หัวข้อเรื่อง 1. การบริหารความมั่นคงปลอดภัยสารสนเทศ

บรรยายโดย อาจารย์ปริญญา หอมอเนก

ประธานและผู้ก่อตั้ง, ACIS Professional Center Co., Ltd. (ACIS)

2. การบริหารความเสี่ยงด้านไอซีที (ICT Risk Management)

บรรยายโดย อาจารย์เมธา สุวรรณสาร

Audit Chair – ISACA

วันพุธที่ 14 มกราคม 2558 ณ ห้องประชุม Kamolmart ชั้น 6 โรงแรม เดอะสุโกศล กรุงเทพฯ

<u>สรุปสาระสำคัญไว้</u> ดังนี้

1. การบริหารความมั่นคงปลอดภัยสารสนเทศฯ โดยอาจารย์ ปริญญา หอมอเนก ประธานและผู้ก่อตั้ง, ACIS Professional Center Co., Ltd. (ACIS) ได้กล่าวไว้ดังนี้ “ในปัจจุบันและอนาคต หน่วยงานของรัฐและองค์กรต่าง ๆ จำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง ซึ่งการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) หรือด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) นั้นไม่เพียงพอ ไม่ว่าจะเป็น Application Security, Network Security, Internet Security, Information Security หากแต่ต้องเป็น “Cybersecurity” ในภาพรวม พร้อมทั้งการป้องกันโครงสร้างพื้นฐานสำคัญตามแนวทาง CIIP (Critical Information Infrastructure Protection) ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบสารสนเทศ จากมาตรฐาน ISO/IEC 27032:2012: Guideline for cybersecurity โดยรวมถึงการจัดการเพื่อรองรับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Resilience) ในการรับมือกับภัยคุกคามความมั่นคงปลอดภัยที่ไม่อาจคาดคิด ที่ไม่แน่นอน ที่ไม่สามารถคาดการณ์ได้ และที่ไม่รู้ (unknown, unpredictable, uncertain, unexpected) ถึงเวลาแล้วที่หน่วยงานของรัฐและองค์กรทุกองค์กร โดยเฉพาะอย่างยิ่งองค์กรในกลุ่มโครงสร้างพื้นฐานสำคัญ ซึ่งความมั่นคงปลอดภัยของระบบควบคุมอุตสาหกรรม (ICS) สำหรับระบบโครงสร้างพื้นฐานสำคัญขององค์กร มีผลกระทบทางกายภาพโดยตรงต่อสังคมและโลก รวมทั้งความเสี่ยงที่อาจเกิดขึ้นต่อสุขภาพและความปลอดภัยของประชาชนและผลกระทบต่อสิ่งแวดล้อม ผู้บริหารหน่วยงานของรัฐและองค์กรทุกองค์กรจำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ ซึ่งต้องมาจากวิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงขององค์กร (Top Management’s Vision and Leadership) ที่ต้องให้เตรียมพร้อมรับมือ ดังคำที่ว่า “ป้องกันไว้ก่อน ดีกว่ามาแก้กันทีหลัง” ด้วยการมองหาแนวทางและโอกาสในการปรับปรุง (Opportunities for improvement: OFI) โดยการดำเนินการป้องกันไว้ก่อนในรูปแบบลักษณะเกราะกันภัย จากกรอบการดำเนินงานที่นำมาปฏิบัติใช้งานได้อย่างจริงจังและต่อเนื่อง ไม่ใช่มีเกราะกันภัยแต่ปล่อยไว้ไม่ใช้งานหรือใช้บ้างไม่ใช้บ้าง หรืออาจต้องมาตามแก้ไขจากภัยคุกคามและความเสี่ยงที่เกิดขึ้น ทั้งที่รู้และไม่รู้ (Known and Unknown Threats/Risk) โดยควรคำนึงถึง Zero Day Attack อยู่เสมอ เพราะการป้องกันที่ดี ย่อมทำให้พร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสมทันท่วงที แต่หากไม่มีการป้องกันที่ดี รอเหตุการณ์เกิดขึ้นก็อาจจะยากที่รับมือหรือ

แก้ไขได้ เมื่อถึงตอนนั้น ภัยคุกคามก็อาจจะเป็นความเสี่ยงที่ยากต่อการบริหารจัดการ เป็นความเสี่ยงที่กระทบต่อความอยู่รอดขององค์กรในระยะยาวและยากที่จะดำเนินธุรกิจแบบยั่งยืนได้ในที่สุด

