SMA1202
SECURITY: THEORY AND PRACTICE
หลักการและทฤษฎีความมั่นคงปลอดภัย

CHAPTER 4
RISK ASSESSMENT AND RISK MANAGEMENT

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

บทที่ 4
การประเมินความเสี่ยงและการบริหารความเสี่ยง
Risk Assessment and Risk Management

1. บทนำ (Introduction)

1.1 บทเรียนจากฮอลลีวูดสู่ความจริงที่โหดร้าย (From Hollywood's Iconic Film to the Harsh Reality)

ในโลกของภาพยนตร์ระดับบล็อกบัสเตอร์ โศกนาฏกรรมของเรือ RMS Titanic มักถูกจดจำผ่านเลนส์โรแมนติกของภาพยนตร์ปี 1997 โดยเจมส์ คาเมรอน ภาพของแจ็คและโรสยืนกางแขนรับสายลมกลางมหาสมุทรแอตแลนติกกลายเป็นสัญลักษณ์แห่งความรักและการเสียสละ แต่หากถอดแว่นตาความบันเทิงออก และมองด้วยสายตาของนักบริหารความมั่นคงปลอดภัยหรือผู้เชี่ยวชาญด้านการบริหารความเสี่ยง Titanic คือ “ตำราเรียนแห่งหายนะ” ที่มีชีวิต เป็นกรณีศึกษาคลาสสิกซึ่งสะท้อนอย่างเจ็บแสบว่าภัยพิบัติระดับโลกแทบไม่เคยเกิดจากโชคร้ายหรือพลังธรรมชาติเพียงลำพัง หากเกิดจากความล้มเหลวเชิงระบบของการตัดสินใจ ได้แก่ การเพิกเฉยต่อสัญญาณเตือน การลดทอนข้อมูลเชิงประจักษ์ การยึดติดกับชื่อเสียง เทคโนโลยี และแรงกดดันด้านเวลา จนก่อให้เกิด “โครงสร้างทางความคิดที่พังทลาย” ของผู้นำที่เลือกบริหารความเสี่ยงด้วยความเชื่อและอารมณ์ มากกว่าหลักฐานและการประเมินเชิงเหตุผล ผลลัพธ์จึงไม่ใช่โศกนาฏกรรมจากโชคชะตา แต่คือบทเรียนคมกริบว่าความมั่นใจเกินขนาด การกำกับดูแลที่อ่อนแอ และการจัดการความเสี่ยงที่ผิดพลาด สามารถพาองค์กรที่ยิ่งใหญ่ที่สุดในยุคนั้นจมลงได้อย่างไร และทำไม Titanic จึงยังคงเป็นกรณีศึกษาที่ทรงพลังสำหรับศาสตร์ความมั่นคงและการบริหารความเสี่ยงมาจนถึงปัจจุบัน

ย้อนกลับไปในปี ค.ศ. 1912 เรือ RMS Titanic ถูกยกย่องว่าเป็นสุดยอดความสำเร็จของวิศวกรรมสมัยใหม่ ด้วยโครงสร้างห้องกันน้ำ (watertight compartments) ถึง 16 ห้อง และระบบประตูปิดอัตโนมัติที่ถูกโฆษณาว่าเพียงพอจะทำให้เรือลำนี้ “แทบไม่มีวันจม” (practically unsinkable) ความเชื่อมั่นดังกล่าวไม่ได้เป็นเพียงข้อความทางการตลาด หากแต่ค่อย ๆ พัฒนาเป็น “คำบรรยายเชิงอุดมการณ์ขององค์กร” (confidence narrative) ที่ฝังรากลึกอยู่ในจิตสำนึกของผู้บริหารและลูกเรือ มันทำหน้าที่เสมือน “เกราะทางจิตวิทยา” (psychological shield) ที่ลดทอนความไวต่อความเสี่ยง ทำให้การตั้งคำถามเชิงวิพากษ์ต่อเทคโนโลยีถูกมองว่าไม่จำเป็น และนำไปสู่ความสับสนเชิงแนวคิด

ระหว่าง ศักยภาพทางเทคโนโลยี (technological capability) กับ ความสามารถในการอยู่รอดของระบบ (organizational and system resilience) (Battles, 2001)

คืนวันที่ 14 เมษายน ค.ศ. 1912 กลายเป็นจุดทดสอบความเชื่อมั่นนั้นอย่างโหดร้าย ท่ามกลางความหนาวเหน็บของมหาสมุทรแอตแลนติกเหนือ กัปตันเอ็ดเวิร์ด สมิธ เลือกนำเรือเดินหน้าด้วยความเร็วเกือบสูงสุดราว 22 น็อต ทั้งที่ตลอดทั้งวันได้รับคำเตือนเรื่องภูเขาน้ำแข็งจากเรือลำอื่นอย่างต่อเนื่องอย่างน้อย 6–7 ครั้ง คำเตือนเหล่านี้คือ risk signals ที่มีความถี่และความรุนแรงสูง แต่กลับถูกลดสถานะให้เป็นเพียง “ข้อมูลรบกวน” (noise) ในกระบวนการตัดสินใจ เนื่องจากการประเมินความเสี่ยงที่บกพร่อง (risk assessment failure) ซึ่งให้ค่าน้ำหนักของโอกาสเกิดเหตุ (likelihood) และผลกระทบ (impact) ต่ำกว่าความเป็นจริง ภายใต้สมมติฐานว่าเทคโนโลยีของเรือสามารถรองรับสถานการณ์เลวร้ายได้เสมอ การเดินเรือด้วยความเร็วสูงจึงไม่ใช่เพียงความประมาทส่วนบุคคล หากแต่เป็นผลผลิตของโครงสร้างการตัดสินใจที่ถูกครอบงำด้วยความมั่นใจเกินขนาดและแรงกดดันด้านชื่อเสียงและเป้าหมายเชิงพาณิชย์ (Labib & Read, 2013)

ภาพที่ 4.1
เรือ RMS Titanic จากภาพยนตร์ *Titanic* (1997)
ที่มา: Paramount Pictures; 20th Century Fox.

ขณะเดียวกัน ความล้มเหลวเชิงโครงสร้างที่ร้ายแรงไม่แพ้กันเกิดขึ้นในระบบการสื่อสารความเสี่ยง (risk communication) ห้องวิทยุโทรเลขของ Titanic ซึ่งดำเนินการโดย

พนักงานของบริษัท Marconi ให้ความสำคัญกับการส่งข้อความส่วนตัวของผู้โดยสารชั้นหนึ่งเพื่อสร้างรายได้มากกว่าการจัดการข้อมูลเตือนภัย เมื่อเรือ Californian พยายามแจ้งเตือนถึงทุ่งน้ำแข็งที่อยู่ใกล้เข้ามา ข้อความกลับถูกปฏิเสธด้วยประโยคสั้น ๆ ว่า “หุบปาก! ฉันกำลังยุ่ง!” ประโยคนี้ไม่ใช่เพียงเกร็ดประวัติศาสตร์ หากแต่เป็นสัญลักษณ์ของ risk communication failure อย่างสมบูรณ์แบบ เพราะข้อมูลข่าวกรองด้านความเสี่ยงที่สำคัญที่สุด (critical risk intelligence) ถูกปิดกั้น ไม่ถูกส่งต่อ และไม่ถูกแปลงเป็นการตัดสินใจเชิงปฏิบัติ ในท้ายที่สุด โศกนาฏกรรมของ Titanic จึงไม่ได้สะท้อนเพียงข้อจำกัดของเทคโนโลยี หากแต่เผยให้เห็นความล้มเหลวของวัฒนธรรมความปลอดภัยและการกำกับความเสี่ยงทั้งระบบ (Bigg & Billings, 2014)

ผลลัพธ์สุดท้ายคือการสูญเสียชีวิตมากกว่า 1,500 คน ทั้งนี้ ไม่ใช่เพราะการชนภูเขาน้ำแข็งเพียงอย่างเดียว หากแต่เป็นผลสะสมของความล้มเหลวด้านการเตรียมพร้อมรับมือเหตุฉุกเฉิน (contingency planning) และการจัดลำดับความสำคัญที่บิดเบี้ยว เรือชูชีพบน Titanic ถูกจัดให้มีเพียงพอสำหรับผู้โดยสารแค่ประมาณครึ่งหนึ่ง โดยให้เหตุผลด้านความสวยงามของดาดฟ้าเรือและประสบการณ์เชิงหรูหราของลูกค้าเหนือหลัก “Safety First” อย่างชัดเจน นี่คือบทเรียนคลาสสิกของการบริหารความเสี่ยงที่ยึด ความสอดคล้องตามกฎหมาย (compliance) มากกว่า ความปลอดภัยเชิงสาระ (substantive safety) เพราะแม้จำนวนเรือชูชีพจะ “ถูกต้องตามข้อกำหนด” แต่กลับไม่เพียงพอต่อสถานการณ์จริง เมื่อเวลา 23:38 น. ภูเขาน้ำแข็งปรากฏขึ้นในระยะเพียงราว 500 เมตร ลูกเรือมีเวลาตัดสินใจไม่ถึง 40 วินาที ระบบหางเสือซึ่งถูกออกแบบภายใต้สมมติฐานว่าอันตรายจะถูกตรวจพบจากระยะไกล ไม่อาจหักเลี้ยวเรือขนาดมหึมาให้พ้นภัยในระยะประชิดได้ การชนเกิดขึ้น น้ำทะลักจากห้องกันน้ำหนึ่งสู่อีกห้องหนึ่งราวกับถาดหลุมที่ถูกเติมจนล้น และภายในเวลาเพียง 2 ชั่วโมง 40 นาที “เรือที่ไม่มีวันจม” ก็จมหายไปพร้อมชีวิตผู้คนจำนวนมหาศาล โศกนาฏกรรมครั้งนี้จึงเป็นภาพสะท้อนอันเจ็บปวดของสิ่งที่นักบริหารความเสี่ยงรู้ดีว่าอันตรายที่สุด นั่นก็คือ ความประมาทที่มาในคราบของความถูกต้องตามระเบียบ แต่ไร้ซึ่งการคำนึงถึงความเป็นจริงของชีวิตมนุษย์ (Battles, 2001)

