การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์
THAILAND'S NATIONAL CYBER EXERCISE 2022

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์

THAILAND'S NATIONAL CYBER EXERCISE 2022

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์

THAILAND'S NATIONAL CYBER EXERCISE 2022

พิมพ์ครั้งที่ ๑ กุมภาพันธ์ ๒๕๖๕

จำนวนพิมพ์ ๓๐๐ เล่ม

เจ้าของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

พิมพ์ที่

บริษัท ทริปเพิ้ล กรุ๊ป จำกัด www.triple-group.co.th

สารบัญ

เรื่อง	หน้า
บทที่ ๑ บทนำ	**๙**
๑.๑ ความเป็นมา	๑๐
๑.๒ วัตถุประสงค์การฝึก	๑๑
๑.๓ ประเด็นการฝึก	๑๑
๑.๔ รูปแบบการฝึก	๑๑
๑.๕ แนวคิดการจัดการฝึกตาม MITRE Cyber Exercise Playbook	๑๒
๑.๖ โครงสร้างการจัดการฝึก	๑๓
๑.๗ ผลลัพธ์ที่คาดหวัง	๑๔
บทที่ ๒ การประชุมวางแผนและพัฒนาโจทย์ฝึก	**๑๕**
๒.๑ การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference: CDC)	๑๗
๒.๒ การประชุมวางแผนขั้นต้น (Initial Planning Conference: IPC)	๓๐
๒.๓ การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC)	๓๓
๒.๔ การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)	๓๗
บทที่ ๓ การฝึกเตรียมการ	**๕๙**
๓.๑ วัตถุประสงค์การฝึกเตรียมการ	๖๐
๓.๒ สถานที่การฝึกเตรียมการ	๖๐
๓.๓ ผู้เข้าร่วมการฝึกเตรียมการ	๖๐
๓.๔ หัวข้อการฝึกเตรียมการ	๖๑
๓.๕ ผลของการฝึกเตรียมการ	๗๕
๓.๖ ความคิดเห็นและข้อเสนอแนะจากผู้ที่เข้ารับการฝึกเตรียมการ	๗๖
บทที่ ๔ การดำเนินการฝึก และผลการฝึก	**๗๙**
๔.๑ วัตถุประสงค์	๘๐
๔.๒ วันและเวลา	๘๐
๔.๓ สถานที่ฝึก	๘๐
๔.๔ ผู้เข้าร่วมการฝึก	๘๑
๔.๕ สาระสำคัญของการฝึก	๘๑
๔.๖ ผลการฝึก	๘๔
๔.๗ การตรวจเยี่ยมการฝึก	๑๐๔

สารบัญ (ต่อ)

เรื่อง	หน้า
บทที่ ๕ การสรุปบทเรียนจากการฝึก	**๑๑๑**
๕.๑ แนวทางการสรุปบทเรียนจากการฝึก	๑๑๒
๕.๒ ผลการสรุปบทเรียน จากผู้เข้ารับการฝึก	๑๑๔
๕.๓ ผลการสรุปบทเรียน จากส่วนควบคุมการฝึก	๑๑๘
๕.๔ ผลการสรุปบทเรียน จาก Co-Agent	๑๑๙
๕.๕ ผลการสรุปบทเรียน จากส่วนประเมินผลการฝึก	๑๒๐
ภาคผนวก	**๑๒๕**
ผนวก ก กฎหมายที่เกี่ยวข้อง	**๑๒๖**
ผนวก ข นิยามศัพท์ และบัญชีคำย่อ	**๑๒๗**
ข ๑ นิยามศัพท์	๑๒๗
ข ๒ บัญชีคำย่อ	๑๒๘
ผนวก ค รายชื่อคณะทำงาน	**๑๓๐**
ผนวก ง รายชื่อผู้ที่เข้าร่วมการฝึก	**๑๓๑**
ง ๑ รายชื่อหน่วยงานที่เข้าร่วมการฝึก	๑๓๑
ง ๒ รายชื่อผู้แทนหน่วยงานที่เข้าร่วมการประชุมวางแผนการฝึก	๑๓๔
ง ๓ รายชื่อผู้ทำหน้าที่ในส่วนควบคุมการฝึกและส่วนประเมินผล	๑๔๐
ง ๔ รายชื่อผู้เข้ารับการฝึก	๑๔๖

สารบัญภาพ

รูปที่	หน้า
รูปที่ ๑-๑ โครงสร้างการจัดการฝึก	๑๓
รูปที่ ๒-๑ การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference : CDC)	๑๗
รูปที่ ๒-๒ ร่างโครงสร้างการฝึก	๒๖
รูปที่ ๒-๓ การประชุมวางแผนขั้นต้น (Initial Planning Conference: IPC)	๓๐
รูปที่ ๒-๔ การการประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC)	๓๓
รูปที่ ๒-๕ การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)	๓๗
รูปที่ ๒-๖ ข้อตกลงเรื่องการแลกเปลี่ยนข้อมูล (Traffic Light Protocol : TLP)	๓๙
รูปที่ ๒-๗ โครงสร้างของส่วนควบคุมการฝึก	๓๙
รูปที่ ๒-๘ กิจกรรมสร้างความคุ้นเคย	๔๒
รูปที่ ๒-๙ กิจกรรมทบทวนหลักการที่สำคัญ	๔๓
รูปที่ ๒-๑๐ ผลการกำหนดประเภทโจทย์ฝึก	๔๔
รูปที่ ๒-๑๑ ผลการกำหนดลักษณะการโจมตีและผลกระทบ	๔๕
รูปที่ ๒-๑๒ ตารางประสานสอดคล้อง (MSEL Sync Table)	๔๕
รูปที่ ๒-๑๓ การจัดทำสถานการณ์และโจทย์ฝึก (เพิ่มเติม)	๔๖
รูปที่ ๒-๑๔ กิจกรรมการกำหนดผลกระทบข้ามหน่วยงาน	๔๗
รูปที่ ๒-๑๕ วิธีการสื่อสารและการส่งโจทย์ฝึก (Inject)	๔๗
รูปที่ ๒-๑๖ ผลกระทบข้าม Sector	๔๘
รูปที่ ๒-๑๗ รายการโจทย์ฝึก (MSEL Sync Table)	๔๘
รูปที่ ๒-๑๘ ตาราง MSEL log	๕๐
รูปที่ ๒-๑๙ คาบการปล่อยโจทย์ฝึก	๕๑
รูปที่ ๒-๒๐ การทดสอบก่อนการฝึก (Dry Run)	๕๑
รูปที่ ๒-๒๑ การประชุมส่วนประเมินผล (Exercise Evaluation Group : EEG)	๕๔
รูปที่ ๒-๒๒ การจัดทำแบบประเมิน	๕๕
รูปที่ ๒-๒๓ การประชุมส่วนประเมินผล (เพิ่มเติม)	๕๖
รูปที่ ๒-๒๔ แบบประเมิน (Checklist)	๕๗
รูปที่ ๒-๒๕ การตรวจสอบแบบประเมินกับทีม ECG	๕๘

สารบัญภาพ (ต่อ)

รูปที่		หน้า
รูปที่ ๓-๑	หัวข้อการฝึกเตรียมการ	๖๑
รูปที่ ๓-๒	การอบรม World Class Cyber Security Practices by MITRE/CISA/SEI	๖๑
รูปที่ ๓-๓	การอบรม บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	๖๔
รูปที่ ๓-๔	การอบรม บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan)	๖๖
รูปที่ ๓-๕	การอบรม ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	๖๘
รูปที่ ๓-๖	การอบรม การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan)	๗๐
รูปที่ ๓-๗	การอบรม Incident Response Fundamental	๗๒
รูปที่ ๓-๘	การอบรม วิธีการใช้งานเครื่องมือสนับสนุนการฝึก	๗๔
รูปที่ ๔-๑	การตรวจเยี่ยม ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร	๑๐๔
รูปที่ ๔-๒	การตรวจเยี่ยมในรูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์	๑๐๗
รูปที่ ๕-๑	กำหนดการและลำดับการนำเสนอ	๑๑๒
รูปที่ ๕-๒	ผลการสรุปบทเรียน จากผู้เข้ารับการฝึก	๑๑๔
รูปที่ ๕-๓	ผลการสรุปบทเรียน จากส่วนควบคุมการฝึก	๑๑๘
รูปที่ ๕-๔	ผลการสรุปบทเรียน จาก Co-Agent	๑๑๙
รูปที่ ๕-๕	ผลการสรุปบทเรียน จากส่วนประเมินผล	๑๒๐

สารบัญตาราง

ตารางที่	หน้า
ตารางที่ ๒-๑ ร่างกำหนดการฝึก	๒๑
ตารางที่ ๒-๒ ร่างบทบาทหน้าที่	๒๘
ตารางที่ ๒-๓ หน่วยงานที่จะเชิญเข้าร่วมการฝึก	๒๙
ตารางที่ ๒-๔ ตารางจำนวนผู้แทนหน่วยงานเข้าร่วมเป็นส่วนควบคุมการฝึก (ECG)	๕๓
ตารางที่ ๔-๑ กำหนดการฝึก	๘๑
ตารางที่ ๔-๒ กำหนดการตรวจเยี่ยม	๑๐๙
ตารางที่ ๕-๑ กำหนดการและลำดับการนำเสนอ	๑๑๓

บทที่ ๑
บทนำ

บทที่ ๑
บทนำ

๑.๑ ความเป็นมา

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้เมื่อวันที่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๒ มาตรา ๒๒ (๑๓) กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ และมาตรา ๕๖ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) หรือ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่ สกมช. จัดขึ้น

