**รายงานสรุปบทเรียน**

**ชื่อโครงการฝึกอบรม** : ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
**วันที่เข้ารับการอบรม** : ๒๓ กุมภาพันธ์ ๒๕๖๙
**สถานที่** : พัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ (TDGA e-Learning)
**จัดโดย** : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
**ผู้จัดทำรายงาน** : นางสาวนงลักษณ์ หนองกุ่ม ตำแหน่ง เจ้าพนักงานการเงินและบัญชีปฏิบัติงาน
**วัตถุประสงค์** :

๑. เรียนรู้ความหมายและความสำคัญของ Cybersecurity และ Cybersecurity Risk กระบวนการของ Cybersecurity Risk ความรู้เบื้องต้นของ Risk Assessment และ Risk Management แนวทางการวางแผนความต่อเนื่องทางธุรกิจ Business Continuity Planning (BCP)

**สรุปเนื้อหาการฝึกอบรม** :

**๑. Cyber Security และ Information Security**

Cyber Security (ความปลอดภัยทางไซเบอร์) คือ ป้องกันการโจมตีที่มาจากโลกออนไลน์ หรือเครือข่ายเป็นหลัก เพื่อปกป้องระบบคอมพิวเตอร์ เครือข่าย และโปรแกรมจากการถูกแฮก(Hack) ไวรัส หรือมัลแวร์ โดยครอบคลุมเฉพาะข้อมูลหรือทรัพย์สินที่เป็นดิจิทัล และเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต ตัวอย่างเช่น การใช้ VPN (๐.๔.๒), การทำ Multi-factor Authentication (MFA), และการป้องกันการเจาะระบบ (Penetration Testing)

Information Security (ความปลอดภัยของข้อมูลสารสนเทศ) คือ การปกป้องข้อมูลไม่ให้ถูกเข้าถึง เปิดเผย แก้ไข หรือทำลาย โดยไม่ได้รับอนุญาต เน้นการรักษาความปลอดภัยของ "ข้อมูล" ในทุกรูปแบบ มีเป้าหมายรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลตามหลัก CIA Triad โดยครอบคลุมทั้งข้อมูลดิจิทัล และข้อมูลที่เป็นกระดาษ/เอกสาร รวมถึงความปลอดภัยทางกายภาพ เช่น การล็อกห้องเก็บเอกสาร ตัวอย่างเช่น การจัดชั้นความลับของเอกสาร การกำหนดสิทธิ์การเข้าถึงไฟล์ และการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

**๒. Cyber Security Risk Management**

Risk Management (การบริหารความเสี่ยง) คือ กระบวนการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงเพื่อให้องค์กรบรรลุเป้าหมายและลดผลกระทบที่อาจเกิดขึ้น โดยมีขั้นตอนหลักดังนี้

๑. Identifying risk (การระบุความเสี่ยง) การประเมินสภาพแวดล้อมขององค์กรเพื่อระบุความเสี่ยงที่เกิดขึ้นในปัจจุบันหรือความเสี่ยงที่อาจเกิดขึ้น ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของธุรกิจ

๒. Assess risk (การประเมินความเสี่ยง) การวิเคราะห์ความเสี่ยงที่ระบุไว้แล้ว เพื่อดูว่ามีโอกาสเกิดขึ้นมากน้อยเพียงใด และผลกระทบที่จะเกิดขึ้นรุนแรงแค่ไหน

๓. Control risk (การควบคุมความเสี่ยง) การกำหนดวิธีการ ขั้นตอน เทคโนโลยี หรือมาตรการอื่น ๆ ที่ช่วยให้องค์กรลดหรือบรรเทาความเสี่ยง

๔. Review controls (การทบทวนการควบคุม) การประเมินอย่างต่อเนื่องว่ามาตรการควบคุมมีประสิทธิภาพในการลดความเสี่ยงหรือไม่

**๓. Cybersecurity Framework**

Cybersecurity Frameworks คือ กรอบการทำงานด้านความปลอดภัยไซเบอร์ที่เป็นมาตรฐานสากล ได้แก่

✦ ISO ๒๗๐๐๑ : มาตรฐานระดับโลกสำหรับการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) เน้นโครงสร้างพื้นฐาน การประเมินความเสี่ยง และการควบคุมเพื่อรักษาความลับและความถูกต้องของข้อมูล

