สรุปบทเรียน

หลักสูตร “Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น”

ของนางสาวณัฐสุดา แซ่ลิ้ม นักจัดการงานทั่วไปชำนาญการ

ผ่านระบบการเรียนออนไลน์ของสถาบันพัฒนาบุคลากรภาครัฐดิจิทัล

(TDGA e-learning)

คำอธิบายหลักสูตร เป็นช่องทางการสร้างการเรียนรู้ ด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น (Beginner) จนถึงระดับกลาง (Intermediate) โดยหลักสูตรนี้เหมาะกับผู้ที่สนใจ เจ้าหน้าที่รัฐ พนักงานรัฐ พนักงานเอกชน ที่ต้องการดูแลรักษาและการป้องกัน ธำรงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) เพื่อให้ระบบ/บริการ/ผลิตภัณฑ์ มีความมั่นคงปลอดภัย และสามารถป้องกัน รับมือภัยคุกคามที่เกิดจากความมั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือโอกาสที่จะทำให้เกิดข้อผิดพลาด การสูญเสีย ที่จะเกิดขึ้นต่อระบบ/บริการ/ผลิตภัณฑ์

วัตถุประสงค์ในรายวิชา

1. เพื่อให้ผู้เรียนตระหนักและทราบถึงวิธีการป้องกัน cybersecurity
2. เพื่อให้ผู้เรียนเข้าใจความหมายและเห็นถึงความสำคัญของการประยุกต์ใช้งาน

เนื้อหา ประกอบด้วย 7 หัวข้อหลัก

หัวข้อที่ 1 แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

C-I-A Security Model หรือ Cyber Physical system Security & Safety ประกอบด้วย การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ข้อมูล (Availability) เพื่อให้ระบบ/บริการ/ผลิตภัณฑ์ทางไซเบอร์มีความมั่นคงปลอดภัยและสามารถรับมือกับภัยคุกคามที่เกิดจากไซเบอร์หรือเหตุการณ์ที่ไม่พึ่งประสงค์ หรือโอกาสที่ทำให้เกิดข้อผิดพลาด การสูญเสียที่เกิดขึ้นต่อระบบ/บริการ/ผลิตภัณฑ์ผ่านความตระหนักและทักษะของคน กระบวนการของหน่วยงานและการใช้งานเทคโนโลยี เพื่อให้การทำงานหรือใช้งานผ่านระบบเครือข่ายอินเตอร์เน็ตมีความปลอดภัยตามหลักการของ CIA Security Model

ปัจจุบันความปลอดภัยทางไซเบอร์กลายเป็นข้อมูลที่มีความกังวลที่หน่วยงานให้ความสำคัญ เนื่องจากการให้บริการในปัจจุบันเป็นการให้บริการผ่านอินเตอร์เน็ตที่ต้องพึ่งพาเทคโนโลยีเป็นอย่างมาก เมื่อถูกคุกคามด้านการดำเนินงาน การพัฒนา อาจมีความเสี่ยงหรือช่องโหว่ที่อาจเกิดขึ้นกับตัวระบบ ฉะนั้น การกำหนดมาตรการด้านการป้องกัน การรับมือ จึงมีการกำหนดให้มีประสิทธิภาพฟื้นตัวได้เร็ว ทำให้เกิดความต่อเนื่อง ลดโอกาสผิดพลาดในอนาคต

กรอบมาตรฐานที่ใช้ในประเทศไทย คือ

1) NIST (National Institute of Standards and Technology) เป็นหนึ่งในกรอบการดำเนินงานทางด้านความมั่นคงปลอดภัยที่นิยมอย่างมากทั่วโลก หลายองค์กรนำกรอบนี้ไปประยุกต์ใช้เพื่อรับมือกับภัยคุกคามทางด้านไซเบอร์ และมีการปรับประยุกต์ใช้กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

2) ISO (International Organization for Standardization) และ IEC (International Electrotechnical Commission) คือ มาตรฐานผลิตภัณฑ์อุตสาหกรรมของอังกฤษ ที่ทุกภูมิภาคทั่วโลกรวมถึงไทย หลายองค์กรนำมาเน้นในเรื่องของการให้ความปลอดภัยของข้อมูลและความลับในองค์กร

หัวข้อที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

2.1 การประเมินความเสี่ยง

ความเสี่ยงเป็นสิ่งที่ใกล้ตัว อยู่กับกิจวัตรประจำวันตั้งแต่ตื่นนอนจนเข้านอน ทุกอย่างล้วนมีความเสี่ยงกับชีวิตของคนเรา ดังนั้นความเสี่ยงที่เกิดขึ้นอาจจะเกิดจากการตั้งใจให้เกิดหรือไม่ก็ได้

ความเสี่ยง คือ เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ/หรือสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้ ซึ่งแบ่งได้ 3 รูปแบบ

- โอกาสที่เกิดขึ้น (Change of loss)
- ความเป็นไปได้ (Possibility of Loss)

- ความไม่แน่นอน (Uncertainty of Event)

ฉะนั้น เพื่อจัดการกับความเสี่ยงจึงต้องวางแผนเพื่อลดความเสี่ยง เพื่อให้ชีวิตหรือการดำเนินงานมีความราบรื่น

การบริหารจัดการความเสี่ยง (Risk Management) คือ วิธีการหรือกลยุทธ์ หรือ ผลที่นำมาใช้ในการวิเคราะห์ จัดการ ประเมินผล ติดตาม การสื่อสาร รวมถึงกาจัดการกิจกรรมต่างๆ ที่เกี่ยวข้องกับคนหมู่มาก เช่น การบริหารจัดการความเสี่ยงภายในองค์กร เพื่อลดความสูญเสีย ให้องค์กรบรรลุวัตถุประสงค์ตามที่องค์กรคาดหวังเพื่อเพิ่มโอกาสทางธุรกิจ รวมถึงการทำงานที่สะดวกขึ้น ลดความเสี่ยงในการทำงาน

สภาพแวดล้อมกับความเสี่ยง มีความหลากหลายซึ่งความเสี่ยงอาจจะเกิดจากการเมือง สภาพเศรษฐกิจ รวมถึงโซเชียลและเทคโนโลยีต่างๆ ที่เข้ามา หรืออาจเกิดจากกฎหมายหรือภัยธรรมชาติ ล้วนเป็นความเสี่ยงที่นำพาไปสู่สภาพแวดล้อมของความเสี่ยงที่เกิดขึ้นและกระทบต่อชีวิตได้