1.2 จากมหาสมุทรแอตแลนติก สู่บริบทความเสี่ยงของไทย (From the Atlantic Ocean to the Risk Context of Thailand)

กว่าหนึ่งศตวรรษต่อมา บทเรียนจากแอตแลนติกกลับมาหลอนซ้ำอีกครั้งในบริบทของประเทศไทย ณ เมืองหาดใหญ่ จังหวัดสงขลา ในเดือนพฤศจิกายน พ.ศ. 2568 (ค.ศ. 2025) เมืองศูนย์กลางเศรษฐกิจทางภาคใต้แห่งนี้เคยผ่านความบอบช้ำจากน้ำท่วมใหญ่มาหลายครั้ง จนกระทั่งรัฐได้ทุ่มงบประมาณมหาศาลสร้างระบบป้องกันน้ำท่วมและคลอง

ระบายน้ำภูมินาถดำริ ความสำเร็จของระบบในอดีตทำให้เกิดภาวะ “ความคุ้นชินกับความผิดปกติ” (Normalization of Deviance) ผู้นำเมืองและผู้วางผังเมืองเชื่อมั่นในโครงสร้างพื้นฐานเหล่านี้ราวกับมันคือ Titanic ที่ไม่มีวันจมลำใหม่ จนปล่อยให้เมืองขยายตัวทับถมพื้นที่รับน้ำดั้งเดิมอย่างย่ามใจ

แต่แล้วธรรมชาติก็ยื่นบททดสอบที่ไม่เคยมีอยู่ในแผนแม่บท ระหว่างวันที่ 19-21 พฤศจิกายน 2568 พายุกระหน่ำหาดใหญ่ด้วยปริมาณฝนที่สูงถึง 630 มิลลิเมตรภายใน 72 ชั่วโมง และพุ่งสูงถึง 335 มิลลิเมตรในวันเดียว ซึ่งตามหลักสถิตินี่คือเหตุการณ์ระดับ “หนึ่งครั้งในรอบ 300 ปี” (300-year return period) ระบบระบายน้ำที่ถูกออกแบบมาเพื่อรับมือเหตุการณ์ที่ “รุนแรงตามมาตรฐานเดิม” จึงพ่ายแพ้อย่างราบคาบ ไม่ใช่เพราะขาดงบประมาณ แต่เพราะการประเมินความเสี่ยงยึดติดกับตัวเลขในอดีต (Past Precedent Fallacy) โดยละเลยสัญญาณเตือนเรื่องการเปลี่ยนแปลงสภาพภูมิอากาศที่นักวิทยาศาสตร์กระซิบเตือนมาตลอดทศวรรษ (Sangsinchai, 2025)

ความล้มเหลวที่หาดใหญ่ไม่ได้หยุดอยู่เพียงแค่ปริมาณน้ำ แต่ขยายตัวไปสู่ความล้มเหลวในการบริหารจัดการวิกฤต (Crisis Governance Failure) เมื่อรัฐบาลแต่งตั้งผู้บัญชาการขึ้นมาหลายศูนย์พร้อมกัน ทั้งจากส่วนกลาง ส่วนหน้า และหน่วยงานทหาร โครงสร้างการสั่งการที่ควรจะเป็นเอกภาพจึงกลายเป็นความสับสนทับซ้อน (Fragmented Command Structure) ข้อมูลความเสี่ยงถูกส่งต่ออย่างล่าช้าและบิดเบือนไปตามสายการบังคับบัญชาที่ยุ่งเหยิง ทำให้การตอบสนองเป็นไปในเชิงรับ (Reactive) มากกว่าเชิงรุก (Proactive) ความเสียหายจึงไม่ได้เกิดจากมวลน้ำเพียงอย่างเดียว แต่เกิดจากการตัดสินใจที่อัมพาตท่ามกลางความขัดแย้งของข้อมูล (Sangsinchai, 2025)

สิ่งที่ทั้ง Titanic และหาดใหญ่สอนเราเหมือนกันคือ “ภูเขาน้ำแข็งและมวลน้ำไม่ใช่ปัญหาที่แท้จริง” แต่ปัญหาคือการบริหารความเสี่ยงที่ไร้จินตนาการ (Failure of Risk Imagination) ผู้นำมักประเมินโอกาสเกิด (Likelihood) ต่ำเกินไป และประเมินผลกระทบ (Impact) ต่ำยิ่งกว่า เพียงเพราะ “มันไม่เคยเกิดขึ้นมาก่อนในยุคของฉัน” การมองโลกในแง่ดีเกินไป (Optimism Bias) และการยึดติดกับกฎระเบียบขั้นต่ำ (Compliance Shortcut) คือไวรัสร้ายที่กัดกินระบบความปลอดภัยจากภายใน จนเมื่อวิกฤตมาถึง ระบบที่เคยดูแข็งแกร่งกลับกลายเป็นกรงขังที่ไม่มีทางออก (Battles, 2001)

บทเรียนเหล่านี้ย้ำเตือนว่า การประเมินความเสี่ยง (Risk Assessment) ไม่ใช่การพยายามเดาอนาคตให้แม่นยำ 100% เพราะไม่มีใครรู้ว่าภูเขาน้ำแข็งจะลอยมาตรงไหน หรือฝนจะตกกี่มิลลิเมตรในคืนนั้น แต่การบริหารความเสี่ยงคือ “การตัดสินใจภายใต้ความไม่แน่นอนอย่างมีระบบ” (Decision-making under Uncertainty) มันคือการถามตัวเองอยู่

เสมอว่า “หากระบบที่ล้ำสมัยที่สุดของเราล้มเหลวในวันพรุ่งนี้ เรามีแผนรองรับที่ใช้งานได้จริงหรือไม่?” และที่สำคัญที่สุดคือ ผู้นำมีความกล้าหาญพอที่จะฟังเสียงเตือนที่ขัดใจก่อนที่หายนะจะมาถึงหรือไม่

ในบริบทขององค์กรในประเทศไทยยุค 2026 ภัยคุกคามอาจไม่ได้มาในรูปของก้อนน้ำแข็งมหึมา แต่มาในรูปของรหัสคอมพิวเตอร์ที่ซับซ้อน แก๊งคอลเซ็นเตอร์ที่ใช้ AI หลอกลวงคนไทยกว่า 168 ล้านครั้งต่อปี หรือการรั่วไหลของข้อมูลขนาดใหญ่ องค์กรที่ยังคงเชื่อในระบบป้องกันแบบเดิม ๆ โดยไม่ฝึกซ้อมแผนรับมือเหตุฉุกเฉิน (BCP) ไม่สร้างวัฒนธรรมความมั่นใจที่ตั้งอยู่บนฐานข้อมูล หรือไม่มีระบบยืนยันตัวตนหลายชั้น (MFA) ก็ไม่ต่างจากการเดินเรือลำยักษ์ฝ่าดงน้ำแข็งด้วยความเร็วสูงโดยปิดเรดาร์ เพียงเพราะเชื่อว่า “ครั้งก่อน ๆ เราก็รอดมาได้”

บทสรุปของความพินาศทั้งสองเหตุการณ์จึงชัดเจนอย่างยิ่ง: เทคโนโลยีและวิศวกรรมอาจกระซิบเตือนเราเบา ๆ ผ่านข้อมูลและตัวเลข แต่ผู้นำที่ตกอยู่ในภวังค์ของความสำเร็จมักจะตะโกนกลบเสียงเหล่านั้นด้วยคำว่า “เดินหน้าต่อด้วยความเร็วสูงสุด!” และในโลกของการบริหารความมั่นคงปลอดภัย (Security Management) เสียงตะโกนแห่งความทระนงเช่นนั้น มักถูกกลบหายไปในเสียงคำรามของหายนะที่ไม่อาจย้อนคืนเสมอ

2. ความเข้าใจเรื่องความเสี่ยงในการจัดการความมั่นคงปลอดภัย (Understanding Risk in Security Management)

2.1 นิยามศัพท์: ความเสี่ยง ภัยคุกคาม และความเปราะบาง

เพื่อให้การสื่อสารและการบริหารจัดการเป็นไปในทิศทางเดียวกัน นักศึกษาจำเป็นต้องแยกแยะความแตกต่างระหว่างคำศัพท์สำคัญ 3 คำ ได้แก่ ภัยคุกคาม (Threat) ความเปราะบาง (Vulnerability) และ ความเสี่ยง (Risk) ซึ่งมักถูกใช้ปะปนกันในภาษาพูดทั่วไป แต่มีความหมายทางเทคนิคที่แตกต่างกันอย่างสิ้นเชิง

1. ภัยคุกคาม (Threat): คือ สิ่งที่เป็นต้นเหตุของอันตราย หรือสิ่งที่มีศักยภาพที่จะก่อให้เกิดความเสียหายต่อสินทรัพย์ขององค์กร ภัยคุกคามเป็นสิ่งที่ “อยู่นอกเหนือการควบคุมของเรา” และมักจะเกิดขึ้นไม่ว่าเราจะป้องกันหรือไม่ก็ตาม

ตัวอย่าง: พายุดีเปรสชันที่พัดถล่มภาคใต้ แฮกเกอร์ที่พยายามเจาะระบบธนาคาร หรือผู้ก่อการร้ายที่วางแผนวางระเบิด

2. **ความเปราะบาง (Vulnerability):** คือ จุดอ่อน ช่องโหว่ หรือข้อบกพร่อง ในระบบการป้องกัน ที่เปิดโอกาสให้ภัยคุกคามเข้ามาทำอันตรายได้ ความเปราะบางเป็นสิ่งที่ "เราสามารถควบคุมและแก้ไขได้"

ตัวอย่าง: ประตูรั้วที่ผุพัง ซอฟต์แวร์ที่ไม่ได้อัปเดตแพตช์ (Unpatched Software) พนักงานที่ขาดความตระหนักรู้เรื่องความปลอดภัย (Security Awareness) หรือวัฒนธรรมองค์กรแบบ “เกรงใจ” ที่ทำให้ไม่กล้ารายงานความผิดปกติ

3. **ความเสี่ยง (Risk):** คือ ผลลัพธ์ที่เกิดขึ้นจากการที่ภัยคุกคามฉกฉวยโอกาสจากความเปราะบาง เข้ามาทำอันตรายต่อสินทรัพย์ ความเสี่ยงคือ “โอกาสของความสูญเสีย” ที่เราต้องบริหารจัดการ

