

สรุปบทเรียน E Learning

หลักสูตร “ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์”

(Understanding Cybersecurity Risk Management)

โดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล <https://tdga.dga.or.th/>



ผศ. (พิเศษ) ดร.สันติพัฒน์ อรุณธารี

Asst.Prof. Dr. Santipat Arunthari Academic
and Special Project Director Center of
Digital Transformation Excellence

ด้านความปลอดภัยไซเบอร์ (Cybersecurity) มีขึ้นเพื่อป้องกันความเสียหายต่อข้อมูล ระบบเครือข่าย และทรัพย์สินดิจิทัลจากภัยคุกคามรูปแบบต่าง ๆ โดยมุ่งเน้นการเตรียมความพร้อมรับมือเชิงรุก ลดผลกระทบที่จะเกิดขึ้น และสร้างเกราะป้องกันที่มีประสิทธิภาพ ซึ่งในบทเรียนนี้แบ่งเนื้อหาออกเป็น 6 เรื่อง ได้แก่

1. Cyber Security vs. Information Security

Cyber Security เป็นส่วนหนึ่ง (Subset) ของ Information Security โดยการทำ Cyber Security จะมุ่งเน้นไปที่การใช้เทคโนโลยี ฮาร์ดแวร์ และซอฟต์แวร์เพื่อสกัดกั้นภัยคุกคามออนไลน์ ส่วน Information Security จะมองภาพรวมไปถึงนโยบายองค์กร กฎหมาย (เช่น PDPA) และพฤติกรรมของคนด้วย

ความแตกต่างของ Cyber Security vs. Information Security

หัวข้อ	Information Security	Cyber Security
เป้าหมาย	ปกป้องข้อมูลทุกประเภท	ปกป้องระบบและข้อมูลจากภัยคุกคามทางไซเบอร์ (Cyberspace)
ขอบเขต	กว้างกว่า ครอบคลุมทั้งโลกจริงและโลกดิจิทัล	แคบกว่า เน้นเฉพาะระบบที่เชื่อมต่ออินเทอร์เน็ต
รูปแบบข้อมูล	ไฟล์ดิจิทัล, เอกสารกระดาษ, คำพูด	ไฟล์ดิจิทัล, ข้อมูลบนระบบคลาวด์, อุปกรณ์ IoT
องค์ประกอบหลัก	มุ่งรักษา - Confidentiality (การรักษาความลับ) ป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงข้อมูล - Integrity (ความถูกต้องสมบูรณ์ ครบถ้วนของข้อมูล) Availability ความพร้อมใช้งานของข้อมูล	มุ่งป้องกันการโจมตีทางไซเบอร์ - Network Security - Application Security - Cloud Security - Critical Infrastructure

2. Cyber Security Risk Management

Cyber Security Risk Management คือ กระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์ (Cyber Attack) และอาชญากรรมไซเบอร์ (Cybercrime) ที่อาจส่งผลกระทบต่อบุคลากร ระบบสารสนเทศ ข้อมูล และการดำเนินงานขององค์กร

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือสถานการณ์ที่อาจก่อให้เกิดความเสียหายต่อองค์กร โดยพิจารณาจาก 2 ปัจจัยสำคัญ คือ

- **Impact (ผลกระทบ)** : หากเหตุการณ์เกิดขึ้น จะสร้างความเสียหายมากน้อยเพียงใด
- **Likelihood (โอกาสเกิด)** : เหตุการณ์นั้นมีโอกาสเกิดขึ้นบ่อยหรือไม่

ในการวิเคราะห์ความเสี่ยงด้านไซเบอร์ ต้องพิจารณาองค์ประกอบสำคัญ 3 ส่วน ได้แก่

- **Asset (สินทรัพย์)** เช่น ข้อมูล ระบบคอมพิวเตอร์ เครือข่าย บุคลากร
- **Threat (ภัยคุกคาม)** เช่น Malware, Ransomware, Phishing, Hacker
- **Vulnerability (ช่องโหว่)** เช่น ระบบไม่ได้อัปเดตซอฟต์แวร์ ใช้รหัสผ่านอ่อนแอ หรือไม่มีการสำรองข้อมูล

แนวคิดสำคัญของการบริหารความเสี่ยง ประกอบด้วย

- **Risk Identification** : ระบุความเสี่ยง
- **Risk Assessment** : ประเมินระดับความเสี่ยง
- **Risk Control / Mitigation** : กำหนดมาตรการควบคุมหรือลดความเสี่ยง
- **Review & Monitoring** : ติดตามและทบทวนผลการควบคุม

