สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 2
ปีงบประมาณ พ.ศ. 2568

หลักสูตร ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)

จัดทำโดย นางสาวชัชชษา ใหม่จีน
ตำแหน่ง นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

๑. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กรอบมาตรฐานที่หน่วยงานในไทยนิยมใช้ มีรายละเอียดดังนี้

๑) กรอบการประเมินความมั่นคงปลอดภัยไซเบอร์ จัดทำโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เน้นให้หน่วยงานของรัฐและเอกชน เข้าใจความเสี่ยง และสามารถวางระบบป้องกันได้อย่างเหมาะสม ให้สอดคล้องกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒) NIST Cybersecurity Framework (CSF) พัฒนาโดย National Institute of Standards and Technology : NIST ของประเทศสหรัฐอเมริกา นิยมใช้เป็นแนวทางในระดับนานาชาติ

๓) ISO/IEC ๒๗๐๐๑ พัฒนาโดย International Organization for Standardization : ISO ร่วมกับ International Electrotechnical Commission : IEC เน้นการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล โดยระบุข้อกำหนดสำหรับการ วางนโยบาย, การประเมินความเสี่ยง, และ ควบคุมการเข้าถึงข้อมูล ได้รับการยอมรับทั่วโลก

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Risk Assessment)

ความเสี่ยง คือ เหตุการณ์ การกระทำใดๆ ที่อาจเกิดขึ้นกายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ/หรือสร้างความเสียหายความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

โมเดล CIA คือ กรอบแนวคิดพื้นฐานในการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) และมักถูกใช้ร่วมกับมาตรฐานอื่น เช่น ISO ๒๗๐๐๑, NIST, หรือ กรอบของไทย เพื่อออกแบบระบบป้องกันความเสี่ยงที่ครอบคลุม ซึ่งประกอบด้วย ๓ องค์ประกอบหลัก

๑) ความลับของข้อมูล (Confidentiality) การเข้าถึงได้เฉพาะบุคคลหรือระบบที่ได้รับอนุญาตเท่านั้น เช่น การตั้งรหัสผ่าน การเข้ารหัส (encryption) และการควบคุมการเข้าถึง (access control)

๒) ความถูกต้องครบถ้วนของข้อมูล (Integrity) ข้อมูลต้องถูกต้อง ไม่ถูกดัดแปลงโดยไม่ได้รับอนุญาต เช่น การตรวจสอบความถูกต้อง (checksums, hash functions) และการบันทึก log

๓) ความพร้อมใช้งานของข้อมูล (Availability) ข้อมูลและระบบต้องสามารถเข้าถึงและใช้งานได้ตลอดเวลาเมื่อจำเป็น เช่น การสำรองข้อมูล (backup) ระบบสำรองไฟ (UPS) การป้องกัน DDoS

๓. กระบวนการบริหารความเสี่ยงของผู้ปฏิบัติงาน (Risk Management Process for Practitioners) คือ แนวทางที่ช่วยให้ผู้ปฏิบัติงานสามารถระบุ วิเคราะห์ ประเมิน และจัดการกับความเสี่ยงที่อาจเกิดขึ้นจากการทำงานได้อย่างเป็นระบบ

๔. การบริหารความเสี่ยงตามกรอบแนวคิด COSO ERM (Enterprise Risk Management) เวอร์ชันปรับปรุง (ปี ๒๐๑๗) ได้ปรับให้สอดคล้องกับยุคดิจิทัล เป็นแนวทางที่องค์กรทั่วโลกใช้เพื่อจัดการความเสี่ยงอย่างเป็นระบบ เน้นการผสานความเสี่ยงเข้ากับการบริหารจัดการองค์กร โดยแบ่งออกเป็น ๕ กระบวนการ ดังนี้

๑) ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance & Culture) คือ รากฐานของการบริหารความเสี่ยงมุ่งเน้นโครงสร้างการบริหารจัดการ ความรับผิดชอบ และค่านิยมองค์กร

๒) การกำหนดกลยุทธ์และวัตถุประสงค์ (Strategy & Objective Setting) คือ การบูรณาการความเสี่ยงเข้ากับการกำหนดทิศทางขององค์กรวางกลยุทธ์โดยพิจารณาความเสี่ยงควบคู่ไปกับโอกาส

๓) ผลการดำเนินงาน (Performance) คือ มุ่งประเมินผลและติดตามว่าความเสี่ยงมีผลกระทบต่อผลลัพธ์ขององค์กรอย่างไร เชื่อมโยงความเสี่ยงกับการวัดผล

