SMA1202
SECURITY: THEORY AND PRACTICE
หลักการและทฤษฎีความมั่นคงปลอดภัย

CHAPTER 1
INTRODUCTION TO SECURITY MANAGEMENT

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

บทที่ 1
บทนำสู่การจัดการความมั่นคงปลอดภัย
(Introduction to Security Management)

1. บทนำ (Introduction)

1.1 ความล้มเหลวเชิงระบบและภาพลวงตาแห่งความมั่นคงปลอดภัย (Systemic Failure and the Illusion of Safety)

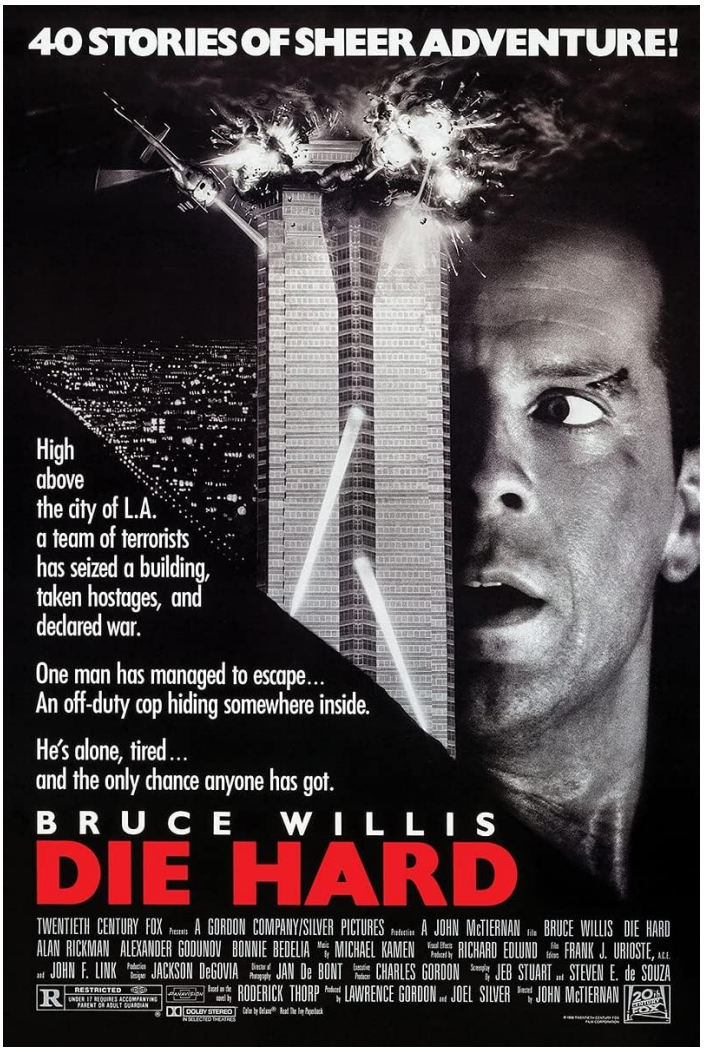
ในประวัติศาสตร์ภาพยนตร์แอ็กชันระดับตำนานของฮอลลีวูด น้อยเรื่องนักที่จะสามารถถ่ายทอดแก่นแท้ของ “ความล้มเหลวในการรักษาความมั่นคงปลอดภัย” (Security Failure) ได้อย่างชัดเจนและเป็นอมตะเท่ากับภาพยนตร์เรื่อง *Die Hard* หรือในชื่อภาษาไทยว่า “นรกระฟ้า” (1988) ซึ่งฉากเปิดของเรื่องนำเสนอภาพของตึกระฟ้า “นากาโตมิ พลาซ่า” (Nakatomi Plaza) ใจกลางนครลอสแอนเจลิส อาคารแห่งนี้ไม่ได้เป็นเพียงสิ่งปลูกสร้าง แต่ถูกนำเสนอในฐานะสัญลักษณ์แห่งอำนาจ ความมั่งคั่ง และความทันสมัยขององค์กรข้ามชาติญี่ปุ่นในช่วงทศวรรษที่ 80 ด้วยสถาปัตยกรรมกระจกและเหล็กกล้าที่ตั้งตระหง่าน ระบบล็อกประตูรหัสผ่านอิเล็กทรอนิกส์ที่ชั้นผู้บริหาร (Executive Floor) กล้องวงจรปิดที่ครอบคลุมพื้นที่ส่วนกลาง และเจ้าหน้าที่รักษาความปลอดภัยในเครื่องแบบที่เฝ้าประจำการอยู่บริเวณล็อบบี้อย่างเคร่งครัด ในมุมมองของพนักงานที่กำลังสังสรรค์ในงานปาร์ตี้วันคริสต์มาสและบุคคลภายนอก นากาโตมิ พลาซ่า คือ “ป้อมปราการ” (Fortress) ที่ไม่มีวันถูกเจาะทะลวงได้

อย่างไรก็ตาม เพียงไม่กี่นาทีต่อมา ภาพลักษณ์ความมั่นคงปลอดภัยเหล่านั้นกลับพังทลายลงอย่างสิ้นเชิง กลุ่มผู้ก่อการร้ายที่มีการจัดการองค์กรอย่างดีเยี่ยม นำโดย ฮานส์ กรูเบอร์ (Hans Gruber) สามารถยึดครองอาคารทั้งหลังได้อย่างง่ายดายจนน่าตกใจ สิ่งที่น่าสนใจสำหรับการศึกษาการจัดการความมั่นคงปลอดภัยคือ “วิธีการ” ที่พวกผู้ก่อการร้ายใช้ พวกเขาไม่ได้ใช้รถถังพังประตู หรือโรยตัวลงมาจากเฮลิคอปเตอร์เพื่อระเบิดดาดฟ้าในขั้นตอนแรก แต่ผู้บุกรุกใช้วิธีการที่เรียบง่ายและแนบเนียนกว่านั้น คือการ “เดินเข้าไป” ผ่านจุดที่อ่อนแอที่สุดขององค์กร

กลุ่มผู้ก่อการร้ายแฝงตัวมาในคราบของพนักงานส่งของ ขับรถบรรทุกเข้าไปในจุดโหลดสินค้าใต้ดิน (Loading Dock) ซึ่งเป็นจุดที่มักถูกมองข้ามในการออกแบบระบบรักษาความปลอดภัย (Security Design) เพราะถือว่าเป็นพื้นที่บริการ (Service Area) ที่ไม่มีความสวยงามและมักมีมาตรการควบคุมที่หละหลวมกว่าล็อบบี้หลัก เจ้าหน้าที่รักษาความปลอดภัยที่จุดต้อนรับ (Concierge) ซึ่งทำหน้าที่เป็นด่านหน้า ขาดการฝึกอบรมในทักษะ

การสังเกตและตรวจสอบบุคคล (Observation and Screening Skills) เขาถูกหลอกด้วยกลอุบายง่าย ๆ และถูกสังหารในทันทีโดยไม่มีโอกาสได้แจ้งเตือนภัย

เมื่อผู้บุกรุกเข้าสู่พื้นที่ภายในได้แล้ว พวกเขาแสดงให้เห็นถึงความเข้าใจในระบบของอาคารดีกว่าเจ้าของสถานที่ ระบบคอมพิวเตอร์ที่ทันสมัยที่สุดในยุคนั้น ซึ่งถูกออกแบบมาเพื่ออำนวยความสะดวกและควบคุมอาคาร กลับกลายเป็น “อาวุธ” ที่ผู้ก่อการร้ายใช้ย้อนกลับมาทำร้ายผู้อยู่อาศัย พวกเขาทำการตัดขาดช่องทางการสื่อสารทั้งหมด ปิดระบบลิฟต์ และล็อกประตูทุกบานเพื่อเปลี่ยนอาคารสำนักงานให้กลายเป็นคุกสำหรับตัวประกัน ความล้มเหลวที่นากาโตมิ พลาซ่า จึงไม่ใช่ความล้มเหลวทางเทคโนโลยี (Technological Failure) เพราะประตูนิรภัยของห้องมั่นคงนั้นมีความหนาและซับซ้อนตามมาตรฐานสากล แต่สิ่งที่เกิดขึ้นคือ “ความล้มเหลวในการบริหารจัดการ” (Management Failure)



ภาพที่ 1.1
โปสเตอร์ภาพยนต์ *Die Hard*
ที่มา: 20th Century Fox (1988)

บทเรียนสำคัญจากภาพยนตร์เรื่องนี้ที่ยังคงใช้สอนในหลักสูตรความมั่นคงปลอดภัยทั่วโลกคือ **“ความมั่นคงปลอดภัยไม่ใช่ผลิตภัณฑ์ แต่เป็นกระบวนการ”** (Security is a process, not a product) การมีกล้องวงจรปิดราคาแพงหรือเจ้าหน้าที่รปภ. จำนวนมากไม่ได้การันตีความมั่นคงปลอดภัยหากขาดการวางแผนเชิงกลยุทธ์ (Strategic Planning) การประเมินความเสี่ยงที่ครอบคลุม (Comprehensive Risk Assessment) และการขาดความตระหนักรู้ว่าภัยคุกคามสามารถมาในรูปแบบที่ไม่คาดคิดเสมอ

1.2 จากนากาโตมิสู่สยามพารากอน: บริบทความจริงในสังคมไทย (Contextualizing to Thailand)

สำหรับนักศึกษาและผู้ประกอบวิชาชีพในประเทศไทย ฉากในภาพยนตร์ข้างต้นไม่ใช่เรื่องไกลตัวหรือเป็นเพียงจินตนาการของผู้กำกับ หากเราพิจารณาเหตุการณ์โศกนาฏกรรมกราดยิงที่ศูนย์การค้าสยามพารากอน (Siam Paragon Shooting) เมื่อวันที่ 3 ตุลาคม 2023 (Thailand Convention and Exhibition Bureau [TCEB], 2023) เราจะพบความคล้ายคลึงกันในเชิงโครงสร้างของปัญหากับกรณีนากาโตมิ พลาซ่า อย่างน่าตกใจ

ศูนย์การค้าสยามพารากอน เปรียบเสมือนนากาโตมิของกรุงเทพมหานคร เป็นสัญลักษณ์ของความทันสมัย ไลฟ์สไตล์ระดับโลก และเป็นจุดหมายปลายทางของนักท่องเที่ยวทั่วโลก ในวันเกิดเหตุ อาคารแห่งนี้มีมาตรการรักษาความมั่นคงปลอดภัยตามมาตรฐานปกติ มีเจ้าหน้าที่รักษาความปลอดภัยประจำจุดต่าง ๆ มีระบบกล้องวงจรปิด และมีเครื่องตรวจจับโลหะ (Walk-through Metal Detector) ที่ประตูทางเข้าบางจุด แต่ผู้ก่อเหตุซึ่งเป็นเยาวชนอายุเพียง 14 ปี สามารถพกพาอาวุธปืนดัดแปลง (Modified Blank Gun) เข้าสู่พื้นที่ห้างสรรพสินค้าได้อย่างง่ายดาย

ทำไมระบบจึงล้มเหลว? การวิเคราะห์เชิงลึกชี้ให้เห็นว่า ความล้มเหลวในกรณีนี้ไม่ได้อยู่ที่ “จำนวน” ของเจ้าหน้าที่ แต่อยู่ที่ “คุณภาพ” และ “กระบวนการ” (Process and Quality) นั่นเอง

1. มาตรการคัดกรองที่เน้นพิธีกรรม (Ritualistic Screening): กล่าวได้ว่า การตรวจค้นที่ประตูทางเข้ามักทำเพื่อผลทางจิตวิทยา (Psychological Deterrence) มากกว่าการป้องกันจริง การตรวจกระเป๋าแบบขอไปที หรือเครื่องตรวจจับโลหะที่ร้องเตือนแต่ไม่มีการตรวจสอบต่อ (Security Theater) กลายเป็นช่องว่างที่ผู้ก่อเหตุใช้ประโยชน์

