


# แนวทางปฏิบัติการประเมินความเสี่ยง
# ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
# มหาวิทยาลัยราชภัฏมหาสารคาม
# พ.ศ. 2566

# สารบัญ

๑. บทนำ (INTRODUCTION)

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๑.๒ ปัญหาทั่วไปที่สังเกตได้

๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต (PURPOSE, AUDIENCE & SCOPE)

๒.๑ วัตถุประสงค์ของเอกสาร

๒.๒ กลุ่มเป้าหมายและขอบเขต (Audience & Scope)

๓. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

๓.๑ กำหนดความเสี่ยง (Define Risk)

๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

๔. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

๔.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

๕. ตอบสนองต่อความเสี่ยง

๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options) ๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

เอกสารอ้างอิง

## ๑. บทนำ (INTRODUCTION)

### ๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น หน่วยงานต่าง ๆ อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงานและวัตถุประสงค์ทางธุรกิจ ดังนั้นจึงมีความจำเป็นสำหรับหน่วยงาน ในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยง ระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจาก การกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์

- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดี เกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด

- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยง เป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธี ที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

### ๑.๒ ปัญหาทั่วไปที่สังเกตได้

ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติ ในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่ง ก็ประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกตเห็น ได้แก่

ก. การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็น เรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้ การเข้าใจขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมาย เพื่อจัดการกับความเสี่ยง กระทำได้ยาก

ข. การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุม ความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่าง เทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยงทำให้ เกิดพฤติกรรม

“รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัย ว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

ค. การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

ง. การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้ อาจไม่ ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับ เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

จ. จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

## ๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต (PURPOSE, AUDIENCE & SCOPE)

### ๒.๑ วัตถุประสงค์ของเอกสาร

วัตถุประสงค์ของเอกสารนี้คือเพื่อให้คำแนะนำแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน) เกี่ยวกับวิธีดำเนินการประเมินความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

เอกสารนี้จะระบุถึงความคาดหวังที่หน่วยงานพึงปฏิบัติจำเป็นต้องรับทราบเมื่อทำการประเมินความเสี่ยง ความคาดหวังจะแสดงด้วยไอคอนด้านล่างในแนวทางฉบับนี้

### ๒.๒ กลุ่มเป้าหมายและขอบเขต (Audience & Scope)

เอกสารนี้มีขึ้นเพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) (เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบ หัวหน้าเจ้าหน้าที่ รักษาความมั่นคงปลอดภัยสารสนเทศ ฯลฯ) ภายในหน่วยงาน
- ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน
- ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น

สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความ เสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

**๓. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)**

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

**๓.๑ กำหนดความเสี่ยง (Define Risk)**

มีคำจำกัดความมากมายเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น ก่อนที่จะ กำหนดรายละเอียดเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยง สิ่งสำคัญคือต้องกำหนดคำนิยามทั่วไป ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยงถูก กำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ:

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

| Risk = Function (Likelihood, Impact) |
|---|

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

**เหตุการณ์ภัยคุกคาม** (Threat Event)

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

**ช่องโหว่** (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ

**ความน่าจะเป็น** (Likelihood)

ความน่าจะเป็น หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์ จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ

(Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และ ความสามารถในการทำซ้ำ (Reproducibility)

**ผลกระทบ** (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

**๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)**

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance)" หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุ ได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยงและต้องปรับแต่งตามแต่ละรายการเพื่อให้เหมาะสมกับบริบทของหน่วยงาน

| ระดับความเสี่ยง (Risk Level) | คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description) |
|---|---|
| High | ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนจำเป็น ต้องดำเนินการทันที |
| Medium | ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับ การพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า |
| Low | ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจ ว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม |

ตัวอย่างการแสดงการยอมรับความเสี่ยง

**สิ่งที่หน่วยงานพึงปฏิบัติ**

ในรายงานการประเมินความเสี่ยงหน่วยงาน จะต้องกำหนดระดับการยอมรับความเสี่ยงให้ชัดเจน ทั้งนี้หน่วยงานอาจพิจารณาใช้ระดับความน่าจะเป็น ผลกระทบที่เกิดขึ้น และความเสี่ยงที่ยอมรับได้ ที่แตกต่างกันไปตามที่หน่วยงานเห็นสมควร

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

**หัวหน้าหน่วยงาน** (Head of Organization)

เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่ และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับ การจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