2. การบริหารความเสี่ยงในด้าน ไอซีที ICT Risk Management โดยท่าน อาจารย์เมธา สุวรรณสาร Audit Chair – ISACA (Information Security Audit and Control Association) Bangkok Chapter ได้แบ่งเป็น หัวข้อไว้ดังนี้

2.1 การกำหนดขอบเขตของการดำเนินการจัดทำความเสี่ยงของหน่วยงานและองค์กร โดยในแต่ละหน่วยงานจะต้องกำหนดขอบเขตของการจัดทำแผนความเสี่ยงทางด้าน ICT โดยใช้ทรัพย์สินเป็นการกำหนดส่วนงานที่ต้องบริหารจัดการ กำหนดวิสัยทัศน์ ภารกิจ ค่านิยม วัตถุประสงค์ นโยบาย เป้าหมาย หลักธรรมาภิบาล พันธกิจมุ้งเน้นการป้องกันทั้งระยะยาวและระยะสั้นขององค์กร ซึ่งต้องมีความสอดคล้องกันระหว่าง พันธกิจของ IT และพันธกิจขององค์กร เป็นต้น

2.2 การกำหนดบทบาทและหน้าที่หลัก โดยในแต่ละหน่วยงานจะต้องมีการกำหนดแผนการดำเนินการที่ชัดเจน เป้าหมาย ระยะเวลา ผู้รับผิดชอบ จุดมุ่งหมาย Mind stone เพื่อให้รู้ สถานะของการปฏิบัติงาน การแบ่งงานหรือมอบหมายงานที่ชัดเจน โดยมีการกำหนด นโยบาย คำสั่ง ระเบียบ กติกา เงื่อนไขและความเข้าใจที่แท้จริงในการปฏิบัติงาน โดยมีเป้าหมายของการสื่อสารดังนี้ ความเข้าใจ > นำไปปฏิบัติ >การประเมินผล > การสั่งการ >การเฝ้าติดตาม >ความเสี่ยง ภายใต้แผนการดำเนินการขององค์กร

2.3 การวิเคราะห์ความเสี่ยง โดยการจัดทำตามแผนโดยวิเคราะห์ความเสี่ยงจากสินทรัพย์ที่องค์กรครอบครองอยู่ โดยตรวจสอบสถานะความเสี่ยงที่เป็นอยู่ ว่ามีความเสี่ยงใดบ้างจัดทำแผนโดยมีตัวกำหนดระดับความเสี่ยงที่ชัดเจน โอกาสการเกิด ความรุนแรง มูลค่าความเสียหายทั้ง เชิงปริมาณและเชิงคุณภาพ โดยความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT RISK) ประกอบด้วย ความเสี่ยงในการบริหารงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านการปฏิบัติการ การรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ของข้อมูล ความพร้อมในการใช้งาน ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านการปฏิบัติตามกฎหมาย

2.4 ลำดับความสำคัญของความเสี่ยง โดยทำการจัดเรียงว่าความเสี่ยงที่เกิดขึ้น สิ่งใดส่งผลรุนแรงต่อองค์กรมากที่สุดเพื่อ จัดทำแผนในการรับมือ ถ่ายโอน ความเสี่ยง ที่ชัดเจน แนวทางการปฏิบัติกำหนดนโยบาย บทลงโทษที่ชัดเจนในการบริหารจัดการความเสี่ยงโดยมี 8 ขั้นตอน 1. สภาพแวดล้อมในองค์กร ๒.กำหนดเป้าหมาย ๓.ระบุเหตุการณ์ 4. ประเมินความเสี่ยง ๕.การตอบสนองความเสี่ยง 6.การควบคุม 7.ระบบสารสนเทศและการติดต่อสื่อสาร ๘.การติดตามและประเมินผล

2.5 การตรวจสอบและควบคุม โดยการจัดทำความเสี่ยง ในองค์กรนั้นมาสารถมีความเสี่ยงเกิดขึ้นได้เรื่อยๆและมีจากหลายปัจจัย การตรวจสอบความเสี่ยงอยู่เสมอไม่ว่าจะเป็นจากภายในและภายก็จะต้องมีการกำหนดแผนที่ชัดเจนในการตรวจสอบ รวมไปถึงการควบคุมในกรณีที่เกิดความเสี่ยง เพื่อให้เกิดความเสียหายต่อองค์กรมาก โดยจะต้องมีกระบวนในการเก็บข้อมูลความเสี่ยงที่เกิดขึ้นเพื่อเป็นแหล่งความรู้ขององค์กร ในการวางแผนรองรับโอกาสที่อาจจะเกิดขึ้นซ้ำในครั้งต่อๆไป