SMA1202
SECURITY: THEORY AND PRACTICE
หลักการและทฤษฎีความมั่นคงปลอดภัย

CHAPTER 3
THREATS, RISKS, AND VULNERABILITIES

ผศ.ดร.หทัยพันธน์ สุนทรพิพิธ
Asst.Prof.Hathaipan Soonthornpipit, Ph.D.

บทที่ 3

ภัยคุกคาม ความเสี่ยง และจุดอ่อน: การวิเคราะห์ภูมิทัศน์ความมั่นคงปลอดภัยในโลกสมัยใหม่

Threats, Risks, and Vulnerabilities: Analyzing the Security Landscape in the Modern World

1. บทนำ

1.1 บทเรียนจากเกาะล้านปี: เมื่อจุดอ่อนเพียงจุดเดียวเปลี่ยนแปลงทุกสิ่ง (When One Weak Link Changes Everything)

ในประวัติศาสตร์ภาพยนตร์ฮอลลีวูด คงไม่มีเรื่องใดที่ฉายภาพความล้มเหลวของระบบรักษาความปลอดภัยได้ชัดเจนและเป็นอมตะเท่ากับ *Jurassic Park* (1993) ภาพยนตร์ที่ดัดแปลงจากนวนิยายของ Michael Crichton นี้ ไม่ได้เป็นเพียงเรื่องราวการผจญภัยหนีตายจากไดโนเสาร์ที่สูญพันธุ์ไปแล้ว แต่หากมองผ่านเลนส์ของนักบริหารจัดการความปลอดภัย (Security Management) มันคือกรณีศึกษาชั้นครูว่าด้วย “ภัยคุกคามจากคนใน” (Insider Threat) และ “จุดอ่อนของระบบที่ซับซ้อน” (Systemic Vulnerability) ที่ยังคงเกี่ยวข้องกับการบริหารจัดการความมั่นคงในโลกปัจจุบัน

จอห์น แฮมมอนด์ (John Hammond) ผู้ก่อตั้งสวนสนุกบนเกาะได้สร้างสิ่งปรกติวิสัยที่แทบสมบูรณ์แบบ สวนของเขา คือตัวแทนของความสำเร็จสูงสุดทางเทคโนโลยี นั่นคือ สวนสนุกที่ไดโนเสาร์ซึ่งสูญพันธุ์ไปแล้วถูกปล่อยให้เดินได้อย่างอิสระภายใต้การควบคุมของระบบคอมพิวเตอร์สุดล้ำ รั้วไฟฟ้าแรงสูง 10,000 โวลต์ล้อมรอบกรงขัง ระบบควบคุมการเข้าถึงที่ทำงานด้วยคอมพิวเตอร์ ตารางให้อาหารอัตโนมัติ และขั้นตอนการปฏิบัติงานที่ดูเหมือนจะรัดกุม แฮมมอนด์เชื่อมั่นอย่างสุดหัวใจว่าเขาได้เตรียมพร้อมรับมือกับทุกอันตรายที่เป็นไปหมดแล้ว และเขายืนยันกับนักลงทุนและผู้มาเยือนว่า “ราไม่ได้ประหยัดอะไรเลย” (we spared no expense)

แต่ความผิดพลาดมหันต์ของแฮมมอนด์ไม่ได้อยู่ที่การประเมินความดุร้ายของ Tyrannosaurus Rex หรือความฉลาดของ Velociraptor ต่ำเกินไป หากแต่อยู่ที่การมองข้าม “จุดอ่อน” ที่เล็กที่สุดแต่มีอำนาจสูงสุด นั่นคือ **มนุษย์** และวิธีที่มนุษย์นั้นถูกบัญชาการ และแม้ว่านักทฤษฎีความโกลาหลชื่อ เอียน มัลคอล์ม (Ian Malcolm) ซึ่งถูกเชิญ

มาเพื่อประเมินสวนสนุก ได้เตือนไว้ว่าระบบที่ซับซ้อนนั้นไม่อาจคาดเดาได้โดยธรรมชาติ แต่ข้อกังวลของเขาถูกเพิกเฉย หายนะเริ่มต้นขึ้นมาจริง ๆ เมื่อ เดนนิส เนดรี (Dennis Nedry) หัวหน้าโปรแกรมเมอร์ ผู้ที่ไม่พอใจในค่าตอบแทนและแบกรับหนี้สิน ได้ตัดสินใจรับสินบนจากบริษัทคู่แข่งเพื่อขโมยตัวอ่อนไดโนเสาว์

ภาพที่ 3.1
ฉากจากภาพยนตร์ *Jurassic Park* (1993)
ที่มา: Universal Pictures

เนดรี่ไม่ได้ใช้กำลังเข้าปล้น แต่เขาใช้ “สิทธิ์ในการเข้าถึง” (Authorized Access) และ “ความรู้ในระบบ” (System Knowledge) ซึ่งเป็นอาวุธที่ร้ายกาจที่สุดของภัยคุกคามภายใน (Insider Threat) เขาควบคุมระบบรักษาความมั่นคงปลอดภัย การทำงานของประตู กล้องวงจรปิด และพลังงานของรั้วไฟฟ้า ด้วยความเชื่อว่าการดำเนินการของเขาเป็นเรื่องง่ายและชั่วคราว โดยคิดว่าเขาจะสามารถกู้คืนระบบได้ภายใน 18 นาทีก่อนที่ใครจะสังเกตเห็น แต่เนดรี่กลับพบกับสิ่งที่เขาไม่ได้คาดการณ์ นั่นก็คือ พายุโซนร้อนทำให้ทัศนวิสัยลดลง เรือที่นัดพบเขาออกเดินทางก่อนเวลา และเขาตกรถจี๊ปหลังจากเลี้ยวผิดทางในสวนสนุกที่มืดมิด เมื่อไดโนเสาร์ Dilophosaurus สังหารเนดรี่ ข้อมูลเกี่ยวกับรหัสผ่านที่จำเป็นในการกู้คืนระบบก็สูญหายไปกับเขา

สิ่งที่เกิดขึ้นตามมาไม่ใช่ความโกลาหลจากไดโนเสาร์เพียงอย่างเดียว แต่เป็นความล้มเหลวที่ไหลล้นต่อเนื่อง (Cascading Effect) ซึ่งมีรากฐานมาจากความเปราะบางของ

มนุษย์ การพึ่งพาระบบ และการวางแผนสำรองที่ไม่ดี นี่คือสิ่งที่ Charles Perrow เรียกว่า **“ทฤษฎีอุบัติเหตุแบบปกติ” (Normal Accident Theory)** ซึ่งในระบบที่มีความซับซ้อนสูง (Complex Systems) และมีการเชื่อมโยงกันอย่างแน่นแฟ้น (Tightly Coupled) ความผิดพลาดเพียงจุดเล็ก ๆ สามารถลุกลามกลายเป็นหายนะใหญ่หลวงได้ ในกรณีนี้ รั้วไฟฟ้ายังคงดับ ไดโนเสาร์หลุดออกจากพื้นที่กักกัน ระบบสื่อสารล้มเหลว และผู้เยี่ยมชมถูกทิ้งไว้โดยไร้การป้องกัน เมื่อรวมเข้ากับ “ภัยธรรมชาติ” คือพายุโซนร้อนที่พัดถล่มเกาะในเวลาเดียวกัน (Complex Emergency) ระบบความปลอดภัยที่ถูกออกแบบมาอย่างดีบนหน้ากระดาษก็พังทลายลงอย่างสิ้นเชิง

ระบบความมั่นคงปลอดภัยของสวนสนุกขึ้นอยู่กับบุคคลเพียงคนเดียวซึ่งกลายเป็น “จุดล้มเหลวเดียว” (Single Point of Failure) ไม่มีผู้ดูแลระบบสำรอง ไม่มีระบบซ้ำซ้อนเพื่อปกป้องระบบวิกฤต ไม่มีแผนฟื้นฟูหลังภัยพิบัติที่คำนึงถึงภัยคุกคามจากภายใน องค์กรให้ความสำคัญกับนวัตกรรมและภาพลักษณ์ ในขณะที่ละเลยหลักการความมั่นคงพื้นฐาน เช่น หลักการให้สิทธิ์น้อยที่สุด (Least Privilege) การแบ่งแยกหน้าที่ (Separation of Duties) การเฝ้าระวังและการแจ้งเตือน (Monitoring and Alerting) การจัดการการเปลี่ยนแปลง และการกระจายความรู้

บทเรียนราคาแพงจากภาพยนตร์เรื่องนี้ชัดเจน คือ **ภัยคุกคาม (Threats) ไม่ได้กลายเป็นหายนะด้วยตัวมันเอง แต่มันต้องอาศัยการเจาะผ่านจุดอ่อน (Vulnerabilities)** ไม่ว่าจะเป็นจุดอ่อนทางเทคนิค (โค้ดที่เนดรี่เขียน) จุดอ่อนทางกายภาพ (รั้วที่ไม่มีไฟสำรอง) หรือจุดอ่อนทางองค์กร (การพึ่งพาคนเพียงคนเดียวดูแลระบบทั้งเกาะ) อันตรายที่ใหญ่ที่สุดมักไม่ได้อยู่ที่ตัวภัยคุกคามเอง แต่อยู่ที่ข้อสมมติฐานที่องค์กรมีต่อความพร้อมของตนเอง

สำหรับนักศึกษาวิชาความปลอดภัยและผู้บริหารจัดการในประเทศไทย บทเรียนนี้มีความสำคัญอย่างยิ่ง เรากำลังอยู่ในยุคที่องค์กรต้องเผชิญกับ “พายุที่สมบูรณ์แบบ” (Perfect Storm) ทั้งจากภัยคุกคามทางไซเบอร์ที่ซับซ้อนและไม่หยุดยั้ง ภัยพิบัติทางธรรมชาติที่รุนแรงขึ้น เช่นน้ำท่อมใหญ่หาดใหญ่ในเดือนพฤศจิกายน 2025 ที่มีผู้เสียชีวิต 145 รายและกระทบต่อครัวเรือนกว่า 1.2 ล้านครัวเรือน และโครงสร้างสังคมไทยที่มีวัฒนธรรมเฉพาะตัวซึ่งอาจกลายเป็นทั้งจุดแข็งและจุดอ่อน แม้แต่โครงสร้างพื้นฐานที่ทันสมัยก็ยังล้มเหลวเมื่อช่องโหว่ (ระบบจัดการน้ำท่วมที่ล้าสมัย โครงสร้างการบังคับบัญชาที่ไม่เป็นเอกภาพ ระบบเตือนภัยที่ไม่ประสิทธิผล) ปะทะกับภัยคุกคาม (ฝนตกหนักที่สุดในรอบ 300 ปี การขยายตัวของเมืองอย่างรวดเร็ว) (Sangsinchai, 2025)

