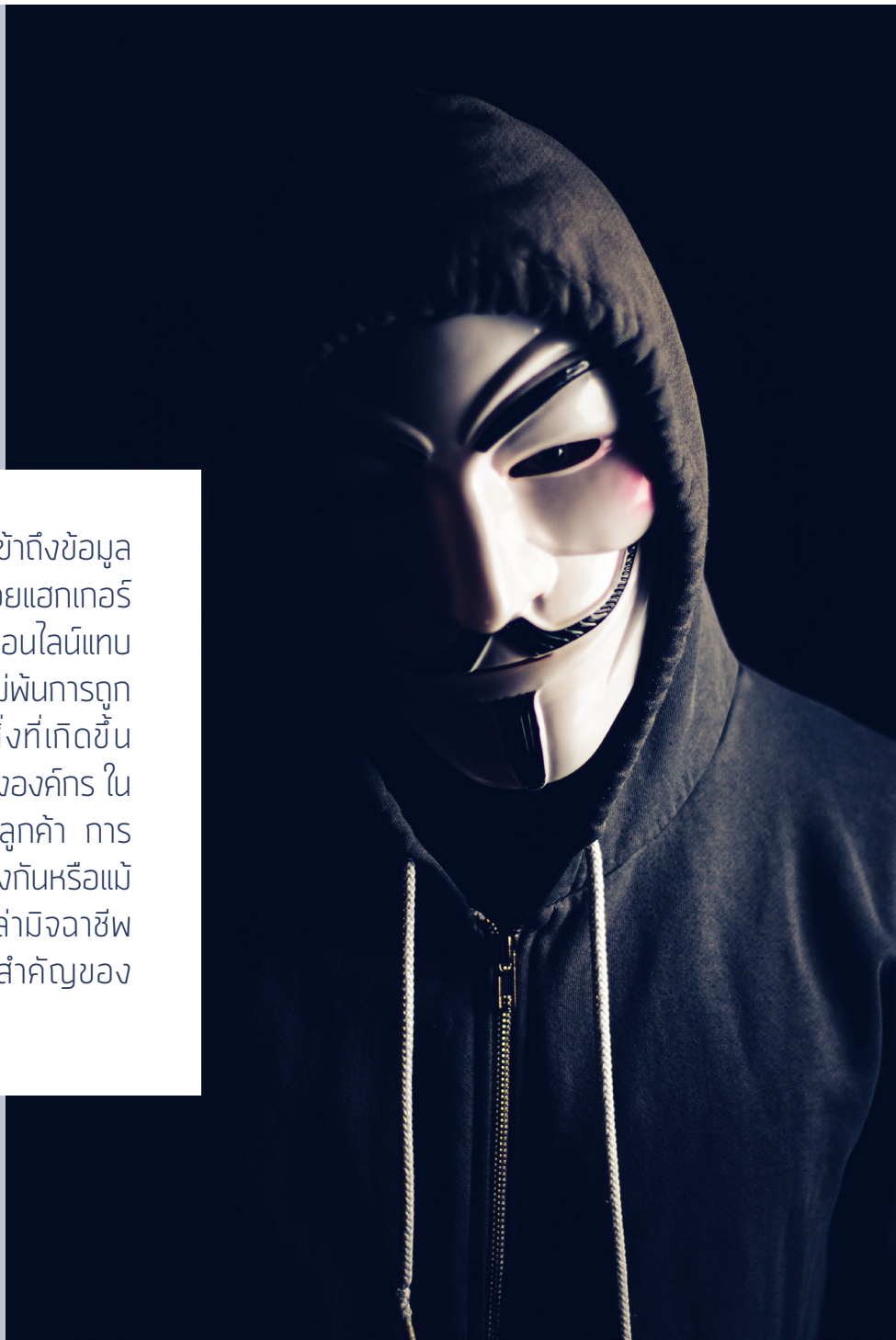
เริ่มต้นกับการรักษาความมั่นคงปลอดภัย สำหรับสารสนเทศ

วิษณุ เรืองวิทยานนท์
สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย
35 หมู่ที่ 3 เทคโนธานี ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี 12120



ปัจจุบันมีการโจรกรรม การเข้าถึงข้อมูลผู้อื่นโดยมิชอบ หรือการถูกโจมตีด้วยแฮกเกอร์ (Hacker) มีมากมายผ่านสื่อสังคมออนไลน์แทบจะทุกวัน แม้แต่ในองค์กรใหญ่ๆ ก็ไม่พ้นการถูกโจมตีหรือถูกโจรกรรมข้อมูล แต่สิ่งที่เกิดขึ้นหลังจากการนั้นคือความน่าเชื่อถือขององค์กร ในการปกป้องรักษาข้อมูลที่สำคัญของลูกค้า การต้องสูญเสียเงินในการจัดทำระบบป้องกันหรือแม้กระทั่งการยินยอมจ่ายเงินให้กับเหล่ามิจฉาชีพต่างๆ เพื่อแลกกับการได้ข้อมูลที่สำคัญของบริษัทกลับมา

