Unit 2

สินทรัพย์และมาตรการ รักษาความมั่นคงปลอดภัย

บทที่ 2

สินทรัพย์และมาตรการรักษาความมั่นคงปลอดภัย

บทนำ

โปรแกรมการรักษาความมั่นคงปลอดภัยโดยทั่วไปนั้น ถูกออกแบบมาเพื่อปกป้องทรัพย์สิน โดยเฉพาะทรัพย์สินมีค่า โดยบทนี้จะกล่าวถึงแนวคิดของสินทรัพย์และการระบุสินทรัพย์ (Asset Identification) นอกจากนี้จะกล่าวถึงการวิเคราะห์ผลกระทบความรุนแรงจากการที่สินทรัพย์เกิดความเสียหาย ถูกทำลาย หรือโจรกรรม หลักในการพิจารณาอย่างเหมาะสมว่าทรัพย์สินใดต้องการการปกป้องคุ้มครองซึ่งเป็นขั้นตอนแรกที่ต้องปฏิบัติในกระบวนการการจัดการความเสี่ยง เพราะถ้าหากไม่มีการระบุสินทรัพย์ มาตรการการรักษาความมั่นคงปลอดภัยจะถูกเลือกปฏิบัติและปรับใช้อย่างหละหลวมและสุ่มเสี่ยง

การจัดประเภทสินทรัพย์

สินทรัพย์คืออะไร? สินทรัพย์ (Asset) เป็นสิ่งที่มีค่าสำหรับองค์กร ตั้งแต่ระดับพื้นฐานไปจนถึงภารกิจที่สำคัญ สินทรัพย์ที่สำคัญต่อภารกิจขององค์กรมีความสำคัญเป็นอันดับแรกสำหรับการกำหนดโปรแกรมการรักษาความมั่นคงปลอดภัย โดยทั่วไป สินทรัพย์ประกอบด้วยบุคคล ทรัพย์สิน และข้อมูล ทั้งนี้ ทุกองค์กรจำเป็นต้องมีทรัพย์สินที่สำคัญในการดำเนินภารกิจและหน้าที่หลัก

Karim Vellani (2021) อธิบายไว้ว่า สินทรัพย์ ประกอบไปด้วย บุคคล ทรัพย์สิน และข้อมูล บุคคลอาจรวมถึงพนักงาน ลูกค้า และบุคคลอื่นที่มีความเกี่ยวข้องกับลูกค้า เช่น ผู้รับเหมาหรือผู้มาติดต่อทำธุรกรรม สินทรัพย์ที่เป็นทรัพย์สิน (Property) ประกอบด้วยวัตถุที่มีรูปร่าง (Tangible) และไม่มีรูปร่าง (Intangible) ที่สามารถกำหนดมูลค่าได้ สินทรัพย์ที่ไม่มีรูปร่างนั้นรวมถึงชื่อเสียงและข้อมูลที่เป็นกรรมสิทธิ์ ลิขสิทธิ์ สิทธิบัตร ข้อมูลอาจรวมถึงฐานข้อมูล รหัสซอฟต์แวร์ บันทึกสำคัญของบริษัท และรายการที่จับต้องไม่ได้อื่น ๆ

สินทรัพย์บุคคล หมายถึง สินทรัพย์ที่อาจรวมถึงพนักงาน ลูกค้า และบุคคลที่ได้รับเชิญอื่น ๆ เช่น ผู้รับเหมาหรือแขก ยกตัวอย่างเช่น ในโรงงานอุตสาหกรรมสารเคมี พนักงานและผู้รับเหมาคือคนที่ต้องการการปกป้องจากภัยคุกคามต่าง ๆ รวมถึงการรั่วไหลของสารเคมีและการระเบิดไปจนถึงภัยธรรมชาติ ในทางกลับกัน ในสถานประกอบการ เช่น โรงแรม พนักงานและแขกที่เข้าพัก ถือเป็น

ทรัพย์สินบุคคล เพราะหากไม่มีพนักงาน โรงแรมก็จะดำเนินกิจการไม่ได้ และหากไม่มีแขก โรงแรมก็ไม่สามารถตอบสนองวัตถุประสงค์ที่ตั้งใจไว้ได้

สินทรัพย์ที่เป็นทรัพย์สินขององค์กรนั้น อาจประกอบด้วยทรัพย์สินที่มีตัวตนจับต้องได้และไม่มีตัวตน เป็นที่แน่นอนว่าสินทรัพย์ที่มีตัวตนมักจะระบุและกำหนดมูลค่าได้ง่าย ในขณะที่สินทรัพย์ที่ไม่มีตัวตนนั้นยากต่อการระบุตัวตนและกำหนดมูลค่า สินทรัพย์ที่มีตัวตนอาจเป็นสินทรัพย์ถาวรที่มีอายุการใช้งานมากกว่าหนึ่งปี เช่น โรงงาน อุปกรณ์ และอาคาร ในขณะที่สินทรัพย์ที่ไม่มีตัวตนนั้น อาจรวมถึงชื่อเสียงขององค์กรและข้อมูลที่เป็นกรรมสิทธิ์ซึ่งรวมถึงสิทธิบัตร เครื่องหมายการค้า ลิขสิทธิ์ และค่าความนิยม (Goodwill) อย่างไรก็ตาม แม้ว่าสินทรัพย์ที่เป็นทรัพย์สินทั้งหมดจะมีมูลค่า แต่ไม่ได้หมายความว่าทรัพย์สินทั้งหมดมีความสำคัญต่อภารกิจขององค์กร (Barone, 2022)