หลังจากประเมินความเสี่ยงแล้ว องค์กรต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ ได้แก่

- **Risk Appetite** : ระดับความเสี่ยงที่องค์กรยินยอมรับเพื่อบรรลุเป้าหมาย
- **Risk Tolerance** : ระดับความเสี่ยงสูงสุดที่องค์กรสามารถยอมรับได้

เป้าหมายของ Cyber Security Risk Management คือ การลดโอกาสเกิดเหตุการณ์ ลดผลกระทบ และทำให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องแม้เกิดเหตุการณ์ทางไซเบอร์

3. Frameworks

Framework คือ กรอบแนวทางหรือมาตรฐานที่ช่วยให้องค์กรสามารถบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงได้อย่างเป็นระบบ มีแนวทางปฏิบัติที่ชัดเจน และสามารถประเมินหรือปรับปรุงการดำเนินงานได้อย่างต่อเนื่อง องค์กรส่วนใหญ่มักนำ Framework มาใช้เป็นแนวทางในการกำหนดนโยบาย กระบวนการ และมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นไปในมาตรฐานเดียวกัน โดย Framework ที่สำคัญ ได้แก่

- COSO : กรอบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)
- ISO 31000 : มาตรฐานการบริหารความเสี่ยง
- ISO 27001 : ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)
- ISO 27005 : แนวทางการบริหารความเสี่ยงด้านสารสนเทศ
- ISO 27032 : แนวทางด้าน Cybersecurity
- COBIT : กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ
- NIST Cybersecurity Framework (CSF) : กรอบการจัดการความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยอมรับทั่วโลก

ในบรรดา Framework ต่าง ๆ NIST Cybersecurity Framework (NIST CSF) ถือเป็น Framework หลักที่ได้รับการยอมรับอย่างแพร่หลาย เนื่องจากเข้าใจง่าย สามารถนำไปประยุกต์ใช้ได้กับทุกประเภทองค์กร และเชื่อมโยงกับมาตรฐานอื่น ๆ ได้เป็นอย่างดี

การเลือกใช้ Framework ที่เหมาะสมจะช่วยให้องค์กรสามารถระบุความเสี่ยง วางมาตรการป้องกัน ตรวจสอบ รับมือ และฟื้นฟูจากเหตุการณ์ด้านไซเบอร์ได้อย่างมีประสิทธิภาพ

4. NIST Cybersecurity Framework

NIST Cybersecurity Framework (NIST CSF) เป็นกรอบการจัดการความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา และได้รับการยอมรับอย่างกว้างขวางทั่วโลก

NIST ใช้แนวคิด Risk-Based Approach หรือการบริหารจัดการตามระดับความเสี่ยง โดยมุ่งเน้นให้องค์กรสามารถระบุ ประเมิน และจัดการความเสี่ยงด้านไซเบอร์ได้อย่างเป็นระบบ

NIST CSF ไม่ได้ลงรายละเอียดเชิงเทคนิคมากนัก แต่ทำหน้าที่เป็น "Roadmap" หรือ "Checklist" เพื่อให้องค์กรทราบว่าควรดำเนินการอะไรบ้าง ส่วนรายละเอียดเชิงลึกสามารถศึกษาเพิ่มเติมจากมาตรฐานหรือแนวปฏิบัติอื่น เช่น ISO 27001 หรือ NIST SP 800 Series

NIST CSF ประกอบด้วย 3 ส่วนหลัก ได้แก่

1.) Framework Core

เป็นหัวใจสำคัญของ Framework ประกอบด้วย 6 Functions

- Govern : กำกับดูแลและบริหารจัดการ
- Identify : ระบุสินทรัพย์และความเสี่ยง
- Protect : ป้องกันภัยคุกคาม

- Detect : ตรวจจับเหตุการณ์ผิดปกติ
- Respond : ตอบสนองเมื่อเกิดเหตุการณ์
- Recover : ฟื้นฟูและกลับสู่สภาวะปกติ

2.) Implementation Tiers

ใช้ประเมินระดับความพร้อมด้าน Cybersecurity ขององค์กร ตั้งแต่ระดับเริ่มต้นไปจนถึงระดับที่มีการบริหารจัดการอย่างเป็นระบบ