2. การตอบสนองต่อเหตุวิกฤต (Crisis Response): ในกรณีนี้ เมื่อเสียงปืนดังขึ้น ความโกลาหลเกิดขึ้นทันที ปรากฏการณ์ที่เห็นชัดคือ “การขาดการสื่อสารที่ชัดเจน” (Lack of Clear Communication) ประชาชนวิ่งหนีอย่างไร้ทิศทาง บางส่วนเข้าไปซ่อนตัวในห้องน้ำที่ประตูไม่แข็งแรง หรือร้านค้าที่ไม่มีระบบล็อกนิรภัยจากด้านใน ซึ่งสะท้อนให้เห็นว่าแผนเผชิญเหตุ (Incident Response Plan) อาจยังไม่ได้ถูกซ้อมหรือสื่อสารไปยังผู้เช่าพื้นที่และพนักงานอย่างทั่วถึงเพียงพอ

ผลกระทบจากเหตุการณ์นี้รุนแรงและกว้างขวางกว่าความเสียหายทางกายภาพ ชื่อเสียงของประเทศในฐานะแหล่งท่องเที่ยวที่ปลอดภัย (Safe Destination) ถูกสั่นคลอนทันที สื่อต่างชาติรายงานข่าวไปทั่วโลก ส่งผลให้นักท่องเที่ยวชาวจีนซึ่งเป็นกลุ่มเป้าหมายหลัก ยกเลิกการเดินทางเข้าไทยกว่า 60,000 รายในระยะเวลาสั้น ๆ นี่คือตัวอย่างที่ชัดเจนว่า ความล้มเหลวของการจัดการความมั่นคงปลอดภัยเพียงจุดเดียว สามารถสร้างความเสียหายทางเศรษฐกิจระดับมหภาค (Macro-economic Impact) ได้อย่างมหาศาล (Newport, 2023)

1.3 ภัยคุกคามในยุคดิจิทัล: กรณีศึกษา 9Near (Digital Threats)

นอกจากภัยคุกคามทางกายภาพ (Physical Threats) แล้ว ประเทศไทยยังเผชิญกับภัยคุกคามในรูปแบบดิจิทัลที่ท้าทายไม่แพ้กัน กรณีศึกษาของแฮกเกอร์ที่ใช้นามแฝงว่า “9Near” ในปี 2023 ซึ่งประกาศขายข้อมูลส่วนบุคคลของคนไทย 55 ล้านคน เปรียบเสมือนการบุกรุกเข้าไปในตู้นิรภัยของนากาโตมิ พลาซ่า แต่ในเวอร์ชันดิจิทัล จะเห็นได้ว่า อาชญากรในกรณีนี้ไม่ต้องใช้ปืน ไม่ต้องใช้ระเบิด C4 และไม่ต้องเดินทางมายังสถานที่จริง แต่ใช้การเจาะผ่านช่องโหว่ของการบริหารจัดการข้อมูล (Data Governance) และความหละหลวมของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานของรัฐหรือ Third-party vendor ที่เชื่อมต่อระบบ ข้อมูลที่รั่วไหลประกอบด้วย ชื่อ-นามสกุล, เลขประจำตัวประชาชน, วันเดือนปีเกิด และเบอร์โทรศัพท์ ซึ่งเป็นกุญแจสำคัญที่มิจฉาชีพสามารถนำไปต่อยอดในการหลอกลวง (Scam) หรือการสวมรอยอัตลักษณ์ (Identity Theft) (Allan, 2025)

เหตุการณ์ 9Near และการโจมตีทางไซเบอร์ที่เพิ่มขึ้นกว่า 70% ในประเทศไทย เมื่อเทียบกับค่าเฉลี่ยโลกในปี 2024-2025 เป็นสัญญาณเตือนภัยระดับชาติว่า “สินทรัพย์” (Assets) ที่สำคัญที่สุดในศตวรรษที่ 21 อาจไม่ใช่ทองคำหรือเงินสดในตู้เซฟอีกต่อไป แต่เป็น “ข้อมูล” (Information) และหน้าที่ของผู้จัดการความปลอดภัยสมัยใหม่ คือการปกป้องสินทรัพย์ที่มองไม่เห็นเหล่านี้ด้วยความเข้มข้นเท่ากับ หรือมากกว่าการปกป้องอาคารสถานที่ ((Mascellino, 2024)

บทที่ 1 นี้ จะพานักศึกษาไปทำความเข้าใจรากฐานของวิชาชีพนี้ เพื่อตอบคำถามว่า ทำไม “การรักษาความมั่นคงปลอดภัย” (Security) จึงไม่ใช่แค่เรื่องของการจ้างยามมาเฝ้าประตู หรือการติดตั้งกล้องวงจรปิดให้ครบทุกมุม แต่เป็น ศาสตร์แห่งการบริหารจัดการ (Management Discipline) ที่ต้องอาศัยการวางแผนเชิงกลยุทธ์ การวิเคราะห์ความเสี่ยง การบริหารทรัพยากรมนุษย์ และความเข้าใจในกฎหมายและวัฒนธรรมไทย เพื่อปกป้องค์กรให้รอดพ้นจากภัยคุกคามที่ซับซ้อนและไร้พรมแดน

2. ความหมายและแนวคิดของการจัดการความมั่นคงปลอดภัย (Meaning and Concept of Security Management)

2.1 นิยามของความมั่นคงปลอดภัย: มุมมองทวิลักษณ์ (Dual Perspective of Security)

ในการศึกษาด้านความมั่นคงปลอดภัย สิ่งแรกที่ต้องทำความเข้าใจคือนิยามของคำศัพท์ ในภาษาอังกฤษคำว่า “Security” เป็นคำที่กินความหมายกว้างและครอบคลุม แต่ในบริบทของภาษาไทยและในการบริหารจัดการจริง เราจำเป็นต้องแยกแยะคำศัพท์สองคำที่มีความหมายเกี่ยวเนื่องแต่แตกต่างกัน ซึ่งผู้จัดการความมั่นคงปลอดภัย (Security Manager) ทุกคนต้องบริหารให้เกิดความสมดุล:

1. Safety (ความปลอดภัย):

คำนี้หมายถึง สภาวะที่ปราศจากอันตรายที่เกิดจาก “อุบัติเหตุ” (Accidental Incidents), ความผิดพลาดโดยไม่เจตนา (Unintentional Error), หรือภัยธรรมชาติ (Natural Disasters) (Fay, 2010) โดยงานในด้านนี้มักเกี่ยวข้องกับ:

(1) **อาชีวอนามัย (Occupational Health & Safety):** การป้องกันพนักงานจากการบาดเจ็บจากการทำงาน เช่น การพลัดตกจากที่สูง การถูกเครื่องจักรหนีบ

(2) **ความปลอดภัยทางอัคคีภัย (Fire Safety):** การป้องกันไฟไหม้ การบริหารจัดการเส้นทางหนีไฟ

(3) **ความปลอดภัยในโรงงานอุตสาหกรรม (Industrial Safety):** การควบคุมสารเคมีรั่วไหล

2. Security (ความมั่นคงปลอดภัย):

คำนี้มีความหมายที่เจาะจงถึงการปกป้องสินทรัพย์จากอันตรายที่เกิดจาก “เจตนาประสงค์ร้าย” (Intentional/Malicious Acts) ของมนุษย์ ไม่ว่าจะเป็นบุคคลภายนอกหรือภายในองค์กร (Fay, 2010) ทั้งนี้ งานด้านนี้ครอบคลุม:

(1) **การป้องกันอาชญากรรม (Crime Prevention):** การป้องกันการขโมย การปล้นทรัพย์ การบุกรุก

(2) **การต่อต้านการก่อการร้าย (Counter-Terrorism):** การป้องกันการวินาศกรรม การวางระเบิด

(3) **การรักษาความมั่นคงปลอดภัยข้อมูล (Information Security):** การป้องกันแฮกเกอร์ การจารกรรมข้อมูล

ตัวอย่างที่ชัดเจนในการแยกแยะสองคำนี้คือ ในนิคมอุตสาหกรรมใน **เขตพัฒนาพิเศษภาคตะวันออก (EEC)** ผู้จัดการความมั่นคงปลอดภัยต้องดูแลทั้ง Safety โดยการตรวจสอบว่าพนักงานสวมหมวกนิรภัยและรองเท้าเซฟตี้เพื่อป้องกันของตกใส่ และต้องดูแล

Security โดยการตรวจสอบระบบ Access Control เพื่อให้แน่ใจว่าไม่มีใครขโมยชิ้นส่วนอิเล็กทรอนิกส์ราคาแพงหรือจารกรรมความลับทางการค้าออกจากสายการผลิต (U.S. Department of State, 2024)

2.2 ความมั่นคงปลอดภัยเชิงวัตถุวิสัยและจิตวิสัย (Objective vs. Subjective Security)

นักวิชาการด้านความมั่นคงปลอดภัยสมัยใหม่ยังแบ่งมิติของความมั่นคงปลอดภัยออกเป็นอีกสองด้านที่ต้องพิจารณาควบคู่กัน:

1. ความมั่นคงปลอดภัยเชิงวัตถุวิสัย (Objective Security):

คือสถานะความมั่นคงปลอดภัยที่สามารถวัดผลและจับต้องได้จริง (Measurable and Tangible) เป็นเรื่องของข้อเท็จจริงทางกายภาพและเทคนิค เช่น:

(1) ความสูงและความแข็งแรงของรั้วรอบโรงงาน

(2) จำนวนเจ้าหน้าที่รักษาความปลอดภัยต่อผลัด

(3) ความละเอียดของกล้องวงจรปิด (เช่น 4K) และระยะเวลาการบันทึกภาพ

(4) มาตรฐานการเข้ารหัสข้อมูล (Encryption Standard) ในระบบธนาคาร

ในทางทฤษฎี หมายความว่า ประตูบานหนึ่งจะถูกระบุว่า “ล็อก” หรือ “ไม่ล็อก” อย่างชัดเจนในมิตินี้ (Vellani, 2020)

2. ความมั่นคงปลอดภัยเชิงจิตวิสัย (Subjective Security):

คือ “ความรู้สึก” (Perception) หรือสภาวะทางจิตวิทยาของผู้มีส่วนได้ส่วนเสีย (Stakeholders) ว่าตนเองมีความปลอดภัยหรือไม่ ซึ่งอาจไม่สอดคล้องกับความเป็นจริงเสมอไป:

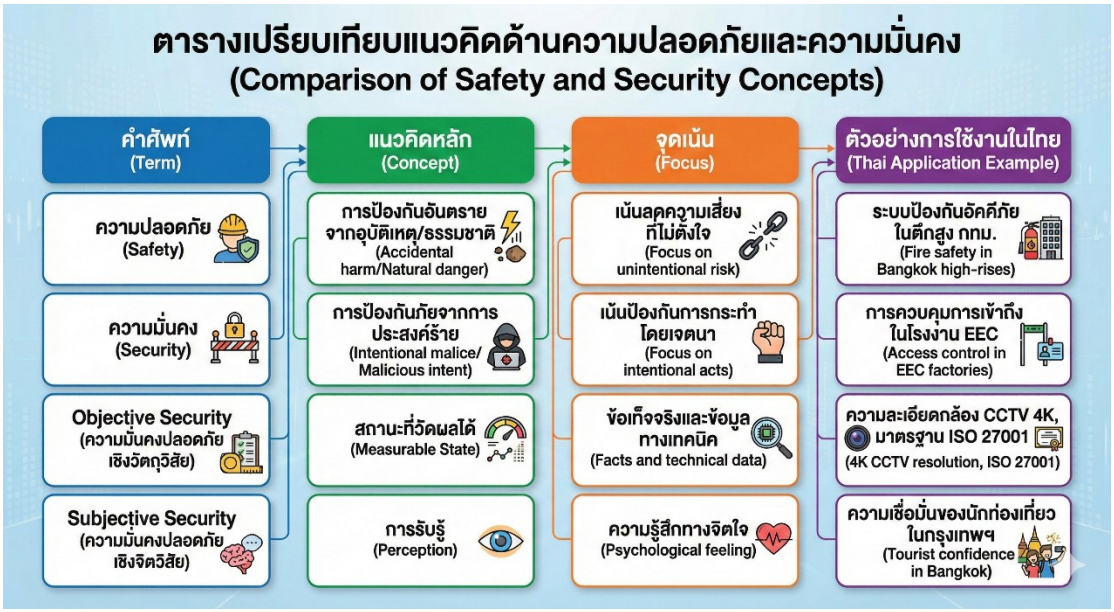
(1) พนักงานกะดึกรู้สึกอุ่นใจที่จะเดินไปลานจอดรถที่มีไฟส่องสว่าง แม้ว่าจริง ๆ แล้วอาจจะไม่มีรปภ. เฝ้าอยู่เลย

