Unit 3

การประเมินภัยคุกคาม

บทที่ 3

การประเมินภัยคุกคาม

บทนำ

จากขั้นตอนการระบุสินทรัพย์และมาตรการการรักษาความมั่นคงนั้น ขั้นตอนต่อมาคือการประเมินภัยคุกคาม โดยทั่วไป ภัยคุกคาม (threat) คือสิ่งใดก็ตามที่สามารถใช้ประโยชน์จากจุดอ่อนทั้งโดยตั้งใจหรือโดยบังเอิญ ทำให้ได้มา สร้างความเสียหาย หรือทำลายสินทรัพย์ โดยที่ภัยคุกคามสามรถแบ่งออกเป็น 2 ประเภทคือ โดยมนุษย์หรือโดยธรรมชาติ อีกทั้ง ภัยคุกคามยังหมายถึงเจตนาแรงจูงใจ และความสามารถในการโจมตีทรัพย์สินของฝ่ายตรงข้ามอีกด้วย การประเมินภัยคุกคาม (threat assessment) คือการประเมินการกระทำของมนุษย์หรือเหตุการณ์ทางธรรมชาติที่อาจส่งผลเสียต่อการดำเนินธุรกิจและทรัพย์สิน ทั้งนี้ ข้อมูลในอดีตเป็นแหล่งข้อมูลหลักสำหรับการประเมินภัยคุกคาม รวมถึงเหตุการณ์อาชญากรรมและการก่อการร้ายในอดีตด้วย โดยการนำมาวิเคราะห์ร่วมกับข้อมูลปัจจุบัน (real time) อย่างไรก็ดี การประเมินภัยคุกคามอาจเป็นเชิงปริมาณหรือเชิงคุณภาพ การวิเคราะห์อาชญากรรมเป็นตัวอย่างเชิงปริมาณของการประเมินภัยคุกคาม ในขณะที่การวิเคราะห์ภัยคุกคามจากการก่อการร้ายมักจะเป็นเชิงคุณภาพ ความแตกต่างที่สำคัญคือ ภัยคุกคามคือการกระทำหรือสภาวการณ์ที่อาจเป็นอันตรายต่อทรัพย์สินขององค์กร ในขณะที่ฝ่ายตรงข้ามคือบุคคล กลุ่ม และองค์กรที่เป็นภัยต่อทรัพย์สิน ฝ่ายตรงข้ามยังมีลักษณะเฉพาะจากประวัติการโจมตีต่อทรัพย์สิน ความตั้งใจที่จะโจมตี และความสามารถและแรงจูงใจในการโจมตีในอนาคต

ความสำคัญของการประเมินภัยคุกคาม

การประเมินภัยคุกคาม คือ การประเมินความเป็นไปได้ของเหตุการณ์ไม่พึงประสงค์ เช่น การก่อการร้ายและอาชญากรรมต่อทรัพย์สินและอันตรายอื่น ๆ เช่น ภัยพิบัติทางธรรมชาติ ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ ด้วยเหตุนี้ จุดโฟกัสของการประเมินภัยคุกคามจึงอยู่ที่สินทรัพย์ (เป้าหมาย) และภัยคุกคามที่พยายามมุ่งร้ายต่อเป้าหมายเหล่านั้น การประเมินภัยคุกคามจะมุ่งเน้นไปที่คำถามสำคัญ คือ ใครคือผู้ประสงค์ร้าย? พร้อมด้วยการประเมินภัยคุกคามตามความสามารถ เจตนา และผลกระทบของการโจมตี ทั้งนี้ การประเมินภัยคุกคามโดยทั่วไปจะประเมินความเป็นไปได้ของการโจมตีของฝ่ายตรงข้าม รวมถึงประเภทของฝ่ายตรงข้าม กลยุทธ์ และความสามารถ การประเมินภัยคุกคามเฉพาะสถานที่ยังกำหนดจำนวนฝ่ายตรงข้ามและวิธีการปฏิบัติการหรือการโจมตีอีกด้วย ด้วยข้อมูลนี้ ผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยจะใช้การประเมินภัยคุกคามเป็นเครื่องมือในการ

ตัดสินใจที่ช่วยจัดทำและจัดลำดับความสำคัญของข้อกำหนด การวางแผน และการจัดสรรทรัพยากรของระบบการรักษาความมั่นคงปลอดภัย โดยทั่วไป กระบวนการประเมินภัยคุกคามประกอบด้วย:

ภาพ 3.1 จากสูตรภัยคุกคาม (Threat formula) ผู้คุกคามมีความคาดหวังอย่างสมเหตุสมผลว่าการโจมตีจะสำเร็จโดยพิจารณาจากความตั้งใจ ความสามารถและแรงจูงใจของพวกเขา (Vellani, 2021)

ไม่ว่าผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจะอยู่ในภาครัฐ หรือภาคธุรกิจด้านการค้าและอุตสาหกรรม การประเมินภัยคุกคามควรดำเนินการบ่อยเท่าที่จำเป็นเพื่อตอบสนองความต้องการขององค์กร โดยเฉพาะองค์กรธุรกิจและองค์กรอื่น ๆ ควรมุ่งมั่นในการประเมินภัยคุกคามประจำปี ทั้งนี้ การประเมินภัยคุกคามเฉพาะตำแหน่งที่โครงสร้างพื้นฐาน เช่น ท่าเรือ จะดำเนินการไม่บ่อยนัก แต่ข้อมูลภัยคุกคามมักจะได้รับการอัปเดตอย่างต่อเนื่อง ควรสังเกตว่าความล้มเหลวที่ใหญ่ที่สุดในการประเมินภัยคุกคามคือการขาดความเฉพาะเจาะจง ตัวอย่างเช่น เมื่อมีการเปิดตัวระบบการแจ้งเตือนการก่อการร้ายระดับชาติ ความเคลื่อนไหวในระดับภัยคุกคามทำให้อุตสาหกรรมและหน่วยงานทั้งหมดต้องเปลี่ยนระดับความพร้อมโดยไม่คำนึงถึงที่ตั้งทางภูมิศาสตร์ แม้ว่าข้อมูลภัยคุกคามที่เกี่ยวข้องจะได้รับการอัปเดตตลอดเวลาก็ตาม ข้อบกพร่องที่เห็นได้ชัดเจนในแนวทางปฏิบัติในการประเมินภัยคุกคามคือการไม่มีความเฉพาะเจาะจง ยกตัวอย่างจากการตอบสนองแบบเดียวกันที่ได้รับคำสั่งจากระบบเตือนภัยก่อการร้ายระดับชาติเบื้องต้น โดยไม่คำนึงถึงสถานที่ ผู้เชี่ยวชาญด้านความปลอดภัยจึงได้รับการสนับสนุนให้ใช้วิธีการที่เหมาะสมและมุ่งเน้นมากขึ้นในการประเมินภัยคุกคาม

โดยพิจารณาจากตัวแปรทางภูมิศาสตร์หรือสินทรัพย์เฉพาะ ปัญหาสำคัญในการเพิ่มระดับภัยคุกคามสากลคือภาระทางการเงินของความพร้อมที่เพิ่มขึ้น ด้วยการเข้าถึงข้อมูลโดยละเอียดเกี่ยวกับเป้าหมายที่เป็นไปได้ ผู้เชี่ยวชาญด้านความปลอดภัยสามารถวัดความน่าจะเป็นและประเภทของการโจมตี ทำให้สามารถดำเนินมาตรการตอบโต้ที่แม่นยำและมีประสิทธิภาพได้

การประเมินภัยคุกคามจะพิจารณาถึงอันตรายทั้งหมดที่อาจส่งผลกระทบต่อสิ่งที่เราให้ความสำคัญ เช่น ภัยพิบัติทางธรรมชาติ อาชญากรรม การก่อการร้าย อุบัติเหตุ และปัญหาความปลอดภัยทั่วไป เช่น การเข้าถึงโดยไม่ได้รับอนุญาต ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจะตรวจสอบอันตรายที่เป็นไปได้ทุกอย่างอย่างใกล้ชิด โดยใช้ข้อมูลทั้งหมดที่หาได้เพื่อพิจารณาว่ามีแนวโน้มที่จะเกิดขึ้นมากน้อยเพียงใด ตัวอย่างเช่น จังหวัดต่าง ๆ ตามแนวชายฝั่งอ่าวไทย เช่น ชุมพร นครศรีธรรมราช และสุราษฎร์ธานี ใช้ข้อมูลในอดีตเพื่อเตรียมพร้อมสำหรับพายุไต้ฝุ่นเมื่อมีแนวโน้มที่จะเกิดขึ้นมากที่สุด ในทำนองเดียวกันร้านสะดวกซื้อในเมืองสามารถบอกความเสี่ยงในการก่ออาชญากรรมจากประสบการณ์ในอดีตได้ แต่การรู้เกี่ยวกับความเสี่ยงทั่วไปเหล่านี้ยังไม่เพียงพอ ผู้ปฏิบัติงานด้านความปลอดภัยจำเป็นต้องพิจารณาสถานการณ์เฉพาะเพื่อรักษาสิ่งต่าง ๆ ให้ปลอดภัย หากร้านค้าในพื้นที่ที่มีอาชญากรรมสูงมีอาชญากรรมมากกว่าปกติ ร้านค้าจะต้องดำเนินการอย่างจริงจังและให้ความสำคัญกับความปลอดภัยมากขึ้นเพื่อรับมือกับความเสี่ยงที่สูงขึ้น