ข้อมูลเป็นทรัพย์สินที่มีความสำคัญมากในปัจจุบันและมีความแตกต่างเฉพาะขึ้นอยู่กับประเภทขององค์กร สินทรัพย์ข้อมูลอาจรวมถึงฐานข้อมูล รหัสซอฟต์แวร์ และบันทึกทางการเงินของบริษัท ข้อมูลที่เป็นกรรมสิทธิ์ เช่น บันทึกสำคัญ (records) สูตร (formulas) และวิธีการ (methods) ถือเป็นสินทรัพย์ บันทึกของบริษัทที่สำคัญอาจรวมถึงใบรับรองการจัดตั้งบริษัท บันทึกหุ้นส่วน รายงานการประชุมของบริษัท และบันทึกทางการเงินบางรายการ เป็นต้น

สินทรัพย์ที่สำคัญ

การระบุสินทรัพย์ที่สำคัญ (Critical Asset) ขององค์กรเป็นขั้นตอนแรกในการจัดการความเสี่ยง ทรัพย์สินที่สำคัญในประเทศที่มีการพัฒนาด้านอุตสาหกรรม ได้แก่ พลังงานไฟฟ้า การผลิตก๊าซและน้ำมัน การโทรคมนาคม การธนาคารและการเงิน ระบบน้ำประปา ระบบการขนส่ง การดำเนินงานของรัฐบาล และบริการฉุกเฉิน ในขณะที่ ทรัพย์สินที่สำคัญทางธุรกิจคือ ‘ทรัพย์สินที่จำเป็นในการปฏิบัติภารกิจหลักของธุรกิจ’ สินทรัพย์ประเภทนี้ถือว่ามีความสำคัญมาก โดยพิจารณาจากปัจจัยหลักสองประการ คือ (1) มูลค่าที่กำหนดโดยองค์กร และ (2) ผลที่ตามมาในระยะสั้นและระยะยาวต่อการดำเนินธุรกิจเนื่องจากการสูญหาย เสียหาย หรือถูกทำลาย

ทรัพย์สินที่สำคัญของธุรกิจคือทรัพย์สินที่จำเป็นสำหรับการดำเนินธุรกิจอย่างต่อเนื่องและต้องการการปกป้อง แต่สำหรับรัฐบาลของประเทศใดประเทศหนึ่งนั้น สินทรัพย์ที่สำคัญจะค้ำจุนเศรษฐกิจ ความมั่นคง ภูมิทัศน์ทางการเมือง และบริการทางสังคม โดยปกติแล้ว สินทรัพย์จะมีมูลค่าไม่เท่ากับการดำเนินธุรกิจ ไม่ว่าสินทรัพย์ที่สำคัญขององค์กรใดก็ตาม จะต้องประเมินมูลค่าสำหรับแต่ละสินทรัพย์ และสินทรัพย์แต่ละรายการต้องได้รับการจัดลำดับความสำคัญตามผลที่ตามมาของการสูญเสียเนื่องจากการกระทำของมนุษย์ ตัวอย่างเช่น ในอุตสาหกรรมน้ำมันและก๊าซ ท่อส่งน้ำมันและก๊าซถือเป็นทรัพย์สินที่สำคัญ เนื่องจากความเสียหายหรือการสูญเสียใด ๆ ของท่อส่งน้ำมันจะส่งผลกระทบต่อประสิทธิภาพของความพร้อมของโรงกลั่นเพื่อดำเนินการผลิตต่อไป

ภาพ 2.1 จากเหตุการณ์น้ำมันรั่วไหลนอกชายฝั่ง บริษัท BP ต้องจ่ายเงินกว่า 65,000 ล้านเหรียญสหรัฐ จากโทษทั้งทางอาญาและทางแพ่งสำหรับความเสียหายทางทรัพยากรธรรมชาติ ทางเศรษฐกิจ และการทำความสะอาด (Vaughan, 2018)

การปกป้องทรัพย์สินเป็นเป้าหมายหลักของโปรแกรมรักษาความมั่นคงปลอดภัยใด โดยสินทรัพย์นั้นมีทั้งมูลค่าที่จับต้องได้และไม่สามารถจับต้องได้ โดยสามารถประเมินมูลค่าในเชิงปริมาณได้โดยใช้องค์ประกอบดังต่อไปนี้

1. ความสำคัญของสินทรัพย์ต่อการดำเนินธุรกิจ
2. มูลค่าทดแทน (Replacement value)
3. มูลค่าสัมพัทธ์ของสินทรัพย์ (Relative value of the asset)

