UNIT 4

กลยุทธ์การรักษาความมั่นคงปลอดภัย

บทที่ 4

กลยุทธ์การรักษาความมั่นคงปลอดภัย

บทนำ

บทเรียนที่ผ่านมาเป็นการปูพื้นฐานสำหรับบทที่ 4 นี้ โดยเป็นการอธิบายถึงแนวคิดและทฤษฎีที่ใช้ในการวางแผนกลยุทธ์ด้านความมั่นคงปลอดภัย ซึ่งจะอธิบายและแสดงไว้ในส่วนต่อไป โดยในส่วนแรกจะกล่าวถึงกลยุทธ์ด้านความมั่นคงปลอดภัยทั่วไปที่ผู้ปฏิบัติงานใช้กัน รวมถึงความท้าทายต่าง ๆ ด้านการป้องกัน จากนั้นจะกล่าวถึงมุมมองและข้อเสนอแนะต่าง ๆ ที่เกี่ยวกับวิธีคิดด้านการรักษาความมั่นคงปลอดภัยตามรูปแบบที่ได้มีการวางแผนไว้ ก่อนที่จะประยุกต์ใช้กลยุทธ์ความมั่นคงปลอดภัยที่มีรูปแบบเฉพาะ ในบทนี้ยังรวมเนื้อหาด้านอาชญวิทยาที่เกี่ยวข้องกับความมั่นคงปลอดภัยและปัญหาในที่ทำงาน และกลยุทธ์ด้านความมั่นคงปลอดภัยเกี่ยวกับการใช้ความรุนแรง การโจรกรรม และยาเสพติด อีกด้วย

ความมั่นคงปลอดภัยทั่วไปและความมั่นคงปลอดภัยเฉพาะ

กลยุทธ์การรักษาความมั่นคงปลอดภัย พัฒนาจากขึ้นจากวิธีการรักษาความปลอดภัยและการมุ่งเน้นการประยุกต์ใช้การจัดการของทรัพยากรบุคคล เทคโนโลยีสารสนเทศ การรักษาความปลอดภัยทางกายภาพ รวมถึงนโยบายและขั้นตอนการดำเนินงาน การตอบสนองเหตุฉุกเฉินและการกู้คืน การสืบสวน และส่วนประกอบด้านความปลอดภัยอื่น ๆ เพื่อการใช้งานและข้อได้เปรียบที่เหมาะสมที่สุด

การรักษาความมั่นคงปลอดภัยทั่วไป (Generic Security) เป็นการรวมกลยุทธ์การป้องกันทั่วไปและการปฏิบัติงานขององค์ประกอบทุกภาคส่วนจำนวนมาก โดยองค์ประกอบ 3 ประเภทหลัก ได้แก่ บุคลากร (personnel) นโยบายและขั้นตอน (policies & procedures) และเทคโนโลยี (technology) โดยตัวอย่างของ “บุคลากร” ได้แก่ เจ้าหน้าที่รักษาความปลอดภัยและเจ้าหน้าที่ฝ่ายสืบสวนสอบสวน ในขณะที่ “นโยบาย” และระเบียบปฏิบัติจัดทำขึ้นโดยฝ่ายบริหาร ซึ่งมีหน้าที่มอบหมายภาระงานประจำวันของบุคลากรเพื่อให้สอดคล้องกับเป้าหมายขององค์กร อีกทั้ง นโยบายคือข้อกำหนดที่ต้องปฏิบัติตามในขณะปฏิบัติหน้าที่ นอกจากนั้น “ขั้นตอน” คือแนวทางหรือขั้นตอนในการปฏิบัติให้สอดคล้องกับนโยบาย ตัวอย่างของ “นโยบาย” เช่น ผู้เยี่ยมชมสถานที่ทั้งหมดต้องได้รับการดูแลและถูกนำพาอย่างใกล้ชิด ในขณะที่ “ขั้นตอน” ระบุว่าผู้เข้าชมต้อง “เข้าสู่ระบบการ

รักษาความมั่นคงปลอดภัย” โดยแสดงบัตรประจำตัวที่มีรูปถ่าย รับป้ายชั่วคราว และมีฝ่ายบริหารหรือเจ้าหน้าที่รักษาความปลอดภัยติดตามไปด้วย ตัวอย่าง “เทคโนโลยีความปลอดภัย” ได้แก่ ระบบควบคุมการเข้าออก กล้องวงจรปิด และระบบเตือนการบุกรุก กลยุทธ์ทั้งหมดในองค์ประกอบทั้ง 3 ประเภทของการรักษาความมั้นคงปลอดภัยเหล่านี้เป็นกลยุทธ์ทั่วไปที่มีการนำไปใช้ในหลายพื้นที่ในหลากหลายอุตสาหกรรม

การรักษาความมั่นคงปลอดภัยเฉพาะ (Specific Security) ได้รับการออกแบบมาเป็นพิเศษเพื่อตอบสนองความต้องการของหน่วยงานที่มีลักษณะเฉพาะและลูกค้าของหน่วยงานนั้น ๆ (เช่น พนักงาน ผู้รับจ้าง ผู้ซื้อผลิตภัณฑ์และบริการ) รวมถึงความท้าทายด้านความมั่นคงปลอดภัยของหน่วยงานอีกด้วย กล่าวอีกนัยหนึ่ง ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยต้องเข้าใจวัตถุประสงค์และความต้องการทางธุรกิจของหน่วยงาน จากนั้นจัดโปรแกรมการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับวัตถุประสงค์และความต้องการเหล่านั้น

เมื่ออ้างอิงถึงองค์ประกอบการรักษาความมั่นคงปลอดภัยหลัก 3 ประเภท หน่วยงานอาจจัด “บุคลากร” ที่เป็นกองกำลังรักษาความปลอดภัยที่มีการฝึกอบรมเฉพาะทาง อุปกรณ์พิเศษ และเครื่องแบบเฉพาะเพื่อตอบสนองความต้องการเฉพาะขององค์กร ทั้งนี้ “นโยบาย” และระเบียบปฏิบัติสามารถออกแบบเพื่อจัดการกับปัญหาพิเศษ เช่น บทบาทของเจ้าหน้าที่รักษาความปลอดภัยในการควบคุมผู้ป่วยสุขภาพจิตที่ก่อกวนความสงบในโรงพยาบาล หรือ “เทคโนโลยี” ความปลอดภัยเฉพาะที่ตอบสนองความต้องการเฉพาะของธุรกิจ เช่น ระบบป้องกันการโจรกรรมหรือขโมยสินค้า (EAS หรือ Electronic Article Surveillance) ที่ใช้ในอุตสาหกรรมต่าง ๆ เช่น ร้านค้าปลีก และห้องสมุดเพื่อป้องกันการโจรกรรมและตรวจสอบตำแหน่งของสินค้า เป็นต้น

ภัยคุกคาม อันตราย หรือเหตุการณ์ที่ไม่พึงประสงค์อาจส่งผลให้เกิดการเปลี่ยนแปลงองค์ประกอบการรักษาความมั่นคงปลอดภัยประเภทที่ หนึ่ง สอง หรือทั้งสามประเภท อาทิ การโจมตีเรือรบ USS Cole เรือพิฆาตของกองทัพเรือสหรัฐที่จอดลอยลำเพื่อเติมน้ำมันอยู่ที่ท่าเรือเอเดน ประเทศเยเมน โดยผู้ก่อการร้าย อัล – กออิดะห์ ได้ใช้เรือขนาดเล็กบรรทุกระเบิด C4 ทำการระเบิดพลีชีพในระยะประชิด เมื่อวันที่ 12 ตุลาคม พ.ศ. 2543 ทำให้ลูกเรือเสียชีวิต 17 นาย และบาดเจ็บ 39 นาย เป็นเหตุให้กองทัพเรือสหรัฐจึงได้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเฉพาะสำหรับเรือของกองทัพเรือสหรัฐฯ ใหม่ทั้งหมด

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยทั่วไปและการรักษาความมั่นคงปลอดภัยเฉพาะนั้นก็ได้มีความแตกต่างกันอย่างชัดเจนเท่าใดนัก นักวางแผนและนักออกแบบด้านความมั่นคงปลอดภัยมักจะเริ่มต้นด้วยการรักษาความปลอดภัยทั่วไป จากนั้นจึงปรับรูปแบบการรักษาความปลอดภัยให้เข้ากับความต้องการเฉพาะของธุรกิจ หรืออาจคิดค้นและพัฒนาสิ่งใหม่ ๆ เพื่อตอบสนองความต้องการเฉพาะ

กลยุทธ์การรักษาความมั่นคงปลอดภัย (Security Strategy)

กลยุทธ์การรักษาความมั่นคงปลอดภัยที่จะกล่าวถึงต่อไปนี้ ไม่เกี่ยวข้องกับลำดับความสำคัญสถานที่ในการป้องกัน หากแต่มีบทบาทสำคัญทั้งสิ้นในกรณีเกิดเหตุการณ์ที่เกี่ยวข้องกับอาชญากรรมหรือการโจมตีขึ้น

