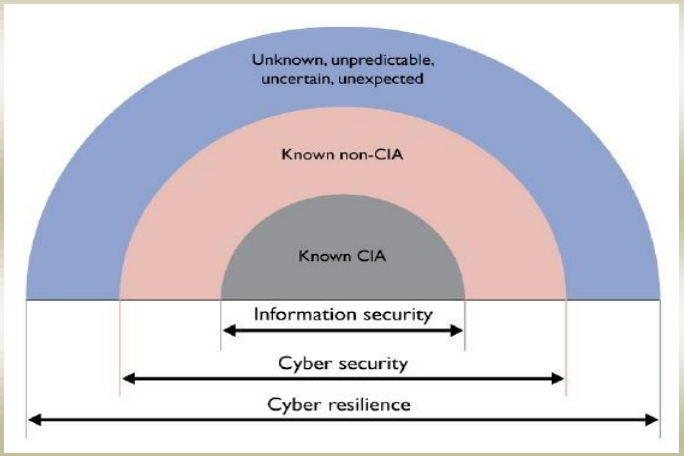
จาก Cybersecurity ไปสู่ Cyber Resilience

จากความแพร่หลายของการใช้อินเตอร์เน็ตในการทำธุรกรรมต่างๆ ทางธุรกิจ ไม่ว่าจะเป็นการทำธุรกรรมระหว่างองค์กรด้วยกัน หรือการทำธุรกรรมของผู้บริโภค มีผลทำให้เกิดอาชญากรรมในโลกไซเบอร์ในรูปแบบต่างๆ ตามมามากมาย ไม่ว่าจะเป็นการโจมตีเว็บไซต์เพื่อให้บริการหยุดชะงัก การขโมยข้อมูลที่มีความสำคัญ และการเรียกค่าไถ่ระบบ

ความพยายามขององค์กรต่างๆ ที่จะปกป้องข้อมูล ระบบงาน และความต่อเนื่องของการดำเนินธุรกิจ จำเป็นต้องขยายขอบเขตในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของตน (Information security) ให้ครอบคลุมถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) อย่างไรก็ดี ด้วยความก้าวหน้าของเทคโนโลยีที่เป็นไปอย่างรวดเร็ว ทำให้การคาดคะเนถึงความเสี่ยงที่อาจเกิดขึ้นและรูปแบบของการโจมตีทางไซเบอร์ที่เกิดขึ้นใหม่เป็นไปได้ยาก มีผลทำให้แผนในการบริหารความเสี่ยงนั้น ไม่สามารถลดความเสี่ยงและความเสียหายได้อย่างมีประสิทธิภาพ แนวคิดของ Cyber Resilience จึงเกิดขึ้น เพื่อให้องค์กรต่างๆ สามารถรับมือกับการโจมตีทางไซเบอร์ที่คาดไม่ถึงเหล่านี้

ความทนทานต่อการถูกโจมตีทางไซเบอร์หรือ "Cyber Resilience" คืออะไร?



นอกเหนือจากการรักษาความมั่นคงปลอดภัยของสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์แล้ว Cyber Resilience เน้นถึงความสามารถในการรับมือกับภัยคุกคามจากการโจมตีทางไซเบอร์ที่คาดไม่ถึง ช่วยให้องค์กรสามารถอยู่รอดจากการโจมตี โดยได้รับความเสียหายและมีช่วงเวลาของการหยุดชะงักของระบบน้อยที่สุด สามารถฟื้นฟูหรือกู้คืนความเสียหายกลับมาให้ได้อย่างรวดเร็วที่สุด

การให้ความสำคัญต่อ Cyber Resilience

ในช่วงสองปีที่ผ่านมา (พ.ศ. 2558-2559) มีการยกระดับมาตรฐานและกฎระเบียบของหน่วยงานกำกับดูแลสถาบันการเงินในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ทั่วโลก โดยหนึ่งในสิบของแนวโน้มด้านความมั่นคงปลอดภัยทางไซเบอร์ในปี 2561 ที่หน่วยงานกำกับดูแลสถาบันการเงิน ตลาดทุน ธุรกิจหลักทรัพย์ ธุรกิจจัดการลงทุน ธุรกิจสัญญาซื้อขายล่วงหน้า และธุรกิจประกันภัย ทั้งในและต่างประเทศ ล้วนแต่ให้ความสำคัญในเรื่อง "Cybersecurity" เป็นประเด็นสำคัญ ไม่ว่าจะเป็น Monetary Authority of Singapore (MAS) ของสิงคโปร์, Hong Kong Monetary Authority (HKMA) ของฮ่องกง โดยเน้นให้มีการพัฒนาจาก "Information Security State" มาเป็น "Cybersecurity State" และเข้าสู่สภาวะ "Cyber Resilience" ในที่สุด