ภาวะวิกฤตเป็นหน้าที่ของผลกระทบในการปฏิบัติงานต่อภารกิจขององค์กร เนื่องจากการสูญหาย เสียหาย หรือถูกทำลายของสินทรัพย์ ยิ่งสินทรัพย์มีผลกระทบต่อการดำเนินธุรกิจมากเท่าไหร่ก็ยิ่งมีความสำคัญมากขึ้นเท่านั้น ยิ่งไปกว่านั้น เกณฑ์การประเมินระดับวิกฤตควรมีความเฉพาะเจาะจง อาทิ สินทรัพย์มีผลกระทบต่อการดำเนินงานเพียงบางส่วนหรือทั่วทั้งบริษัท? หรือการเกิดความสูญเสีย ความเสียหาย หรือการถูกทำลายของสินทรัพย์จะส่งผลกระทบต่อการอยู่รอดของบริษัท ตัวอย่างเช่น ในอุตสาหกรรมน้ำมัน ท่อส่งเป็นทรัพย์สินที่สำคัญ อย่างไรก็ตาม มูลค่าการผลิตน้ำมันและก๊าซจะแตกต่างกันไป ท่อส่งบางจุดมีความสำคัญกว่าบางจุดขึ้นอยู่กับปริมาณน้ำมันที่ส่งผ่านแตกต่างกัน

สินทรัพย์ถูกจัดประเภทตามระดับความสำคัญ ซึ่งอาจเป็นการประเมินเชิงปริมาณตามมูลค่าที่แท้จริงหรือผลกระทบต่อการดำเนินธุรกิจจากการสูญหาย เสียหาย หรือถูกทำลาย ระดับวิกฤตที่ถึงแม้ว่าการประเมินสินทรัพย์เป็นตัวเลขเป็นเรื่องที่ซับซ้อน แต่มีความสำคัญมากต่อการประเมินความเสี่ยงโดยรวม อีกทางหนึ่ง การประเมินเชิงคุณภาพสามารถทำได้โดยการจัดลำดับสินทรัพย์ในระดับสัมพัทธ์ เช่น สูง ปานกลาง หรือต่ำ ค่าเชิงพรรณนา เช่น ระดับภัยพิบัติ (catastrophic) ระดับวิกฤต (critical) ระดับเล็กน้อย (marginal) ระดับไม่สำคัญ (negligible) อาจใช้เพื่อทำความเข้าใจมูลค่าสัมพัทธ์ของการดำเนินธุรกิจ ด้วยเหตุนี้ การใช้เมทริกซ์ประเมินทรัพย์สินที่สำคัญอาจเป็นประโยชน์ในการทำความเข้าใจลักษณะสัมพัทธ์ของการสูญเสีย ความเสียหาย และการทำลายทรัพย์สิน

สำหรับการวางแผนความต่อเนื่องทางธุรกิจที่มีประสิทธิภาพ ผู้มีอำนาจตัดสินใจด้านความปลอดภัยควรพิจารณาผลกระทบที่อาจเกิดขึ้นในทันทีของการสูญเสียสินทรัพย์ รวมถึงเวลาและต้นทุนในการเปลี่ยนสินทรัพย์ ทั้งนี้ เวลาในการเปลี่ยนทดแทนอาจส่งผลกระทบอย่างมากในระดับวิกฤตเนื่องจากการหยุดทำงานย่อมนำไปสู่การสูญเสียรายได้ ในกรณีที่มีการใช้เวลาที่ในการเปลี่ยนสินทรัพย์ที่สำคัญนานเท่าใด ผลที่ตามมาก็จะยิ่งสูงขึ้นเท่านั้น ในขณะเดียวกัน สินทรัพย์ที่สำคัญบางอย่าง เช่น ข้อมูลดิจิทัล จำเป็นต้องมีการสำรองข้อมูลที่ใช้งานได้อย่างสมบูรณ์ ยิ่งไปกว่านั้น การสูญเสียของสินทรัพย์หนึ่งอาจส่งผลกระทบต่อสินทรัพย์อื่น ๆ อีกด้วย และควรได้รับการพิจารณาในการระบุการวิเคราะห์การวิจารณ์สินทรัพย์โดยรวม ตัวอย่างเช่น ในการเตรียมพร้อมรับมือกับภัยพิบัติทางธรรมชาติ โรงพยาบาลใช้เครื่องกำเนิดไฟฟ้าเพื่อเป็นแหล่งพลังงานสำรองในกรณีที่ไฟฟ้าดับเพื่อช่วยเหลือผู้ป่วยอย่างต่อเนื่อง (Vellani, 2021)

การวิเคราะห์ผลกระทบความรุนแรง

เหตุการณ์ในประวัติศาสตร์บ่งชี้ว่าแนวโน้มการเกิดขึ้นของอาชญากรรมและการก่อการร้ายตลอดจนภัยคุกคามอื่น ๆ มีความสัมพันธ์แบบผกผันกับขนาดของความรุนแรง ความน่าจะเป็นของการโจมตีจะลดลงเมื่อผลกระทบความรุนแรงเพิ่มขึ้น เนื่องจากการโจมตีขนาดเล็กทำได้ง่ายกว่าการโจมตีขนาดใหญ่ ตัวอย่างของการวิเคราะห์ผลกระทบความรุนแรง (Consequence Analysis) อาทิ องค์การก่อการร้ายอัลกออิดะห์ได้ดำเนินการโจมตีเป้าหมายในระดับค่อนข้างเล็กหลายครั้ง ก่อนที่จะมีการโจมตีเมื่อวันที่ 11 กันยายน ซึ่งเป็นการโจมตีขนาดใหญ่ที่มีผลกระทบความรุนแรงสูง