ดังนั้น การทำความเข้าใจความสัมพันธ์สามเส้าของ “ภัยคุกคาม-ความเสี่ยง-จุดอ่อน” จึงไม่ใช่แค่เรื่องทางวิชาการ แต่เป็นรากฐานของการอยู่รอดและการสร้างความยืดหยุ่นในศตวรรษที่ 21 การทำความเข้าใจปฏิสัมพันธ์ระหว่างภัยคุกคามและช่องโหว่ไม่ใช่ทางเลือกอีกต่อไป แต่มันคือรากฐานที่การจัดการความมั่นคงที่มีประสิทธิภาพจะต้องถูกสร้างขึ้น

ภาพที่ 3.2

ลักษณะของภัยคุกคาม (เจตนา/ไม่เจตนา, มนุษย์/ธรรมชาติ, ภายใน/ภายนอก)

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

2. ภัยคุกคามในบริบทการจัดการความมั่นคงปลอดภัย (Threats in Security Management Context)

2.1 นิยามและพลวัตของภัยคุกคาม (Defining Threats)

ในทางทฤษฎีความมั่นคงปลอดภัย **ภัยคุกคาม (Threat)** หมายถึง ปัจจัยใด ๆ ไม่ว่าจะเป็นบุคคล วัตถุ เหตุการณ์ หรือแนวคิด ที่มีศักยภาพในการก่อให้เกิดอันตราย โดยการฉกฉวยโอกาสจากจุดอ่อน เพื่อสร้างผลกระทบเชิงลบต่อสินทรัพย์ (Assets) ขององค์กร ไม่ว่าสินทรัพย์นั้นจะเป็นชีวิตมนุษย์ ทรัพย์สินทางกายภาพ ข้อมูล หรือชื่อเสียง (Sinha et al., 2015)

สิ่งสำคัญที่ทุกคนต้องตระหนักคือ ภัยคุกคามมีลักษณะเป็น **พลวัต (Dynamic)** และ **ขึ้นอยู่กับบริบท (Context-dependent)** ภัยคุกคามชนิดหนึ่งอาจเป็นเรื่องคอขาดบาดตายสำหรับองค์กรหนึ่ง แต่เป็นเรื่องไร้สาระสำหรับอีกองค์กรหนึ่ง

ตัวอย่าง: สำหรับธนาคารพาณิชย์ในกรุงเทพฯ "มัลแวร์เรียกค่าไถ่" (Ransomware) คือภัยคุกคามระดับวิกฤตที่อาจทำให้ระบบการเงินล่มสลาย แต่สำหรับชาวประมงพื้นบ้านในจังหวัดสตูล ภัยคุกคามนี้แทบไม่มีความหมาย ในขณะที่ "พายุไต้ฝุ่น" คือภัยคุกคามที่แท้จริงสำหรับชาวประมง แต่ธนาคารอาจได้รับผลกระทบเพียงเล็กน้อยหากศูนย์ข้อมูล (Data Center) ตั้งอยู่ในที่ปลอดภัย

2.2 ภัยคุกคาม vs. ความเสี่ยง (Threats vs. Risks)

หนึ่งในความสับสนที่พบบ่อยที่สุดในหมู่นักศึกษาและแม้แต่ผู้ปฏิบัติงานมืออาชีพ คือ การใช้คำว่า “ภัยคุกคาม” และ “ความเสี่ยง” สลับกัน ทั้งที่ในความเป็นจริง สองคำนี้มีนัยสำคัญที่แตกต่างกันอย่างสิ้นเชิงในสมการความปลอดภัย:

ภัยคุกคาม (Threat): คือ “สิ่งที่อาจจะเกิดขึ้น” (Possibility) เป็นปัจจัยภายนอกที่เรามักควบคุมไม่ได้โดยตรง เช่น เราไม่สามารถสั่งให้แฮกเกอร์เลิกแฮก หรือสั่งให้ฝนหยุดตกได้

ความเสี่ยง (Risk): คือ “โอกาสและผลกระทบ” (Likelihood & Impact) ของภัยคุกคามนั้นต่อองค์กรของเรา เป็นสิ่งที่เราสามารถ “บริหารจัดการ” ได้

สมการความเสี่ยง (Risk Equation):

$$Risk = f\,(Threats, Vulnerability, Impacts)$$

การแยกแยะนี้ช่วยให้บริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดได้อย่างมีประสิทธิภาพและมีเหตุผล ตัวอย่างเช่น “อุกกาบาตชนโลก” อาจเป็นภัยที่มีผลกระทบรุนแรงมหาศาล **(High Impact)** แต่โอกาสเกิดต่ำมาก **(Low Likelihood)** จึงถูกจัดว่ามีความเสี่ยงต่ำ **(Low Risk)** ไม่สมควรทุ่มงบประมาณพันล้านสร้างหลังคากันอุกกาบาต ในทางกลับกัน “สายไฟเก่าในโรงงาน” อาจดูไม่น่ากลัว แต่มีโอกาสเกิดไฟไหม้สูงและจุดอ่อนชัดเจน จึงเป็นความเสี่ยงสูง **(High Risk)** ที่ต้องจัดการทันที (Sinha et al., 2015) สำหรับประเทศไทย ภัยคุกคามทางไซเบอร์เป็นกรณีที่ร้ายแรงที่สุด ในปี พ.ศ. 2568 มีการโจมตีเฉลี่ย 3,180 ต่อสัปดาห์ (สูงกว่าค่าเฉลี่ยโลก 70%) และมีความเสี่ยงที่

สูงเนื่องจากจุดอ่อนสำคัญ (ความซับซ้อนของระบบ IT ขาดแคลนบุคลากรด้านความมั่นคง การเปลี่ยนไปใช้ดิจิทัลรวดเร็วโดยไม่มีการควบคุมความมั่นคงที่เพียงพอ) ในทางตรงกันข้าม อุบัติเหตุโรงไฟฟ้านิวเคลียร์เป็นภัยเชิงทฤษฎีเท่านั้น เพราะไทยไม่มีโรงไฟฟ้านิวเคลียร์ ทำให้ความเสี่ยงเป็นศูนย์

3. ประเภทของภัยคุกคาม: ภายนอกและภายใน (Typologies of Threats: Internal vs. External)

เพื่อความชัดเจนในการวิเคราะห์ เราสามารถจำแนกภัยคุกคามออกเป็น 2 ประเภทหลักตามแหล่งกำเนิด แต่ในปัจจุบันเส้นแบ่งนี้กำลังเลือนลางลงเรื่อย ๆ

3.1 ภัยคุกคามภายนอก (External Threats)

ภัยคุกคามที่มีต้นกำเนิดจากภายนอกขอบเขตการควบคุมขององค์กร ผู้กระทำไม่มีสิทธิ์ในการเข้าถึง (Unauthorized) และต้องพยายามเจาะผ่านระบบป้องกันเข้ามา (Chen et al., 2024)

1. อาชญากรรมพื้นฐาน (Traditional Crime): การลักทรัพย์ การปล้นสดมภ์ การฉ้อโกง การบุกรุก และการทำลายทรัพย์สิน ซึ่งในประเทศไทยสถิติปี 2024-2025 ชี้ให้เห็นว่าแม้คดีอุกฉกรรจ์จะลดลง แต่คดีลักทรัพย์ในบางพื้นที่ยังคงสูง โดยเฉพาะการโจรกรรมรถจักรยานยนต์

2. อาชญากรรมไซเบอร์ (External Cyber Attacks): การโจมตีจากภายนอกจากตัวแสดงมากมาย ตั้งแต่กลุ่มอาชญากรที่มุ่งหวังผลกำไร ปฏิบัติการของรัฐชาติที่พยายามโจมตีการทำงานของประเทศ ไปจนถึงแฮ็กทิวิสต์ที่มีจุดประสงค์ทางการเมือง ภัยคุกคามเหล่านี้ได้แก่ การโจรกรรมข้อมูล การฟิชชิ่ง มัลแวร์เรียกค่าไถ่ การโจมตีแบบปฏิเสธการให้บริการ (DDoS) และการละเมิดข้อมูล ผู้ไม่ประสงค์ดีเหล่านี้ใช้ประโยชน์จากจุดอ่อนทางเทคนิค (ระบบปล่อยปละละเลย แพตช์ที่ล้าหลัง) และจุดอ่อนของมนุษย์ (พฤติกรรมไม่ปลอดภัย ติดกับลิงก์ที่เป็นอันตราย) เพื่อเจาะผ่านป้องกันระบบ

3. ภัยธรรมชาติ (Natural Hazards): น้ำท่วม แผ่นดินไหว พายุโซนร้อน โรคระบาด และอันตรายอื่น ๆ จากสิ่งแวดล้อม ในประเทศไทย น้ำท่วมเป็นภัยคุกคามภายนอกที่เกิดซ้ำ ๆ ส่งผลกระทบต่อโครงสร้างพื้นฐาน ระบบโลจิสติกส์ และบริการสาธารณะ เหตุการณ์น้ำท่วมใหญ่หาดใหญ่ในเดือนพฤศจิกายน 2568 แสดงให้เห็นว่าแม้แต่ศูนย์กลาง

เมืองที่พัฒนาดีแล้วก็ยังคงเสี่ยงต่อเหตุการณ์สภาพอากาศรุนแรงที่ทวีความรุนแรงขึ้นจากภาวะการเปลี่ยนแปลงสภาพภูมิอากาศ (Sangsinchai, 2025)

4. การก่อการร้าย (Terrorism): การโจมตีที่มีเป้าหมายเพื่อสร้างความเสียหายจำนวนมาก สร้างความวุ่นวายในสังคม หรือเพื่อส่งเสริมวาระเชิงอุดมการณ์ การเมือง หรือศาสนา แม้ว่าประเทศไทยจะเคยเผชิญกับการก่อการร้ายในจังหวัดชายแดนภาคใต้ แต่กรุงเทพมหานครก็เคยประสบกับความรุนแรงจากแรงจูงใจทางการเมืองในช่วงที่มีความวุ่นวายภายในประเทศเช่นกัน

3.2 ภัยคุกคามภายใน (Internal Threats)

นี่คือภัยคุกคามที่อันตรายที่สุดและป้องกันยากที่สุด ดังคำกล่าวที่ว่า “เกลือเป็นหนอน” ผู้กระทำคือคนที่มีสิทธิ์เข้าถึง (Authorized Access) อยู่แล้ว เช่น พนักงาน ผู้บริหาร หรือคู่ค้า ที่ลักขโมยทรัพย์สิน เงินทุน หรือทรัพย์สินทางปัญญา งานวิจัยชี้ให้เห็นว่า 60% ของการละเมิดข้อมูลเกิดจากภัยคุกคามภายใน และพนักงานที่กำลังจะลาออก 59% นำข้อมูลความลับของบริษัทติดตัวไปด้วย (Chen et al., 2024)

ประเภทของภัยคุกคามจากภายใน:

1. การก่อวินาศกรรม: การทำลายระบบ การดำเนินงาน หรือทรัพย์สินโดยจงใจ มักจากแรงจูงใจแก้แค้น เป้าหมายเชิงอุดมการณ์ หรือการได้เปรียบทางการแข่งขัน ดังเช่น การกระทำของเดนนิส เนดรีในเรื่อง *Jurassic Park*

2. ความประมาทและความผิดพลาดของมนุษย์: การกระทำที่ไม่เจตนาที่ทำให้ความมั่นคงบกพร่อง เช่น การตั้งค่าระบบผิดพลาด การสูญเสียอุปกรณ์ หรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ งานวิจัยพบว่า 90% ของการละเมิดความมั่นคงทางไซเบอร์ที่ประสบความสำเร็จเกี่ยวข้องกับความผิดพลาดของมนุษย์

3. การละเมิดนโยบาย: พนักงานเลี่ยงขั้นตอนความมั่นคงเพื่อความสะดวก เช่น การแชร์รหัสผ่าน การใช้สิ่งของหนีบประตู หรือการใช้ซอฟต์แวร์ที่ไม่ได้อนุมัติ

4. ความรุนแรงในที่ทำงาน: การทำร้ายร่างกายหรือจิตใจจากพนักงานหรืออดีตพนักงาน มักมีแรงจูงใจจากความไม่พอใจหรือภาวะวิกฤตทางสุขภาพจิต

ความได้เปรียบของคนใน: ภัยคุกคามจากภายในเป็นอันตรายอย่างยิ่ง เพราะบุคคลภายในมีสิทธิ์เข้าถึงที่ถูกต้องตามกฎหมาย ได้รับความไว้วางใจ และมีความรู้เกี่ยวกับระบบ ซึ่งผู้โจมตีจากภายนอกขาดแคลน พวกเขารู้จุดเด่นและจุดอ่อนของระบบการวิตระ

หว่างที่อยู่ยาง ตารางเวรยาม และตำแหน่งของทรัพย์สินที่มีคุณค่าที่สุด บุคคลภายในเข้าใจมาตรการควบคุมความมั่นคงและรู้วิธีหลบเลี่ยงมาตรการเหล่านั้น พวกเขามีหลักฐานยืนยันตัวตนที่ถูกต้องซึ่งอนุญาตให้พวกเขาดำเนินการโดยไม่กระตุ้นการแจ้งเตือน การตรวจจับจึงทำได้ยากเพราะกิจกรรมของพวกเขาดูเหมือนปกติจนกว่าความเสียหายจะปรากฏชัดเจน (Chen et al., 2024)

สถิติและกรณีศึกษา: ปี 2025 ผล สำรวจจากผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ระบุว่า 64% มองว่าภัยคุกคามจากคนใน มีความเสี่ยงสูงกว่าการโจมตีจากภายนอก ในประเทศไทย กรณีพนักงานธนาคารระดับผู้จัดการ ผู้ร่วมคิดกับแก๊งคอลเซ็นเตอร์ชาวจีน สร้าง “บัญชีม้า” (Mule Accounts) จำนวนมากโดยใช้สิทธิ์ของตนเองในการยืนยันตัวตนลูกค้าปลอม ทำให้เกิดความเสียหายกว่า 2,200 ล้านบาท เหตุการณ์นี้สะท้อนให้เห็นว่าภัยคุกคามภายในไม่ได้เกิดจากแค่ “ความแค้น” แต่เกิดจาก “ความโลภ” และ “โอกาส” ซึ่งเป็นปัจจัยที่องค์กรสามารถควบคุมได้ผ่านการจัดการทรัพยากรมนุษย์ที่มีประสิทธิภาพและการเฝ้าระวังระบบอย่างเข้มงวด

ภาพที่ 3.3

Hybrid Threats: ภัยคุกคามแบบผสมผสาน

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

4. อาชญากรรม การก่อการร้าย และภัยคุกคามไซเบอร์ (Specific Threat Categories)

4.1 จากท้องถนนสู่โลกออนไลน์ (From Streets to Screens)

ในอดีต เมื่อพูดถึงอาชญากรรม เรามักนึกถึงโจรปล้นธนาคารหรือขโมยขึ้นบ้าน แต่ในปี 2025 ภูมิทัศน์อาชญากรรมในประเทศไทยได้เปลี่ยนไปอย่างสิ้นเชิง

สกมเมอร์ครองเมือง: ภูมิทัศน์อาชญากรรมของประเทศไทยในปี 2025 เปลี่ยนโฉมไปจากการกระทำทางกายภาพไปเป็นอาชญากรรมดิจิทัล โดยสำนักงานตำรวจแห่งชาติเผยว่าการเสียแจ้งความสูงสุดในปัจจุบันไม่ใช่ทำร้ายร่างกายหรือโจรกรรมอีกต่อไป แต่คือ “การฉ้อโกงทางออนไลน์” โดยเฉพาะแก๊งคอลเซ็นเตอร์และ Hybrid Scam ที่มีมูลค่าความเสียหายสูงและการเข้าถึงเหยื่อได้กว้างขวาง (Scholz, 2017)

วิวัฒนาการของแก๊งคอลเซ็นเตอร์: แก๊งคอลเซ็นเตอร์ได้พัฒนาจากการโทรสุ่มแบบง่าย ๆ กลายเป็นเครือข่ายอาชญากรรมไซเบอร์ที่ซับซ้อนและใช้เทคโนโลยีขั้นสูง กลยุทธ์อันตรายที่สุดคือการใช้ AI และ Deepfake ในการปลอมแปลงใบหน้าและเสียงของบุคคลที่มีความน่าเชื่อถือ เช่น เจ้าหน้าที่ตำรวจ ทนายความ หรือผู้บริหารสถาบันการเงิน เทคโนโลยีนี้ทำลายความระแวงโดยสร้างสถานการณ์สมจริง ยกตัวอย่างเช่น ผู้บริหารการเงินของบริษัทข้ามชาติถูกหลอกให้โอนเงินมหาศาลเนื่องจากเชื่อว่าสื่อสารกับ CEO ผ่าน Zoom ทั้งที่บุคคลในวิดีโอคอลล์เป็นภาพ/เสียงปลอม (Scholz, 2017)

พื้นที่สีเทาชายแดน: ภัยคุกคามนี้เป็นอาชญากรรมข้ามชาติที่มีการบริหารจัดการเป็นระบบในพื้นที่เศรษฐกิจพิเศษและชายแดน เช่น KK Park ในเมียนมาและเมืองสีหนุวิลล์ในกัมพูชา ที่กลายเป็นศูนย์กลางของ Scam Compounds โดยภายในครฐานที่ตั้งมีการบังคับแรงงานและค้ามนุษย์รูปแบบใหม่ เหยื่อจำนวนมากจากเอเชียตะวันออกเฉียงใต้ถูกล่อลวงหรือลักพาตัวมา เกี่ยวข้องกับการกักขัง บังคับทำงานเป็น “นักหลอกลวง” เพื่อหลอกเพื่อนร่วมชาติ พร้อมกับสภาพการทำงานเลวร้าย การควบคุมด้วยความรุนแรง และการละเมิดสิทธิมนุษยชนอย่างร้ายแรง

การก่อการร้ายและความไม่สงบ (Terrorism and Insurgency)

ภัยคุกคามด้านความมั่นคงอย่างต่อเนื่องของประเทศไทยคือ ความไม่สงบในจังหวัดชายแดนภาคใต้ ตั้งแต่ปี 2547 ปัญหานี้ได้ขยายจากความรุนแรงในปัตตานี ยะลา และนราธิวาส ไปยังบางส่วนของสงขลา ทำให้กลายเป็นหนึ่งในพื้นที่ความขัดแย้งภายในประเทศที่ยืดเยื้อที่สุดในเอเชียตะวันออกเฉียงใต้

การเปลี่ยนรูปของความรุนแรง: แม้จำนวนเหตุการณ์รุนแรงลดลงเมื่อเทียบกับจุดสูงสุดในทศวรรษก่อน แต่รูปแบบและวิธีการได้ซับซ้อนขึ้น การโจมตีเปลี่ยนจากการสร้างความเสียหายแบบวงกว้างมาใช้กลยุทธ์แม่นยำสูง (High Precision) ที่มุ่งสร้างผลกระทบทางจิตวิทยา เช่น การลอบวางระเบิดแสวงเครื่อง (IEDs) และโจมตีเป้าหมายสัญลักษณ์ เช่น สถานที่ราชการ สถาบันการศึกษา หรือผู้นำศาสนาสายกลาง เพื่อทำลายความเชื่อมั่นของประชาชนและขยายพื้นที่แห่งความหวาดกลัว

ความซับซ้อนทับซ้อน: ปัญหาความไม่สงบได้วิวัฒนาการเกินกว่ากรอบความขัดแย้งทางการเมืองแบบดั้งเดิม มันหลอมรวมเข้ากับเครือข่ายธุรกิจผิดกฎหมายที่เข้มแข็ง ได้แก่ การค้ายาเสพติด การลักลอบขนส่งน้ำมัน และการค้ามนุษย์ การทับซ้อนนี้ทำให้เส้นแบ่งระหว่าง “ผู้ก่อการร้าย” กับ “นายทุนอาชญากร” เลือนรางและแยกจากกันได้ยาก ผู้ก่อเหตุอาจมีแรงจูงใจทางอุดมการณ์และส่วนได้เสียในธุรกิจผิดกฎหมายพร้อมกัน การเงินจากอาชญากรรมสนับสนุนทั้งการดำรงชีพและการจัดหาอาวุธ

4.3 อาชญากรรมไซเบอร์: ภัยเงียบที่รุนแรงที่สุด (Cyber Threats)

อาชญากรรมไซเบอร์กลายเป็นภัยคุกคามที่มีผลกระทบเชิงระบบและต่อเนื่องมากที่สุดสำหรับประเทศไทย แม้ไม่ปรากฏเป็นความเสียหายทางกายภาพ แต่ความเสียหายทางเศรษฐกิจและการสูญเสียความเชื่อมั่นนั้นมูลค่ามหาศาล

Ransomware: ภัยคุกคามอันดับหนึ่ง: ในปี 2025 มัลแวร์เรียกค่าไถ่ (Ransomware) ครองตำแหน่งอันดับหนึ่งสำหรับองค์กรธุรกิจและหน่วยงานรัฐไทย โดยเฉพาะโรงพยาบาล ระบบสาธารณสุข โรงงาน และระบบผลิต เนื่องจากองค์กรเหล่านี้ยินดีจ่ายค่าไถ่เพื่อกู้คืนข้อมูลและฟื้นการบริการ ทั้งนี้ สถิติระดับโลกแสดงการโจมตี Ransomware เกิดขึ้นทั่วโลกทุก 11 วินาที ประเทศไทยมีความเสี่ยงสูงเนื่องจากอัตราการใช้ซอฟต์แวร์ไม่ถูกลิขสิทธิ์สูงและระบบคอมพิวเตอร์จำนวนมากไม่ได้อัปเดตแพตช์ความปลอดภัยหรือใช้ซอฟต์แวร์รุ่นเก่า (Legacy Systems) สิ่งนี้สร้างช่องโหว่มหาศาลให้แฮกเกอร์ใช้เครื่องมืออัตโนมัติเจาะระบบได้ง่าย