ความเสี่ยงแบ่งออกเป็น 2 หลักใหญ่ๆ

1) สภาพแวดล้อมภายนอก

1.1) Socio-cultural Factors: ความซับซ้อนทางสังคม โครงสร้างประชากร การศึกษา อาชีพ ค่านิยม และอื่นๆ

1.2) Economic Factors: ภาวะเศรษฐกิจ การจ้างงาน อัตราดอกเบี้ย ฯลฯ

1.3) Political and Legal Factors: เสถียรภาพของรัฐบาล นโยบายรัฐ กฎหมาย

1.4) Physical Factors: สภาพทางภูมิศาสตร์ ดินฟ้าอากาศ ภัยธรรมชาติ

1.5) Technological Factors: นวัตกรรม ความมีอยู่ของเทคโนโลยี

2) สภาพแวดล้อมภายใน

2.1) Structure and Policy: โครงสร้างขององค์กร กลยุทธ์ ฯลฯ

2.2) Service: ผลผลิตและผลลัพธ์ ความพึงพอใจของผู้ขอรับบริการ

2.3) Manpower: อัตรากำลัง คุณภาพบุคลากร การบริหารบุคคล ฯลฯ

2.4) Money: ประสิทธิภาพด้านการเงิน การระดมทุน

2.5) Materials: วัสดุ อุปกรณ์ เครื่องจักร ฯลฯ

2.6) Management: กระบวนการ ภาวะความเป็นผู้นำ วัฒนธรรมองค์กร สารสนเทศ ฯลฯ

นอกจากสภาพปัจจัยทั้งภายในและภายนอกแล้ว รูปแบบการจัดการความเสี่ยงก็เป็นเรื่องสำคัญถึงการรับมือเพื่อจัดการกับความเสี่ยง ดังภาพกระบวนการการจัดการ

Input คือ ปัจจัยความเสี่ยงเข้า

Process คือ วิธีการจัดการความเสี่ยงที่เกิดขึ้น ซึ่งต้องเลือกวิธีการหรือมาตรฐานมาจัดการความเสี่ยง

Output คือ ตัวชี้วัด เนื่องจากการจัดการความเสี่ยงจะต้องกำหนดตัวชี้วัดเพื่อให้การจัดการความเสี่ยงมีประสิทธิภาพและบรรลุตามเป้าหมายตามสมควร

หลังการมีการจัดการความเสี่ยงแล้ว จะต้องสร้างความเข้าใจในการบริหารความเสี่ยงร่วมกัน เพราะโดยทั่วไปแล้วจะมีโอกาสที่เกิดความเข้าใจผิดหรือคลาดเคลื่อนเกี่ยวกับการบริหารความเสี่ยงได้ 5 ประเด็น คือ

1) ความเสี่ยง คือ ปัญหา

- ปัญหา หมายถึง สภาพอะไรก็ตามที่เกิดขึ้นในปัจจุบันที่เป็นอุปสรรคในการทำงาน
- ความเสี่ยง หมายถึง การคาดการณ์ในอนาคต โดยการนำหลักฐานเชิงประจักษ์หรือข้อมูลหรือปัญหาที่เคยเกิดขึ้น มาประเมินและหาทางจัดการปัญหา เพื่อให้ปัญหาไม่เกิด

ดังนั้น ความเสี่ยง คือ ปัญหา จึงไม่ใช่ข้อเท็จจริง หรือความหมายเดียวกันเสมอไป เพราะปัญหา คือ สิ่งที่เกิดขึ้นแล้ว แต่ความเสี่ยง คือ เหตุการณ์ที่สร้างความเสียหายที่อาจจะเกิดขึ้นในอนาคต เป็นสิ่งที่จะเกิด หรืออาจไม่เกิดในอนาคตก็ได้หากมีแผนป้องกันที่ดี

2) ความเสี่ยงเป็นสิ่งไม่ดี แต่แท้จริงแล้ว ความเสี่ยงอาจจะเป็นโอกาสเกิดแนวทางใหม่ๆ
3) ไม่เสี่ยงย่อมปลอดภัยที่สุด
4) หากมีความเสี่ยงต้องกำจัดให้หมดสิ้นไป ซึ่งไม่จำเป็นเพราะสามารถควบคุม และความเสี่ยงไม่มีโอกาสเป็นศูนย์

5) ความเสี่ยงที่เกิดขึ้นเป็นความไม่แน่นอน ซึ่งความไม่แน่นอนคือสิ่งที่ไม่สามารถคาดการณ์ได้ แต่ความเสี่ยงคือสิ่งที่ประเมินออกมาจากข้อมูลหลักฐานที่ชัดเจน ว่าสิ่งนั้นมีโอกาสจะเกิดขึ้น ดังนั้น ความเสี่ยงกับความไม่แน่นอนจึงไม่ใช่สิ่งเดียวกัน

ความสำคัญของการจัดการความเสี่ยง

1) เพื่อส่งเสริมให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน
2) เพื่อสะท้อนการพัฒนาในด้านการกำกับดูแลที่มีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน
3) เพื่อให้ฝ่ายบริหารเกิดความมั่นใจว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย
4) เพื่อเป็นกลไกในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงในองค์กร จะมีผู้เกี่ยวข้อง คือ ผู้ปฏิบัติงานหน้างานต้องเป็นผู้ประเมินความเสี่ยงเอง เพราะเป็นผู้รู้จักงานที่ปฏิบัติดีที่สุด หลังจากประเมินความเสี่ยงเรียบร้อยแล้วต้องเสนอหรือรายงานให้หัวหน้าและผู้บริหารระดับสูงรับทราบเพื่อการจัดการความเสี่ยงที่ตนเองไม่สามารถกระทำได้ด้วยตนเอง อาจต้องมีนโยบายที่เหมาะสมจากผู้บริหารเข้ามาช่วยจัดการความเสี่ยงนั้น โดยกระบวนการประเมินความเสี่ยงต้องมีมาตรฐานที่องค์กรประยุกต์ใช้นำมาประเมินความเสี่ยง ซึ่งอาจต้องเรียนรู้ศึกษาทำความเข้าใจกับตัวมาตรฐาน รวมถึงวิธีการประเมินความเสี่ยงก่อนดำเนินการประเมินความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยง แบ่งออกเป็น 7 หัวข้อหลัก

1) กำหนดวัตถุประสงค์ขอบเขตการประเมิน
2) ระบุความเสี่ยง คือ ตรวจดูช่องโหว่ของภัยคุกคามที่อาจเกิดขึ้น
3) ประเมินความเสี่ยงในเรื่องโอกาสการเกิดกับผลกระทบ
4) ประเมินมาตรการควบคุม
5) การจัดการความเสี่ยง ให้ระบุกิจกรรม วิธีการ
6) รายงานผลเป็นภาพรวมของการประเมิน
7) การติดตามและทบทวนตามรอบการประเมิน