(2) นักท่องเที่ยวรู้สึกมั่นใจที่จะเดินเที่ยวในย่านเมืองเก่าภูเก็ตเพราะเห็นตำรวจท่องเที่ยวปั่นจักรยานตรวจตรา

(3) ลูกค้าธนาคารรู้สึกกลัวที่จะใช้แอปพลิเคชันทางการเงินเพราะข่าวแก๊งคอลเซ็นเตอร์ แม้ว่าแอปพลิเคชั่นนั้นจะมีระบบความปลอดภัยระดับสูงก็ตาม

กับดักของ “ละครรักษาความมั่นคงปลอดภัย” (The Danger of Security Theater): แนวคิดที่สำคัญที่สุดที่นักศึกษาต้องตระหนักและระมัดระวังคือ “Security Theater” หรือ “ปาหี่ความมั่นคงปลอดภัย” คือการใช้มาตรการที่เน้นสร้างความรู้สึกปลอดภัย (เพิ่ม Subjective Security) แต่แทบไม่มีประสิทธิผลในการป้องกันภัยจริง (ไม่มี Objective Security) (Vellani, 2020)

ตัวอย่างที่พบบ่อยในสังคมไทย คือ การที่เจ้าหน้าที่รักษาความปลอดภัยหน้าหมู่บ้านจัดสรรหรือคอนโดมิเนียมยืนทำความเคารพตะเบ๊ะรถทุกคันที่ผ่านเข้าออกอย่างแข็งขัน แต่กลับไม่เคยตรวจสอบท้ายรถ หรือไม่เคยขอบัตรประชาชนผู้มาติดต่ออย่างเคร่งครัด การกระทำเช่นนี้สร้างบรรยากาศที่เป็นมิตรและดูเหมือนมีการดูแล (Feeling Safe) แต่หากมีผู้ร้ายซ่อนตัวอยู่ในท้ายรถ หรือผู้ก่อการร้ายขับรถบรรทุกระเบิดเข้ามา มาตรการ “ตะเบ๊ะ” นี้ก็ไร้ค่าโดยสิ้นเชิงในทางปฏิบัติ หน้าที่ของผู้จัดการความมั่นคงปลอดภัยมืออาชีพคือการสร้างสมดุล โดยต้องขจัด “ละคร” ที่ไร้ประโยชน์ทิ้งไป และแทนที่ด้วยมาตรการที่สร้างความมั่นคงปลอดภัยจริงพร้อม ๆ กับสร้างความอุ่นใจให้กับประชาชน ลูกค้า หรือผู้รับบริการ



ภาพที่ 1.2

การเปรียบเทียบแนวคิดด้านความปลอดภัยและความมั่นคง

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

2.3 นิยามของการจัดการความมั่นคงปลอดภัย (Defining Security Management)

ดังนั้น การจัดการความมั่นคงปลอดภัย (Security Management) จึงไม่ใช่เพียงการจ้างบริษัท รปภ. มายืนเฝ้าจุด หรือการซื้อกล้องวงจรปิดมาติดตั้ง แต่มันคือ “ศาสตร์และศิลป์ในการบริหารจัดการความเสี่ยงเชิงระบบ” (Systematic Risk Management Discipline) เพื่อปกป้องสินทรัพย์ขององค์กร โดยมีการบูรณาการองค์ประกอบสำคัญ 4 ประการเข้าด้วยกัน (4 Ps of Security Management):

1. **Policies (นโยบาย):** กฎกติกาที่ชัดเจน
2. **Procedures (กระบวนการปฏิบัติ):** ขั้นตอนการทำงานที่รัดกุม

3. **People (บุคลากร):** คนที่มีความรู้ ทักษะ และทัศนคติที่ถูกต้อง

4. **Technology (เทคโนโลยี):** เครื่องมือที่ทันสมัยและเหมาะสม (Fay, 2010)

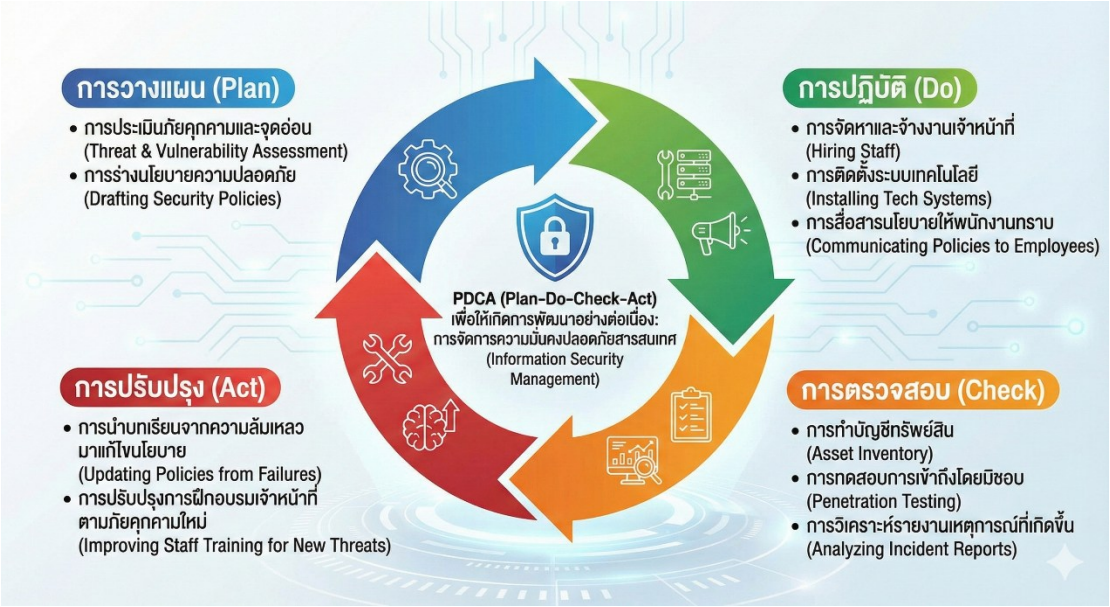
กระบวนการจัดการความมั่นคงปลอดภัยมักดำเนินตามวัฏจักรคุณภาพ **PDCA (Plan-Do-Check-Act):**

Plan (วางแผน): การระบุสินทรัพย์ (Asset Identification) และการประเมินความเสี่ยง (Risk Assessment) ว่าภัยคุกคามคืออะไร โอกาสเกิดมากน้อยเพียงใด

Do (ปฏิบัติ): การออกแบบและนำมาตรการป้องกันไปใช้จริง (Implementation) เช่น การติดตั้งระบบสแกนใบหน้า การฝึกอบรมพนักงาน

Check (ตรวจสอบ): การตรวจสอบสถานะระบบ (Audit) การทดสอบเจาะระบบ (Penetration Testing) หรือการซ้อมแผนเผชิญเหตุ (Drill) เพื่อดูว่ามาตรการที่วางไว้ใช้งานได้จริงหรือไม่

Act (ปรับปรุง): การนำผลการตรวจสอบมาวิเคราะห์และปรับปรุงแก้ไข (Continuous Improvement) เมื่อพบช่องโหว่ หรือเมื่อสถานการณ์ภัยคุกคามเปลี่ยนแปลงไป (Vellani, 2020)



ภาพที่ 1.3

วงจรการบริหารจัดการความมั่นคงปลอดภัยแบบ Plan–Do–Check–Act (PDCA)

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

3. ขอบเขตและวัตถุประสงค์ของการจัดการความมั่นคงปลอดภัย (Scope and Objectives)

ขอบเขตของงานความมั่นคงปลอดภัยในองค์กรสมัยใหม่กว้างขวางกว่าในอดีตมาก เราไม่สามารถมองความมั่นคงปลอดภัยเป็นเพียงเรื่องของ “ประตูและแม่กุญแจ” (Gates and Locks) ได้อีกต่อไป เพื่อให้เห็นภาพรวมที่ชัดเจน เราสามารถพิจารณาผ่านโมเดล “ระบบนิเวศความมั่นคงปลอดภัย” (The Security Ecosystem) ซึ่งประกอบด้วยสินทรัพย์ 4 ประเภทหลักที่ต้องได้รับการปกป้องอย่างบูรณาการ (Fay, 2010)

3.1 ระบบนิเวศความมั่นคงปลอดภัย (The Security Ecosystem)

1. คน (People - Human Assets)

มนุษย์คือสินทรัพย์ที่มีค่าที่สุดและเปราะบางที่สุดของทุกองค์กร ขอบเขตงานความมั่นคงปลอดภัยต้องครอบคลุมความมั่นคงปลอดภัยของ ผู้บริหาร (Executives), พนักงาน (Employees), ลูกค้า (Customers), ผู้รับเหมา (Contractors), และผู้มาติดต่อ (Visitors)

บริบทไทย: การปกป้อง “คน” กลายเป็นวาระเร่งด่วนระดับชาติหลังเกิดเหตุการณ์โศกนาฏกรรมที่ศูนย์พัฒนาเด็กเล็ก จ.หนองบัวลำภู (ตุลาคม 2022) เหตุการณ์นี้ได้พลิกโฉมหน้าการจัดการความมั่นคงปลอดภัยในโรงเรียนและสถานที่ราชการ กระตุ้นให้เกิดการตื่นตัวเรื่องมาตรการรับมือ **“ผู้ก่อเหตุรุนแรง” (Active Shooter/Attacker Protocol)** อย่างจริงจัง รวมถึงการเน้นย้ำความสำคัญของ **การตรวจสอบประวัติก่อนเข้าทำงาน (Pre-employment Screening)** ทั้งประวัติอาชญากรรมและสุขภาพจิต เพื่อคัดกรองบุคคลที่มีความเสี่ยงไม่ให้เข้าสู่องค์กร ลดโอกาสเกิดภัยคุกคามจากภายใน (Insider Threat) (Vellani, 2020)

2. สินทรัพย์ทางกายภาพ (Physical Assets)

ครอบคลุมถึง อาคารสถานที่, เครื่องจักร, วัตถุดิบ, สินค้าคงคลัง, เงินสด, และยานพาหนะ

กรณีศึกษา: ธุรกิจที่มีความเสี่ยงสูงอย่าง **ร้านทอง (Gold Shops)** ซึ่งมีกระจายอยู่ทั่วทุกชุมชนในประเทศไทย ถือเป็นเป้าหมายคลาสสิกของอาชญากรรมทรัพย์สิน การจัดการความมั่นคงปลอดภัยในธุรกิจนี้ต้องใช้ทฤษฎี **“การเลือกอย่างมีเหตุผล” (Rational Choice Theory)** มาประยุกต์ใช้ คือการทำให้โจร “คำนวณแล้วไม่คุ้ม” โดยการใช้มาตรการที่เข้มข้น เช่น การติดตั้งลูกกรงสแตนเลส (Hardened Architecture), การจ้างเจ้าหน้าที่ตำรวจนอกเวลาราชการมาเฝ้าระวัง (Police Presence), และนวัตกรรมใหม่อย่าง **“Fog Cannon”** ที่จะพ่นควันทึบออกมาทันทีที่กดปุ่มแจ้งเหตุ เพื่อตัดวิสัยทัศน์ของคนร้าย ทำให้ไม่สามารถกวาดทรัพย์สินหรือหาทางออกได้ (Vellani, 2020)