**เจ้าของกระบวนการธุรกิจ** (Business Owner)

เจ้าหน้าที่อาวุโสระดับสูงสุดของหน่วยธุรกิจ (Business Unit) ที่รับผิดชอบในการตรวจสอบ ให้แน่ใจว่ากิจกรรมทางธุรกิจบรรลุเป้าหมายทางธุรกิจ หรือแบ่งปันข้อกังวลเกี่ยวกับผลกระทบที่มีต่อธุรกิจในกรณีที่ระบบมีการหยุดชะงัก

**ฟังก์ชั่นการบริหารความเสี่ยง** (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยง ที่สอดคล้องกัน

**ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน** (Technology and Operations Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุน กิจกรรมทางธุรกิจ พวกเขาควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

**ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์** (Cybersecurity Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมทางธุรกิจ โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนด โอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

**สิ่งที่หน่วยงานพึงปฏิบัติ**

ในรายงานการประเมินความเสี่ยงหน่วยงาน จะต้องระบุบทบาทและความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการดำเนินการประเมินความเสี่ยงอย่างชัดเจน

**๔. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)**

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)




รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๔.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

**งาน A: ระบุทรัพย์สิน (Identify Assets)**

ดังสุภาษิตความมั่นคงปลอดภัยโบราณที่ว่า “คุณไม่สามารถปกป้องสิ่งที่คุณไม่รู้ได้” ดังนั้น สิ่งแรกที่ควรดำเนินการคือการระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็น ระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง เมื่อระบุทรัพย์สิน สิ่งสำคัญคือต้องจดบันทึกทรัพย์สินเหล่านั้น

• ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์ทาง ธุรกิจโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์

ตัวอย่าง: ในระบบควบคุมแบบกระจาย (Distributed Control System (DCS)) ของโรงไฟฟ้า โปรแกรมควบคุมลอจิกแบบตั้งโปรแกรมได้ (Programmable Logic Controller (PLC)) ที่ควบคุมระบบไฟฟ้ามักจะได้รับการพิจารณาว่าเป็นทรัพย์สินสำคัญ เนื่องจากมีผลโดยตรงต่อการผลิตไฟฟ้า ซึ่งเป็นวัตถุประสงค์ ทางธุรกิจโดยรวมของโรงไฟฟ้า

ผู้โจมตีที่ต้องการขัดขวางการผลิตไฟฟ้ามีแนวโน้มที่จะโจมตีและควบคุมตรรกะภายใน PLC

• ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการ ควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สิน
สำคัญ

ตัวอย่าง: ในสภาพแวดล้อม Windows ทั่วไป เซิร์ฟเวอร์ Active Directory (AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ไปยังเซิร์ฟเวอร์หลายเครื่องมักจะได้รับการพิจารณาว่าเป็นทรัพย์สินที่เกี่ยวข้อง เนื่องจากเป็นสะพานเชื่อมให้ผู้โจมตีเปลี่ยนเข้าสู่เซิร์ฟเวอร์เหล่านี้

ใช้รายการทรัพย์สินที่รวมเข้าด้วยกันเพื่อสร้างแผนผังสถาปัตยกรรมเครือข่ายที่ให้การแสดงภาพของเส้นทางการเชื่อมต่อระหว่างกันและการสื่อสารระหว่างทรัพย์สิน ระบุจุดเข้าทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายในระบบ รวมถึงทรัพย์สินที่เกี่ยวข้องและทรัพย์สินสำคัญ สิ่งนี้จะช่วยอำนวยความสะดวกในงานต่อไปในการระบุภัยคุกคาม

**งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)**

ด้วยรายการทะเบียนทรัพย์สินและไดอะแกรมสถาปัตยกรรมเครือข่าย ควรระบุเหตุการณ์ ภัยคุกคามที่อาจใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการเพื่อการวิเคราะห์เชิงลึก เทคนิคประการหนึ่งที่หน่วยงานควรใช้คือการสร้างแบบจำลองภัยคุกคาม โดยการสร้างแบบจำลองภัยคุกคาม เป็นกระบวนการที่มีโครงสร้างสำหรับการระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับระบบ เพื่อให้หน่วยงาน สามารถสร้างการป้องกันที่มุ่งเน้นมากขึ้นเพื่อปกป้องระบบ

**การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้**

**๑. การระบุขอบเขตและการจำแนกระบบ** (Scope Identification and System Decomposition) - สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำในงาน A

**๒. การระบุภัยคุกคาม** (Threat Identification) - หน่วยงานควรใช้แนวทางที่เป็นระบบ เพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