ความน่าดึงดูดใจของสินทรัพย์ (asset attractiveness) ควรได้รับการพิจารณาในการประเมินภัยคุกคามด้วย สินทรัพย์และธุรกิจบางอย่างมีระดับภัยคุกคามโดยธรรมชาติที่สูงกว่าเนื่องจากมีความน่าดึงดูดใจต่อองค์ประกอบทางอาชญากรรม ตัวอย่างหนึ่งที่ชัดเจนคือร้านขายเครื่องประดับหรือร้านทอง มักจะเผชิญกับภัยคุกคามที่สูงกว่าของการก่ออาชญากรรม ถึงแม้ว่าร้านนั้น ๆ อาจจะไม่เคยประสบเหตุอาชญากรรมมาก่อน แต่ระดับภัยคุกคามของการโจรกรรมและการลักขโมยยังคงสูงกว่าร้านทั่วไป อีกตัวอย่างหนึ่งของธุรกิจที่มีระดับภัยคุกคามอยู่ในระดับสูงก็คือสถานที่ก่อสร้าง ซึ่งเมื่อเปรียบเทียบกับสถานที่อื่น ๆ มักมีอัตราการเกิดอุบัติเหตุที่สูงกว่า ส่งผลให้คนงานได้รับบาดเจ็บ แสดงถึงระดับภัยคุกคามที่สูงขึ้น อย่างไรก็ตาม ภัยคุกคามที่เพิ่มขึ้นนี้ไม่ได้หมายความว่าสถานที่เหล่านี้มีความเสี่ยงมากขึ้นโดยอัตโนมัติ เพียงแต่ยอมรับถึงความเสี่ยงที่อาจเกิดขึ้น

การระบุและการจำแนกภัยคุกคาม (Threat Identification and Classification)

การระบุภัยคุกคามหมายถึง กระบวนการรับรู้ ประเมิน และจัดหมวดหมู่ภัยคุกคามที่อาจเกิดขึ้นซึ่งอาจเป็นอันตรายต่อทรัพย์สิน การดำเนินงาน หรือบุคลากรขององค์กร เป็นขั้นตอนสำคัญในการบริหารความเสี่ยงที่เกี่ยวข้องกับการวิเคราะห์แหล่งที่มาของภัยคุกคามต่าง ๆ ตั้งแต่การโจมตีทางไซเบอร์ ภัยพิบัติทางธรรมชาติ ไปจนถึงภัยคุกคามภายใน โดยมีจุดประสงค์เพื่อทำความเข้าใจลักษณะ แนวโน้ม และผลกระทบที่อาจเกิดขึ้นของภัยคุกคามเหล่านี้ต่อองค์กร (Stoneburner, Goguen, &

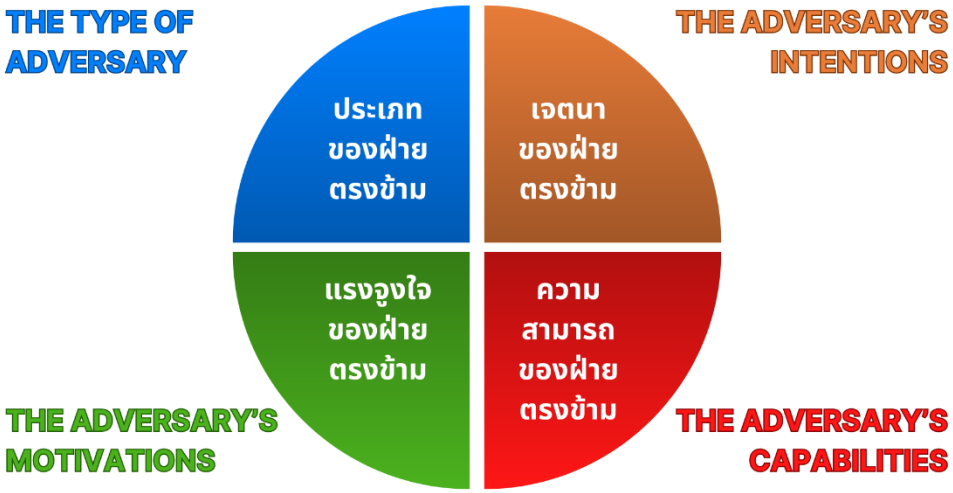
Feringa, 2002) โดยเป็นที่เข้าใจโดยทั่วไปว่า อดีตมักทำหน้าที่เป็นตัวทำนายเหตุการณ์ในอนาคตที่น่าเชื่อถือที่สุด ซึ่งเป็นหลักการที่สามารถนำไปใช้ในการประเมินภัยคุกคามจากฝ่ายตรงข้ามได้อย่างดี ทั้งนี้ จากการวิเคราะห์พฤติกรรมในอดีตของฝ่ายตรงข้าม ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจึงสามารถคาดการณ์การกระทำในอนาคตได้แม่นยำยิ่งขึ้น ตัวอย่างเช่น ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจำนวนมากสามารถสรุปอย่างแม่นยำว่าการโจมตีตึกเวิลด์เทรดเซ็นเตอร์และเพนตากอนเมื่อวันที่ 11 กันยายน ค.ศ. 2001 เป็นการโจมตีของ โอซามา บิน ลาเดน ทันทีที่เครื่องบินลำที่สองชนตึกเวิลด์เทรดเซ็นเตอร์ โดยการประเมินที่แม่นยำนี้อิงจากข้อมูลและความรู้เกี่ยวกับรูปแบบของการโจมตีครั้งก่อน ๆ โดยกลุ่มก่อการร้ายที่รู้จักกันในชื่อ อัลกออิดะห์ ด้วยเหตุนี้ การสรุปตัดสินนี้จึงมีพื้นฐานมาจากการเข้าใจกิจกรรมในอดีตของกลุ่มอย่างลึกซึ้งนั่นเอง

แม้ว่าตัวอย่างของ อัลกออิดะห์ จะเข้าใจกันทั่วโลกในอุตสาหกรรมความมั่นคงปลอดภัย ตรรกะเดียวกันนี้ก็สามารถใช้กับเป้าหมายเชิงพาณิชย์และอุตสาหกรรมได้ ทั้งนี้ หากผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยเข้าใจมุมมองของฝ่ายตรงข้าม ก็สามารถจัดสรรมาตรการป้องกันที่มีประสิทธิภาพเพื่อลดภัยคุกคามได้อย่างมีประสิทธิภาพ อาทิ ศัตรูจะเลือกเป้าหมายได้อย่างไร? สินทรัพย์ประเภทใดที่เคยตกเป็นเป้าหมายในอดีต? ความตั้งใจ ความสามารถ และแรงจูงใจของผู้ประสงค์ร้ายคืออะไร? ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของธนาคารและสถาบันการเงินได้ใช้การแบ่งปันข้อมูลภัยคุกคามเพื่อป้องกันอาชญากรรมบางอย่าง ในทำนองเดียวกัน ผู้ค้าปลีกก็มีการแชร์ข้อมูลเกี่ยวกับเทคนิคในการขโมยสินค้าในรูปแบบต่าง ๆ เพื่อป้องกันทรัพย์สินสูญหาย

แม้ว่าผู้บริหารงานด้านความมั่นคงปลอดภัยจะมุ่งเป้าไปที่การวัดภัยคุกคามในเชิงปริมาณหรือด้วยตัวเลข แต่บางครั้งก็ไม่สามารถทำได้เสมอไป เนื่องจากการประเมินภัยคุกคามบางอย่างต้องอาศัยสมมติฐานและการคาดเดาอย่างมีหลักการ ตัวอย่างเช่น ผู้บริหารสามารถใช้ข้อมูลอาชญากรรมในอดีตเพื่อประเมินภัยคุกคามทางอาชญากรรมเป็นตัวเลข อย่างไรก็ตาม การทำความเข้าใจในตัวอาชญากรรายใดรายหนึ่งต้องใช้แนวทางเชิงคุณภาพมากกว่า โดยอิงจากข้อมูลเชิงลึกมากกว่าข้อมูลที่เป็นรูปธรรม สิ่งนี้เน้นย้ำประเด็นสำคัญของการวิเคราะห์อาชญากรรม โดยเน้นไปที่รูปแบบของอาชญากรรมในอดีตมากกว่าตัวอาชญากรเอง

ด้วยเหตุนี้ การประเมินภัยคุกคามจะเน้นไปที่การทำความเข้าใจฝ่ายตรงข้ามหรือในมุมมองเชิงคุณภาพ ในขณะที่ส่วนของการวิเคราะห์อาชญากรรมจะมุ่งเน้นไปกับวิธีการเชิงปริมาณที่ขับเคลื่อนด้วยข้อมูล ดังนั้น ในการประเมินภัยคุกคามเชิงคุณภาพผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยจำเป็นที่จะต้องมีข้อมูลสำคัญดังภาพ 3.2 ทั้งนี้ ข้อมูลเกี่ยวกับประเภทของฝ่ายตรงข้าม แรงจูงใจ เจตนา และความสามารถของฝ่ายตรงข้าม เป็นสิ่งที่ขาดไม่ได้ในการกำหนดกลยุทธ์ความมั่นคงปลอดภัยที่เหมาะสม โดยการระบุประเภทของฝ่ายตรงข้ามจะทำให้ทราบถึงความซับซ้อนและทรัพยากรที่ต้องสอดคล้องกับระดับการคุกคาม การทำความเข้าใจกับแรงจูงใจสามารถอธิบายถึงเหตุผลที่อยู่เบื้องหลังการกำหนดเป้าหมาย ไม่ว่าจะเป็นผลประโยชน์ทางการเงิน อิทธิพลทางการเมือง

