

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สถานีพัฒนาที่ดินสตูล
รอบการประเมินที่ ๑/๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นายธีระพงศ์ บิลสุริยะ ตำแหน่ง เจ้าพนักงานการเกษตรอาวุโส
หน่วยงาน กลุ่ม/ฝ่าย/สพด./ศูนย์ ฝ่ายวิชาการเพื่อการพัฒนาที่ดิน สถานีพัฒนาที่ดินสตูล
หัวข้อการพัฒนา หลักสูตร ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
(Understanding Cybersecurity Risk Management)

วิธีการพัฒนา อบรมออนไลน์ผ่านทางไกลด้วยระบบอิเล็กทรอนิกส์ (TDGA e-Learning)

วันที่พัฒนา ๑๖ - ๑๘ กุมภาพันธ์ ๒๕๖๙ สถานที่ สถานีพัฒนาที่ดินสตูล

หน่วยที่จัดอบรม สำนักงานพัฒนาบุคลากรภาครัฐด้านดิจิทัล (องค์การมหาชน)

บรรยายโดย ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร. สันติพัฒน์ อรุณธาริ

อาจารย์ คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร
มหาวิทยาลัยหอการค้าไทย

สรุปสาระสำคัญ

ความหมายและความสำคัญของ Cybersecurity

Cybersecurity (ความมั่นคงปลอดภัยไซเบอร์) หมายถึง กระบวนการ มาตรการ และเทคโนโลยีที่นำมาใช้ในการป้องกัน คุ้มครอง และรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เครือข่าย คอมพิวเตอร์ อุปกรณ์ดิจิทัล และข้อมูล จากการเข้าถึง การใช้งาน การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

หลักการสำคัญของ Cybersecurity ยึดตามแนวคิด CIA Triad ได้แก่

- Confidentiality (การรักษาความลับ)
- Integrity (ความถูกต้องครบถ้วนของข้อมูล)
- Availability (ความพร้อมใช้งานของระบบและข้อมูล)

ความสำคัญ

- ป้องกันความเสียหายต่อข้อมูลสำคัญขององค์กร
- ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น มัลแวร์ ฟิชชิ่ง หรือแรนซัมแวร์
- สร้างความเชื่อมั่นแก่ประชาชนและผู้มีส่วนได้ส่วนเสีย
- สนับสนุนการดำเนินงานให้เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

๒. ความหมายของ Cybersecurity Risk

Cybersecurity Risk หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อทรัพย์สินสารสนเทศ ระบบงาน หรือการดำเนินงานขององค์กร โดยความเสี่ยงเกิดจากองค์ประกอบ ๓ ส่วน ได้แก่

- Threat (ภัยคุกคาม)
- Vulnerability (ช่องโหว่)

- Impact (ผลกระทบ)

ความเสี่ยงจะเพิ่มสูงขึ้นเมื่อมีภัยคุกคามที่สามารถใช้ประโยชน์จากช่องโหว่ และก่อให้เกิดผลกระทบในระดับรุนแรง

๓. กระบวนการของ Cybersecurity Risk

กระบวนการบริหารความเสี่ยงด้านไซเบอร์สามารถอ้างอิงแนวทางจาก National Institute of Standards and Technology (NIST) โดยเฉพาะกรอบการทำงาน NIST Cybersecurity Framework ซึ่งประกอบด้วยขั้นตอนหลัก ดังนี้

๓.๑ Identify (การระบุความเสี่ยง)

- สำรวจทรัพย์สินสารสนเทศ
- ระบุภัยคุกคามและช่องโหว่

๓.๒ Protect (การป้องกัน)

- จัดทำมาตรการควบคุม เช่น การกำหนดสิทธิ์การเข้าถึง การเข้ารหัสข้อมูล

๓.๓ Detect (การตรวจจับ)

- ติดตามและเฝ้าระวังเหตุการณ์ผิดปกติ

๓.๔ Respond (การตอบสนอง)

- จัดทำแผนตอบสนองเหตุการณ์ (Incident Response Plan)

๓.๕ Recover (การฟื้นฟู)

- ดำเนินการกู้คืนระบบและปรับปรุงมาตรการป้องกัน

๔. ความรู้เบื้องต้นของ Risk Assessment

Risk Assessment (การประเมินความเสี่ยง) คือ กระบวนการวิเคราะห์และประเมินระดับความเสี่ยง เพื่อจัดลำดับความสำคัญในการจัดการ ขั้นตอนหลัก ได้แก่

๔.๑ การระบุสินทรัพย์ (Asset Identification)

๔.๒ การวิเคราะห์ภัยคุกคามและช่องโหว่

๔.๓ การประเมินโอกาสเกิด (Likelihood)

๔.๔ การประเมินผลกระทบ (Impact)

๔.๕ การคำนวณระดับความเสี่ยง (Risk Level)

