

ข้อหลักรัฐฯ พัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

โดย นางสาวศิริกานา มีแก้ว

ตำแหน่ง นักวิชาการแผนกที่ภาพถ่ายปฏิบัติการ

หน่วยงาน กลุ่มสำรวจเพื่อทำแผนที่ สำนักงานพัฒนาที่ดินเขต ๑๐

วัตถุประสงค์

๑. สามารถใช้งานเทคโนโลยีดิจิทัลและระบบสารสนเทศได้อย่างปลอดภัย
๒. สามารถป้องกัน รับมือ ภัยคุกคามที่เกิดจากความมั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์
๓. เป็นพื้นฐานในการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับที่สูงขึ้นต่อไป

สรุปรายละเอียดเนื้อหาของหลักสูตร

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง แนวคิด มาตรการ การ และกระบวนการที่ใช้ในการปกป้องระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสารสนเทศจากการเข้าถึง การใช้งาน การเปิดเผย หรือการทำลายโดยไม่ได้รับอนุญาต ในยุคที่หน่วยงานและองค์กรพึ่งพาาระบบดิจิทัลเป็นหลัก ความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นปัจจัยสำคัญที่ส่งผลต่อความต่อเนื่องของการดำเนินงานและความเชื่อมั่นของผู้ใช้งาน

การประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

ความเสี่ยง คือ เหตุการณ์ การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบต่อหรือสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

การบริหารความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรม หน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด สภาพแวดล้อมกับความเสี่ยง ได้แก่

- สภาพแวดล้อมภายนอก เช่น ความสลับซับซ้อนทางสังคม ภาวะทางเศรษฐกิจ เสถียรภาพของรัฐบาล สภาพทางภูมิศาสตร์ และนวัตกรรม

- สภาพแวดล้อมภายใน เช่น โครงสร้างขององค์กร ผลผลิตและผลลัพธ์ อัตรากำลัง และคุณภาพบุคลากร

ความสำคัญของการบริหารความเสี่ยง

- เพื่อส่งเสริมให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน
- เพื่อสะท้อนการพัฒนา ในด้านการกำกับดูแลที่ดีขององค์กร การกำหนด วัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

- เพื่อให้ฝ่ายบริหารเกิดความมั่นใจว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

- เพื่อเป็นกลไกในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยงกระบวนการบริหารจัดการความเสี่ยง

ประเภทความเสี่ยง

๑ ความเสี่ยงด้านยุทธศาสตร์ Strategic คือ การบรรลุเป้าหมาย และวัตถุประสงค์ ชื่อเสียง/ภาพลักษณ์ สำนักงาน เช่น การเปลี่ยนแปลงนโยบายระดับรัฐ กฎหมายสั่ง นโยบายขององค์กร รูปแบบธุรกิจ และข้อร้องเรียน

๒ ความเสี่ยงด้านปฏิบัติการ Operational คือ ความพร้อมของบุคลากร, รูปแบบ วิธีการ กระบวนการดำเนินงาน และการขึ้นทะเบียนบริการใหม่ เช่น การรักษาบุคลากร อัตราค่าจ้างขาดการบูรณาการ

๓ ความเสี่ยงด้านการเงิน Financial คือ การบริหารจัดการงบประมาณ ค่าใช้จ่าย เช่น การขาดสภาพคล่อง งบประมาณที่ได้รับไม่สอดคล้องกับสถานการณ์ของภารกิจที่เปลี่ยนแปลงไป

๔ ความเสี่ยงด้านกฎหมาย Compliance คือ การปฏิบัติตามกฎหมาย ระเบียบที่เกี่ยวข้อง เช่น การปฏิบัติงานไม่เป็นไปตามคำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร

๕ ความเสี่ยงด้านเทคโนโลยี Information Technology คือ การรักษาความลับ และความมั่นคงปลอดภัยทางไซเบอร์ความถูกต้องเชื่อถือได้ของระบบ เช่น การเปิดเผยข้อมูล การแก้ไขทำลายข้อมูลโดยไม่ได้รับ อนุญาต

กระบวนการจัดการความเสี่ยงตามมาตรฐาน COSO ERM

COSO ERM เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กร อย่างเป็นระบบ จนกระทั่งเป็นที่รู้จักและมีความนิยม ต่อมา COSO ได้กำหนดคำนิยามและรูปแบบต่าง "ในการจัดการกับความเสี่ยง โดยได้กำหนดออกมาเป็น COSO ERM (COSO Enterprise Risk Management) การประเมินความเสี่ยง เป็นการวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากการระบุความเสี่ยงมาทำการประเมินหาค่าระดับความเสี่ยง โดยแบ่งออกเป็น ๒ มิติ แต่ละมิติจะมีคะแนน ในการประเมินออกเป็น ๕ ระดับ ประกอบด้วย (๑) เกิดขึ้นได้ยาก (๒) เกิดขึ้นบ้างเป็นบางครั้ง (๓) เกิดขึ้นค่อนข้างบ่อย (๔) เกิดขึ้นบ่อย (๕) เกิดขึ้นเป็นประจำ

ปัจจัยความเสี่ยง (Risk Factor) ปัจจัยความเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้องค์กรไม่บรรลุ วัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน กระบวนการใด เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไมถึงเกิด ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อวิเคราะห์และกำหนดมาตรการป้องกันความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยง หมายถึง กระบวนการระบุ ความเสี่ยง การวิเคราะห์ความเสี่ยงและ จัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิดผลกระทบ และระดับของความเสี่ยงนั้นๆ