การโจมตีโครงสร้างพื้นฐาน ความเสียหายจากไซเบอร์สู่กายภาพ: ภัยคุกคามใหม่ที่มีศักยภาพรุนแรงที่สุดคือการโจมตีระบบควบคุมทางอุตสาหกรรม (OT/ICS) ที่ควบคุมโครงสร้างพื้นฐานสำคัญของชาติ เป้าหมายไม่ใช่แค่ข้อมูลหรือเงิน แต่คือความสามารถในการทำให้บริการสาธารณะหยุดชะงักหรือสร้างความเสียหายทางกายภาพ (Ghazal et al., 2020)

เป้าหมายการโจมตี:

1. ระบบควบคุมไฟฟ้า: อาจนำไปสู่การดับไฟฟ้าเป็นวงกว้าง
2. ระบบจ่ายน้ำประปา: อาจเกิดการขาดแคลนน้ำหรือปนเปื้อน
3. ระบบขนส่งสาธารณะ (รถไฟฟ้า สัญญาณไฟจราจร): อาจก่อให้เกิดอุบัติเหตุ
4. โรงงานอุตสาหกรรม: อาจนำไปสู่รั่วไหลของสารเคมีหรือการระเบิด

ภาพที่ 3.4

Intentional Threats: ภัยคุกคามโดยเจตนา

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

การโจมตี OT/ICS แตกต่างจากการโจมตี IT ทั่วไป เพราะสามารถข้ามจากโลกดิจิทัลไปสร้างผลกระทบทางกายภาพโดยตรง เช่น ทำให้เมืองทั้งเมืองไม่มีไฟฟ้า หรือทำให้ระบบน้ำประปามีปัญหา ด้วยเหตุนี้ ผลกระทบมีทั้งการสูญเสียความเชื่อมั่นต่อรัฐบาล ความตื่นตระหนกในสังคม และในกรณีรุนแรงอาจนำไปสู่ความไม่สงบทางสังคม ภัยคุกคามนี้จึงกลายเป็น ปัญหาเชิงยุทธศาสตร์ด้านความมั่นคงแห่งชาติ ต้องอาศัยความร่วมมือระหว่างภาครัฐ ภาคเอกชน และหน่วยงานด้านความมั่นคงไซเบอร์เร่งด่วน (Ghazal et al., 2020)

5. ภัยธรรมชาติและภาวะฉุกเฉินซับซ้อน (Natural Hazards and Complex Emergencies)

5.1 กรณีศึกษา: มหาอุทกภัยหาดใหญ่ พฤศจิกายน 2025

มหาอุทกภัยหาดใหญ่ไม่ได้เป็นเพียงภัยธรรมชาติ แต่เป็น “ภัยพิบัติที่มนุษย์สร้างขึ้น” ในแง่ของการบริหารจัดการที่ล้มเหลว

1. ภัยคุกคาม (Threat)

เหตุการณ์เริ่มจากพายุฝนรุนแรงต่อเนื่อง 3 วัน ส่งผลให้มีปริมาณน้ำฝนสะสมกว่า 600 มิลลิเมตร นักอุตุนิยมวิทยาระบุว่าเป็นเหตุการณ์ “300 ปีมีครั้ง” ซึ่งสะท้อนผลของการเปลี่ยนแปลงสภาพภูมิอากาศที่ทำให้สภาพอากาศสุดขั้วมีความรุนแรงและความถี่เพิ่มขึ้น (Sangsinchai, 2025)

2. จุดอ่อน (Vulnerability)

ด้านกายภาพ: การเติบโตของเมืองแบบไร้วางแผน (Urban Sprawl) เป็นหลายทศวรรษ ส่งผลให้สิ่งปลูกสร้างรุกล้ำพื้นที่ชุ่มน้ำและทางน้ำธรรมชาติ ขัดขวางการไหลของน้ำ นอกจากนี้ระบบระบายน้ำในเมืองออกแบบจากข้อมูลในอดีต ไม่สามารถรองรับปริมาณน้ำขนาดใหญ่และกะทันหันได้

ด้านการจัดการ: เกิดความล้มเหลวในกระบวนการแจ้งเตือนภัย โครงสร้างราชการแบบแบ่งส่วน (Silo Mentality) เป็นอุปสรรคสำคัญ ข้อมูลพยากรณ์ฝนตกหนักจากกรมอุตุนิยมวิทยาไม่ได้รับการแปลความเสี่ยงให้ชัดเจนและไม่ส่งต่อรวดเร็วไปสู่การตัดสินใจอพยพประชาชน ผลคือประชาชนในพื้นที่เสี่ยงได้รับคำเตือนล่าช้า จนกระทั่งน้ำท่วมเข้าใจเมืองแล้ว

ภาวะฉุกเฉินซับซ้อน (Complex Emergency): สิ่งที่ทำให้วิกฤตรุนแรงขึ้นคือการล่มสลายของโครงสร้างพื้นฐาน (Cascading Failure) น้ำท่วมทำให้ศูนย์ชุมสายสื่อสารและสถานีฐานโทรศัพท์เสียหาย เกิด “ภาวะสื่อสารดับสนิท” (Communication Blackout) ประชาชนไม่สามารถโทรขอความช่วยเหลือหรือติดต่อญาติได้ ส่วนทีมกู้ภัยก็ไม่สามารถประสานงานได้อย่างมีประสิทธิภาพ

สถานการณ์กลายเป็น “วิกฤตซ้อนวิกฤต” ที่ขาดการสื่อสารและข้อมูลเวลาวิกฤต ผลคือเสียชีวิตกว่า 145 ราย และความเสียหายทางเศรษฐกิจกว่า 2.5 หมื่นล้านบาท เป็นบทเรียนสำคัญที่แสดงให้เห็นว่าภัยธรรมชาติในยุคใหม่มักนำไปสู่ภาวะฉุกเฉินซับซ้อน ต้อง

อาศัยการบริหารจัดการรวดเร็ว สื่อสารที่ยืดหยุ่น และเตรียมรับมือกับความล้มเหลวที่เกิดขึ้นเป็นลูกโซ่

5.2 ฝุ่น PM 2.5: ภัยคุกคามความมั่นคงรูปแบบใหม่

ฝุ่น PM 2.5 ไม่ได้เป็นเพียงปัญหามลพิษทางอากาศเท่านั้น แต่เป็น “ภัยคุกคามแบบช้า ๆ” (Slow-onset Hazard) ที่บั่นทอนรากฐานความเข้มแข็งของชาติอย่างต่อเนื่อง ต่างจากน้ำท่วมหรือแผ่นดินไหวที่มีผลกระทบฉับพลัน ฝุ่น PM 2.5 สะสมผลกระทบยาวนาน แต่ความรุนแรงลึกลับและกว้างขวาง

บั่นทอนทรัพยากรมนุษย์: PM 2.5 เป็นสารก่อมะเร็งและทำลายระบบทางเดินหายใจและหัวใจโดยตรง ในปี 2025 ประเทศไทยมีผู้ป่วยด้วยโรคระบบทางเดินหายใจและหัวใจเพิ่มขึ้นนับล้านเคส โดยเฉพาะเด็กเล็ก ผู้สูงอายุ และผู้มีโรคประจำตัว สิ่งนี้สร้างความทุกข์ทรมานและภาระค่าใช้จ่ายด้านสุขภาพมหาศาลต่อระบบสาธารณสุข

ลดผลิตภาพทางเศรษฐกิจ: วันที่ค่าฝุ่นสูง ผู้ป่วยนอกและผู้ป่วยในเพิ่มขึ้นอย่างชัดเจน แรงงานที่มีสุขภาพไม่ดีทำงานไม่เต็มที่ โรงเรียนต้องปิด นักท่องเที่ยวลดการเดินทาง ผลกระทบทับซ้อนนี้สร้าง การสูญเสียผลิตภาพของประเทศ เป็นมูลค่าหลายหมื่นล้านบาทต่อปี และบ่อนทำลายขีดความสามารถแข่งขันทางเศรษฐกิจในระยะยาว

ภาพที่ 3.5
Unintentional Threats (ภัยคุกคามโดยไม่เจตนา)
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

สร้างความไม่มั่นคงทางสังคม: ประชาชนต้องเผชิญกับอากาศเป็นพิษเป็นเวลาหลายเดือน สร้างความเครียดเรื้อรัง ความรู้สึกสูญเสียการควบคุม และความไม่พอใจต่อภาครัฐที่ดูเหมือนแก้ปัญหาไม่ได้ ความไม่ไว้วางใจและเรียกร้องทางการเมืองที่เพิ่มขึ้นเป็นสัญญาณของ ความไม่มั่นคงทางสังคม

6. การวิเคราะห์จุดอ่อน (Vulnerability Analysis)

ภัยคุกคามจะไม่มีความหมายหากปราศจาก “จุดอ่อน” (Vulnerability) ให้โจมตี ทั้งนี้ **จุดอ่อน** หมายถึง ความบกพร่องหรือช่องโหว่ที่ภัยคุกคามสามารถใช้ประโยชน์เพื่อก่อให้เกิดอันตราย จุดอ่อนไม่ก่อให้เกิดอันตรายด้วยตัวของมันเอง แต่จะเกิดอันตราย เมื่อภัยคุกคามเข้ามาใช้ประโยชน์จากจุดอ่อนนั้นสำเร็จ การแยกแยะนี้มีความสำคัญอย่างยิ่ง การกำจัดภัยคุกคามทั้งหมดเป็นเรื่องที่เป็นไปไม่ได้ในทางปฏิบัติ (องค์กรไม่สามารถป้องกันภัยธรรมชาติได้ทั้งหมดหรือกำจัดอาชญากรทุกคนได้) แต่การลดจุดอ่อนเป็นเป้าหมายที่สามารถบรรลุได้ผ่านการจัดการอย่างเป็นระบบ (Anton & Nedelcu, 2018)

การระบุจุดอ่อนจำเป็นต้องอาศัย การวิเคราะห์องค์กรอย่างตรงไปตรงมาและไม่เข้าข้างตนเอง องค์กรต้องถามคำถามที่อาจไม่สบายใจแต่จำเป็น:

1. ระบบควบคุมการเข้าถึงของเรามีจุดอ่อนที่สุดที่ไหน?
2. ระบบใดบ้างที่ไม่มีระบบสำรองที่เพียงพอ?
3. พนักงานมักละเมิดนโยบายที่จุดใดเป็นประจำ?
4. ความรู้ที่สำคัญใดบ้างที่ถูกกักเก็บอยู่กับบุคคลคนเดียว?
5. สินทรัพย์ใดบ้างที่ขาดการเฝ้าระวังที่เหมาะสม?