3. ข้อมูลและสารสนเทศ (Information and Data)

ในระบบเศรษฐกิจดิจิทัล ข้อมูลลูกค้า, ความลับทางการค้า, สูตรการผลิต, และฐานข้อมูลทางการเงิน คือสินทรัพย์ระดับวิกฤต (Critical Assets) แนวคิดหัวใจสำคัญในการบริหารจัดการส่วนนี้คือ CIA Triad:

Confidentiality (ความลับ): ข้อมูลต้องเข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น (เช่น เงินเดือนพนักงาน, เวชระเบียนคนไข้)

Integrity (ความถูกต้องครบถ้วน): ข้อมูลต้องไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต (เช่น ยอดเงินในบัญชีธนาคาร)

Availability (ความพร้อมใช้): ระบบต้องสามารถใช้งานได้เมื่อต้องการ ไม่ล่ม ไม่ถูกปิดกั้น (เช่น ระบบจ่ายไฟของโรงพยาบาล, แอปพลิเคชันธนาคาร)

บทลงโทษที่รุนแรง: การบังคับใช้ **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล** (PDPA) ของไทยอย่างเต็มรูปแบบ ทำให้ความล้มเหลวในด้านนี้มีราคาแพงมาก ตัวอย่างเช่น กรณีบริษัท JIB Computer Group ที่ถูกคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) สั่งปรับเป็นเงิน 7 ล้านบาท ในปี พ.ศ. 2567 เนื่องจากมาตรการรักษาความมั่นคงปลอดภัยข้อมูลหละหลวมจนถูกแฮกเกอร์เจาะระบบ (Boonnark, 2025) กรณีนี้เป็นบรรทัดฐานใหม่ที่เตือนให้ผู้บริหารตระหนักว่า Cyber Security ไม่ใช่ทางเลือก แต่เป็นความอยู่รอดทางกฎหมายและการเงิน

ภาพที่ 1.4

CIA Triad: ความมั่นคงปลอดภัยสารสนเทศ

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

4. ชื่อเสียงและความเชื่อมั่น (Reputation and Trust)

ชื่อเสียงเป็นสินทรัพย์ที่จับต้องไม่ได้ (Intangible Asset) แต่เปราะบางที่สุด การสร้างชื่อเสียงใช้เวลาหลายสิบปี แต่การทำลายอาจใช้เวลาเพียงไม่กี่นาทีจากเหตุการณ์ความไม่ปลอดภัยเพียงครั้งเดียว

ผลกระทบ: กรณีเหตุการณ์กราดยิงที่สยามพารากอน ส่งผลกระทบโดยตรงต่อความเชื่อมั่นของนักท่องเที่ยวจีน หรือกรณีการรั่วไหลของข้อมูล 9Near ที่ทำให้ประชาชนตั้งคำถามต่อความสามารถของหน่วยงานรัฐในการดูแลข้อมูลส่วนตัว หน้าที่ของผู้จัดการความมั่นคงปลอดภัยจึงรวมถึงการสนับสนุน **"การบริหารวิกฤต" (Crisis Management)** การเตรียมข้อมูลที่ถูกต้องสำหรับการสื่อสาร (Crisis Communication) เพื่อจำกัดความเสียหายและกอบกู้ความเชื่อมั่นกลับคืนมา (Newport, 2023)

3.2 วัตถุประสงค์หลัก (Core Objectives)

เป้าหมายสูงสุดของการจัดการความมั่นคงปลอดภัยไม่ใช่การทำให้ความเสี่ยงเป็นศูนย์ (Zero Risk) เพราะในโลกความเป็นจริงไม่มีระบบใดที่สมบูรณ์แบบและงบประมาณมีจำกัด แต่เป้าหมายคือการบริหารความเสี่ยงให้อยู่ใน **"ระดับที่ยอมรับได้" (Acceptable Risk Level)** โดยมีวัตถุประสงค์ย่อยดังนี้:

1. ป้องกันความสูญเสีย (Loss Prevention): ลดโอกาสการเกิดการขโมย การยักยอก การสูญหายของทรัพย์สิน และความสูญเสียจากอุบัติเหตุ

2. รับรองความต่อเนื่องทางธุรกิจ (Business Continuity Management - BCM): สร้างหลักประกันว่าองค์กรจะสามารถดำเนินงานต่อได้หรือฟื้นตัวได้เร็วที่สุดแม้เกิดวิกฤตการณ์รุนแรง เช่น บทเรียนจากมหาอุทกภัยปี 2011 ที่ทำให้นิคมอุตสาหกรรมจมน้ำ โรงงานหลายแห่งต้องปิดตัวเพราะขาดแผน BCM ที่ดี

3. การปฏิบัติตามกฎหมายและระเบียบข้อบังคับ (Compliance): เพื่อป้องกันองค์กรจากการถูกปรับ ถูกฟ้องร้อง หรือถูกระงับใบอนุญาต (เช่น กฎหมายแรงงาน, กฎหมายสิ่งแวดล้อม, PDPA)

4. สร้างความเชื่อมั่น (Confidence Building): การทำให้ผู้ถือหุ้น ลูกค้า พนักงาน และสังคม รู้สึกมั่นใจและไว้วางใจในการดำเนินงานขององค์กร (Fay, 2010)

4. วิวัฒนาการของความมั่นคงปลอดภัย (Evolution of the Security)

4.1 ประวัติศาสตร์วิชาชีพมั่นคงปลอดภัยทั่วไป (General Historical of the Security Profession)

1. ยุคเริ่มต้น (Early Period)

วิชาชีพความมั่นคงในสมัยโบราณและยุคกลางเน้นหน้าที่การป้องกันทางกายภาพและการเฝ้าระวังสถานที่สำคัญ ตั้งแต่ยุคอียิปต์โบราณ ผู้รับผิดชอบความมั่นคงปลอดภัยได้ปกป้องขบวนคาราวานค้าขาย คฤหาสน์ผู้มั่งคั่ง และข้าราชการชั้นสูง ในขณะที่ปราสาทในยุคกลางใช้ระบบหอสังเกตการณ์ ยามรักษาการณ์ และแนวรั้วเพื่อป้องกันการบุกรุก แนวคิดสถาปัตยกรรมเหล่านี้กลายมาเป็นรากฐานของระบบความมั่นคงสมัยใหม่ ในช่วง

เหล่านี้ บทบาทความมั่นคงถูกจำกัดอยู่ที่การเฝ้าระวังและการแสดงตัวป้องกัน มีความต้องการการฝึกอบรมอย่างเป็นทางการน้อยมาก มีอำนาจในการตัดสินใจจำกัด และทำงานในลักษณะรับมือเหตุการณ์ด้วยการตอบสนองหลังเหตุการณ์เกิดขึ้น ทำให้ความมั่นคงถูกมองว่าเป็นวิชาชีพที่มีสถานะต่ำและไม่เกี่ยวข้องกับยุทธศาสตร์ขององค์กร (Vellani, 2020)

2. การขยายตัวในยุคอุตสาหกรรมและ (Industrial Expansion Era)

การปฏิวัติอุตสาหกรรมในศตวรรษที่ 18 และ 19 นำมาซึ่งการเปลี่ยนแปลงโครงสร้างในวิชาชีพความมั่นคงปลอดภัย เนื่องจากการขยายตัวของโรงงาน คลังสินค้า และทางขนส่ง ความต้องการบริการความมั่นคงปลอดภัยที่เป็นระบบและเป็นมืออาชีพจึงเพิ่มขึ้นอย่างชัดเจน การสถาปนาอุตสาหกรรมความมั่นคงเอกชนสมัยใหม่ส่วนใหญ่ถูกสืบย้อยไปถึงอัลลัน พิงเคอร์ตัน ผู้ก่อตั้ง Pinkerton National Detective Agency ในชิคาโก ปี ค.ศ. 1850 โดยบริษัทดังกล่าวให้บริการสืบสวน การคุ้มครองทางขนส่งทางรถไฟ และความมั่นคงสำหรับสถานที่อุตสาหกรรม สร้างโมเดลธุรกิจที่ยังคงแพร่หลายถึงปัจจุบัน ความพยายามในการทำให้วิชาชีพเป็นทางการเกิดขึ้นเมื่อปี ค.ศ. 1915 เมื่อรัฐแคลิฟอร์เนียออกใบอนุญาตบังคับสำหรับนักสืบเอกชนและบุคลากรด้านความมั่นคงปลอดภัย ซึ่งเป็นการยอมรับถึงความจำเป็นในการทำให้ภาคสนามนี้มีมาตรฐานและภาระรับผิดชอบ (Pinkerton, 2024)

ความต้องการบริการความมั่นคงเพิ่มขึ้นอย่างมีนัยสำคัญในช่วงสงครามโลกครั้งที่สอง (ค.ศ. 1940-1945) เมื่อรัฐบาลและบรรษัทต่างต้องการปกป้องฐานทัพ ผู้รับจ้างด้านการป้องกันประเทศ และโครงสร้างพื้นฐานสำคัญจากการก่อวินาศกรรมและการจารกรรม อย่างไรก็ตาม ในช่วงเศรษฐกิจตกต่ำครั้งใหญ่ (ค.ศ. 1929-1939) การจ้างงานด้านความมั่นคงได้ลดลงตามสภาพเศรษฐกิจที่หดตัว หลังจากสงคราม ทหารผ่านศึกจำนวนมากที่มีประสบการณ์ด้านตำรวจทหารและการยุทธวิธีทหาร หันเข้าสู่อาชีพความมั่นคงปลอดภัยเอกชน ซึ่งนำมาซึ่งองค์ความรู้ระดับสูงและมีส่วนช่วยให้ภาคสนามนี้เป็นมืออาชีพและมีการบริหารจัดการที่ดีขึ้น (Vellani, 2020)

3. ยุคการเป็นวิชาชีพและการมุ่งเน้นการจัดการ (Professionalization and Management Orientation Era)

ภายในทศวรรษ 1970 และ 1980 วิชาชีพความมั่นคงได้วิวัฒนาการจากหน้าที่ปฏิบัติการไปสู่สาขาวิชาการจัดการที่ได้รับการยอมรับอย่างกว้างขวาง องค์กรต่าง ๆ เริ่มตระหนักว่าความเสี่ยงทั้งด้านการขโมย การฉ้อโกง การก่อวินาศกรรม ความรุนแรงในที่ทำงาน และอุบัติเหตุ นั้นเป็นปัญหาเชิงยุทธศาสตร์ที่ต้องการการวางแผนอย่างเป็นระบบ การพัฒนานโยบาย และความเข้าใจจากระดับบริหารสูงสุด ผู้จัดการด้านความมั่นคงจึงได้ขยายบทบาทของตนเข้าสู่การประเมินความเสี่ยง การตรวจสอบ การริเริ่มด้านการปฏิบัติตามกฎระเบียบ และการวางแผนยุทธศาสตร์ ซึ่งบทบาทใหม่เหล่านี้ต้องการการคิด

วิเคราะห์อย่างลึกซึ้ง ทักษะการสื่อสารอย่างมีประสิทธิผล และความเข้าใจในธุรกิจ มากกว่าเพียงการปรากฏตัวเพื่อการคุ้มครองทางกายภาพ การมุ่งเน้นนี้ได้รับการเสริมแรงจากสมาคมวิชาชีพ เช่น ASIS International (ก่อตั้งปี ค.ศ. 1955) ซึ่งพัฒนาโปรแกรมการรับรองมาตรฐาน เช่น Certified Protection Professional (CPP) การรับรองเหล่านี้กำหนดข้อกำหนดด้านความรู้ รหัสจริยธรรม และมาตรฐานการศึกษาต่อเนื่อง โดยครอบคลุมโดเมนหลากหลาย อาทิ หลักการความมั่นคง การจัดการความเสี่ยง การสืบสวน ความมั่นคงด้านบุคลากร ความมั่นคงทางกายภาพ ความมั่นคงข้อมูล และการจัดการวิกฤต (ASIS International, 2024)