✦ ISO ๒๗๐๐๕ : มาตรฐานที่ช่วยขยายความ ISO ๒๗๐๐๑ โดยเน้นกระบวนการบริหารความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างละเอียด โดยการระบุ วิเคราะห์ และจัดการความเสี่ยง

✦ ISO ๒๗๐๓๒ : เน้นแนวทางปฏิบัติเฉพาะทางด้าน Cybersecurity ในโลกไซเบอร์โดยเฉพาะ เช่น ความปลอดภัยบนอินเทอร์เน็ต (Internet Security) และการป้องกันโครงสร้างพื้นฐานวิกฤต

✦ ISO ๓๑๐๐๐ : เป็นกรอบงานกว้างๆ สำหรับการบริหารจัดการความเสี่ยง (Risk Management) ในภาพรวมขององค์กร ไม่ได้จำกัดเฉพาะไอที แต่ใช้เป็นรากฐานในการวิเคราะห์ความเสี่ยงด้านไซเบอร์ได้

**๔. NIST Cybersecurity Framework**

การนำ NIST Cybersecurity Framework (NIST CSF) ไปปรับใช้ในองค์กรเพื่อสร้างระบบป้องกันที่ตรงจุดและมีประสิทธิภาพ

๑. Prioritize and Scope (กำหนดลำดับความสำคัญและขอบเขต) ระบุว่าอะไรคือเป้าหมายหลักทางธุรกิจ และส่วนไหนของระบบไอทีที่สำคัญที่สุด เพื่อให้รู้ว่าควรทุ่มทรัพยากรและงบประมาณไปป้องกันที่จุดไหนก่อน ไม่ให้เป็นการทำงานแบบหว่านแห

๒. Orient (ระบุความเสี่ยงและจุดอ่อน) วิเคราะห์ดูว่ามีภัยคุกคามอะไรบ้างที่อาจเกิดขึ้นกับระบบที่เลือกไว้ในข้อแรก และระบบเหล่านั้นมีจุดอ่อนตรงไหน เพื่อให้เข้าใจสภาพแวดล้อมความปลอดภัยและช่องโหว่ที่แท้จริงขององค์กร

๓. Create a Current Profile (สร้างโปรไฟล์สถานะปัจจุบัน) สำรวจและบันทึกว่าในตอนนี้องค์กรมีการจัดการความปลอดภัยอย่างไรบ้าง เช่น ใช้วิธีไหน มีซอฟต์แวร์อะไร มีมาตรฐานแค่ไหน เพื่อให้เห็นภาพชัดเจนว่าสถานะปัจจุบันอยู่ตรงไหนก่อนที่จะพัฒนาต่อ

๔. Conduct a Risk Assessment (การประเมินความเสี่ยง) นำข้อมูลจากข้อ ๒ และ ๓ มาวิเคราะห์หาโอกาสที่จะเกิดเหตุร้ายและผลกระทบที่จะตามมา โดยใช้วิธีการประเมินความเสี่ยงตามมาตรฐานที่องค์กรยอมรับ เพื่อนำผลลัพธ์ไปใช้ตัดสินใจว่าความเสี่ยงตัวไหนต้องรีบแก้ไขด่วนที่สุด

**๕. Business Continuity Planning (BCP)**

Business Continuity Planning (BCP) คือ แผนบริหารความต่อเนื่องทางธุรกิจ ซึ่งเป็นกระบวนการเตรียมความพร้อมเพื่อให้ธุรกิจสามารถดำเนินต่อไปได้หรือฟื้นตัวได้โดยเร็วเมื่อเกิดเหตุวิกฤต โดยแบ่งออกเป็น ๓ ระยะหลักตามลำดับเวลา (Time) และระดับประสิทธิภาพการทำงาน (Performance) ดังนี้

๑. Plan (ระยะเตรียมการ - ก่อนเกิดเหตุ) เป็นวงจรการวางแผนที่ต้องทำอย่างต่อเนื่องเพื่อให้พร้อมรับมือเสมอ

๒. Respond (ระยะตอบโต้ - เมื่อเกิดเหตุการณ์ขัดข้อง) เมื่อเกิดเหตุการณ์ไม่คาดฝันที่ทำให้ธุรกิจหยุดชะงัก ประสิทธิภาพการทำงานจะตกลงอย่างรวดเร็ว