สมการความเสี่ยง: ในทางปฏิบัติ เรามักใช้นิยามอย่างง่ายว่า:

$$\textit{Risk} = \textit{Likelihood (or Probability)} \times \textit{Impact (or Consequence)}$$

ภาพที่ 4.2
การวิเคราะห์ความสัมพันธ์ระหว่าง Threat, Vulnerability และ Risk
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

กล่าวคือ *ความเสี่ยง* เกิดจากการผสมกันของ โอกาสที่เหตุการณ์จะเกิดขึ้น (Likelihood หรือ Probability) และ ความรุนแรงของผลกระทบเมื่อมันเกิดขึ้นจริง (Impact หรือ Consequence) ต่อองค์กร ชีวิต หรือระบบ หากเหตุการณ์มีโอกาสเกิดต่ำ แต่ผลกระทบรุนแรงมาก ความเสี่ยงก็ยังคงอยู่ในระดับสูงได้ เช่นเดียวกับเหตุการณ์ที่เกิด

บ่อยแต่ผลกระทบเล็กน้อย ดังนั้น การบริหารความเสี่ยงจึงไม่ใช่การมองเพียงว่า “จะเกิดหรือไม่” หรือ “รุนแรงแค่ไหน” แยกกัน แต่ต้องประเมิน สองมิติพร้อมกัน เพื่อใช้เป็นฐานในการตัดสินใจเชิงนโยบายและมาตรการควบคุมอย่างเหมาะสม

ภาพที่ 4.3

Risk Matrix ของ RMS Titanic (1912): ความเป็นจริง vs การประเมินเดิม

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

2.2 พลวัตของความเสี่ยง (The Dynamic Nature of Risk)

ความเสี่ยงไม่ใช่ค่าคงที่ (Static) แต่มีความเป็นพลวัต (Dynamic) เปลี่ยนแปลงได้ตลอดเวลาตามบริบทและสภาพแวดล้อม ทั้งนี้ ภัยคุกคามเดียวกันอาจก่อให้เกิดระดับความเสี่ยงที่แตกต่างกันในแต่ละองค์กร หรือแม้แต่ในองค์กรเดียวกันแต่ต่างช่วงเวลา

กรณีศึกษา: น้ำท่วมโรงงานในนิคมอุตสาหกรรม

โรงงาน A: ตั้งอยู่ในพื้นที่ต่ำ (Vulnerability สูง) ไม่มีเขื่อนกั้นน้ำ และเก็บเครื่องจักรราคาแพงไว้ที่ชั้นล่าง (Asset Value สูง) นำไปสู่ ความเสี่ยงระดับวิกฤต (Catastrophic Risk)

โรงงาน B: ตั้งอยู่ในพื้นที่เดียวกัน (Threat เท่ากัน) แต่มีการยกพื้นโรงงานสูง มีกำแพงกันน้ำ และย้ายเครื่องจักรสำคัญไปไว้ชั้น 2 (Vulnerability ต่ำ) นำไปสู่ ความเสี่ยงระดับจัดการได้ (Manageable Risk)

จะเห็นได้ว่า แม้ “ภัยคุกคาม” (น้ำท่วม) จะเหมือนกัน แต่ “ความเสี่ยง” แตกต่างกันอย่างสิ้นเชิงขึ้นอยู่กับการเตรียมพร้อม นี่คือเหตุผลว่าทำไมเราจึงต้องบริหารความเสี่ยง ไม่ใช่แค่บริหารภัยคุกคาม

2.3 ทำไมต้องบริหารความเสี่ยง? (Why Risk Management Matters?)

ในอดีต การรักษาความปลอดภัยมักยึดถือแนวคิด “ความมั่นคงปลอดภัยสมบูรณ์แบบ” (Absolute Security) หรือการพยายามทำให้ความเสี่ยงเป็นศูนย์ (Zero Risk) ซึ่งในทางปฏิบัติแล้วเป็นไปไม่ได้และสิ้นเปลืองทรัพยากรอย่างมหาศาล แนวคิดสมัยใหม่จึงเปลี่ยนมาเป็น “การบริหารความเสี่ยง” (Risk Management) ซึ่งยอมรับความจริงว่าความเสี่ยงบางอย่างต้องคงอยู่ แต่เราต้องควบคุมให้อยู่ในระดับที่ยอมรับได้ (Acceptable Level)

เหตุผลสำคัญที่องค์กรไทยต้องให้ความสำคัญกับการบริหารความเสี่ยง ได้แก่:

1. **ความซับซ้อนของภัยคุกคาม:** จากภัยธรรมชาติที่รุนแรงขึ้น (Climate Change) ไปจนถึงภัยไซเบอร์ที่ไร้พรมแดน ทำให้การป้องกันแบบเดิม ๆ (เช่น การสร้างกำแพง หรือ Firewall) ไม่เพียงพออีกต่อไป

2. **ข้อกำหนดทางกฎหมาย:** กฎหมายอย่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) หรือ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) กำหนดให้องค์กรต้องมีการประเมินความเสี่ยงเป็นมาตรฐานขั้นต่ำ หากละเลยอาจมีโทษทั้งจำและปรับ (National Cyber Security Agency, 2025)

3. **การจำกัดความเสียหาย:** เมื่อเกิดเหตุการณ์ไม่คาดฝัน การมีการประเมินความเสี่ยงที่ดีจะช่วยให้องค์กรฟื้นตัวได้เร็ว (Resilience) ลดความสูญเสียทั้งชีวิตและทรัพย์สิน เหมือนกับการมีเรือชูชีพที่เพียงพอและแผนอพยพที่ซักซ้อมมาอย่างดีบนเรือ Titanic

ในปัจจบัน บริษัทหลากหลายแห่งในประเทศไทยแห่ซื้อประกันภัยไซเบอร์เพื่อรับมือกับการรั่วไหลของข้อมูลที่พุ่งสูงขึ้น แต่ความจริงที่น่ากังวลคือ “ประกันภัยไม่ใช่ยาสามัญประจำบ้านที่แก้ความเสี่ยงได้ทุกอย่าง” โดยบทเรียนจากคลื่นการโจมตีในปี 2025 ชี้ให้เห็นว่าองค์กรส่วนใหญ่ขาดการประเมินความเสี่ยงอย่างเป็นระบบและมักจะพบช่องโหว่เมื่อสายเกินไป ข้อมูลจาก Kaspersky ยืนยันว่ายังมีเซิร์ฟเวอร์ในไทยกว่า 200,000 เครื่อง ที่ตกอยู่ในอันตราย ซึ่งสะท้อนถึงความล้มเหลวในการประเมินความเสี่ยงและการอัปเดตแพตช์ (Patching) ที่ล่าช้า เปรียบเสมือนการซื้อประกันชีวิตแต่ยังคงเดินฝ่าดงระเบิดโดยไม่ใส่ใจสัญญาณเตือนใด ๆ (Chuthapiphat, 2025)

ภาพที่ 4.4
วัตถุประสงค์สำคัญของการประเมินความเสี่ยง
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

3. กระบวนการประเมินความเสี่ยง (The Risk Assessment Process)

กระบวนการประเมินความเสี่ยงเปรียบเสมือนการตรวจสุขภาพประจำปีของระบบรักษาความปลอดภัย เพื่อค้นหาโรคร้ายที่ซ่อนอยู่ก่อนที่จะแสดงอาการรุนแรง กระบวนการนี้เป็นมาตรฐานสากลที่อ้างอิงจาก ISO 31000 โดยประกอบด้วย 4 ขั้นตอนหลักที่วนเป็นวัฏจักร (International Organization for Standardization, 2018)

3.1 การระบุสินทรัพย์ (Asset Identification)

ขั้นตอนแรกและสำคัญที่สุดคือการตอบคำถามว่า “เรามีอะไรที่มีค่าบ้าง?” เพราะเราไม่สามารถป้องกันสิ่งที่เราไม่รู้ว่ามีอยู่ได้ (You cannot protect what you don't know)

1. สินทรัพย์ที่จับต้องได้ (Tangible Assets): อาคาร เครื่องจักร เงินสด สินค้าคงคลัง อุปกรณ์ไอที ฯลฯ

2. สินทรัพย์ที่จับต้องไม่ได้ (Intangible Assets): ข้อมูลลูกค้า (Customer Data) ทรัพย์สินทางปัญญา (IP) สูตรการผลิต และที่สำคัญที่สุดคือ ชื่อเสียง (Reputation)

3. บุคลากร (Human Assets): พนักงาน ผู้บริหาร ลูกค้า ความปลอดภัยของชีวิตคนต้องมาก่อนเสมอ (Life Safety First)

ในบริบทของประเทศไทย ข้อมูลส่วนบุคคล (Personal Data) กลายเป็นสินทรัพย์ที่มีความเสี่ยงสูงมากภายใต้กฎหมาย PDPA การรั่วไหลของรายชื่อลูกค้าเพียงไฟล์เดียวอาจนำมาซึ่งค่าปรับสูงสุดถึง 5 ล้านบาท และความเสียหายทางชื่อเสียงที่ประเมินค่าไม่ได้ (Vellani, 2020)

ภาพที่ 4.5
การระบุสินทรัพย์ (Asset Identification)
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

3.2 การระบุภัยคุกคาม (Threat Identification)

ขั้นตอนนี้คือการสแกนหา “ศัตรู” หรือปัจจัยเสี่ยงที่อาจสร้างความเสียหายให้แก่สินทรัพย์ โดยแบ่งเป็นกลุ่มหลัก ๆ ได้แก่:

1. **ภัยธรรมชาติ (Natural Threats):** น้ำท่วม พายุ แผ่นดินไหว โรคระบาด ฯลฯ

2. **ภัยจากมนุษย์ (Human-Caused Threats):** แบ่งออกเป็น

   (1) **โดยเจตนา (Malicious):** อาทิ การลักขโมย การก่อวินาศกรรม การโจมตีทางไซเบอร์ การก่อการร้าย

   (2) **โดยไม่เจตนา (Accidental):** อาทิ ความผิดพลาดของพนักงาน (Human Error) หรืออุบัติเหตุจากการทำงาน เป็นต้น (Macrae, 2009)