นอกจากนี้ ตามประกาศ เรื่อง นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ - ๒๕๖๕) ข้อ ๓.๗.๔ การพัฒนาระบบการเตรียมพร้อมแห่งชาติ รองรับนโยบายที่ ๑๓ : พัฒนาระบบการเตรียมพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงของชาติ ได้มีการกำหนดตัวชี้วัดที่ ๒ ระดับความสำเร็จในการบูรณาการการฝึกการบริหารวิกฤตการณ์ ทั้งภายในประเทศและระหว่างประเทศเพื่อรับมือภัยคุกคามทุกรูปแบบ โดยนโยบายดังกล่าวข้างต้นมีความสอดคล้องกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ ในประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์ แนวทางการดำเนินการ ๒.๖ ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือกับสถานการณ์ทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ ตลอดจนสถิติการตรวจพบภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างมีนัยสำคัญ

เพื่อเป็นการเตรียมความพร้อมให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อโครงสร้างพื้นฐานสำคัญ

ทางสารสนเทศ ซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ สกมช. จึงได้จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ ๒๕๖๕ (Thailand's National Cyber Exercise 2022) ขึ้น

๑.๒ วัตถุประสงค์การฝึก

เพื่อให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๓ ประเด็นการฝึก

การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ จนอาจส่งผลกระทบรุนแรงเป็นวงกว้าง ทำให้การทำงานหรือบริการต่าง ๆ ล้มเหลวทั้งระบบ รัฐไม่สามารถควบคุมการทำงานจากส่วนกลางได้ และยังลุกลามไปยังโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่น ๆ ของประเทศ จนมีผลทำให้บุคคลจำนวนมากเสียชีวิตอีกด้วย นอกจากนี้ ยังพบว่ามีความเป็นไปได้ที่จะมีการโจมตีทางไซเบอร์ต่อระบบไฟฟ้าของประเทศ รวมถึงการโจมตีโรงพยาบาลโดยใช้มัลแวร์เรียกค่าไถ่ (Ransomware) ร่วมด้วย

๑.๔ รูปแบบการฝึก

ใช้รูปแบบการฝึกซ้อมแผนบนโต๊ะ (Table Top Exercise) โดยมีขั้นตอนการดำเนินการตามแนวคิดของ MITRE Cyber Exercise Playbook[๑] สรุปได้ดังนี้

๑.๔.๑ ขั้นตอนที่ ๑ การประชุมวางแผนและพัฒนาโจทย์ฝึก (Exercise Planning and Scenario/Inject Development) รายละเอียดตามบทที่ ๒

๑.๔.๒ ขั้นตอนที่ ๒ การฝึกเตรียมการ (Pre-exercise) รายละเอียดตามบทที่ ๓

๑.๔.๓ ขั้นตอนที่ ๓ การดำเนินการฝึก (Exercise Execution) และผลการฝึก รายละเอียดตามบทที่ ๔

๑.๔.๔ ขั้นตอนที่ ๔ การสรุปบทเรียนจากการฝึก (After Action Review : AAR) รายละเอียดตามบทที่ ๕

[๑] https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook

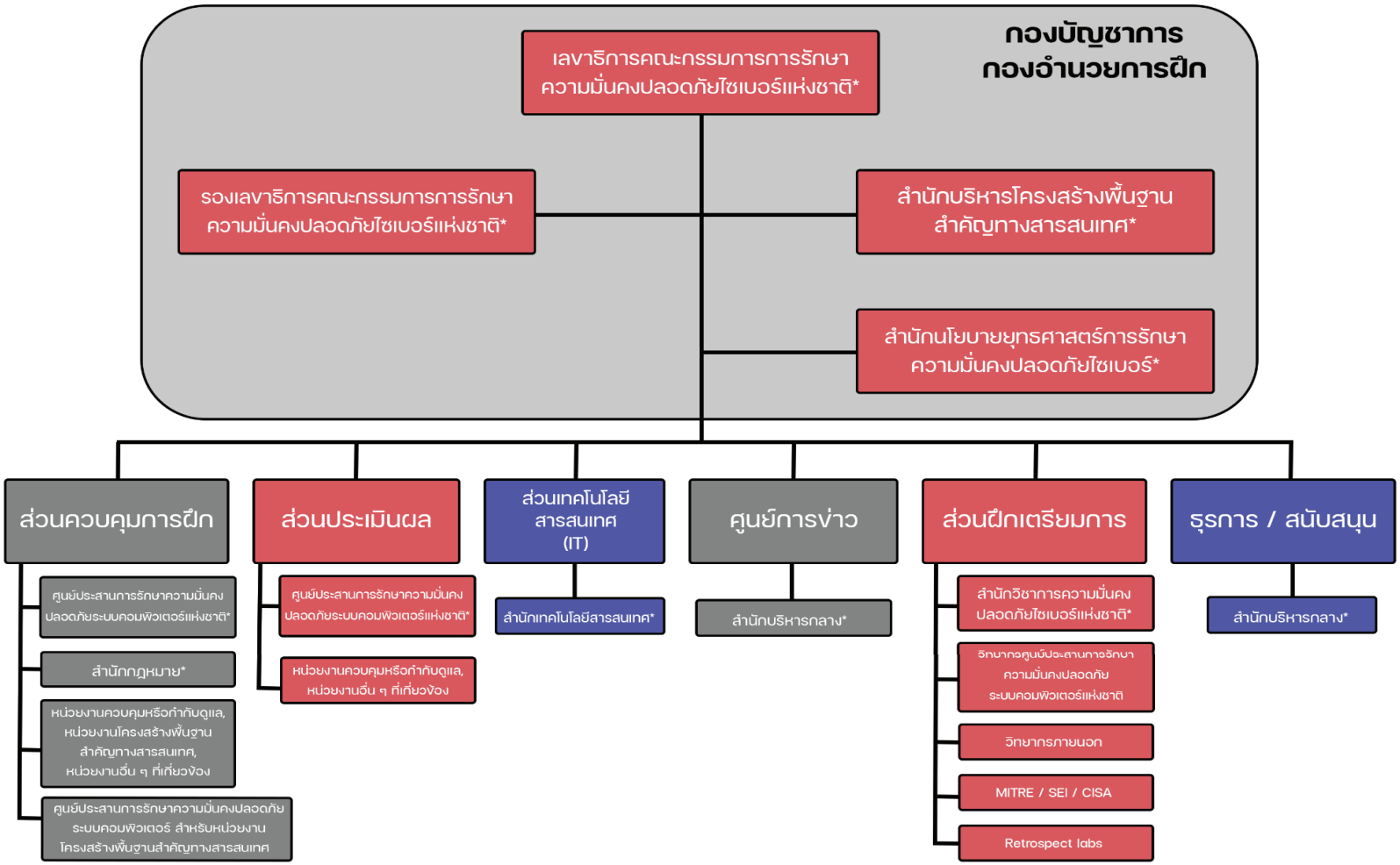
๑.๕ แนวคิดการจัดการฝึกตาม MITRE Cyber Exercise Playbook

MITRE เป็นองค์กรไม่แสวงหาผลกำไรของสหรัฐอเมริกา มีศูนย์วิจัยและพัฒนาซึ่งได้รับการสนับสนุนจากหน่วยงานของรัฐ เพื่อให้สนับสนุนงานทางด้านการบิน การป้องกันประเทศ สาธารณสุข ความมั่นคงแห่งมาตุภูมิ และความมั่นคงปลอดภัยไซเบอร์ มานานกว่า ๔๐ ปี

ทั้งนี้ MITRE มีโครงการด้านความมั่นคงปลอดภัยไซเบอร์จำนวนมากที่ได้รับการยอมรับจากทั่วโลก อาทิ MITRE ATT&CK framework, The Structured Threat Information Exchange (STIX), the Common Vulnerabilities and Exposures (CVE), the Common Weakness Enumeration (CWE) เป็นต้น

ในด้านการฝึกทางไซเบอร์ MITRE เป็นหนึ่งในหน่วยงานที่เข้าไปสนับสนุนงานค้นคว้าวิจัยเชิงเทคนิคให้กับหน่วยงานของสหรัฐอเมริกา และได้ออกเป็นเอกสารเผยแพร่ฉบับนี้ตั้งแต่ปี ค.ศ. ๒๐๑๔ ให้กับหน่วยงานอื่น ๆ นำไปใช้ประโยชน์ได้ โดยเนื้อหาเป็นการนำเสนอแนวคิดการจัดการฝึกทางไซเบอร์ ประกอบด้วย นิยามศัพท์ (Terminology) ขั้นตอนการจัดการฝึกทางไซเบอร์ (Life Cycle of a Cyber Exercise) แนวทางในการวางแผนการฝึก (Exercise Planning) และแนวทางในการดำเนินการฝึก (Execution) โดยครอบคลุมหลักการสำคัญ ประกอบด้วย การกำหนดวัตถุประสงค์การฝึก (Objectives) สถานการณ์ฝึก (Scenarios) การรายงานและประเมินผลการฝึก (Reporting and Assessment Procedures) สถาปัตยกรรมเครือข่าย (Network Architecture) เครื่องมือสนับสนุนการฝึก (Tools) รวมถึงการสรุปบทเรียนจากการฝึก (Lessons Learned) เป็นต้น

๑.๖ โครงสร้างการจัดการฝึก



*หน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รูปที่ ๑-๑ โครงสร้างการจัดการฝึก

