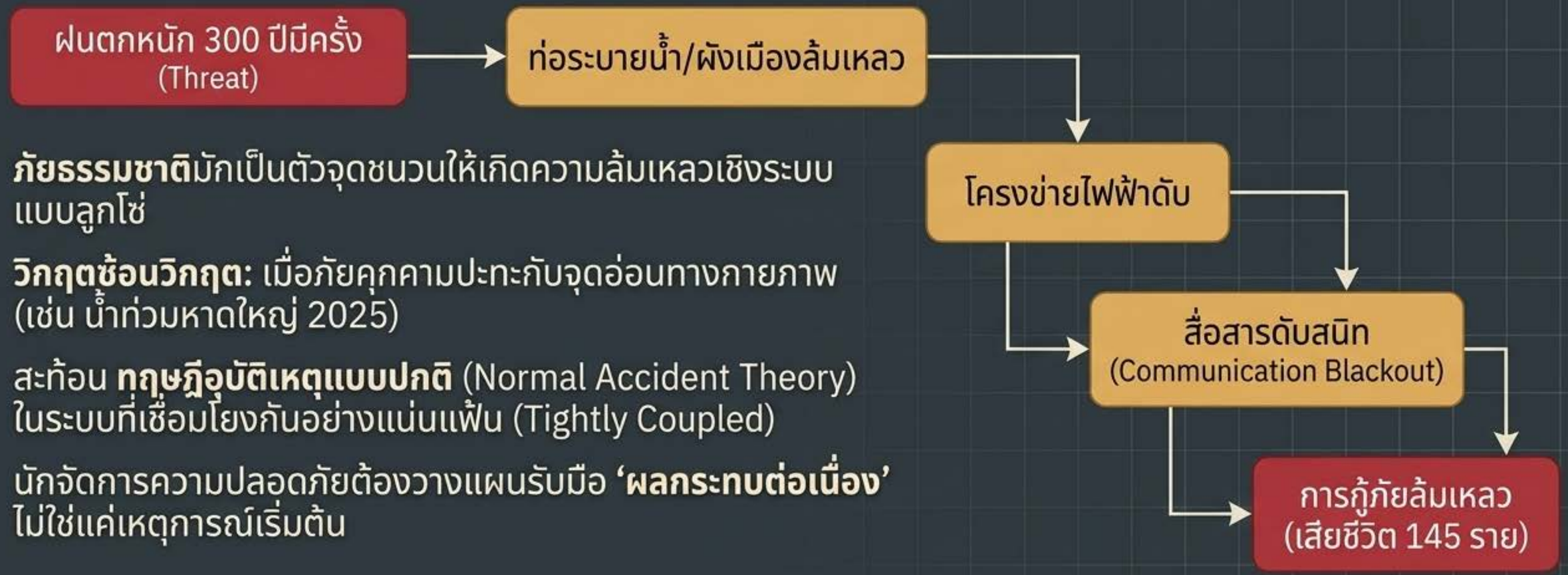
การแก้ไข: ต้องบังคับใช้หลักการให้สิทธิ์น้อยที่สุด (Least Privilege) และการแบ่งแยกหน้าที่อย่างเด็ดขาด

Think About It: วัฒนธรรมองค์กรที่มีความไว้วางใจส่วนบุคคลสูง ทำให้องค์กรปลอดภัยขึ้น หรือสร้างช่องโหว่ให้ภัยคุกคามภายในมากขึ้น?

Access Matrix

	System Core		Financial Data		Personnel Records		Personnal Records		Network Control		Segregation of Duties
	Read	Write	Read	Write	Read	Write	Read	Write	Execute	Admin	
Excessive Privilege (ช่องโหว่)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Least Privilege (ปลอดภัย)			✓	✓			✓	✓			✓

ภัยธรรมชาติและภาวะฉุกเฉินซับซ้อน



ภัยธรรมชาติมักเป็นตัวจุดชนวนให้เกิดความล้มเหลวเชิงระบบแบบลูกโซ่

วิกฤตซ้อนวิกฤต: เมื่อภัยคุกคามปะทะกับจุดอ่อนทางกายภาพ (เช่น น้ำท่วมหาดใหญ่ 2025)

สะท้อน **ทฤษฎีอุบัติเหตุแบบปกติ** (Normal Accident Theory) ในระบบที่เชื่อมโยงกันอย่างแน่นแฟ้น (Tightly Coupled)

นักจัดการความปลอดภัยต้องวางแผนรับมือ **'ผลกระทบต่อเนื่อง'** ไม่ใช่แค่เหตุการณ์เริ่มต้น

Think About It: หากมีระบบสื่อสารและไฟฟ้าสำรองที่แยกอิสระจากส่วนกลาง น้ำท่วมหาดใหญ่จะกลายเป็นวิกฤตซ้อนวิกฤตหรือไม่?