ประเภทความเสี่ยงมีอยู่ 5 กลุ่ม ดังนี้

1) ความเสี่ยงด้านยุทธศาสตร์ : การบรรลุเป้าหมายและวัตถุประสงค์ ชื่อเสียง ภาพลักษณ์สำนักงาน
2) ความเสี่ยงด้านการดำเนินงาน : ความพร้อมของบุคลากร รูปแบบ วิธีการ กระบวนการดำเนินงาน
3) ความเสี่ยงด้านการเงิน : การบริหารจัดการงบประมาณ และค่าใช้จ่าย
4) ความเสี่ยงด้านกฎหมาย : การปฏิบัติตามกฎหมาย ระเบียบที่เกี่ยวข้อง
5) ความเสี่ยงด้านข้อมูลเทคโนโลยี : การรักษาความลับ และความมั่นคงทางไซเบอร์ ความถูกต้องเชื่อถือได้ของระบบและข้อมูล ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ

2.2 กระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ERM

COSO ERM เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กรอย่างเป็นระบบ (Internal Framework) จนกระทั่งเป็นที่รู้จักและมีความนิยม ต่อมา **COSO** ได้กำหนดคำนิยามและรูปแบบต่างๆ ในการจัดการกับความเสี่ยง โดยได้กำหนดออกมาเป็น **COSO ERM** มีใช้ตั้งแต่ ค.ศ. 1990 จนปัจจุบันนี้หน่วยงานภาครัฐนำมาปรับใช้ประเมินความเสี่ยงขององค์กร

COSO ERM แบ่งเป็น 5 ส่วนหลัก

1) Governance and Culture: แต่งตั้งคณะกรรมการกำกับดูแลการบริหารความเสี่ยง จัดโครงสร้างสายการบังคับบัญชาด้านการบริหารความเสี่ยง กำหนดวัฒนธรรมความเสี่ยงขององค์กร แสดงความมุ่งมั่นต่อค่านิยมองค์กร และจูงใจ พัฒนาและรักษาไว้ซึ่งบุคคลที่มีความสามารถ
2) Strategy & Objective Setting: วิเคราะห์โครงสร้างธุรกิจ กำหนดความเสี่ยงที่องค์กรสามารยอมรับได้ การประเมินกลยุทธ์ในรูปแบบต่างๆ กำหนดวัตถุประสงค์ในการดำเนินธุรกิจ
3) Performance: การระบุปัจจัยเสี่ยง การประเมินความเสี่ยง การจัดลำดับความเสี่ยง การตอบสนองต่อความเสี่ยง และภาพรวมความเสี่ยงขององค์กร
4) Review & Revision: ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ ทบทวนความเสี่ยงและผลการดำเนินงาน และหาแนวทางในการปรับปรุงการบริหารความเสี่ยง
5) Information Communication & Reporting: ผลักดันการใช้เทคโนโลยีสารสนเทศ สื่อสารด้านการบริหารความเสี่ยง และรายงานผลการบริหารความเสี่ยง

การกำหนดความเสี่ยง

1) ปัจจัยเสี่ยงในปีที่ผ่านมาที่ไม่สามารถจัดการได้
2) ตัวชี้วัดตามแผนปฏิบัติการ
3) นโยบายของรัฐบาล
4) ผลการดำเนินงานที่สำคัญตามวัตถุประสงค์ขององค์กร
5) ความคาดหวังและความต้องการของผู้มีส่วนได้เสีย
6) ปัจจัยที่ส่งผลต่อภาพลักษณ์และชื่อเสียง
7) แผนแม่บทต่างๆ ที่เกี่ยวข้อง

ยกตัวอย่าง

การประเมินความเสี่ยง เป็นการวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงมาทำการประเมินหาค่าระดับความเสี่ยงโดยแบ่งเป็น 2 มิติ แต่ละมิติจะมีคะแนนในการประเมินออกเป็น 5 ระดับ ประกอบด้วย

เกณฑ์การประเมินระดับโอกาสเกิด (Likelihood)

1=เกิดขึ้นได้ยาก	2=เกิดขึ้นบ้างเป็นบางครั้ง	3=เกิดขึ้นค่อนข้างบ่อย	4=เกิดขึ้นบ่อย	5=เกิดขึ้นเป็นประจำ
แทบจะไม่เกิดเหตุการณ์ หรือเกิดเหตุการณ์ไม่เกินปีละ 1 ครั้ง	โอกาสเกิดเหตุการณ์ต่ำ หรือเกิดเหตุการณ์ไม่เกินปีละ 2 ครั้ง	โอกาสเกิดเหตุการณ์ปานกลาง หรือเกิดเหตุการณ์ปีละ 3-5 ครั้ง	โอกาสเกิดเหตุการณ์สูง หรือเกิดเหตุการณ์ปีละ 6-10 ครั้ง	โอกาสเกิดเหตุการณ์สูงมาก หรือเกิดเหตุการณ์อย่างน้อยเดือนละ 1 ครั้ง
เป็นไปไม่ได้	ไม่มีข้อบ่งชี้หรือหลักฐานที่แสดงให้เห็นถึงความเป็นไปได้ที่จะเกิดเหตุการณ์ขึ้นในระยะเวลาอันใกล้	มีข้อบ่งชี้ที่อาจจะมีความเป็นไปได้บ้างที่จะเกิดเหตุการณ์ขึ้นในระยะเวลาอันใกล้	มีข้อบ่งชี้ที่อาจจะคาดว่าจะเกิดเหตุการณ์ขึ้นในระยะเวลาอันใกล้	มีข้อบ่งชี้หรือหลักฐานที่แสดงให้เห็นถึงความเป็นไปที่จะเกิดเหตุการณ์ในปัจจุบัน

การจัดลำดับความเสี่ยง

การจัดลำดับความเสี่ยง (Risk Prioritization) คือ กระบวนการประเมินและเรียงลำดับเหตุการณ์ที่ไม่พึงประสงค์ตามระดับความรุนแรง (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) โดยใช้เมทริกซ์ความเสี่ยง (Risk Matrix) เพื่อให้องค์กรสามารถจัดสรรทรัพยากรและจัดการความเสี่ยงที่สำคัญที่สุด (มุมบนขวา: โอกาสสูง - ผลกระทบรุนแรง) ได้ก่อน