**๓. การสร้างแบบจำลองการโจมตี** (Attack Modelling) - หลังจากระบุเหตุการณ์ภัยคุกคามที่ เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่ เป็นไปได้ ทั้งนี้การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถ ระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

**งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)**

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

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้

ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้

**- ทรัพย์สิน (Asset)** - สิ่งที่มีค่าที่ได้รับการระบุในงาน A

**- เหตุการณ์ภัยคุกคาม** (Threat event) - เหตุการณ์การโจมตีที่ระบุในงาน B

**- ช่องโหว่ (Vulnerability)** - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถ ใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

**- ผลที่ตามมา** (Consequence) - ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

ตัวอย่างของสถานการณ์ความเสี่ยงที่สร้างมาอย่างดีแสดงไว้ด้านล่าง

Legend: Threat Event | Vulnerability | Asset | Consequence

ผู้โจมตีทำการแทรก SQL บนเว็บแอปพลิเคชันเดิมที่ไม่ได้แพตช์เพื่อดาวน์โหลดเวชระเบียนผู้ป่วยที่มีความอ่อนไหว

| |
|---|
| Attacker performs an SQL injection on an unpatched legacy web application to download sensitive patient medical records. |

ตัวอย่างที่ ๑: เหตุการณ์ความเสี่ยง (Risk Scenario)

พนักงานภายในทำการหลอกลวงให้ชำระเงินเกินยอดเงินในบัญชีธนาคารในระบบการชำระเงินโดยไม่มีกำหนด ส่งผลให้เกิดการเบิกเกินบัญชีธนาคาร

| |
|---|
| Internal staff makes a fraudulent payment instruction exceeding bank account balance on the payment system with no set limit, resulting in a bank overdraft. |

ตัวอย่างที่ ๒: เหตุการณ์ความเสี่ยง

พนักงานที่ไม่ได้รับอนุญาตเข้าถึงเซิร์ฟเวอร์ SCADA โดยใช้ข้อมูลรับรองการเข้าสู่ระบบเริ่มต้นและดำเนินการคำสั่งปิดระบบเพื่อรบกวนการจ่ายน้ำไปยังฝั่งตะวันออกของกรุงเทพมหานครทั้งหมด

| |
|---|
| Unauthorised employee accesses the SCADA server using default login credentials and execute shutdown command to disrupt the water supply to the entire east side of Bangkok. |

ตัวอย่างที่ ๓: เหตุการณ์ความเสี่ยง

ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้ที่ไม่สงสัย ซึ่งเมื่อคลิกแล้ว จะทำให้บัญชีผู้ใช้ดำเนินการตรวจสอบสิทธิ์ SMB กับเซิร์ฟเวอร์ที่เป็นอันตรายและเปิดเผยข้อมูลประจำตัวที่แฮชไว้

| |
|---|
| Attacker delivers spear-phishing email to unsuspecting user, which when clicked, triggers the user account to perform SMBauthentication with malicious server and discloses hashed credentials. |

ตัวอย่างที่ ๔. เหตุการณ์ความเสี่ยง

**สิ่งที่หน่วยงานพึงปฏิบัติ**

ในรายงานการประเมินความเสี่ยงหน่วยงาน สถานการณ์ความเสี่ยงต้องมีองค์ประกอบของเหตุการณ์ ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมา

**๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)**

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น และ

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

**งาน A: กำาหนดโอกาส (Determine Likelihood)**

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าว เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับ การประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- ความสามารถในการค้นพบ (Discoverability) - ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผย ของทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) - ฝ่ายตรงข้ามจะใช้ประโยชน์จาก ช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะ ทางเทคนิคที่จำเป็นในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) - ฝ่ายตรงข้ามจะสามารถสร้างการโจมตี ทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่ จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

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

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

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

| Likelihood Rating | Discoverability | Exploitability | Reproducibility |
|---|---|---|---|
| **High (๓)** | ช่องโหว่ของเป้าหมาย:<br>• สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB)<br>• สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต) | การโจมตี:<br>• สามารถดำเนินการได้ โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย<br>• สามารถทำได้ด้วย เครื่องมือที่หาได้ทั่วไป โดยไม่ต้องมีความรู้ ด้านเทคนิค | การโจมตี:<br>• สามารถทำซ้ำได้ ตามต้องการโดยไม่มีการกำหนดค่า(Configuration) หรือ เงื่อนไขของเหตุการณ์ (Event Condition)<br>• สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่ |
| **Medium (๒)** | ช่องโหว่ของเป้าหมาย:<br>• สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง | การโจมตี:<br>• สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access | การโจมตี:<br>• สามารถทำซ้ำได้ ตามเงื่อนไขเหตุการณ์ ที่คาดเดาได้บางอย่าง |

| | | | |
|---|---|---|---|
| | พฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing))<br>• สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน | Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root)<br>• สามารถดำเนินการได้ ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง | • สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย |
| **Low (๑)** | ช่องโหว่ของเป้าหมาย:<br>• สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย<br>• สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล | การโจมตี:<br>• สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root)<br>• สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะซึ่งต้องการความรู้ด้าน เทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน | การโจมตี:<br>• สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง<br>• สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่ |

