

สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์

(Understanding Cybersecurity Risk Management)

ชื่อ-สกุล นางสาวจรรุวรรณ เขียงมะณี ตำแหน่ง นักวิชาการเกษตรชำนาญการ

สังกัด กลุ่มวิจัยและพัฒนาการอนุรักษ์ดินและน้ำเพื่อการเกษตร กองวิจัยและพัฒนาการจัดการที่ดิน

วันที่อบรม 11 สิงหาคม 2569

อาจารย์ผู้สอน ผศ.(พิเศษ) ดร.สันติพัฒน์ อรุณธาริ สังกัด มหาวิทยาลัยหอการค้าไทย

วัตถุประสงค์ของหลักสูตร

1. ปูพื้นฐานการเชื่อมโยง Cybersecurity, IT Standard, Risk Management, Process และ Life cycle เพื่อให้เกิดความรู้ ความเข้าใจ และนำไปปฏิบัติได้
2. เรียนรู้ Core concept ของการจัดการความเสี่ยงด้านไซเบอร์ (Risk Management) เพื่อเข้าใจ Framework และ IT Standard ที่สำคัญต่างๆ
3. ประยุกต์แนวคิดในการจัดทำ BCP และการบริหารความต่อเนื่องทางธุรกิจเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

สรุปบทเรียน

Cybersecurity vs Information security

Cyber Security (ความมั่นคงปลอดภัยไซเบอร์) คือ การปกป้องระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบดิจิทัล จากภัยคุกคามทางไซเบอร์ (Cyber attack) ทั้งจากภายในและภายนอกองค์กร

Information Security (ความมั่นคงปลอดภัยสารสนเทศ) คือ เป็นพื้นฐานในการปกป้องข้อมูลทุกรูปแบบให้เป็นความลับทั้ง Online และ Offline ทำให้ข้อมูลมีความถูกต้องและพร้อมใช้งาน ดังนั้น **Cyber Security** จึงเป็นส่วนหนึ่งของ **Information Security**

Cyber Security Risk Management คือ การจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber attack) และอาชญากรรมทางไซเบอร์ (Cyber Crime) ที่กระทบต่อบุคคลในองค์กรและองค์กรในภาพใหญ่ จึงต้องมีการจัดการความเสี่ยงในเรื่องของ Cybersecurity และ Cyber attack โดยคำนึงถึง ความเสี่ยง (Risk) Impact (ผลกระทบ) และ โอกาสในการเกิด (Likelihood) ซึ่งมีองค์ประกอบหลัก ดังนี้

1. **Identifying Risk (การระบุความเสี่ยง)** ระบุประเด็นต่างๆ ที่อาจก่อให้เกิดความเสี่ยง
2. **Assess Risk (การประเมินความเสี่ยง)** วิเคราะห์ว่า โอกาสในการเกิด (Likelihood) เท่าไร ผลกระทบ (Impact) รุนแรงแค่ไหน
3. **Control Risk (การควบคุม/ลดความเสี่ยง)** คือการกำหนดมาตรการควบคุม
4. **Review Controls (การทบทวนและปรับปรุง)** ทบทวนกระบวนการ

Frameworks

Frameworks คือ โครงสร้างแนวทางที่ช่วยให้องค์กรทำงานอย่างเป็นระบบ มีมาตรฐาน และควบคุมความเสี่ยงได้ ซึ่งมีหลายวิธี เช่น

- ✓ COSO (Committee of Sponsoring Organizations of the Treadway Commission) ใช้สำหรับ Enterprise Risk Management (ERM) เน้นบริหารความเสี่ยงระดับองค์กรทั้งหมด ไม่ใช่เฉพาะ IT
- ✓ ISO 27001 มาตรฐานสำหรับ Information Security Management System (ISMS) - ISO 27032 ISO/IEC 27032 แนวทางด้าน Cybersecurity โดยเฉพาะเน้นการป้องกันภัยไซเบอร์ในโลกออนไลน์
- ✓ NIST (National Institute of Standards and Technology) เป็น Framework ที่นิยมใช้มากที่สุด
- ✓ ISO 31000 มาตรฐานด้าน Risk Management ทั่วไปใช้ได้กับทุกอุตสาหกรรม
- ✓ ISO 27005 แนวทางบริหารความเสี่ยงด้าน Information Security ทำงานคู่กับ ISO 27001 - COBIT Framework สำหรับ IT Governance และ IT Management