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ หรือที่เรียกกันว่า ISO/IEC 27001 ฟังดูเหมือนเป็นเรื่องที่น่าเบื่อและเป็นวิชาการ แต่จริงๆ แล้วมาตรฐานดังกล่าวสร้างมาจากพื้นฐานของการบริหารจัดการ เริ่มจากเรื่องง่ายๆ ว่าเราคือใคร ทำธุรกิจและวัตถุประสงค์อะไร มีใครมาเกี่ยวข้องกับเราบ้าง และเค้าเหล่านั้นคาดหวังหรือสร้างผลกระทบกับองค์กรของเราอย่างไร สิ่งต่างๆ เหล่านี้จะกลายเป็นต้นเรื่องให้เราสร้างวัตถุประสงค์ของระบบมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ เพื่อสนับสนุนให้องค์กรของเราบรรลุวัตถุประสงค์ที่องค์กรตั้งไว้ และตอบสนองต่อผู้มีส่วนได้ส่วนเสีย (ทั้งภายในและภายนอก) ที่มาเกี่ยวข้อง โดยใช้ระบบรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศมาเป็นตัวผลักดันและเน้นที่ สิทธิการเข้าถึงข้อมูล ความถูกต้องของข้อมูล และความพร้อมใช้งาน (Confidentiality, Integrity และ Availability)

ก่อนอื่นเราต้องเริ่มทำความเข้าใจคำว่า Data หรือข้อมูล ในทางด้านคอมพิวเตอร์หมายถึงข้อเท็จจริง ยังคงอยู่ในรูปแบบข้อมูลดิบ แต่เมื่อข้อมูลเหล่านั้นถูกนำมาประมวลผลและสามารถนำไปใช้ประโยชน์ได้เราจะเรียกมันว่าเป็นสารสนเทศ หรือ Information ดังนั้นจะเห็นว่าข้อมูลกับสารสนเทศมีความแตกต่างกัน

เมื่อข้อมูลกลายเป็นสารสนเทศที่มีประโยชน์ต่อองค์กร ดังนั้นมันจึงกลายมาเป็นทรัพย์สินที่มีค่าจึงมีความจำเป็นต้องรักษาสารสนเทศเหล่านี้ให้มั่นคงปลอดภัย แล้วถ้ามีการดำเนินการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศแล้วจะส่งผลอย่างไรกับองค์กร

1. ก่อให้เกิดการปรับปรุงความมั่นคงปลอดภัยสำหรับสารสนเทศในองค์กรจะส่งผลไปถึงลูกค้าขององค์กรให้มีความน่าเชื่อถือตอบสนองต่อความคาดหวังของลูกค้า

2. เพิ่มคุณภาพในกระบวนการบริหารจัดการต่างๆ ในองค์กร

3. ให้พนักงานมีความรู้สึกร่วมให้ความร่วมมือในการดูแลรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ หรือเป็นการสร้างให้พนักงานเกิดความตระหนัก

4. การตรวจสอบ/ตรวจประเมิน เช่น ลูกค้าตรวจองค์กรของเรา หรือองค์กรของเราตรวจผู้จัดจำหน่าย ทำให้ได้มาทั้งความโปร่งใส และความสอดคล้องในธุรกิจ

ประโยชน์ในการจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศสำหรับองค์กร เมื่อเราดำเนินการแล้ว นอกจากจะช่วยลดความเสี่ยงจากภัยคุกคามต่างๆ ในปัจจุบันยังช่วยให้เกิดสิ่งต่างๆ เหล่านี้ในองค์กรตามมา

1. เหตุละเมิดด้านความมั่นคงปลอดภัยลดลง
2. ทำให้พนักงานมั่นใจในการปฏิบัติงานกับองค์กร
3. ชื่อเสียงองค์กรน่าเชื่อถือ
4. ลดต้นทุนด้านเวลาแก้ไขปัญหาต่างๆ ที่อาจเกิดขึ้นในอนาคต
5. สามารถรักษากลุ่มลูกค้าให้อยู่กับองค์กรได้นานขึ้น
6. สร้างจุดแตกต่างระหว่างองค์กรเรากับองค์กรอื่นทำให้องค์กรมีจุดแข็งในการแข่งขันในตลาด