3. **ภัยทางเทคนิค (Technical Threats):** ไฟฟ้าลัดวงจร ระบบไอทีล่ม อุปกรณ์เสื่อมสภาพ ฯลฯ

กรณีศึกษา: สำหรับโครงการก่อสร้างบนถนนพระราม 2 ภัยคุกคามหลักคือ “อุบัติเหตุจากการก่อสร้าง” (Construction Accidents) ซึ่งสถิติระบุว่ามีอุบัติเหตุกว่า 2,500 ครั้งในช่วงปี 2562-2568 ทำให้มีผู้เสียชีวิตและบาดเจ็บจำนวนมาก 12 คน การระบุภัยคุกคามนี้ต้องพิจารณาทั้งปัจจัยเครื่องจักรล้มเหลวและความประมาทของผู้ปฏิบัติงาน

ภาพที่ 4.6

การระบุภัยคุกคาม (Threat Identification)

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

3.3 การประเมินความเปราะบาง (Vulnerability Assessment)

เมื่อรู้ว่าศัตรูคือใคร ขั้นต่อไปคือการหันกลับมามองตัวเองว่า “เรามีจุดอ่อนตรงไหน?” ความเปราะบางอาจอยู่ในรูปแบบของ:

1. **ทางกายภาพ:** อาทิ รั้วพัง กล้องวงจรปิดเสีย หรือระบบดับเพลิงไม่ทำงาน

2. **ทางเทคนิค:** ตัวอย่างเช่น ซอฟต์แวร์ไม่อัปเดตแพตช์ รหัสผ่านง่ายเกินไป (เช่น 123456) เป็นต้น

3. **ทางกระบวนการ/คน:** ได้แก่ พนักงานขาดการอบรม รปภ. หลับยาม การไม่มีแผนฉุกเฉิน หรือทีมเผชิญเหตุ

ความเปราะบางทางวัฒนธรรม (Cultural Vulnerability) ในสังคมไทย อาทิ วัฒนธรรม “ความเกรงใจ” เป็นดาบสองคม ในแง่หนึ่งคือความสุภาพ แต่ในแง่ความ

ปลอดภัย มันคือจุดอ่อนร้ายแรง เมื่อผู้น้อยไม่กล้าตักเตือนผู้ใหญ่ที่ทำผิดกฎความปลอดภัย หรือลูกน้องไม่กล้ารายงานความผิดพลาดให้หัวหน้าทราบเพราะกลัวจะทำให้ไม่สบายใจ สิ่งนี้ปิดกั้นการไหลเวียนของข้อมูลความเสี่ยงที่สำคัญ (Vellani, 2020)

3.4 การวิเคราะห์ความเสี่ยง (Risk Analysis)

เมื่อรวบรวมข้อมูลครบทั้ง 3 ส่วนแล้ว เราจะนำมาวิเคราะห์เพื่อกำหนด “ระดับความเสี่ยง” (Risk Level) เพื่อใช้ในการจัดลำดับความสำคัญ โดยมี 2 วิธีหลัก คือ การวิเคราะห์เชิงคุณภาพ (Qualitative) และการวิเคราะห์เชิงปริมาณ (Quantitative) โดยจะกล่าวในหัวข้อต่อไป

4. การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Risk Assessment)

การประเมินเชิงคุณภาพเป็นวิธีที่ใช้กันอย่างแพร่หลายที่สุด โดยเฉพาะในการประเมินเบื้องต้น หรือเมื่อข้อมูลสถิติมีไม่เพียงพอ วิธีนี้เน้นการใช้ ดุลยพินิจของผู้เชี่ยวชาญ (Expert Judgment) และประสบการณ์ เพื่อจัดกลุ่มความเสี่ยงออกเป็นระดับต่าง ๆ เช่น สูง กลาง ต่ำ (Jensen, Bird, & Nichols, 2022)

ภาพที่ 4.7

ตัวอย่างตารางเมทริกซ์ประเมินความเสี่ยง (Risk Matrix)

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

4.1 เครื่องมือ: เมทริกซ์ความเสี่ยง (Risk Matrix)

เมทริกซ์ความเสี่ยง (หรือ Heat Map) เป็นเครื่องมือที่ทรงพลังในการแปลงนามธรรมให้เป็นรูปธรรม โดยการนำ “โอกาสเกิด” (Likelihood) มาพล็อตตัดกับ “ผลกระทบ” (Impact) ในตาราง

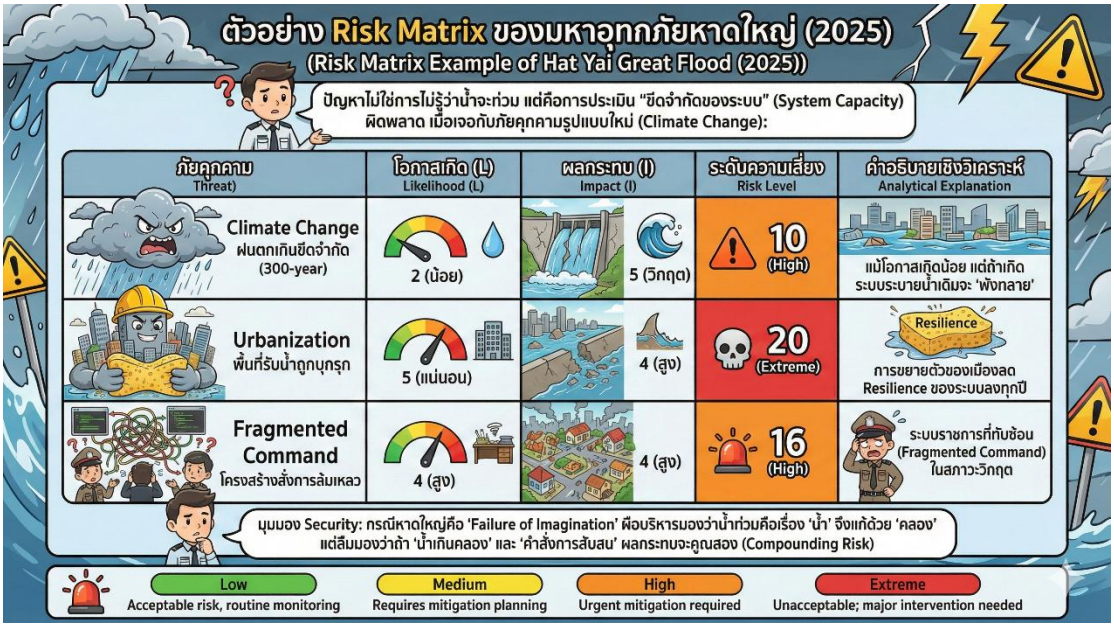
ความหมายของสี:

สีแดง (E): ความเสี่ยงระดับวิกฤต ต้องหยุดการทำงานหรือแก้ไขทันที (Immediate Action)

สีส้ม (H): ความเสี่ยงสูง ต้องมีมาตรการจัดการอย่างเร่งด่วนและผู้บริหารระดับสูงต้องรับทราบ

สีเหลือง (M): ความเสี่ยงปานกลาง ยอมรับได้ชั่วคราวแต่ต้องมีแผนลดความเสี่ยง

สีเขียว (L): ความเสี่ยงต่ำ ยอมรับได้ (Acceptable) เพียงแค่ติดตามเฝ้าระวัง



ภาพที่ 4.8

การระบุภัยคุกคาม (Threat Identification)

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

ตัวอย่างการประเมิน: เหตุการณ์น้ำท่วมหาดใหญ่ (ปี 2568)

โอกาส: หากพิจารณาจากสถิติเดิมอาจมองว่า “ต่ำ” (2) แต่เมื่อคำนึงถึง Climate Change โอกาสจะขยับเป็น “ปานกลาง” (3) หรือ “สูง” (4)

ผลกระทบ: “วิกฤต” (5) เพราะเมืองจมน้ำ เศรษฐกิจเสียหายแสนล้าน

ผลลัพธ์: ตกอยู่ในช่องสีแดง (High/Extreme) ซึ่งแปลว่าระบบป้องกันเดิมที่มีอยู่นั้นไม่เพียงพอ

4.2 เทคนิควิเคราะห์โบว์ไท (Bow-Tie Analysis)

การวิเคราะห์แบบโบว์ไท (Bow Tie Analysis) เป็นเครื่องมือที่ยอดเยี่ยมในการใช้เทคนิคเชิงภาพที่ช่วยให้เห็นภาพรวมของความเสี่ยงได้ชัดเจน โดยเชื่อมโยงสาเหตุ (Threats) เหตุการณ์วิกฤต (Top Event) และผลกระทบ (Consequences) เข้าด้วยกัน ผ่านตัวกั้นหรือมาตรการป้องกัน (Barriers) ต่าง ๆ โดยมี “เหตุการณ์อันตราย” (Hazard Event) อยู่ตรงกลาง (Clamir, 2020)

ด้านซ้าย (สาเหตุ): อะไรทำให้เกิดเหตุการณ์นี้? (เช่น ฝนตกหนัก การระบายน้ำไม่ทัน) → นำไปสู่การสร้าง **มาตรการป้องกัน (Preventive Controls)**

ด้านขวา (ผลกระทบ): เมื่อเกิดเหตุแล้วจะเกิดอะไรขึ้น? (เช่น น้ำท่วมเมือง คนเสียชีวิต) → นำไปสู่การสร้าง **มาตรการบรรเทา (Mitigation/Recovery Controls)** เทคนิคนี้ช่วยให้เราไม่ลืมที่จะเตรียมการทั้ง “ก่อนเกิดเหตุ” และ “หลังเกิดเหตุ”

ภาพที่ 4.9

ตัวอย่างการวิเคราะห์โบว์ไท (Bow-Tie Analysis)

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

การวิเคราะห์ Bow Tie ของ Titanic แสดงให้เห็นทฤษฎี “Swiss Cheese Model” (เนยแข็งสวิส) ได้อย่างชัดเจน คือการที่อุบัติเหตุใหญ่เกิดจากช่องโหว่เล็ก ๆ ในระบบป้องกันหลาย ๆ ชั้นมาเรียงตรงกันพอดี ตั้งแต่การไม่มีกล้องส่องทางไกล การขับเรือเร็ว การออกแบบผนังกั้นน้ำที่บกพร่อง ไปจนถึงการมีเรือบดไม่เพียงพอ เมื่อทุกอย่างมารวมกัน จึงเกิดเป็นโศกนาฏกรรมครั้งประวัติศาสตร์นี้ (Labib & Read, 2013)