หรือเหตุผลทางอุดมการณ์ ทำให้สามารถวางแผนการป้องกันที่ครอบคลุมมากขึ้น การรู้ถึงเจตนาจะให้ข้อมูลเชิงลึกเกี่ยวกับวัตถุประสงค์เฉพาะที่ฝ่ายตรงข้ามมุ่งหวัง เช่น การโจรกรรม การทำให้เกิดความเสียหาย หรือการทำอันตราย และสุดท้าย การประเมินความสามารถของฝ่ายตรงข้ามจะให้มุมมองที่เป็นจริงของวิธีการทางเทคนิคและวิธีการในการจัดการฝ่ายตรงข้าม ทำให้การตอบโต้ที่พัฒนาขึ้นสามารถลดภัยคุกคามได้อย่างมีประสิทธิภาพ องค์ประกอบของข้อมูลทั้ง 4 ด้านนี้จะช่วยให้องค์กรสามารถจัดสรรทรัพยากรได้อย่างมีประสิทธิภาพและเสริมสร้างการป้องกันต่อภัยคุกคามที่อันตรายโดยปรับเปลี่ยนจากการรักษาความมั่นคงปลอดภัยทั่วไปสู่รูปแบบที่ลักษณะมุ่งเป้าและเชิงรุกได้



ภาพ 3.2 ในการทำความเข้าใจในมุมมองของฝ่ายตรงข้าม ประเภทของข้อมูลทั้ง 4 ด้าน เป็นสิ่งจำเป็นในการประเมินภัยคุกคาม (Vellani, 2021)

โดยทั่วไป ภัยคุกคามสามารถจำแนกได้ว่าเป็นภัยคุกคามโดยมนุษย์หรือโดยธรรมชาติ ภัยคุกคามโดยมนุษย์เกี่ยวข้องกับบุคคลที่ทำงานภายในองค์กร เช่น นายจ้างและผู้รับเหมา (ภายใน) ผู้ที่ประสงค์ร้ายจากภายนอกองค์กร (ภายนอก) หรือทั้งสองอย่างรวมกัน ภัยคุกคามทางธรรมชาติคือเหตุการณ์ที่ไม่ได้เกิดจากฝีมือมนุษย์ เช่น พายุไต้ฝุ่น น้ำท่วม ไฟไหม้ และเหตุการณ์ด้านสิ่งแวดล้อมอื่น ๆ

ภัยคุกคามต่อความมั่นคงปลอดภัยโดยมนุษย์สามารถแบ่งออกได้เป็น 3 ประเภทหลัก ได้แก่ บุคคลภายใน บุคคลภายนอก และบุคคลภายในที่ทำงานร่วมกับบุคคลภายนอก ทั้งนี้ บุคคลภายในได้แก่ พนักงานหรือผู้รับเหมาที่อาจมีความเกี่ยวข้องกับกิจกรรมที่ผิดกฎหมายหรือผู้ที่ไม่พอใจกับหน้าที่การงานของตน เนื่องจากบุคคลภายในมีความรู้เกี่ยวกับระบบรักษาความปลอดภัยขององค์กรและเข้าถึงสถานที่ได้ง่าย บุคคลกลุ่มนี้จึงเป็นผู้ที่มีความเสี่ยงเป็นพิเศษ เนื่องจากสามารถกระทำการละเมิดอย่างเปิดเผยหรือปิดบังซ่อนเร้น ซึ่งบางครั้งก็อาจกระทำการร่วมกับอาชญากรภายนอกด้วย แม้ว่าการละเมิดจากบุคคลภายในอาจเป็นอันตรายต่อเพื่อนพนักงานด้วยกัน แต่ปัญหาที่ซับซ้อนมากขึ้นจะเกิดขึ้นเมื่อบุคลากรภายในองค์กรถูกละเมิดหรือรุกรานจากบุคคลภายนอก ซึ่งจะทำให้งานของผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยมีความซับซ้อนมากขึ้น ในกรณีดังกล่าว เครื่องมือรักษาความปลอดภัยแบบดั้งเดิม ๆ เช่น สัญญาณเตือนภัยและกล้องวงจรปิด มักจะใช้ไม่ได้ผลกับบุคคลภายใน ด้วยเหตุนี้ เพื่อตอบโต้ภัยคุกคามภายใน การใช้นโยบายที่เข้มงวด รวมถึงการตรวจสอบความน่าเชื่อถือของพนักงาน การสอบสวนภูมิหลังเป็นประจำ และการจำกัดการเข้าถึงพื้นที่สำคัญ จึงเป็นวิธีการที่ได้รับการพิสูจน์แล้วว่าเป็นกลยุทธ์ที่มีประสิทธิภาพมาก

บุคคลภายนอกที่ก่อให้เกิดภัยคุกคามอาจมาจากกลุ่มต่าง ๆ เช่น รัฐบาลต่างประเทศ หน่วยทหาร แก๊ง อาชญากรทั่วไป กลุ่มหัวรุนแรง และผู้ก่อการร้าย ระดับรายละเอียดในการจัดหมวดหมู่ภัยคุกคามเหล่านี้ควรมีความสอดคล้องกับสิ่งที่องค์กรรักษาความมั่นคงปลอดภัยต้องการ ตัวอย่างเช่น ภาครัฐจำแนกผู้ก่อการร้ายตามแรงจูงใจ ซึ่งอาจเป็นเรื่องการเมือง ศาสนา หรือสิ่งแวดล้อม ลักษณะของผู้ก่อการร้ายมักรวมถึงการพร้อมที่จะเสียสละชีวิต มุ่งเป้าที่จะสร้างความเสียหายและการบาดเจ็บล้มตายครั้งใหญ่ สร้างความทุกข์ทรมานทางจิตใจต่อสาธารณะ และแสดงความสามารถของกลุ่มต่อผู้ที่ให้ทุนสนับสนุนองค์กร เหตุผลที่บุคคลภายนอกอาจเป็นภัยคุกคามมีตั้งแต่ความเชื่อทางอุดมการณ์และการแสวงหาผลตอบแทนทางการเงินไปจนถึงความอาฆาตแค้นส่วนตัว

ยิ่งไปกว่านั้น การรวมมือกันของบุคคลภายในที่ทำงานร่วมกับบุคคลภายนอกแสดงถึงความเสี่ยงสูงสุด บุคคลภายในเหล่านี้สามารถแบ่งออกเป็นสองกลุ่ม คือ (1) กลุ่มที่ถูกกดดันให้เข้าร่วมและ (2) กลุ่มที่เลือกเข้าร่วม บุคคลภายในที่ถูกกดดันคือผู้ที่ช่วยในการบุกรุกโจมตีเพราะบุคคลเหล่านี้หรือครอบครัวอาจถูกคุกคามหรือเพราะถูกแบล็กเมล์ ในทางกลับกัน บุคคลภายในที่เต็มใจร่วมมือมักจะทำเช่นนั้นเพื่อผลประโยชน์ทางการเงิน เช่น รับสินบน หรือเพราะบุคคลเหล่านี้สนับสนุนเป้าหมายทางอุดมการณ์ของบุคคลภายนอก

ด้วยเหตุนี้ การประเมินภัยคุกคามควรคำนึงถึงความเป็นไปได้ของภัยคุกคามจากมนุษย์ทั้งสามประเภท ข้อมูลเหล่านี้ควรอิงจากข่าวกรองที่เชื่อถือได้จากหลากหลายแหล่ง รวมถึงข้อมูลภายในข้อมูลจากหน่วยงานภาครัฐ หน่วยงานที่บังคับใช้กฎหมาย ทีมสีแดง (ทีมที่มีบทบาทเป็นผู้โจมตีโดยพยายามค้นหาจุดอ่อนและฝ่าระบบป้องกันความปลอดภัย) ผู้เชี่ยวชาญ รายงานของสื่อ และแหล่งข่าวกรองของรัฐบาลและภาคเอกชน บ่อยครั้งที่ผู้บริหารงานด้านความมั่นคงปลอดภัยมีความรู้

และข้อมูลที่เกี่ยวกับภัยคุกคามที่เฉพาะเจาะจงล่วงหน้าไม่เพียงพอ ข้อมูลอาจไม่สมบูรณ์หรือคลุมเครือ ดังนั้นจึงต้องอาศัยวิจารณญาณในการระบุภัยคุกคาม ยิ่งข้อมูลภัยคุกคามที่มีอยู่สมบูรณ์มากเท่าไร การประเมินก็จะยิ่งดีขึ้นเท่านั้น

แรงจูงใจของฝ่ายตรงข้าม (Adversary Motivation)

ปัจจัยหลากหลายประการที่เป็นแรงจูงใจขับเคลื่อนฝ่ายตรงข้าม อาทิ ผลประโยชน์ทางเศรษฐกิจ เหตุผลส่วนตัว และความเชื่อทางอุดมการณ์ การแสวงหาความมั่งคั่ง เช่น เงินหรือสิ่งของมีค่า ปัจจัยเหล่านี้มักเป็นเหตุผลสำคัญที่สุดของกิจกรรมที่ผิดกฎหมาย ซึ่งครอบคลุมถึงบุคคล เช่น โจรและขโมย อย่างไรก็ตาม แรงจูงใจที่ซ่อนอยู่อาจมีรายละเอียดมากกว่าที่ปรากฏให้เห็นในตอนแรก ตัวอย่างเช่น ผู้ติดยาอาจก่ออาชญากรรมเพื่อหาเงินมาซื้อยาเสพติด นำไปสู่การก่ออาชญากรรมทางเศรษฐกิจเพียงเพื่อให้ได้มาซึ่งสิ่งมีค่าเพื่อแลกกับยา ในทำนองเดียวกัน วัยรุ่นอาจขโมยสิ่งของที่มีมูลค่าสูง เช่น Apple Phone หรือกระเป๋า Gucci เพื่อเพิ่มสถานะทางสังคมในหมู่เพื่อนฝูง โดยเชื่อมโยงการดำเนินการทางเศรษฐกิจเข้ากับความปรารถนาที่จะได้รับการยอมรับจากสังคมและเข้ากับคนรอบข้าง