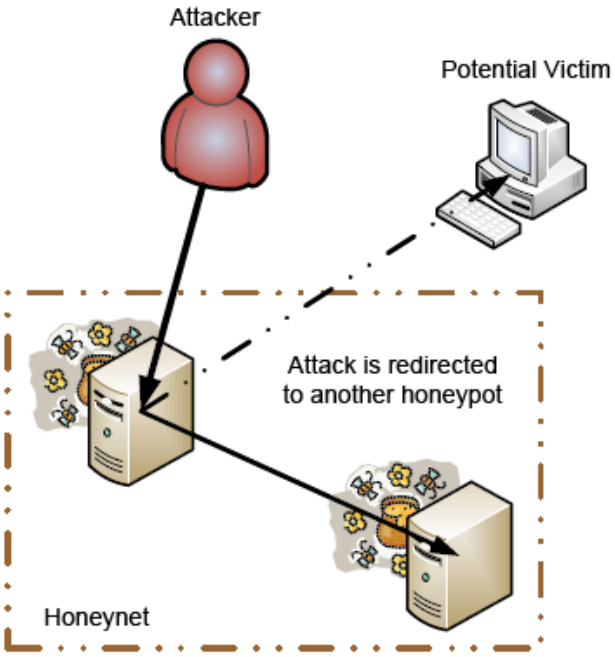
การป้องปราม (Deterrence) การป้องปรามเป็นกลยุทธ์การรักษาความมั่นคงปลอดภัยที่ป้องกันไม่ให้บุคคลก่ออาชญากรรม อาจอยู่ในรูปแบบของการลาดตระเวนเชิงป้องกันโดยเจ้าหน้าที่ตำรวจสายตรวจ หรือโทษจำคุกที่รุนแรงสำหรับผู้กระทำผิด ซึ่งเป็นเทคนิคที่ใช้กันมากที่สุด และเป็นกลไกหลักของกระบวนการยุติธรรมทางอาญาและการใช้อำนาจรัฐโดยมุ่งเป้าในการลดการกระทำความผิดและเพิ่มความปลอดภัยสาธารณะ (Kennedy, 2009) อย่างไรก็ตาม การป้องปรามจะได้ผลดีก็ต่อเมื่อผู้กระทำความผิดได้ดำเนินการ “วิเคราะห์ความเสี่ยง” (ผ่านการตัดสินใจอย่างรวดเร็ว การเฝ้าระวัง การรวบรวมข้อมูลข่าวกรอง ข้อมูลวงใน หรือวิธีการอื่น ๆ) และทำการ “เลือกอย่างมีเหตุผล” ที่ “โอกาส” สำหรับการก่ออาชญากรรมยังไม่ถึงโอกาสเหมาะ และตัดสินใจไม่ก่ออาชญากรรมในสถานที่ใดสถานที่หนึ่ง เนื่องจากหลากหลายสาเหตุ อาทิ ไม่สามารถระบุตัวเหยื่อ ไม่สามารถระบุช่องโหว่ทางกายภาพ โอกาสที่จะเกิดอันตรายต่อผู้กระทำความผิด เป็นต้น

กล่าวได้ว่า การป้องปรามเกี่ยวข้องกับการใช้มาตรการและกลยุทธ์เพื่อกีดกันภัยคุกคามและฝ่ายตรงข้ามที่อาจเกิดขึ้นจากการพยายามที่จะทำให้ความมั่นคงปลอดภัยขององค์กรอ่อนแอลง เป้าหมายหลักของการป้องปรามคือการสร้างสภาพแวดล้อมที่ทำให้เกิดความเสี่ยงและต้นทุนที่สูงหรือการรับรู้ได้ถึงกิจกรรมที่เป็นอันตรายนั้นมีมากกว่าผลประโยชน์ที่ได้รับ ที่อาจเกิดขึ้นสำหรับผู้โจมตี การป้องปรามมักเกี่ยวเนื่องกับมาตรการและการควบคุมความมั่นคงปลอดภัยที่มองเห็นได้ชัดเจน ด้วยการสร้างมาตรการรักษาความมั่นคงปลอดภัยที่ชัดเจนทางกายภาพ เช่น รั้ว สิ่งกีดขวาง กล้องวงจรปิด ระบบควบคุมการเข้าออก ระบบเตือนภัย และเจ้าหน้าที่รักษาความปลอดภัย ทั้งนี้เพื่อยับยั้งการเข้าถึงสิ่งอำนวยความสะดวกทางกายภาพโดยไม่ได้รับอนุญาต ในทางกลับกัน มาตรการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ รวมถึงการควบคุมการเข้าถึงที่รัดกุม การเข้ารหัส และระบบตรวจจับการบุกรุก สามารถยับยั้งอาชญากรไซเบอร์ที่อาจมองว่าองค์กรเป็นเป้าหมายที่ยากลำบาก เป็นต้น

การลวง (Deception) ในบริบทของกลยุทธ์การจัดการความมั่นคงปลอดภัย หมายถึงการใช้ข้อมูล กลยุทธ์ หรือเทคโนโลยีที่ทำให้เข้าใจผิดโดยเจตนาเพื่อสร้างความสับสน เป็นการขัดขวางหรือส่งข้อมูลหรือสัญญาณที่ไม่ถูกต้องต่อภัยคุกคามหรือฝ่ายตรงข้าม โดย “การลวง” นั้นสามารถนำไปใช้เพื่อทำให้สถานที่ดูเหมือนเป็นสถานที่ ๆ ได้รับการคุ้มครองหรือมีความเสี่ยงต่ำกว่าที่เป็นอยู่ ดังนั้นจึงทำให้ดูเหมือนเป็นเป้าหมายที่น่าสนใจน้อยลง การลวงยังสามารถใช้เพื่อส่งให้ฝ่ายตรงข้ามเข้าใจผิดและโจมตีไปยังส่วนที่ไม่สำคัญของสถานที่ได้ (Federal Emergency Management

Agency, 2003) ทั้งนี้ การลวงเป็นแนวทางเชิงรุกเพื่อเพิ่มความปลอดภัยด้วยการสร้างความไม่แน่นอนและความสงสัยให้เกิดขึ้นกับผู้ที่พยายามจะทำอันตรายต่อระบบความมั่นคงปลอดภัยขององค์กร อย่างไรก็ตาม การลวงอาจไม่มีประสิทธิภาพเท่าที่ควรหากฝ่ายตรงข้ามได้รับข้อมูลภายใน รับรู้ถึงการดำเนินการเฝ้าระวัง หรือใช้การวิเคราะห์ความเสี่ยงในด้านต่าง ๆ ได้

การลวงอาจมีรูปแบบต่าง ๆ มากมาย รวมถึง ข้อมูลที่ไม่ถูกต้องหรือข้อมูลบิดเบือน ซึ่งเป็นกลยุทธ์การลวงที่เกี่ยวข้องกับการเปลี่ยนเส้นทางผู้โจมตีให้ห่างออกจากทรัพย์สินที่สำคัญ หรือล่อลวงฝ่ายตรงข้ามให้เดินทางไปสู่สภาพแวดล้อมที่มีการควบคุม ซึ่งเปิดโอกาสให้ฝ่ายความมั่นคงปลอดภัยสามารถสังเกตและวิเคราะห์การกระทำของฝ่ายตรงข้ามได้ โดยไม่ก่อให้เกิดภัยคุกคามต่อระบบหลักขององค์กรอย่างแท้จริง หรือในด้านความมั่นคงปลอดภัยไซเบอร์ จะมีการนำระบบ “Honeypots” หรือ “เครื่องเป้าหมายลวง” ซึ่งหมายถึงเครื่องคอมพิวเตอร์หลักในระบบเครือข่าย หรือ “server” ที่ถูกปล่อยให้มีช่องโหว่ (vulnerability) เพื่อลวงให้ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ หรือแฮกเกอร์ (hacker) เข้ามาเจาะระบบที่เรียกว่า “Honeynets” หรือ “ระบบเป้าหมายลวง” นั่นเอง (ปริญญา หอมอเนก, 2546) อย่างไรก็ตาม การลวงที่มีประสิทธิผลจะต้องใช้กลยุทธ์และเทคนิคที่มีการพัฒนาอย่างต่อเนื่อง เพื่อก้าวนำหน้าผู้ไม่ประสงค์ดีหรือฝ่ายตรงข้ามที่มีความสามารถและอาจเรียนรู้กลยุทธ์การลวงขององค์กรได้