๑.๗ ผลลัพธ์ที่คาดหวัง

๑.๗.๑ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้องมีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๗.๒ (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ (The National Cyber Incident Response Plan of Thailand (Draft))

๑.๗.๓ การจัดการฝึกมีความสอดคล้องกับการฝึกการบริหารวิกฤตการณ์ระดับชาติ (National Crisis Management Exercise : C-MEX 21)

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งจะนำไปสู่ความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ รวมถึงโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

บทที่ ๒
การประชุมวางแผนและพัฒนาโจทย์ฝึก

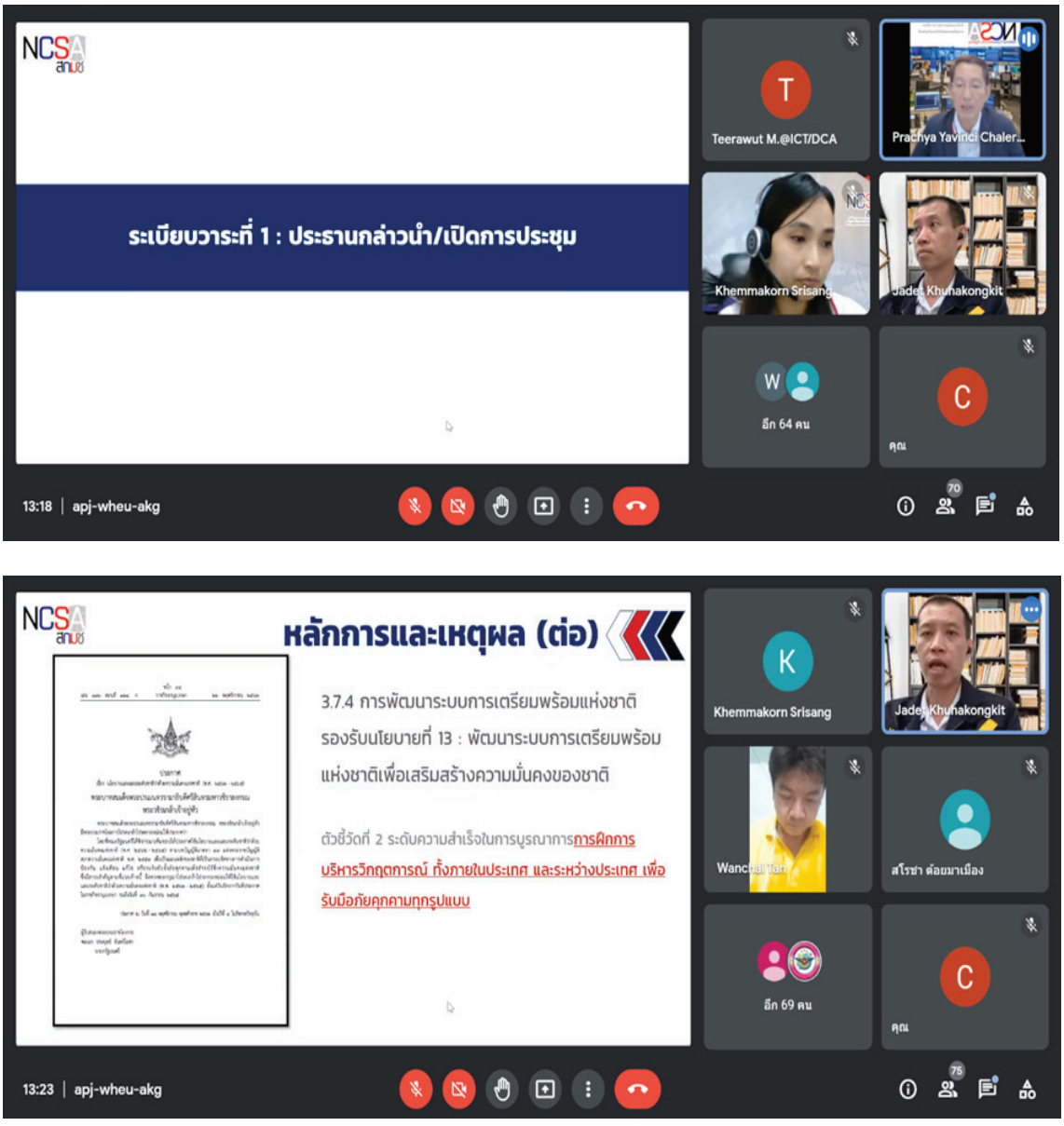
บทที่ ๒
การประชุมวางแผนและพัฒนาโจทย์ฝึก

การวางแผนการฝึก (Exercise Planning) เป็นกระบวนการในการกำหนดผู้เข้าร่วมการฝึก (Participants) สถานการณ์ฝึก (Exercise Scenario) โจทย์ฝึก (Injects) และลำดับการดำเนินการฝึก (Execution Order) กล่าวคือ การเลือกวิธีการที่ดีที่สุดเพื่อให้บรรลุวัตถุประสงค์เหล่านั้น และพัฒนาแผนการฝึกที่สมบูรณ์ ซึ่งเรียกว่า รายการโจทย์ฝึก (Master Scenario Event List : MSEL) โดยรายการโจทย์ฝึกนี้จะทำหน้าที่เป็นลำดับขั้นตอนสำหรับการดำเนินการฝึก (Exercise Execution) โดยสรุปจะประกอบด้วย ลำดับของโจทย์ฝึก (Ordering of Injects) เวลาในการดำเนินการ (Time of Execution) รวมไปถึงผลลัพธ์ที่คาดหวังจากผู้เข้ารับการฝึก โดยกลุ่มผู้วางแผนการฝึกที่จะต้องมุ่งเน้นการดำเนินการให้เป็นไปตามวัตถุประสงค์การฝึก (Expected Reactions from The Training Audience)[๒]

ในการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ได้กำหนดกิจกรรมการประชุมวางแผนการฝึกไว้จำนวนทั้งสิ้น ๔ กิจกรรม คือ (๑) การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference : CDC) (๒) การประชุมวางแผนขั้นต้น (Initial Planning Conference : IPC) (๓) การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development) และ (๔) การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference : FPC) โดยมีรายละเอียด ดังนี้

[๒] Exercise Planning, MITRE Cyber Exercise Playbook

๒.๑ การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference : CDC)



รูปที่ ๒-๑ การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference : CDC)

๒.๑.๑ วัตถุประสงค์การประชุม

เพื่อให้ผู้แทนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ร่วมแสดงความคิดเห็นเพื่อพัฒนาแนวคิดการฝึก

๒.๑.๒ วันและเวลาการประชุม

วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ - ๑๖.๐๐ น.

๒.๑.๓ สถานที่การประชุม

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๒.๑.๔ ผู้เข้าร่วมการประชุม

๒.๑.๔.๑ ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล ๑๗ หน่วยงาน

๒.๑.๔.๒ ผู้แทนจากหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ๑๐ หน่วยงาน

รวมจำนวนทั้งสิ้น ๖๓ คน

๒.๑.๕ สาระสำคัญของการประชุม

๒.๑.๕.๑ หลักการและเหตุผล

(๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้เมื่อวันที่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๒ มาตรา ๒๒ (๑๓) กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ และมาตรา ๕๖ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) หรือ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่ สกมช. จัดขึ้น

(๒) ประกาศ เรื่อง นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ - ๒๕๖๕) ข้อ ๓.๗.๔ การพัฒนาระบบการเตรียมพร้อมแห่งชาติ รองรับนโยบายที่ ๑๓ : พัฒนาระบบการเตรียมพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงของชาติ ได้มีการกำหนดตัวชี้วัดที่ ๒ ระดับความสำเร็จในการบูรณาการการฝึกการบริหารวิกฤตการณ์ ทั้งภายในประเทศและระหว่างประเทศ เพื่อรับมือภัยคุกคามทุกรูปแบบ

(๓) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ ในประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์ แนวทางการดำเนินการ ๒.๖ ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือกับสถานการณ์ทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ

(๔) สถิติการตรวจพบภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างมีนัยสำคัญ

๒.๑.๕.๒ ร่างวัตถุประสงค์การฝึก และผลลัพธ์ที่คาดหวัง

(๑) วัตถุประสงค์การฝึก

เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๒) ผลลัพธ์ที่คาดหวัง

(๒.๑) หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๒.๒) (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ (The National Cyber Incident Response Plan of Thailand (Draft))

(๒.๒) การจัดการฝึกมีความสอดคล้องกับการฝึกการบริหารวิกฤตการณ์ระดับชาติ (National Crisis Management Exercise : C-MEX 21)

๒.๑.๕.๓ ร่างกำหนดการฝึก

วันที่	กิจกรรม	ผลผลิตที่สำคัญ
๑ ตุลาคม พ.ศ. ๒๕๖๔	การประชุมพัฒนาแนวคิดการฝึก (Concept Development Conference : CDC)	(๑) วัตถุประสงค์การฝึก และผลลัพธ์ที่คาดหวัง (๒) สถานการณ์ฝึก รูปแบบการฝึก (๓) ร่างโครงสร้างการฝึก (๔) ร่างรายชื่อหน่วยงานและจำนวนคนที่จะเข้าร่วมการฝึก (๕) ร่างกำหนดการฝึก
๑๒ ตุลาคม พ.ศ. ๒๕๖๔	การประชุมวางแผนขั้นต้น (Initial Planning Conference : IPC)	(๑) วัตถุประสงค์การฝึก และผลลัพธ์ที่คาดหวัง (๒) สถานการณ์ฝึก รูปแบบการฝึก (๓) ร่างประเภทของโจทย์ฝึก (๔) ร่างหัวข้อสำหรับการฝึกเตรียมการ (๕) ร่างกำหนดการฝึก (๖) ร่างโครงสร้างการฝึก (๗) ร่างรายชื่อผู้ติดต่อประสานหน่วยงานที่จะเข้ารับการฝึก (๘) ร่างรายชื่อหน่วยงานและจำนวนคนที่จะเข้าร่วมการฝึก
๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔	การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)	(๑) สถานการณ์ฝึกทั่วไป รูปแบบการฝึก และผลลัพธ์ที่คาดหวัง (๒) สถานการณ์ฝึกเฉพาะ (๓) โจทย์หรือประเภทของโจทย์ฝึก และผลลัพธ์ที่คาดหวัง (๔) หัวข้อสำหรับการฝึกเตรียมการ