โดยทั่วไป แรงจูงใจส่วนบุคคลมักถูกขับเคลื่อนด้วยอารมณ์ ตัวอย่างเช่น สามีที่ปฏิบัติต่อภรรยาอย่างไม่ดีอาจทำแบบนั้นด้วยความโกรธ หรือพนักงานที่ไม่มีความสุขอาจโวยวายอย่างรุนแรงในที่ทำงานเพราะพวกเขาไม่พอใจกับสิ่งที่เกิดขึ้น แรงจูงใจในการคุกคามจากบุคคลภายในมักเป็นเรื่องส่วนตัวและขับเคลื่อนโดยการจัดการสถานที่ทำงานที่ไม่ดี และเมื่อมีคนในองค์กรอยู่ในสถานะมีความเสี่ยง มักเป็นเพราะบุคคลเหล่านี้ไม่พอใจกับงานของตน มักกล่าวโทษฝ่ายบริหารและยึดมั่นในความขุ่นเคืองนั้น การหยุดยั้งอาชญากรรมที่เกิดจากปัญหาส่วนตัวอาจเป็นเรื่องยาก สิ่งเหล่านี้อาจเกิดขึ้นในช่วงเวลาที่มีการโต้เถียงรุนแรงเนื่องจากความโกรธกะทันหันหรือเพราะความผิดปกติเนื่องจากปัญหาสุขภาพจิต

อุดมการณ์ ความเชื่อและค่านิยมของผู้คนมักจะเป็นตัวขับเคลื่อนการกระทำของกลุ่ม โดยเฉพาะอย่างยิ่งเมื่อมีการทำอันตรายต่อสิ่งแวดล้อมหรือปกป้องสิทธิสัตว์ ตัวอย่างเช่น ในสหรัฐอเมริกา กลุ่มอนุรักษ์ เช่น Earth Liberation Front ซึ่งมุ่งมั่นเกี่ยวกับการปกป้องสิ่งแวดล้อมได้จุดไฟเผาตัวแทนจำหน่ายรถยนต์ที่ขายรถยนต์ที่ใช้น้ำมัน หรือ Sea Shepherd Conservation Society มีส่วนร่วมในการต่อต้านปฏิบัติการล่าวาฬของญี่ปุ่น ด้วยการใช้เรือเข้าสกัดกั้น การใช้กับดักใบพัด และการยิงระเบิดเหม็นใส่เรือล่าวาฬ อย่างไรก็ตาม ตัวอย่างที่รู้จักกันดีของกลุ่มที่ขับเคลื่อนด้วยอุดมการณ์ความเชื่ออันแรงกล้าคือ อัลกออิดะห์ ที่ทำการโจมตีตึกเวิลด์เทรดเซ็นเตอร์ในปี ค.ศ. 1993 แม้ว่าเหตุการณ์นั้นจะไม่ได้สร้างความเสียหายอย่างรุนแรง แต่ก็แสดงให้เห็นถึงความตั้งใจที่จะมุ่งเป้าโจมตีไปที่อาคารสถานที่ ๆ สำคัญ

ภาพ 3.3 Sea Shepherd Conservation Society อ้างว่าการล่าวาฬของญี่ปุ่นละเมิดกฎหมายและข้อตกลงระหว่างประเทศ เช่น การหยุดการล่าวาฬเชิงพาณิชย์อย่างไม่มีกำหนดของคณะกรรมาธิการการล่าวาฬระหว่างประเทศ (IWC) ซึ่งบังคับใช้ในปี ค.ศ. 1986 (Schuler, 2016)

ขีดความสามารถของฝ่ายตรงข้าม (Adversary Capability)

การประเมินขีดความสามารถของฝ่ายตรงข้ามถือเป็นองค์ประกอบที่สำคัญของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัย โดยต้องอาศัยข้อมูลข่าวกรองที่ถูกต้อง แม่นยำ และครอบคลุมอย่างมาก เหตุการณ์ทางประวัติศาสตร์ เช่น การโจมตีฐานทัพเรือสหรัฐที่อ่าวเพิร์ลฮาร์เบอร์ในปี ค.ศ. 1941 โดยกองทัพเรือจักรวรรดิญี่ปุ่นอย่างไม่คาดคิด เน้นย้ำถึงผลที่ตามมาจากการประเมินความสามารถของฝ่ายตรงข้ามต่ำเกินไปเนื่องจากการข่าวที่ไม่สมบูรณ์หรือหลงทาง ในบริบทของธุรกิจและอุตสาหกรรม ซึ่งในปัจจุบันมีการแข่งขันที่รุนแรง การได้มาซึ่งข่าวกรองที่เชื่อถือได้ถือเป็นเรื่องท้าทายที่สำคัญอย่างมาก อย่างไรก็ตาม บางภาคส่วน เช่น การธนาคาร ก็ประสบความสำเร็จในการแบ่งปันข้อมูลภัยคุกคามเพื่อแก้ไขปัญหาด้านความปลอดภัยทางการเงินจากการจู่โจมล่วงหน้า

การประเมินขีดความสามารถของฝ่ายตรงข้ามเกี่ยวข้องกับการพิจารณาปัจจัยต่าง ๆ เช่น จำนวนฝ่ายตรงข้าม ทักษะและความรู้ อาวุธ อุปกรณ์ วิธีการ และการสมรู้ร่วมคิดจากบุคคลภายในที่อาจเกิดขึ้น ตัวอย่างเช่น กลุ่มผู้ก่อการร้ายอาจมีอาวุธทางการทหาร วัตถุระเบิด และวิธีการสร้างระเบิดแสวงเครื่อง (improvised explosive devices) โดยเน้นย้ำถึงความสำคัญของความเข้าใจที่ลึกซึ้งเกี่ยวกับภาพรวมภัยคุกคาม โดยการประเมินรูปแบบนี้เป็นรากฐานของ Design Basis Threat

(DBT) ซึ่งสรุปเจตนา ความสามารถ และวิธีการโจมตีที่อาจเกิดขึ้นของฝ่ายตรงข้ามต่อเป้าหมายทรัพย์สิน ซึ่งช่วยในการกำหนดกลยุทธ์ด้านความมั่นคงปลอดภัยที่มีประสิทธิภาพ

ยิ่งไปกว่านั้น ลักษณะที่เป็นพลวัตของภัยคุกคามจำเป็นต้องมีการประเมินอย่างต่อเนื่อง เนื่องจากความสามารถของฝ่ายตรงข้ามมีการพัฒนาไปตามสถานการณ์ที่เปลี่ยนแปลงและการเข้าถึงทรัพยากร การทำความเข้าใจความสามารถเหล่านี้ ร่วมกับข้อมูลภัยคุกคามโดยละเอียดจากแหล่งที่มาที่หลากหลาย ช่วยให้ผู้เชี่ยวชาญด้านความปลอดภัยสามารถใช้มาตรการที่กำหนดเป้าหมายได้อย่างมีประสิทธิภาพ ลดโอกาสของความสำเร็จในการโจมตีทรัพย์สินที่สำคัญ

แหล่งข้อมูลภัยคุกคาม (Threat Information Sources)

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยต้องใช้เครือข่ายอย่างกว้างขวางในการรวบรวมข้อมูลภัยคุกคามเพื่อปกป้องทรัพย์สินอย่างครอบคลุม ซึ่งรวมถึงการใช้ประโยชน์จากข้อมูลภายในเกี่ยวกับการละเมิดความปลอดภัย ข้อมูลการบังคับใช้กฎหมาย ข้อมูลเชิงลึกจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และการรายงานข่าวของสื่อ ด้วยการใช้แหล่งข้อมูลข่าวกรองของรัฐบาลและเอกชนที่ผสมผสานกัน พร้อมด้วยการวิเคราะห์โดยละเอียดจากการฝึกซ้อมของทีมสีแดง องค์กรต่าง ๆ จะได้รับมุมมองที่หลากหลายเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้น แหล่งข้อมูลที่กว้างขวางนี้มีความสำคัญอย่างยิ่งต่อการสร้างมาตรการรักษาความมั่นคงปลอดภัยที่แข็งแกร่ง ที่สามารถคาดการณ์และบรรเทาภัยคุกคามได้อย่างมีประสิทธิภาพ

ขั้นตอนแรกสำหรับที่ปรึกษาด้านความมั่นคงปลอดภัย คือการสัมภาษณ์เชิงลึกกับเจ้าหน้าที่รักษาความปลอดภัยในสถานที่และพนักงานคนอื่น ๆ แนวทางระดับรากหญ้านี้จำเป็นสำหรับการระบุสินทรัพย์ที่อาจเป็นเป้าหมายในการโจมตีล่วงหน้า การทำความเข้าใจลักษณะและผลลัพธ์ของการโจมตีที่คาดการณ์ไว้ และการประเมินประสิทธิภาพของมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่ด้วยการถามคำถามที่ตรงเป้าหมายเกี่ยวกับเหตุการณ์ในอดีต ที่ปรึกษาด้านความมั่นคงปลอดภัยสามารถเปิดเผยรูปแบบและช่องโหว่ที่ไม่ชัดเจนได้ทันทีจากรายงานอย่างเป็นทางการหรือการวิเคราะห์ข้อมูลเบื้องต้น ทั้งนี้ บุคลากรที่ทำงานปฏิบัติงานอยู่เป็นแหล่งข้อมูลที่ดี คำถามพื้นฐานที่ควรถามบุคลากรในสายงานเกี่ยวกับสินทรัพย์ ประกอบไปด้วย (1) ทรัพย์สินใดที่เคยตกเป็นเป้าหมายในอดีต? (2) ทรัพย์สินถูกโจมตีเมื่อใด? (3) ใครมุ่งโจมตีเป้าหมายทรัพย์สิน? (4) เหตุใดทรัพย์สินนั้นจึงเป็นเป้าหมาย? (5) ทรัพย์สินถูกโจมตีอย่างไร? (6) มีการใช้มาตรการรักษาความปลอดภัยเพื่อตอบสนองต่อการโจมตีหรือไม่?