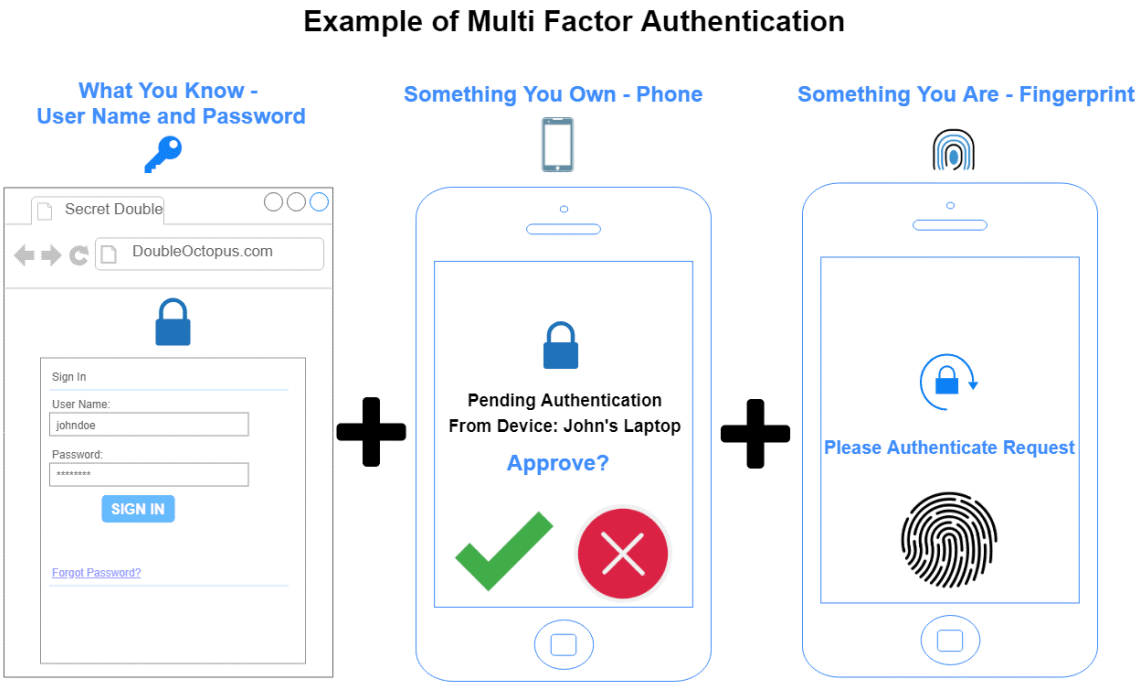
ภาพ 4.1 honeypot คือเครื่องคอมพิวเตอร์เดี่ยวหรือคอมพิวเตอร์บนระบบเครือข่ายที่ได้รับการกำหนดค่าให้ทำหน้าที่เป็นเป้าหมายลวง หรือ ตัวล่อ (decoy) เพื่อดึงดูดและดักจับผู้โจมตี ในทางกลับกัน honeynet คือระบบเครือข่ายของ honeypot ที่ใช้ล่อผู้โจมตีระบบเครือข่ายและวิเคราะห์พฤติกรรมของแฮกเกอร์จากเครื่องล่อ honeypots หลายเครื่อง (Peter & Schiller, 2008)

การตรวจจับ (Detection) เป็นกลยุทธ์ด้านความมั่นคงปลอดภัยเกี่ยวข้องกับการระบุเหตุการณ์ด้านความปลอดภัยและภัยคุกคามภายขององค์กรในเชิงรุกและอย่างต่อเนื่อง เป้าหมายหลักของการตรวจจับคือ การระบุและตอบสนองต่อการละเมิดความมั่นคงปลอดภัย และช่องโหว่ที่อาจเกิดขึ้นอย่างรวดเร็ว เพื่อลดผลกระทบและป้องกันความเสียหายเพิ่มเติม หรืออีกนัยหนึ่ง ในกรณีที่ผู้กระทำความผิดเลือกที่จะกำหนดเป้าหมายในการโจมตีเนื่องจากการป้องปรามล้มเหลว ผู้บริหารด้านความมั่นคงปลอดภัยควรใช้กลยุทธ์เพื่อตรวจจับการบุกรุกทางกายภาพหรือเสมือนจริง ตัวอย่างเช่น ระบบตรวจจับการบุกรุก (intrusion-detection) ที่สามารถตรวจจับการบุกรุก แจ้งเจ้าหน้าที่รักษาความปลอดภัยและ/หรือตำรวจ และการติดตามเพื่อจับกุมผู้กระทำความผิด กลยุทธ์การตรวจจับอื่น ๆ ได้แก่ กล้องวงจรปิด (CCTV) การรับรู้ของพนักงานเพื่อรายงานพฤติกรรมที่น่าสงสัย การเฝ้าระวังอาชญากรรมในละแวกบ้าน (neighborhood watch) และข่าวกรอง (intelligence) ทั้งนี้ รวมถึงระบบเทคโนโลยีสารสนเทศที่มีซอฟต์แวร์ตรวจจับการบุกรุกที่สามารถตรวจจับแฮกเกอร์ และบุคคลอื่นที่พยายามฝ่าฝืน หรือผู้ที่ฝ่าฝืนระบบควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรได้สำเร็จ

ในกรณีของความมั่นคงปลอดภัยไซเบอร์ การตรวจจับเกี่ยวข้องกับการติดตามตรวจสอบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เครือข่าย ระบบ และแอปพลิเคชันขององค์กรอย่างต่อเนื่อง เพื่อหากิจกรรมที่ผิดปกติหรือน่าสงสัยที่อาจบ่งบอกถึงภัยคุกคามด้านความปลอดภัย ซึ่งรวมถึงการตรวจสอบสัญญาณการติดไวรัสหรือมัลแวร์ (malware infections) ความพยายามในการเข้าถึงโดยไม่ได้รับอนุญาต รูปแบบการรับส่งข้อมูลเครือข่ายที่ผิดปกติ และอื่น ๆ ทั้งนี้ ทีมรักษาความมั่นคงปลอดภัยทำหน้าที่วิเคราะห์และบันทึกข้อมูลเหตุการณ์จากแหล่งต่าง ๆ เช่น ไฟร์วอลล์ ระบบตรวจจับการบุกรุก (IDS) ซอฟต์แวร์ป้องกันไวรัส และบันทึกกิจกรรมของผู้ใช้ เพื่อระบุรูปแบบหรือความผิดปกติที่อาจส่งสัญญาณถึงเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ การใช้เครื่องมือ อาทิ Security Information and Event Management (SIEM) เพื่อรวบรวม เชื่อมโยง และวิเคราะห์ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยจากหลายแหล่งโดยอัตโนมัติ ช่วยให้ทีมรักษาความมั่นคงปลอดภัยสามารถตรวจจับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น

การหน่วง (Delay) เกี่ยวข้องกับการใช้มาตรการและกลยุทธ์เพื่อชะลอหรือขัดขวางความคืบหน้าของผู้โจมตีหรือภัยคุกคามในกรณีที่องค์กรไม่อาจขัดขวาง (deter) หรือตรวจพบได้ (detect) เป็นผลให้ผู้โจมตีสามารถลักลอบผ่านระบบการป้องกันขององค์กรได้ ด้วยเหตุนี้ เป้าหมายหลักของวัตถุประสงค์การหน่วงคือการซื้อเวลาให้กับทีมรักษาความมั่นคงปลอดภัยในการตรวจจับการลักลอบตอบสนองต่อเหตุการณ์ และบรรเทาผลกระทบก่อนที่ความเสียหายจะเกิดขึ้น ทั้งนี้ กลยุทธ์ในการหน่วงฝ่ายตรงข้ามหรือผู้โจมตีให้เกิดความล่าช้า ได้แก่ ประตูหรือหน้าต่างที่แข็งแรงซึ่งสร้างจากวัสดุที่แข็งแรงและล็อคที่มีความปลอดภัยสูง ซึ่งทำให้ผู้กระทำผิดเกิดความล่าช้าในการบุกรุก ในสถานการณ์เช่นนี้ เมื่อการหน่วงเวลาเพิ่มขึ้น ก็จะทำให้ความวิตกกังวลและความหงุดหงิดของผู้กระทำความผิด

เพิ่มขึ้นตามไปด้วย และเป็นการเพิ่มโอกาสในการที่จะตรวจจับหรือจับกุมหรือผู้กระทำผิด หรืออาจทำให้ผู้กระทำความผิดตัดสินใจหยุดหรือยกเลิกการก่ออาชญากรรมได้



ภาพ 4.2 “การยืนยันตัวตนโดยใช้หลายปัจจัย” เป็นวิธีการรับรองความถูกต้องที่ต้องให้ผู้ป้อนข้อมูล (ไม่ว่าจะเป็นบุคคล ซอฟต์แวร์ หรือโมดูลฮาร์ดแวร์) สร้างตัวระบุตัวตน (หรือ “ปัจจัย”) ที่บ่งบอกถึงข้อมูลประจำตัวแยกกันหลายตัว แทนที่จะเป็นตัวระบุมาตรฐานตัวเดียว ระบบอาจขอให้ผู้ใช้ป้อนรหัสที่ส่งไปยังอีเมล ตอบคำถามลับ หรือสแกนลายนิ้วมือร่วมกับการป้อนรหัสผ่าน (Secret Double Octopus, 2023)