การวิเคราะห์ผลกระทบความรุนแรงเป็นประเมินผลกระทบต่อการดำเนินงานหากสินทรัพย์สูญหาย เสียหาย หรือถูกทำลาย การดำเนินงานอาจรวมถึงการดำเนินธุรกิจหรือการป้องกันประเทศ ด้วยเหตุนี้ การวางแผนความต่อเนื่องทางธุรกิจจะขึ้นอยู่กับการวิเคราะห์ผลที่ตามมา ทั้งนี้ การประมาณความเป็นไปได้และขนาดของการสูญเสียทรัพย์สินที่แม่นยำ จะทำให้ผู้ที่มีอำนาจในการ

ตัดสินใจด้านความมั่นคงปลอดภัยสามารถเตรียมวิธีการต่าง ๆ เพื่อดำเนินงานให้เกิดความต่อเนื่องและฟื้นฟูความสามารถในการปฏิบัติงานหลักขององค์กรได้ ดังนั้น องค์กรจำเป็นต้องเตรียมพร้อมสำหรับการโจมตีที่หลากหลายตามความน่าจะเป็นหรือที่โอกาสจะเกิดขึ้น ในท้ายที่สุด การวิเคราะห์ผลที่กระทบความรุนแรงจะช่วยให้ทีมประเมินความเสี่ยงสามารถจัดลำดับความสำคัญของสินทรัพย์ที่ต้องการการปกป้องคุ้มครอง โดยยึดความสำคัญกับองค์กรเป็นหลัก การวิเคราะห์ผลกระทบความรุนแรงจึงเป็นขั้นตอนพื้นฐานในกระบวนการประเมินความเสี่ยง เนื่องจากองค์กรอาจไม่สามารถให้ความคุ้มครองสินทรัพย์ในระดับการป้องกันเดียวและในเวลาเดียวกันได้ทั้งหมด ดังนั้น การจัดลำดับความสำคัญของสินทรัพย์จะช่วยให้องค์กรสามารถปกป้องสิ่งที่สำคัญที่สุดได้นั่นเอง

ผลกระทบความรุนแรงสามารถแบ่งออกได้หลายประเภท คือ เศรษฐกิจ การเงิน สิ่งแวดล้อม สุขภาพและความปลอดภัย เทคโนโลยี ปฏิบัติงาน และเวลา ตัวอย่างเช่น ศูนย์ควบคุมการปฏิบัติงานที่ทำหน้าที่ควบคุมการผลิตสินค้าหรือผลิตภัณฑ์ให้แล้วเสร็จอย่างปลอดภัย หากเกิดการสูญเสียความสามารถในการควบคุม หรือไม่สามารถทำงานได้อย่างถูกต้อง อาจส่งผลให้การผลิตหยุดชะงัก (เนื่องจากการสูญเสียรายได้และค่าใช้จ่ายเพิ่มเติมที่เกี่ยวข้อง) แต่ยังอาจส่งผลให้เกิดการสูญเสียในชีวิตและทรัพย์สิน หรือความเสียหายต่อสิ่งแวดล้อมหากกระบวนการควบคุมการผลิตเกี่ยวข้องกับวัตถุอันตราย ยิ่งไปกว่านั้น การสูญเสียสินทรัพย์อาจลดความได้เปรียบทางการแข่งขันของบริษัท ไม่เพียงเพราะต้นทุนทางการเงินที่เกี่ยวข้องกับการสูญเสีย แต่ยังเป็นเพราะการสูญเสียความได้เปรียบทางเทคโนโลยี หรือความรู้เฉพาะ หรือข้อมูลที่ยากต่อการทดแทนหรือผลิตซ้ำ

การประเมินความวิกฤต (Criticality Assessment) เป็นกระบวนการที่ถูกออกแบบมาเพื่อระบุและประเมินสินทรัพย์และโครงสร้างพื้นฐานที่สำคัญอย่างเป็นระบบ ตัวอย่างเช่น โรงไฟฟ้านิวเคลียร์ สะพาน และเครือข่ายคอมพิวเตอร์ อาจได้รับการถูกระบุว่าเป็น “วิกฤต” เนื่องจากมีความเกี่ยวข้องกับความมั่นคงของชาติ กิจกรรมทางเศรษฐกิจ และความปลอดภัยสาธารณะ นอกจากนี้ สิ่งอำนวยความสะดวกบางประเภทอาจมีความสำคัญในบางช่วงเวลา ตัวอย่างเช่น สนามกีฬาขนาดใหญ่ ห้างสรรพสินค้า หรืออาคารสำนักงาน เมื่อมีการใช้งานโดยคนจำนวนมาก อาจเป็นเป้าหมายสำคัญต่อการโจมตี แต่อาจมีความสำคัญน้อยเมื่อว่างเปล่า กล่าวได้ว่า การประเมินความวิกฤต มีความสำคัญเนื่องจากเป็นพื้นฐานสำคัญในการระบุว่าทรัพย์สินและโครงสร้างใดมีความสำคัญต่อการปกป้องจากการโจมตี ในท้ายที่สุด การประเมินจะให้ข้อมูลเพื่อจัดลำดับความสำคัญของทรัพย์สินและจัดสรรทรัพยากรเพื่อการดำเนินการป้องกัน โดยการประเมินเหล่านี้ได้พิจารณาปัจจัยต่างๆ เช่น ความสำคัญที่มีต่อการดำเนินการให้บรรลุภารกิจ ความสามารถในการจัดหาขึ้นใหม่เพื่อทดแทน และต้นทุนที่อาจเกิดขึ้นในการซ่อมแซมหรือเปลี่ยนสินทรัพย์