ดังนั้น การประเมินจุดอ่อนจึงเป็นกระบวนการที่ต้อง มองเข้าไปภายในเป็นหลัก — องค์กรต้องตรวจสอบจุดอ่อนของตัวเองอย่างตรงไปตรงมา แทนที่จะมุ่งความสนใจไปที่ภัยคุกคามจากภายนอกเพียงอย่างเดียว การวิเคราะห์จุดอ่อนจึงเป็นหัวใจสำคัญของการป้องกัน (Anton & Nedelcu, 2018) เราสามารถแบ่งจุดอ่อนออกเป็น 4 มิติสำคัญ:

6.1 จุดอ่อนทางกายภาพ (Physical Vulnerabilities)

คือความอ่อนแอของสถานที่และโครงสร้าง

ตัวอย่าง: รั้วที่เตี้ยเกินไป กล้องวงจรปิดที่มีจุดบอด ระบบไฟส่องสว่างที่ไม่เพียงพอ หรืออาคารที่ไม่ทนต่อแผ่นดินไหว

กรณีศึกษาซานติก้าผับ: โศกนาฏกรรมปี 2009 เกิดจากจุดอ่อนทางกายภาพที่ร้ายแรง คือ การไม่มีทางหนีไฟที่เพียงพอ ประตูทางออกถูกปิดตาย และการใช้วัสดุตกแต่งที่ติดไฟง่าย เมื่อเกิดเหตุเพลิงไหม้ (Threat) จุดอ่อนเหล่านี้จึงเปลี่ยนอุบัติเหตุให้เป็นโศกนาฏกรรม

6.2 จุดอ่อนทางมนุษย์ (Human Vulnerabilities)

มนุษย์คือ “ห่วงโซ่ที่อ่อนแอที่สุด” (The Weakest Link) ในระบบความปลอดภัย ตัวอย่างที่เกิดขึ้นบ่อยและเห็นได้ชัด เช่น

ความรู้เท่าไม่ถึงการณ์ (Lack of Awareness): พนักงานตั้งรหัสผ่านว่า “123456” หรือเขียนรหัสแปะไว้หน้าจอคอมพิวเตอร์

วิศวกรรมสังคม (Social Engineering): ความใจดีและความเห็นอกเห็นใจของคนไทย มักถูกมิจฉาชีพนำมาใช้เป็นจุดอ่อน เช่น การแกล้งทำเป็นเดือดร้อนเพื่อขอให้เปิดประตูให้ หรือการโทรมาหลอกว่ามีพัสดุตกค้าง

ความเหนื่อยล้า (Fatigue): เจ้าหน้าที่ รปภ. ที่ต้องเข้าเวรติดต่อกัน 12 ชั่วโมง ย่อมมีความตื่นตัวลดลงและมีโอกาสผิดพลาดสูง

6.3 จุดอ่อนทางเทคโนโลยี (Technological Vulnerabilities)

จุดอ่อนประเภทนี้หมายถึง ความบกพร่องในซอฟต์แวร์ ฮาร์ดแวร์ เครือข่าย และกระบวนการทางดิจิทัลที่เปิดช่องให้ภัยคุกคามสามารถโจมตีหรือใช้ประโยชน์ได้ (Lansweeper, 2024; C-STEM, 2024)[383][386] ตัวอย่างที่พบได้บ่อย ได้แก่:

ระบบที่ล้าสมัย (Legacy Systems): องค์กรจำนวนมากในไทยยังใช้ Windows รุ่นเก่าที่เลิกสนับสนุนแล้ว ทำให้มีช่องโหว่ (Exploits) ที่แฮกเกอร์เจาะได้ง่าย

Shadow IT: พฤติกรรมการทำงานของคนไทยที่นิยมใช้ LINE หรือ Google Drive ส่วนตัวในการส่งไฟล์งานสำคัญ โดยที่ฝ่าย IT ไม่รับรู้และควบคุมไม่ได้ ข้อมูลความลับจึงหลุดรอดออกไปนอกระบบรักษาความปลอดภัยขององค์กรได้ง่าย

6.4 จุดอ่อนทางองค์กรและวัฒนธรรม (Organizational & Cultural Vulnerabilities)

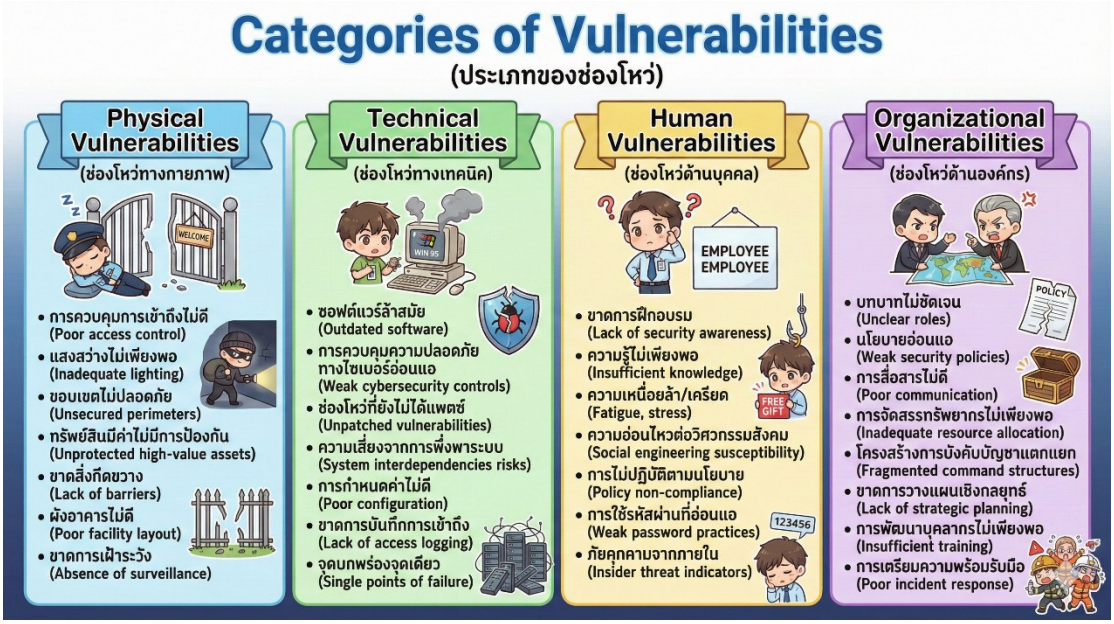
จุดอ่อนเหล่านี้เกี่ยวกับความบกพร่องในการกำกับดูแล การบริหารจัดการ และโครงสร้างและวัฒนธรรมของสถาบัน จุดอ่อนที่เกี่ยวกับไทยและแก้ไขยากที่สุด เช่น

ระบบอาวุโสและความเกรงใจ: ในวัฒนธรรมไทย ผู้น้อยมักไม่กล้าทักท้วงผู้ใหญ่ หรือลูกน้องไม่กล้าเตือนหัวหน้าเมื่อเห็นความไม่ปลอดภัย (เช่น พยาบาลไม่กล้าเตือนหมอที่

ลืมล้างมือ หรือวิศวกรไม่กล้าค้านผู้บริหารเรื่องตัดงบซ่อมบำรุง) ความ “เกรงใจ” นี้คือเพชฌฆาตเงียบในงานความปลอดภัย

วัฒนธรรม “ไม่เป็นไร”: ทัศนคติที่ยอมรับความเสี่ยงเล็กๆ น้อยๆ หรือมองข้ามกฎระเบียบเพื่อความสะดวกสบาย (Sabai Sabai) เช่น การขี่มอเตอร์ไซค์ย้อนศร หรือการไม่สวมหมวกนิรภัยในไซต์งาน ก่อให้เกิดวัฒนธรรมความปลอดภัยที่อ่อนแอ (Weak Safety Culture)

ระบบอุปถัมภ์ (Patronage System): การแต่งตั้งคนตามความใกล้ชิดมากกว่าความสามารถ (Competency) ในตำแหน่งที่ดูแลความปลอดภัย ส่งผลให้การตัดสินใจและการแก้ปัญหาไร้ประสิทธิภาพ โดยเฉพาะในหน่วยงานราชการ



ภาพที่ 3.6

Categories of Vulnerabilities (ประเภทของช่องโหว่)

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

7. ความเสี่ยงที่แท้จริง vs. การรับรู้ความเสี่ยง (Actual Risk vs. Risk Perception)

7.1 ช่องว่างแห่งความกลัว (The Fear Gap)

มนุษย์เราไม่ได้ตัดสินความเสี่ยงจากสถิติ แต่ตัดสินจาก “ความรู้สึก” (Feeling) แทน ความแตกต่างระหว่างความเสี่ยงที่แท้จริงกับสิ่งที่เรารับรู้ว่า เป็นเสี่ยงสร้าง “ช่องว่าง

แห่งความกลัว” (Fear Gap) ซึ่งมีผลกระทบต่อการตัดสินใจด้านความปลอดภัยและการจัดสรรทรัพยากร (Petersen, 2017)

ความเสี่ยงที่แท้จริง (Actual Risk) วัดจากข้อมูลสถิติและเหตุการณ์ที่บันทึก ตัวอย่างที่ชัดเจนคือ อุบัติเหตุทางถนนในไทยซึ่งมีอัตราการเสียชีวิตสูงเป็นอันดับต้น ๆ ของโลก ประมาณ 50-60 ศพต่อวัน ทำให้ถนนเป็นสถานที่ที่มีความเสี่ยงต่อชีวิตสูงสุดเมื่อเปรียบเทียบกับสถานการณ์อื่นๆ ในสังคม

การรับรู้ความเสี่ยง (Perceived Risk) วัดจากความกังวล ความเครียด และความหวาดกลัวที่คนรู้สึกจริงๆ คนไทยจำนวนมากอาจกลัวการก่อการร้ายหรือการกราดยิงในห้างสรรพสินค้ามากกว่าการข้ามถนน ทั้งที่สถิติแสดงชัดว่าโอกาสเสียชีวิตจากการก่อการร้ายน้อยกว่ามาก เหตุผลที่การรับรู้ความเสี่ยงสูงสุดกว่าความเป็นจริง ก็เพราะเหตุการณ์ที่น่ากลัวเหล่านี้มี “ความน่ากลัว” (Dread) สูง กล่าวคือมีความรุนแรง ไม่คาดการณ์ได้ และ “ควบคุมไม่ได้” (Uncontrollable) ในมุมมองของประชาชน ความรู้สึกว่าตัวเองไม่มีอำนาจต่อสถานการณ์ทำให้ความกลัวมีความรุนแรงมากขึ้น (Majlingová, 2024)

7.2 อิทธิพลของสื่อและโซเชียลมีเดีย

ช่องว่างแห่งความกลัวขยายตัวเมื่อมีการหลอมรวมกับอิทธิพลของสื่อและแพลตฟอร์มดิจิทัล ข่าวอาชญากรรมที่ถูกนำเสนอซ้ำๆ ใน TikTok, Facebook, YouTube และแพลตฟอร์มข่าวออนไลน์ต่างๆ สร้างภาพจำจดจำที่ผิดเพี้ยนเกี่ยวกับสังคมไทย มีการสร้างความเข้าใจว่าสังคมเต็มไปด้วยอันตราย ความรุนแรง และความไม่ปลอดภัย ปรากฏการณ์นี้เรียกว่า “Mean World Syndrome” (syndrome ของโลกที่เต็มไปด้วยความชั่ร้าย)

