ISACA
Bangkok Chapter

Cyber Resilience

& Incident Response

ความทนทานต่อการโจมตี และ

การรับมือภัยคุกคามทางไซเบอร์

วันที่ 22 – 23 สิงหาคม 2567 ณ โรงแรมแมนดาริน สามย่าน

จาก Cybersecurity ไปสู่ Cyber Resilience

จากความแพร่หลายของการใช้อินเตอร์เน็ตในการทำธุรกรรมต่าง ๆ ทางธุรกิจ ไม่ว่าจะเป็นการทำธุรกรรมระหว่างองค์กรด้วยกัน หรือการทำธุรกรรมของผู้บริโภค มีผลทำให้เกิดอาชญากรรมในโลกไซเบอร์ในรูปแบบต่าง ๆ ตามมามากมาย ไม่ว่าจะเป็นการโจมตีเว็บไซต์เพื่อให้บริการหยุดชะงัก การขโมยข้อมูลที่มีความสำคัญ และการเรียกค่าไถ่ระบบ ความพยายามขององค์กรต่าง ๆ ที่จะปกป้อง ข้อมูล ระบบงาน และความต่อเนื่องของการดำเนินธุรกิจ จำเป็นต้องขยายขอบเขตในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของตน (Information security) ให้ครอบคลุมถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) อย่างไรก็ดี ด้วยความก้าวหน้าของเทคโนโลยีที่เป็นไปอย่างรวดเร็ว ทำให้การคาดคะเนถึงความเสี่ยงที่อาจเกิดขึ้น และรูปแบบของการโจมตีทางไซเบอร์ที่เกิดขึ้นใหม่นี้ เป็นไปได้ยาก ระบบออนไลน์ไม่มีความปลอดภัย 100% ต้องพร้อมรับมือเสมอกับภัยที่จะเกิดขึ้นเมื่อใดก็ตาม มีผลทำให้แผนในการบริหารความเสี่ยงนั้นไม่สามารถลดความเสี่ยงและความเสียหายได้อย่างมีประสิทธิภาพ ดังนั้นแนวทางการบริหารจัดการความทนทานต่อการโจมตี และ การรับมือภัยคุกคามทางไซเบอร์ (**Cyber Resilience & Incident Response)** จึงเกิดขึ้น เพื่อให้องค์กรต่าง ๆ สามารถรับมือกับการโจมตีทางไซเบอร์ที่คาดไม่ถึงเหล่านี้

ความทนทานต่อการโจมตีทางไซเบอร์ (Cyber Resilience) คืออะไร?

นอกเหนือจากการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) แล้ว แนวคิด Cyber Resilience เน้นถึงความสามารถในการรับมือกับภัยคุกคามจากการโจมตีทางไซเบอร์ที่คาดไม่ถึง ช่วยให้องค์กรสามารถอยู่รอดจากการโจมตี โดยได้รับความเสียหายและมีช่วงเวลาของการหยุดชะงักของระบบน้อยที่สุด สามารถฟื้นฟู หรือกู้คืนความเสียหายกลับมาให้ได้อย่างรวดเร็วที่สุด

"Cyber Resilience" จึงหมายถึง ความสามารถในการเตรียมตัวและการปรับตัวต่อการเปลี่ยนแปลงและความทนทานต่อการบุกรุก โจมตี รวมถึงความสามารถในการคืนสภาพของระบบ

ประโยชน์ที่จะได้รับจากการสัมมนาในครั้งนี้

องค์กรทั่วโลกจำเป็นต้องปรับตัวเพื่อรองรับ Digital Transformation/Digital Disruption ซึ่งจะต้องมีการเปลี่ยนผ่านจาก Information Security State เข้าสู่ Cybersecurity State ก่อนที่จะต่อยอดในการสร้างความทนทานต่อการถูกโจมตีทางไซเบอร์ให้กับองค์กร โดยจะต้องศึกษารายละเอียดของ CISA CRR (Cyber Resilience Review) ให้เข้าใจอย่างถ่องแท้ และนำ Cyber Resilience Suite Platform ไปดำเนินการวิเคราะห์ช่องว่างในองค์กร (Self Assessment) เพื่อให้เห็นความเสี่ยงที่เป็นอยู่ ในปัจจุบัน ("AS-IS") และสิ่งที่ต้องการจะเป็น ("TO-BE") ตลอดจนระบุระดับวุฒิภาวะ (Maturity Level) ในปัจจุบันและระดับที่ต้องการขององค์กร

ผู้ควรเข้าร่วมในหลักสูตรนี้ ประกอบด้วย

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

หัวข้อเนื้อหาหลักสูตร

1. **What is Cyber Resilience? Why Cyber Resilience?**

   What is difference between Cybersecurity and Cyber Resilience
2. **From Information Security to Cybersecurity,**

   From Cybersecurity to Cyber Resilience
3. **Understand Cyber Kill Chain & MITRE ATT&CK**
4. **How to assess Cyber Risk using CISA CRR (Cyber Resilience Review)**
5. **Understand WEF Cyber Resilience Framework and Cyber Resilience Index**
6. **Understand Cyber Resilience Suite Platform**
7. **Understand Cyber Resiliency Engineering Framework (CREF)**
8. **What is Incident Response ? Why is Incident Response important?**
9. **Understand NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide**
10. **How to implement Cyber Resilience in your organization using Cyber Resilience Suite Platform**