นอกจากนั้น องค์กรยังได้รับประโยชน์จากการเก็บรักษาข้อมูลภายในอย่างละเอียดที่เกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยในอดีต ซึ่งสามารถเปิดเผยแนวโน้มและเน้นย้ำจุดอ่อนที่เกิดซ้ำได้ การตรวจสอบการบันทึกข้อมูลเหล่านี้เป็นประจำ ควบคู่ไปกับการประเมินภัยคุกคามล่วงหน้า จะช่วย

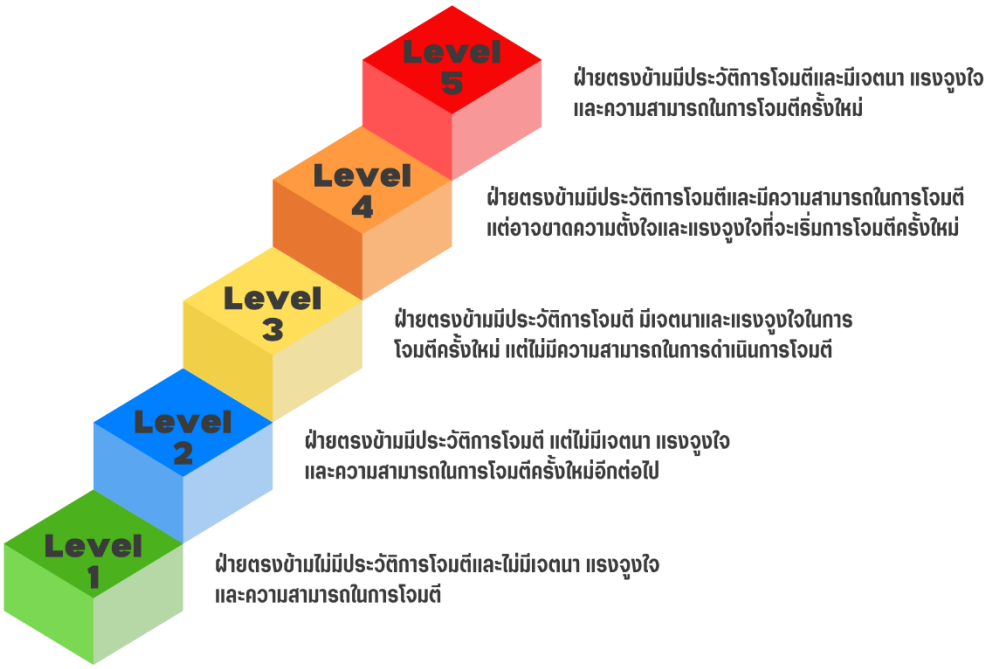
ให้ทีมรักษาความปลอดภัยสามารถปรับกลยุทธ์ของตนให้เข้ากับภัยคุกคามที่กำลังพัฒนาได้ ข้อมูลภายนอก เช่น สถิติอาชญากรรมจากหน่วยงานบังคับใช้กฎหมายในท้องถิ่นและข้อมูลเชิงลึกจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยภาคเอกชน จะช่วยเพิ่มบริบทความมั่นคงปลอดภัยอีกหนึ่งชั้น ซึ่งจะช่วยสร้างภาพรวมที่ครอบคลุมของภัยคุกคามที่อาจเกิดขึ้น กระบวนการรวบรวม ตรวจสอบ และอัปเดตข้อมูลภัยคุกคามซ้ำ ๆ นี้ จะทำให้มั่นใจได้ว่ามาตรการรักษาความมั่นคงปลอดภัยยังคงเป็นปัจจุบันและมีประสิทธิภาพ ปรับเปลี่ยนให้เหมาะกับความต้องการเฉพาะขององค์กรและภูมิทัศน์ด้านความปลอดภัยของอุตสาหกรรมที่เกี่ยวข้อง

การประเมินภัยคุกคาม

การประเมินภัยคุกคามเกี่ยวข้องกับการประเมินความเสี่ยงที่อาจเกิดขึ้นอย่างละเอียดครอบคลุม ที่อาจส่งผลต่อความปลอดภัยของสินทรัพย์ขององค์กร กระบวนการนี้เริ่มต้นด้วยการรวบรวมและตรวจสอบข้อมูลภัยคุกคามที่มีอยู่ทั้งหมดจากแหล่งต่าง ๆ เช่น บันทึกภายใน ข้อมูลการบังคับใช้กฎหมาย รายงานของสื่อ และข้อมูลเชิงลึกของผู้เชี่ยวชาญ จากนั้นผู้เชี่ยวชาญด้านความปลอดภัยจะใช้ข้อมูลที่รวบรวมนี้เพื่อระบุภัยคุกคามที่อาจเกิดขึ้นกับทรัพย์สินของตน โดยมุ่งเน้นไปที่ทรัพย์สินที่สำคัญเป็นหลัก แต่ยังพิจารณาสิ่งอื่นๆ ในระหว่างขั้นตอนการประเมินด้วย เป้าหมายคือการประเมินความเป็นไปได้ที่ภัยคุกคามจะกำหนดเป้าหมายไปที่สินทรัพย์ ไม่ว่าจะในเชิงปริมาณหรือเชิงคุณภาพ โดยอาศัยความเข้าใจอย่างถ่องแท้ถึงเจตนา แรงจูงใจ และความสามารถของฝ่ายตรงข้าม ยกตัวอย่างในกรณีการโจมตีตึกเวิลด์เทรดเซ็นเตอร์ในปี ค.ศ. 1993 จะเห็นว่ากลุ่มผู้ก่อการร้ายอัลกออิดะห์มีแรงจูงใจที่จะโจมตีทำลายตึกเวิลด์เทรดเซ็นเตอร์ แต่ความสามารถของกลุ่มในขณะนั้นไม่สัมพันธ์กับเจตนาความตั้งใจของกลุ่ม อย่างไรก็ดี ตึกเวิลด์เทรดเซ็นเตอร์ก็ยังคงเป็นเป้าหมายที่น่าสนใจในการก่อการร้ายของกลุ่ม และหากไม่มีข่าวกรองที่น่าเชื่อถือได้ว่าเครื่องบินโดยสารพาณิชย์จะถูกใช้เป็นขีปนาวุธนำวิถี กลุ่มผู้ก่อการร้ายอัลกออิดะห์ก็จะไม่มีความสามารถในการทำลายตึกเวิลด์เทรดเซ็นเตอร์ในวันที่ 11 กันยายน ค.ศ. 2001 ได้อย่างแน่นอน

การประเมินภัยคุกคามเชิงคุณภาพมีการระบุและประเมินภัยคุกคามตามลักษณะและผลกระทบที่อาจเกิดขึ้น ตัวอย่างเช่น การโจมตีทางไซเบอร์ซึ่งมีเป้าหมายเพื่อขโมย เปลี่ยนแปลง หรือทำลายข้อมูล อาจถือเป็นภัยคุกคามที่มีความเป็นไปได้สูงและมีผลกระทบสูง เนื่องจากองค์กรมีการเชื่อมต่อออนไลน์เกือบตลอดเวลาและมีสินทรัพย์ดิจิทัลที่มีค่าสูง ในขณะที่ภัยคุกคามจากภายใน (พนักงาน) อาจจัดอยู่ในระดับปานกลางแต่มีผลกระทบสูง เมื่อพิจารณาจากระดับการเข้าถึงข้อมูลที่ละเอียดอ่อนของพนักงาน ยิ่งไปว่านั้น ภัยคุกคามทางกายภาพอาจถูกมองว่ามีโอกาสต่ำแต่มีผลกระทบปานกลาง เมื่อพิจารณาจากมาตรการรักษาความปลอดภัยทางกายภาพที่แข็งแกร่ง และสุดท้าย ภัยพิบัติทางธรรมชาติ (เช่น น้ำท่วมและแผ่นดินไหว) เป็นสิ่งที่คาดเดาไม่ได้และอาจก่อให้เกิด