ISO/IEC 27001:2013 เป็นมาตรฐานที่ถูกจัดทำขึ้นมาจากคณะกรรมการ 2 องค์กรร่วมกัน คือ The International for Standardization (ISO) ร่วมกับ The International Electrotechnical Commission (IEC) ทั้งนี้ได้มีการกำหนดมาตรฐานคุณลักษณะสำหรับใช้ในการตรวจประเมินขึ้นมา (27001) พร้อมกับสร้างแนวทางการปฏิบัติ (guideline) สำหรับใช้เป็นแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยขององค์กร (27002)

หลักการที่ใช้สำหรับมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศ มีแนวทางลักษณะเดียวกับ PDCA (Plan, Do, Check และ Action) ซึ่งเป็นวิธีการที่เกี่ยวกับการจัดการคุณภาพและถูกนำมาปรับใช้กับบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้มีการปรับปรุงอย่างต่อเนื่อง ซึ่งโดยปกติแล้วในการบริหารจัดการที่เป็นระบบต้องเริ่มจากการวางแผน (Plan) นำไปปฏิบัติ (Do) การตรวจสอบ (Check) จากนั้นผลของการตรวจสอบจะนำมาซึ่งสิ่งที่ต้องดำเนินการหรือที่เรียกว่า Action (ถ้าผลลัพธ์จากการตรวจสอบพบว่ายังไม่ตรงตามแผนต้องนำกลับไปดำเนินการไม่ว่าจะปรับปรุงแผนหรือเพิ่มเติมกระบวนการเพื่อให้ได้ผลลัพธ์ที่ตรงกับแผนที่วางเอาไว้)

สิ่งสำคัญคือปัจจัยนำเข้าสู่ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศต้องมาจากผู้มีส่วนได้เสีย ซึ่งไม่ได้มีเพียงแค่ลูกค้า แต่ยังมีคนหรือกลุ่มคนต่างๆ อีกมากมาย (ขึ้นอยู่กับแต่ละองค์กร) เช่น มีผู้จัดจำหน่าย (supplier) ที่มาเกี่ยวข้อง หรือ บุคลากรในองค์กรที่มีหลายระดับและเกี่ยวข้องกับการดำเนินธุรกิจขององค์กร บุคลากรเหล่านี้มีความต้องการระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศเป็นอย่างไร ล้วนเป็นปัจจัยนำเข้าที่เริ่มจากวางแผนและเอาไปปฏิบัติดังที่ได้กล่าวไว้ จากนั้นติดตามวัดผล ทบทวน นำไปปฏิบัติ เพื่อบำรุงรักษาระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ระบบจะได้มีการพัฒนาให้ดียิ่งขึ้น (ซึ่งการวนแต่ละรอบของ PDCA เพื่อให้เกิดการพัฒนาและปรับปรุงอย่างต่อเนื่อง) สิ่งที่จะได้รับคือการทำให้องค์กรสามารถส่งผลลัพธ์ออกไปหาผู้ที่สนใจ ผู้ที่สนใจเหล่านี้คือคนที่มีความต้องการหรือมีความคาดหวังในระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ดังนั้นสิ่งที่องค์กรส่งมอบคือระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศที่ตรงตามความต้องการ

จริงๆ แล้วโครงสร้างตามมาตรฐานของระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศเริ่มตั้งแต่ Introduction, Scope, Normative Reference และ Term and Definition แต่สิ่งที่องค์กรต้องดำเนินการจริงจะเริ่มจากข้อกำหนดที่ 4 - 10 ได้แก่

ข้อกำหนดที่ 4 – 7	คือ	Plan
ข้อกำหนดที่ 8	คือ	Do
ข้อกำหนดที่ 9	คือ	Check
ข้อกำหนดที่ 10	คือ	Action

โดยมีรายละเอียดดังนี้

- ข้อกำหนดที่ 4 บริบทองค์กร เหมือนระบบบริหารจัดการอื่นๆ (คล้าย ISO 9001) สาเหตุคือต้องการให้ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศเข้าใจง่าย เนื่องจากบางองค์กรเริ่มนำระบบบริหารจัดการอื่นมาใช้งานก่อน จะทำให้ระบบภายในองค์กรมีความเข้ากันได้ง่ายขึ้น เพราะใช้โครงสร้างแบบเดียวกันเพียงแค่ต้องรู้ว่า ISO/IEC 27001 เน้นลักษณะใด แบ่งออกได้ ดังนี้
    - เข้าใจองค์กร
    - เข้าใจผู้มีส่วนได้เสีย
    - ขอบข่ายของระบบการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