การตอบสนองความเสี่ยง มี 4 ประเภท

1) การยอมรับความเสี่ยง : ถ้าความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้
2) การลด/ควบคุมความเสี่ยง : เป็นการกำหนดกิจกรรม/มาตรการเพื่อลดความเสี่ยง
3) การหลีกเลี่ยง : เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ความเสี่ยงนั้น
4) การกระจาย/ถ่ายโอนความเสี่ยง : เป็นการ่ายโอนความรับผิดชอบหรือภาระของการสูญเสียให้บุคคลอื่น

วิธีการตอบสนองความเสี่ยงทั้ง 4 ประเภทไม่สิ่งใดที่บอกได้ว่าถูกหรือผิด ขึ้นอยู่กับวัฒนธรรมองค์กรที่จะทำให้เกิดแผนการลดความเสี่ยง และความเสี่ยงเป็นเรื่องของคนในองค์กร เป็นเรื่องนโยบาย

2.3 กระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

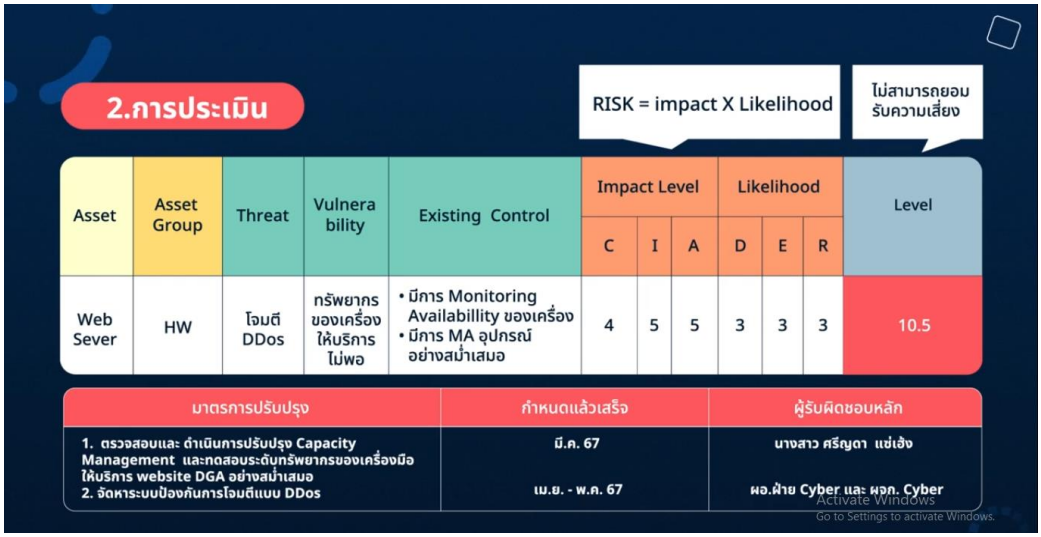
การประเมินความเสี่ยงทาง **Cyber Security** เป็นสิ่งที่เพิ่งเกิดขึ้นใหม่ตามที่มีการกำหนดพระราชบัญญัติทางไซเบอร์ พ.ศ.2562 ซึ่งการโจมตีทางไซเบอร์ในปัจจุบันทางหน่วยงานรัฐก็มีข้อมูลรั่ว ความเสี่ยงทางด้านไซเบอร์จะเน้นหนักไปทางด้านข้อมูลเป็นส่วนใหญ่ ที่ทำให้เกิดการสูญเสียเงิน ข้อมูลถูกทำลาย รวมถึงระบบบริการถูกรบกวนการทำงาน โดยมีรูปแบบมาจาก Cyber Attack, User Error หรือความเข้าใจคลาดเคลื่อนของบุคคลในองค์กร

กรอบการประเมินความเสี่ยงไซเบอร์

ในปัจจุบันสามารถเลือกใช้ได้หลายรูปแบบทั้ง COSO หรือ ISO 27001 หรือ NIST 800-30 หรือมาตรฐานต่างๆ ที่ใช้กัน ฉะนั้นก่อนการประเมินความเสี่ยงทางด้านไซเบอร์ ผู้ประเมินจะต้องมีความรู้ความเข้าใจเกี่ยวกับการ***เลือกหลักการประเมินความเสี่ยง***ของแต่ละมาตรฐาน รวมถึงกระบวนการทำงาน (Framework) ที่จะประยุกต์ใช้ในการประเมินความเสี่ยงทางไซเบอร์ โดย***ผู้ตรวจประเมิน***จะต้องมีความรู้ความเข้าใจหลักการประเมินความเสี่ยง ผ่านการหาความรู้ ผ่านการอบรม หรือเรียนออนไลน์ หรือหารือผู้ที่มีความรู้เรื่องการประเมินความเสี่ยง ฉะนั้น ***การรายงานการประเมินความเสี่ยง***อาจต้องสรุปรายงานแยกออกจากรายงานการประเมินความเสี่ยงของหน่วยงาน อาจทำตามแบบฟอร์มของแต่ละมาตรฐานที่เลือกใช้ จากนั้น***จำแนก/กำหนดชั้นข้อมูล*** ให้มีผลสรุปรายงานการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และเอกสารที่เกี่ยวข้อง ควรคำนึงเรื่องการใช้งานและจัดเก็บด้วย เพราะว่าผลการประเมินอาจมีผลกระทบต่อข้อมูลข่าวสารที่หากมีการรั่วไหลจะเกิดผลเสียหรือกระทบต่อองค์กรได้ ทั้งนี้การประเมินความเสี่ยงต้องกำหนด***บทบาทหน้าที่***ของผู้รับผิดชอบผู้ที่ทำหน้าที่ประเมินความเสี่ยง ควรเป็นคนละคนกับผู้ตรวจสอบ

กรอบการประเมินความเสี่ยงไซเบอร์ไม่ได้แตกต่างจากการประเมินความเสี่ยงทั่วไปยังมีการใช้ 7 หัวข้อหลัก แต่อาจต้องชี้บ่งทางด้านความมั่นคงปลอดภัยทางไซเบอร์ และนำสินทรัพย์มาใช้ในการประเมินหรือการนำเอากระบวนการภายในองค์กรมาเป็นตั้งตั้งในการประเมินความเสี่ยง