ในส่วนของความมั่นคงปลอดภัยไซเบอร์ การใช้ “การยืนยันตัวตนโดยใช้หลายปัจจัย” หรือ Multi-Factor Authentication (MFA) สำหรับระบบและบัญชีที่สำคัญขององค์กร สามารถที่จะชะลอเวลาผู้โจมตีที่ต้องการจารกรรมข้อมูลสำคัญ เนื่องจากจะต้องมีการยืนยันตัวตนเพื่อรับรองความถูกต้อง 2 ระดับขึ้นไปเพื่อเข้าในระบบได้ หรือการใช้ “การตรวจจับและตอบสนองปลายทาง” หรือ Endpoint Detection and Response (EDR) ซึ่งสามารถตรวจจับ เก็บหลักฐาน และแยกอุปกรณ์ปลายทางที่ถูกบุกรุก เช่น เครื่องคอมพิวเตอร์ เพื่อป้องกันการบุกรุกเพิ่มเติมและแจ้งเตือนผู้ใช้งาน ทำให้การโจมตีไม่คืบหน้าและล่าช้าได้ ยิ่งไปกว่านั้น ในส่วนของการต่อต้านการก่อการร้าย การออกแบบภูมิทัศน์และลักษณะทางสถาปัตยกรรมอย่างเหมาะสมสามารถชะลอการก่อการร้ายไม่ให้ไปถึงเป้าหมายได้ ซึ่งสามารถทำได้โดยการออกแบบเส้นทางสิ่งกีดขวางหรือเส้นทางคดเคี้ยวสำหรับ

ยานพาหนะ และสร้างเขตกันชนระหว่างพื้นที่ส่วนกลางและพื้นที่สำคัญ เป็นต้น (Federal Emergency Management Agency, 2003)

การยับยั้ง (Deny) เกี่ยวข้องกับการดำเนินการโดยมีเจตนาเพื่อป้องกันหรือกีดขวางการเข้าถึง กิจกรรม หรือภัยคุกคามที่ไม่ได้รับอนุญาตไม่ให้กระทบต่อบุคคล องค์กร ทรพย์สิน ระบบเครือข่าย และข้อมูลขององค์กร เป้าหมายหลักของวัตถุประสงค์ของการยับยั้ง คือการสร้างการป้องกันที่แข็งแกร่งซึ่งทำให้ฝ่ายตรงข้ามพบอุปสรรคในการฝ่าฝืนระบบความมั่นคงปลอดภัยและดำเนินกิจกรรมที่เป็นอันตรายต่อองค์กรได้อย่างยากลำบาก ทั้งนี้ ผู้กระทำผิดสามารถถูกยับยั้งได้หลายวิธี ตัวอย่างเช่น การถูกจับกุม การเข้าถึงเป้าหมายและพบว่าบุคคลหรือทรัพย์สินที่ต้องการหายไป ไม่สามารถเข้าถึงทรัพย์สินที่สำคัญได้เนื่องจากการรักษาความมั่นคงปลอดภัยที่แข็งแกร่งซับซ้อน และแน่นหนา (เช่น ตู้เซฟ) หรือถูกหลอกให้กำหนดเป้าหมายไปยังสถานที่ ๆ เป็นเป้าหมายลวง

การยับยั้งจะต้องเริ่มต้นด้วยกลไกการควบคุมการเข้าถึงที่เข้มงวด ซึ่งจำกัดผู้ที่สามารถเข้าถึงทรัพยากรที่ละเอียดอ่อนภายในองค์กรได้ ซึ่งรวมถึงการตรวจสอบสิทธิ์ผู้เข้าใช้ การอนุญาต (authorization) และหลักการสิทธิ์ขั้นต่ำเพื่อให้แน่ใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงจุดที่เปราะบาง ทรัพย์สิน ระบบเครือข่ายและข้อมูลเฉพาะขององค์กรได้ ในกรณีความมั่นคงปลอดภัยไซเบอร์ ไฟร์วอลล์ (firewalls) และการแบ่งส่วนเครือข่าย (network segmentation) จะสามารถปฏิเสธการรับส่งข้อมูลเครือข่ายที่ไม่ได้รับอนุญาต และแยกระบบและข้อมูลที่ละเอียดอ่อนออกจากภัยคุกคามที่อาจเกิดขึ้น ในขณะที่ “ระบบตรวจจับและป้องกันการบุกรุก” หรือ Intrusion Detection and Prevention Systems (IDS/IPS) สามารถใช้เพื่อตรวจสอบการรับส่งข้อมูลเครือข่ายและบล็อก หรือแจ้งเตือนเกี่ยวกับกิจกรรมที่น่าสงสัยหรือเป็นอันตราย เช่น ความพยายามในการบุกรุกหรือรูปแบบการโจมตีที่ทราบ การจู่โจมกลับ หรือหยุดยั้งผู้บุกรุกได้ ด้วยตัวเอง

การบรรเทา (Mitigate) เป็นกลยุทธ์ที่เกี่ยวข้องกับการดำเนินการเพื่อลดขนาดหรือลดผลกระทบและอันตรายที่อาจเกิดขึ้นจากเหตุการณ์ด้านความมั่นคงปลอดภัย การละเมิด หรือช่องโหว่ที่ได้รับการระบุหรือตรวจพบ เป้าหมายหลักของการบรรเทาผลกระทบคือการจำกัดความเสียหายและป้องกันไม่ให้สถานการณ์เลวร้ายมากขึ้น ซึ่งจะช่วยลดผลกระทบของเหตุการณ์อาชญากรรมหรือการโจมตีเมื่อกลยุทธ์ด้านความมั่นคงปลอดภัยอื่น ๆ ล้มเหลว ทั้งนี้ การบรรเทาผลกระทบเป็นขั้นตอนสำคัญในกระบวนการตอบสนองต่อเหตุการณ์ในวงกว้าง (incident response) เมื่อเหตุการณ์ด้านความมั่นคงปลอดภัยเกิดขึ้น การดำเนินแผนการตอบสนองต่อเหตุการณ์ที่กำหนดไว้อย่างดีจะทำให้ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสามารถควบคุมและบรรเทาผลกระทบของเหตุการณ์นั้น ซึ่งอาจเกี่ยวข้องกับการแยกระบบ เครือข่าย หรือพื้นที่ที่ได้รับผลกระทบ เพื่อป้องกันการแพร่กระจายหรือความเสียหายเพิ่มเติม นั่นเอง

กลยุทธ์การบรรเทาด้านความมั่นคงปลอดภัยมีหลากหลายวิธี อาทิ แนวทางปฏิบัติในการรักษาจำนวนเงินขั้นต่ำไว้ในร้านค้าปลีก ในกรณีการโจมตีของผู้ก่อการร้าย การเสริมความแข็งแกร่งของโครงสร้างอาคารสามารถช่วยชีวิตคนเป็นจำนวนมาก อาทิ สามารถจำกัดเศษซากที่กระเด็นอำนวยความสะดวกในการอพยพและช่วยเหลือ และป้องกันการพังทลายของอาคาร อย่างไรก็ดี ในกรณีความมั่นคงปลอดภัยไซเบอร์ กลยุทธ์การใช้แพทช์ (patch) หรือการอัปเดตทันที สามารถลดความเสี่ยงของการโจมตีจากช่องโหว่ที่ถูกค้นพบได้ หรือในกรณีที่มีการระบุพบมัลแวร์ (malware) ภายในระบบเครือข่ายคอมพิวเตอร์ ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยจะต้องดำเนินการลบมัลแวร์นั้นออกทันที เพื่อป้องกันความเสียหายและการสูญหายของข้อมูลเพิ่มเติมที่อาจเกิดขึ้นได้ และถ้าเกิดการสูญหายของข้อมูลขึ้น การบรรเทาผลกระทบจะเกี่ยวข้องกับการกู้คืนข้อมูลที่สูญหายทุกครั้งที่เป็นไปได้ ดังนั้น การสำรองข้อมูลเป็นประจำจึงมีความสำคัญอย่างยิ่งต่อกลยุทธ์การบรรเทานี้ (Federal Emergency Management Agency, 2003)

การตอบสนอง (Respond) เกี่ยวข้องกับการดำเนินการเฉพาะและการดำเนินการตามแผนเพื่อจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย การละเมิด และภัยคุกคามเมื่อตรวจพบหรือรับทราบแล้ว ทั้งนี้ เมื่อฝ่ายรักษาความมั่นคงปลอดภัยได้รับแจ้งถึงเหตุการณ์ไม่พึงประสงค์ การตอบสนองเป็นสิ่งจำเป็นที่สุดในการช่วยเหลือผู้ได้รับบาดเจ็บ จับกุมผู้กระทำผิด และปกป้องทรัพย์สิน อย่างไรก็ตาม การตอบสนองสามารถเกิดขึ้นได้ในทุกช่วงเวลาตลอดห่วงโซ่ของเหตุการณ์ที่นำไปสู่การก่ออาชญากรรม ตัวอย่างเช่น เมื่อมีคนสังเกตเห็นว่าฝ่ายตรงข้ามกำลังทำการสอดแนมองค์กร บุคลากร ทรัพย์สิน หรือการปฏิบัติงาน ซึ่งอาจจะยังไม่เป็นเหตุที่นำไปสู่การจับกุมได้ อย่างเช่นในกรณีที่ผู้กระทำผิดทำการฝ่าฝืนบุกรุกทางประตูหรือหน้าต่างอย่างชัดเจน