วันที่	กิจกรรม	ผลผลิตที่สำคัญ
๑ พฤศจิกายน พ.ศ. ๒๕๖๔	การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference : FPC)	(๑) วัตถุประสงค์การฝึก (๒) สถานการณ์ฝึกทั่วไป รูปแบบการฝึก และผลลัพธ์ที่คาดหวัง (๓) สถานการณ์ฝึกเฉพาะ (๔) โจทย์หรือประเภทของโจทย์ฝึก และผลลัพธ์ที่คาดหวัง (๕) หัวข้อสำหรับการฝึกเตรียมการ (๖) กำหนดการฝึก (๗) โครงสร้างการฝึก (๘) รายชื่อผู้ติดต่อประสานหน่วยงานที่จะเข้ารับการฝึก (๙) รายชื่อหน่วยงานและจำนวนคนที่จะเข้าร่วมการฝึก (๑๐) บทบาทและความรับผิดชอบ
๘ พฤศจิกายน - ๑๕ ธันวาคม พ.ศ. ๒๕๖๔	การฝึกเตรียมการ (Pre-exercise)	(๑) จัดการฝึกเตรียมการ (๒) ประเมินผล
๒๒ - ๒๔ ธันวาคม พ.ศ. ๒๕๖๔	การดำเนินการฝึก (Exercise Execution)	(๑) ทดสอบระบบฝึก (๒๐ - ๒๑ ธันวาคม พ.ศ. ๒๕๖๔) (๒) จัดการฝึกซ้อมแผนบนโต๊ะ (๒๒ - ๒๔ ธันวาคม พ.ศ. ๒๕๖๔) (๓) รับคณะตรวจเยี่ยม (๔) ประเมินผล (๕) ใบประกาศนียบัตร

ตารางที่ ๒-๑ ร่างกำหนดการฝึก

๒.๑.๕.๔ ร่างสถานการณ์ฝึก

(๑) สถานการณ์ฝึกทั่วไป (C-MEX 21)

ประเทศไทยได้รับเลือกให้เป็นเจ้าภาพจัดการประชุมความร่วมมือทางเศรษฐกิจเอเชีย - แปซิฟิก (Asia-Pacific Economic Cooperation : APEC) ซึ่งมีกำหนดจัดขึ้นในปี พ.ศ. ๒๕๖๕ โดยจะมีผู้แทนจากประเทศสมาชิกต่าง ๆ เข้าร่วมการประชุมที่เกี่ยวข้องทั้งในระดับรัฐมนตรี เจ้าหน้าที่อาวุโส คณะกรรมการ และคณะทำงานในพื้นที่ที่เป็นจุดยุทธศาสตร์สำคัญทางเศรษฐกิจและอุตสาหกรรมของประเทศ อาทิ กรุงเทพมหานคร จังหวัดชลบุรี และจังหวัดภูเก็ต เพื่อหารือการขับเคลื่อนเศรษฐกิจผ่านแนวคิดเศรษฐกิจชีวภาพ เศรษฐกิจหมุนเวียน และเศรษฐกิจสีเขียว (Bio-Circular-Green Economy) ที่สอดคล้องกับบริบทโลกในช่วงการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID - 19)

ตลอดทั้งปี พ.ศ. ๒๕๖๔ ประเทศไทยสามารถรับมือกับการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID - 19) ได้เป็นอย่างดี โดยประชาชนภายในประเทศบางส่วนได้รับการฉีดวัคซีนและมีภูมิคุ้มกันจากโรคดังกล่าว อย่างไรก็ตาม ข้อมูลจากหน่วยงานด้านสาธารณสุขเปิดเผยว่ายังคงพบการแพร่ระบาดภายในประเทศ แต่เพื่อการขับเคลื่อนเศรษฐกิจของประเทศ ตั้งแต่เดือนมกราคม พ.ศ. ๒๕๖๕ เป็นต้นมา รัฐบาลจึงตัดสินใจผ่อนคลายการเดินทางเข้ามาในราชอาณาจักรทั้งทางบก ทางน้ำ และทางอากาศ สำหรับนักธุรกิจและนักท่องเที่ยวที่ประสงค์เดินทางเข้ามาในพื้นที่ที่ทางราชการกำหนด เพื่อกระตุ้นเศรษฐกิจการท่องเที่ยวและส่งเสริมให้เกิดการลงทุนภายในประเทศ

ห้วงเดือนมีนาคม พ.ศ. ๒๕๖๕ หน่วยงานฝ่ายความมั่นคงได้รับการแจ้งเตือนจากหน่วยงานด้านการข่าว เพื่อให้มีการแจ้งเตือนหน่วยงานที่เกี่ยวข้องในการเฝ้าระวังการลักลอบขนส่งอาวุธที่มีอานุภาพทำลายล้างสูง ระบบเครื่องส่ง และวัสดุอุปกรณ์ ต่อมาสำนักงานศุลกากรแหลมฉบัง ได้รายงานไปยังสถานีตำรวจภูธรแหลมฉบัง สำนักงานปรมาณูเพื่อสันติ และหน่วยงานฝ่ายความมั่นคงที่เกี่ยวข้องว่ามีกลุ่มบุคคลได้ลักลอบขนวัสดุกัมมันตรังสีซีเซียม – ๑๓๗ ระบบเครื่องส่ง และวัสดุอุปกรณ์ ผ่านทางท่าเรือแหลมฉบัง จังหวัดชลบุรี โดยผู้ลักลอบได้ทำร้ายร่างกายเจ้าหน้าที่และหลบหนีในขณะที่เจ้าหน้าที่กำลังตรวจสอบสถานการณ์ดังกล่าว ได้พบว่ามีการแผ่รังสีของซีเซียม – ๑๓๗ จากเครื่อง RPM และพบว่ามีการใช้ใบอนุญาตปลอมนำเข้าหรือส่งออกวัสดุกัมมันตรังสีวัสดุนิวเคลียร์ ซึ่งสำนักงานศุลกากรแหลมฉบัง ห่วงกังวลว่าจะมีการนำไปใช้ประกอบวัตถุระเบิด Dirty Bomb ทั้งนี้ เจ้าหน้าที่ตำรวจได้รับแจ้งเบาะแสว่าหนึ่งในบุคคลต้องสงสัยชื่อนาย A เป็นเจ้าของโรงงานอุตสาหกรรมในนิคมอุตสาหกรรม X จังหวัดชลบุรี ซึ่งได้รับแนวความคิดความรุนแรงของกลุ่มก่อการร้ายในภูมิภาคตะวันออกกลางผ่านทางดาร์กเว็บ (Dark Web) แห่งหนึ่ง โดยมักมีพฤติกรรมชอบใช้ความรุนแรงกับลูกจ้างอยู่เป็นประจำ ซึ่งสาเหตุที่ลงมือก่อเหตุคาดว่าน่าจะมาจากความไม่พอใจที่ไม่ได้รับการช่วยเหลือเยียวยาจากรัฐบาลอันเป็นเหตุให้โรงงานของตน

ประสบปัญหาขาดทุนอย่างหนักและจำเป็นต้องปิดตัวลง ทั้งนี้ คาดว่าหลบหนีไปยังโกดังร้างแห่งหนึ่งในกรุงเทพมหานคร

ห้วงเดือนพฤษภาคม พ.ศ. ๒๕๖๕ สถานีตำรวจภูธรเมืองชลบุรีได้รับแจ้งจากประชาชนว่ามีชายคุ้มคลั่งคล้ายคนเสพยาเสพติดไล่กราดยิงประชาชนในห้างสรรพสินค้าชื่อดังในพื้นที่จังหวัดชลบุรี โดยได้จับประชาชนและเจ้าหน้าที่รักษาความปลอดภัยของห้างสรรพสินค้าไว้เป็นตัวประกัน ส่งผลให้เจ้าหน้าที่ตำรวจต้องเร่งปิดล้อมพื้นที่และระดมบุคลากรที่เกี่ยวข้องเพื่อเจรจาเกลี้ยกล่อมแต่ไม่สำเร็จ จึงจำเป็นต้องวิสามัญชายดังกล่าว โดยสืบทราบภายหลังว่าผู้กระทำความผิดชื่อนาย B เป็นอดีตพนักงานโรงงานของ นาย A โดยมีอาการเครียดสะสมเนื่องจากถูกนาย A ทำร้ายร่างกายอยู่บ่อยครั้งและเพิ่งถูกไล่ออกจากงาน รวมทั้งไม่ได้รับการช่วยเหลือเยียวยาจากรัฐบาลในโครงการ “เราชนะ” เฟสสอง สำหรับผู้ที่ได้รับผลกระทบจากโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID – 19) ที่เปิดให้มีการลงทะเบียนในช่วงเดือนเมษายน พ.ศ. ๒๕๖๕ ทั้งนี้ สำนักข่าวหลายสำนักต่างรายงานข่าวทั้งในขณะที่นาย B กำลังลงมือก่อเหตุและภายหลังการเสียชีวิต ทำให้ข่าวดังกล่าวกำลังเป็นที่สนใจของประชาชนทั่วประเทศ