ยกตัวอย่าง



การบริหารจัดการความเสี่ยงที่ดี ประกอบด้วย

1) ผู้ประเมินจะต้องมีความรู้ความเข้าใจเกณฑ์การประเมินความเสี่ยงขององค์กร
2) ทราบบริบทปัจจัยความเสี่ยงภายนอกและภายใน เพื่อนำมาประเมินในส่วนเป็นที่ผลกระทบกับความเสี่ยงที่เกิดขึ้นจากภัยคุกคามและช่องโหว่
3) เจ้าของงานเป็นผู้ประเมินความเสี่ยงเอง
4) พิจารณาวิธีการจัดการความเสี่ยงที่ถูกต้อง และไม่ทิ้งความเสี่ยงที่เป็นความเสี่ยงเกินกว่าที่องค์กรยอมรับได้ จะต้องหามาตรการมาลดความเสี่ยงนั้น
5) นำความเสี่ยงที่ยังเหลือมาจัดการและทบทวนอย่างน้อยปีละ 1 ครั้งหรือหากมีการเปลี่ยนแปลงที่สำคัญกับองค์กรก็ต้องมีการจัดการบริหารความเสี่ยงไว้

หัวข้อที่ 3 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

3.1 กรอบการดำเนินงาน NIST Cybersecurity Framework

Cybersecurity Framework Version 1.1 หรือ CSF V.1.1 เริ่มใช้มาตั้งแต่ปี ค.ศ. 2014 และ NIST Cybersecurity Framework Version 2.0 เริ่มใช้เมื่อ 16 กุมภาพันธ์ พ.ศ.2567 ซึ่งทั้ง 2 เวอร์ชั่นนี้จะมีความแตกต่างกันเล็กน้อย

Cybersecurity Framework Version 1.1 มี 5 Function คือ Identify Protect Detect Respond และ Recover เช่นเดียวกับ NIST Cybersecurity Framework Version 2.0 แต่ Version 2.0 จะเพิ่มอีก 1 Function คือ Govern และจะมีการปรับ Function แยกเป็น Category ย่อย ๆ อีก จากเดิม 23 ลดเหลือ 22 รายการ และตัวควบคุมจาก 108 เหลือ 106 ตัว โดย ใน CSF 2.0 มี 6 แกนหลักสำคัญ (Functions):

1) Govern (การกำกับดูแล): ใหม่! เน้นวางนโยบาย บทบาท และการบริหารความเสี่ยงระดับผู้บริหาร รวมถึงการวางโครงสร้างขององค์กร เหตุผลที่เพิ่มเข้ามาเพื่อให้เกิดการเรียนรู้บริบทองค์กร (Organizational Context) ที่ชัดเจนมากขึ้นก่อนที่จะมีการประยุกต์ใช้ Cybersecurity Framework ภายในองค์กร ควรมีการกำหนดความรับผิดชอบและกรอบนโยบาย

2) Identify (การระบุ): ทำความเข้าใจสินทรัพย์, ข้อมูล, และความเสี่ยง

3) Protect (การป้องกัน): วางระบบป้องกัน เช่น จำกัดสิทธิ์, เทคโนโลยีรักษาความปลอดภัย

4) Detect (การตรวจจับ): ตรวจจับสิ่งผิดปกติอย่างรวดเร็ว

5) Respond (การรับมือ): แผนตอบสนองเมื่อเกิดเหตุ

6) Recover (การกู้คืน): ฟื้นฟูระบบให้กลับมาทำงานต่อเนื่อง

3.2 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564

กรอบมาตรฐาน ประกอบด้วย 5 หัวข้อหลัก คือ

1) การระบุความเสี่ยง (Identify)

- การจัดการทรัพย์สิน (Asset Management) : ทะเบียนสินทรัพย์ รายการสินทรัพย์ที่สำคัญ รายการประเมินความเสี่ยงไซเบอร์ ผลการตรวจสอบ
- การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy): กระบวนการประเมินความเสี่ยง เกณฑ์การยอมรับความเสี่ยง ผลการประเมินความเสี่ยง แผนการจัดการความเสี่ยง
- การประเมินช่องโหว่ (ระบบสำคัญ ระบบใหม่) และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing): ผลการประเมินช่องโหว่ แผนการจัดการช่องโหว่ ผลการทดสอบเจาะระบบ(เท่าที่จำเป็น)
- การจัดการผู้ให้บริการภายนอกตามหลักการของ Security (CIA) ในการกำหนดหน้าที่และความรับผิดชอบ (Information Technology): การเปิดเผยข้อมูล สัญญา ความรับผิดชอบต่อสินทรัพย์ ความเสี่ยง

2) การป้องกันความเสี่ยง (Protect)

- การควบคุมการเข้าถึง (Access Control): กำหนกสิทธิ์ Log access การเข้าถึงทางกายภาพ
- การทำให้ระบบมีความแข็งแรงและจัดทำ Change management Process (System Hardening): รายการตรวจสอบ security bassline ปีละครั้ง
- การเชื่อต่อระยะไกล (Remote Connection): Secure Connection (https, ssh, scp, VPN)
- สื่อเก็บข้อมูลแบบถอดได้ เช่น Laptops, USB (Removable Storage Media): กระบวนการควบคุม กิจกรรมการควบคุม
- การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุม กฎหมาย นโยบาย แนวปฏิบัติ มาตรฐาน (Cybersecurity Awareness): ผลการจัด Cyber Awareness
- การแบ่งปันข้อมูลเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ให้ผู้เกี่ยวข้อง (Information Sharing): แนวทางการแชร์ แนวทางการประยุกต์ใช้งาน

3) การตรวจจับ (Detect)

- การตรวจจับเหตุการณ์ที่เกี่ยวข้องความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญ ซึ่งต้องทราบขอบเขตสินทรัพย์ที่สำคัญ หาซอฟแวร์ในการเฝ้าระวัง ออกแบบกระบวนการเฝ้าระวังและการแจ้งเหตุการณ์
- การจัดประเภทและวิเคราะห์เหตุกาณณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ โดยมีกระบวนการจัดประเภทและวิธีการวิเคราะห์ข้อมูล และการส่งต่อหากพบเหตุการณ์
- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ โดยมีเอกสารรายงานการจัดเก็บและการแก้ไขเหตุการณ์ทางความมั่นคงปลอดภัยทางไซเบอร์

4) การรับมือ/การเผชิญเหตุ (Respond)

- แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan): แผนรับมือภัยคุกคาม Incident Response Plan ผลการทดสอบแผนการรับมือในระดับหน่วยงานอย่างน้อยปีละครั้ง
- แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan): ตั้งทีมสื่อสาร กระบวนการขั้นตอน การสื่อสารที่ระบุเป้าหมายและโฆษกหลักและผู้เชี่ยวชาญทางเทคนิค การระบุช่องทางทางการสื่อสาร

- การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise): ฝึกซ้อมตามที่ระบุในแผนรับมือขององค์กร

5) การฟื้นฟูความเสียหาย (Recover)

- มาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery): หลังจากผ่านพ้นเหตุการณ์ภัยคุกคาม การฟื้นฟูระบบและข้อมูลถือเป็นสิ่งสำคัญ หน่วยงานควรมีแผนสำรองข้อมูล (Backup) ที่อัพเดทอยู่เสมอ. BCP Plan, IT DRP

หัวข้อที่ 4 การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)

ปัจจุบัน หลายองค์กรมีการให้ความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์กับบุคลากรภายในองค์กรมากขึ้น อีกทั้งยังมีการติดตั้งอุปกรณ์ป้องกันภัยคุกคามต่างๆ เพิ่มมากขึ้น แต่ไม่อาจมั่นใจได้ว่าจะปลอดภัย 100% เนื่องจากแฮกเกอร์หรือผู้ประสงค์ร้ายมีการปรับเปลี่ยนรูปแบบการโจมตีระบบอยู่สม่ำเสมอ เพื่อค้นหาช่องทางในการเข้าถึงระบบผ่านเครือข่าย ดังนั้น การตรวจสอบช่องโหว่อย่างสม่ำเสมอจะช่วยป้องกันการโจมตีที่อาจจะเกิดขึ้นได้ในอนาคตได้

การประเมินช่องโหว่ (Vulnerability Assessment: VA) คือ กระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่ และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัย ซึ่งกระบวนการนี้ช่วยให้ทราบึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชันจนนำไปสู่การแก้ไขได้อย่างูกจุดเพื่อความปลอดภัย

เพื่อตรวจสอบความปลอดภัยระบบเครือข่ายค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ฯลฯ ซึ่งนับเป็นเรื่องสำคัญที่ใช้ระบุระดับความรุนแรงของช่องโหว่ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS

ประโยชน์ของการทำ Vulnerability Assessment

1) ช่วยในการประเมินระดับความเสี่ยงที่มาจากช่องโหว่ โดยประเมินความรุนแรงของช่องโหว่ และความเสี่ยงที่อาจเกิดขึ้นหากไม่แก้ไขช่องโหว่นั้น
2) ช่วยในการสร้างรายงานที่รวมข้อมูลเกี่ยวข้องกับช่องโหว่ที่พบ และให้คำแนะนำในการแก้ไข รายงานเหล่านี้ช่วยให้มีความมั่นคงปลอดภัยที่ทำการประเมินและตัดสินใจในการแก้ไขช่องโหว่ได้อย่างประสิทธิภาพ
3) ช่วยในการตรวจอบว่าระบบสอดคล้องกับมาตรฐาน เช่น PCI หรือ HIPAA หากไม่สอดคล้องจะช่วยในการปรับปรุงความปลอดภัยเพื่อเป็นไปตามข้อกำหนด

4) ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย ในระหว่างการพัฒนาระบบหรือแอปพลิเคชัน อีกทั้งยังช่วยประหยัดเวลาและค่าใช้จ่ายที่เกิดขึ้นได้ในอนาคตหากมีการโจมตีที่ไม่คาดคิดเกิดขึ้น

รูปแบบของการทำ Vulnerability Assessment Scan

1) Host **Assessment** คือ การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้ หากไม่ได้รับการทดสอบอย่างเพียงพอ
2) Network and Wireless **Assessment** คือ การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต
3) Database **Assessment** คือ การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล
4) Application Scan คือ การใช้วิธีการระบุช่องโหว่ทางด้านความปลอดภัยใน Web Application และ Source Code โดยการ Scan แบบอัตโนมัติ Front-end หรือไม่ก็วิเคราะห์ที่ Source Code

ขั้นตอนการทำ Vulnerability Assessment Scan

1) Testing: การระบุช่องโหว่โดยใช้วิธีการทดสอบ

   จุดประสงค์ของขั้นตอนนี้ คือ การเตรียมรายการของช่องโหว่ใน Application ผู้ที่วิเคราะห์จะทำการทดสอบความแข็งแรงของระบบ Security หรือระบบอื่นๆ โดยใช้เครื่องมือในการ Scan ระบบให้อัตโนมัติซึ่งต้องใช้ข้อมูลจากการประกาศของ Vendor ที่มีการเก็บ Vulnerability Database ไว้เพื่อให้ง่ายต่อการระบุช่องโหว่ที่เคยเกิดขึ้นมาแล้ว

2) Vulnerability Analysis: การวิเคราะห์ช่องโหว่และภัยคุกคาม

   จุดประสงค์ของขั้นตอนนี้ คือ การหาสาเหตุหรือต้นตอที่เจอช่องโหว่มาจากข้อที่ 1 รวมไปถึงการระบุรายละเอียดของกรทำงานของระบบและสาเหตุของการเกิดช่องโหว่ เช่น ปัญหาที่อาจเกิดจากการใช้งาน Software ที่เป็น Open Source ที่ใช้ Library Version เก่า

3) Risk Assessment: การประเมินความเสี่ยง

   จุดประสงค์ของขั้นตอนนี้ คือ การจัดลำดับความสำคัญของช่องโหว่ จะระบุเป็น Rank หรือ Score ว่าช่องโหว่ไหนร้ายแรงกว่ากัน โดยอ้างอิงมาจากปัจจัยเหล่านี้ ระบบที่ได้รับผลกระทบ ข้อมูลอะไรบ้างที่เป็นความเสี่ยงง่ายต่อการโจมตี ความรุนแรงของการโจมตี ความเสียหายที่อาจจะเกิดขึ้นของช่องโหว่

4) Remediation: การแก้ไข

จุดประสงค์ของขั้นตอนนี้ คือ การอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการร่วมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่า การอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุด โดยไม่กระทบกับระบบปัจจุบัน หรืออาจกระทบน้อยลง

โดยขั้นตอนทั้ง 4 เป็นกระบวนการกรหลักในการดำเนินการ โดยมีการแนะนำให้วางระบบ Security ใหม่ มาตรการต่างๆ รวมไปถึงการใช้เครื่องมือต่างๆ มีการปรับปรุงวิธีการทำงานในส่วนของ Operation และการเปลี่ยนแปลงการตั้งค่าต่างๆ มีการพัฒนาและติดตั้งเพิ่มเติม โดยใช้แบบใหม่ในการอุดช่องโหว่ นอกจากนี้การจัดหาบุคลากรและอุปกรณ์ ยังช่วยลดความเสี่ยงจาการโจมตีของผู้ไม่หวังดี

ฉะนั้น **การประเมินช่องโหว่ (Vulnerability Assessment: VA)** ควรทำอย่างน้อยปีละ 2 ครั้ง