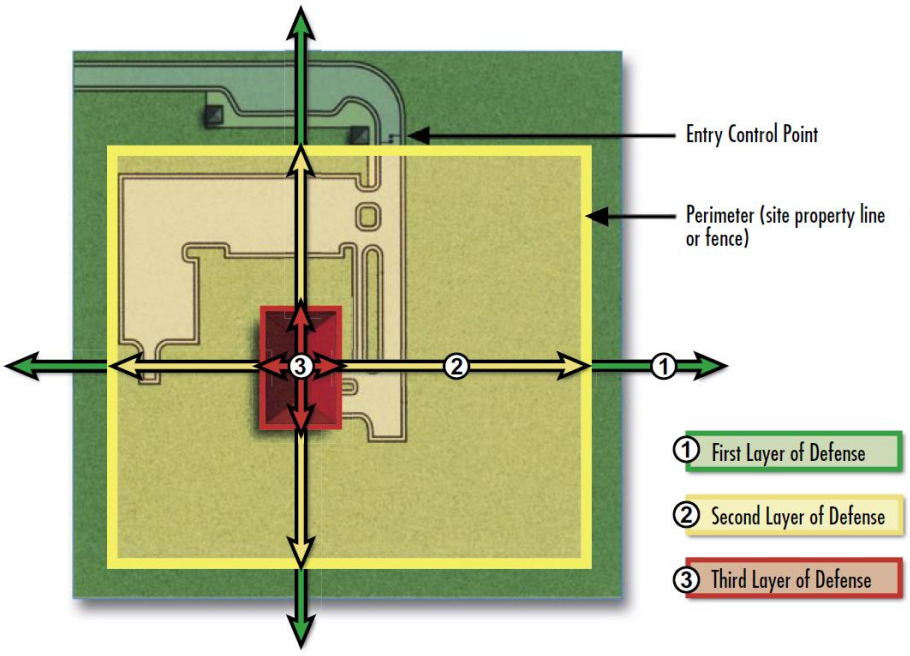
ตามหลักการ กระบวนการตอบสนองสถานการณ์ (incident response) มีขั้นตอนในการจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย ดังนี้ (1) การแจ้ง (notification) ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างทันท่วงที รวมถึงทีมงานภายใน ฝ่ายบริหาร การบังคับใช้กฎหมาย (หากจำเป็น) และฝ่ายที่ได้รับผลกระทบ เช่น ลูกค้า (2) กระบวนการขั้นต่อมาคือการควบคุม (containment) เหตุการณ์ดังกล่าว ซึ่งเกี่ยวข้องกับการกแยกส่วนที่ได้รับผลกระทบออกเพื่อป้องกันไม่ให้เหตุการณ์ลุกลามต่อไป (3) หลังจากการควบคุม ทีมรักษาความมั่นคงปลอดภัยจะทำงานเพื่อระบุสาเหตุของเหตุการณ์และกำจัดแหล่งที่มาของภัยคุกคาม (eradication) ซึ่งมักจะเกี่ยวข้องกับการปิดช่องโหว่และตรวจสอบให้แน่ใจว่าผู้โจมตีไม่สามารถเข้าถึงเป้าหมายได้อีกต่อไป (4) ขั้นตอนต่อมาคือกระบวนการฟื้นตัว (recovery) เป็นกระบวนการที่รวมถึงความพยายามในการกู้คืนสิ่งที่สูญเสียหรือได้รับผลกระทบ เพื่อให้การปฏิบัติงานกลับสู่ภาวะปกติโดยเร็วที่สุดอย่างมีประสิทธิภาพนั่นเอง

โดยสรุป เป้าหมายของการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพ คือการใช้กลยุทธ์การรักษาความมั่นคงปลอดภัยที่สามารถปรับปรุงได้ หรือคาดเดาไม่ได้นั่นเอง ซึ่งหมายความว่า ควรออกแบบการรักษาความมั่นคงปลอดภัยเพื่อหลีกเลี่ยงรูปแบบที่คาดเดาได้ หากเป็นไปได้ เจ้าหน้าที่

รักษาความมั่นคงปลอดภัยไม่ควรมีพฤติกรรมแบบซ้ำ ๆ เดิม ๆ คาดเดาได้ (creatures of habit) จนกลายเป็นนิสัย อาทิ การลาดตระเวนตามสถานที่เดิม ๆ พร้อม ๆ กัน ในกะทำงาน ผู้ดูแลความมั่นคงปลอดภัยควรหลีกเลี่ยงการตรวจสอบคุณลักษณะด้านความปลอดภัยในลักษณะเดียวกันตามความเคยชิน โดยวิธีการนี้สามารถนำไปใช้กับรูปแบบต่าง ๆ ของการรักษาความปลอดภัยทางกายภาพ (เช่น การเคลื่อนย้ายจุดติดตั้งไฟส่องสว่าง กล้องวงจรปิด หรือระบบเตือนการบุกรุกไปยังตำแหน่งต่าง ๆ ในเวลาที่ไม่สามารถคาดเดาได้) และรวมถึงการใช้นโยบายและขั้นตอนต่าง ๆ (เช่น การใช้ความสุภาพและความละเอียดในการปฏิบัติงาน การตรวจสอบบุคคล ยานพาหนะ หรือสิ่งของเป็นระยะ ๆ) (Purpura, 2018)

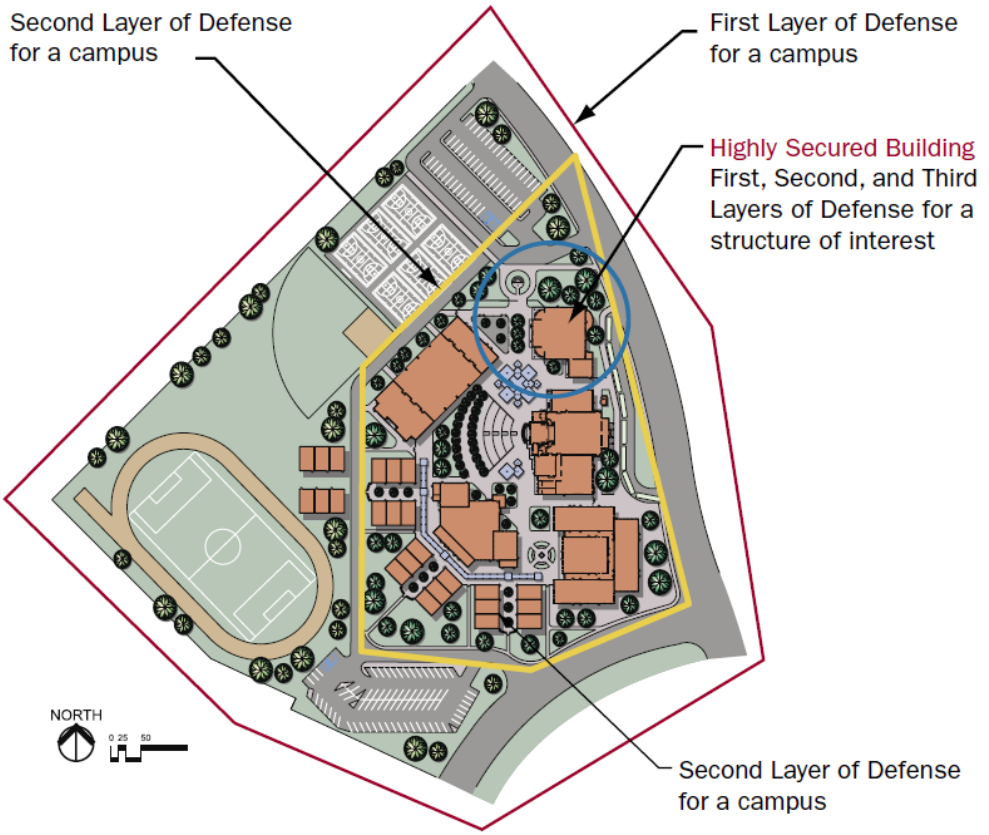
ระดับชั้นความมั่นคงปลอดภัยและการสำรองหรือซ้ำซ้อน (Security Layers and Redundancy)

ระดับชั้นความมั่นคงปลอดภัยใช้วิธีการแบ่งเขตของการรักษาความมั่นคงปลอดภัยที่ขยายจากพื้นที่ ๆ ต้องการการป้องกัน (ลักษณะคล้ายวงกลมที่มีจุดศูนย์กลางเดียวกัน) โดยสามารถอธิบายได้ดังนี้



ภาพ 4.3 ระดับชั้นของการป้องกันจะกำหนดจุดแบ่งเขตสำหรับกลยุทธ์การรักษาความปลอดภัยที่แตกต่างกัน และกำหนดตำแหน่งของทรัพย์สินที่สำคัญที่อยู่ในพื้นที่ โดยทั่วไปแล้ว ชั้นแรกจะอยู่ภายนอกบริเวณอาณาเขต ชั้นที่สองจะอยู่ระหว่างเส้นกำหนดอาณาเขตและทรัพย์สินที่สำคัญ และชั้นที่สามคือการปกป้องทรัพย์สินนั่นเอง (Federal Emergency Management Agency, 2005)