CPE ที่ได้รับ : 12 หน่วย

ค่าธรรมเนียมในการเข้าสัมมนา

ผู้ร่วมสัมมนา	ค่าธรรมเนียม
• สำหรับสมาชิก ISACA	10,700 บาท
• สำหรับสมาชิกของสมาคมที่มีความร่วมมือกับทาง ISACA และองค์กรที่สมัครเป็นกลุ่มตั้งแต่ 3 คนขึ้นไป	11,770 บาท
• สำหรับบุคคลทั่วไป	12,840 บาท

ค่าธรรมเนียมข้างต้นรวมภาษีมูลค่าเพิ่ม 7% แล้ว

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

การสมัครเข้าอบรมและชำระค่าธรรมเนียม

ผู้สมัครจะต้องลงทะเบียนออนไลน์ทาง **www.isaca-bangkok.org/event** และทำรายการโอนเงินเพื่อชำระค่าธรรมเนียมผ่านทางบัญชีธนาคาร โดยโอนเข้าบัญชีเงินฝากออมทรัพย์ ธนาคารไทยพาณิชย์จำกัด (มหาชน) สาขาเซ็นทรัลเวิลด์ หมายเลข 247-231087-1 ชื่อบัญชี: สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ - ภาคพื้นกรุงเทพฯ หลังจากชำระเงินกรุณาแจ้งการชำระเงินและส่งหลักฐานการโอนเงิน (Pay-in Slip) ไปที่เว็บไซต์

http://www.isaca-bangkok.org/payment ทั้งนี้ ผู้สมัครจะต้องโอนเงินก่อนวันที่ **13 ส.ค. 2567**

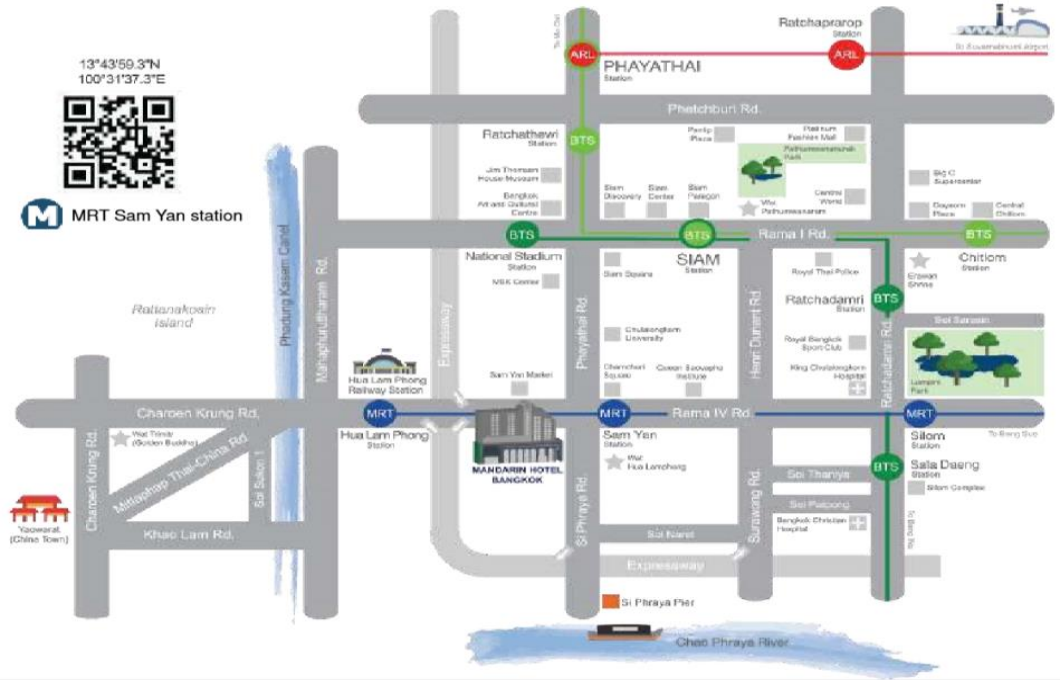
จำนวนเงินค่าสัมมนาที่ชำระจะต้องเป็นจำนวนเงินตามที่ระบุไว้ข้างต้น โดยไม่มีการหักค่าธรรมเนียมการโอนเงินของธนาคารหรือค่าธรรมเนียมอื่นใด ทั้งนี้สมาคมฯ ไม่มีนโยบายรับและชำระเงินในวันสัมมนาหรือภายหลังการสัมมนา

เนื่องจากการสัมมนาในครั้งนี้ **จำกัดจำนวนที่ 20 ท่าน** หากมีผู้สมัครเข้ามามากกว่าจำนวนที่รับได้ จะให้สิทธิ์ผู้ที่ส่งหลักฐานการชำระเงินเข้ามาก่อน

ติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่ คุณประทักษ์ วงศ์สินคงมั่น

โทรศัพท์หมายเลข 089-777-0900 Email: training@isaca-bangkok.org

แผนที่โรงแรม (โรงแรมแมนดาริน สามย่าน)



ของสมนาคุณกรณีพิเศษ

เพื่อเป็นการตอบแทนสำหรับท่านที่ได้ชำระค่าอบรมสำหรับหลักสูตรนี้ ในวันแรกที่เปิดหลักสูตร จะได้รับเสื้อยืดโปโลของสมาคมฯ เป็นกรณีพิเศษท่านละ 1 ตัว โดยสมาคมฯ ขอสงวนสิทธิ์ในการแจกให้ตามขนาดของเสื้อที่สมาคมฯ มีอยู่จำนวนจำกัด