ตัวอย่างตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

**สิ่งที่หน่วยงานพึงปฏิบัติ**

ในรายงานการประเมินความเสี่ยงหน่วยงาน

- ความน่าจะเป็นของความเสี่ยงจะต้องให้คะแนนตามระดับ ๑ ถึง ๓ (เช่น ๑ เป็น “เป็นไปได้ยาก” และ ๓ คือ “มีแนวโน้มสูง”)

- ความน่าจะเป็นของความเสี่ยงจะต้องพิจารณาจากภัยคุกคามและช่องโหว่

- แนะนำให้ใช้ปัจจัยความน่าจะเป็น (เช่น ความสามารถในการค้นพบ ความสามารถในการใช้ ประโยชน์ และความสามารถในการทำซ้ำ) เพื่อกำหนดความเป็นไปได้ของความเสี่ยง

**งาน B: 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

**- หน่วยงาน (Organisational)** – ในระดับหน่วยงาน ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงัก ในการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

**- บุคคล (Individual)** - ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิต และการบาดเจ็บ

ตารางด้านล่าง คือ ตัวอย่างตารางประเมินสำหรับการพิจารณาผลกระทบของความเสี่ยง ในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่างเป็นข้อมูลทั่วไป เมื่อใช้ตารางผลกระทบที่คล้ายกัน หน่วยงานควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการเพื่อให้แน่ใจว่า

**- เกี่ยวข้องกับบริบททางธุรกิจ (Relevant to business context)** - เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของหน่วยงานหรือวัดผลงาน

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

**- มุมมองที่หลากหลาย (Multi-perspectives)** - ระบุประเภทย่อยของผลกระทบจากแต่ละระดับ จาก ๓ ระดับ (เช่น ระดับประเทศ หน่วยงาน และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

| **วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)** | **ผลกระทบที่อาจเกิดขึ้น (potential impact)*** | | |
|---|---|---|---|
| | **ต่ำ** | **กลาง** | **สูง** |
| ด้านการรักษาความลับ (Confidentiality) | การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์ | การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์ แห่งชาติที่ | การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิด |

| วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective) | ผลกระทบที่อาจเกิดขึ้น (potential impact)* | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| | แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests) | สำคัญ(Important National Interests) | ผลประโยชน์ แห่งชาติสำคัญยิ่ง (Extremely Important National Interests) |
| | มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ) | มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง) | มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด) |
| ด้านการรักษาความถูกต้อง ครบถ้วน (Integrity) | การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited)และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests) | การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests) | การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญ ยิง (Extremely Important National Interests) |
| ด้านการรักษาสภาพพร้อมใช้งาน (Availability) | การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or | การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests) | การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์ แห่งชาติสำคัญยิ่ง (Extremely Important |

| วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective) | ผลกระทบที่อาจเกิดขึ้น (potential impact)* | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| | Secondary National Interests) | | National Interests) |

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

| ด้านผลกระทบ | ระดับผลกระทบ | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| การเงินหรือรัพย์สิน | ไม่เกินหนึ่งล้านบาท | ไม่เกินหนึ่งร้อยล้านบาท | เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป |
| อันตรายต่อชีวิต ร่างกาย หรืออนามัย | ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย | ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน | ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกาย หรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน |
| ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย | ไม่เกินหนึ่งหมื่นคน | เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน | เกินกว่าหนึ่งแสนคน |
| ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน | ไม่มีผลกระทบ หรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงาน เพียงเล็กน้อย | การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมากแต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน | การดำเนินการตามหน้าที่หลัก ของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่องและไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลา ตามแผนกู้คืนระบบของหน่วยงาน |
| ความมั่นคงของรัฐ | ไม่มีผลกระทบต่อความมั่นคงของรัฐ | ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับ | ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับ |

| ด้านผลกระทบ | ระดับผลกระทบ | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| | | ความมั่นคงของรัฐด้อยประสิทธิภาพลงมากแต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน | ความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้ |