ในเวลาต่อมา หน่วยงานด้านข่าวกรองได้ตรวจพบร่องรอยการเคลื่อนไหวของกลุ่มนาย A บนสื่อสังคมออนไลน์ที่เป็นที่นิยม โดยได้มีการใช้ถ้อยคำรุนแรงด่าทอการทำงานของรัฐบาลในการแก้ไขปัญหาการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID – 19) พร้อมทั้งเชิญชวนให้ผู้ที่ไม่ได้รับความเป็นธรรมจากนโยบายการเยียวยาของรัฐบาลมาเข้าร่วมขบวนการกับกลุ่มตน โดยได้มีการเผยแพร่คลิปวิดีโอที่มีการทำร้ายร่างกายลูกจ้าง การจับเด็กผู้หญิงเพื่อเรียกค่าไถ่ พร้อมทั้งแสดงวัตถุระเบิดที่เก็บไว้อยู่ในโกดังเป็นจำนวนมาก

ห้วงเดือนมิถุนายน พ.ศ. ๒๕๖๕ พลเมืองดีได้แจ้งเบาะแสกับเจ้าหน้าที่ตำรวจของสถานีตำรวจนครบาลบางซื่อ ที่กำลังตรวจตราสวนสาธารณะชื่อดังแห่งหนึ่งย่านหมอชิตว่าพบเด็กผู้หญิงมีอาการสั่นกลัวได้ทิ้งกระเป๋าสะพายสีดำขนาดใหญ่จำนวน ๒ ใบไว้ที่เก้าอี้นั่งเล่นของสวนสาธารณะและได้หายตัวไป ซึ่งเกรงว่าภายในจะมีวัตถุอันตราย เจ้าหน้าที่ตำรวจจึงรีบลงไปในพื้นที่เพื่อกั้นพื้นที่เกิดเหตุ พร้อมประสานเจ้าหน้าที่หน่วยเก็บกู้และตรวจพิสูจน์วัตถุระเบิดจากการตรวจสอบพบว่าภายในกระเป๋ามีวัตถุระเบิดแสวงเครื่องที่มีสารกัมมันตรังสีพร้อมแผงวงจรอิเล็กทรอนิกส์ห่อด้วยกระดาษ จึงเร่งเก็บกู้เพื่อนำของกลางทั้งหมดไปดำเนินการสืบสวนขยายผลผู้ที่เกี่ยวข้องเพื่อพิสูจน์ทราบถึงเจ้าของวัตถุต้องสงสัยดังกล่าว ต่อมาเจ้าหน้าที่ตำรวจได้จับกุมผู้ต้องสงสัยชื่อนาย C ซึ่งเป็นเจ้าของร้านอาหารในตลาดนัดแห่งหนึ่งย่านหมอชิต โดยให้การสารภาพว่านำวัตถุระเบิดมาจากชายนิรนามคนหนึ่ง และได้ติดตามชายดังกล่าวผ่านดาร์กเว็บที่มีเนื้อหาแสดงกลวิธีในการก่อการร้าย ซึ่งตนเองมีความสนใจจึงได้ติดต่อกับชายดังกล่าวผ่านอีเมลส่วนตัวโดยใช้นามแฝงและมีการเข้ารหัสการสนทนารายละเอียดรูปแบบปฏิบัติการต่าง ๆ ซึ่งนาย C จะลบอีเมลทุกฉบับ

ทันทีที่การสนทนาดังกล่าวสิ้นสุดลง นอกจากนี้ นาย C ยังให้การเพิ่มเติมว่าก่อนเกิดเหตุได้มีการพบปะกับชายนิรนามดังกล่าวเพื่อสำรวจพื้นที่ที่ใช้ในการก่อเหตุโดยเลือกจากพื้นที่ที่ไม่มีการแลกบัตรแสดงตนก่อนเข้าพื้นที่ รวมทั้งมีสถานที่จอดรถที่ปราศจากกล้องวงจรปิด ท้ายที่สุดจึงได้ตกลงใจร่วมกันในการก่อเหตุที่สวนสาธารณะดังกล่าว โดยชายนิรนามได้มอบโทรศัพท์มือถือเครื่องหนึ่ง เพื่อใช้ในการติดต่อสื่อสารระหว่างกัน รวมทั้งใช้ทัมบ์ไดรฟ์ (Thumb Drive) ซึ่งมีการเข้ารหัส โดยภายในบรรจุข้อมูลแผนการก่อเหตุโดยละเอียด ขณะเดียวกันหน่วยกู้ภัยได้รับแจ้งจากประชาชนว่าพบควันไฟขนาดใหญ่และมีเสียงระเบิดดังออกมาจากอาคารหน่วยงานเศรษฐกิจแห่งหนึ่งของประเทศไทย ส่งผลให้มีผู้ได้รับบาดเจ็บและเสียชีวิตเป็นจำนวนมาก นอกจากนี้ สืบทราบภายหลังได้ว่าผลของแรงระเบิดทำให้เกิดฝุ่นผงของกัมมันตรังสีกระจายตัวอยู่ในอากาศ เจ้าหน้าที่กู้ภัย ตำรวจ บุคลากรทางการแพทย์และหน่วยงานที่เกี่ยวข้องจึงได้ลงไปในพื้นที่และรับทราบภายหลังว่าเป็นการระเบิดฆ่าตัวตายโดยนาย A ซึ่งพบว่าติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID – 19) ชนิดกลายพันธุ์ที่สามารถติดเชื้อได้ง่ายและเร็วกว่าสายพันธุ์ปกติโดยติดต่อผ่านสัตว์สู่คนและคนสู่คน อย่างไรก็ตาม มีข่าวลวง (Fake News) ในสื่อสังคมออนไลน์ว่าเจ้าหน้าที่ทั้งหมดที่อยู่ใกล้กับศพนาย A ติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID – 19) ซึ่งเป็นข้อมูลอันเป็นเท็จหรือบิดเบือนข้อเท็จจริงเพื่อสร้างความตื่นตระหนกในหมู่ประชาชน

ห้วงเดือนกรกฎาคม พ.ศ. ๒๕๖๕ หน่วยงานด้านสาธารณสุขพบผู้เจ็บป่วยด้วยอาการอาหารเป็นพิษเป็นจำนวน ๕๕๐ ราย ซึ่งเกิดจากเชื้อแบคทีเรีย Salmonella Typhimurium โดยพบว่าผู้ติดเชื้อดังกล่าวได้เข้าไปรับประทานอาหารหรือทำงานอยู่ในร้านอาหารหลายแห่งในย่านหมอชิต รวมถึงร้านของนาย C เจ้าหน้าที่จึงต้องตรวจสอบว่าการแพร่ระบาดที่มาจากการปนเปื้อนสารแบคทีเรียดังกล่าวเป็นการปนเปื้อนโดยเจตนาหรือไม่ และในห้วงเวลาเดียวกัน กลุ่มแฮกเกอร์ Red_Axe ได้โพสต์ข้อความผ่านทวิตเตอร์ว่าเป็นผู้โจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บไซต์ของรัฐบาลไทย (thaigov.go.th) เกี่ยวกับข้อมูลรายงานสถานการณ์โรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID – 19) ในประเทศไทย เพื่อหวังทำลายความน่าเชื่อถือของรัฐบาล โดยมีสาเหตุมาจากความไม่พอใจที่รัฐบาลไทยจำกัดสิทธิในการแสดงความคิดเห็นในการประท้วงการทำงานของรัฐบาลและมีการจับกุมผู้เห็นต่างทางการเมือง นอกจากนี้กลุ่มแฮกเกอร์ Red_Axe ยังได้ขู่ว่าจะมีการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมถึงหน่วยงานภาครัฐของประเทศไทย เพิ่มเติมอีกด้วย

(๒) ร่างสถานการณ์ฝึกเฉพาะ

ห้วงเดือนสิงหาคม พ.ศ. ๒๕๖๕ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ตรวจพบความเคลื่อนไหวของกลุ่มแฮกเกอร์ Red_Axe ในการสร้างความร่วมมือกับกลุ่มแฮกเกอร์ Blue_Eagle ซึ่งถือว่าเป็นกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนโดยรัฐ (State - Sponsored Hackers) มีขีดความสามารถในการโจมตีทางไซเบอร์