การทำความเข้าใจจุดอ่อน

จุดอ่อนไม่ทำอันตรายด้วยตัวมันเอง
แต่เป็นช่องโหว่ที่รอให้ภัยคุกคามเข้ามาฉกฉวย

การประเมินจุดอ่อนเป็นกระบวนการ
‘มองเข้าไปภายใน’ อย่างตรงไปตรงมา

ช่องโหว่ทั้งหมดเชื่อมโยงกัน:
วัฒนธรรมองค์กรที่หละหลวมนำไปสู่
ความประมาทของมนุษย์
ซึ่งก่อให้เกิดความล้มเหลวทางเทคโนโลยี

Think About It: ทำไมจุดอ่อนทางองค์กรและวัฒนธรรมจึงมักแก้ไขได้ยากที่สุด ทั้งที่แทบไม่ต้องใช้งบประมาณทางการเงินเลย?

การประเมินจุดอ่อน (Vulnerability Assessment)

ขั้นตอนที่ 1: อะไรคือสิ่งที่มีมูลค่าสูงสุดและส่งผลต่อความอยู่รอดขององค์กร?

ขั้นตอนที่ 4: อัปเดตแพตช์, ปรับปรุงสถาปัตยกรรม, แก้ไขนโยบาย, หรือฝึกอบรมพนักงาน

ขั้นตอนที่ 2: ระบบป้องกันของเรากำลังบกพร่องที่จุดใด? (Physical, Technical, Human, Org)

ขั้นตอนที่ 3: ภัยคุกคามประเภทใดบ้างที่สามารถเจาะผ่านช่องโหว่นี้ได้?

ต้องทำผสานกันทั้งการตรวจประเมินหน้างานจริง (Physical Audits) และการทำ Penetration Testing

Think About It: หากองค์กรจัดทำการประเมินจนพบช่องโหว่แล้ว แต่ไม่ยอมลงทุนแก้ไข (Remediation) ถือว่าความปลอดภัยขององค์กรเพิ่มขึ้นหรือไม่?