ในช่วงกลางทศวรรษ 1970 รัฐทั้งหมดในสหรัฐอเมริกาได้บังคับใช้ข้อกำหนดการออกใบอนุญาตสำหรับบริษัทและบุคลากรความมั่นคงเอกชน พร้อมกับข้อเรียกร้องด้านการตรวจประวัติและการตรวจสารเสพติด การเปลี่ยนแปลงเหล่านี้สะท้อนการเปลี่ยนแปลงในการรับรู้ของอุตสาหกรรมต่อบทบาทด้านความมั่นคง ผู้ปฏิบัติงานและผู้จัดการด้านความมั่นคงที่มีวิสัยทัศน์กว้างขวางเริ่มมองความมั่นคงว่าเป็นปัจจัยสำคัญในการสร้างความสำเร็จขององค์กร แทนที่จะถูกมองว่าเป็นเพียงศูนย์ต้นทุน ผลทำให้แผนกความมั่นคงได้รับการบูรณาการเข้าเป็นส่วนหนึ่งของวัฒนธรรมองค์กรของหลายบริษัท โดยผู้จัดการความมั่นคงได้รับมอบหมายให้ร่วมมือกับผู้นำของแผนกอื่น ๆ ในการจัดการความเสี่ยงในระดับองค์กรที่ครอบคลุม (Vellani, 2020)

4. ยุคหลังเหตุการณ์ 9/11 (Post-9/11 Era)

เหตุการณ์โจมตีของผู้ก่อการร้ายเมื่อ 11 กันยายน ค.ศ. 2001 ถือเป็นจุดเปลี่ยนครั้งสำคัญในการบริหารจัดการความมั่นคง การโจมตีดังกล่าวเปิดเผยว่าภัยคุกคามสาหัสที่ก่อให้เกิดความเสียหายครั้งใหญ่สามารถมาจากแหล่งที่ไม่ใช่แบบดั้งเดิม และสามารถใช้ประโยชน์จากช่องโหว่ของระบบในลักษณะที่มาตรการความมั่นคงแบบเดิมไม่สามารถคาดการณ์ได้ ผลทำให้ขอบเขตของความมั่นคงได้ขยายตัวไปไกลเกินกว่าการป้องกันอาชญากรรมเพื่อครอบคลุมการต่อต้านการก่อการร้าย การปกป้องโครงสร้างพื้นฐานสำคัญ ความมั่นคงไซเบอร์ การเตรียมพร้อมสำหรับสถานการณ์ฉุกเฉิน และการสร้างความเป็นยืดหยุ่นขององค์กร ในสหรัฐอเมริกา รัฐบาลกลางได้จัดตั้งกรมความมั่นคงแห่งมาตุภูมิ (DHS) และสำนักงานบริหารความปลอดภัยการขนส่ง (TSA) เพื่อรวมศูนย์และส่งเสริมความพยายามด้านความมั่นคงในระดับชาติ นอกจากนี้ หน่วยงานบังคับใช้กฎหมายในทุกระดับได้เพิ่มขีดความสามารถในการต่อต้านการก่อการร้าย การแบ่งปันข้อมูลกรรมการ และการประสานงานกับผู้ให้บริการความมั่นคงเอกชน ในขณะที่ความมั่นคงการบินได้รับการปฏิรูปแบบมีเป้าหมาย โดยเปลี่ยนจากระบบการจ้างเอกชนไปสู่การตรวจสอบและการบังคับใช้ที่จัดการโดยหน่วยงานของรัฐบาลกลาง (Pinkerton, 2024)

ยุคหลัง 9/11 ยังส่งเสริมการพัฒนาการทำงานร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnerships - P3s) ด้านความมั่นคง เนื่องจากภาคเอกชนควบคุม

โครงสร้างพื้นฐานสำคัญส่วนใหญ่ เช่น เครือข่ายการขนส่ง ระบบโครงข่ายไฟฟ้า ระบบการเงิน และโทรคมนาคม รัฐบาลจึงเริ่มสร้างความร่วมมือกับบริษัทความมั่นคงเอกชนเพื่อแลกเปลี่ยนข้อมูลกรรมการ ดำเนินการประเมินภัยคุกคาม และประสานการตอบสนองต่อเหตุการณ์วิกฤต ตัวอย่างสำคัญของโมเดลร่วมมือนี้คือ Joint Cyber Defense Collaborative (JCDC) ซึ่งจัดตั้งโดยสำนักงานความมั่นคงไซเบอร์และโครงสร้างพื้นฐาน (CISA) โดยรวบรวมหน่วยงานรัฐและบริษัทเอกชนเข้าด้วยกันเพื่อร่วมมือจัดการกับภัยคุกคามทางไซเบอร์อย่างเป็นระบบ (ASIS International, 2024)

4.2 ประวัติศาสตร์วิชาชีพมั่นคงปลอดภัยของไทย (Evolution of Security Profession in Thailand)

เพื่อให้เข้าใจสถานะของวิชาชีพในปัจจุบัน เราต้องย้อนมองเส้นทางประวัติศาสตร์ของงานรักษาความมั่นคงปลอดภัยในประเทศไทย ซึ่งสะท้อนการเปลี่ยนแปลงทางเศรษฐกิจและสังคมของประเทศอย่างชัดเจน

1. ยุค “เฝ้ายาม” แบบดั้งเดิม (Traditional Era: ยุคก่อน พ.ศ. 2520)

ในอดีต งานรักษาความมั่นคงปลอดภัยในประเทศไทยเป็นเรื่องของ “ความไว้วางใจส่วนบุคคล” (Personal Trust) มากกว่าระบบอาชีพ บ้านเศรษฐี คหบดี หรือกิจการร้านค้ามักจ้างคนรู้จัก ญาติห่าง ๆ จากต่างจังหวัด หรือแรงงานสูงอายุ มาทำหน้าที่ “เฝ้าบ้าน” หรือ “เฝ้ายาม”

ลักษณะงาน: ไม่มีมาตรฐานการฝึกอบรมหรือมาตรฐานคุณวุฒิใด ๆ ไม่มีเครื่องแบบที่ชัดเจน (อาจใส่ชุดธรรมดาหรือชุดสีกากีคล้ายราชการ) และไม่มีกฎหมายควบคุมวิชาชีพโดยเฉพาะ

เครื่องมือ: มีเพียงไฟฉาย นกหวีด และกระบองไม้ หน้าที่หลักคือการนั่งเฝ้าไม่ให้คลาดสายตาและส่งเสียงดังหากมีผู้บุกรุก (Chambers & Waitoolkiat, 2021)

2. ยุคอุตสาหกรรมและการพาณิชย์ (Industrialization Era: พ.ศ. 2520 - 2550)

จุดเปลี่ยนเริ่มขึ้นเมื่อประเทศไทยเปิดรับการลงทุนจากต่างประเทศ (FDI) และเริ่มมีการพัฒนาพื้นที่ชายฝั่งทะเลตะวันออก (Eastern Seaboard) ให้เป็นนิคมอุตสาหกรรม บริษัทข้ามชาติ (MNCs) ที่เข้ามาลงทุนต้องการมาตรฐานความมั่นคงปลอดภัยในระดับสากล เพื่อปกป้องโรงงานและทรัพย์สินมูลค่าสูง

การเปลี่ยนแปลง: เกิดการเข้ามาของบริษัทรักษาความปลอดภัยระดับโลก (Global Security Firms) เช่น G4S, Securitas ซึ่งนำระบบการบริหารจัดการแบบตะวันตกเข้ามาใช้ มีการฝึกอบรม มีระเบียบปฏิบัติประจำ (SOPs) มีการใช้เครื่องแบบที่ดูเป็นทางการ มีวิทยุสื่อสาร และมีการนำเข้าความรู้ด้าน “การป้องกันความสูญเสีย” (Loss Prevention)

ปัญหา: อย่างไรก็ตาม ตลาดในประเทศยังคงมีบริษัท รปภ. ขนาดเล็ก (Local/Mom-and-Pop shops) จำนวนมากที่แข่งขันด้วยราคาต่ำ ซึ่งมักจ้างแรงงานราคาถูก บริษัทหลายแห่งจ้างแรงงานต่างด้าว ขาดการตรวจสอบประวัติอาชญากรรม หรือจ้างบุคคลที่ไม่มีใบรับรองการศึกษาเพียงเพื่อให้มีคนยืนประจำจุด นำไปสู่ปัญหาคุณภาพบริการ เช่น รปภ. หลับยาม เมาสุราขณะปฏิบัติหน้าที่ หรือร้ายแรงที่สุดคือ รปภ. กลายเป็นผู้ก่อเหตุขโมยทรัพย์สินเสียเอง (Chambers & Waitoolkiat, 2021)

3. ยุคการยกระดับมาตรฐาน: พ.ร.บ. ธุรกิจรักษาความปลอดภัย พ.ศ. 2558 (The 2015 Regulatory Turning Point)

เพื่อแก้ไขปัญหาคุณภาพและมาตรฐานความมั่นคงปลอดภัย รัฐบาลไทยได้ประกาศใช้ **พระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558 (Security Guard Business Act B.E. 2558)** ซึ่งถือเป็นการ "จัดระเบียบ" (Regulatory Overhaul) ครั้งใหญ่ที่สุดของวงการธุรกิจความปลอดภัย โดยสาระสำคัญ ได้แก่:

(1) **บริษัท:** ต้องจดทะเบียนและได้รับใบอนุญาตประกอบธุรกิจจากนายทะเบียนกลาง (สำนักงานตำรวจแห่งชาติ)

(2) **พนักงาน:** ผู้ที่จะเป็น "พนักงานรักษาความปลอดภัยรับอนุญาต" (ธภ.) ต้องมีสัญชาติไทย จบการศึกษาภาคบังคับ (ม.3) และที่สำคัญที่สุดคือ **ต้องผ่านการตรวจสอบประวัติอาชญากรรม** โดยต้องไม่มีประวัติคดีร้ายแรงเกี่ยวกับร่างกาย ชีวิต ทรัพย์สิน หรือคดีทางเพศ

(3) **การฝึกอบรม:** ต้องผ่านการฝึกอบรมหลักสูตรมาตรฐาน 40 ชั่วโมง จากศูนย์ฝึกที่ได้รับการรับรอง ครอบคลุมวิชากฎหมายเบื้องต้น การดับเพลิง การปฐมพยาบาล การต่อสู้ป้องกันตัว และจริยธรรม

ผลกระทบของกฎหมายนี้คือการยกระดับมาตรฐานและได้รับการยอมรับในฐานะ "วิชาชีพ" มากขึ้นอย่างชัดเจน แต่ก็สร้างผลกระทบข้างเคียง (Side Effect) คือภาวะ **"ขาดแคลนแรงงาน" (Labor Shortage)** เนื่องจากเงื่อนไขด้านวุฒิการศึกษา (ม.3) ทำให้แรงงานรุ่นเก่าที่มีประสบการณ์แต่ขาดวุฒิต้องออกจากระบบ ประกอบกับเงื่อนไขการตรวจสอบประวัติที่เข้มงวด ทำให้การหาคนมาทำงานยากขึ้น (Ministerial Regulation Authorizing Security Guard Business Operation B.E. 2560 (2017))

4. ยุคปัจจุบันและอนาคต (พ.ศ. 2560 - ปัจจุบัน): วิกฤตแรงงานและการเปลี่ยนผ่านสู่เทคโนโลยี (The Crisis & Tech Transition)

ในปัจจุบัน อุตสาหกรรมความมั่นคงปลอดภัยไทยกำลังเผชิญกับพายุลูกใหม่ นั่นคือ "การปรับขึ้นค่าแรงขั้นต่ำ" และ "สังคมผู้สูงอายุ"