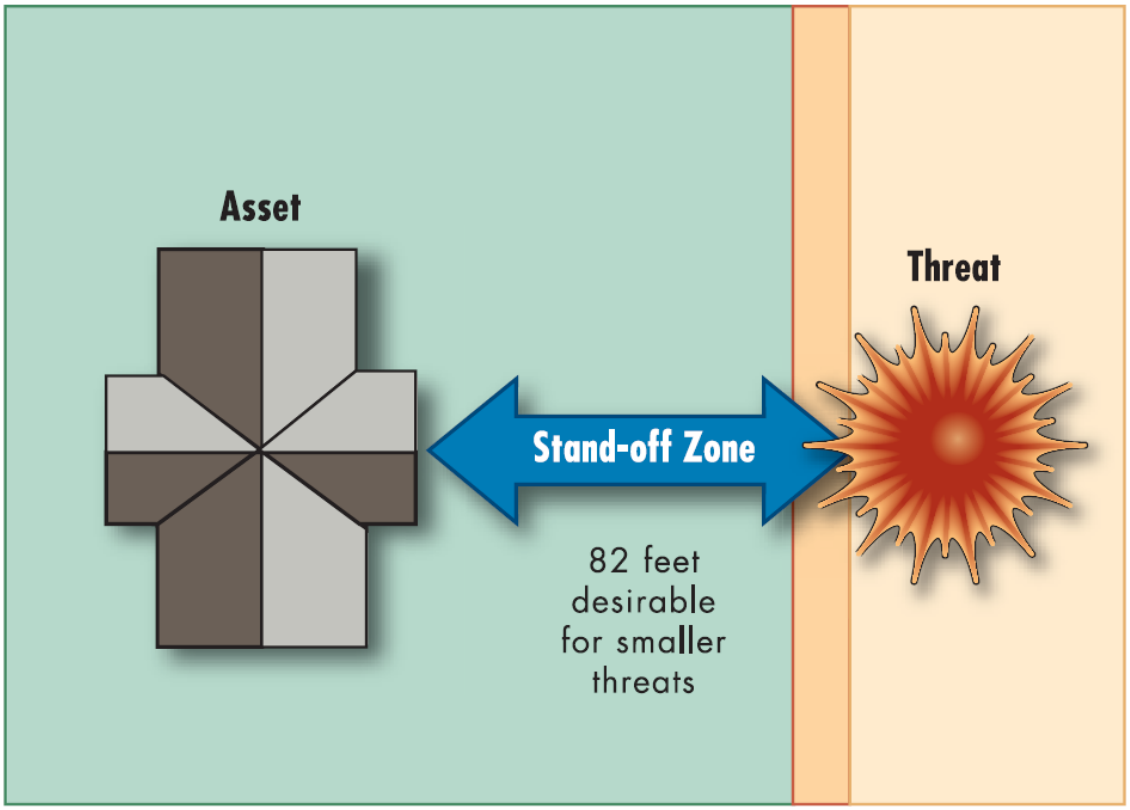
การป้องกันชั้นที่ 1 (first layer of defense) มุ่งเน้นที่การป้องปรามและป้องกัน โดยจะต้องมีการศึกษาลักษณะของพื้นที่โดยรอบที่อยู่ภายนอกนอกขอบเขตพื้นที่ (ภาพ 4.3) ซึ่งรวมถึงสิ่งอำนวยความสะดวกและประเภทของธุรกิจที่อยู่บริเวณใกล้เคียงว่ามีประเภทใดบ้าง? อย่างไรก็ตาม ลักษณะของสถานประกอบการย่อมต้องการระบบการรักษาความมั่นคงปลอดภัยที่แตกต่างกัน อาทิ โรงเรียนมัธยมต้องมีการพิจารณาการป้องกันที่แตกต่างจากโรงงานอุตสาหกรรมเคมี รวมถึงการพิจารณาว่าสถานที่นั้นอยู่ในระยะสายตาของอาคารอื่น ๆ (การเฝ้าระวังที่ไม่ต้องการ) หรือใกล้กับแนวต้นไม้หนาแน่นที่อยู่ติดกันหรือไม่? ยิ่งไปกว่านั้น ถ้าพื้นที่อยู่ในเขตเมือง ปัจจัยทางกายภาพ เช่น ทางเท้า ขอบถนน ถนน และบริเวณใกล้เคียง จำเป็นต้องมีการศึกษาอย่างละเอียด ยิ่งไปกว่านั้น การรักษาความปลอดภัยอาจรวมถึงวัตถุที่อยู่ภายในพื้นที่ เช่น กระถางต้นไม้ ม้านั่ง ถังขยะ ไฟถนน และกล้องวงจรปิด ทั้งนี้ การใช้ระบบสารสนเทศทางภูมิศาสตร์ (GIS) นับว่าเป็นเครื่องมือที่สำคัญสำหรับการศึกษาระดับชั้นความปลอดภัยอีกด้วย (Federal Emergency Management Agency, 2005)



ภาพ 4.4 มหาวิทยาลัยอาจมีทางเข้าแบบเปิด และอาคารแต่ละหลังอาจมีการป้องกันที่แตกต่างกันตั้งแต่การควบคุมการเข้าถึงขั้นต่ำไปจนถึงการป้องกันทั้ง 3 ระดับที่สมบูรณ์รอบอาคารที่มีความเสี่ยงสูง ในกรณีพื้นที่ตัวอย่างนี้ สถานที่ต่าง ๆ รวมถึงอาคารภายในมหาวิทยาลัยจะเป็นส่วนหนึ่งของชั้นป้องกันชั้นที่ 1 และ 2 ของอาคารที่มีความเสี่ยงสูง (Federal Emergency Management Agency, 2007)

การป้องกันชั้นที่ 2 (second layer of defense) จะอยู่ระหว่างพื้นที่บริเวณของที่ตั้งและอาคาร (ภาพ 4.3 และ 4.4) โดยส่วนใหญ่พื้นที่ภายนอกอาคารมักเป็นอาณาบริเวณที่อยู่ในเขตเมือง ซึ่งทำให้เกิดปัญหาด้านความมั่นคงปลอดภัยที่เพิ่มมากขึ้น การป้องกันชั้นที่สองจะต้องพิจารณาการรักษาความมั่นคงปลอดภัยสามประเภทหลัก ได้แก่ (1) บุคลากร (2) นโยบายและกระบวนการ และ (3) เทคโนโลยี โดยมุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยอาณาเขตโดยรอบ จุดทางเข้า จุดขนถ่ายสินค้า ทางเดินรถ ที่จอดรถ ทางเดินเท้า สิ่งกีดขวางตามธรรมชาติและที่ถูกสร้างขึ้น ความหนาแน่นของพรรณไม้ การปกป้องระบบสาธารณูปโภคและช่องเปิด ไฟส่องสว่าง ระบบตรวจจับการบุกรุก กล้องวงจรปิด และการลาดตระเวนรักษาความปลอดภัย ทั้งนี้ ในกรณีของการป้องกันการวางระเบิด พื้นที่ป้องกันจำเป็นต้องมีระยะห่างในการเผชิญหน้า (stand-off distance) ยิ่งระยะห่างจากจุดที่มีการระเบิดห่างจากอาคารมากเท่าไรก็ยิ่งดี (ภาพ 4.5) อย่างไรก็ตาม ในพื้นที่เมืองที่มีความหนาแน่นสูง ระยะห่างในการเผชิญหน้าก็จะมีขนาดที่จำกัดด้วยเช่นกัน ซึ่งอาจแก้ไขได้ด้วยการหลีกเลี่ยงการออกแบบทางเดินรถที่ตรงไปยังอาคารและบริเวณที่จอดรถที่ใกล้เคียงกับอาคาร อย่างไรก็ดี แนวคิดที่สำคัญที่ควรพิจารณาสำหรับการป้องกันชั้นที่สอง ได้แก่ พื้นที่ป้องกันตนเอง การป้องกันอาชญากรรมด้วยการออกแบบสิ่งแวดล้อม (CPTED) การป้องกันอาชญากรรมตามสถานการณ์ ทฤษฎีการตัดสินใจเลือกอย่างมีเหตุผล และทฤษฎีอื่น ๆ ของอาชญาวิทยาที่เกี่ยวข้องกับความปลอดภัย (Purpura, 2018)