4.4 เทคนิคเดลฟาย (Delphi Technique)

เทคนิคเดลฟายเป็นวิธีการพยากรณ์หรือประเมินปัญหาเชิงระบบที่ใช้การรวบรวมความคิดเห็นจากผู้เชี่ยวชาญหลายท่านอย่างเป็นขั้นตอนและไม่เปิดเผยชื่อ เพื่อหาข้อสรุปที่เป็นเอกฉันท์ เทคนิคนี้พัฒนาขึ้นโดยบริษัท RAND Corporation ในช่วงทศวรรษ 1950 สำหรับโครงการวิจัยด้านความมั่นคงของสหรัฐอเมริกา ในยุคสงครามเย็น เมื่อผู้เชี่ยวชาญมีความเห็นไม่ตรงกัน หรือมีผู้อาวุโสที่มีอิทธิพลครอบงำความคิดเห็นในที่ประชุม (ซึ่งพบบ่อยในวัฒนธรรมไทย) เทคนิคนี้จะช่วยได้ โดยการให้ผู้เชี่ยวชาญตอบแบบสอบถามประเมินความเสี่ยงแบบ “นิรนาม” (Anonymous) หลาย ๆ รอบ และสรุปผลกลับไปให้ทุกคนทราบ เพื่อให้ปรับความคิดเห็นเข้าหากันโดยปราศจากแรงกดดันทางสังคม (Markmann, Darkow, & von der Gracht, 2013)

ภาพที่ 4.10

ตัวอย่างการวิเคราะห์เทคนิคเดลฟาย (Delphi Technique)

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

การใช้เทคนิคเดลฟาย ในการวิเคราะห์ความเสี่ยงกรณีศึกษาน้ำท่วมหาดใหญ่ เป็นกระบวนการระดมสมองจากผู้เชี่ยวชาญแบบไม่เผชิญหน้า เพื่อลดอคติจากการคล้อยตามกลุ่ม (Groupthink) และเพื่อให้ได้ฉันทามติ (Consensus) เกี่ยวกับความเสี่ยงที่ซับซ้อนในพื้นที่ จุดเด่นของเดลฟายในกรณีนี้คือการดึง “ความรู้ที่ฝังอยู่ในตัวคน” (Tacit Knowledge) ของคนในพื้นที่หาดใหญ่มาประเมินร่วมกับ “ข้อมูลทางวิศวกรรม” (Explicit Knowledge) ทำให้ผลการวิเคราะห์มีความแม่นยำและเป็นไปได้จริงสูงกว่าการใช้ข้อมูลสถิติเพียงอย่างเดียว

5. การประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment)

เมื่อการประเมินเชิงคุณภาพบอกเพียงแค่ “สูง/ต่ำ” อาจไม่เพียงพอสำหรับการอนุมัติงบประมาณหลักล้าน ผู้บริหารมักมีคำถามว่า “ความเสี่ยงนี้จะทำให้เราเสียเงินกี่บาท?” การประเมินเชิงปริมาณจึงเข้ามาตอบโจทย์นี้โดยใช้คณิตศาสตร์และสถิติ

5.1 การคำนวณความสูญเสียที่คาดว่าจะเกิดขึ้นต่อปี (ALE)

ALE (Annualized Loss Expectancy) คือ ตัวชี้วัดทางการเงินที่ใช้ในการประเมินความเสี่ยง โดยประมาณการมูลค่าความเสียหายทางเศรษฐกิจที่คาดว่าจะเกิดขึ้นจากภัยคุกคามต่อสินทรัพย์หนึ่ง ๆ ภายในระยะเวลา 1 ปี

สูตรการคำณวน:

$$\mathbf{ALE = SLE \times ARO}$$

โดยที่:

SLE (Single Loss Expectancy) = มูลค่าความสูญเสีย 1 ครั้ง หากเกิดเหตุ โดยคำนวณจาก **มูลค่าของสินทรัพย์ (Asset Value) × ร้อยละความสูญเสีย (Exposure Factor)**

ARO (Annualized Rate of Occurrence) = อัตราความถี่ที่คาดว่าจะเกิดเหตุใน 1 ปี

จุดประสงค์หลักของ ALE คือ การช่วยองค์กรจัดลำดับความสำคัญของความเสี่ยง และตัดสินใจได้ว่าควรลงทุนในการป้องกัน (เช่น ระบบสำรองข้อมูล) มากน้อยเพียงใด โดยเปรียบเทียบกับค่าใช้จ่ายที่คาดว่าจะสูญเสียหากไม่ป้องกัน (Babenko et al., 2025)

ภาพที่ 4.11
กรณีศึกษาการคำนวณความเสี่ยง Ransomware
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

จากภาพที่ 4.11 บริษัทมีความเสี่ยงที่จะสูญเสียเงินเฉลี่ยปีละ 1.2 ล้านบาทจาก Ransomware ตัวเลขนี้จะเป็นฐานในการตั้งงบประมาณรักษาความปลอดภัย หากฝ่ายไอทีของบซื้อ Firewall ราคา 5 แสนบาท ผู้บริหารจะเห็นทันทีว่าคุ้มค่า เพราะถูกกว่าความเสียหายคาดการณ์ (1.2 ล้านบาท)

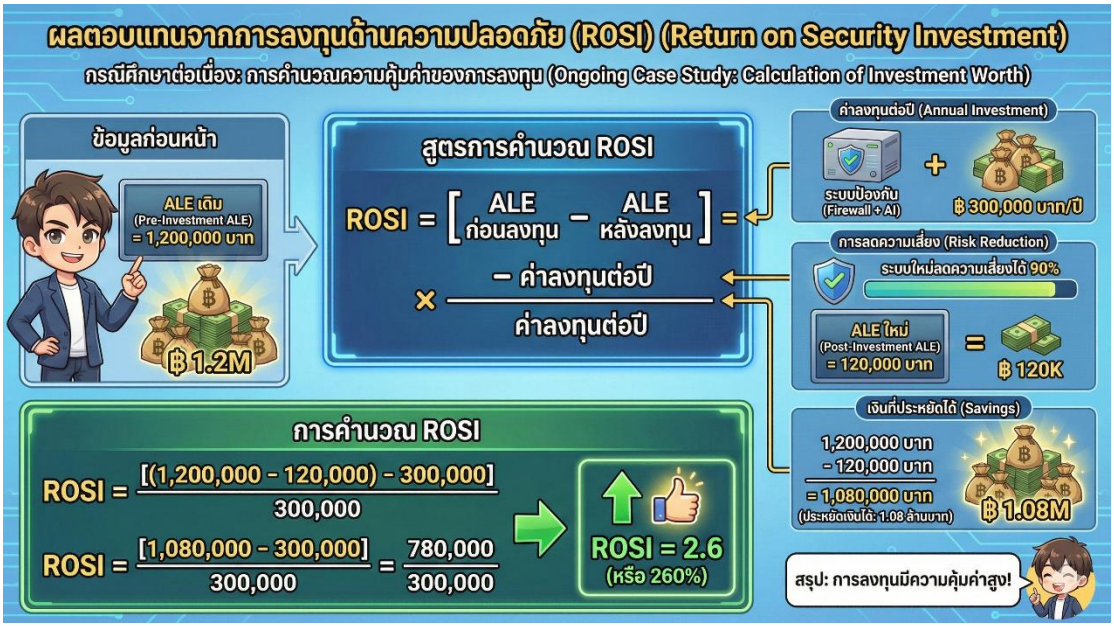
5.2 ผลตอบแทนจากการลงทุนด้านความปลอดภัย (ROSI)

ในโลกธุรกิจ ทุกการลงทุนต้องวัดผลตอบแทนได้ แม้แต่ความปลอดภัย ทั้งนี้ ROSI (Return on Security Investment) คือ ตัวชี้วัดทางการเงินที่ใช้ประเมินประสิทธิผลของการลงทุนในมาตรการหรือโซลูชันด้านความปลอดภัย โดยการเปรียบเทียบ ผลประโยชน์ทางเศรษฐกิจจากมาตรการลดความเสี่ยง กับ ต้นทุนของการลงทุน นั้น

สูตรการคำนวณ ROSI:

$$\text{ROSI} = \frac{(\text{ALE ก่อนลงทุน} - \text{ALE หลังลงทุน}) - \text{ต้นทุนการป้องกัน}}{\text{ต้นทุนการป้องกัน}} \text{ X } 100\%$$

โดย ALE (Annualized Loss Expectancy) คือความสูญเสียที่คาดว่าจะเกิดขึ้นต่อปีที่อธิบายไว้ก่อนหน้านี้ (Babenko et al., 2025)



ภาพที่ 4.12

ผลตอบแทนจากการลงทุนด้านความปลอดภัย (ROSI)

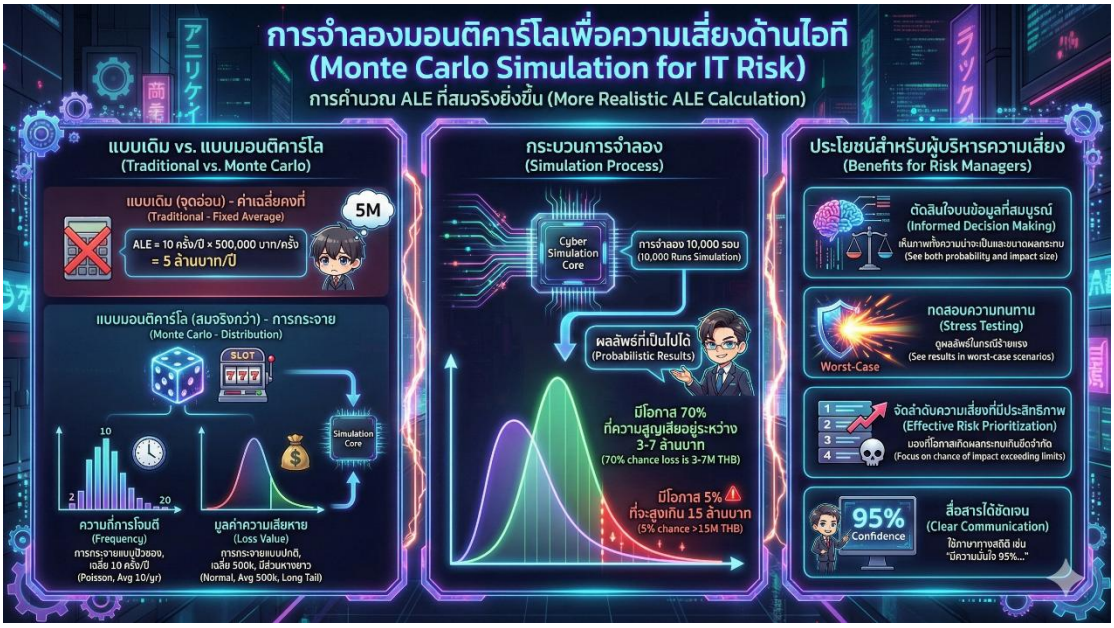
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