ปัญหาเกิดจากลักษณะของการนำเสนอข้อมูลทั่วไป สื่อมีแนวโน้มที่จะสดใจและเน้นเรื่องที่น่าสนใจ หน่วงใจ หรือกล่าวโต แต่ไม่นำเสนออาชญากรรมที่เป็นส่วนน้อยจำนวนมาก ผลที่ตามมาคือ สถิติการเกิดเหตุการณ์ร้ายแรง เช่น การท่วมท้นหรือการก่อการร้ายถูกขยายให้ใหญ่โตออกไปในจิตสำนึกของประชาชน ดังนั้นการรับรู้ความเสี่ยงจึงสูงกว่าความเป็นจริง

ขณะเดียวกัน ภัยเงียบ (Silent Threats) เช่น โรคไม่ติดต่อเรื้อรัง (Non-Communicable Diseases: NCDs) ที่รวมถึงโรคหัวใจ เบาหวาน มะเร็ง หรือมลพิษทางสิ่งแวดล้อมอย่างฝุ่น PM 2.5 ถูกมองข้ามและไม่ได้รับความสนใจเพียงพอ ถึงแม้ว่าการเสียชีวิตและความเจ็บป่วยจากโรคเหล่านี้มีจำนวนมากกว่าอาชญากรรม แต่เนื่องจากเป็น

เหตุการณ์ที่เกิดขึ้นเรื้อรัง ค่อย ๆ และไม่มีตัวร้ายที่ชัดเจน ประชาชนจึง “คุ้นชิน” (Familiarity) กับสถานการณ์เหล่านี้ และรับรู้ว่าไม่มีความเสี่ยง หรือความเสี่ยงต่ำกว่าความเป็นจริง (Majlingová, 2024)

ผลกระทบต่อการบริหารความปลอดภัย: การให้ความสำคัญกับภัยคุกคามที่ส่งผลกระทบที่มีความรุนแรงสูง (dread risks) มากกว่าภัยเงียบที่เป็นสาเหตุการเสียชีวิตมากขึ้น ทำให้ทรัพยากรและความพยายามในการป้องกันไม่ได้มีการจัดสรรอย่างเหมาะสม บ่อยครั้งที่งบประมาณความปลอดภัยไปใช้กับการป้องกันการก่อการร้ายหรือการปลน แต่ไม่เพียงพอสำหรับการควบคุมความปลอดภัยทางถนน การลดมลพิษ หรือการป้องกันโรค

7.3 ความเชื่อและไสยศาสตร์

ในสังคมไทย การรับรู้ความเสี่ยงบางครั้งถูกบิดเบือนด้วยความเชื่อเรื่อง “ดวง” หรือ “กรรม” (Karma/Fatalism) คนบางกลุ่มอาจเชื่อว่าอุบัติเหตุเกิดจากเคราะห์กรรมที่หลีกเลี่ยงไม่ได้ ทำให้ละเลยมาตรการป้องกันทางวิทยาศาสตร์ เช่น การไม่คาดเข็มขัดนิรภัยเพราะ “มีพระดี” การศึกษาวิจัยพบความสัมพันธ์ระหว่างความเชื่อเรื่องโชคชะตากับพฤติกรรมเสี่ยงบนท้องถนน

ภาพที่ 3.7
กลยุทธ์การจัดการความมั่นคงปลอดภัย
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

8. การวิเคราะห์อาชญากรรม: เครื่องมือการจัดการความมั่นคงปลอดภัย

การวิเคราะห์อาชญากรรม (Crime Analysis) คือการตรวจสอบอย่างเป็นระบบของรูปแบบ แนวโน้ม และปัจจัยบริบทของอาชญากรรมเพื่อสนับสนุนการป้องกัน การจัดสรรทรัพยากร และการตัดสินใจ แม้ว่าเดิมเชื่อมโยงกับการบังคับใช้กฎหมายเท่านั้น แต่ปัจจุบันมีการประยุกต์ใช้อย่างแพร่หลายในบริบทความปลอดภัยระดับองค์กรเช่น ร้านค้า มหาวิทยาลัย โรงพยาบาล ห้องเรียน และระบบขนส่ง การวิเคราะห์นี้มีความสำคัญเพราะช่วยองค์กรให้เข้าใจว่า ความสูญเสียเกิดขึ้นอย่างไร ที่ไหน เมื่อไร และเพราะเหตุใด

การวิเคราะห์อาชญากรรมแปลงข้อมูลดิบจากรายงานเหตุการณ์ สถิติการเกิดความเสียหาย และการสืบสวนเป็นข่าวกรองที่สามารถดำเนินการได้ **(Actionable Intelligence)** โดยการระบุ รูปแบบ (เวลา สถานที่ วิธีการกระทำ อายุของผู้กระทำความผิด) แนวโน้ม (การเปลี่ยนแปลงความถี่หรือประเภทของอาชญากรรมเมื่อเวลาผ่านไป) จุดเสี่ยง (ทางภูมิศาสตร์ที่อาชญากรรมรวมตัวเป็นกลุ่ม) และ วิธีการ **(modus operandi)** ของผู้กระทำความผิด (Nikolic, 2022)

ประเภทของการวิเคราะห์อาชญากรรม

1. การวิเคราะห์เชิงยุทธวิธี (Tactical Analysis): มุ่งเน้นไปที่รูปแบบระยะสั้น (วัน-สัปดาห์) และความต้องการในการตอบสนองทันที มีหน้าที่ระบุรูปแบบอาชญากรรมที่เกิดขึ้นในปัจจุบัน เช่น ซีรีย์การขโมย พื้นที่กระจุกตัวของการลักขโมย ช่วงเวลาที่เกิดเหตุบ่อย และวิธีการกระทำ (MO) ที่ช่วยระบุว่าผู้กระทำความผิดคนเดียวกันหรือต่างคน

2. การวิเคราะห์เชิงกลยุทธ์ (Strategic Analysis): ตรวจสอบแนวโน้มระยะยาว (หลายเดือนถึงหลายปี) เพื่อให้ข้อมูลแก่การวางแผนนโยบาย การจัดสรรงบประมาณ และการตัดสินใจระดับผู้บริหาร มีจุดประสงค์เพื่อระบุสาเหตุพื้นฐาน (Root Causes) ภัยคุกคามที่เกิดใหม่ (Emerging Threats) และรูปแบบระยะยาวที่อาจมีการเปลี่ยนแปลง

3. การวิเคราะห์บริหารงาน (Administrative Analysis): สนับสนุนการรายงานการบริหารจัดการ บัญชี และการปฏิบัติตามกฎหมาย โดยให้สรุปสถิติรวม (Aggregate Statistics) เมตริกประสิทธิภาพ (Key Performance Indicators) และการสื่อสารต่อผู้มีส่วนได้ส่วนเสีย เช่น คณะกรรมการจัดการสถาบัน ผู้บริหาร ประชาชน และสื่อมวลชน การรายงานนี้ใช้เพื่อสาธารณูปการ (Transparency) โต้แย้งความสำเร็จของโปรแกรมความปลอดภัย และความต้องการงบประมาณเพิ่มเติม (Okeke & Oranyelu, 2021)

ภาพที่ 3.8

วัตถุประสงค์ของการวิเคราะห์อาชญากรรม

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

9. ปัจจัยสภาพแวดล้อมและสถานการณ์ (Environmental and Situational Factors)

ความปลอดภัยภายนอกได้รับอิทธิพลอย่างมากจากสภาพแวดล้อมทางกายภาพที่สร้างความสะดวกหรือป้องกันไม่ให้เกิดอาชญากรรม แนวคิดนี้เรียกว่า Crime Prevention Through Environmental Design (CPTED) ซึ่งเสนอว่าการออกแบบและการจัดการสภาพแวดล้อมทางกายภาพสามารถลดโอกาสของการกระทำความผิดได้อย่างมีประสิทธิภาพ (Vellani, 2020)

1. ปัจจัยแสงสว่าง (Lighting): แสงสว่างที่ดีมีบทบาทสำคัญในการป้องกันอาชญากรรม โดยการเพิ่มโอกาสในการถูกพบเห็นและระบุตัวตนของผู้กระทำผิด (Detection Risk) พื้นที่อับแสงหรือมืดสลัวจะกลายเป็นช่องว่างที่เอื้อต่อการแฝงตัวและกระทำผิดโดยไร้พยาน นอกจากนี้ การขาดแคลนแสงสว่างยังส่งสัญญาณเชิงลบถึงการขาดการดูแลเอาใจใส่ (Signal of Neglect) ซึ่งอาจดึงดูดให้เกิดปัญหาอาชญากรรมและพฤติกรรมที่ไม่พึงประสงค์ตามมาได้ ตัวอย่างเช่น ที่จอดรถใต้สะพานลอยหลายแห่งในกรุงเทพฯ ซึ่งเคยมีแสงสว่างไม่เพียงพอ มักเป็นจุดที่เกิดเหตุลักขโมยรถยนต์บ่อยครั้ง

หลังจากที่มีการติดตั้งระบบไฟส่องสว่างแบบ LED เพิ่มเติมอย่างเหมาะสม อัตราการเกิดอาชญากรรมในจุดเหล่านั้นก็ลดลงอย่างเห็นได้ชัด

2. การมองเห็นและแนวสายตา (Visibility and Sightlines): การมองเห็นที่เปิดกว้างช่วยให้มีการเฝ้าระวังตามธรรมชาติ (Natural Surveillance) เนื่องจากบุคคลที่อยู่ในบริเวณอื่น ๆ สามารถสังเกตกิจกรรมที่น่าสงสัยได้ ในทางตรงกันข้าม ต้นไม้ขนาดใหญ่ พุ่มไม้หนาแน่น กำแพงที่สูง หรือการออกแบบอาคารที่มีจุดอับสายตา (Blind Spots) จะลดประสิทธิภาพของการเฝ้าระวังนี้และอาจกลายเป็นที่ซ่อนตัวของผู้ไม่หวังดี ตัวอย่างที่เห็นชัด คือ การจัดการสวนสาธารณะในเมืองที่มักตัดแต่งต้นไม้เป็นระยะเพื่อรักษามุมมองที่โปร่งตาและปลอดภัย