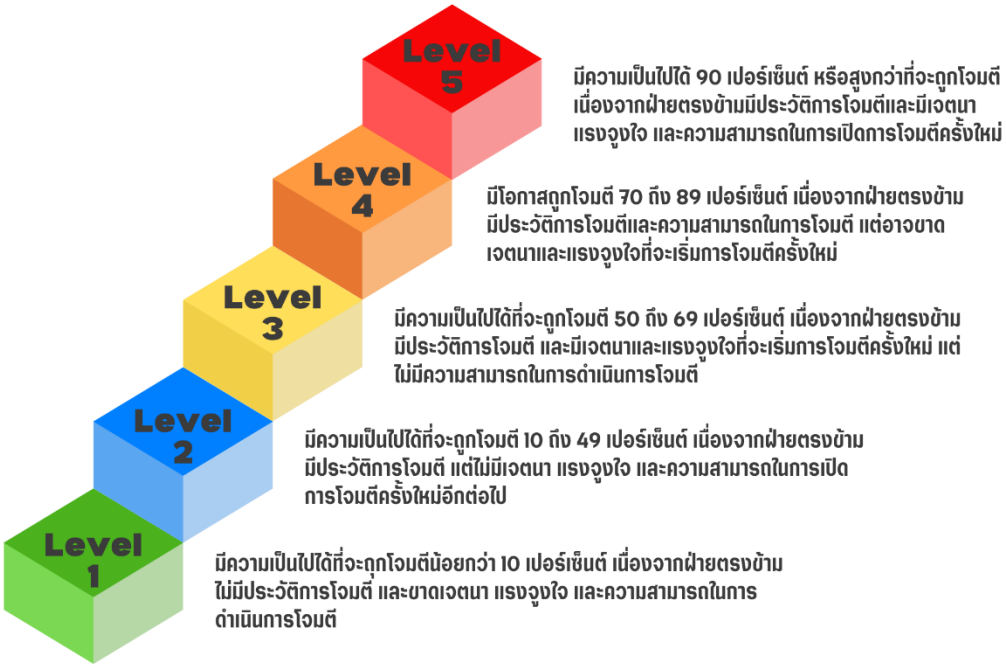
ความเสียหายอย่างมากต่อโครงสร้างพื้นฐานทางกายภาพ ส่งผลให้ข้อมูลสูญหายหรือการหยุดทำงานขององค์กร (Fennelly, 2017)



ภาพ 3.4 การวิเคราะห์ภัยคุกคามเชิงคุณภาพเกี่ยวข้องกับการประเมินและจัดอันดับความเสี่ยงด้วยการการระบุภัยคุกคาม (หรือโอกาส) ความน่าจะเป็นที่จะเกิดขึ้น และความรุนแรงและความน่าจะเป็นของผลที่ตามมา (Evrin, 2021)

การประเมินเชิงปริมาณจะมีประสิทธิภาพในกรณีที่มีข้อมูลประวัติการโจมตีต่อสินทรัพย์ ซึ่งช่วยให้สามารถประเมินแนวโน้มภัยคุกคามที่ขับเคลื่อนด้วยข้อมูล ตัวอย่างเช่น องค์กรอาจคำนวณมูลค่าความเสียหายต่อปี หรือ Annual Loss Expectancy (ALE) สำหรับภัยคุกคามด้านความมั่นคงปลอดภัยที่แตกต่างกัน เช่น การละเมิดทางข้อมูลหรือการหยุดทำงานของระบบ โดยการคูณความถี่โดยประมาณของภัยคุกคามแต่ละรายการที่เกิดขึ้นภายในหนึ่งปี (ความถี่ของภัยคุกคาม) กับการสูญเสียทางการเงินที่อาจเกิดขึ้นที่เกี่ยวข้องกับแต่ละเหตุการณ์ (Loss Magnitude) เป็นต้น อย่างไรก็ตาม การประเมินเชิงคุณภาพจะมีความเหมาะสมมากกว่าในบางกรณี โดยเฉพาะอย่างยิ่งสำหรับสินทรัพย์ที่มีมูลค่าสูงและไม่มีประวัติการโจมตีมาก่อน การประเมินเหล่านี้อาศัยการวิเคราะห์ที่ขับเคลื่อนด้วยสถานการณ์ โดยที่ทีมประเมินภัยคุกคามจะพัฒนาสถานการณ์ตามลักษณะของภัยคุกคามและสินทรัพย์ โดยกำหนดค่าทางภาษาเพื่อประเมินความเป็นไปได้ของการโจมตี แนวทางนี้มีความสำคัญอย่างยิ่งในการประเมินภัยคุกคามด้วยข้อมูลทางประวัติศาสตร์เพียงเล็กน้อย เช่น จาก

อาวุธทำลายล้างสูง (WMD) ซึ่งประกอบด้วยอาวุธเคมี ชีวภาพ และนิวเคลียร์ และเนื่องจากมีเหตุการณ์ทางประวัติศาสตร์ที่มีการใช้อาวุธประเภทนี้น้อยมาก จึงจำเป็นต้องมีการประเมินเชิงคุณภาพ



ภาพ 3.5 แตกต่างจากการประเมินเชิงคุณภาพซึ่งใช้วิจารณญาณเชิงอัตวิสัยเพื่อประเมินภัยคุกคาม การประเมินเชิงปริมาณจะใช้ข้อมูลภววิสัยและวัดผลได้ แนวทางนี้มีการรวมค่าตัวเลขเข้ากับความเสี่ยง เช่น ต้นทุนทางการเงิน เวลา หรือทรัพย์สินที่สูญหาย (Evrin, 2021)

กระบวนการประเมินภัยคุกคามยังเป็นกระบวนการที่เกี่ยวข้องกับการทำซ้ำอย่างต่อเนื่อง เนื่องจากระดับภัยคุกคามอาจผันผวนเมื่อเวลาผ่านไปตามข้อมูลใหม่หรือการเปลี่ยนแปลงในภาพรวมภัยคุกคาม ตัวอย่างเช่น วันครบรอบการโจมตีของผู้ก่อการร้ายอาจทำให้ระดับภัยคุกคามเพิ่มขึ้นชั่วคราว นอกจากนี้ การเกิดขึ้นของภัยคุกคามใหม่ ๆ และความสามารถที่เปลี่ยนแปลงไปของฝ่ายตรงข้ามจำเป็นต้องอาศัยการเฝ้าระวังและการอัปเดตกลยุทธ์ด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง เพื่อบรรเทาภัยคุกคามเหล่านี้อย่างมีประสิทธิภาพ ผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยต้องใช้กรอบแนวคิดคิดที่คล้ายกันกับของฝ่ายตรงข้าม โดยเข้าใจวิธีการและแรงจูงใจในการคาดการณ์และต่อต้านการโจมตีที่อาจเกิดขึ้น แนวทางการประเมินภัยคุกคามแบบพลวัตนี้ช่วยให้มั่นใจได้ว่ามาตรการรักษาความมั่นคงปลอดภัยยังคงมีความเกี่ยวข้องและมีประสิทธิภาพเมื่อเผชิญกับความเสี่ยงที่เปลี่ยนแปลง

พลวัตของภัยคุกคามในปัจจุบัน (Dynamic of Emerging Threats)

เนื่องจากลักษณะของภัยคุกคามมีการพัฒนาเปลี่ยนแปลงอย่างต่อเนื่อง การประเมินภัยคุกคามที่แม่นยำจึงเป็นสิ่งที่ขาดไม่ได้สำหรับผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัย แม้ว่าการประเมินภัยคุกคามที่ครอบคลุมจะเป็นรากฐานที่สำคัญ แต่ก็ไม่สามารถคาดการณ์สถานการณ์ที่อาจเกิดขึ้นได้ทั้งหมด เนื่องจากผู้ไม่หวังดีจะปรับตัวอย่างต่อเนื่องเพื่อเอาชนะมาตรการรักษาความมั่นคงปลอดภัย ในภูมิทัศน์ทางเทคโนโลยีที่ก้าวหน้าอย่างรวดเร็วของโลกปัจจุบัน มาตรการตอบโต้มีความล้าสมัยเร็วขึ้นกว่าที่เคย ทำให้ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจำเป็นต้องรับทราบข้อมูลเกี่ยวกับภัยคุกคามล่าสุด สิ่งนี้เกี่ยวข้องกับการไม่เพียงแต่ใช้แหล่งข้อมูลที่มีอยู่ทั้งหมดเท่านั้น แต่ยังขยายออกไปทุกที่ ๆ เป็นไปได้ เพื่อให้แน่ใจว่ามีความเข้าใจล่าสุดเกี่ยวกับศักยภาพของทรัพยากรที่มีอยู่