NIST Cybersecurity Framework (CSF) ประกอบด้วย

- ✓ Framework Core คือ โครงสร้างหลักของกิจกรรมด้าน Cybersecurity ประกอบด้วย Functions (5 ฟังก์ชันหลัก) คือ Identify/ Protect /Detect/ Respond/ Recover
- ✓ Framework Implementation Tiers คือ เป็นการจัดระดับความพร้อมองค์กร แบ่งเป็น 4 Tiers ได้แก่ Partial/Risk Informed/Repeatable/Adaptive
- ✓ Framework Profiles คือ การเลือกสิ่งที่เหมาะสมกับองค์กร องค์กรจะกำหนด Current Profile (ปัจจุบันทำอะไรอยู่) และ Target Profile (อยากไปถึงระดับไหน)

Business Continuity Planning (BCP) คือ การวางแผนล่วงหน้าเพื่อให้องค์กรสามารถดำเนินธุรกิจต่อไปได้ แม้เกิดเหตุการณ์ไม่คาดคิด เช่น ไฟดับ หรือภัยธรรมชาติ

ISO 22301: Business Continuity Management คือ ระบบบริหารความต่อเนื่องทางธุรกิจ ไม่สะดุดจากการเกิดเหตุการณ์ต่างๆ หรือถ้าเกิดเหตุการณ์ขึ้นก็สามารถกลับมาเป็นปกติได้อย่างรวดเร็ว เป้าหมายหลัก คือ การเตรียมพร้อม รับมือ และฟื้นตัวจากเหตุการณ์หยุดชะงักได้อย่างเป็นระบบขององค์กร ประกอบด้วยโครงสร้างหลัก ดังนี้

- ✓ Context of the Organization วิเคราะห์บริบทองค์กร ผู้มีส่วนได้เสีย และความเสี่ยง
- ✓ Leadership ผู้บริหารต้องสนับสนุนและกำหนดนโยบาย BC Planning ประเมินความเสี่ยง ทำ BIA (Business Impact Analysis) และกำหนด RTO / RPO Support ทรัพยากรบุคลากร การสื่อสาร และเอกสาร
- ✓ Operation การจัดทำและนำ BCP ไปใช้จริง
- ✓ Performance Evaluation ทดสอบแผน ตรวจสอบ ประเมินผล Improvement ปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)



Wrap Up

- ✓ องค์กรต้องบริหารความเสี่ยงด้านไซเบอร์ เพื่อลดโอกาสในการเกิดความเสี่ยง ผลกระทบ และลดความรุนแรงได้
- ✓ จัดทำ Framework เป็นแนวทางทำงานอย่างเป็นระบบ มีมาตรฐาน และควบคุมความเสี่ยงได้
- ✓ สร้างแผน BCP เพื่อรับมือเหตุการณ์ไม่คาดคิดได้ และกลับมาทำธุรกิจได้อย่างต่อเนื่อง
- ✓ ต้องทดสอบและปรับปรุงระบบ และการจัดการอย่างต่อเนื่อง



ประโยชน์ที่ได้รับต่อตนเอง

1. สามารถเข้าใจเรื่องความมั่นคงปลอดภัยไซเบอร์ เพื่อปกป้องระบบเครือข่ายจากการคุกคามและอาชญากรรมทางไซเบอร์
2. เข้าใจระบบการบริหารความเสี่ยงด้านไซเบอร์ Framework และ IT Standard ที่สำคัญต่างๆ
3. เข้าใจบทบาทของ BCP และสามารถประยุกต์ใช้ NIST และ ISO22301 เพื่อเพิ่มความพร้อมในการรับมือภัยคุกคามไซเบอร์



ประโยชน์ที่ได้รับต่อหน่วยงาน

1. สามารถนำแนวทางการประเมินความเสี่ยงด้านไซเบอร์ แนวทางการควบคุมความเสี่ยง มาประยุกต์ใช้ในการปกป้องระบบเครือข่ายของข้อมูลงานวิจัยที่เป็นฐานข้อมูลสำคัญของหน่วยงานให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ เช่น การ Backup ฐานข้อมูลเป็นประจำ
2. ควรมีการปรับปรุงระบบ และจัดการฐานข้อมูลอย่างต่อเนื่อง เพื่อให้เกิดความเสียหายน้อยที่สุด หรือสามารถทำงานได้อย่างต่อเนื่อง เมื่อเกิดเหตุการณ์ไม่คาดคิดต่างๆ เช่น การติดไวรัส หรือเกิดเหตุภัยธรรมชาติต่างๆ
3. สนับสนุนการดำเนินการควบคุมความเสี่ยงด้านไซเบอร์ของหน่วยงานภาครัฐตามมาตรฐาน เพื่อลดโอกาสในการเกิดความเสี่ยง ผลกระทบ และลดความรุนแรงของการคุกคามทางไซเบอร์ เพื่อสร้างความเชื่อมั่นในการใช้บริการข้อมูลทั้งบุคลากรภายในหน่วยงาน และบุคคลภายนอก เช่น ประชาชน องค์กรต่างๆ