3. ความหนาแน่นของฝูงชน (Crowd Density): ความหนาแน่นของฝูงชนมีทั้งด้านบวกและด้านลบ ในระดับที่พอเหมาะ จะมีพยานอยู่รอบข้างเพียงพอที่จะช่วยสังเกตและแจ้งเหตุได้ทันท่วงที แต่หากแออัดเกินไป กลับอาจเกิดความวุ่นวายและยากต่อการควบคุม สภาพเช่นนี้กลายเป็นโอกาสเหมาะสำหรับการกระทำผิด เช่น การลักขโมยหรือฉกชิง ตัวอย่างที่เป็นรูปธรรม คือ ตลาดนัดสุดสัปดาห์ทั่วกรุงเทพฯ ซึ่งมักพบการลักขโมยสูงสุดในชั่วโมงเร่งด่วนที่ผู้คนเบียดเสียดที่สุด

4. การบำรุงรักษาและความเป็นระเบียบ (Maintenance and Order): การดูแลรักษาพื้นที่อย่างดีส่งสัญญาณเชิงบวกว่าบริเวณนั้นอยู่ภายใต้การดูแลเอาใจใส่และมีการเฝ้าระวังอย่างต่อเนื่อง หลักการ “ทฤษฎีหน้าต่างแตก” (Broken Windows Theory) ชี้ให้เห็นว่าความเสื่อมโทรมที่มองเห็นได้ชัดเจน (Visible Disorder) เช่น การวาดกราฟฟิตีโดยไม่อนุญาต ขยะสะสม สิ่งของชำรุดเสียหาย หรือพื้นที่รกรุงรัง ล้วนเป็นเสมือนการเชื้อเชิญให้เกิดพฤติกรรมที่ไม่พึงประสงค์และอาชญากรรมรุนแรงตามมาได้ ในทางกลับกัน การรักษาสภาพแวดล้อมให้สะอาด เรียบร้อย และได้รับการดูแลอย่างดี สื่อถึงการมีผู้รับผิดชอบชัดเจน ซึ่งช่วยสร้างบรรยากาศแห่งการป้องปรามอาชญากรรมได้โดยธรรมชาติ (Wilson & Kelling, 1982)

5. เส้นทางหลบหนี (Escape Routes): ผู้กระทำความผิดมักคำนวณความเสี่ยงด้วยการประเมินโอกาสในการหลบหนีหลังจากกระทำผิด พื้นที่ซึ่งมีทางออกเดียวหรือเป็นทางตัน (Dead Ends) จะเพิ่มความเสี่ยงต่อการถูกจับกุมของผู้กระทำผิด จึงมีผลในการป้องปรามอาชญากรรมได้ดี ในขณะที่พื้นที่ซึ่งมีช่องทางหลบหนีหลายทิศทาง (Multiple Exit Routes) มักเป็นจุดดึงดูดสำหรับผู้ที่มองหาวิธีหลบเลี่ยงการติดตามอย่างรวดเร็ว

ตัวอย่างเช่น สถานีรถไฟฟ้าใต้ดิน (MRT) และรถไฟฟ้าบีทีเอส (BTS) ในกรุงเทพฯ ได้รับการออกแบบและปรับปรุงเพื่อควบคุมจำนวนทางออก-เข้าอย่างเป็นทางการให้มีจำนวนจำกัด ซึ่งช่วยให้การดูแลรักษาความปลอดภัย การติดตามบุคคล และการจัดการในกรณีเกิดเหตุฉุกเฉินมีประสิทธิภาพมากขึ้น ส่งผลให้ผู้ไม่หวังดีประเมินว่ามีโอกาสถูกจับกุมสูงหากกระทำผิดในพื้นที่ดังกล่าว (Okeke & Oranyelu, 2021)

ภาพที่ 3.9
วัตถุประสงค์ของการวิเคราะห์อาชญากรรม
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

10. ข่าวกรองความมั่นคงและการสแกนสถานการณ์ (Intelligence and Situational Scanning)

ข่าวกรองความมั่นคง (Security Intelligence) มิได้เป็นเพียงเรื่องในภาพยนตร์ หากแต่เป็นศาสตร์ที่อาศัยการรวบรวมและวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ อย่างเป็นระบบ เพื่อสนับสนุนการตัดสินใจเชิงนโยบายและปฏิบัติการ (Data-Informed Decision Making) นักบริหารความปลอดภัยสมัยใหม่จำเป็นต้องมีสายตากว้างไกล เพื่อคาดการณ์แนวโน้มภัยคุกคามที่อาจส่งผลกระทบต่อเส้นทางเดินขององค์กรในอนาคต และสามารถออกแบบมาตรการป้องกันเชิงรุกได้อย่างมีประสิทธิภาพ

1. OSINT (Open Source Intelligence) ข่าวกรองจากแหล่งข้อมูลสาธารณะ

OSINT หมายถึงกระบวนการรวบรวมข่าวกรองจากแหล่งข้อมูลเปิดที่ผู้คนทั่วไปเข้าถึงได้ เช่น บนโซเชียลมีเดีย (Facebook, X (Twitter), TikTok, Instagram) ข่าวสารออนไลน์ เว็บบอร์ด สื่อมวลชน และเอกสารราชการ นักบริหารความปลอดภัยนำ OSINT มาใช้เพื่อติดตามประเมินสถานการณ์ภัยคุกคาม ตรวจสอบข่าวสารล่าสุด ติดตามกิจกรรมของกลุ่มที่ไม่พึงประสงค์ รวมถึงระบุสัญญาณบ่งชี้ความเสี่ยงตั้งแต่เนิ่น ๆ (Indicators of Compromise) (Hwang, Lee, Kim, Lee, & Kim, 2022)

ในบริบทไทย ข้อมูล OSINT สามารถรวบรวมได้จากการแถลงการณ์ของทางราชการ ข่าวอาชญากรรม การแจ้งเตือนจากระบบขนส่งสาธารณะ (BTS/MRT) การสื่อสารขององค์กรและมหาวิทยาลัยผ่านช่องทางออนไลน์ ตลอดจนการแลกเปลี่ยนความคิดเห็นในชุมชนดิจิทัล การวิเคราะห์ข้อมูลเหล่านี้ช่วยให้องค์กรตรวจจับการเปลี่ยนแปลงของแนวโน้มภัยคุกคามใหม่ ๆ ได้ทันเวลา และปรับปรุงมาตรการรักษาความปลอดภัยให้สอดคล้องกับสถานการณ์จริง

2. การแสกนสถานการณ์ด้วยกรอบ PESTLE

นักบริหารความปลอดภัยจำเป็นต้องหมั่นสำรวจปัจจัยแวดล้อมภายนอกอย่างสม่ำเสมอ โดยใช้กรอบวิเคราะห์ PESTLE เพื่อตรวจจับสัญญาณที่อาจส่งผลต่อความมั่นคงปลอดภัยขององค์กร:

P - การเมือง (Political): ความไม่แน่นอนทางการเมือง การชุมนุม หรือการเปลี่ยนแปลงนโยบายของรัฐ (เช่น นโยบายกัญชาเสรี หรือการปราบปรามยาเสพติด) อาจส่งผลต่อระดับความเสี่ยง ความปลอดภัยสาธารณะ และการจัดสรรทรัพยากรด้านความปลอดภัย

E - เศรษฐกิจ (Economic): สภาวะเศรษฐกิจที่อาจเผชิญความท้าทายในช่วงปี 2568-2569 อาจส่งผลกระทบต่อกำลังซื้อของครัวเรือน และเพิ่มแรงกดดันทางสังคม ซึ่งมีศักยภาพที่จะกระตุ้นให้เกิดอาชญากรรมประเภทฉ้อโกง การลักขโมย และการกู้ยืมนอกระบบ

S - สังคม (Social): โครงสร้างสังคมผู้สูงอายุของไทย (Aging Society) ทำให้กลุ่มนี้ตกเป็นเป้าหมายของการคุกคามรูปแบบต่าง ๆ เช่น แก๊งคอลเซ็นเตอร์ (Call Center Scams) นอกจากนี้ ประเด็นด้านสุขภาพจิตของวัยรุ่นและระดับความเครียดในสังคม ก็อาจเป็นปัจจัยที่นำไปสู่พฤติกรรมที่ไม่เหมาะสมได้

T - เทคโนโลยี (Technological): ความก้าวหน้าของปัญญาประดิษฐ์ (AI) เทคโนโลยี 5G และควอนตัมคอมพิวติ้ง (Quantum Computing) กำลังเปลี่ยนโฉมภูมิทัศน์ของภัยคุกคามทางไซเบอร์ โดยสร้างวิธีการโจมตีที่ซับซ้อนและยากต่อการตรวจจับมากขึ้น

L - กฎหมาย (Legal): การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎหมายความมั่นคงปลอดภัยไซเบอร์อย่างจริงจังมากขึ้น ส่งผลให้องค์กรต้องให้ความสำคัญกับการลงทุนเพื่อปกป้องข้อมูลมิเช่นนั้นอาจต้องเผชิญบทลงโทษทางกฎหมายและความเสียหายต่อชื่อเสียง

E - สิ่งแวดล้อม (Environmental): ภัยธรรมชาติที่รุนแรงขึ้น เช่น อุทกภัย ภัยแล้ง และปัญหามลภาวะ ถือเป็นความเสี่ยงรูปแบบใหม่ที่กระทบต่อความต่อเนื่องของการดำเนินธุรกิจ (Business Continuity) และความเป็นอยู่ของบุคลากร

การผสานการทำงานระหว่างระบบ OSINT และกรอบวิเคราะห์ PESTLE ช่วยส่งเสริมให้องค์กรก้าวไปสู่การบริหารความเสี่ยงเชิงรุก โดยสามารถคาดการณ์สถานการณ์และเตรียมความพร้อมล่วงหน้า แทนที่จะเพียงตั้งรับหลังเกิดเหตุ (Ricci et al., 2021)

ภาพที่ 3.10
ปัจจัยมนุษย์ในความเสี่ยงด้านไซเบอร์
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

11. ภัยคุกคามทางไซเบอร์และความเสี่ยงในโลกดิจิทัล (Cyber Threats and Digital Vulnerabilities)

ภัยไซเบอร์มีความแตกต่างจากอาชญากรรมรูปแบบดั้งเดิมในหลายประเด็นพื้นฐาน ทำให้กลยุทธ์การป้องกันแบบเดิมไม่สามารถรับมือได้อย่างมีประสิทธิภาพเพียงพอ

ลักษณะเฉพาะของภัยไซเบอร์

1. ไร้พรมแดน (Borderless): ผู้โจมตีสามารถปฏิบัติการจากที่ใดในโลกก็ได้โดยไม่จำเป็นต้องอยู่ในประเทศเดียวกับเป้าหมาย การโจมตีที่กำเนิดจากเซิร์ฟเวอร์ในยุโรป อเมริกา หรือเอเชียอาจมีเป้าหมายเป็นองค์กรในไทยโดยตรง สร้างความซับซ้อนในการสืบสวนและดำเนินคดีตามกฎหมายข้ามเขตอำนาจศาล