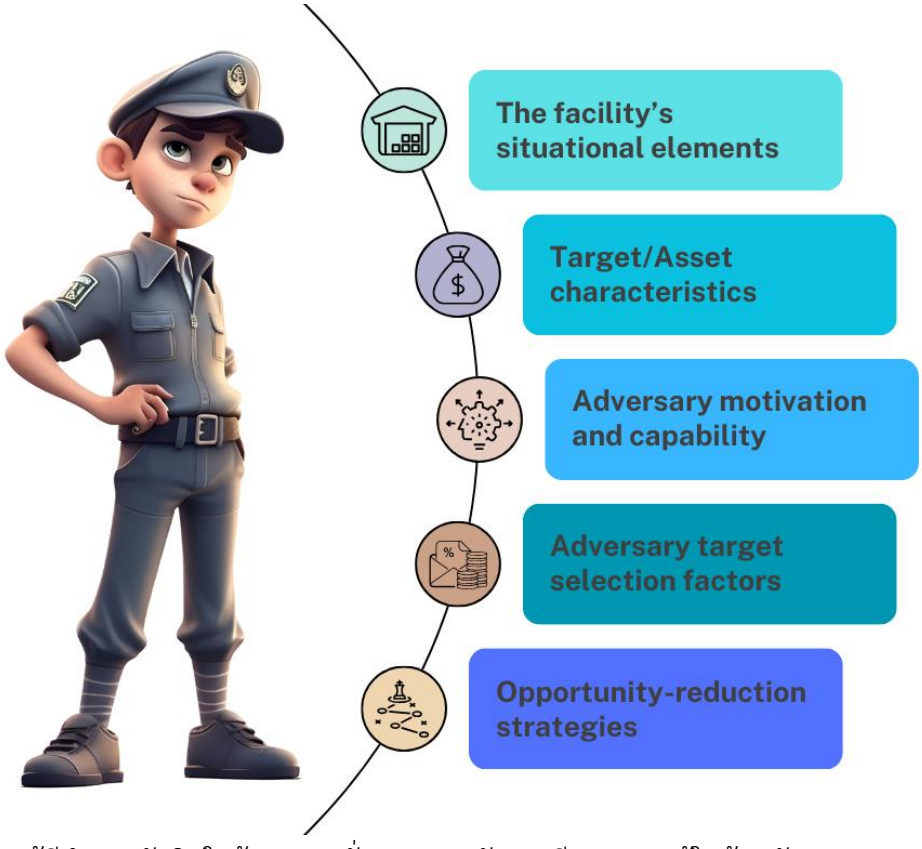
สิ่งสำคัญอย่างหนึ่งในการจัดการกับภัยคุกคามที่เกิดขึ้นคือความสามารถในการคิดเหมือนศัตรูหรือฝ่ายตรงข้าม การทำความเข้าใจวิธีการดำเนินการในอดีตของฝ่ายตรงข้ามให้ข้อมูลเชิงลึกที่มีคุณค่าเกี่ยวกับการกระทำที่อาจเกิดขึ้นในอนาคต อย่างไรก็ตาม การนำแนวคิดของอาชญากรหรือผู้ก่อการร้ายมาใช้ให้เป็นประโยชน์ ช่วยให้ผู้มีอำนาจตัดสินใจด้านความปลอดภัยสามารถคาดการณ์ภัยคุกคามที่แปลกใหม่ นอกเหนือจากกระบวนทัศน์ด้านความมั่นคงปลอดภัยในปัจจุบัน แนวทางเชิงรุกนี้มีความสำคัญในการระบุและลดความเสี่ยงที่ยังไม่พบ

นอกจากนี้ การจัดทำข้อมูลของผู้ประสงค์ร้าย (profiling) ให้ทันสมัยถือเป็นสิ่งสำคัญ โดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยควรตระหนักถึงกลยุทธ์และวิธีการของฝ่ายตรงข้ามที่กำลังพัฒนาที่ประกอบไปด้วย ความคิดสร้างสรรค์ ความสามารถในการปรับตัว และความซับซ้อน องค์ความรู้นี้ช่วยในการปรับปรุงการประเมินภัยคุกคามอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการรักษาความมั่นคงปลอดภัยมีประสิทธิภาพต่อภัยคุกคามในปัจจุบันและที่เกิดขึ้นใหม่ ด้วยการทำความเข้าใจต่อเป้าหมาย แรงจูงใจ และความสามารถของฝ่ายตรงข้าม ผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยสามารถรักษาการประเมินภัยคุกคามที่เกี่ยวข้องและมีประสิทธิภาพได้

พลวัตของภัยคุกคามภายในการจัดการความมั่นคงปลอดภัยมุ่งเน้นไปที่ลักษณะของภัยคุกคามที่องค์กรเผชิญอยู่และกลยุทธ์ที่ใช้ในการบรรเทาผลกระทบ พลวัตเหล่านี้ได้รับอิทธิพลจากปัจจัยหลายอย่างรวมกัน ประกอบไปด้วย เจตนา ความสามารถ และแรงจูงใจของภัยคุกคามที่เกิดขึ้นทั้งจากโดยมนุษย์หรือโดยธรรมชาติ การทำความเข้าใจองค์ประกอบเหล่านี้เป็นสิ่งสำคัญสำหรับการพัฒนามาตรการและการประเมินความมั่นคงปลอดภัยที่มีประสิทธิภาพ

ทั้งนี้ ภัยคุกคามจากมนุษย์ ทั้งภายใน ภายนอก หรือทั้งสองอย่างรวมกัน เป็นความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง แรงจูงใจ และศักยภาพในการทำให้เกิดความเสียหาย ในขณะที่ภัยคุกคามทางธรรมชาติ เช่น ภัยพิบัติด้านสิ่งแวดล้อม ก็จำเป็นต้องพิจารณาด้วยการประเมินความเสี่ยงที่ครอบคลุมด้วยเช่นกัน ความสามารถในการประเมินและปรับตัวเข้ากับภัยคุกคามที่เป็นพลวัตเหล่านี้ถือเป็น

ลักษณะพื้นฐานของการจัดการความมั่นคงปลอดภัยเชิงกลยุทธ์ ซึ่งใช้ข้อมูลในอดีตและแบบปัจจุบัน (real-time data) เพื่อประเมินความเสี่ยงและกำหนดมาตรการรับมือ แนวทางนี้ครอบคลุมถึงการระบุตัวข้ามฝ่ายตรงข้าม การพิจารณาความสามารถของฝ่ายตรงข้าม และการใช้มาตรการความปลอดภัย (security protocols) แบบกำหนดเป้าหมายตามภัยคุกคามที่ประเมิน เป้าหมายคือการปกป้องทรัพย์สินขององค์กรโดยการทำความเข้าใจและลดความเสี่ยงที่เกิดจากทั้งจากมนุษย์และเหตุการณ์ทางธรรมชาติ เพื่อให้มั่นใจในความมั่นคงปลอดภัยและความสมบูรณ์ของการดำเนินงานและทรัพย์สินขององค์กร



ภาพ 3.6 ผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยควรมีความรอบรู้ในด้านภัยคุกคามครบทุกมิติข้อมูลก่อนที่จะเลือกมาตรการรับมือให้ถูกต้องกับสถานการณ์ (Vellani, 2021)

องค์ประกอบสถานการณ์ (Situational elements) คือคุณลักษณะของสถานที่ ๆ สร้างสภาพแวดล้อมที่เอื้อต่อการก่ออาชญากรรมหรือการละเมิดความปลอดภัยบางประเภท ตัวอย่างเช่น บ้านพักคนชราอาจได้รับความเดือดร้อนจากการลักเล็กขโมยน้อยมากกว่าการโจรกรรมรถยนต์ อีกตัวอย่างหนึ่งขององค์ประกอบสถานการณ์ที่ส่งผลกระทบต่ออาชญากรรมอาจเป็นความใกล้ชิดของสถานที่กับเส้นทางหลบหนี เช่น ทุ่งหญ้าหนาแน่นหรือพื้นที่ป่าที่สามารถปกปิดซ่อนเร้นผู้กระทำความผิดด้วยการเดินเท้า หรือการหลบหนีอย่างรวดเร็วผ่านทางหลวงโดยอาชญากรใช้ยานยนต์ในการ

หลบหนี องค์ประกอบสถานการณ์ยังรวมถึงลักษณะของกิจกรรมในทรัพย์สินด้วย ธุรกิจต้องเผชิญกับปัญหาที่แตกต่างจากพื้นที่ที่อยู่อาศัย ประเภทธุรกิจที่ดำเนินการเกี่ยวกับทรัพย์สินอาจดึงดูดอาชญากรรมได้มากขึ้น ตัวอย่างเช่น บาร์และไนต์คลับอาจมีแนวโน้มที่จะมีการก่ออาชญากรรมประเภททำร้ายร่างกายและล่วงละเมิดทางเพศมากกว่าธุรกิจประเภทอื่น เนื่องจากการบริโภคเครื่องดื่มแอลกอฮอล์จะทำให้ความยับยั้งชั่งใจลดลง เป็นต้น

ลักษณะของเป้าหมาย (Target characteristics) มักจะถูกกำหนดโดยลักษณะของธุรกิจ ร้านขายเครื่องประดับมีสินทรัพย์ที่น่าดึงดูดสองประเภท ได้แก่ เงินจำนวนมาก และทรัพย์สินขนาดเล็กที่ง่ายต่อการปกปิด บางครั้งลักษณะของเป้าหมายก็ปรากฏชัดในตัวเอง ตัวอย่างเช่น ธนาคารมีเป้าหมายที่เป็นความกังวลหลักคือเงินสดที่เก็บไว้สาขา ในขณะที่เป้าหมายที่เป็นความกังวลหลักของร้านค้าปลีกคือการขโมยของในร้าน ในขณะที่ แรงจูงใจและความสามารถของฝ่ายตรงข้าม (Adversary motivation and capability) เป็นกุญแจสำคัญในการทำความเข้าใจธรรมชาติของอาชญากรรมในทรัพย์สิน ทั้งนี้ อาชญากรสามารถตัดสินใจอย่างมีเหตุและผลได้ด้วยตัวเองในการเลือกที่จะกระทำหรือหลีกเลี่ยงในการก่ออาญชากรรม อีกทั้ง ในกระบวนการยุติธรรมทางอาญาสมัยใหม่นั้น เป็นที่ยอมรับกันอย่างกว้างขวางว่าโดยทั่วไปแล้วว่าสามารถลดแรงจูงใจในการกระทำความผิดของบุคคลได้หากมีบทลงโทษที่รวดเร็วและรุนแรง ด้วยเหตุนี้ มาตรการป้องกันจึงสามารถดำเนินการได้ในระดับทรัพย์สินโดยการใช้มาตรการตอบโต้ที่เพิ่มความเสี่ยงในการตรวจจับโดยเจ้าหน้าที่รักษาความปลอดภัย ตัวอย่างเช่น การปรากฏตัวของสุนัขรักษาความปลอดภัยหรือระบบกล้องวงจรปิด (CCTV) ซึ่งเป็นอุปสรรคต่อผู้ที่คิดจะกระทำความผิด ในทำนองเดียวกัน หากความเสี่ยงในการถูกตรวจจับอยู่ในระดับต่ำก็จะเป็นการกระตุ้นให้ผู้กระทำความผิดก่ออาชญากรรม อย่างไรก็ตาม ก็จะต้องพิจารณาความสามารถของฝ่ายตรงข้ามด้วย เนื่องจากอาชญากรแต่ละคนมีอาจมีความสามารถในการหลีกเลี่ยงสุนัขรักษาความปลอดภัย อาทิ การใช้ขนมวางยาพิษหรือวิธีการเบี่ยงเบนความสนใจที่แตกต่างกัน ด้วยเหตุนี้ เป้าหมายของผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยคือการลดองค์ประกอบที่เพิ่มความเสี่ยง ตัวอย่างเช่น การซ่อนทรัพย์สินไว้ในตู้นิรภัยเป็นวิธีที่ดีในการทำให้สิ่งของมีค่าไม่ดึงดูดความสนใจหรือล่อตาล่อใจ

