แนวทางปฏิบัติ การประเมินความเสี่ยง ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

สารบัญ

แนวทางปฏิบัติการประเมินความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (INTRODUCTION)

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อทางสถาบัน ดังนั้นจึงมีความจำเป็นในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงของสถาบัน โดยการประเมินความเสี่ยงทำให้สามารถ:

- ระบุเหตุการณ์ความเสี่ยงที่เป็นภัยคุกคาม และอาจนำไปสู่กระทบต่อสถาบันในด้านต่างๆ
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้สถาบันสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในสถาบัน เพื่อให้เจ้าหน้าที่ของสถาบันมีส่วนร่วมในการจัดการเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์ (PURPOSE)

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีกรอบการดำเนินงานเกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

๓. กลุ่มเป้าหมาย (Audience)

กลุ่มเป้าหมายมีดังต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) (เช่น หัวหน้างาน ผู้ดูแลระบบ หัวหน้างาน เจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ ฯลฯ) ภายในสถาบัน
- ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของสถาบัน

๔. ขอบเขต (SCOPE)

ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๕. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

เป็นการสร้างข้อกำหนดที่สำคัญสำหรับการประเมินความเสี่ยง เพื่อให้กลุ่มเป้าหมาย ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๕.๑ นิยามความเสี่ยงทางไซเบอร์

คือแนวโน้มที่จะได้รับผลกระทบจากการหยุดชะงักต่อข้อมูลที่ละเอียดอ่อน การเงิน หรือการดำเนินกิจกรรมทางด้านออนไลน์ รวมถึงการให้บริการที่มีความเกี่ยวข้องต่อการดำเนินงานและการให้บริการประชาชนโดยทั่วไป ความเสี่ยงทางไซเบอร์มีความเกี่ยวข้องกับเหตุการณ์ที่อาจส่งผลให้เกิดการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูลเพื่อให้ไม่สามารถให้บริการได้

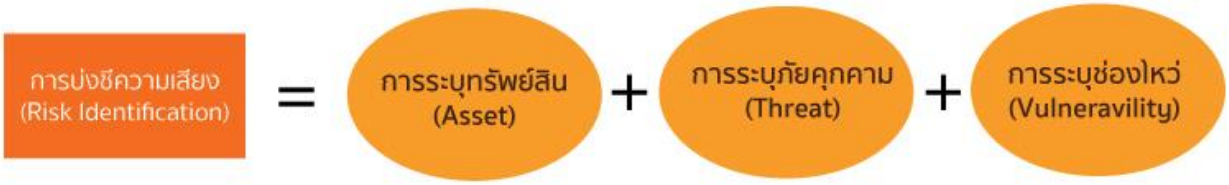
การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ช่วยให้สถาบันเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของสถาบันได้ การใช้มาตรการรักษาความปลอดภัยทางไซเบอร์ มีวิธีการคำนวณตาม OWASP Risk Assessment

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

การบ่งชี้ความเสี่ยง

เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อเป้าหมายของสถาบันหรือการปฏิบัติงาน เช่น ทรัพย์สิน ภัยคุกคาม ห่องโหว่ด้านความปลอดภัย



ภาพการบ่งชี้ความเสี่ยงตามแนวทางของมาตรฐานสากล ISO/IEC 27005

สินทรัพย์สารสนเทศ

หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ได้แก่ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น มีวัตถุประสงค์เพื่อสนับสนุนงานเผยแพร่ประชาสัมพันธ์ งานอบรม ประชุม สัมมนาของสถาบัน

ระบุประเภททรัพย์สินสารสนเทศ (Identification of Asset Types)

เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์ การโจมตี (Threat Vector)) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

• **Ransomware (แรนซัมแวร์)** ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware

• **Phishing (ฟิชชิง)** คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล

• **Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย)** คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น

• **Virus (ไวรัส)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างซึ่งโดยมุ่งเน้นในการโจมตี ขัดขวาง เพื่อไม่ให้ระบบสามารถใช้งานได้

• **Worms (เวิร์ม)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

• **Trojan (โทรจัน)** เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

• **Spyware (สปายแวร์)** ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล

• **Adware (แอดแวร์)** คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้

• **Data leaks (ข้อมูลรั่วไหล)** ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ

๕.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินงานที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าสถาบันยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:
- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนจำเป็นต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับการพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

๕.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

ผู้บริหาร (Head of Organization)

เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในสถาบันที่มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของสถาบัน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในสถาบัน ที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งสถาบัน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และ

จัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในสถาบัน ที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมของสถาบัน พวกเขาควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

บุคคลหรือกลุ่มภายในสถาบัน ที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุม ความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมของสถาบัน โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

๖. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อมและการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)

รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๖.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

- **ระบุทรัพย์สิน (Identify Assets)**
- **การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)**

การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) –ข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคาม

๒. การระบุภัยคุกคาม (Threat Identification) –เพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว สถาบันควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้สถาบันสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

- **สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)**

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันกับสภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้:

- ทรัพย์สิน (Asset) - สิ่งที่มีค่าที่ได้รับการระบุในงาน A

- เหตุการณ์ภัยคุกคาม (Threat event) - เหตุการณ์การโจมตีที่ระบุในงาน B

- ช่องโหว่ (Vulnerability) - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

- ผลที่ตามมา (Consequence) – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

๖.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงตามแต่สถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น; และ

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

- **กำหนดโอกาส (Determine Likelihood)**

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าว เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) ● สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: ● สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย ● สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไปโดยไม่ต้องมีความรู้ด้านเทคนิค	การโจมตี: ● สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configuration)[๑] หรือเงื่อนไขของเหตุการณ์ (Event Condition)[๒] ● สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Medium (๒)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing)) ● สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน	การโจมตี: ● สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root) ● สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: ● สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง ● สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย ● สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	การโจมตี: ● สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root) ● สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	การโจมตี: ● สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง ● สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

ตัวอย่างตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

- **กำหนดผลกระทบ (Determine Impact)**

โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้:

- ระดับชาติ (National) – ในระดับประเทศ ผลกระทบอาจถูกมองว่าเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ

- องค์กร (Organisational) – ในระดับองค์กร ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงักในการดำเนินการ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

- บุคคล (Individual) - ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิตและการบาดเจ็บ

ตารางด้านล่าง คือ ตัวอย่างตารางประเมินสำหรับการพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่างเป็นข้อมูลทั่วไป เมื่อใช้ตารางผลกระทบที่คล้ายกัน สถาบันควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการเพื่อให้แน่ใจว่า

- เกี่ยวข้องกับบริบททางธุรกิจ (Relevant to business context) – เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของสถาบันหรือวัดผลงาน

- ไม่กำกวม (Unambiguous) - ใช้คำอธิบายที่เป็นเลขฐานสองหรือที่มีช่วงเชิงปริมาณ (เช่น การรั่วไหลของข้อมูลที่ถูกจัดประเภทเป็น “ความลับ” หรือทำให้การบริการของลูกค้ามากกว่าร้อยละ ๕๐ หยุดชะงัก)

- มุมมองที่หลากหลาย (Multi-perspectives) - ระบุประเภทย่อยของผลกระทบจากแต่ละระดับจาก ๓ ระดับ (เช่น ระดับประเทศ องค์กร และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	**ผลกระทบที่อาจเกิดขึ้น (potential impact)***		
	ต่ำ	**กลาง**	**สูง**
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
	Secondary National Interests)		National Interests)
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน(Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคนหรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิตร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคนแต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของสถาบัน	ไม่มีผลกระทบหรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของสถาบันเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของสถาบันด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน	การดำเนินการตามหน้าที่หลักของสถาบันต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

๖.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

- **กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)**

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยงสำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง

IMPACT				
	High (๓)	M๓๑	H๓๒	H๓๓
	Medium (๒)	L๒๑	M๒๒	H๒๓
	Low (๑)	L๑๑	L๑๒	L๑๓
		Low (๑)	Medium (๒)	High (๓)
		LIKELIHOOD		

เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยสถาบัน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

- **ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)**

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความ

เสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของสถาบัน มีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบัน เมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- สถานการณ์ความเสี่ยง (Risk Scenario) – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร

- วันที่ระบุความเสี่ยง (Identification Date) – วันที่ที่ระบุสถานการณ์ความเสี่ยง

- มาตรการที่มีอยู่ (Existing Measures) – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง

- ความเสี่ยงในปัจจุบัน (Current Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)

- แผนจัดการความเสี่ยง (Treatment Plan) – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของสถาบัน)

- สถานะความคืบหน้า (Progress Status) – สถานะของการดำเนินการตามแผนจัดการ ความเสี่ยง

- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

- เจ้าของความเสี่ยง (Risk Owner) – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของสถาบัน

๗. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของสถาบัน

๗.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของสถาบันเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้สถาบันมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยงที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือสถาบันอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของการแบ่งปันความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในสถาบันจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการและตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๗.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม สถาบันควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่าตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย สถาบันอาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคาแพง

เมื่อสถาบันเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยงหรือการลดผลกระทบจากความเสี่ยง

เอกสารอ้างอิง

๑. GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, FEBRUARY ๒๐๒๑
Link: https://www.csa.gov.sg/docs/defaultsource/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf

๒. NIST SP ๘๐๐-๓๐ Rev. ๑ Guide for Conducting Risk Assessments, NIST, September ๒๐๑๒
Link: https://csrc.nist.gov/publications/detail/sp/๘๐๐-๓๐/rev-๑/final

๓. ISO ๓๑๐๐๐:๒๐๑๘(en) Risk management — Guidelines, ISO, FEBRUARY ๒๐๑๘
Link: https://www.iso.org/obp/ui/#iso:std:iso:๓๑๐๐๐:ed-๒:v๑:en

๔. ISO/IEC ๒๗๐๐๕:๒๐๑๘ Information technology — Security techniques — Information security risk management, ISO/IEC, July ๒๐๑๘
Link: https://www.iso.org/standard/๗๕๒๘๑.html

๕. ตัวอย่างแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ Link: bit.ly/ncsa44