จากภาพที่ 4.12 การลงทุนนี้ให้ผลตอบแทน 260% ซึ่งสูงมากในทางธุรกิจ ทำให้ผู้บริหารสามารถอนุมัติได้อย่างมั่นใจ ทั้งนี้ จุดสำคัญของ ROSI คือ การเปลี่ยน “ค่าใช้จ่าย” ด้านความปลอดภัยให้เป็น “การลงทุน” ที่วัดผลได้ในเชิงธุรกิจ โดยช่วยสนับสนุนการตัดสินใจและสื่อสารกับฝ่ายบริหารได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ข้อจำกัดหลักอยู่ที่การพึ่งพาข้อมูลประมาณการ (เช่น ALE) ที่อาจไม่แม่นยำ และมักไม่สามารถวัดมูลค่าของผลประโยชน์เชิงคุณภาพ เช่น ชื่อเสียงหรือความไว้วางใจของลูกค้าได้ครบถ้วน (Babenko et al., 2025)

5.3 การจำลองสถานการณ์แบบมอนติคาร์โล (Monte Carlo Simulation)

ในทางปฏิบัติ การวิเคราะห์ความเสี่ยงด้วยค่าคงที่แบบตายตัว (เช่น การประเมินว่าความเสียหายจะอยู่ที่ 60% เสมอ) มักให้ภาพที่เรียบง่ายเกินไปและไม่สะท้อนความไม่แน่นอนที่แท้จริง Monte Carlo Simulation แก้ไขจุดอ่อนนี้ด้วยการกำหนดให้ปัจจัยเสี่ยงสำคัญ (เช่น ความถี่ของเหตุการณ์และขนาดความเสียหาย) มี “การกระจายตัว” ของค่าที่เป็นไปได้ แทนที่จะเป็นค่าเดียว จากนั้นคอมพิวเตอร์จะทำการสุ่มค่าจากการกระจายตัวเหล่านั้น และคำนวณผลลัพธ์ซ้ำหลายหมื่นถึงหลายแสนครั้ง กระบวนการนี้สร้างชุดข้อมูลผลลัพธ์ขนาดใหญ่ที่ครอบคลุมสถานการณ์ที่เป็นไปได้อย่างกว้างขวาง (Vellani, 2020)

ผลลัพธ์ที่ได้จะถูกนำมาจัดเรียงและแสดงในรูปแบบของ “การกระจายตัวของความน่าจะเป็น” ซึ่งมักเห็นเป็นกราฟรูประฆังคว่ำ (Bell Curve) หรือรูปแบบอื่น กราฟนี้ทำให้เราสามารถเห็นภาพความน่าจะเป็นของผลลัพธ์ทุกระดับ ตั้งแต่กรณีที่ดีที่สุด (Best Case) ไปจนถึงกรณีที่เลวร้ายที่สุด (Worst Case) และที่พบได้บ่อยที่สุด (Most Likely Case) วิธีการนี้ให้ข้อมูลเชิงลึกที่เหนือกว่าการพึ่งพา “ค่าเฉลี่ย” เพียงค่าเดียว เพราะช่วยตอบคำถามเชิงกลยุทธ์ได้ เช่น “ความเสี่ยงที่ความสูญเสียจะเกินขีดจำกัดที่บริษัทยอมรับได้มีสูงแค่ไหน” ทำให้การตัดสินใจในการลงทุนป้องกันหรือโอนถ่ายความเสี่ยงมีความแม่นยำและมีหลักฐานสนับสนุนที่แข็งแกร่งขึ้น (Vellani, 2020)



ภาพที่ 4.13

ผลตอบแทนจากการลงทุนด้านความปลอดภัย (ROSI)

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

6. กลยุทธ์การจัดการความเสี่ยง (Risk Treatment Strategies)

เมื่อเราทราบระดับความเสี่ยงแล้ว ขั้นตอนต่อไปคือการ “จัดการ” (Treat) องค์กรมีทางเลือกหลัก 4 ทาง ซึ่งมักเรียกกันว่า 4Ts (Terminate, Treat, Transfer, Tolerate) หรือ 4As (Avoid, Reduce, Transfer, Accept) (Peddada, 2013)

6.1 การหลีกเลี่ยง (Avoid / Terminate)

คือการตัดสินใจหยุดหรือยกเลิกกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้นไปเลย วิธีนี้ทำให้ความเสี่ยงกลายเป็นศูนย์ แต่ก็ทำให้โอกาสทางธุรกิจ (Opportunity) หายไปเป็นศูนย์ด้วย

ตัวอย่าง: บริษัทตัดสินใจไม่ใช้ระบบปฏิบัติการ Windows XP ที่หมดอายุการสนับสนุนแล้ว เพื่อตัดความเสี่ยงจากช่องโหว่ที่ไม่มีการแก้ไข

กรณีศึกษา: โครงการหมู่บ้านจัดสรรตัดสินใจ ยกเลิก การถมดินสร้างบ้านในพื้นที่รับน้ำ (Floodway) ของจังหวัดปทุมธานี เพื่อหลีกเลี่ยงปัญหาน้ำท่วมแบบถาวร แม้จะเสียโอกาสในการขาย แต่คุ้มค่ากว่าการถูกฟ้องร้องในอนาคต

6.2 การลดความเสี่ยง (Reduce / Treat)

เป็นวิธีที่นิยมใช้มากที่สุด คือการยอมรับที่จะทำกิจกรรมต่อ แต่หามาตรการมาลดโอกาส (Likelihood) หรือลด ผลกระทบ (Impact) ให้น้อยลง (Peddada, 2013)

ลดโอกาส: การติดตั้งระบบสแกนใบหน้า (Biometrics) ในแอปธนาคาร เพื่อลดโอกาสที่แก๊งคอลเซ็นเตอร์จะดูดเงินออกไปได้ง่าย ๆ

ลดผลกระทบ: การติดตั้งระบบสปริงเกอร์ดับเพลิง ไม่ได้ช่วยกันไฟไหม้ (โอกาสเท่าเดิม) แต่ถ้าไหม้แล้ว ไฟจะดับเร็วขึ้น ความเสียหายลดลง

กรณีศึกษา: จากอุบัติเหตุซ้ำซากบนถนนพระราม 2 กรมทางหลวงได้ออกมาตรการ “Double Safety” เช่น การติดตั้งคานเหล็กกันสิ่งของร่วงหล่น (Overhead Protection) และการจำกัดเวลาทำงานเฉพาะช่วงกลางคืน เพื่อลดโอกาสและผลกระทบของอุบัติเหตุต่อผู้ใช้รถใช้ถนน

6.3 การโอนย้ายความเสี่ยง (Transfer / Share)

คือการผลักภาระ “ผลกระทบทางการเงิน” ไปให้ผู้อื่นรับผิดชอบแทน โดยการจ่ายค่าธรรมเนียมหรือเบี้ยประกัน (Peddada, 2013)

การประกันภัย (Insurance): การทำประกันภัยไซเบอร์ (Cyber Insurance) หรือประกันอัคคีภัย หากเกิดเหตุ บริษัทประกันจะจ่ายค่าเสียหายแทนเรา

การจ้างบุคคลภายนอก (Outsourcing): การจ้างบริษัทรักษาความปลอดภัย (รปภ.) หรือจ้างบริษัทขนส่งเงิน หากเงินหายระหว่างขนส่ง บริษัทคู่สัญญาต้องรับผิดชอบ

ข้อควรระวัง: เราโอนได้แค่ “ตัวเงิน” แต่ไม่สามารถโอน “ความรับผิดชอบทางกฎหมาย” หรือ “ชื่อเสียง” ได้ หากข้อมูลลูกค้ารั่วไหล แม้ประกันจะจ่ายค่าปรับให้ แต่ลูกค้าก็ยังสูญเสียความเชื่อมั่นในแบรนด์ของเราอยู่ดี และกรรมการบริษัทยังอาจต้องรับโทษทางกฎหมาย (National Cyber Security Agency, 2025)

6.4 การยอมรับความเสี่ยง (Accept / Tolerate)

คือการตัดสินใจอย่างมีสติ (Conscious Decision) ที่จะไม่ทำอะไรเพิ่มเติม เพราะประเมินแล้วว่าความเสี่ยงนั้นอยู่ในระดับที่องค์กรรับได้ (Within Risk Appetite) หรือค่าใช้จ่ายในการป้องกันสูงกว่ามูลค่าความเสียหาย (Peddada, 2013)

ตัวอย่าง: ร้านสะดวกซื้อยอมรับความเสี่ยงที่สินค้าเล็ก ๆ น้อย ๆ (เช่น ปากกา ลูกอม) อาจถูกขโมย (Shrinkage) โดยไม่จ้าง รปภ. มายืนเฝ้าทุกจุด เพราะค่าจ้าง รปภ. แพงกว่าค่าของที่หาย

การยอมรับแบบเชิงรุก (Active Acceptance): เตรียมเงินสำรองไว้จ่ายค่าเสียหาย (Self-insurance)

การยอมรับแบบเชิงรับ (Passive Acceptance): ไม่ทำอะไรเลย (ซึ่งมักเกิดจากความไม่รู้ หรือ Ignorance เหมือนกรณีกัปตันเรือ Titanic)

7. ความปลอดภัยภายใต้กรอบการบริหารความเสี่ยงองค์กร (Security within Enterprise Risk Management - ERM)