- ข้อกำหนดที่ 5 คือ ภาวะผู้นำมีหลักการสำคัญอยู่ 3 ข้อ ได้แก่ ความมุ่งมั่น นโยบาย และบทบาทหน้าที่ความรับผิดชอบที่มีอยู่ในองค์กร
- ข้อกำหนดที่ 6 คือ การวางแผน มีการนำเอา Risk-based approach มาประยุกต์ใช้เป็นแนวทางบริหารระบบ ใช้สนับสนุนการตัดสินใจโดยพิจารณาอ้างอิงเรื่องความเสี่ยงเป็นหลัก ซึ่ง Risk-based approach ถูกนำมาใช้มากทั้งในระบบบริหารงานทั่วไป และระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ
- ข้อกำหนดที่ 7 คือ การสนับสนุน (support) ประกอบด้วย 5 เรื่อง ได้แก่ การสนับสนุนทรัพยากร การสนับสนุนด้านความสามารถ สนันสนุนด้านความตระหนัก สนับสนุนด้านการสื่อสารและเอกสารสารสนเทศ (document information)
- ข้อกำหนดที่ 8 คือ การปฏิบัติและการควบคุม (operation) ในข้อนี้จะหมายถึง Do มีหลักการอยู่ 3 ข้อ ได้แก่ การวางแผนการควบคุมการปฏิบัติงาน การประเมินความเสี่ยงด้านระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ การจัดการหรือการบรรเทาความเสี่ยง (risk Treatment)
- ข้อกำหนดที่ 9 คือ การตรวจสอบ (check) เพื่อดูประสิทธิภาพประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศว่าเป็นอย่างไรเช่นการวัดผลติดตามวิเคราะห์ประเมินผล (monitoring, measurement, analysis and evaluation)
- ข้อกำหนดที่ 10 คือการปรับปรุงอย่างต่อเนื่อง (improvement) ประกอบด้วย 2 ข้อหลัก คือ กรณีมีความไม่สอดคล้องจากการตรวจสอบ ต้องทำการดำเนินการแก้ไข (corrective action) และดำเนินการปรับปรุงอย่างต่อเนื่อง

จากที่ได้กล่าวไปถึงเรื่องของการโจรกรรม การเข้าถึงข้อมูลผู้อื่นโดยมิชอบ หรือการถูกโจมตีด้วยแฮกเกอร์ (Hacker) ถึงแม้ปัจจุบันเราจะไม่สามารถป้องกันได้ทั้งหมด แต่การจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศก็นับได้ว่าประโยชน์เป็นอย่างยิ่งในการทำให้องค์กรเริ่มมีการสำรวจตนเอง ตั้งแต่ความคาดหวังของผู้มีส่วนได้เสีย กฎหมาย กฎระเบียบที่เกี่ยวข้อง รวมถึงการพิจารณาเรื่องต่างๆ ที่สามารถหยิบยกขึ้นมาเพื่อให้องค์กรทำความเข้าใจปัจจัยที่กระทบกับองค์กร วัฒนธรรมในองค์กร ประเภทการดำเนินงานขององค์กร เช่น หน่วยงานรัฐหรือบริษัทเอกชน สิ่งเหล่านี้จะถูกนำมาวิเคราะห์ว่ามีผลกระทบต่อระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างไร และองค์กรคาดหวังสิ่งใดจากระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศนี้นอกจากนี้การจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศยังมุ่งเน้นให้องค์กรต้องกลับมาพิจารณากระบวนการปฏิบัติงานรวมถึงโครงสร้างองค์กร เพื่อนำมากำหนดเป็นขอบข่ายของระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรต่อไป

เอกสารอ้างอิง

สถาบันมาตรฐานอังกฤษ (British Standards Institution หรือ BSI), 2013. บทความ ISO/IEC 27001. [ออนไลน์]. เข้าถึงได้จาก: https://www.bsigroup.com/th-TH/ISOIEC-27001-Information-Security/article-27001/, [เข้าถึงเมื่อ 26 ธันวาคม 2563].

Perry Johnson Registrars, INC., 2018. ISO 27001. [ออนไลน์]. เข้าถึงได้จาก: http://www.pjrthailand.com/standards/iso-27001, [เข้าถึงเมื่อ 26 ธันวาคม 2563]

TURCERT, 2005. ประโยชน์ของระบบการจัดการความปลอดภัยของข้อมูล ISO 27001. [ออนไลน์]. เข้าถึงได้จาก: https://www.turcert.com/th/belgelendirme/sistem-belgelendirme/iso-27001-bilgi-guvenligi-yonetim-sistemi/iso-27001-bilgi-guvenligi-yonetim-sistemi-faydalari-nelerdir, [เข้าถึงเมื่อ 26 ธันวาคม 2563].