หัวข้อที่ 5 การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การเฝ้าระวังภัยทางไซเบอร์ คือ กระบวนการการตรวจจับความผิดปกติของระบบ พฤติกรรมของผู้ใช้งาน หรือการโจมตีที่เกิดขึ้นกับระบบหรือข้อมูล หากพบเหตุการณ์ดังกล่าวสามารถแจ้งเตือนหรือประสานงานไปยังผู้เกี่ยวข้องได้ เพื่อจะได้ทำการแก้ไขหรือตอบสนองในทางใดทางหนึ่ง ทั้งนี้การเฝ้าระวังภัยคุกคามจะต้องกระทำอย่างต่อเนื่อง และให้มีประสิทธิภาพ และสามารถตรวจจับภัยคุกคามหรือเหตุผิดปกติได้อย่างงรวดเร็วโดยมีวัตถุประสงค์เพื่อ

1) ลดความเสียหายที่อาจเกิดขึ้นได้ หรือสามารถจำกัดวงของความเสียหายที่เกิดขึ้นได้
2) สามารถลดโอกาสหรือระยะเวลาของผู้โจมตีระบบได้
3) กระบวนการการเฝ้าระวังที่ดี สามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการการตอบสนองต่อเหตุการณ์หรือการกู้คืนระบบได้

ตัวอย่างเหตุการณ์ผิดปกติ

1) พบการ Login ที่ผิดพลาดหลายครั้ง เพื่อพยายามเข้าสู่ระบบเป็นจำนวนมาก
2) การ Login เข้าสู่ระบบนอกเวลางาน
3) พบการ Login มาจากต้นทางที่น่าสงสัย เช่น พบการ Login มาจากต่างประเทศ โดยที่หน่วยงานเองไม่มีเจ้าหน้าที่ที่อยู่ประเทศนั้นๆ
4) การเรียกใช้งาน Program หรือ Library ที่ผิดปกติ
5) การทำงานของ CPU หรือการใช้งานระบบเครือข่ายมากผิดปกติ
6) มีการติดต่อไปยัง IP Address หรือ Domain ที่ถูกระบุว่าเป็น Malicious

ตัวอย่างระบบหรือเครื่องมือที่ใช้ในการเฝ้าระวัง

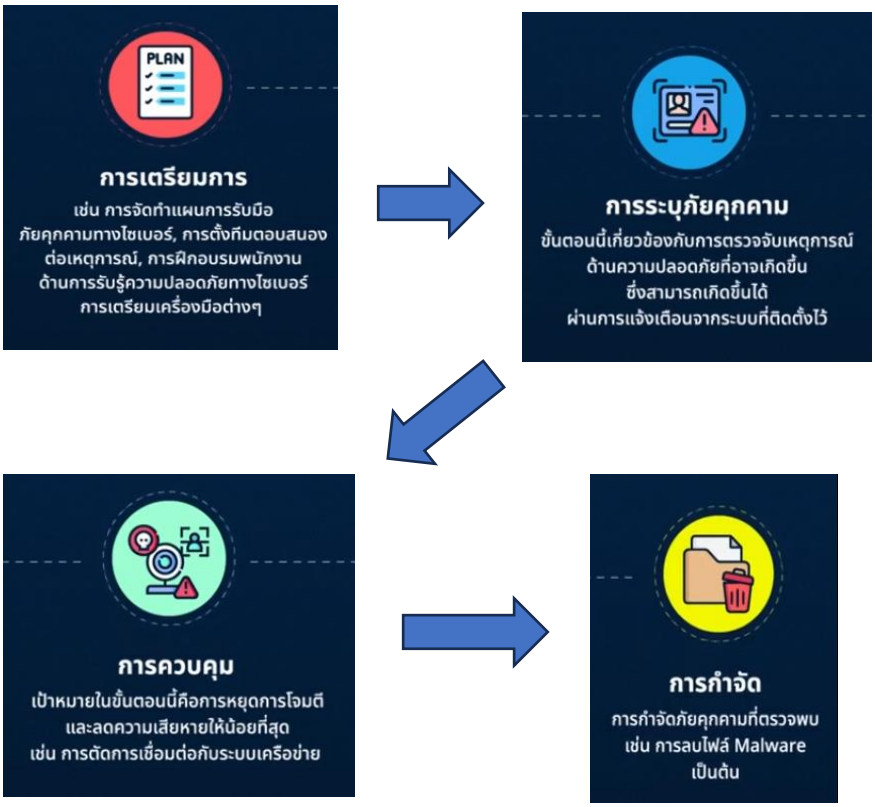
1) ระบบ Intrusion Detection Systems (IDS)
2) ระบบ Intrusion Prevention Systems (IPS)
3) ระบบ Security Information and Event Management (SIEM)
4) ระบบ Endpoint Detection and Response (EDR)

หัวข้อที่ 6 การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์เป็นขั้นตอนที่สำคัญมาก เพราะแม้จะป้องกันข้อมูลได้ดีเพียงใด แต่ก็ยังมีโอกาสที่จะถูกโจมตีได้เสมอ ดังนั้น การตอบสนองที่รวดเร็วคือการตอบสนองที่ถูกต้องและจะช่วยเพิ่มมีประสิทธิภาพและรับมือได้อย่างดี ทำให้ผลกระทบหรือความเสียหายถูกจำกัดวงแคบลงไป

ทั้งนี้ หน่วยงานหรือองค์กรควรมีการทำแผนรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้ทันต่อการเหตุที่อาจเกิดขึ้น และหน่วยงานจะได้ทราบข้อควรปฏิบัติทู่กต้องและรวดเร็ว เป็นขั้นเป็นตอน และในแผนควรมีการกำหนดบทบาทของแต่ละบุคคลให้เหมาะสม ชัดเจน มีกำหนดกฎเกณฑ์เงื่อนไขที่จะต้องดำเนินการ ฉะนั้น เมื่อมีแผนที่เรียบร้อยแล้ว หน่วยงานต้องสื่อสารไปยังบุคคลที่เกี่ยวข้อง และควรมีการซักซ้อมและทบทวน ฝึกปฏิบัติแผนอย่างสม่ำเสมอ โดยมีการซ้อมแผนรับมือปีละ 1 ครั้ง