๔) การทบทวนและปรับปรุง (Review & Revision) คือ ตรวจสอบว่าแนวทางบริหารความเสี่ยงยังเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงหรือไม่ การปรับปรุงอย่างต่อเนื่องเพื่อเพิ่มประสิทธิภาพ

๕) สารสนเทศ การสื่อสาร และการรายงาน (Information, Communication & Reporting) คือ เน้นการมีข้อมูลที่ถูกต้อง ทันเวลา และสื่อสารทั่วถึงทุกระดับ เพื่อให้การตัดสินใจเรื่องความเสี่ยงมีประสิทธิภาพ

๕. การประเมินความเสี่ยง (Risk Assessment) คือ ขั้นตอนสำคัญในกระบวนการบริหารความเสี่ยง โดยมีเป้าหมายเพื่อวิเคราะห์ว่า ความเสี่ยงที่เกิดขึ้นมีโอกาสเกิดและมีผลกระทบมากน้อยเพียงใด จากนั้นจัดระดับความเสี่ยง เพื่อวางแผนการจัดการอย่างเหมาะสม ซึ่งมีขั้นตอนการประเมินความเสี่ยง (Risk Assessment Process) ดังนี้

๑) กำหนดกิจกรรม / วัตถุประสงค์ ให้ระบุงานหรือกระบวนการที่ต้องประเมินความเสี่ยง

๒) ระบุความเสี่ยง (Risk Identification) วิเคราะห์ว่ามีความเสี่ยงใดบ้างที่อาจเกิดขึ้นกับกิจกรรมนั้น ความเสี่ยงอาจเกิดจากบุคคล เทคโนโลยี และกระบวนการ

๓) วิเคราะห์ความเสี่ยงประเมินแต่ละความเสี่ยงใน ๒ มิติ ได้แก่ ด้านโอกาสเกิด เป็นความน่าจะเป็นที่ความเสี่ยงจะเกิดขึ้น และด้านผลกระทบ เป็นความเสียหายหรือผลลัพธ์หากความเสี่ยงเกิดขึ้น

๔) ประเมินระดับความเสี่ยง (Risk Evaluation) นำ "โอกาสเกิด" และ "ผลกระทบ" มาใช้ตัดสินระดับความเสี่ยงใช้ ตารางแมทริกซ์ความเสี่ยง (Risk Matrix) เพื่อจัดลำดับความเสี่ยง

๕) จัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan) ควรวางแนวทางการจัดการ เช่น การปรับปรุงขั้นตอน เพิ่มการควบคุม

๖. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework : CSF) คือ แนวทางในการจัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk) อย่างเป็นระบบ ช่วยให้องค์กร ระบุ ป้องกัน ตรวจจับ ตอบสนอง และฟื้นตัว จากภัยคุกคามไซเบอร์ใช้ได้กับทุกภาคส่วน ซึ่งประกอบด้วย ๖ ฟังก์ชัน ดังนี้

๑) Govern การกำกับดูแลด้านไซเบอร์ให้เป็นส่วนหนึ่งของกลยุทธ์องค์กร สร้างวัฒนธรรมและนโยบายการบริหารความเสี่ยงไซเบอร์อย่างยั่งยืน

๒) Identify การระบุความเสี่ยง และบริบท เข้าใจจุดที่องค์กรเสี่ยง เพื่อวางแผนป้องกัน

๓) Protect การป้องกันระบบและข้อมูล ใช้มาตรการควบคุมเพื่อป้องกันการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต

๔) Detect การตรวจจับเหตุการณ์ผิดปกติ มีระบบที่สามารถแจ้งเตือนภัยไซเบอร์ได้ทันเวลา

๕) Respond การตอบสนองต่อภัยคุกคาม แผนจัดการเหตุการณ์ (Incident Response Plan)

๖) Recover การฟื้นฟูระบบให้กลับมาทำงานได้ แผนฟื้นฟูและเรียนรู้จากเหตุการณ์

๗. การตรวจสอบช่องโหว่ของระบบ (Vulnerability Assessment : VA) คือ กระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัยซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชันจนนำไปสู่วิธีการแก้ไขได้อย่างถูกจุดเพื่อเพื่อเพิ่มความปลอดภัย