3.) Profiles

ใช้เปรียบเทียบสถานะปัจจุบัน (Current Profile) กับสถานะเป้าหมาย (Target Profile) เพื่อวางแผนพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์

จุดเด่นของ NIST CSF คือ มีความยืดหยุ่นสูง เข้าใจง่าย สามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกขนาด และช่วยให้องค์กรบริหารความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพและเป็นมาตรฐานสากล

5. Business Continuity Planning (BCP)

Business Continuity Planning (BCP) คือ การวางแผนล่วงหน้าเพื่อให้องค์กรสามารถดำเนินงานที่สำคัญได้อย่างต่อเนื่อง แม้จะเกิดเหตุการณ์ไม่คาดคิด เช่น Cyber Attack, Ransomware, ไฟฟ้าดับ, ภัยธรรมชาติ หรือเหตุขัดข้องของระบบสารสนเทศ โดยมีเป้าหมายสำคัญคือ Resilience (ความสามารถในการฟื้นตัวและปรับตัวขององค์กร)

BCP ไม่ได้มุ่งเน้นเพียงการป้องกันไม่ให้เกิดเหตุการณ์ แต่เน้นการเตรียมความพร้อมเพื่อให้ผลกระทบต่อธุรกิจน้อยที่สุด และสามารถกลับมาดำเนินงานได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ขึ้น

กระบวนการจัดทำ BCP เริ่มจากการวิเคราะห์ความเสี่ยง (Risk Assessment) และวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อระบุว่าหากเกิดเหตุการณ์ขึ้น ระบบ กระบวนการ หรือบริการใดจะได้รับผลกระทบมากที่สุด จากนั้นจึงกำหนดสถานการณ์จำลอง (Scenario Planning) และจัดทำแผนรองรับล่วงหน้า

โดย BCP เป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ซึ่งเป็นกรอบการบริหารจัดการในระดับองค์กร ประกอบด้วยนโยบาย โครงสร้างการบริหาร บทบาทหน้าที่ของผู้รับผิดชอบ และแนวทางการฟื้นฟูระบบหลังเกิดเหตุการณ์

องค์ประกอบสำคัญของ BCP ได้แก่

- การประเมินความเสี่ยงและผลกระทบทางธุรกิจ
- การกำหนดแผนตอบสนองต่อเหตุการณ์

- การสำรองและกู้คืนข้อมูล (Backup & Recovery)
- การกำหนดผู้รับผิดชอบและช่องทางสื่อสาร
- การซักซ้อมและทดสอบแผนอย่างสม่ำเสมอ

BCP ที่ดีจะช่วยให้องค์กรสามารถรักษาการดำเนินงานที่สำคัญ ลดความเสียหาย และสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียได้อย่างมีประสิทธิภาพ

6. ISO 22301 Business Continuity Management

ISO 22301 เป็นมาตรฐานสากลสำหรับการบริหารความต่อเนื่องทางธุรกิจ หรือ Business Continuity Management System (BCMS) โดยกำหนดข้อกำหนดและแนวทางในการเตรียมความพร้อม รับมือ และฟื้นฟูการดำเนินงานเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อองค์กร

โครงสร้างของ ISO 22301 ประกอบด้วยหัวข้อสำคัญ ได้แก่

- Scope
- Normative References
- Terms and Definitions
- Context of the Organization
- Leadership
- Planning
- Support
- Operation
- Performance Evaluation
- Improvement

หัวใจสำคัญของมาตรฐานอยู่ที่ Operation ซึ่งเป็นส่วนที่เกี่ยวข้องกับการนำไปปฏิบัติจริง โดยแต่ละองค์กรต้องพิจารณาบริบท ความเสี่ยง และลักษณะการดำเนินงานของตนเอง เนื่องจากไม่มีองค์กรใดที่มีความเสี่ยงเหมือนกันทั้งหมด

แนวทางสำคัญของ ISO 22301 ประกอบด้วย

- 1.) พิจารณาความเสี่ยงและกลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategies)
- 2.) ระบุทางเลือกและแนวทางการฟื้นฟูที่เหมาะสม
- 3.) คัดเลือกวิธีการและมาตรการที่เหมาะสมกับองค์กร
- 4.) กำหนดทรัพยากรที่จำเป็นสำหรับการดำเนินการ