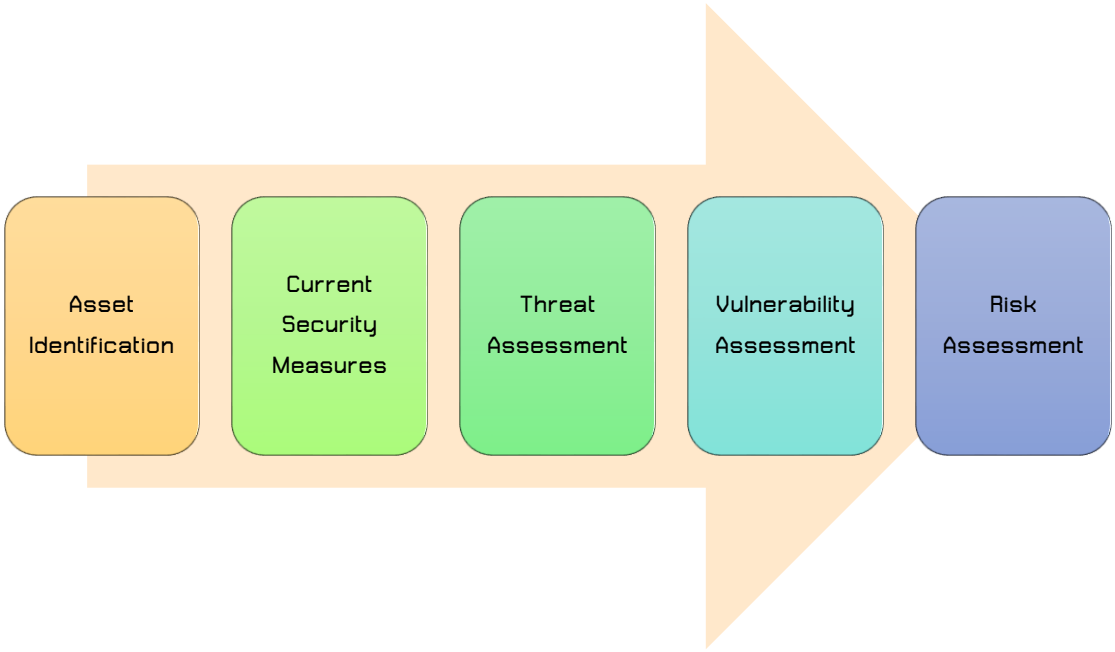
จากบททเรียนข้างต้น จะเห็นได้ว่า การประเมินความวิกฤตที่กล่าวข้างต้นเป็นการประเมินเชิงปริมาณของสินทรัพย์โดยใช้ต้นทุนจริง มูลค่าทดแทน และช่วงหยุดทำงาน ในขณะเดียวกัน เรา

สามารถประเมินความวิกฤตในเชิงคุณภาพได้โดยใช้เงื่อนไขที่เกี่ยวข้องเพื่อจัดลำดับความสำคัญของการสูญเสีย ความเสียหาย หรือการทำลายทรัพย์สิน ดังตาราง 2.1

ตาราง 2.1 *การประเมินความวิกฤตเชิงปริมาณ*	
วิกฤต (Critical)	ทรัพย์สินที่หากสูญหาย เสียหาย หรือถูกทำลาย อาจส่งผลให้การปฏิบัติภารกิจล้มเหลว
สูง (High)	ผลกระทบต่อการดำเนินงานระดับร้ายแรงที่อาจทำให้การดำเนินงานตามปกติเสียหายทั้งหมด หรือเกิดการสูญเสียการดำเนินงานบางส่วนเป็นระยะเวลานาน
กลาง (Medium)	ผลกระทบต่อการดำเนินงานระดับปานกลางที่อาจส่งผลกระทบต่อกระบวนการทางธุรกิจเพียงบางส่วนและในระยะเวลาสั้น ๆ
ต่ำ (Low)	ผลกระทบที่สามารถจัดการได้ ไม่ส่งผลกระทบต่อการดำเนินธุรกิจ และไม่มีความเป็นไปได้ที่จะทำให้ภารกิจล้มเหลว