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือ เป็นคะแนนสุดท้าย

**สิ่งที่หน่วยงานพึงปฏิบัติ**

ในรายงานการประเมินความเสี่ยงหน่วยงาน

ผลกระทบต่อความเสี่ยงที่กำหนดในแนวทางฉบับนี้ ให้คะแนนตามระดับ ๑ ถึง ๓ (โดยระดับคะแนน ๑ คือ “ต่ำ” และระดับคะแนน ๓ คือ “สูง”)

ทั้งนี้ หน่วยงานอาจพิจารณาใช้ระดับความน่าจะเป็น ผลกระทบที่เกิดขึ้น และความเสี่ยง ที่ยอมรับได้ ที่แตกต่างกันไปตามที่หน่วยงานเห็นสมควร

- คำอธิบายสำหรับการให้คะแนนผลกระทบแต่ละรายการต้องปรับให้เหมาะกับบริบทของหน่วยงาน ที่เกี่ยวข้อง

๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

**งาน A: กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)**

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จาก ช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยง สำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง (หัวข้อ ๔.๒)

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

รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญ ของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

**สิ่งที่หน่วยงานพึงปฏิบัติ:**

ในรายงานการประเมินความเสี่ยงหน่วยงาน จะต้องกำหนดระดับความเสี่ยงโดยใช้เมทริกซ์ ๓ คูณ ๓ ตามตัวอย่างนี้ หรือหน่วยงานสามารถกำหนดระดับความเสี่ยงเองได้ตามความเหมาะสม

**งาน B: ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)**

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียการลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยง ที่กำหนด การลงทะเบียนความเสี่ยง

เป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของหน่วยงานมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

**- สถานการณ์ความเสี่ยง (Risk Scenario)** - สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร

**- วันที่ระบุความเสี่ยง (Identification Date)** - วันที่ที่ระบุสถานการณ์ความเสี่ยง

**- มาตรการที่มีอยู่ (Existing Measures)** – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ ความเสี่ยง

**- ความเสี่ยงในปัจจุบัน (Current Risk)** - ระดับความเสี่ยงที่กำหนด (การรวมกันของความ เป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยง โดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)

**- แผนจัดการความเสี่ยง (Treatment Plan)** - กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของหน่วยงาน)

**- สถานะความคืบหน้า (Progress Status)** - สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

**- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk)** - ระดับความเสี่ยงที่กำหนด (การรวมกันของความ เป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

**- เจ้าของความเสี่ยง (Risk Owner)** - บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยง ที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

**สิ่งที่หน่วยงานพึงปฏิบัติ:**

ในรายงานการประเมินความเสี่ยงหน่วยงาน ทะเบียนความเสี่ยงต้องมีองค์ประกอบอย่างน้อย ๘ ประการ ได้แก่ สถานการณ์ความเสี่ยง วันที่ระบุ มาตรการที่มีอยู่ ความเสี่ยงปัจจุบัน แผนจัดการ ความเสี่ยง สถานะความคืบหน้า ความเสี่ยงที่เหลืออยู่ เจ้าของความเสี่ยง

**๕. ตอบสนองต่อความเสี่ยง**

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุ และกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

**๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)**

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน 4 ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยงที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของการแบ่งปัน ความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการและตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

**๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)**

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตามหน่วยงานควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่า ตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลง หรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกัน ปลายทางที่มีราคาแพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบ ให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ ตามคำแนะนำ

ทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยง หรือการลดผลกระทบจากความเสี่ยง

**สิ่งที่หน่วยงานพึงปฏิบัติ:**

ในรายงานการประเมินความเสี่ยงหน่วยงาน

- ผู้บริหารระดับสูงต้องอนุมัติแผนจัดการความเสี่ยงทั้งหมดอย่างเป็นทางการ
- ผู้บริหารระดับสูงต้องยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมดอย่างเป็นทางการ

# 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/default-source/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 ๒๐๑๘ Link: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

๓. ISO ๓๑๐๐๐:๒๐๑๘(en) Risk management — Guidelines, ISO, FEBRUARY ๒๐๑๘
Link: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

๔. ISO/IEC ๒๗๐๐๕:๒๐๑๘ Information technology ── Security techniques ──Information security risk management, ISO/IEC, July ๒๐๑๘ Link: https://www.iso.org/standard/75281.html