๓. Recover (ระยะฟื้นฟู - หลังสถานการณ์เริ่มคงที่) เมื่อสถานการณ์เริ่มนิ่ง องค์กรจะเริ่มเข้าสู่ขั้นตอนการกลับมาดำเนินงานตามปกติ

**๖. ISO ๒๒๓๐๑ Business Continuity Management**

ISO ๒๒๓๐๑ คือ มาตรฐานสากลสำหรับระบบบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ซึ่งถูกออกแบบมาเพื่อให้องค์กรสามารถเตรียมความพร้อม ตอบสนอง และฟื้นตัวจากเหตุการณ์หยุดชะงักต่างๆ เช่น ภัยธรรมชาติ การโจมตีทางไซเบอร์ หรืออุบัติการณ์ร้ายแรงอื่นๆ ได้อย่างเป็นระบบ

**<u>หัวใจสำคัญของ ISO ๒๒๓๐๑</u>** ช่วยให้องค์กรเข้าใจว่างานส่วนไหนสำคัญที่สุด และต้องทำอย่างไรให้งานนั้นดำเนินต่อไปได้แม้ในภาวะวิกฤต โดยมีองค์ประกอบหลักดังนี้

๑. Business Impact Analysis (BIA) การวิเคราะห์ผลกระทบเพื่อระบุกิจกรรมที่สำคัญและกำหนดระยะเวลาที่ยอมรับได้หากเกิดการหยุดชะงัก เช่น RTO และ MTPD

๒. Risk Assessment (RA) การประเมินความเสี่ยงเพื่อระบุภัยคุกคามที่อาจเกิดขึ้นและวางแนวทางป้องกัน

๓. Business Continuity Plan (BCP) การจัดทำแผนปฏิบัติการที่ชัดเจนเพื่อให้บุคลากรรู้หน้าที่ของตนเองเมื่อเกิดเหตุ

๔. Exercising & Testing การซ้อมแผนสม่ำเสมอเพื่อให้มั่นใจว่าแผนที่วางไว้สามารถใช้งานได้จริงเมื่อเกิดวิกฤต

**<u>ประโยชน์ของการทำ ISO ๒๒๓๐๑</u>**

- ลดความเสียหาย ผลกระทบทางการเงินและชื่อเสียงเมื่อเกิดเหตุไม่คาดฝัน
- สร้างความเชื่อมั่น ทำให้ลูกค้า คู่ค้า และผู้ถือหุ้นมั่นใจว่าธุรกิจจะไม่อับปางง่ายๆ
- ความได้เปรียบทางการแข่งขัน หลายบริษัทกำหนดให้คู่ค้าต้องมีมาตรฐานนี้เพื่อรับรองความมั่นคงของห่วงโซ่อุปทาน
- การปรับปรุงอย่างต่อเนื่อง ใช้โครงสร้าง PDCA (Plan-Do-Check-Act) เพื่อพัฒนาความยืดหยุ่นขององค์กรให้ทันต่อโลกที่เปลี่ยนไป

**๗. การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์**

มีองค์ประกอบสำคัญดังนี้

๑. Threat Assessment การประเมินภัยคุกคาม เพื่อรู้ว่าองค์กรเสี่ยงอะไรบ้าง

๒. Policies and Procedures จัดทำนโยบายและขั้นตอนปฏิบัติให้ชัดเจน

๓. Cyber ISMS Implementation นำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ไปใช้จริง

๔. Training and Awareness อบรมและสร้างความตระหนักรู้ให้บุคลากร

๕. Industry and Government Support and Escalation ประสานงานกับหน่วยงานรัฐและอุตสาหกรรม รวมถึงมีกระบวนการแจ้งเหตุยกระดับเหตุการณ์ (Escalation)

๖. Partner with Cybersecurity Vendors ทำงานร่วมกับผู้เชี่ยวชาญหรือผู้ให้บริการด้านความปลอดภัยไซเบอร์

**ประโยชน์ที่ได้รับ :**

๑. มีความรู้ ความเข้าใจ เรื่อง Cybersecurity และ Cybersecurity Risk กระบวนการของ Cybersecurity Risk ความรู้เบื้องต้นของ Risk Assessment และ Risk Management แนวทางการวางแผนความต่อเนื่องทางธุรกิจ Business Continuity Planning (BCP)