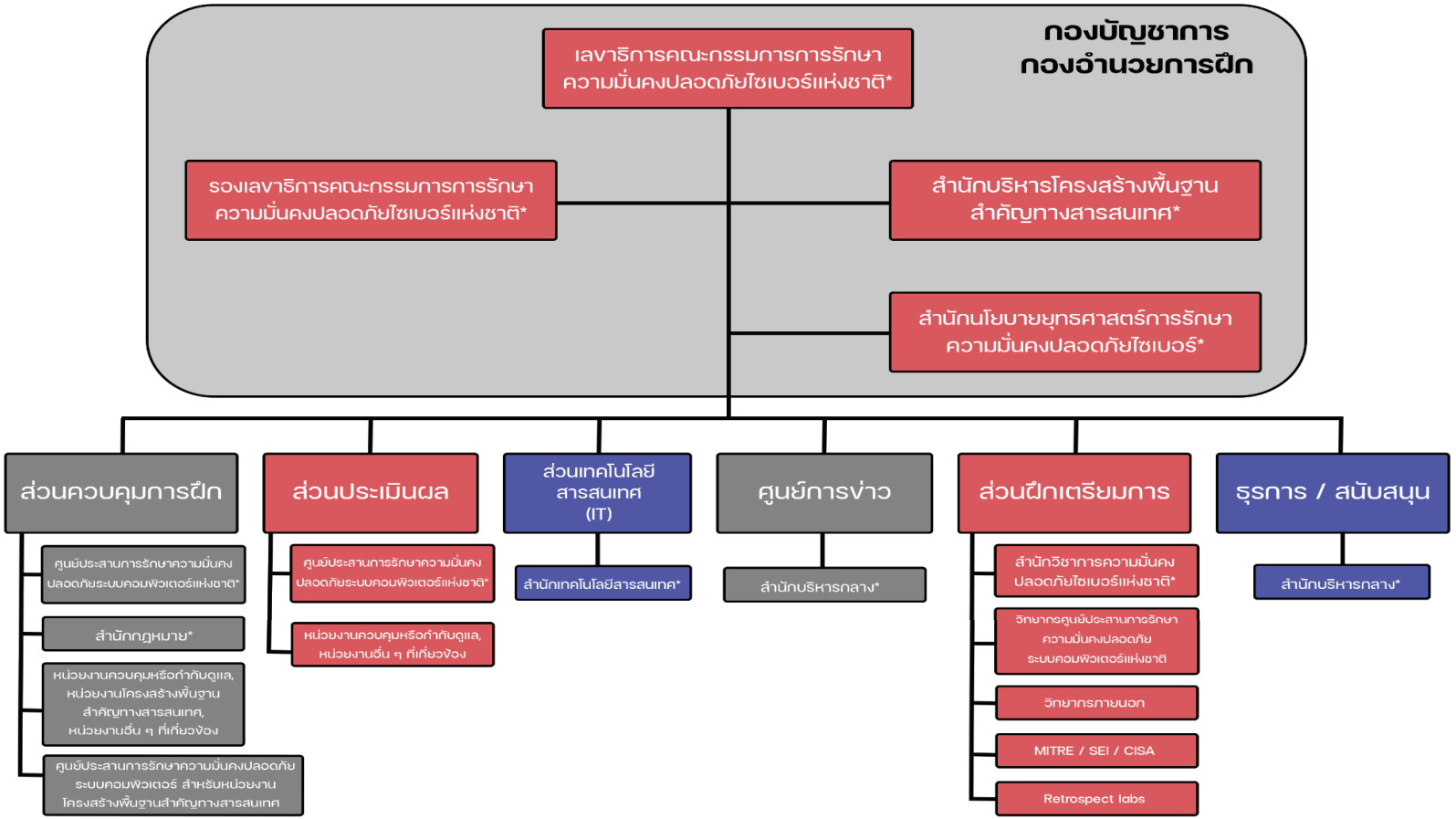
ในลักษณะ Advanced Persistent Threat (APT) และมีความเชี่ยวชาญในการใช้เครื่องมือโจมตีทางไซเบอร์ที่ซับซ้อน รวมถึงเคยมีประวัติในการโจมตีทางไซเบอร์ครั้งใหญ่ต่อประเทศต่าง ๆ ทั่วโลก โดยมุ่งโจมตีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศดังกล่าว จนส่งผลกระทบรุนแรงเป็นวงกว้าง ทำให้การทำงานหรือบริการต่าง ๆ ล้มเหลวทั้งระบบ รัฐไม่สามารถควบคุมการทำงานจากส่วนกลางได้ และยังลุกลามไปยังโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่น ๆ ของประเทศ จนมีผลทำให้ประชาชนจำนวนมากเสียชีวิตอีกด้วย จากรายงานความเคลื่อนไหวดังกล่าวยังพบว่ามีความเป็นไปได้ที่จะมีการโจมตีทางไซเบอร์ต่อระบบไฟฟ้าของประเทศ รวมถึงการโจมตีโรงพยาบาลโดยใช้ Ransomware ร่วมด้วย

๒.๑.๕.๕ รูปแบบการฝึกใช้รูปแบบการฝึกซ้อมแผนบนโต๊ะ (Table Top Exercise : TTX) โดยมีแนวทาง ดังนี้

(๑) แบ่งกลุ่มผู้รับการฝึกเป็นจำนวน ๘ กลุ่ม ประกอบด้วย ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่นๆ ทั้งนี้ หากมีจำนวนคนในแต่ละกลุ่มไม่เหมาะสม สกมช. อาจดำเนินการปรับเปลี่ยนกลุ่มผู้รับการฝึกได้ตามความเหมาะสม

(๒) แต่ละกลุ่ม อาจได้รับโจทย์ฝึกที่เหมือนกัน หรือแตกต่างกัน ซึ่งจะได้พิจารณาถึงข้อดีข้อเสียร่วมกับผู้แทนหน่วยงานที่เข้าร่วมการประชุมวางแผนต่อไป

๒.๑.๕.๖ ร่างโครงสร้างการฝึก



*หน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รูปที่ ๒-๒ ร่างโครงสร้างการฝึก

(๑) ร่างบทบาทหน้าที่

บทบาท	หน้าที่
กองบัญชาการ กองอำนวยการฝึก (บก.กอ.ฝึก)	(๑) วางแผนการฝึก (๒) กำหนดวัตถุประสงค์ และผลผลิตที่ต้องการ (๓) ประสานงาน (๔) รับผิดชอบโครงการ (๕) รายงานผลการฝึก (๖) รับคณะตรวจเยี่ยม
ส่วนควบคุมการฝึก (Exercise Control Group : ECG)	(๑) ออกแบบสถานการณ์ฝึก (Scenario Development) (๒) ออกแบบรายการโจทย์ฝึก (Master Scenario Event List : MSEL Development) (๓) การดำเนินการฝึก (Exercise Execution) (๔) ผลการฝึก (Daily Hotwash) (๕) เป็นผู้สอนในช่วงการฝึกเตรียมการ (Pre-exercise) (๖) รวบรวมหลักฐานประกอบการรายงาน (Global Cybersecurity Index : GCI)
ส่วนประเมินผล (Exercise Evaluation Group : EEG)	(๑) ประเมินความพึงพอใจ (๒) ประเมินทักษะก่อนและหลังการฝึก (๓) สรุปบทเรียนจากการฝึก (After Action Review : AAR)
ส่วนเทคโนโลยีสารสนเทศ (Information Technology : IT)	(๑) ระบบการประชุม (๒) ระบบ Chat (๓) ระบบ Share Drive
ศูนย์การข่าว	(๑) จัดทำสื่อประชาสัมพันธ์ (๒) ประสานงานกับสื่อมวลชน (๓) พิธีเปิด-ปิดการฝึก
ส่วนฝึกเตรียมการ (Pre-exercise)	(๑) วางแผนการฝึกเตรียมการ (๒) จัดการฝึกเตรียมการ (๓) ประเมินผลการฝึกเตรียมการ
ธุรการ/สนับสนุน	(๑) จัดเตรียมอาหาร ของว่าง และเครื่องดื่ม (๒) จัดเตรียมช่างถ่ายภาพ และเก็บภาพตลอดกิจกรรม

บทบาท	หน้าที่
ผู้รับการฝึก	(๑) เข้าร่วมการฝึกเตรียมการ (Pre-exercise) (๒) เข้าร่วมการฝึก (Exercise Execution)
ผู้สังเกตการณ์	(๑) เข้าสังเกตการณ์กิจกรรมการจัดทำสถานการณ์ฝึก (๒) เข้าสังเกตการณ์กิจกรรมการฝึกเตรียมการ (Pre-exercise) (๓) เข้าสังเกตการณ์กิจกรรมการดำเนินการฝึก (Exercise Execution) **กรณีที่นั่งในระบบเต็ม สกมช. จะขอให้สิทธิ์กับผู้รับการฝึก รวมถึงส่วนที่จัดการฝึก เป็นลำดับแรก
ผู้เยี่ยมชม	ตรวจเยี่ยมการฝึก (Onsite & Online)

ตารางที่ ๒-๒ ร่างบทบาทหน้าที่

(๒) หน่วยงานที่จะเชิญเข้าร่วมการฝึก

บทบาท	หน้าที่
กองบัญชาการกองอำนวยการฝึก (บก.กอ.ฝึก)	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ - สำนักงานสภาความมั่นคงแห่งชาติ - สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) - กรมยุทธการทหาร กองบัญชาการกองทัพไทย - ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย
ส่วนควบคุมการฝึก (ECG)	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ - สำนักงานสภาความมั่นคงแห่งชาติ - ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย - หน่วยงานควบคุมหรือกำกับดูแล - หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ - ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector CERT : TB-CERT) - ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
ส่วนประเมินผล (EEG)	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ - หน่วยงานควบคุมหรือกำกับดูแล
ส่วนเทคโนโลยีสารสนเทศ (IT)	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

บทบาท	หน้าที่
ศูนย์การข่าว	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ส่วนฝึกเตรียมการ	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ธุรการ/สนับสนุน	- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ผู้รับการฝึก	- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) - หน่วยงานควบคุมหรือกำกับดูแล - หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ - หน่วยงานอื่น ๆ ที่เกี่ยวข้อง (อาทิ สำนักข่าวกรองแห่งชาติ, กระทรวงการต่างประเทศ, สถาบันการแพทย์ฉุกเฉินแห่งชาติ, สำนักงานตรวจคนเข้าเมือง ฯลฯ)
ผู้สังเกตการณ์	(ถ้ามี)
ผู้เยี่ยมชม	(ถ้ามี)