โอกาสที่จะเกิด หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
ผลกระทบ หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิด เหตุการณ์ความเสี่ยง
ระดับของความเสี่ยง หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การจัดการความเสี่ยง หรือการตอบสนองความเสี่ยง (Risk Response)

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วต้องทำการประเมินวิธีการบริหารจัดการความเสี่ยงทางการทุจริตที่สามารถนำไปปฏิบัติได้โดยการพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงการปิดโอกาส ความเสี่ยงทางการทุจริตทั้งหมดให้ได้เพื่อให้การบริหารความเสี่ยงทางการทุจริตมีประสิทธิภาพ

กระบวนการจัดการความเสี่ยงตามมาตรฐาน COSO ERM

COSO ERM เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กรอย่างเป็นระบบ จนกระทั่งเป็นที่รู้จักและมีความนิยม ต่อมา COSO ได้กำหนดคำนิยามและรูปแบบต่าง "ในการจัดการกับความเสี่ยง โดยได้กำหนดออกมาเป็น COSO ERM (COSO Enterprise Risk Management) การประเมินความเสี่ยง เป็นการวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยง ที่ได้จากการระบุความเสี่ยงมาทำการประเมินหาค่าระดับความเสี่ยง โดยแบ่งออกเป็น ๒ มิติ แต่ละมิติจะมีคะแนน ในการประเมินเป็น ๕ ระดับ ประกอบด้วย (๑) เกิดขึ้นได้ยาก (๒) เกิดขึ้นบ้างเป็นบางครั้ง (๓) เกิดขึ้นค่อนข้างบ่อย (๔) เกิดขึ้นบ่อย (๕) เกิดขึ้นเป็นประจำ

การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)
Vulnerability Assessment (VA) คือ กระบวนการที่ได้รับการตรวจสอบ หรือระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัย ซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชัน จนนำไปสู่วิธีการแก้ไขได้อย่างถูกต้องเพื่อเพิ่มความปลอดภัย

Vulnerability Scanning Tool เพื่อตรวจสอบความปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ซึ่งนับเป็นเรื่องสำคัญที่ใช้ระบุระดับความรุนแรงของช่องโหว่ที่เกิดขึ้น

ประโยชน์ Vulnerability Assessment

- ช่วยในการประเมินระดับความเสี่ยงที่มาจากช่องโหว่
- ช่วยในการสร้างรายงานที่เกิดจากช่องโหว่ที่พบ
- ช่วยในการตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน
- ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย รูปแบบของ VA Scan
- Host Assessment การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้ หากไม่ได้รับการทดสอบ

- Network and Wireless Assessment การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริง เพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

- Database Assessment การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล Remediation คือ การแก้ไขจุดประสงค์ของขั้นตอนสุดท้ายนี้คือการอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการร่วมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่าการอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุดโดยที่ไม่กระทบกับระบบปัจจุบัน หรืออาจจะกระทบน้อยลง

การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

Detect Function การเฝ้าระวังภัยคุกคาม ต้องอย่างต่อเนื่อง โดยมีวัตถุประสงค์ ดังนี้

- ลดความเสียหายที่อาจเกิดขึ้นได้ หรือสามารถจำกัดวงของความเสียหายที่เกิดขึ้นได้
- สามารถลดโอกาสหรือระยะเวลาของผู้โจมตีที่จะทำการโจมตีได้
- กระบวนการเฝ้าระวังที่ดี สามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการ การตอบสนองต่อ

เหตุการณ์ และการกู้คืนระบบได้

การสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์

ถือเป็นปัจจัยสำคัญที่ช่วยเสริมสร้างความปลอดภัยของระบบสารสนเทศอย่างยั่งยืน เนื่องจากภัยคุกคามทางไซเบอร์จำนวนมากเกิดจากพฤติกรรมของผู้ใช้งานที่ขาดความตระหนักรู้หรือไม่ปฏิบัติตามแนวทางด้านความปลอดภัยอย่างเหมาะสม การอบรมจึงมุ่งเน้นให้ผู้เข้าอบรมเข้าใจว่า ความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่หน้าที่ของบุคลากรด้านเทคโนโลยีสารสนเทศเพียงฝ่ายเดียว แต่เป็นความรับผิดชอบร่วมกันของทุกคนในองค์กร

ประโยชน์ที่ได้รับจากการฝึกอบรม

๑. ต่อตนเอง: สามารถไปใช้ในการปฏิบัติงานทางดิจิทัล และป้องกันตัวเองจาก ภัยทางไซเบอร์คุกคามเมื่อต้องใช้งานอินเทอร์เน็ต

๒. ต่อองค์กร: เพื่อให้ระบบ/บริการ/ผลิตภัณฑ์ มีความมั่นคงปลอดภัย ลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นภายในหน่วยงาน

๓. ต่อสาธารณะ: สามารถป้องกันข้อมูลส่วนบุคคลและข้อมูลสาธารณะอย่างเหมาะสม

แหล่งที่มา

หลักสูตร : พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

วิทยากร/ผู้ให้ความรู้ : นางสาวศรีสุดา แซ่เฮ้ง, นายธงไชย จารุสุรเกษม

หน่วยงานที่จัดอบรม : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

รูปแบบหลักสูตร : e-Learning

ช่วงเวลาการฝึกอบรม : ๑๗ สิงหาคม ๒๕๖๙