(1) **ผลกระทบค่าแรง 400 บาท:** การปรับขึ้นค่าแรงขั้นต่ำเป็น 400 บาทในหลายพื้นที่เศรษฐกิจ (เช่น ชลบุรี, ภูเก็ต) และแนวโน้มที่จะปรับขึ้นทั่วประเทศ

ส่งผลกระทบโดยตรงต่อต้นทุนบริการรักษาความมั่นคงปลอดภัยซึ่งเป็นธุรกิจที่ใช้แรงงานเข้มข้น (Labor-Intensive) 20

(2) **Technology Substitution:** เมื่อ “คน” แพงขึ้นและหายากขึ้น (จากโครงสร้างประชากรสูงวัยและคนรุ่นใหม่นิยมงาน Gig Economy) แนวโน้มที่ชัดเจนที่สุดคือการ **“ใช้เทคโนโลยีทดแทนคน” (Manpower Substitution)** บริษัทรักษาความปลอดภัยชั้นนำ (เช่น G4S, Guardforce, SECOM) กำลังเปลี่ยนโมเดลธุรกิจจากการขาย “คน” (Man-guarding) มาเป็นการขาย “โซลูชัน” (Security Solutions) ที่ผสมผสานคนเข้ากับเทคโนโลยี เช่น:

- การใช้กล้อง AI CCTV ที่สามารถตรวจจับผู้บุกรุกได้อัตโนมัติ ลดจำนวนคนเดินตรวจ
- การใช้โดรน (Drones) บินลาดตระเวนในพื้นที่กว้าง
- การใช้ระบบควบคุมการเข้าออก (Access Control) อัตโนมัติและระบบจดจำใบหน้า (Facial Recognition)

ผู้จัดการความมั่นคงปลอดภัยในยุคนี้จึงต้องเป็น **“Hybrid Manager”** ที่ไม่เพียงแต่คุมคนได้ แต่ต้องมีความรู้เรื่องเทคโนโลยี (Tech Literacy) สามารถอ่าน Data จากระบบ AI และบริหารงบประมาณให้คุ้มค่าที่สุดท่ามกลางต้นทุนที่สูงขึ้น (Vellani, 2020)

ภาพที่ 1.5

สภาพแวดล้อมการจัดการความมั่นคงปลอดภัยสมัยใหม่

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

5. ความมั่นคงปลอดภัยสาธารณะ vs ความมั่นคงปลอดภัยเอกชน (Public vs. Private Security)

ความเข้าใจผิดที่พบบ่อยคือการคิดว่า รปภ. คือ “ตำรวจเอกชน” แท้จริงแล้ว สองบทบาทนี้มีความแตกต่างกันอย่างสิ้นเชิงในเชิงอำนาจและหน้าที่

5.1 ความมั่นคงปลอดภัยสาธารณะ (Public Security)

ดำเนินการโดยภาครัฐ (Government Agencies) เช่น สำนักงานตำรวจแห่งชาติ (Royal Thai Police - RTP), กรมสอบสวนคดีพิเศษ (DSI), ทหาร

พันธกิจ: ดูแลความสงบเรียบร้อยของสังคมโดยรวม (Public Order) และบังคับใช้กฎหมายอาญา

อำนาจ: มีอำนาจตามกฎหมายวิธีพิจารณาความอาญา (ป.วิอาญา) ในการ **สืบสวน (Investigate), สอบสวน (Interrogate), จับกุม (Arrest), ค้น (Search), ยึดทรัพย์ (Seize),** และ **พกพาอาวุธปืน** ได้ตามหน้าที่ราชการ

ความรับผิดรับชอบ: รับผิดชอบต่อสาธารณชนและกฎหมายมหาชน

5.2 ความมั่นคงปลอดภัยเอกชน (Private Security)

ดำเนินการโดยบริษัทเอกชนหรือหน่วยงานภายในองค์กร เพื่อปกป้องสินทรัพย์ของ “ลูกค้า” เฉพาะราย (Client-specific) ตามสัญญาจ้าง

พันธกิจ: ป้องกันความสูญเสีย (Loss Prevention) ให้กับผู้ว่าจ้าง

อำนาจจำกัด (Limited Authority): นี่คือจุดสำคัญที่สุด **รปภ. ในไทยไม่มีอำนาจตามกฎหมายมากไปกว่าพลเมืองดีทั่วไป**

การจับกุม: รปภ. **ไม่มีอำนาจจับกุม** ผู้ต้องสงสัย เว้นแต่เป็นกรณี **“ความผิดซึ่งหน้า” (Flagrant Offense)** ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 79 และ 80 ที่อนุญาตให้ “ราษฎร” จับกุมได้ เช่น เห็นคนกำลังวิ่งราวทรัพย์ต่อหน้าต่อตา รปภ. สามารถช่วยจับตัวไว้ได้ แต่ต้องส่งมอบให้ตำรวจทันที (Citizen's Arrest) แต่ไม่สามารถจับกุมตามหมายจับหรือไปสืบสวนจับกุมที่อื่นได้

การค้น: รปภ. **ไม่มีอำนาจค้นตัวหรือค้นกระเป๋า** โดยปราศจากความยินยอม การทำงานของ รปภ. อาศัยหลักการทางแพ่งเรื่อง **“เงื่อนไขการเข้าพื้นที่” (Condition of Entry)** เจ้าของสถานที่มีสิทธิ์กำหนดกติกาว่า “ผู้ที่จะเข้าพื้นที่นี้ ต้องยินยอมให้ตรวจค้นสัมภาระ หากท่านไม่ยินยอม เราขอสงวนสิทธิ์ปฏิเสธไม่ให้เข้าพื้นที่” นี่คืออำนาจในการ “ปฏิเสธการเข้า” (Deny Entry) ไม่ใช่อำนาจในการค้นโดยพลการ

อาวุธ: ตาม พ.ร.บ. อาวุธปืนฯ และ พ.ร.บ. ธุรกิจรักษาความปลอดภัย รปภ. ทั่วไป **ไม่ได้รับอนุญาตให้พกพาอาวุธปืน** ในขณะปฏิบัติหน้าที่ ยกเว้นเจ้าหน้าที่รักษาความ

ปลอดภัยประเภทพิเศษ เช่น รถขนเงิน (Cash-in-Transit: CIT) ที่ต้องมีใบอนุญาตพกพาเฉพาะและผ่านการฝึกอบรมขั้นสูง ((Security Guard Business Act B.E. 2558 (2015), 2015)

ภาพที่ 1.6

การเปรียบเทียบความแตกต่างระหว่างความมั่นคงปลอดภัยสาธารณะและเอกชนในประเทศไทย

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

5.3 การบูรณาการและความร่วมมือ (Collaboration & Synergy)

ในโลกยุคใหม่ ตำรวจไม่สามารถดูแลทุกซอกมุมของสังคมได้ทั่วถึง จึงเกิดโมเดลความร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnership - PPP) ที่ทรงพลัง ตัวอย่างความสำเร็จในไทย ได้แก่:

(1) Smart Safety Zone 4.0: โครงการของสำนักงานตำรวจแห่งชาติที่บูรณาการเทคโนโลยีเข้ากับการป้องกันอาชญากรรม โดยการเชื่อมโยงเครือข่ายกล้อง CCTV ของภาคเอกชน (เช่น โรงแรม, ร้านสะดวกซื้อ 7-11, หมู่บ้านจัดสรร) เข้ากับศูนย์บัญชาการของตำรวจ (Police Command Center) และใช้ AI ในการวิเคราะห์ภาพ ทำให้ตำรวจมี “ตา” เพิ่มขึ้นนับแสนดวงโดยไม่ต้องลงทุนติดตั้งเองทั้งหมด และสามารถระงับเหตุหรือจับกุมคนร้ายได้รวดเร็วขึ้น ดังที่เห็นความสำเร็จในพื้นที่นำร่องอย่างพัทยาหรือย่านธุรกิจในกรุงเทพมหานคร รายงานความสำเร็จในปี 2024 ระบุว่าโครงการนี้ช่วยลดดัชนีความหวาดกลัวภัยอาชญากรรม (Fear of Crime) ของประชาชนลงได้อย่างมีนัยสำคัญ (Hakparn et al., 2024)

(2) Cyber Vaccine: เมื่อภัยคุกคามย้ายไปอยู่บนโลกออนไลน์ ตำรวจเพียงลำพังไม่สามารถป้องกันประชาชนจากการถูกหลอกลวงได้ จึงเกิดความร่วมมือกับภาคเอกชน (ธนาคาร, ผู้ให้บริการมือถือ AIS/True, ไปรษณีย์ไทย) ในโครงการ "Cyber Vaccine" เพื่อฉีดวัคซีนทางปัญญา โดยภาคเอกชนช่วยกระจายสื่อความรู้ แจ้งเตือน SMS หลอกลวง และพัฒนาระบบตรวจสอบบัญชีม้า ในขณะที่ตำรวจทำหน้าที่บังคับใช้กฎหมายและปราบปราม (Mangkhalasiri & Poothakool, 2025).

6. การจัดการความมั่นคงปลอดภัยในองค์กรสมัยใหม่ (Security in Modern Organizations)

ในองค์กรยุคใหม่ปัจจุบัน ความมั่นคงปลอดภัยไม่ได้เป็นเพียงแผนก “ยาม” ที่แยกตัวโดดเดี่ยว (Silo) อยู่ป้อมหน้าประตูอีกต่อไป แต่ได้กลายเป็นฟังก์ชันการบริหารที่แทรกซึม (Embedded) อยู่ในทุกส่วนงานขององค์กร และมีความสำคัญเชิงกลยุทธ์ (Strategic Importance) (Vellani, 2020)

6.1 การบูรณาการข้ามสายงาน (Cross-Functional Integration)

HR & Security: การรักษาความมั่นคงปลอดภัยในองค์กรเริ่มตั้งแต่ก่อนพนักงานก้าวเท้าเข้าบริษัท ฝ่าย HR ต้องทำงานร่วมกับฝ่ายความมั่นคงปลอดภัยในการ คัดกรองพนักงาน (Background Check) ตรวจสอบประวัติอาชญากรรมและประวัติการทำงาน หาก HR รับมิจฉาชีพเข้ามาทำงาน ระบบล็อกประตูที่แข็งแรงที่สุดก็ไร้ความหมาย (The insider threat bypasses the lock)

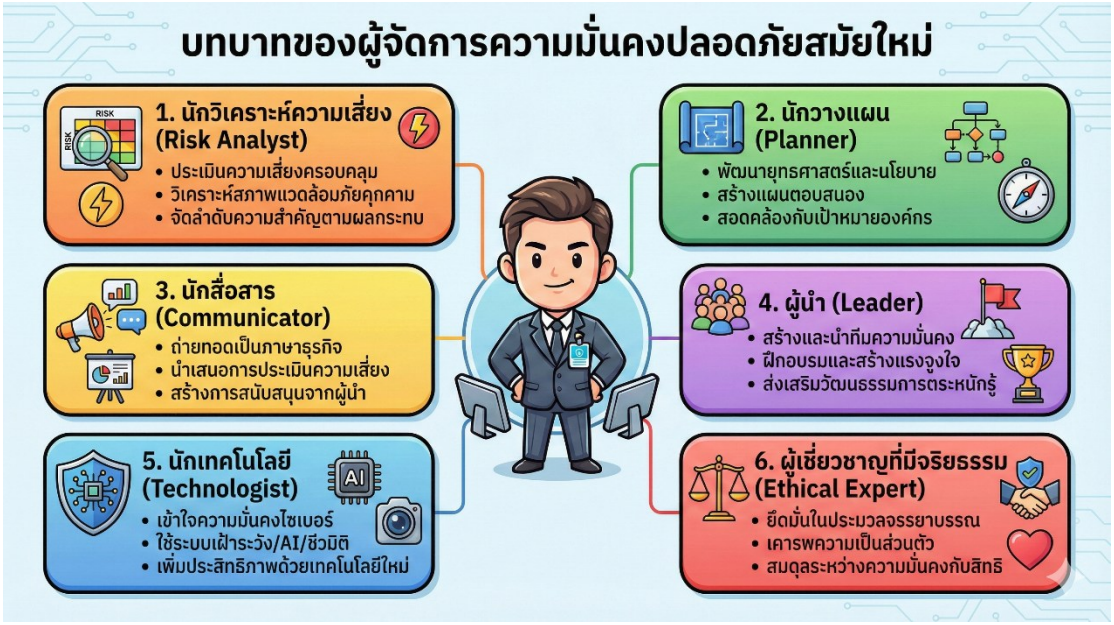
IT & Security: ในยุคที่ระบบกายภาพถูกควบคุมด้วยคอมพิวเตอร์ (Physical-Cyber Convergence) เช่น ประตูอัตโนมัติ กล้องวงจรปิด หรือระบบลิฟต์ ล้วนเชื่อมต่อผ่าน Network หากฝ่าย IT ดูแลความมั่นคงปลอดภัยของเครือข่ายไม่ดี แฮกเกอร์อาจเจาะระบบเพื่อสั่งเปิดประตูให้โจรเข้า หรือสั่งปิดกล้องวงจรปิดเพื่ออำพรางหลักฐานได้ ดังคำกล่าวที่ว่า “ถ้า Cyber ไม่รอด Physical ก็ไม่เหลือ”