ความปลอดภัยในยุคปัจจุบันไม่ใช่หน้าที่ของฝ่าย รปภ. หรือฝ่ายไอทีเท่านั้น แต่เป็นวาระระดับชาติและระดับองค์กร การบริหารความเสี่ยงด้านความปลอดภัยจึงต้องถูกบูรณาการเข้ากับ **Enterprise Risk Management (ERM)** หรือการบริหารความเสี่ยงทั่วทั้งองค์กร (Vellani, 2020)

7.1 กรอบแนวคิด COSO ERM 2017

กรอบการทำงานมาตรฐานโลกที่ตลาดหลักทรัพย์แห่งประเทศไทย (SET) ส่งเสริมให้บริษัทจดทะเบียนนำมาใช้คือ COSO ERM 2017 ซึ่งเชื่อมโยงความเสี่ยงเข้ากับกลยุทธ์และผลการดำเนินงาน (Committee of Sponsoring Organizations of the Treadway Commission, 2017) ประกอบด้วย 5 องค์ประกอบสำคัญ:

1. การกำกับดูแลและวัฒนธรรม (Governance & Culture): บอร์ดบริหารต้องเป็นผู้นำในการกำหนดนโยบายและสร้าง “วัฒนธรรมความเสี่ยง” (Risk Culture) ที่พนักงานกล้าพูดความจริง (ก้าวข้ามความเกรงใจ) และยึดมั่นในจริยธรรม

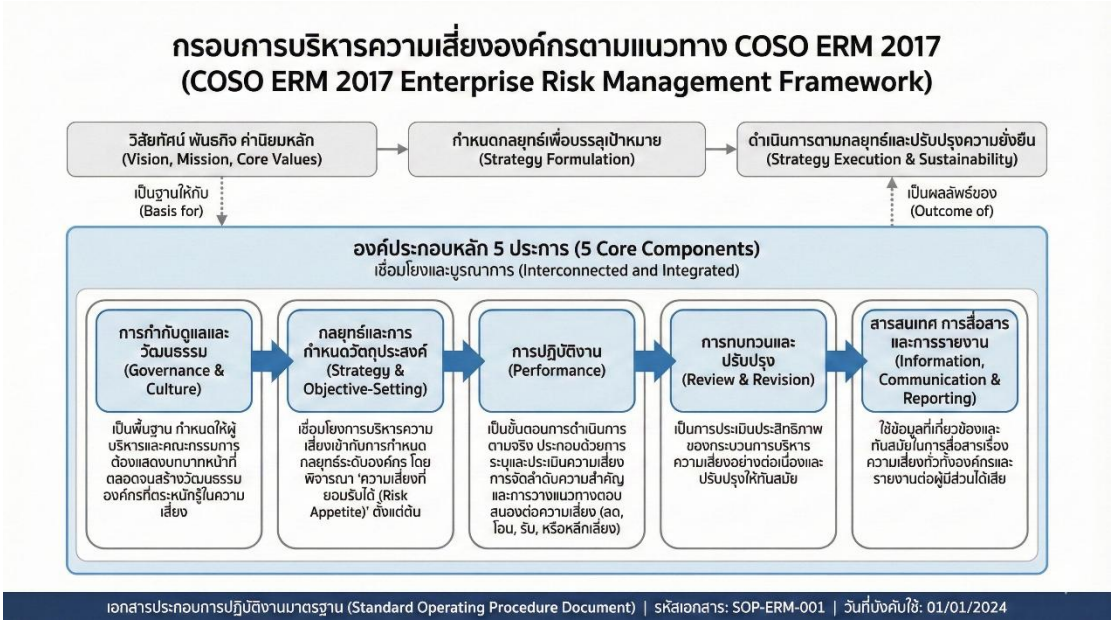
2. กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy & Objective-Setting): การกำหนด Risk Appetite หรือ “ความอยากเสี่ยง” ต้องสอดคล้องกับกลยุทธ์ ตัวอย่างเช่น ธนาคารที่มุ่งสู่ Digital Banking ต้องกำหนด Risk Appetite ด้านไซเบอร์ไว้ต่ำมาก

(ยอมรับความผิดพลาดไม่ได้) แต่ยอมรับความเสี่ยงด้านการลงทุนเทคโนโลยีใหม่ ๆ ได้สูง (National Cyber Security Agency, 2025)

3. ผลการดำเนินงาน (Performance): การระบุ (Identify) ประเมิน (Assess) และจัดลำดับความสำคัญ (Prioritize) ของความเสี่ยงอย่างเป็นระบบ เพื่อให้มั่นใจว่าทรัพยากรถูกใช้ไปอย่างคุ้มค่า

4. การทบทวนและปรับปรุง (Review & Revision): โลกเปลี่ยน ความเสี่ยงก็เปลี่ยน องค์กรต้องทบทวนเสมอว่ามาตรการที่วางไว้นั้นยังใช้ได้ผลหรือไม่ เช่น แผนรับมือน้ำท่วมของหาดใหญ่ที่เคยใช้ได้ผลในอดีต ต้องถูกทบทวนใหม่เมื่อเจอกับ Climate Change

5. สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication, & Reporting): ข้อมูลความเสี่ยงต้องถูกส่งต่ออย่างรวดเร็วและทั่วถึง (ไม่เหมือนกรณี Titanic ที่ข้อมูลน้ำแข็งไปไม่ถึงกัปตัน) ระบบไอทีต้องสนับสนุนการรายงานที่โปร่งใส



ภาพที่ 4.14

กรอบการบริหารความเสี่ยงองค์กรตาม COSO ERM 2017

ที่มา: สร้างโดย Google Gemini (AI-generated) อ้างอิงแนวคิด COSO (2017)

7.2 ISO 31000:2018 มาตรฐานที่มีความยืดหยุ่น

นอกจาก COSO แล้ว มาตรฐาน ISO 31000 ก็เป็นที่นิยมในไทย โดยเป็นมาตรฐานสากลว่าด้วยหลักการและแนวทางการบริหารความเสี่ยงที่สามารถประยุกต์ใช้ได้กับทุกองค์กรและกิจกรรม มาตรฐานนี้ประกอบด้วย**หลักการ (Principles) โครงสร้าง**

กรอบงาน (Framework) และ**กระบวนการ (Process)** ที่เป็นวงจรสำหรับการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง เป้าหมายหลักคือเพิ่มโอกาสในการบรรลุวัตถุประสงค์ และทำให้การตัดสินใจในทุกระดับขององค์กรมีความชัดเจนและแข็งแกร่งขึ้น โดยพิจารณาความไม่แน่นอนต่าง ๆ และเน้นหลักการ “สร้างและปกป้องมูลค่า” (Value Creation and Protection) (International Organization for Standardization, 2018) ซึ่งยืดหยุ่นและปรับใช้ได้กับทุกประเภทองค์กร ตั้งแต่ SMEs ไปจนถึงรัฐวิสาหกิจขนาดใหญ่ เช่น การท่าอากาศยานแห่งประเทศไทย (AOT) ที่นำมาตรฐานนี้มาใช้บริหารความเสี่ยงในสนามบิน

ภาพที่ 4.15

กรอบการประเมินความเสี่ยงในบริบทไทย (Risk Assessment in the Thai Context)

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

8. การตัดสินใจด้านความปลอดภัยและความรับผิดชอบ (Security Decision-Making and Accountability)

การบริหารความเสี่ยงไม่ใช่แค่เรื่องของตัวเลข แต่เป็นเรื่องของ “จริยธรรม” และ “ความรับผิดชอบ” ของผู้นำ

8.1 อคติในการตัดสินใจ (Cognitive Biases)

มนุษย์มักมีอคติที่ทำให้การตัดสินใจผิดพลาด (Macrae, 2009):

- **Normalization of Deviance:** การทำผิดเล็ก ๆ น้อย ๆ จนชินชาและคิดว่าไม่เป็นไร เช่น คนงานก่อสร้างบนถนนพระราม 2 ไม่สวมหมวกนิรภัย หรือผู้รับเหมาลัดขั้นตอนความปลอดภัยจนเป็นเรื่องปกติ จนกระทั่งเกิดอุบัติเหตุคานถล่ม
- **Optimism Bias:** การมองโลกในแง่ดีเกินไป คิดว่า “ภัยพิบัติคงไม่เกิดกับเรา” หรือ “น้ำคงไม่ท่วมสูงขนาดนั้น” ซึ่งเป็นกับดักความคิดที่ทำให้การเตรียมการรับมือหาดใหญ่ 2568 ล้มเหลว (Thailand Development Research Institute, 2025)

8.2 ความรับผิดชอบทางกฎหมาย (Legal Liability)

ในประเทศไทย กฎหมายกำหนดความรับผิดชอบของผู้บริหารไว้อย่างชัดเจน

- **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA):** หากข้อมูลรั่วไหลเพราะขาดมาตรการประเมินความเสี่ยงที่เหมาะสม บริษัทอาจถูกปรับทางปกครองสูงสุด 5 ล้านบาท และผู้บริหารอาจมีโทษทางอาญา
- **ความรับผิดของกรรมการ (Directors’ Liability):** ตามประมวลกฎหมายแพ่งและพาณิชย์และ พ.ร.บ. หลักทรัพย์ฯ กรรมการบริษัทมีหน้าที่ต้องปฏิบัติงานด้วยความระมัดระวัง (Duty of Care) หากละเลยการบริหารความเสี่ยงจนบริษัทเสียหาย กรรมการต้องรับผิดชดใช้ค่าเสียหายส่วนตัว

ภาพที่ 4.16
การบูรณาการประเมินความเสี่ยงสู่กลยุทธ์องค์กร (Integration Risk Assessment)
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

9. บทสรุป (Conclusion)

โศกนาฏกรรมของเรือ Titanic ไม่ได้เกิดขึ้นเพราะภูเขาน้ำแข็งเพียงอย่างเดียว หากแต่มีรากเหง้ามาจาก “ความเชื่อว่าเรือลำนี้ไม่มีวันจม” (Practically unsinkable) ความมั่นใจเกินขอบเขตดังกล่าวทำให้ผู้บริหารและลูกเรือมองข้ามหลักการบริหารความเสี่ยงขั้นพื้นฐาน ตั้งแต่การประเมินสถานการณ์อย่างรอบคอบ ไปจนถึงการเตรียมความพร้อมรับมือเหตุฉุกเฉิน บทเรียนนี้มิได้เป็นเพียงเรื่องราวในประวัติศาสตร์ หากแต่ยังคงสะท้อนความจริงที่ทรงพลังต่อการจัดการความมั่นคงปลอดภัยในศตวรรษที่ 21