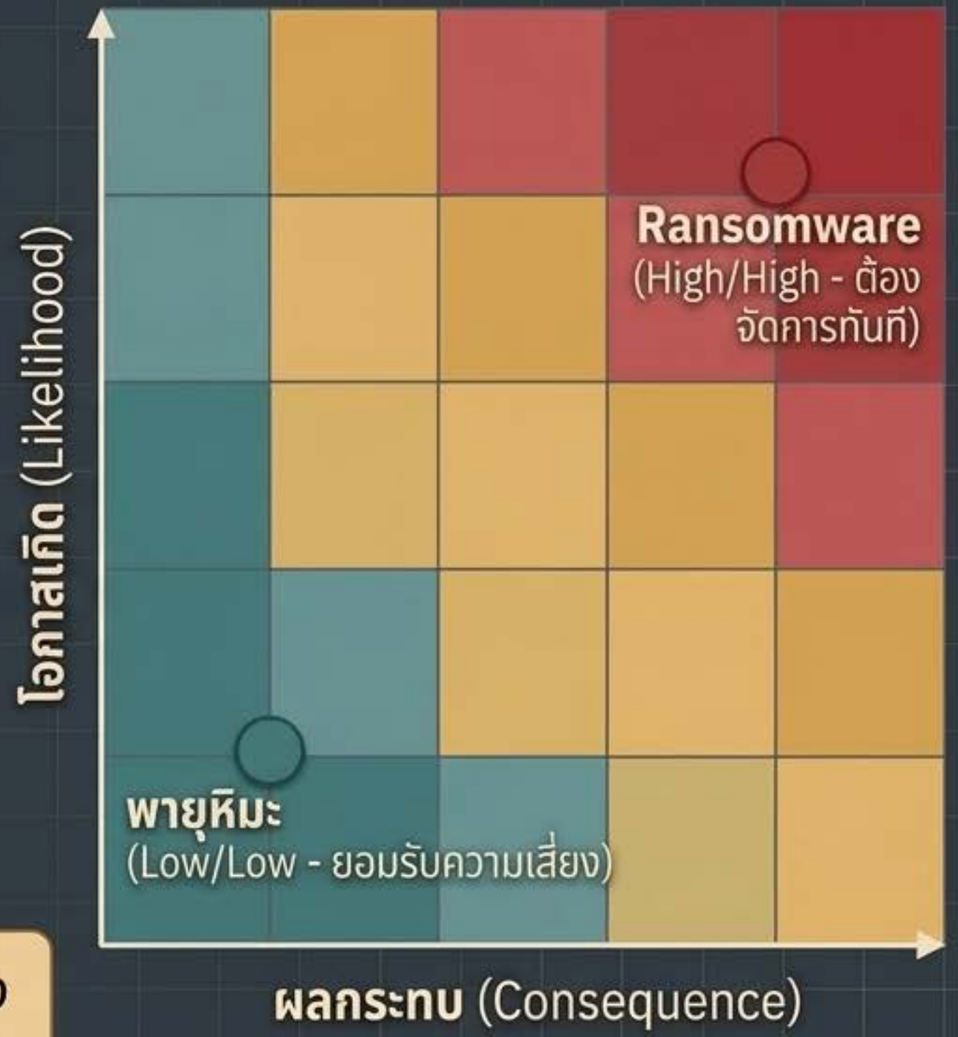
จากจุดอ่อนสู่การจัดลำดับความเสี่ยง

องค์กรมีทรัพยากรจำกัด ไม่สามารถแก้ไขทุกจุดอ่อนได้ทันที จึงต้องมีการจัดลำดับความสำคัญ

สมการ: ความเสี่ยง = โอกาสเกิด (Likelihood) × ผลกระทบ (Consequence)

การจัดลำดับความสำคัญทางคณิตศาสตร์ช่วยเปลี่ยนการตอบสนองจาก **'อารมณ์'** สู่ **'ข้อมูลเชิงประจักษ์'**

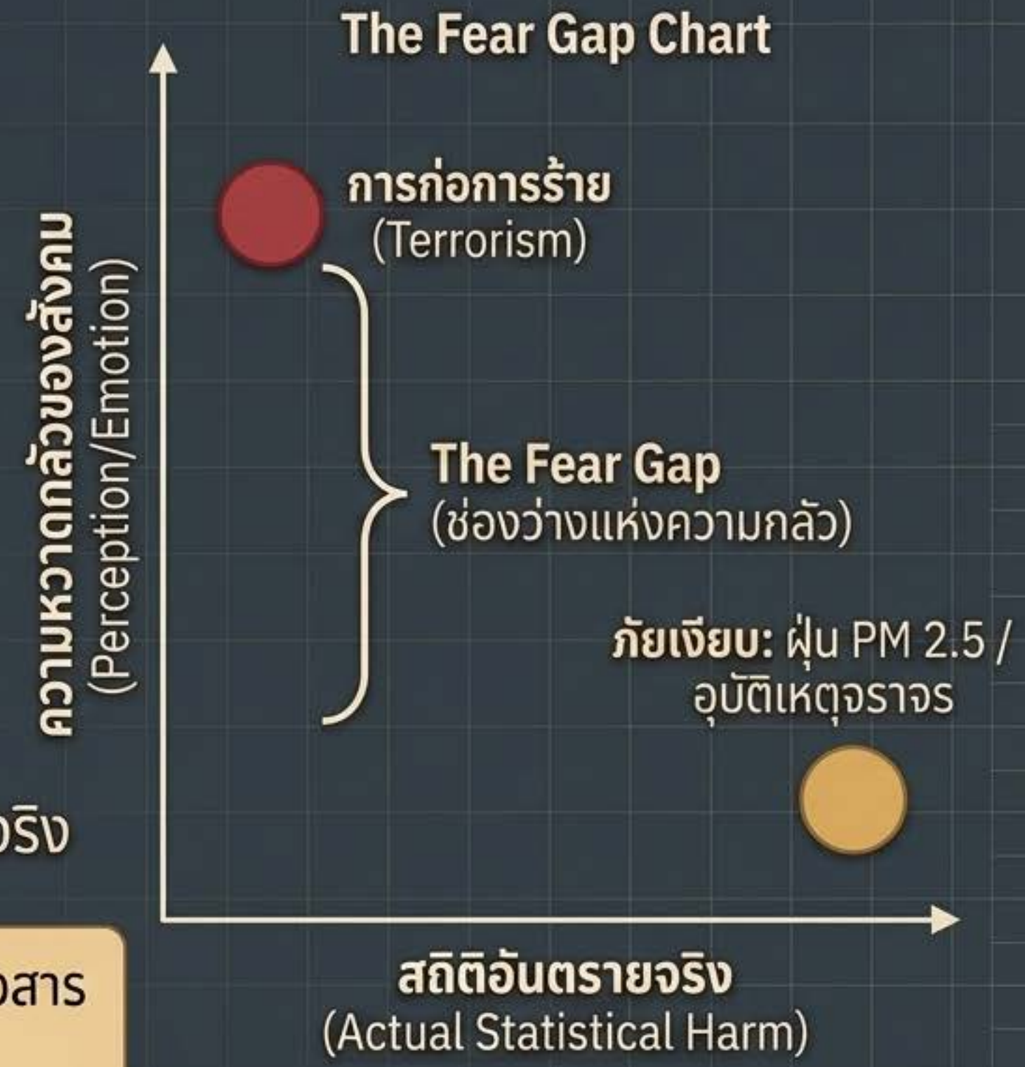
Low/Low = ยอมรับความเสี่ยง หรือเฝ้าระวัง
High/High = ต้องลงทุนลดจุดอ่อนทันที