๕. Risk Management (การบริหารความเสี่ยง)

Risk Management คือ กระบวนการกำหนดแนวทางควบคุมและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) แนวทางการจัดการความเสี่ยงมี ๔ รูปแบบ ได้แก่

๕.๑ Risk Avoidance – หลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง

๕.๒ Risk Reduction – ลดความเสี่ยงด้วยมาตรการควบคุม

๕.๓ Risk Transfer – โอนความเสี่ยง เช่น การทำประกันภัยไซเบอร์

๕.๔ Risk Acceptance – ยอมรับความเสี่ยงในระดับที่ควบคุมได้

๖. แนวทางการวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning: BCP)

Business Continuity Planning (BCP) คือ การจัดทำแผนรองรับเหตุการณ์ที่อาจทำให้องค์กรไม่สามารถดำเนินงานได้ตามปกติ เพื่อให้สามารถฟื้นฟูและดำเนินภารกิจที่สำคัญได้อย่างต่อเนื่อง

๖.๑ องค์ประกอบสำคัญของ BCP

- Business Impact Analysis (BIA)
- วิเคราะห์ผลกระทบต่อการกิจหลัก
- กำหนดค่า RTO (Recovery Time Objective)
- กำหนดค่า RPO (Recovery Point Objective)

๖.๒ Risk Assessment

- ประเมินความเสี่ยงที่อาจกระทบต่อความต่อเนื่อง

๖.๓ Recovery Strategy

- กำหนดแนวทางกู้คืนระบบ
- จัดเตรียมสถานที่สำรอง (Backup Site)

๖.๔ Plan Development

- จัดทำแผนปฏิบัติการอย่างเป็นลายลักษณ์อักษร

๖.๕ Testing and Exercise

- ทดสอบแผนอย่างสม่ำเสมอ

๖.๖ Review and Improvement

- ทบทวนและปรับปรุงแผนให้ทันสมัย

การบริหารจัดการ Cybersecurity และ Cybersecurity Risk มิใช่เพียงการใช้เทคโนโลยีเพื่อป้องกันภัยคุกคามเท่านั้น แต่เป็นกระบวนการบริหารเชิงระบบที่ครอบคลุมการประเมินความเสี่ยง การกำหนดมาตรการควบคุม และการเตรียมความพร้อมด้านความต่อเนื่องทางธุรกิจ (BCP) เพื่อให้องค์กรสามารถดำเนินภารกิจได้อย่างมั่นคง ปลอดภัย และยั่งยืน ภายใต้บริบทของสังคมดิจิทัลในปัจจุบัน

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. เสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ทำให้บุคลากรมีความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ สามารถปฏิบัติงานได้อย่างระมัดระวัง ลดความเสี่ยงจากความผิดพลาดของมนุษย์ (Human Error)

๒. ยกระดับศักยภาพในการประเมินและบริหารความเสี่ยง (Risk Assessment & Risk Management) บุคลากรสามารถวิเคราะห์ ระบุ และจัดลำดับความสำคัญของความเสี่ยงได้อย่างเป็นระบบ ส่งผลให้องค์กรมีแนวทางควบคุมความเสี่ยงที่เหมาะสมและมีประสิทธิภาพ

๓. เพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อเหตุการณ์ทางไซเบอร์ ทำให้องค์กรมีความพร้อมในการป้องกัน ตรวจสอบ และตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างทันท่วงที ลดความเสียหายที่อาจเกิดขึ้น

๔. สนับสนุนการดำเนินงานให้สอดคล้องกับมาตรฐานและกรอบการกำกับดูแล เช่น แนวทางของ National Institute of Standards and Technology และ กรอบ การทำงาน NIST Cybersecurity Framework ซึ่งช่วยยกระดับการบริหารจัดการด้านความมั่นคงปลอดภัยให้เป็นไปตามมาตรฐานสากล

๕. เสริมสร้างความพร้อมด้านความต่อเนื่องทางธุรกิจ (Business Continuity Planning: BCP) องค์กรสามารถจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน และกำหนดมาตรการฟื้นฟูระบบงานได้อย่างเป็นรูปธรรม ลดผลกระทบต่อภารกิจหลักของหน่วยงาน

๖. สร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย การมีระบบบริหารจัดการความมั่นคงปลอดภัยที่เป็นระบบและโปร่งใส ช่วยสร้างความเชื่อมั่นแก่ประชาชน ผู้รับบริการ และหน่วยงานที่เกี่ยวข้อง

๗. สนับสนุนการขับเคลื่อนองค์กรสู่การเป็นองค์กรดิจิทัลอย่างยั่งยืน การพัฒนาความรู้ด้านไซเบอร์เป็นพื้นฐานสำคัญในการปรับตัวสู่การบริหารจัดการข้อมูลและบริการภาครัฐในยุคดิจิทัลอย่างมั่นคงและปลอดภัย