Legal/Compliance & Security: ฝ่ายกฎหมายและฝ่ายความมั่นคงปลอดภัยต้องร่วมมือกันเพื่อให้มั่นใจว่ามาตรการต่าง ๆ สอดคล้องกับกฎหมายแรงงาน กฎหมายความปลอดภัย (Safety) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อป้องกันองค์กรจากความเสี่ยงทางกฎหมาย

6.2 บทบาทผู้บริหารความมั่นคงปลอดภัยข้อมูล (CISO) และโครงสร้างการรายงาน

ตำแหน่ง Chief Information Security Officer (CISO) หรือผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ มีบทบาทสำคัญมากขึ้นเรื่อย ๆ ในปัจจุบัน CISO ไม่ได้อยู่ใต้ฝ่าย IT เสมอไป แต่เริ่มมีการรายงานตรงต่อ CEO หรือคณะกรรมการบริหารความ

เสี่ยง (Risk Committee) เพื่อให้มั่นใจว่าประเด็นความมั่นคงปลอดภัย (ทั้ง Cyber และ Physical) ถูกนำไปพิจารณาในการตัดสินใจทางธุรกิจระดับกลยุทธ์ (Mangkhalasiri & Poothakool, 2025) เช่น หากบริษัทจะขยายสาขาไปยังพื้นที่ที่มีความขัดแย้ง หรือจะเปิดตัวแอปพลิเคชันใหม่ ต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Assessment) ก่อนการอนุมัติโครงการเสมอ



ภาพที่ 1.7
บทบาทของผู้จัดการความมั่นคงปลอดภัยสมัยใหม่
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

7. ความมั่นคงปลอดภัยในบริบทและวัฒนธรรมไทย (Thai Contextual Nuances)

การนำทฤษฎีการจัดการความมั่นคงปลอดภัยจากตะวันตกมาใช้ในประเทศไทย จำเป็นต้องมีการ “ปรับบริบท” (Localization) ให้เข้ากับสภาพสังคมและวัฒนธรรมไทยที่มีเอกลักษณ์เฉพาะตัว

7.1 วัฒนธรรม “เกรงใจ” กับช่องโหว่ความมั่นคงปลอดภัย

“ความเกรงใจ” เป็นคุณธรรมอันดีงามที่ฝังรากลึกในสังคมไทย หมายถึงการไม่อยากทำให้ผู้อื่นลำบากใจ หรือการให้เกียรติผู้อาวุโส แต่ในงานรักษาความมั่นคงปลอดภัย ความเกรงใจคือ **ช่องโหว่ (Vulnerability)** ที่ร้ายแรงที่สุด (Jittichanon, 2018)

ปัญหา: เจ้าหน้าที่รักษาความปลอดภัยผู้น้อยมักจะรู้สึก “เกรงใจ” ที่จะขอดูบัตรประจำตัว หรือขอตรวจค้นรถยนต์ของผู้บริหารระดับสูง (ผู้ใหญ่), ข้าราชการชั้นผู้ใหญ่,

หรือแขก VIP ที่ดูมีฐานะ อาชญากรที่เข้าใจจุดอ่อนทางวัฒนธรรมนี้จะใช้วิธีการ **"วิศวกรรมสังคม" (Social Engineering)** โดยการแต่งกายดูดี ขับรถหรู หรือแสดงท่าทีมีอำนาจ (Acting Authoritatively) เพื่อกดดันให้เจ้าหน้าที่ละเลยมาตรการตรวจสอบ

ทางแก้: ผู้จัดการความมั่นคงปลอดภัยต้องสร้างวัฒนธรรมองค์กรใหม่ โดยปลูกฝังว่า **"การปฏิบัติตามกฎอย่างเท่าเทียมคือการให้เกียรติสูงสุดต่อความมั่นคงปลอดภัยขององค์กร"** และผู้บริหารระดับสูงต้องทำตัวเป็นแบบอย่าง (Role Model) โดยยอมให้ตรวจค้นอย่างเต็มใจ เพื่อส่งสัญญาณว่า "ไม่มีใครอยู่เหนือกฎความมั่นคงปลอดภัย"

7.2 ระบบ "บุญคุณ" และอุปสรรคในการแจ้งเบาะแส

ระบบอุปถัมภ์หรือความสัมพันธ์แบบ "บุญคุณ" (Reciprocity/Patronage) อาจเป็นอุปสรรคต่อการรายงานความผิด (Whistleblowing) พนักงานอาจไม่กล้าแจ้งเบาะแสเมื่อเห็นเพื่อนร่วมงานหรือหัวหน้ากระทำความผิด (เช่น การขโมยของ หรือการละเลยกฎความปลอดภัย) เพราะถือว่าบุคคลนั้นเคยมีบุญคุณช่วยเหลือตนมาก่อน หรือกลัวการถูกมองว่า "เนรคุณ" (Jittichanon, 2018)

ทางแก้: องค์กรต้องสร้างระบบการรายงานที่ **ปกปิดตัวตนอย่างแท้จริง (Truly Anonymous Reporting Channels)** และให้ความคุ้มครองผู้แจ้งเบาะแสอย่างเข้มงวด เพื่อให้พนักงานกล้าที่จะก้าวข้ามกำแพงวัฒนธรรมนี้เพื่อรักษาผลประโยชน์ขององค์กร

7.3 วินมอเตอร์ไซค์: หน่วยข่าวกรองชุมชน (Community Intelligence)

ในบริบทเมืองไทย โดยเฉพาะในกรุงเทพมหานคร "วินมอเตอร์ไซค์" ถือเป็นทรัพยากรด้านความมั่นคงปลอดภัยที่ตำราตะวันตกไม่มีสอน พวกเขาคือ "เจ้าถิ่น" ที่รู้จักพื้นที่และคนในชุมชนดีที่สุด ผู้จัดการความมั่นคงปลอดภัยที่ชาญฉลาดจะสร้างสัมพันธภาพที่ดีกับวินมอเตอร์ไซค์หน้าอาคาร เพราะพวกเขาสามารถทำหน้าที่เป็น **"หน่วยข่าวกรอง" (Intelligence Unit)** ที่มีประสิทธิภาพสูง คอยสังเกตความผิดปกติ แจ้งเตือนเรื่องบุคคลแปลกหน้า หรือแจ้งเหตุทะเลาะวิวาทรอบนอกอาคารได้รวดเร็วกว่ากล้องวงจรปิด หรือแม้แต่ช่วยสกัดจับคนร้ายที่กำลังหลบหนีในซอยแคบ ๆ ที่รถยนต์เข้าไม่ถึง (Punnoi, 2018)

8. ทฤษฎีทางอาชญาวิทยาในบริบทไทย (Criminological Theories in Thai Context)

การเป็นผู้จัดการความมั่นคงปลอดภัยมืออาชีพต้องสามารถอธิบายปรากฏการณ์ด้วยหลักการและทฤษฎีได้ ไม่ใช่ใช้เพียงสามัญสำนึก

8.1 ทฤษฎีกิจกรรมประจำวัน (Routine Activity Theory - RAT):

ทฤษฎีนี้ระบุว่าอาชญากรรมจะเกิดขึ้นเมื่อองค์ประกอบ 3 อย่างมาบรรจบกันในเวลาและสถานที่เดียวกัน:

1. ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender)

2. เป้าหมาย/เหยื่อที่เหมาะสม (Suitable Target)

3. การขาดผู้พิทักษ์ที่เข้มแข็ง (Lack of Capable Guardian) (Fay, 2010)

การประยุกต์ใช้ในไทย: โครงการ **"Smart Safety Zone 4.0"** คือความพยายามของรัฐในการแทรกแซงองค์ประกอบที่ 3 โดยการติดตั้งกล้อง AI และปุ่ม SOS เพื่อทำหน้าที่เป็น "Capable Guardian" (ผู้พิทักษ์) ในพื้นที่ ๆ มีความเสี่ยง เพื่อทำลายวงจรก่อนที่อาชญากรรมจะเกิด (Hakparn et al., 2024)

8.2 ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory):

อาชญากรคือมนุษย์ที่มีเหตุผล พวกเขาจะตัดสินใจก่อเหตุโดยการชั่งน้ำหนักระหว่าง "ต้นทุน/ความเสี่ยง" (Cost/Risk) กับ "ผลตอบแทน" (Benefit) (Fay, 2010)

การประยุกต์ใช้ในไทย: ร้านทองทั่วไปที่ติดตั้งประตูนิรภัยสองชั้น (Double Interlocking Doors) และลูกกรงเหล็ก ไม่ได้หวังว่าจะหยุดโจรได้ 100% แต่ต้องการ **"เพิ่มต้นทุน" (Increase Effort)** และ **"เพิ่มความเสี่ยง" (Increase Risk)** ให้สูงจนโจรคำนวณแล้วว่า "ไม่คุ้ม" และเปลี่ยนใจไปหาเป้าหมายอื่นที่ง่ายกว่า

8.3 ทฤษฎีหน้าต่างแตก (Broken Windows Theory):

ความไร้ระเบียบเล็กน้อยที่ไม่ได้รับการแก้ไข จะส่งสัญญาณว่า "ที่นี่ไม่มีใครดูแล" และนำไปสู่อาชญากรรมที่รุนแรงขึ้น (Fay, 2010)

การประยุกต์ใช้ในไทย: หากผู้จัดการอาคารปล่อยให้มีขยะสะสม หรือหลอดไฟทางเดินเสียในลานจอดรถเพียงไม่กี่ดวง มันจะเป็นสัญญาณเชิญชวนให้มิจฉาชีพเข้ามางัดแงะรถยนต์ การจัดการความมั่นคงปลอดภัยที่ดีจึงต้องใส่ใจเรื่อง **การบำรุงรักษาสภาพแวดล้อม (Maintenance)** ให้ดูเป็นระเบียบเรียบร้อยอยู่เสมอ เพื่อส่งสัญญาณแห่งการควบคุม **(Signal of Control)**

9. ความท้าทายและแนวโน้มในอนาคต (Challenges and Future Trends 2026+)

9.1 สังคมผู้สูงอายุ (Aging Society) และค่าแรง:

ประเทศไทยกำลังก้าวเข้าสู่สังคมผู้สูงอายุระดับสุดยอด (Super-Aged Society) ซึ่งส่งผลให้แรงงานหนุ่มสาวที่จะมาทำงาน รปภ. หายากขึ้นเรื่อย ๆ ประกอบกับการปรับขึ้นค่าแรงขั้นต่ำในปี 2024-2025 (400 บาท) ทำให้ต้นทุนการจ้างคนสูงขึ้นอย่างมาก