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์



เมื่อดำเนินการครบทุกขั้นตอนแล้ว ควรมีการวิเคราะห์ถึงสาเหตุของต้นตอเหตุการณ์ที่เกิดขึ้น รวมถึงผลกระทบที่เกิดขึ้นทั้งหมด และมีการบันทึกเป็นข้อเสนอเพื่อเสนอแนะไปยังหน่วยงานที่เกี่ยวข้อง เพื่อลดผลกระทบหรือปรับปรุงกระบวนการทำงาน เพื่อไม่ให้เกิดปัญหาซ้ำในอนาคต ทั้งนี้ในขั้นตอนการรับมือภัยคุกคามหน่วยงานควรมีแผนการสื่อสารในภาวะวิกฤต เพื่อให้ข่าวสารที่ส่งออกไปมีความครบถ้วนถูกต้องและรวดเร็ว เพื่อให้ผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้เสียกับระบบหรือเหตุการณ์ที่เกิดขึ้นมีความสามารถในการรับมือกับภัยคุกคามได้ หรือสามารถเตรียมตัวดำเนินการได้อย่างมีประสิทธิภาพ

ขั้นตอนการกู้คืนระบบ

1) จัดทำแผนความเสี่ยงทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้มั่นใจได้ว่า เมื่อเกิดเหตุการณ์หยุดชะงักที่ระบบที่สำคัญแล้ว จะสามารถดำเนินการกู้คืนระบบ เพื่อให้สามารถใช้บริการได้อย่างต่อเนื่อง
2) การสำรองข้อมูล ควรทำอย่างสม่ำเสมอ และต้องมีการทดสอบข้อมูลสำรองว่าสามารถใช้งานได้
3) ปรับปรุงมาตรการรักษาความปลอดภัย โดยเรียนรู้จากเหตุการณ์และใช้มาตรการรักษาความปลอดภัยเพิ่มเติม เพื่อป้องกันเหตุการณ์ที่คล้ายกันในอนาคต

หัวข้อที่ 7 บทสรุป

ในยุคที่เทคโนโลยีและอินเตอร์เน็ตเข้ามามีบทบาทสำคัญในชีวิตประจำวัน ความปลอดภัยทางไซเบอร์กลายเป็นสิ่งที่ไม่สามารมองข้ามได้ การรักษาข้อมูลถือเป็นหัวใจสำคัญที่ช่วยป้องกันความเสี่ยงจากการโจมตีทางไซเบอร์ ฉะนั้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น ประกอบด้วย

1) การปกป้องข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลการเงิน เป็นเป้าหมายหลักในการโจมตีทางไซเบอร์ การถูกขโมยข้อมูลส่วนบุคคลสามารถนำไปสู่การสูญเสียทางการเงินหรือถูกนำไปใช้ในทางที่ผิด โดยการตั้งรหัสผ่านที่บากต่อการคาดเดา หลีกเลี่ยงการใช้รหัสซ้ำๆ รวมการสร้างความปลอดภัย 2 ชั้น หรือการยืนยันตัวตน 2 ขั้นตอน (2FA - Two-Factor Authentication)

2) การป้องกันการโจมตีทางไซเบอร์ มีแนวคิดหลักเป็นการดำเนินการเพื่อให้คงไว้ซึ่งหลัก CIA คือ Confidentiality Availability และ Integrity ของข้อมูลและระบบที่ให้บริการเป็นหลัก

3) การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ ไม่ว่าจะลงทุนป้องกันและดำเนินการป้องกันดีแค่ไหน ก็ไม่สามารรับรองได้ว่า สินทรัพย์นั้นจะปลอดภัย 100% ฉะนั้น จึงต้องดำเนินการประเมินความเสี่ยงและดำเนินการตามแผนพร้อมรับมือหากเกิดภัยคุกคามตามแผนรับมือที่เกิดอย่างรวดเร็ว ลดความเสียหายและระงับเหตุได้ทันท่วงที และมีแผนสุดท้าย คือ แผนในการฟื้นฟูบริการเพื่อให้สามารถกลับมาให้บริการได้อย่างต่อเนื่อง

4) การสร้างความเชื่อมั่นและความน่าเชื่อถือในโลกธุรกิจ ความปลอดภัยทางไซเบอร์มีความสำคัญต่อการสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจ องค์กรที่มีมาตรการรักษาความปลอดภัยที่ดีจะได้รับความเชื่อถือจากลูกค้า เนื่องจากลูกค้าจะมั่นใจว่า ข้อมูลของตนจะปลอดภัยไม่ถูกละเมิด

นอกจากนี้ ความปลอดภัยทางไซเบอร์ที่เข้มแข็งจะป้องกันความเสียหายทางธุรกิจที่อาจจะเกิดจากการโจมตีทางไซเบอร์ได้ เช่น การถูกเรียกค่าไถ่ข้อมูล หรือ การสูญเสียความสามารถในการดำเนินธุรกิจ

สรุป การมีความรู้พื้นฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นสิ่งจำเป็นสำหรับทุกคนในยุคดิจิทัล เพราะไม่เพียงแต่ป้องกันข้อมูลส่วนบุคคล และระบบคอมพิวเตอร์ของตนเอง แต่ยังสร้างความมั่นคงแก่องค์กร และสร้างความเชื่อมั่นให้ลูกค้าและพันธมิตรทางธุรกิจ การลงทุนในความรู้และการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ควรทำเพื่อเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่จะเกิดในอนาคต

ประโยชน์ที่ได้รับจากการฝึกอบรม

- ต่อตนเอง คือ ได้รับความรู้ ความเข้าใจ เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การประเมินความเสี่ยง และการรับมือกับภัยคุกคาม สามารถนำมาปรับใช้ในการทำงาน ทำให้การทำงานมีประสิทธิภาพ และยังสามารถนำไปใช้ในชีวิตประจำวันได้ เพื่อป้องกันตนเองและข้อมูลส่วนบุคคลรวมถึงอุปกรณ์เครื่องมือและระบบต่างๆ ให้ปลอดภัยจากการโจมตี

- ต่อหน่วยงาน สามารถนำความรู้ที่ได้รับไปช่วยให้ความรู้แก่บุคลากรเจ้าหน้าที่ผู้ปฏิบัติงานในองค์กรได้ และช่วยในการวางแผน จัดทำแผนในการการประเมินความเสี่ยงขององค์กร เป็นส่วนหนึ่งที่ช่วยให้ระบบและอุปกรณ์ของหน่วยงานปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้นได้ ลดความเสียของข้อมูลหน่วยงาน และสามารถแนะนำและแก้ไขปัญหาเบื้องต้นให้แก่บุคลากรในหน่วยงานได้

(นางสาวณัฐสุดา แซ่ลิ้ม)
นักจัดการงานทั่วไปชำนาญการ
ผู้สรุปการอบรม
วันที่ 26 กุมภาพันธ์ 2569