ในโลกปัจจุบัน ภูเขาน้ำแข็งได้แปรเปลี่ยนรูปจากกายภาพไปสู่ดิจิทัล องค์กรจำนวนไม่น้อยยังคงยึดติดกับความเชื่อว่า “เราไม่น่าจะตกเป็นเป้าหมาย” หรือ “ระบบของเราปลอดภัยเพียงพอแล้ว” จนกระทั่งต้องเผชิญกับการรั่วไหลของข้อมูลจำนวนมหาศาลหรือการโจมตีด้วยมัลแวร์เรียกค่าไถ่ สถิติอาชญากรรมไซเบอร์ของประเทศไทยที่เพิ่มขึ้นอย่างก้าวกระโดดในช่วงไม่กี่ปีที่ผ่านมา สะท้อนอย่างชัดเจนว่า ภัยคุกคามในยุคดิจิทัลมิได้ลดน้อยลง หากแต่มีจำนวนมากขึ้น ซับซ้อนขึ้น และคาดการณ์ได้ยากยิ่งกว่าเดิม

บทเรียนจาก Titanic ชี้ให้เห็นว่า ความหายนะมักเกิดจากการบรรจบกันของสามปัจจัยสำคัญ ประการแรก คือ ความเชื่อที่ผิดพลาดและไม่ผ่านการตรวจสอบอย่างเป็นระบบ ประการที่สอง คือ การเพิกเฉยต่อสัญญาณเตือน แม้จะมีข้อมูลหรือคำแนะนำจากผู้เชี่ยวชาญอย่างชัดเจน และประการสุดท้าย คือ การเตรียมความพร้อมที่ไม่เพียงพอ ทั้งในด้านทรัพยากร แผนฉุกเฉิน และการฝึกซ้อม เมื่อทั้งสามปัจจัยนี้เกิดขึ้นพร้อมกัน องค์กรย่อมตกอยู่ในภาวะเปราะบางอย่างยิ่ง ไม่ต่างจากเรือที่แล่นด้วยความเร็วสูงเข้าสู่เขตอันตรายโดยไร้แผนสำรอง

อย่างไรก็ตาม โศกนาฏกรรมของ Titanic มิได้สูญเปล่า เพราะมันนำไปสู่การปฏิรูปมาตรฐานความปลอดภัยทางทะเลในระดับสากล International Convention for the Safety of Life at Sea (SOLAS) ในปี 1914 บังคับให้เรือทุกลำต้องมีเรือชูชีพเพียงพอ มีระบบวิทยุทำงาน 24 ชั่วโมง และมีมาตรฐานความปลอดภัยที่เข้มงวด ในทำนองเดียวกัน วิกฤตด้านความมั่นคงปลอดภัยในปัจจุบันได้ตอกย้ำว่า การบริหารความเสี่ยงไม่ใช่ภาระหรือค่าใช้จ่ายที่สิ้นเปลือง แต่คือการลงทุนเชิงกลยุทธ์ องค์กรไม่จำเป็นต้องป้องกันทุกภัยคุกคาม หากแต่ต้องประเมินความเสี่ยงอย่างเป็นระบบ ตัดสินใจบนพื้นฐานข้อมูล สร้างวัฒนธรรมที่เปิดรับการตั้งคำถาม และเตรียมแผนรับมือที่สามารถใช้งานได้จริงยามเกิดเหตุไม่คาดฝัน

ท้ายที่สุด ภารกิจของผู้นำด้านความมั่นคงปลอดภัยในโลกยุคใหม่ มิใช่การสร้าง “เรือที่ไม่มีวันจม” เพราะระบบเช่นนั้นไม่มีอยู่จริง หากแต่คือการทำหน้าที่เป็นกัปตันที่มี

วิสัยทัศน์ รับฟังสัญญาณเตือน และเตรียมพร้อมอยู่เสมอ เพื่อให้เมื่อภูเขาน้ำแข็งปรากฏขึ้น องค์กรของท่านจะหลบหลีกได้ทัน หรือถึงแม้จะโดนกระทบ ก็มีระบบรองรับที่พร้อมช่วยให้ทุกคนรอดปลอดภัย นี่คือความหมายที่แท้จริงของการบริหารความเสี่ยง ไม่ใช่การหลีกเลี่ยงความเสี่ยงทั้งหมด แต่คือการเปลี่ยนภัยคุกคามที่ไม่แน่นอนให้เป็นความเสี่ยงที่จัดการได้ และพร้อมรับมือเมื่อเหตุไม่คาดฝันเกิดขึ้น

10. คำถามทบทวน (Review Questions)

1. จงวิเคราะห์ความล้มเหลวของเรือ *Titanic* โดยใช้องค์ประกอบความเสี่ยง (Asset, Threat, Vulnerability) และอธิบายว่าหากท่านเป็นกัปตัน ท่านจะใช้กลยุทธ์ 4Ts อย่างไรในคืนนั้น?

2. จากกรณีศึกษา “น้ำท่วมหาดใหญ่ 2568” จงอธิบายว่าเหตุใดการพึ่งพาข้อมูลสถิติในอดีต (Historical Data) เพียงอย่างเดียวจึงไม่เพียงพอสำหรับการประเมินความเสี่ยงในยุค Climate Change?

3. สมมติท่านเป็น CISO ของธนาคารแห่งหนึ่ง จงคำนวณหาค่า ALE และ ROSI ของการลงทุนระบบยืนยันตัวตน (MFA) มูลค่า 2 ล้านบาท/ปี หากทราบว่าระบบนี้สามารถป้องกันการโจรกรรมเงินที่มีมูลค่าความเสียหาย 50 ล้านบาท ซึ่งมีโอกาสเกิดขึ้น 1 ครั้งในทุก 10 ปี ได้อย่างสมบูรณ์?

4. จากกรณีศึกษาการโจมตีด้วย Ransomware ในภาพที่ 4.11 (ALE = 1.2 ล้านบาท/ปี) ถ้าบริษัทพิจารณาลงทุนในระบบตรวจสอบและตอบสนองเหตุการณ์ (SIEM) ที่มีต้นทุนการดำเนินงาน 400,000 บาทต่อปี และคาดว่าจะสามารถลดโอกาสเกิดเหตุลงได้ 70% โดยไม่เปลี่ยนผลกระทบทางการเงินต่อเหตุการณ์เดียว จงคำนวณหาค่า ALE ใหม่หลังลงทุน และค่าผลตอบแทนจากการลงทุนด้านความปลอดภัย (ROSI) ของระบบ SIEM นี้?

5. วัฒนธรรม “ความเกรงใจ” ในบริบทไทย สร้างความท้าทายในการบริหารความเสี่ยงอย่างไร จงยกตัวอย่างผลกระทบเชิงลบที่ชัดเจน 1 ตัวอย่าง พร้อมเสนอแนวทาง 1 ข้อในการปรับเปลี่ยนวัฒนธรรมนี้ให้ส่งเสริมการสื่อสารความเสี่ยงอย่างมีประสิทธิภาพ?

11. เอกสารอ้างอิง (References)

Babenko, T., Kolesnikova, K., Panchenko, M., Abramkina, O., Kiktev, N., Meish, Y., & Mazurchuk, P. (2025). Risk assessment of cryptojacking attacks on

endpoint systems: Threats to sustainable digital agriculture. *Sustainability, 17*(12), 5426. https://doi.org/10.3390/su17125426

Battles, J. B. (2001). Disaster prevention: Lessons learned from the Titanic. *Baylor University Medical Center Proceedings, 14*(2), 150–153.

Bigg, G., & Billings, S. (2014). The iceberg risk in the *Titanic* year of 1912: Was it exceptional? *Significance, 11*(3), 6–10. https://doi.org/10.1111/j.1740-9713.2014.00746.x

Chuthapiphat, B. (2025, July 17). Thai servers breached, caused 16.57% higher cyber incidents. *The Nation Thailand*. https://www.nationthailand.com/business/tech/40052717

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO.

Elamir, H. (2020). The bowtie diagrams: Better understanding, wider spectrum, and easier communication. *Journal of Emergency Medicine, Trauma & Acute Care, 2020* (Qatar Health 2020 Conference), Article 16. https://doi.org/10.5339/jemtac.2020.qhc.16

International Organization for Standardization. (2018). *ISO 31000:2018 – Risk management – Guidelines*. Author. https://www.iso.org/standard/65694.html

Jensen, R. C., Bird, R. L., & Nichols, B. W. (2022). Risk assessment matrices for workplace hazards: Design for usability. *International Journal of Environmental Research and Public Health, 19*(5), 2763. https://doi.org/10.3390/ijerph19052763

Labib, A., & Read, M. (2013). Not just rearranging the deckchairs on the Titanic: Learning from failures through risk and reliability analysis. *Safety Science, 51*(1), 397–413. https://doi.org/10.1016/j.ssci.2012.08.014

Macrae, C. (2009). Human factors at sea: Common patterns of error in groundings and collisions. *Maritime Policy & Management, 36*(1), 21–38. https://doi.org/10.1080/03088830802652262

Markmann, C., Darkow, I.-L., & von der Gracht, H. A. (2013). A Delphi-based risk analysis: Identifying and assessing future challenges for supply chain

security in a multi-stakeholder environment. *Technological Forecasting and Social Change, 80*(9), 1815–1833. https://doi.org/10.1016/j.techfore.2012.10.019

Peddada, K. (2013, April 18–19). *Risk assessment and control*. In *Governance & control in finance & banking: A new paradigm for risk & performance* (pp. 51–59). International conference held in Paris, France.

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

Thailand Development Research Institute. (2025, December 24). *The anatomy of preventable ruin: How the Hat Yai floods were manufactured when the rain weren't falling*. https://tdri.or.th/en/2025/12/the-anatomy-of-preventable-ruin-how-the-hat-yai-floods-were-manufactured-when-the-rain-werent-falling

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