มาตรการรักษาความมั่นคงปลอดภัย

การระบุสินทรัพย์ (Asset Identification) เป็นขั้นตอนพื้นฐานและเป็นขั้นตอนแรกในการสร้างกลยุทธ์การรักษาความปลอดภัยที่ครอบคลุม โดยเกี่ยวข้องกับการระบุและจัดทำรายการทรัพย์สินที่มีค่าทั้งหมดภายในองค์กรที่ต้องการการคุ้มครองอย่างเป็นระบบ ทรัพย์สินเหล่านี้สามารถจับต้องได้ เช่น อาคาร อุปกรณ์ และเทคโนโลยี หรือจับต้องไม่ได้ เช่น ข้อมูล ทรัพย์สินทางปัญญา และชื่อเสียงของแบรนด์ โดยที่การระบุสินทรัพย์จะเป็นกระบวนการที่ให้ข้อมูลและกำหนดมาตรการรักษาความมั่นคงปลอดภัยในปัจจุบัน โดยการให้ข้อมูลที่จำเป็นเพื่อดำเนินการควบคุมความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ การทำงานร่วมกันระหว่างการระบุสินทรัพย์และมาตรการรักษาความปลอดภัยทำให้มั่นใจได้ว่าองค์กรต่าง ๆ สามารถตอบสนองการแจ้งเตือนด้านความปลอดภัยได้อย่างรวดเร็ว จัดการความยืดหยุ่นด้านความมั่นคงปลอดภัย โดยเชื่อมโยงกับการจัดทำรายการมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่ ที่ได้รับการออกแบบมาเพื่อปกป้องทรัพย์สินในสถานประกอบการหรือองค์กร โดยจะเป็นตัวชี้ให้เห็นว่ามาตรการการรักษาความมั่นคงปลอดภัยที่มีอยู่มีความเหมาะสมหรือไม่เหมาะสมในการปกป้องสิ่งอำนวยความสะดวกและทรัพย์สินที่สำคัญขององค์กร ทั้งนี้ ขึ้นอยู่กับคุณภาพของการประเมินครั้งที่ผ่าน ๆ มาอีกด้วย อย่างไรก็ตาม ถึงแม้ว่าสินทรัพย์และมาตรการป้องกันมีการเปลี่ยนแปลงไปตามกาลเวลา วัตถุประสงค์ของการประเมินความเสี่ยงและการออกแบบโปรแกรมความมั่นคงปลอดภัยก็คือการปกป้องทรัพย์สินนั่นเอง (Shedden, Ahmad, Smith, Tscherning, & Scheepers, 2016)



ภาพ 2.1 กระบวนการการประเมินความเสี่ยง (Threat Analysis Group, 2023)

มาตรการตอบโต้ (Countermeasures) คือการกระทำ อุปกรณ์ ขั้นตอน เทคนิค หรือมาตรการอื่น ๆ ที่นำมาใช้เพื่อลดความเสี่ยงขององค์กร มาตรการเหล่านี้มีความสำคัญอย่างยิ่งในการปกป้องบุคลากร ข้อมูลความลับ ทรัพย์สิน และความพร้อมในการใช้งานของอุปกรณ์และเครื่องมือสำคัญจากภัยคุกคาม รวมถึงการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรมข้อมูล และกิจกรรมที่เป็นอันตรายอื่น ๆ ทั้งนี้ มาตรการรักษาความมั่นคงปลอดภัย อาจรวมถึงเจ้าหน้าที่รักษาความปลอดภัย มาตรการทางกายภาพ นโยบายและระเบียบปฏิบัติ โดยเจ้าหน้าที่รักษาความปลอดภัยนั้น รวมถึงบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าปกป้องทรัพย์สินทั้งโดยตรงและโดยอ้อม โดยปกติ เจ้าหน้าที่รักษาความปลอดภัยในเครื่องแบบจะเป็นตัวอย่างที่ชัดเจนของเจ้าหน้าที่รักษาความปลอดภัย ในขณะที่เจ้าหน้าที่อื่น ๆ ที่อาจมีส่วนร่วมในการป้องกันนั้นอาจรวมถึง เจ้าหน้าที่นอกเครื่องแบบ ผู้จัดการด้านความมั่นคงปลอดภัย ผู้จัดการฝ่ายอาคารสถานที่ และพนักงานทั่วไปที่ได้รับการฝึกอบรมให้รับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัย ทั้งนี้ มาตรการรักษาความมั่นคงปลอดภัยทางกายภาพประกอบไปด้วยอุปกรณ์พื้นฐาน เช่น แผงกั้นและเครื่องกั้น ไปจนถึงมาตรการที่ใช้เทคโนโลยีสูง เช่น กล้องโทรทัศน์วงจรปิด (CCTV) ไบโอเมตริก (biometrics) หรือรั้วไฟฟ้า ยิ่งไปกว่านั้น มาตรการรักษาความมั่นคงปลอดภัยทางกายภาพอาจรวมถึงสิ่งที่มองไม่เห็นด้วยตาเปล่า เช่น เซ็นเซอร์เตือนภัยรูปแบบต่าง ๆ สุดท้าย นโยบายและระเบียบปฏิบัติเป็นเอกสารทั้งที่เป็นและไม่ได้เป็นลายลักษณ์อักษรเกี่ยวข้องโดยตรงกับการปกป้องทรัพย์สินและเป็นแนวทางของการกำหนดโปรแกรมความปลอดภัย อาทิ คู่มือความปลอดภัยและวิธีการสื่อสารกับเจ้าหน้าที่รักษาความปลอดภัยที่ปฏิบัติหน้าที่เป็นตัวอย่างของนโยบายและขั้นตอน (Scheldt, 2023)

ภาพ 2.2 ระบบ CCTV แบบ Hybrid พร้อมเทคโนโลยีตรวจจับการเคลื่อนไหว (motion sensing) เป็นนวัตกรรมของระบบรักษาความปลอดภัยที่ลดต้นทุนพลังงานและประสิทธิภาพที่เพิ่มขึ้น (Nosiri, Akwiwu-Uzoma, Nmaju, & Elumeziem, 2018)