Think About It: การนำเหตุการณ์มาพล็อตลงบนเมทริกซ์ความเสี่ยงช่วยลดอคติและอารมณ์ในการตัดสินใจของบอร์ดบริหารได้อย่างไร?

ความเสี่ยงที่รับรู้ vs ความเสี่ยงที่แท้จริง

- มนุษย์มักประเมินความเสี่ยงจาก ‘อารมณ์’ (ความน่ากลัว) ไม่ใช่หลักสถิติ
- **ภัยที่ถูกขยาย (Dread Risk):** เหตุการณ์รุนแรงที่มองเห็นชัดเจน ทำให้คนรับรู้ว่าเสี่ยงสูง ร้านโอกาสเกิดต่ำมาก
- **ภัยเงียบ (Silent Threats):** ถูกทำให้เป็นเรื่องปกติ (Normalized) ทำให้ลงทุนป้องกันต่ำ ทั้งที่คร่าชีวิตมหาศาล
- **หน้าที่ของผู้จัดการความปลอดภัย:** ต้องใช้ข้อมูลสถิติ (Evidence-based) เพื่อดึงทรัพยากรกลับมาจัดการภัยที่แท้จริง



Think About It: โซเชียลมีเดียทำให้เราปลอดภัยขึ้นด้วยการกระจายข่าวสาร หรือทำให้เราอันตรายขึ้นจากการบิดเบือนการรับรู้ความเสี่ยง?

กรอบแนวคิดบูรณาการ ภัยคุกคาม-ความเสี่ยง-จุดอ่อน

กรณีศึกษา: วิทยาเขตมหาวิทยาลัยในประเทศไทยช่วงต้นเทอม

ภัยคุกคาม (Threat):
อาชญากรที่ฉวยโอกาส
ขโมยจักรยาน
(ข้อมูลจาก Crime Analysis)

+

จุดอ่อน (Vulnerability):
แสงสว่างไม่เพียงพอใกล้
หอพัก, ขาดกล้อง CCTV,
นศ. ไม่ล็อครถ

→

ความเสี่ยง (Risk):
การโจรกรรมจักรยานสำเร็จ

↓

การลดความเสี่ยง (Mitigation):
ตัดแต่งกิ่งไม้/เพิ่มไฟ (CPTED) + จัด รปภ. เดินเท้า (Tactical)
+ ทำระบบลงทะเบียนรถ (Strategic) = Risk Mitigated

บทสรุป: ความปลอดภัยที่มีประสิทธิภาพคือการเชื่อมโยง
ข่าวกรองภัยคุกคาม → การลดจุดอ่อน → การจัดสรร
ทรัพยากรอย่างตรงจุด

Think About It: คุณจะประยุกต์ใช้กรอบแนวคิดนี้เพื่อแก้ปัญหาความท้าทายด้านความปลอดภัยที่ซับซ้อนในอาชีพของคุณในอนาคตได้อย่างไร?