สรุปได้ว่า การบริหารความเสี่ยง เป็นเครื่องมือที่มีความสำคัญและจำเป็นอย่างยิ่งต่อทุกหน่วยงาน เนื่องจากช่วยป้องกันและควบคุมความเสี่ยงที่อาจเกิดจากปัจจัยหลากหลาย ไม่ว่าจะเป็นปัจจัยด้านบุคคล เทคโนโลยี กระบวนการทำงาน หรือสถานการณ์ที่ไม่แน่นอน ซึ่งอาจส่งผลกระทบต่อการดำเนินงานและเป้าหมายขององค์กรได้ หากขาดการบริหารจัดการที่รัดกุมและเป็นระบบ หน่วยงานจึงควรดำเนินการวิเคราะห์ ตรวจสอบและประเมินความเสี่ยงในทุกมิติ เพื่อให้สามารถระบุโอกาสเกิดเหตุ ความรุนแรงของผลกระทบ ตลอดจนวางแผนป้องกันและควบคุมความเสี่ยงอย่างเหมาะสม ไม่ว่าจะเป็นการเตรียมมาตรการป้องกันล่วงหน้า หรือการจัดทำแผนตอบสนองและฟื้นฟูเมื่อเกิดเหตุ เพื่อลดความเสียหายให้น้อยที่สุด ซึ่งการบริหารความเสี่ยงยังควรดำเนินไปอย่างต่อเนื่องและเป็นส่วนหนึ่งของวัฒนธรรมองค์กร โดยผู้ปฏิบัติงานทุกระดับควรได้รับ การพัฒนาศักยภาพบุคลากรถือเป็นอีกปัจจัยที่มีความสำคัญอย่างยิ่ง เนื่องจากบุคลากรถือเป็นองค์ประกอบที่สำคัญในการเผชิญและตอบสนองต่อภัยคุกคามทางไซเบอร์ หน่วยงานจึงควรดำเนินการฝึกอบรมและสร้างความตระหนักรู้ให้แก่เจ้าหน้าที่อย่างต่อเนื่อง โดยการฝึกอบรมควรมีทั้งในเชิงพื้นฐาน เช่น การใช้งานระบบสารสนเทศอย่างปลอดภัย การบริหารจัดการรหัสผ่าน การเฝ้าระวังอีเมลหรือเว็บไซต์ที่น่าสงสัย และในเชิงเชี่ยวชาญ เช่น การตรวจสอบ วิเคราะห์ และตอบสนองต่อเหตุการณ์ การทดสอบเจาะระบบ หรือการใช้เครื่องมือด้านความมั่นคงปลอดภัยขั้นสูง เพื่อยกระดับความพร้อมของหน่วยงาน สร้างความเข้าใจ และทักษะในการใช้เครื่องมือบริหารความเสี่ยงที่เหมาะสม ช่วยให้สามารถตัดสินใจและปฏิบัติงานได้อย่างมีประสิทธิภาพ การบูรณาการนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ควรดำเนินการควบคู่กับการฝึกอบรมอย่างเป็นระบบ โดยกำหนดให้เป็นส่วนหนึ่งของยุทธศาสตร์และแผนการดำเนินงานของหน่วยงาน ทั้งนี้ จะช่วยให้เจ้าหน้าที่ทุกระดับมีความเข้าใจตรงกัน ตระหนักถึงบทบาทหน้าที่ และสามารถปฏิบัติงานได้สอดคล้องกับมาตรการที่กำหนดไว้ ส่งผลให้หน่วยงานภาครัฐมีความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่เข้มแข็ง ลดความเสี่ยงจากการถูกโจมตี ลดโอกาสเกิดปัญหาและอุปสรรคต่าง ๆ อันอาจกระทบต่อความสำเร็จของงาน และช่วยให้องค์กรมีความมั่นคง ปลอดภัย และพร้อมเผชิญกับความเปลี่ยนแปลงในอนาคต

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)

ด้านการพัฒนา (ระบุ ✓) : ☑ ดิจิทัล

☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน

☐ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน

บรรยายโดย : 1. นายปณิธาน เขินอำนวย ตำแหน่ง ผู้อำนวยการฝ่ายความมั่นคงปลอดภัยทางไซเบอร์

2. นายคมกริช คำสวัสดิ์ ตำแหน่ง หัวหน้าทีมปฏิบัติการการให้บริการด้านความมั่นคงปลอดภัยทางไซเบอร์ ฝ่ายความมั่นคงปลอดภัยทางไซเบอร์

3. นางสาวศรีสุดา แซ่เฮ้ง ตำแหน่ง หัวหน้าทีมแผนและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ ฝ่ายความมั่นคงปลอดภัยทางไซเบอร์

4. นายธงไชย จารุสุรเกษม ตำแหน่ง นักเทคโนโลยีดิจิทัล 2 ฝ่ายความมั่นคงปลอดภัยทางไซเบอร์

หน่วยงานผู้รับผิดชอบ : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิธีการพัฒนาตนเอง : e-learning

วันที่ได้รับการฝึกอบรม : 21 ส.ค. 2568 **สถานที่ :** ผ่านระบบออนไลน์