การป้องกันชั้นที่ 3 (third layer of defense) จะมุ่งเน้นไปที่ตัวทรัพย์สินเป็นหลัก เช่น อาคาร หากการป้องกันในชั้นที่ 1 และชั้นที่ 2 ล้มเหลว ชั้นที่ 3 จะมีความสำคัญมากเป็นพิเศษ เนื่องจากเป็นสเหมือนเส้นเลือดใหญ่ขององค์กร กล่าวคือ ผู้คน และทรัพย์สินทั้งทางกายภาพและเสมือนจริง ทั้งนี้ การป้องกันชั้นที่ 3 จะมุ่งเน้นไปที่กลยุทธ์หลายอย่างที่พิจารณาในชั้นที่ 2 แต่นำไปใช้กับตัวอาคาร ซึ่งรวมถึงกลยุทธ์ที่เกี่ยวข้องกับบุคลากรด้านความมั่นคงปลอดภัย นโยบายและกระบวนการ เทคโนโลยี และทฤษฎีอาชญวิทยาที่เกี่ยวข้องกับความมั่นคงปลอดภัย อาทิ การขโมยทรัพย์สินเป็นอันตรายมากอย่างยิ่งสำหรับอาคารที่อาจเป็นที่ตั้งของทรัพย์สินที่มีค่าที่สุด ดังนั้น กลยุทธ์ด้านความปลอดภัยที่เหมาะสมสำหรับอาคาร ได้แก่ ระบบควบคุมการเข้าออก ประตูล็อค กล้องวงจรปิด ไฟส่องสว่าง เจ้าหน้าที่รักษาความมั่นคงปลอดภัย และระบบตรวจจับการบุกรุกภายใน ยิ่งไปกว่านั้น ในกรณีของการก่อการร้าย อาคารควรมีแผนฉุกเฉินและการอพยพ และระบบป้องกันอัคคีภัยในการป้องกันการก่อการร้าย ทั้งนี้ มาตรการที่สำคัญ ได้แก่ โครงสร้างและกระจกที่ทนต่อแรงระเบิด ระบบกลไกและไฟฟ้าที่มีความต้านทานสูง ระบบปรับอากาศ (heating, ventilation, and air conditioning หรือ HVAC) ที่มีการกรองอากาศที่มีประสิทธิภาพ รวมถึงช่องรับอากาศจากภายนอกที่ปลอดภัยที่อยู่สูงเหนือพื้นดิน ระบบดูดควัน (smoke evacuation system) และการควบคุมการเข้าถึงที่เข้มงวดสำหรับอาคารจอดรถและชั้นใต้ดิน เป็นต้น (Johnston, 2010)



ภาพ 4.5 ระยะห่างในการเผชิญหน้าเป็นปัจจัยที่สำคัญในการกำหนดขอบเขตของความเสียหาย ทั้งนี้ระยะห่างที่เหมาะสมนั้นขึ้นอยู่กับประเภทของภัยคุกคาม ประเภทของสิ่งปลูกสร้าง และระดับการป้องกันที่ต้องการ อย่างไรก็ตาม แนวทางปฏิบัติที่ยอมรับโดยทั่วไปของระยะห่างในการเผชิญหน้าขั้นต่ำคือ 25 เมตร (82 ฟุต) ในการป้องกันภัยคุกคามจากการระเบิดขนาดเล็ก (Federal Emergency Management Agency, 2007)

ประโยชน์ของการจัดระดับชั้นความมั่นคงปลอดภัยคือการนำเสนอภาพลักษณ์ของสถานที่เป้าหมายที่มีการป้องกันอย่างดี รวมถึงการให้ความสำคัญกับความมั่นคงปลอดภัยอย่างจริงจัง ทั้งนี้ขึ้นอยู่กับความต้องการทางธุรกิจและช่องโหว่ของการป้องกัน การแบ่งระดับชั้นความมั่นคงปลอดภัยจะทำให้ผู้คนและยานพาหนะเข้าถึงหรือเข้าไปในสถานที่ได้ยากลำบากขึ้นหรือช้าลง ทำให้องค์กรมีเวลามากขึ้นในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัย เช่น การสังเกตพฤติกรรมและวัตถุที่ต้องสงสัย ยิ่งไปกว่านั้น ผู้บริหารงานด้านความมั่นคงปลอดภัย จะต้องให้ความสำคัญกับการวางแผนอย่างมีวิจารณญาณในการวางระบบการรักษาความมั่นคงปลอดภัยแบบหลายชั้น เพื่อให้มั่นใจว่าแต่การรักษาความมั่นคงปลอดภัยแต่ละระดับชั้นมีความคุ้มค่ากับค่าใช้จ่ายอย่างไร ไม่มีการพึ่งพาชั้นใดชั้นหนึ่งมากเกินไป หรือเกิดอุปสรรคขัดขวางการกันระหว่างระดับชั้นการรักษาความมั่นคงปลออดภัย

ความซ้ำซ้อน (redundancy) หมายถึงการทำซ้ำของระบบหรือกระบวนการรักษาความมั่นคงปลอดภัยที่สำคัญ เพื่อให้มั่นใจว่ามาตรการรักษาความมั่นคงปลอดภัยมีความพร้อมในการใช้งาน เพิ่มความน่าเชื่อถือและประสิทธิผลอย่างต่อเนื่อง แม้ว่าจะเผชิญกับความล้มเหลวของระบบป้องกัน ไม่ว่าจากการทำงานผิดปกติหรือการโจมตีก็ตาม ทั้งนี้ เป้าหมายหลักของความซ้ำซ้อนในการจัดการความมั่นคงปลอดภัยคือการลดความเสี่ยงของการละเมิดความปลอดภัยและการหยุดชะงักของการปฏิบัติงาน โดยการจัดเตรียมกลไกและทรัพยากรสำรอง ความซ้ำซ้อนจึงถือว่าเป็นสิ่งสำคัญในการรับรองความยืดหยุ่นและความต่อเนื่องของมาตรการรักษาความปลอดภัยเพื่อลดโอกาสที่จะเกิดความล้มเหลวจากเพียงจุดเดียวที่อาจกระทบต่อความปลอดภัยและการปกป้องทรัพย์สิน รวมถึงสิ่งอำนวยความสะดวกทั้งหมด

โดยทั่วไป ความซ้ำซ้อนเกี่ยวข้องกับการมีมาตรการรักษาความมั่นคงปลอดภัยทางเลือกเพื่อลดความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางกายภาพ เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม หรือการก่อกวน ทั้งนี้ ระบบสำรองอาจมีหลายรูปแบบ อาทิ กล้องวงจรปิดสำรอง จุดควบคุมการเข้าถึงหลายจุด ระบบเตือนภัยสำรอง หรือกำลังเสริมของหน่วยรักษาความมั่นคงปลอดภัย หรืออีกนัยหนึ่ง ระบบการรักษาความมั่นคงปลอดภัยแบบซ้ำซ้อนประกอบด้วยกลยุทธ์การรักษาความมั่นคงปลอดภัยที่คล้ายกันตั้งแต่สองระบบขึ้นไป เช่น ระบบตรวจจับการบุกรุกสองระบบตามแนวเส้นรอบวง ตัวอย่างเช่น เรือนจำมักจะมีรั้วสองหรือสามชั้นล้อมรอบเพื่อป้องกันการหลบหนี ในขณะที่ โรงงานไฟฟ้าพลังงานนิวเคลียร์มักจะมีระบบรักษาความปลอดภัยที่ซ้ำซ้อน นอกเหนือจากระบบดับเพลิงและระบบความปลอดภัยอื่น ๆ โดยที่ประโยชน์ของการรักษาความมั่นคงปลอดภัยแบบซ้ำซ้อนอีกข้อหนึ่งก็คือ หากระบบหนึ่งล้มเหลว อีกระบบหนึ่งจะดำเนินการทำงานตามที่ต้องการต่อไปได้ เช่น จุดประสงค์ของระบบตรวจจับการบุกรุกสองระบบ คือ การตรวจสอบซ้ำว่าสัญญาณเตือนเป็นสัญญาณแท้จริงหรือไม่นั่นเอง (ASIS International, 2018)

ตัวคูณกำลัง (force multipliers) ในการจัดการความมั่นคงปลอดภัย หมายถึง กลยุทธ์ เทคโนโลยี หรือมาตรการที่ขยายประสิทธิผลของบุคลากรและทรัพยากรด้านความมั่นคงปลอดภัย ซึ่งเป็นการทำให้บุคลากร ทรัพย์สิน และองค์กรได้รับการปกป้อง ป้องกัน และการบรรเทาภัยคุกคามที่สูงขึ้น กลยุทธ์ตัวคูณกำลังนี้ครอบคลุมเครื่องมือและเทคนิคต่าง ๆ อาทิ ระบบเฝ้าระวัง (surveillance systems) ระบบควบคุมการเข้าถึง (access control system) ระบบตรวจจับการบุกรุก (intrusion detection system) และเทคโนโลยีระบบรักษาความมั่นคงปลอดภัยอัตโนมัติ (security automation technology) ด้วยเหตุนี้ การรวมตัวคูณกำลังเหล่านี้เข้ากับกรอบการทำงานด้านความมั่นคงปลอดภัย องค์กรต่าง ๆ จะสามารถเพิ่มประสิทธิภาพของกระบวนการรักษาความมั่นคงปลอดภัยและทรัพยากรของตนเองได้ และจะช่วยให้เจ้าหน้าที่รักษาความมั่นคงปลอดภัยสามารถตอบสนองต่อภัยคุกคามและเหตุการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพมากขึ้น