ประโยชน์ที่จะได้รับจากการสัมมนาในครั้งนี้

องค์กรทั่วโลกจำเป็นต้องปรับตัวเพื่อรองรับ Digital Transformation/Digital Disruption ซึ่งจะต้องมีการเปลี่ยนผ่านจาก Information Security State เข้าสู่ Cybersecurity State ก่อนที่จะต่อยอดในการสร้างความทนทานต่อการถูกโจมตีทางไซเบอร์ให้กับองค์กร โดยจะต้องศึกษารายละเอียดของ NIST Cybersecurity Framework ให้เข้าใจอย่างถ่องแท้ และนำ NIST Cybersecurity Framework ไปดำเนินการวิเคราะห์ช่องว่างในองค์กร เพื่อให้เห็นสิ่งที่เป็นอยู่ในปัจจุบัน ("AS-IS") และสิ่งที่ต้องการจะเป็น ("TO-BE") ตลอดจนระบุระดับวุฒิภาวะ (Maturity Level) ในปัจจุบันและระดับที่ต้องการขององค์กร โดยเป็นที่คาดหมายว่า หน่วยงานกำกับดูแลสถาบันการเงินในประเทศไทยจะมีการประกาศข้อกำหนดเหล่านี้ในรูปแบบของกรอบการประเมินความพร้อมด้าน Cyber Resilience ในเวลาอีกไม่นานนี้ ทั้งนี้เพื่อสนับสนุนส่งเสริมนโยบายการเข้าสู่ Thailand 4.0

ผู้ควรเข้าร่วมหลักสูตรนี้ประกอบด้วย

- ผู้บริหารด้านเทคโนโลยีสารสนเทศ
- ผู้ตรวจสอบ ผู้บริหารงานตรวจสอบ และกรรมการในคณะกรรมการตรวจสอบ
- ผู้บริหารด้านความเสี่ยง ผู้บริหารด้านความเสี่ยงทางไซเบอร์
- ผู้บริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (CISO,CSO)
- ผู้เชี่ยวชาญด้านการบริหารจัดการความเสี่ยงทางไซเบอร์
- อาจารย์และนักวิชาการ

หัวข้อการสัมมนา

- BACK TO THE BASIC : "Security" and "Resilience"
- From Information Security to Cybersecurity, From Cybersecurity to Cyber Resilience
- Understand Cyber Kill Chain
- Why Cyber Resilience?
- Foundation of Cyber Resiliency
- Understand NIST Cybersecurity Framework
- Understand Threat Models, Threat information and Frameworks
- Understand Cyber Resiliency Engineering Framework
- Understand Cyber Resiliency Design Principle
- Understand Cyber Resilience Review (CRR)

CPE ที่ได้รับ : 6 หน่วย

วันที่จัดสัมมนา 12 ธันวาคม 2560 (1 วัน)
สถานที่ โรงแรมอะริสตั้น สุขุมวิท 24
วิทยากร : อ. ปริญญา หอมเอนก, CISSP, CISA, CISM, CRISC, CGEIT, SSCP, CSSLP, CSX

ค่าสัมมนา (รวมภาษีมูลค่าเพิ่ม 7% แล้ว)

ผู้สมัครเข้าร่วมสัมมนา	อัตราค่าธรรมเนียม
สมาชิกของ ISACA	4,280.-
สมาชิก ITSMF, IIAT และกลุ่มบุคคลจากองค์กรเดียวกัน ตั้งแต่ 3 คนขึ้นไป	4,815.-
บุคคลทั่วไป	5,350.-

(สมาคมได้รับการยกเว้นไม่ต้องถูกหักภาษี ณ ที่จ่ายตามคำสั่งกรมสรรพากรที่ ท.ป. 4/2528 ข้อ 12/1)

การลงทะเบียน:
ลงทะเบียนออนไลน์ ที่ http://www.isaca-bangkok.org/EVENT
วิธีการชำระค่าสัมมนา:
โอนเข้าบัญชีเงินฝากออมทรัพย์ ธนาคารไทยพาณิชย์จำกัด (มหาชน)
สาขาเซ็นทรัลเวิลด์ หมายเลข 247-231087-1
ชื่อบัญชี: สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพ
หลังจากชำระเงินกรุณาอีเมล์หลักฐานการโอนเงิน (Pay-in Slip) ไปยัง
conference@isaca-bangkok.org
หมายเหตุ: สมาคมฯ ไม่มีนโยบายรับชำระค่าอบรมภายในวันหรือภายหลังการสัมมนา

ติดต่อสอบถามข้อมูลได้ที่ คุณประทักษ์ วงศ์สินคงมั่น โทรศัพท์หมายเลข 081-840-5835

แผนที่สถานที่จัดสัมมนา