นอกจากนี้ มาตรฐานยังให้ความสำคัญกับการปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ เช่น รายชื่อผู้ติดต่อสำคัญ ผังการติดต่อฉุกเฉิน (Call Tree) และแผนการสื่อสารในภาวะวิกฤต อย่างไรก็ตาม ข้อมูลบางประเภท เช่น รายชื่อบุคคล เบอร์โทรศัพท์ สถานที่สำรอง หรือรายละเอียดเชิงปฏิบัติการ ควรได้รับการคุ้มครองตามหลัก Data Protection และไม่ควรเปิดเผยต่อสาธารณะ

ISO 22301 ช่วยให้องค์กรสามารถเตรียมความพร้อมรับมือกับเหตุการณ์ไม่คาดคิด ลดระยะเวลาหยุดชะงักของธุรกิจ และสร้างความเชื่อมั่นให้แก่ลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสีย

7. Wrap Up

การบริหารความมั่นคงปลอดภัยไซเบอร์ไม่ได้เป็นเพียงเรื่องของเทคโนโลยีหรือฝ่าย IT เท่านั้น แต่เป็นกระบวนการบริหารจัดการความเสี่ยงขององค์กรโดยรวม (Cybersecurity Governance) ที่ต้องอาศัยการมีส่วนร่วมของทุกภาคส่วน

Cybersecurity เป็นส่วนหนึ่งของ Information Security ที่มุ่งเน้นการปกป้องข้อมูลและระบบในโลกดิจิทัลจากภัยคุกคามทั้งภายในและภายนอกองค์กร ขณะที่ Information Security ครอบคลุมการปกป้องข้อมูลทั้งในรูปแบบดิจิทัลและกายภาพ หัวใจสำคัญของการบริหารความมั่นคงปลอดภัยไซเบอร์ คือ การระบุความเสี่ยง (Risk Identification) ประเมินผลกระทบและโอกาสเกิด (Risk Assessment) กำหนดมาตรการควบคุม (Risk Treatment) และติดตามทบทวนอย่างต่อเนื่อง โดยอาศัย Framework และมาตรฐานต่าง ๆ เช่น NIST, ISO 27001, ISO 27005 และ ISO 22301 เป็นแนวทาง

เมื่อเกิดเหตุการณ์ทางไซเบอร์ องค์กรต้องมี Business Continuity Planning (BCP) และ Business Continuity Management (BCM) เพื่อให้สามารถดำเนินงานต่อได้และฟื้นตัวได้อย่างรวดเร็ว

ปัจจัยสำคัญสู่ความสำเร็จของ Cybersecurity Governance ประกอบด้วย

- Risk Assessment และ Risk Treatment ที่มีประสิทธิภาพ
- นโยบายและขั้นตอนปฏิบัติ (Policies & Procedures)
- การนำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) มาใช้
- การสร้างความตระหนักรู้และการฝึกอบรมบุคลากร (Training & Awareness)
- การสนับสนุนจากผู้บริหารและหน่วยงานภาครัฐ
- ความร่วมมือกับผู้เชี่ยวชาญและผู้ให้บริการด้าน Cybersecurity

สรุป: เป้าหมายสูงสุดของ Cyber Security Risk Management ไม่ใช่การทำให้ความเสี่ยงหมดไปทั้งหมด แต่คือการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ พร้อมทั้งทำให้องค์กรสามารถป้องกัน รับมือ และฟื้นตัวจากเหตุการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพและยั่งยืน

ประโยชน์ที่ได้รับ

การเรียนรู้เรื่อง **Cyber Security Risk Management** ช่วยให้เข้าใจความแตกต่างระหว่าง Information Security และ Cyber Security รวมถึงตระหนักถึงภัยคุกคามที่อาจส่งผลกระทบต่อข้อมูลและระบบสารสนเทศขององค์กร การเรียนรู้ครั้งนี้ทำให้เข้าใจหลักการบริหารความเสี่ยงด้านไซเบอร์อย่างเป็นระบบ ตลอดจนรู้จัก Framework และมาตรฐานสากลที่ใช้ในการจัดการความมั่นคงปลอดภัยสารสนเทศ

สรุปบทเรียนโดย นางสาวสลิรัตน์ วิชัยพานิช นักวิชาการเกษตรชำนาญการพิเศษ
ศูนย์ปฏิบัติการพัฒนาที่ดินโครงการหลวง 3 สิงหาคม 2569