2. ขยายผลได้สูง (Highly Scalable): แค่การโจมตีครั้งเดียวสามารถพุ่งเป้าไปยังผู้ใช้หลายพันหรือหลายล้านรายได้พร้อมกัน ตัวอย่างเช่น แคมเปญฟิชชิ่งสามารถส่งอีเมลหลอกลวงถึงหนึ่งแสนฉบับได้ในเวลาไม่กี่นาที ขณะที่แรนซัมแวร์ (Ransomware) สามารถแพร่กระจายทั่วเครือข่ายขององค์กรได้ภายในระยะเวลาอันสั้น

3. ไม่ระบุตัวตน (Anonymity) และปิดบังร่องรอย (Obfuscation): ผู้โจมตีมักใช้เทคโนโลยีเช่น เครือข่ายส่วนตัวเสมือน (VPN) เครือข่าย Tor และสกุลเงินดิจิทัล (Cryptocurrency) เพื่อปกปิดตัวตนและเส้นทางการเงิน การใช้ Proxy Servers และการปลอมแปลง IP Address ทำให้การติดตามกลับไปยังแหล่งที่มาทำได้ยากยิ่งขึ้น

4. ปรับตัวได้เร็ว (Adaptive) และคุกคามอย่างต่อเนื่อง (Advanced Persistent Threats - APTs): โดยเฉพาะกลุ่มโจมตีขั้นสูงที่อาจได้รับการสนับสนุนจากรัฐ (State-Sponsored) สามารถปรับเปลี่ยนเทคนิคเมื่อพบกับระบบป้องกัน และสามารถแฝงตัวอยู่ในระบบเป็นเวลานานเพื่อขโมยข้อมูลหรือสร้างความเสียหายอย่างต่อเนื่อง

5. ปัจจัยมนุษย์เป็นจุดอ่อนสำคัญ: ข้อมูลทางสถิติบ่งชี้ว่าการโจมตีทางไซเบอร์ส่วนใหญ่ (มากกว่า 90%) มีสาเหตุจากความผิดพลาดของมนุษย์ เช่น การคลิกลิงก์ในอีเมลปลอม (Phishing) การใช้รหัสผ่านที่คาดเดาได้ง่าย หรือการเปิดไฟล์อันตราย

ภาพที่ 3.11
สถานการณ์ภัยคุกคามไซเบอร์ในประเทศไทย
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

องค์กรที่สามารถจัดการความเสี่ยงกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมักนิยมใช้แนวทางแบบผสมผสาน (Hybrid Approach) โดยการลงทุนในโซลูชันทางเทคโนโลยีที่ทันสมัยควบคู่ไปกับการบ่มเพาะวัฒนธรรมความปลอดภัยไซเบอร์ที่ฝังรากลึกในทีมงานทุกคน (Sonar, Anvekar, & Hebbalkar, 2025)

12. บทสรุป (Conclusion)

จากเกาะ Isla Nublar ในจินตนาการมาสู่โลกแห่งความเป็นจริงบนท้องถนนและโลกไซเบอร์ บทนี้ได้สำรวจภูมิทัศน์ของภัยคุกคามอย่างรอบด้าน สะท้อนให้เห็นว่าความปลอดภัยมิได้อยู่แค่การสร้างกำแพงสูงหรือติดตั้งอุปกรณ์ทันสมัย หากแต่อยู่ที่การเข้าใจธรรมชาติของ “ภัยคุกคาม” และ “จุดอ่อน” ที่เหล่ามิจฉาชีพหาประโยชน์ ดังเช่นกรณีเดนนิส เนดรีใน *Jurassic Park* ที่สอนเราว่า แม้จะมีระบบชั้นสูง แต่หากขาดการตรวจสอบการควบคุมการเข้าถึงที่รัดกุม และระบบสำรองข้อมูลที่เชื่อถือได้ จุดอ่อนเหล่านี้ก็จะกลายเป็นช่องว่างที่ภัยคุกคามฉกฉวยโอกาสเสมอ ปรัชญาที่แท้จริงจึงไม่ใช่การพยายามกำจัดภัยคุกคามให้หมดไป แต่คือการลดจุดอ่อนให้มากที่สุดและทำให้ต้นทุนของการโจมตีสูงจนไม่คุ้มค่าการเสี่ยง

บทเรียนที่สำคัญอีกประการคือ การออกแบบความปลอดภัยต้องหยั่งรากลงในบริบทและวัฒนธรรมท้องถิ่น มาตรการที่ได้ผลในหนึ่งประเทศอาจล้มเหลวในอีกประเทศหากไม่เข้าใจค่านิยมทางสังคม เช่น ความ “เกรงใจ” ที่อาจทำให้พนักงานไม่กล้าแจ้งปัญหา ความ “ไม่เป็นไร” ที่ทำให้มาตรการคลายตัว หรือ “ระบบอุปถัมภ์” ที่ส่งผลต่อการบังคับใช้กฎ การสร้างความปลอดภัยที่ยั่งยืนจึงต้อง “ปรับสูตร” ให้เข้ากับรสนิยมและวิถีชีวิตของสังคมไทย ไม่ใช่เพียงการคัดลอกแนวทางสากลมาปรับใช้อย่างผิวเผิน

ในยุคที่ภัยคุกคามพัฒนารวดเร็วกว่าการตั้งรับ ความรู้เท่าทันและข่าวกรองจึงเป็นเกราะป้องกันที่สำคัญที่สุด การใช้กรอบวิเคราะห์ PESTLE เพื่อสแกนสัญญาณจากสภาพแวดล้อมรอบตัว และการสกัดข้อมูลจากแหล่งสาธารณะ (OSINT) ไม่ใช่เพียงเครื่องมือของหน่วยงานบังคับใช้กฎหมายอีกต่อไป แต่เป็นทักษะพื้นฐานที่ทุกองค์กรต้องมีเพื่อเปลี่ยนจากการตั้งรับเป็นการคาดการณ์และเตรียมรับมืออย่างฉลาด บทต่อไปจะนำเราเข้าสู่ขั้นตอนปฏิบัติการที่สำคัญ นั่นคือ “การประเมินความเสี่ยง” ซึ่งเป็นกระบวนการที่จะแปลงความกังวลและข้อมูลที่สับสนให้กลายเป็นแผนงานที่เป็นระบบ มีลำดับความสำคัญชัดเจน และนำไปสู่การตัดสินใจที่มั่นคง เพื่อสร้างเกราะป้องกันที่แข็งแกร่งและเหมาะสมสำหรับชุมชนและองค์กรไทยในโลกที่เปลี่ยนแปลงไม่หยุดนิ่ง

13. คำถามทบทวน (Review Questions)

1. จงอธิบายความแตกต่างระหว่าง “ภัยคุกคาม (Threat)”, “ความเสี่ยง (Risk)” และ “จุดอ่อน (Vulnerability)” พร้อมยกตัวอย่างสถานการณ์เดียวกันที่สามารถอธิบายทั้งสามแนวคิดได้อย่างชัดเจน?

2. เหตุใดการประเมินภัยคุกคามโดยไม่พิจารณาจุดอ่อนขององค์กรจึงอาจนำไปสู่การตัดสินใจด้านความมั่นคงปลอดภัยที่ผิดพลาด หรือสิ้นเปลืองทรัพยากรโดยไม่จำเป็น?

3. จงอธิบายความแตกต่างระหว่างภัยคุกคามที่เกิดจากมนุษย์ (Human-made Threats) และภัยคุกคามจากธรรมชาติ (Natural Hazards) และอภิปรายว่าผู้จัดการความมั่นคงปลอดภัยควรปรับแนวทางการจัดการอย่างไรให้เหมาะสมกับภัยทั้งสองประเภท?

4. อธิบายความแตกต่างระหว่าง “ความเสี่ยงที่รับรู้” (Perceived Risk) กับ “ความเสี่ยงที่แท้จริง” (Actual Risk) และวิเคราะห์ว่าความไม่สอดคล้องกันระหว่างความเสี่ยงทั้งสองรูปแบบนี้อาจส่งผลต่อการตัดสินใจด้านงบประมาณและมาตรการความมั่นคงปลอดภัยขององค์กรอย่างไร?

5. จากความสัมพันธ์ระหว่างภัยคุกคาม ความเสี่ยง และจุดอ่อน จงอภิปรายว่าบทบาทของผู้จัดการความมั่นคงปลอดภัยควรเน้นไปที่การ “ลดภัยคุกคาม” หรือ “ลดจุดอ่อน” มากกว่ากัน และเพราะเหตุใด?

14. เอกสารอ้างอิง (References)

Anton, N., & Nedelcu, A. (2018). Security risk analysis and management. *MATEC Web of Conferences, 178*, 08015. https://doi.org/10.1051/matecconf/201817808015

Chen, S., Xiang, D., Jin, B., & Jin, H. (2024). Vulnerability assessment for physical protection systems of cave temples: A fuzzy Petri net approach. *Heliyon, 10*, e33100.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Ghazal, T. M., Hasan, M. K., Hassan, R., Islam, S., Sheikh Abdullah, S. N. H., Afifi, M. A. M., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technology, 63*(1s), 1566–1574.

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing, 2022*, Article 1290129. https://doi.org/10.1155/2022/1290129

Majlingová, A. (2024). *Safety and security risks theory* [University textbook]. Technical University in Zvolen, Faculty of Wood Sciences and Technology. ISBN 978-80-228-3417-9.

Nikolic, S. (2022, October 8). *Intelligence analysis and crime investigation*. Interpolice (IPO Law Enforcement Department). https://www.interpolice.org/post/intelligence-analysis-and-crime-investigation

Okeke, O. C., & Oranyelu, F. O. (2021). An overview of crime analysis, prevention and prediction using data mining based on real time and

location data. *International Journal of Engineering Applied Sciences and Technology, 5*(10), 99–103.

Ricci, S., Janout, V., Parker, S., Jerabek, J., Hajny, J., Chatzopoulou, A., & Badonnel, R. (2021). PESTLE analysis of cybersecurity education. In *ARES 2021: Proceedings of the 16th International Conference on Availability, Reliability and Security* (Article 21, 1–8). ACM. https://doi.org/10.1145/3465481.3469184

Scholz, R. W. (2017). Digital threat and vulnerability management: The SVIDT method. *Sustainability, 9*(4), 554. https://doi.org/10.3390/su9040554

Sangsinchai, S. (2025, December 29). *Catastrophe in the South: How record rainfall and fragmented governance triggered Thailand's deadliest flood crisis*. The Nation. https://www.nationthailand.com/blogs/the-nation-special-report/40059516nationthailand+1

Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X. (2015). From physical security to cybersecurity. *Journal of Cybersecurity, 1*(1), 19–36.

Sonar, O., Anvekar, N., & Hebbalkar, S. (2025). Phishing and social engineering: Analyzing human vulnerability. *International Journal of Scientific Research and Engineering Development, 8*(4), 1322–1331.IJSRED-V8I4P132.pdf

Vellani, K. (2020). *Strategic security management: A risk assessment guide for decision makers* (2nd ed.). CRC Press.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows: The police and neighborhood safety. *The Atlantic Monthly, 249*(3), 29–38.