แนวโน้ม: ธุรกิจจะเปลี่ยนผ่านสู่ **Security System Integration** มากขึ้น คือการใช้คนน้อยลงแต่ใช้คนที่มีทักษะสูงขึ้น ควบคู่ไปกับการใช้เทคโนโลยี (AI Cameras, Drones, IoT Sensors) มาทดแทนแรงงานคนในงานที่ซ้ำซ้อน

9.2 ภัยคุกคามไซเบอร์และ AI (Cyber & AI Threats):

สถิติปี 2025 ชี้ว่าการโจมตีด้วย Spyware ในไทยพุ่งสูงขึ้นกว่า 21,000 ครั้ง ในช่วงครึ่งปีแรก 36 นอกจากนี้ การใช้ AI สร้าง Deepfake (ปลอมเสียง/หน้าผู้บริหาร เพื่อหลอกโอนเงิน) กำลังกลายเป็นภัยคุกคามใหม่ ผู้จัดการความมั่นคงปลอดภัยในอนาคต ต้องมีความรู้เรื่อง Tech Literacy เพื่อรู้เท่าทันภัยเหล่านี้

9.3 การคุ้มครองข้อมูล (Data Privacy):

การบังคับใช้กฎหมาย PDPA จะเข้มข้นขึ้น การรักษาความมั่นคงปลอดภัยข้อมูลจะไม่ใช่แค่เรื่องไอที แต่เป็นเรื่องความรับผิดชอบขององค์กร การจัดการความมั่นคงปลอดภัยจะต้องทำงานใกล้ชิดกับ DPO (Data Protection Officer) เพื่อป้องกันข้อมูลรั่วไหล ซึ่งมีโทษปรับทางปกครองที่สูงมาก (Boonnark, 2025)

ภาพที่ 1.8

ทักษะความสามารถหลักสำหรับผู้จัดการความมั่นคงปลอดภัย

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

10. บทสรุป (Conclusion)

การจัดการความมั่นคงปลอดภัยในศตวรรษที่ 21 ไม่ใช่เรื่องของ “การใช้กำลัง” แต่คือเรื่องของ **“สติปัญญาและการบริหารจัดการ”** มากกว่า ภาพยนตร์ *Die Hard* ชี้ให้เห็นชัดว่าเหตุการณ์ร้ายแรงมักเริ่มจากความล้มเหลวด้านระบบ การควบคุมพื้นที่อาณาเขตหละหลวม การเฝ้าระวังที่ไม่เพียงพอ และทีมตอบสนองเหตุการณ์ที่ไม่ได้รับการฝึก ซึ่งทำให้ภัยคุกคามขยายเพิ่มเติมขึ้นได้เองแม้ก่อนศัตรูจะลงมือจริง บทเรียนนี้สะท้อนบริบทของไทยที่องค์กรต้องเผชิญทั้งความเสี่ยงทางกายภาพและภัยไซเบอร์ที่เปลี่ยนรูปเร็ว ความ

ปลอดภัยจึงต้องถูกออกแบบให้ “ฝังอยู่ในงานหลัก” ขององค์กร ไม่ใช่ภารกิจประกอบที่คอยตามแก้ปัญหาทีหลัง

ในโลกที่เทคโนโลยีใหม่ กฎหมายใหม่ และความเสี่ยงที่คลุมเครือเกิดขึ้นพร้อมกัน แนวทางความมั่นคงแบบเดิมที่ยึดโปรโตคอลตายตัวจะกลายเป็นจุดอ่อนทันที เพราะขาดความยืดหยุ่นและการคิดเชิงกลยุทธ์ ความมั่นคงที่มีประสิทธิผลจึงต้องเป็นระบบที่เรียนรู้ได้ ปรับตัวได้ และพร้อมรับ “ภัยที่ยังไม่รู้จัก” ผู้บริหารความมั่นคงยุคใหม่จึงทำหน้าที่คล้ายผู้จัดการความเสี่ยงเชิงรุกที่สามารถ คาดการณ์ ป้องกัน ลดผลกระทบ และทำให้ทั้งองค์กรเข้าใจว่าเหตุใดความมั่นคงจึงเป็นเรื่องของการตัดสินใจและการจัดสรรทรัพยากรอย่างชาญฉลาด

สำหรับนักศึกษาที่มุ่งสู่บทบาทผู้บริหารความมั่นคงในอนาคต เป้าหมายไม่ใช่การเป็น “หัวหน้ายาม” แต่คือการเป็น **“Strategic Risk Manager”** ที่บูรณาการ 3 แกนหลักให้ทำงานร่วมกันได้จริง ได้แก่ คน (วัฒนธรรมความมั่นคง การพัฒนาทักษะ ความตื่นตัว), เทคโนโลยี (คัดเลือก ควบคุม ใช้อย่างมีสติ), และ กฎหมาย (การกำกับดูแล ความรับผิด และการคุ้มครองสิทธิ) ภารกิจส่วนตัวของคุณคือทำให้ “นากาโตมิ พลาซ่า” ที่คุณรับผิดชอบทั้งโลกกายภาพและโลกดิจิทัล ต้องไม่พังลงเพราะความประมาทหรือการบริหารที่ไม่รอบคอบ และทำให้ความมั่นคงถูกมองเป็น “การลงทุนเชิงกลยุทธ์” ที่สร้างความเชื่อมั่นและความต่อเนื่องให้แก่องค์กร ไม่ใช่เพียงศูนย์ต้นทุนอีกต่อไป

11. คำถามทบทวน (Review Questions)

1. จากกรณีศึกษาอาคารนากาโตมิ พลาซ่า (*Die Hard*) และเหตุการณ์กราดยิงที่ศูนย์การค้าสยามพารากอน จงอธิบายความหมายของ “ความล้มเหลวเชิงระบบในการจัดการความมั่นคงปลอดภัย” (Systemic Failure) และอภิปรายว่าความล้มเหลวดังกล่าวสะท้อนจุดอ่อนด้านใดของการบริหารจัดการมากกว่าความล้มเหลวทางเทคโนโลยีอย่างไร?

2. จงอธิบายความแตกต่างระหว่างแนวคิด “Safety” และ “Security” พร้อมยกตัวอย่างสถานการณ์ในบริบทองค์กรหรือสังคมไทยที่แสดงให้เห็นว่าผู้จัดการความมั่นคงปลอดภัยจำเป็นต้องบริหารทั้งสองมิติไปพร้อมกัน?

3. แนวคิด “ความมั่นคงปลอดภัยเชิงวัตถุวิสัย (Objective Security)” และ “ความมั่นคงปลอดภัยเชิงจิตวิสัย (Subjective Security)” แตกต่างกันอย่างไร และเพราะเหตุใดแนวคิดเรื่อง “Security Theater” จึงถือเป็นกับดักที่อันตรายต่อการจัดการความมั่นคงปลอดภัยในองค์กร?

4. อธิบายองค์ประกอบของ “ระบบนิเวศความมั่นคงปลอดภัย” (Security Ecosystem) ทั้ง 4 ประเภท พร้อมวิเคราะห์ว่าทำไม “ข้อมูลและชื่อเสียง” จึงกลายเป็นสินทรัพย์ที่มีความเปราะบางสูงที่สุดในยุคดิจิทัลของประเทศไทย?

5. จากวิวัฒนาการของวิชาชีพความมั่นคงปลอดภัยในประเทศไทย ตั้งแต่ยุคเฝ้ายามแบบดั้งเดิมจนถึงยุคเทคโนโลยีและ AI จงอภิปรายว่าบทบาทและทักษะของผู้จัดการความมั่นคงปลอดภัยในอนาคตควรเปลี่ยนแปลงไปอย่างไร เพื่อรับมือกับความท้าทายด้านแรงงาน ค่าแรง และภัยคุกคามรูปแบบใหม่?

12. เอกสารอ้างอิง (References)

Allan, J. (2025, February 24). *Thailand grapples with a cybersecurity crisis as attacks soar 70% higher than the global average*. Thailand Business News. https://www.thailand-business-news.com/corporate/196696-thailand-grapples-with-a-cybersecurity-crisis-as-attacks-soar-70-higher-than-the-global-average

ASIS International. (2024). *Standards & guidelines*. https://www.asisonline.org

Boonnark, C. (2025, September 2). *Thailand: PDPA crackdown 2025: Are you next? – Major fines and lessons from Thailand's latest enforcement*. *Privacy Matters – DLA Piper*.

https://privacymatters.dlapiper.com/2025/09/thailand-pdpa-crackdown-2025-are-you-next-major-fines-and-lessons-from-thailands-latest-enforcement/

Chambers, P., & Waitoolkiat, N. (2021). *Thailand's security sector "deform" and "reform"* (PRIF Working Paper No. 52). Peace Research Institute Frankfurt (PRIF). https://www.prif.org/fileadmin/Daten/Publikationen/Prif_Working_Papers/PRIF_WP_52.pdf

Fay, J. J. (2010). *Contemporary security management* (3rd ed.). Butterworth-Heinemann.

Hakparn, S., Sinloyma, P., Ruangrod, T., Rattanapratheep, K., Pongratchatanan, P., Pongratchatanan, P., Yaemyim, W., & Pullteap, S. (2024). Smart safety zones using intelligent surveillance systems for public crime prevention and emergency response. *International Journal of Control Systems and Robotics, 9*, 5–12.

Jittichanon, S. (2018). "Bunkhun" the ideology effect of Thai business management. *Journal of Global Business Review, 20*(2), 61–75.

Krisanaraj, J. (2022, November 15). *Thailand's award-winning 'Smart Safety Zone' makes cities much safer: Police*. Nation Thailand.

https://www.nationthailand.com/thailand/general/40022107

Mangkhalasiri, P., & Poothakool, K. (2025). Data science in policing in Thailand: Challenges and future directions – A review from international perspectives. *Journal of Contemporary Social Sciences and Humanities, 12*(2), 18–34. https://doi.org/10.59796/jcsh.v12i2.18-34

Mascellino, A. (2024, January 23). *Thai court blocks 9near.org to avoid exposure of 55M citizens*. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/thai-court-blocks-9nearorg/

Ministerial Regulation Authorizing Security Guard Business Operation B.E. 2560 (2017). (2017). Royal Thai Police.

https://www.royalthaipolice.go.th/downloads/laws/laws_05_05.pdf

Newport, A. (2023, October 26). *Tourism stakeholders remain cautious after Bangkok mall shooting*. TTG Asia.

https://www.ttgasia.com/2023/10/26/tourism-stakeholders-remain-cautious-after-bangkok-mall-shooting/

Pinkerton. (2024). *The evolution of security in a post-9/11 landscape*. https://pinkerton.com/our-insights/blog/the-evolution-of-security-in-a-post-911-landscape

Punnoi, N. (2018). The motorcycle taxi driver as a community reporter: Guidelines for the promotion of a marginalized group's participation in the improvement of public space by using information and communication technology. *NAKHARA: Journal of Environmental Design and Planning, 14*(1), 145–160.

Security Guard Business Act B.E. 2558 (2015). (2015). Office of the Council of State (unofficial English translation).

https://world.moleg.go.kr/cms/commonDown.do?DLD_CFM_NO=ESMSVF2FGY3U26B9XPR4&FL_SEQ=82750

Thailand Convention and Exhibition Bureau. (2023, October 4). *TCEB situation update: Shooting incident at Siam Paragon Mall in Bangkok on October 3, 2023* [Press release]. Business Events Thailand.

https://www.businesseventsthailand.com/press-media/news-press-release/detail/1549-tceb-situation-update-shooting-incident-at-siam-paragon-mall-in-bangkok-on-october-3-2023

U.S. Department of State. (2024). *2024 investment climate statements: Thailand*. United States Department of State. https://www.state.gov/reports/2024-investment-climate-statements/thailand

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