โดยทั่วไป ตัวคูณกำลังมีบทบาทสำคัญในการยกระดับมาตรการรักษาความมั่นคงปลอดภัย โดยรวมและเพิ่มความยืดหยุ่นขององค์กร โดยใช้ประโยชน์จากเทคโนโลยีและกลยุทธ์ขั้นสูงเพื่อเพิ่มขีดความสามารถของทีมรักษาความมั่นคงปลอดภัย ทั้งนี้ ตัวคูณกำลังอาจใช้เทคนิค เช่น กล้องวงจรปิดช่วยให้เจ้าหน้าที่หนึ่งคนสามารถรับชมสถานที่หลายแห่งในคราวเดียวจากที่เดียว ในทำนองเดียวกัน ระบบตรวจจับการบุกรุกที่ติดตั้งหลายจุดทำให้สามารถติดตามได้โดยเจ้าหน้าที่คนเดียวจากที่เดียว ด้วยเหตุนี้ ผู้บริหารความมั่นคงปลอดภัยที่ชาญฉลาดจะเข้าใจถึงคุณค่าและประโยชน์ของการสรรหาบุคลากรที่มีความสามารถเข้าสู่กระบวนการรักษาความมั่นคงปลอดภัย ซึ่งสามารถทำได้ผ่านโครงการปฐมนิเทศพนักงานใหม่ การฝึกอบรม และโปรแกรมพิเศษที่สร้างความตระหนักรู้เกี่ยวกับความปลอดภัยและการรายงานเหตุการณ์

ผู้บริหารงานด้านความมั่นคงปลอดภัยสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยผ่านทางอีเมล หรือระบบอินทราเน็ตของบริษัท โปสเตอร์ จดหมายข่าว การประชุม และฝึกอบรมหรือการฝึกซ้อม โดยเฉพาะการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยและการฝึกอบรมเพื่อให้สอดคล้องกับกฎระเบียบและกฎหมายเฉพาะที่เกี่ยวข้องหรือตามนโยบายของรัฐบาล นอกจากนี้ การประเมินประสิทธิผลของโปรแกรมการรับรู้ผ่านการสำรวจเป็นระยะ ๆ เช่น ผ่านอินทราเน็ตขององค์กรก็เป็นสิ่งสำคัญ นอกจากนี้ ผู้บริหารงานด้านความมั่นคงปลอดภัยควรทำงานร่วมกับผู้บริหารในแผนกอื่น ๆ ขององค์กร (เช่น ทรัพยากรบุคคล การบริหารความเสี่ยง กฎหมาย และฝ่ายปฏิบัติการ) เพื่อสร้างการสนับสนุนสำหรับวัตถุประสงค์ด้านความมั่นคงปลอดภัย (Kotwica, 2007) นอกจากนั้น อีกช่องทางหนึ่งสำหรับการรับรู้คือ ‘กลุ่มธุรกิจเตือนภัย’ (Business Watch) ซึ่งได้แนวคิดมาจาก ‘การเฝ้าระวังอาชญากรรมในละแวกบ้าน’ หรือ ‘เพื่อนบ้านเตือนภัย’ (Neighborhood Watch) ที่ช่วยอำนวยความสะดวกในการสร้างความสัมพันธ์ระหว่างภาคเอกชนและเจ้าหน้าที่ตำรวจในการป้องกันอาชญากรรม (ดวงฤทธิ์ เบ็ญจาธิกุล ชัยรุ่งเรือง, 2559) การฝึกอบรมพนักงานให้รายงานกิจกรรมและอาชญากรรมที่ต้องสงสัย การส่งเสริมการใช้ป้ายระบุวัตถุที่สามารถตรวจสอบย้อนหลัง (traceable identification tag) และแนะนำพนักงานเกี่ยวกับการป้องกันตนเองและการป้องกันอาชญากรรม เป็นต้น

กล่าวได้ว่า ตัวคูณกำลัง ส่วนหนึ่งเป็นผลมาจากการมีความสัมพันธ์ที่ดีกับหน่วยงานของรัฐเมื่อเกิดเหตุการณ์ไม่พึงประสงค์ หน่วยงานเหล่านี้ได้แก่ ตำรวจ ดับเพลิง บริการการแพทย์ฉุกเฉิน โรงพยาบาล และหน่วยจัดการเหตุฉุกเฉิน เช่น ฝ่ายป้องกันและบรรเทาสาธารณภัย ทั้งนี้ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยควรสร้างความสัมพันธ์เชิงบวกกับหน่วยงานภาครัฐก่อนที่เหตุการณ์ไม่พึงประสงค์จะเกิดขึ้น ด้วยเหตุนี้ กลยุทธ์ที่สำคัญที่สุดประการหนึ่งของผู้บริหารหรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยคือการสร้างความสัมพันธ์ที่แน่นแฟ้นกับหน่วยงานภาครัฐ โดยเฉพาะหน่วยงานบังคับใช้กฎหมาย ซึ่งสามารถทำได้โดยการร่วมประชุมกัน ส่งเสริมการสร้างความสัมพันธ์ผ่านการช่วยเหลือซึ่งกันและกัน การฝึกอบรมข้ามสายงาน และแบ่งปันข้อมูลและองค์ความรู้ เป็นต้น (Mallery, 2007)

บทสรุป

กลยุทธ์การจัดการความมั่นคงปลอดภัยที่ดีจะต้องครอบคลุมการป้องกันหลายชั้น และใช้เทคนิคต่าง ๆ เพื่อปกป้องบุคคล ทรัพย์สิน และลดความเสี่ยงอย่างมีประสิทธิภาพ กลยุทธ์การรักษาความมั่นคงปลอดภัยได้รับการออกแบบมาเพื่อจัดการกับภัยคุกคามและช่องโหว่ต่าง ๆ โดยการใช้ชั้นการรักษาความปลอดภัยหลายระดับชั้น เช่น การควบคุมการเข้าถึง การเฝ้าระวัง และการเตือนภัย เพื่อสร้างระบบการป้องกันที่แข็งแกร่ง ยิ่งไปกว่านั้น ความซ้ำซ้อนเป็นองค์ประกอบสำคัญที่เกี่ยวข้องกับระบบสำรองข้อมูลและมาตรการต่าง ๆ เพื่อให้มั่นใจถึงความต่อเนื่องและความยืดหยุ่นเมื่อเผชิญกับความล้มเหลวหรือการหยุดชะงักของการปฏิบัติงานเนื่องจากเหตุการณ์ที่ไม่พึงประสงค์ นอกจากนี้ กลยุทธ์ดังกล่าวยังรวมเอาตัวคูณกำลัง เช่น เทคโนโลยีขั้นสูงและระบบอัตโนมัติ เพื่อขยายขีดความสามารถของบุคลากรและทรัพยากรด้านความมั่นคงปลอดภัย เพิ่มประสิทธิภาพและประสิทธิผลของความพยายามป้องกันด้านความมั่นคงปลอดภัย องค์ประกอบเหล่านี้ เมื่อบูรณาการร่วมกันแล้ว จะสร้างแนวทางการรักษาความมั่นคงปลอดภัยที่มีความเป็นพลวัตและปรับเปลี่ยนได้ ซึ่งมีความสำคัญในภูมิทัศน์การรักษาความมั่นคงปลอดภัยที่มีการพัฒนาอยู่ตลอดเวลาในปัจจุบัน ซึ่งการป้องกันแบบหลายแง่มุม (multifaceted) ถือเป็นสิ่งสำคัญในการป้องกันภัยคุกคามทางกายภาพและทางไซเบอร์ที่หลากหลายนั่นเอง

เอกสารอ้างอิง

ASIS International. (2018). *Physical Asset Protection: An Interdisciplinary Approach.* ASIS International.

Federal Emergency Management Agency. (2003, December). Primer: for design of commercial buildings to mitigate terrorist attacks. *FEMA 427*. Washington, DC: U.S. Department of Homeland Security.

Federal Emergency Management Agency. (2005, Januray). Risk assessment: A how-to guide to mitigate potential terrorist attacks against. *FEMA 452*. Washington, DC: U.S. Department of Homeland Security.

Federal Emergency Management Agency. (2007, December). Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks. *FEMA 430*. Washington, DC: U.S. Department of Homeland Security.

Johnston, R. G. (2010). Security Management. *Lessons for layering, 54*(January), 65-69.

Kennedy, D. M. (2009). *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction.* London: Routledge. doi:10.4324/9780203892022

Kotwica, K. (2007, September). Is your security awareness program all it can be? *Security Technology & Design, 17*, p. 20.

Mallery, J. (2007, September). Security cooperation. *Security Technology & Design, 17*, p. 44.

Peter, E., & Schiller, T. (2008, April 15). *A Practical Guide to Honeypots*. Retrieved February 14, 2023, from Washington University in St. Louis: https://www.cse.wustl.edu

Purpura, P. P. (2018). *Security and Loss Prevention: An Introduction* (7th ed.). Cambridge, MA: Butterworth-Heinemann.

Secret Double Octopus. (2023). *Multi Factor Authentication (MFA)*. Retrieved January 15, 2023, from The Secret Security Wiki: https://doubleoctopus.com

ดวงฤทธิ์ เบ็ญจาธิกุล ชัยรุ่งเรือง. (2559). ยุทธ์ศาสตร์แบบมีส่วนร่วมต่อการป้องกันและปราบปรามอาชญากรรมของสถานีตำรวจนครบาลในพื้นที่เขตบางแค. *วารสารวิชาการ มหาวิทยาลัยกรุงเทพธนบุรี, 5*(1), 30-41.

ปริญญา หอมอเนก. (18 กันยายน 2546). *จะลงทุนกับ IDS, IPS หรือ Honeypot อย่างไหนจะคุ้มค่ากว่ากัน?* Retrieved ธันวาคม 15, 2565, from ACIS Professional Center: https://www.acisonline.net