โดยทั่วไป แรงจูงใจ (motivation) เกี่ยวข้องกับเจตนาหรือความปรารถนาที่มีอิทธิพลต่อภัยคุกคามที่อาจเกิดขึ้นที่มุ่งเป้าไปที่ช่องโหว่ (vulnerability) ในการเข้าถึงหรือสร้างความเสียหายให้กับทรัพย์สิน ในขณะที่ ช่องโหว่คือจุดอ่อนหรือช่องว่างในการปกป้องทรัพย์สินเหล่านี้ที่ภัยคุกคามอาจนำไปใช้ประโยชน์ได้ จึงกล่าวได้ว่า แรงจูงใจในการก่ออาชญากรรมเกิดขึ้นจากเป้าหมายของอาชญากรรม (สินทรัพย์) อย่างไรก็ตาม องค์กรต้องการสินทรัพย์ในการประกอบกิจการ ดังนั้น การลดแรงจูงใจในการก่ออาชญากรรมจึงเป็นเรื่องที่ยากจะกระทำได้ ทั้งนี้ ปฏิสัมพันธ์ระหว่างสินทรัพย์ ช่องโหว่ และแรงจูงใจของภัยคุกคามเป็นพื้นฐานของความเสี่ยงในการจัดการความมั่นคงปลอดภัย องค์กรสามารถพัฒนากลยุทธ์และมาตรการรับมือที่มีประสิทธิภาพเพื่อปกป้องทรัพย์สินอันมีค่าของตนจากเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น หรือลดโอกาสในการก่ออาชญากรรม โดยการระบุและประเมินองค์ประกอบเหล่านี้ ดังภาพที่ 2.2 ทั้งนี้ การลดช่องโหว่ในการรักษาความมั่นคงปลอดภัยจะทำให้เหตุการณ์ความเสี่ยงต่าง ๆ ลดลง ดังนั้น เป้าหมายเชิงกลยุทธ์ของผู้มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยคือการลดโอกาสในการก่อการละเมิดความมั่นคงปลอดภัยโดยการลดช่องโหว่ โปรแกรมป้องกันทรัพย์สินรวมเอานโยบายและระเบียบปฏิบัติ มาตรการตอบโต้ทางกายภาพ และเจ้าหน้าที่รักษาความปลอดภัยเข้าด้วยกันเพื่อป้องกันทรัพย์สินจากภัยคุกคาม (Alberts, Behrens, Pethia, & Wilson, 1999)

ภาพ 2.2 แผนภาพเวนน์—สินทรัพย์ ภัยคุกคาม และช่องโหว่ (Vellani, 2021)

มาตรการรักษาความมั่นคงปลอดภัยโดยทั่วไปของโปรแกรมรักษาความมั่นคงปลอดภัยที่ดีประกอบด้วยนโยบายและขั้นตอนรักษาความมั่นคงปลอดภัย มาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ และเจ้าหน้าที่รักษาความปลอดภัย มาตรการรักษาความปลอดภัยเหล่านี้ได้รับการจัดทำขึ้นในระหว่างการประเมินความเสี่ยง โดยสามารถแบ่งออกเป็นส่วนสำคัญได้ดังตาราง 2.2

ตาราง 2.2 นโยบายและระเบียบการรักษาความมั่นคงปลอดภัย	
แผนการจัดการด้านความปลอดภัย	Security Management Plan
แผนจัดการเหตุฉุกเฉิน	Emergency Management Plan
การป้องกันความรุนแรงในที่ทำงาน	Workplace Violence Prevention
การรับมือภาวะวิกฤต	Crisis intervention
การป้องกันข้อมูลสำคัญ	Vital Records Protection
การคุ้มกันความปลอดภัย	Security Escort
การทดสอบระบบความปลอดภัยทางกายภาพ	Physical Security System Testing
การป้องกันและตอบโต้อัคคีภัย	Fire Prevention and Response
การควบคุมการเข้าถึง	Access Control
การตรวจสอบประวัติการจ้างงาน	Employment Background Investigations

การประเมินความมั่นคงปลอดภัย

ขั้นตอนสุดท้ายของการประเมินความเสี่ยงเกี่ยวข้องกับการประเมินต่าง ๆ ที่ออกแบบมาเพื่อวิเคราะห์ภัยคุกคาม ช่องโหว่หรือจุดอ่อน และความเสี่ยงโดยรวม และแนวทางการแก้ไข แต่ละขั้นตอนจะมีการกำหนดความเสี่ยงที่เกิดขึ้นจริงกับสินทรัพย์อย่างเป็นระบบ โดยเฉพาะความเสี่ยงต่อภารกิจที่สำคัญ โดยจากบทเรียนจะเห็นว่าการประเมินความมั่นคงปลอดภัยมี 3 ประเภท (1) ช่องโหว่ (2) ภัยคุกคาม และ (3) ความเสี่ยง ดังนั้น ขั้นตอนสุดท้ายของการประเมินความเสี่ยงคือการประเมินต้นทุนและผลประโยชน์ของมาตรการแก้ไข รวมถึงการปรับใช้ทรัพยากรเพื่อปกป้องพื้นที่หรือสินทรัพย์ที่มีความเสี่ยงสูง สินทรัพย์ที่สำคัญหรือมีความเสี่ยงมากขึ้น กล่าวโดยย่อ การประเมินความเสี่ยงได้รับการออกแบบมาเพื่อให้เกิดความต่อเนื่องจากกระบวนการระบุสินทรัพย์ที่สำคัญและภัยคุกคามต่อสินทรัพย์ และลดช่องโหว่ในการปกป้องสินทรัพย์เหล่านั้น โดยการวิเคราะห์อย่างรอบคอบและใช้มาตรการตอบโต้ที่มีประสิทธิภาพเพื่อให้ได้ระดับการป้องกันที่เหมาะสมที่สุด