ตารางที่ ๒-๓ หน่วยงานที่จะเชิญเข้าร่วมการฝึก

๒.๑.๖ สรุปประเด็นการหารือและข้อเสนอแนะ ดังนี้

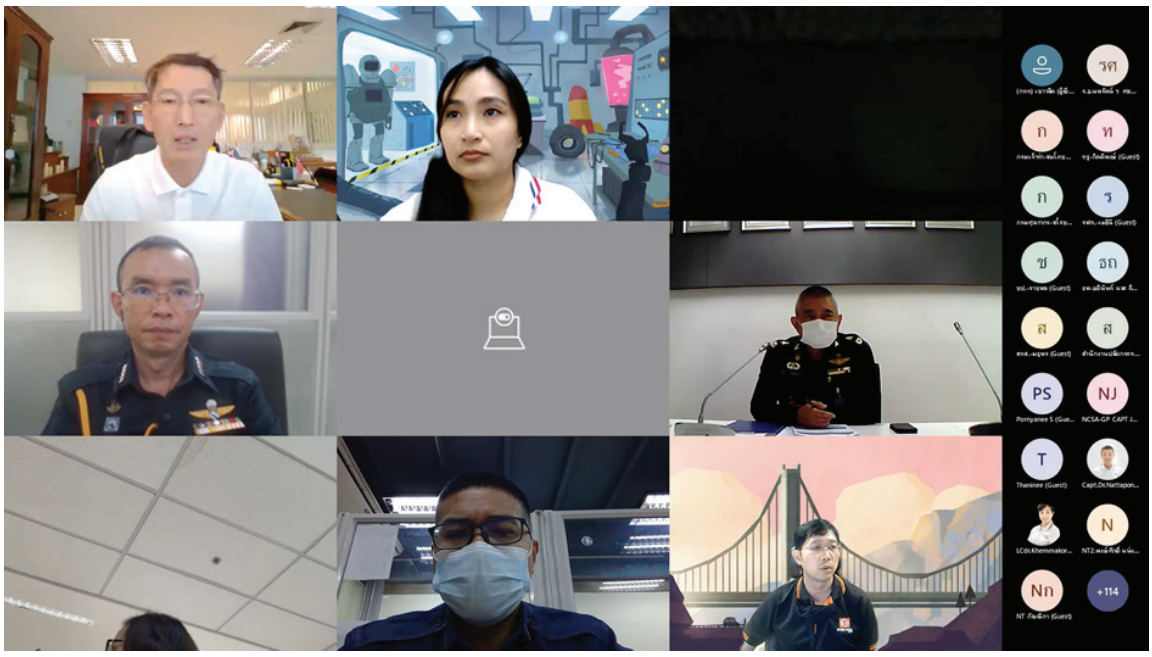
๒.๑.๖.๑ ในห้วงการฝึกเตรียมการ (Pre-exercise) ขอให้มีการแบ่งกลุ่มการอบรมที่ชัดเจน เช่น กลุ่มผู้รับการฝึกที่มีทักษะเบื้องต้น กลุ่มผู้รับการฝึกที่มีทักษะขั้นสูง และกลุ่มผู้บริหาร

๒.๑.๖.๒ ในห้วงดำเนินการฝึก (Exercise Execution) ขอให้มีจำนวนผู้เข้ารับการฝึกอย่างน้อย ๕ คนต่อหน่วยงาน เพื่อให้หน่วยงานสามารถส่งคนที่เกี่ยวข้องและมีบทบาทที่แตกต่างกันเข้ารับการฝึกได้อย่างครอบคลุมและได้รับประโยชน์สูงสุด

๒.๑.๖.๓ เรื่องการประชาสัมพันธ์ ขอให้พิจารณางดการถ่ายทอดสดขณะทำการฝึกผ่าน Facebook Live เนื่องจาก ข้อมูลที่มีการพูดคุยกันในห้วงเวลาดังกล่าวมีความสำคัญและเกี่ยวข้องกับการทำงานจริงของหน่วยงาน

๒.๑.๖.๔ เรื่องการตรวจเยี่ยม ขอให้เพิ่มรายชื่อผู้บริหารจากหน่วยงานเพิ่มเติมจากในร่างรายชื่อ

๒.๒ การประชุมวางแผนขั้นต้น (Initial Planning Conference: IPC)



รูปที่ ๒-๓ การประชุมวางแผนขั้นต้น (Initial Planning Conference: IPC)

๒.๒.๑ วัตถุประสงค์การประชุม

เพื่อให้ผู้แทนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ร่วมพิจารณาและตัดสินใจประเด็นสำคัญที่เกี่ยวข้องกับการฝึก

๒.๒.๒ วันและเวลาการประชุม

วันที่ ๑๒ ตุลาคม พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ - ๑๖.๐๐ น.

๒.๒.๓ สถานที่การประชุม

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๒.๒.๔ ผู้เข้าร่วมการประชุม

๒.๒.๔.๑ ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล ๑๙ หน่วยงาน

๒.๒.๔.๒ ผู้แทนจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๔๖ หน่วยงาน

๒.๒.๔.๓ ผู้แทนจากหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ๔ หน่วยงาน

รวมจำนวนทั้งสิ้น ๑๔๐ คน

๒.๒.๕ สาระสำคัญของการประชุม

๒.๒.๕.๑ ที่ประชุมมีมติยืนยันผลการประชุมพัฒนาแนวคิดการฝึก (CDC) ซึ่งฝ่ายเลขานุการได้มีการปรับแก้ตามข้อเสนอแนะในที่ประชุมเรียบร้อยแล้ว สรุปได้ดังนี้

(๑) วัตถุประสงค์การฝึกและผลลัพธ์ที่คาดหวัง (Objective & Expected Outcomes) ไม่เปลี่ยนแปลง

(๒) สถานการณ์ฝึกและรูปแบบการฝึก (Initial Scenarios & Selected Style) ไม่เปลี่ยนแปลง

(๓) กำหนดการ (Exercise Timeframe) ไม่เปลี่ยนแปลง

(๔) โครงสร้างการฝึก (Exercise Structures) มีการเปลี่ยนแปลงในหัวข้อจำนวนผู้เข้ารับการฝึก โดยเพิ่มจากเดิม ๒ คนต่อหน่วยงาน เป็น ๕ คนต่อหน่วยงาน

(๕) บทบาทหน้าที่ (Role and Responsibilities) มีการเพิ่มเติมรายละเอียดของผู้ที่จะเข้ารับการฝึก ได้แก่ จำนวนผู้เข้ารับการฝึก และแนวทางการพิจารณาบุคคลที่เหมาะสมที่จะเข้าร่วมการฝึก

(๖) รายชื่อหน่วยงานที่จะเข้าร่วมการฝึก (Expected Participants) มีการเปลี่ยนแปลง ในเรื่องรายชื่อหน่วยงานที่จะเชิญเข้าตรวจเยี่ยมการฝึก โดยเพิ่มรายชื่อหน่วยงานเข้าร่วมตรวจเยี่ยมการฝึก ๑ หน่วยงาน คือ สำนักข่าวกรองแห่งชาติ

(๗) การงดการถ่ายทอดกิจกรรมการฝึกผ่าน Facebook Live รวมถึงสำนักข่าวต่าง ๆ

๒.๒.๕.๒ หัวข้อพิจารณาในการประชุม

(๑) ร่างรายชื่อผู้ติดต่อประสาน (Point of Contact) โดยขอความร่วมมือให้หน่วยงานที่ยังส่งรายชื่อผู้ติดต่อประสานไม่ครบถ้วนให้กับฝ่ายเลขาฯ ภายหลังการประชุมวางแผนขั้นต้น

(๒) ร่างจำนวนคนที่จะเข้าร่วมการฝึก (Number of Participants) โดยแบ่งออกเป็น ๔ กลุ่ม คือ บก.กอ.ฝึก ส่วนควบคุมการฝึก ส่วนประเมินผล และผู้เข้ารับการฝึก ซึ่งจะจัดคนเข้าร่วมแต่ละกลุ่มจากหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยพิจารณาจากรายชื่อหน่วยงานตามประกาศมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงรายชื่อหน่วยงานที่เกี่ยวข้องกับการบริหารวิกฤตการณ์ระดับชาติด้วย

(๓) ร่างแนวทางรับมือกับภัยคุกคามทางไซเบอร์ที่มีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (National Cyber Incident Response Process) ซึ่ง สกมช. จะร่างขึ้นเพื่อใช้ในห้วงการฝึก โดยให้มีความสอดคล้องกับการรับมือกับภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๕๘ และมาตรา ๕๙ รวมถึงร่างประกาศมาตรา ๖๐ ด้วย ทั้งนี้ ร่างแนวทางรับมือดังกล่าว จะนำไปใช้เป็นข้อมูลสำคัญเพื่อประกอบการจัดทำ (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ (The National Cyber Response Plan of Thailand) ด้วยต่อไป

(๔) ร่างแนวทางการจัดทำโจทย์ฝึก (Inject Development Timeline) โดยกำหนดให้มีการประชุมย่อยเพื่อจัดทำสถานการณ์และโจทย์ฝึก จำนวน ๒ ครั้ง ได้แก่ ครั้งที่ ๑ ในวันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔ และครั้งที่ ๒ ในวันที่ ๒๐ ตุลาคม พ.ศ. ๒๕๖๔ เพื่อเตรียมความพร้อมก่อนการจัดทำสถานการณ์และโจทย์ฝึกจริง ระหว่างวันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ ทั้งนี้ ฝ่ายเลขาฯ จะได้ประสานขอรายชื่อผู้ทำหน้าที่ส่วนควบคุมการฝึกทันทีหลังเสร็จสิ้นการประชุมวางแผนขั้นต้น