โดยทั่วไป หลักการในการเลือกเป้าหมาย (Adversary target selection factors) ของอาชญากรคือการเลือกเป้าหมายที่ง่ายที่สุดที่จะให้ผลตอบแทนสูงสุด สถานที่ให้บริการที่เปิดกว้างจะเป็นเป้าหมายที่ดึงดูดใจสำหรับอาชญากร อาทิ พื้นที่ของมหาวิทยาลัย เนื่องจากเป็นเป้าหมายโดยที่มีสภาพแวดล้อมแบบเปิด เข้าถึงได้ง่าย และมีมาตรการรักษาความปลอดภัยที่ไม่ค่อยแน่นหนาเนื่องจากไม่ต้องการสร้างอุปสรรคต่อเป้าหมายหลักด้านการศึกษาของสถาบัน หรืออาชญากรอาจเลือกเป้าหมายที่ผลตอบแทนสูง ตัวอย่างเช่น ห้างสรรพสินค้าเป็นเป้าหมายในการโจรกรรมรถยนต์ได้อย่างดีแก่อาชญากรที่เชี่ยวชาญเรื่องการขโมยรถยนต์ ทั้งนี้ ปัจจัยหลักในการเลือกเป้าหมายส่วนใหญ่มาจาก ‘โอกาส’ ดังนั้น เป้าหมายของผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยคือการลด ‘โอกาส’ ที่จะเกิดอาชญากรรมในสถานประกอบการ นั่นเอง

กลยุทธ์การลดโอกาส (Opportunity-reduction strategies) เกี่ยวข้องกับลักษณะของสถานที่ ๆ ทำให้เกิดการส่งเสริมหรือยับยั้งอาชญากรรม เนื่องจากสิ่งอำนวยความสะดวกของสถานที่แต่ละแห่งมีความแตกต่างกัน ทำให้ประสิทธิภาพของกลยุทธ์ในการรักษาความมั่นคงปลอดภัยมีความแตกต่างกัน ทั้งนี้ ขึ้นอยู่กับลักษณะเฉพาะและภัยคุกคามที่เป็นเอกลักษณ์ของตัวเอง กลยุทธ์ที่ใช้ได้ผลในโรงงานแห่งหนึ่งอาจไม่สามารถใช้ได้กับโรงงานลักษณะเดียวกันในพื้นที่ทางภูมิศาสตร์อื่น ๆ กลยุทธ์การลดโอกาสอาจอยู่ในรูปแบบของนโยบายและขั้นตอนที่ได้รับการปรับปรุง มาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ หรือเจ้าหน้าที่รักษาความปลอดภัย แม้ว่าทั้งหมดที่กล่าวมาอาจฟังดูเป็นหลักการพื้นฐานเท่าไป แต่ถ้าจะยกตัวอย่างให้เข้าใจ ก็สามารถกล่าวได้ว่า กลยุทธ์พื้นฐานประการหนึ่งในการลดโอกาสในการทิ้งขยะมูลฝอยก็คือการติดตั้งถังขยะ

จากที่กล่าวมาทั้งหมด การจัดการภัยคุกคามที่มีประสิทธิภาพเกี่ยวข้องกับการประเมินอย่างสม่ำเสมอเพื่อปรับให้เข้ากับการเปลี่ยนแปลงที่เป็นพลวัต โดยเน้นถึงความสำคัญของความยืดหยุ่นและความสามารถในการปรับตัวในกลยุทธ์ด้านความปลอดภัย ด้วยการตระหนักถึงธรรมชาติของภัยคุกคามที่เปลี่ยนแปลงไป ทำให้องค์กรต่าง ๆ สามารถจัดลำดับความสำคัญของทรัพยากรได้อย่างมีประสิทธิภาพ โดยมุ่งเน้นไปที่ความเสี่ยงที่มากที่สุด และใช้มาตรการรักษาความปลอดภัยที่ปรับให้เหมาะสม แนวทางการจัดการภัยคุกคามแบบเป็นพลวัตนี้มีความสำคัญอย่างยิ่งต่อการรักษาสภาพแวดล้อมที่ปลอดภัยเมื่อเผชิญกับความท้าทายที่คาดเดาได้และคาดไม่ถึง

บทสรุป

บทนี้มุ่งเน้นไปที่การประเมินภัยคุกคาม ซึ่งเป็นขั้นตอนสำคัญต่อจากการระบุสินทรัพย์และมาตรการรักษาความปลอดภัยภายในองค์กร ภัยคุกคามอาจเกิดจากมนุษย์หรือโดยธรรมชาติ เป็นการกระทำหรือเหตุการณ์ที่อาจเกิดขึ้นจากการใช้ประโยชน์จากช่องโหว่เพื่อสร้างความเสียหายหรือทำลายทรัพย์สิน การประเมินภัยคุกคามต้องวิเคราะห์เจตนา แรงจูงใจ และความสามารถในการโจมตี ยิ่งไปกว่านั้นต้องวิเคราะห์ว่าเป็นภัยคุกคามภายใน (บุคคลภายใน เช่น พนักงานหรือผู้รับเหมา) หรือภายนอก (บุคคลภายนอกหรือทั้งสองอย่างรวมกัน) กระบวนการประเมินภัยคุกคามเกี่ยวข้องกับการประเมินความเป็นไปได้ของเหตุการณ์ไม่พึงประสงค์ เช่น การก่อการร้าย อาชญากรรม และภัยพิบัติทางธรรมชาติ และผลกระทบต่อการดำเนินธุรกิจและทรัพย์สิน โดยเน้นย้ำถึงความสำคัญของข้อมูลในอดีตรวมกับข้อมูลแบบปัจจุบันเพื่อการประเมินเชิงปริมาณหรือเชิงคุณภาพที่แม่นยำ ในการใช้จัดลำดับความสำคัญของมาตรการรักษาความปลอดภัยอย่างมีประสิทธิภาพ ทั้งนี้ องค์กรต่าง ๆ โดยเฉพาะองค์กร ประเมินภัยคุกคามเป็นประจำทุกปี เพื่อปรับมาตรการรักษาความปลอดภัยโดยทันที ความล้มเหลวในการระบุภัยคุกคามอาจนำไปสู่การจัดสรรทรัพยากรที่ไม่มีประสิทธิภาพและเพิ่มภาระทางการเงิน ด้วยการประเมินภัยคุกคามที่ครอบคลุม ซึ่งรวมถึงการระบุและการจำแนกประเภท

ของภัยคุกคาม การประเมินแรงจูงใจของฝ่ายตรงข้าม และการวิเคราะห์ความสามารถ องค์กรต่าง ๆ สามารถพัฒนากลยุทธ์ด้านความปลอดภัยที่ตรงเป้าหมายและมีประสิทธิภาพเพื่อลดความเสี่ยง

คำถามท้ายบท

1. ภัยคุกคามหลักสองประเภทคืออะไร? และมีความแตกต่างกันอย่างไร?
2. อธิบายความสำคัญของความแตกต่างระหว่างภัยคุกคามกับฝ่ายตรงข้ามในบริบทการจัดการความมั่นคงปลอดภัย?
3. กระบวนการประเมินภัยคุกคามมีความสำคัญในการกำหนดกลยุทธ์การรักษาความมั่นคงปลอดภัยขององค์กรอย่างไร?
4. อธิบายถึงบทบาทของข้อมูลในอดีตและข้อมูลปัจจุบันในการประเมินภัยคุกคาม?
5. เหตุใดการประเมินภัยคุกคามประจำปีจึงมีความสำคัญสำหรับธุรกิจ และผลที่อาจเกิดขึ้นจากการไม่ระบุภัยคุกคามในการประเมินคืออะไร?

เอกสารอ้างอิง

Evrin, V. (2021, April 28). Risk Assessment and Analysis Methods: Qualitative and Quantitative. *ISACA Journal, 2*, 1-6. Retrieved from https://www.isaca.org

Fennelly, L. J. (2017). *Effective Physical Security* (5th ed.). Cambridge, MA: Butterworth-Heinemann.

Schuler, M. (2016, December 23). *Sea Shepherd Finds Japanese Whaling Fleet in Southern Ocean*. Retrieved from gCaptain: https://gcaptain.com

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *Special Publication (NIST SP)*. doi:10.6028/nist.sp.800-30

Vellani, K. (2021). *Strategic Security Management: A Risk Assessment Guide for Decision Makers* (2nd ed.). Boca Raton: FL: CRC Press.