การประเมินความมั่นคงปลอดภัยมีความเฉพาะเจาะจงมากขึ้นอยู่กับประเภทขององค์กรหรือสถานที่ ๆ ได้รับการประเมิน ในทำนองเดียวกัน วิธีการจะต้องเฉพาะเจาะจงสำหรับองค์กรหรือประเภทของอุตสาหกรรมที่ได้รับการประเมิน ยกตัวอย่างเช่น วิธีการประเมินโรงงานอุตสาหกรรมเคมีจะไม่สามารถใช้ได้กับการประเมินสถานศึกษา เช่น โรงเรียนหรือมหาวิทยาลัย หากใช้วิธีการเฉพาะสำหรับอุตสาหกรรมใดอุตสาหกรรมหนึ่ง ก็ควรระบุประเภทของสถานที่ อาคาร โรงงาน เครื่องจักร และข้อจำกัดต่าง ๆ ให้ชัดเจน ทั้งนี้ วิธีการประเมินความปลอดภัยได้รับการออกแบบมาเพื่อจัดการกับความมั่นคงปลอดภัยเฉพาะรูปแบบ ซึ่งในปัจจุบัน แบ่งเป็น 2 ประเภทหลักคือ ความมั่นคงปลอดภัยทางกายภาพและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ถึงแม้ว่าท้ายที่สุดกระบวนการประเมินระบบความมั่นคงปลอดภัยจะมาบรรจบกัน แต่ทั้ง 2 ประเภทก็ยังคงใช้รูปแบบการประเมินและวิธีการที่แตกต่างกัน

บทสรุป

ทุก ๆ องค์กร ไม่ว่าภาครัฐหรือเอกชน หรืออยู่ในอุตสาหกรรมประเภทใด หรือการประเมินเกี่ยวข้องกับความมั่นคงปลอดภัยทางกายภาพหรือความปลอดภัยด้านเทคโนโลยีสารสนเทศหรือไม่ การประเมินที่มีประสิทธิภาพต้องระบุว่าทรัพย์สินที่สำคัญที่ต้องการการป้องกันมีอะไรบ้าง ข้อมูลประเภทใดที่จำเป็นสำหรับทรัพย์สินแต่ละรายการ และการสูญหาย เสียหาย หรือถูกทำลายของทรัพย์สินแต่ละประเภทจะส่งผลกระทบต่อพันธกิจขององค์กรอย่างไร การประเมินความมั่นคงปลอดภัยควรรวมถึงการประเมินภัยคุกคาม (Threat Assessment) การประเมินช่องโหว่ (Vulnerability) และการประเมินความเสี่ยง (Risk Assessment) ซึ่งจะช่วยให้ผู้ที่มีอำนาจตัดสินใจด้านความมั่นคงปลอดภัยจัดลำดับความสำคัญของมาตรการ (Protocol) ในการปกป้องทรัพย์สิน

ท้ายที่สุด การประเมินควรให้คำแนะนำเฉพาะในปิดกั้นหรือลดโอกาสในการก่ออาชญากรรมหรือการโจรกรรมได้เป็นอย่างดี

คำถามท้ายบท

1. จงอธิบายว่า ‘สินทรัพย์คืออะไร’ แบ่งออกเป็นกี่ประเภท มีอะไรบ้าง?
2. สินทรัพย์มีตัวตนกับไม่มีตัวตนแตกต่างกันอย่างไร?
3. การระบุสินทรัพย์ (Asset Identification) มีความสำคัญอย่างไร?
4. จงอธิบายความสัมพันธ์ระหว่างสินทรัพย์ ภัยคุกคาม และช่องโหว่?
5. การประเมินความมั่นคงปลอดภัยกี่ประเภท มีอะไรบ้าง?

เอกสารอ้างอิง

Alberts, C. J., Behrens, S., Pethia, R. D., & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* Pittsburgh, PA: Software Engineering Institute.

Barone, A. (2022, July 1). *What Is an Asset? Definition, Types, and Examples*. Retrieved May 18, 2023, from www.investopedia.com: https://www.investopedia.com/terms/a/asset.asp#citation-3

Nosiri, O., Akwiwu-Uzoma, C., Nmaju, U., & Elumeziem, C. (2018). Motion Detector Security System for Indoor Geolocation. *International Journal of Engineering and Applied Sciences, 5*(11), 24-30.

Scheldt, A. (2023, August 21). *What Is a Countermeasure in Computer Security?* Retrieved from CompTIA: https://www.comptia.org

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset Identification in Information Security Risk Assessment: A Business Practice Approach. *Communications of the Association for Information Systems, 39*(1), 297-320. doi:10.17705/1CAIS.03915

Threat Analysis Group, L. (2023). *Security Risk Management*. Retrieved May 18, 2023, from www.threatanalysis.com: https://www.threatanalysis.com/security-risk-management/

Vaughan, A. (2018, January 16). *BP's Deepwater Horizon bill tops $65bn*. Retrieved 3 31, 2023, from The Guardian: https://www.theguardian.com/business/2018/jan/16/bps-deepwater-horizon-bill-tops-65bn

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