(๕) ร่างใบประกาศนียบัตร (Certification) แบ่งออกเป็น ๓ ประเภท ได้แก่ ใบประกาศนียบัตรสำหรับผู้ที่เข้าร่วมการฝึก ผู้ที่สนับสนุนการฝึก และผู้ที่เข้าร่วมการอบรมพิเศษกับ MITRE/SEI/CISA

๒.๒.๖ ผลผลิตจากการประชุม

ผู้แทนหน่วยงานที่เข้าร่วมประชุม ยืนยันผลการประชุมพัฒนาแนวคิดการฝึก (CDC) ตามข้อ ๒.๒.๕.๑

๒.๒.๗ สรุปประเด็นการหารือและข้อเสนอแนะ ดังนี้

๒.๒.๗.๑ มีบางหน่วยงานขอนำร่างจำนวนคนที่จะเข้าร่วมการฝึก กลับไปพิจารณาว่าสามารถส่งได้ตามจำนวนที่ สกมช. กำหนดหรือไม่

๒.๒.๗.๒ ผู้ทำหน้าที่ส่วนควบคุมการฝึก ผู้ประเมินการฝึก ผู้เข้ารับการอบรม และผู้เข้ารับการฝึกควรมีคุณสมบัติอย่างไร

๒.๒.๗.๓ ขอปรับเพิ่ม/ลด จำนวนผู้เข้ารับการฝึก

๒.๒.๗.๔ ขอให้ สกมช. ทำหนังสือถึงหน่วยงาน เพื่อให้ผู้บริหารทราบและอนุมัติตัวบุคคลเข้าร่วมการฝึก

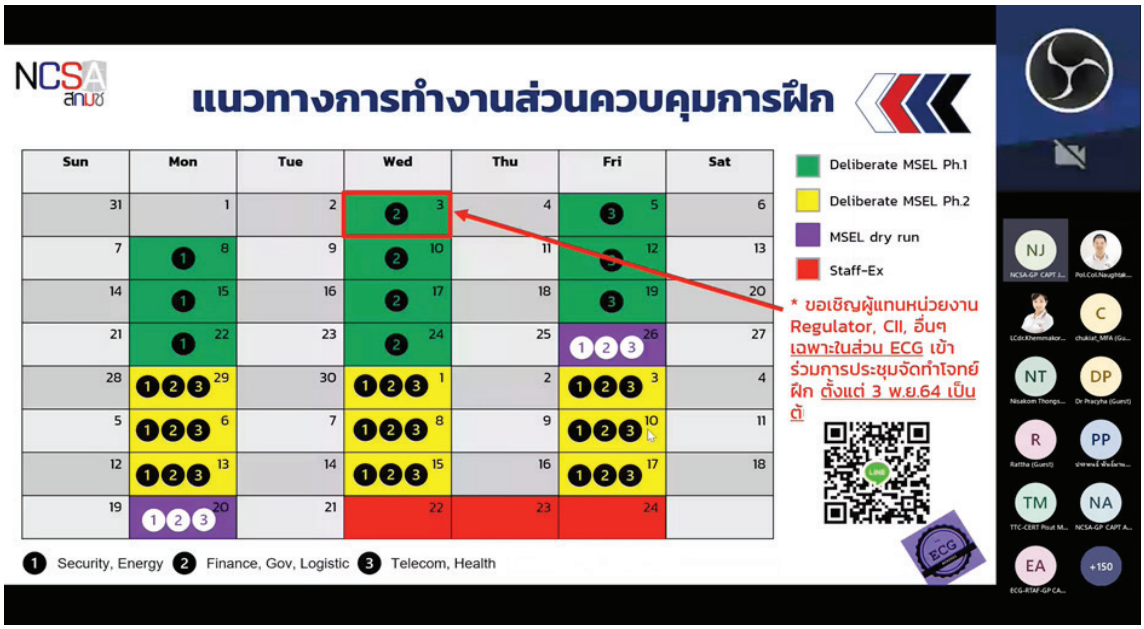
๒.๒.๗.๕ ผู้เข้ารับการฝึกในฐานะหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะได้รับโจทย์ฝึกเดียวกันหรือไม่

๒.๒.๗.๖ หน่วยงานที่จะเข้ารับการฝึกในครั้งนี้ มีหน่วยงานตามประกาศมาตรา ๕๐ หรือไม่ และการออกแบบโจทย์ฝึกจะเป็นโจทย์ในภาพรวมหรือเจาะจงเฉพาะ Sector[๓] นั้น ๆ

๒.๓ การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC)

รูปที่ ๒-๔ การการประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC)

[๓] ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒



รูปที่ ๒-๔ การประชุมวางแผนขั้นสุดท้าย (Final Planning Conference: FPC)

๒.๓.๑ วัตถุประสงค์การประชุม

เพื่อให้ผู้แทนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ร่วมพิจารณาและตัดสินใจประเด็นสำคัญที่เกี่ยวข้องกับการฝึก และยืนยันประเด็นสำคัญต่าง ๆ เป็นครั้งสุดท้าย ก่อนการดำเนินการฝึกที่จะเกิดขึ้นในห้วงเดือนธันวาคม พ.ศ. ๒๕๖๔

๒.๓.๒ วันและเวลาการประชุม

วันที่ ๑ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ - ๑๖.๐๐ น.

๒.๓.๓ สถานที่การประชุม

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๒.๓.๔ ผู้เข้าร่วมการประชุม

๒.๓.๔.๑ ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล จำนวน ๑๗ หน่วยงาน

๒.๓.๔.๒ ผู้แทนจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน ๓๘ หน่วยงาน

๒.๓.๔.๓ ผู้แทนจากหน่วยงานที่เกี่ยวข้อง จำนวน ๓ หน่วยงาน

รวมจำนวนทั้งสิ้น ๑๑๙ คน

๒.๓.๕ สาระสำคัญของการประชุม

๒.๓.๕.๑ ทบทวนเนื้อหาที่ได้มีการยืนยันไปแล้วจากการประชุมวางแผนขั้นต้น (IPC) โดยมีการดำเนินการเพิ่มเติม ตามข้อเสนอแนะในที่ประชุมฯ สรุปได้ดังนี้

(๑) บก.กอ.ฝึก ชี้แจงคุณสมบัติของผู้ทำหน้าที่ในส่วนควบคุมการฝึก ส่วนประเมินผล และผู้รับการฝึกเพิ่มเติมแล้ว

(๒) ส่วนฝึกเตรียมการ เพิ่มเติมคุณสมบัติของผู้เข้ารับการอบรม ในหนังสือเชิญแล้ว

(๓) บก.กอ.ฝึก มีหนังสือถึงหน่วยงานผู้เข้าร่วมการฝึก เรื่องขอให้หน่วยงานอนุมัติตัวบุคคลเข้าร่วมในบทบาทหน้าที่ที่ได้รับ

(๔) บก.กอ.ฝึก ชี้แจงเพิ่มเติมว่า หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับดูแลของตน จะเป็นผู้เข้ารับการฝึกอยู่ใน Sector เดียวกัน และจะได้รับโจทย์ฝึกร่วมกัน ทั้งนี้ จะต้องร่วมกันแก้ไขโจทย์ฝึกตามบทบาทหน้าที่ของตน อีกทั้ง หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องส่งคำตอบแยกกันด้วย

(๕) ส่วนควบคุมการฝึก หารือร่วมกับผู้แทนหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ในการประชุมจัดทำสถานการณ์และโจทย์ฝึก เมื่อวันที่ ๑๕, ๒๐, ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ ได้ข้อสรุปร่วมกันว่าจะใช้โจทย์ฝึกที่แตกต่างกันตาม Sector ขณะที่มีโจทย์ฝึกบางส่วนจะเป็นภาพรวม (ทุกหน่วยงานได้รับเหมือนกัน)

๒.๓.๕.๒ ยืนยันหัวข้อสำคัญในการประชุมวางแผนขั้นสุดท้าย (FPC) ดังนี้

(๑) นาวาอากาศเอก จเด็ด คูหะก้องกิจ ผู้ช่วยผู้อำนวยการฝึก ๑ ชี้แจงร่างจำนวนคนที่จะเข้าร่วมการฝึกแบ่งออกเป็น ๔ กลุ่ม คือ บก.กอ.ฝึก ส่วนควบคุมการฝึก ส่วนประเมินผล และผู้เข้ารับการฝึก โดยจัดจากหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยพิจารณารายชื่อหน่วยงานจากประกาศมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงรายชื่อหน่วยงานที่เกี่ยวข้องกับการบริหารวิกฤตการณ์ระดับชาติ

(๒) พันตำรวจเอก ณัทกฤช พรหมจันทร์ รองหัวหน้าส่วนควบคุมการฝึก ๒ ชี้แจงร่างลำดับสถานการณ์ และประเภทโจทย์ฝึก โดยสรุปภาพรวมของการจัดทำสถานการณ์และโจทย์ฝึก เมื่อวันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ ที่ผ่านมา ให้ที่ประชุมรับทราบ รวมถึงชี้แจงแนวทางการทำงานในส่วนควบคุมการฝึกเพื่อทำให้สถานการณ์และโจทย์ฝึกมีความสมบูรณ์

(๓) นาวาเอกหญิง ศิริเนตร รักษ์วงศ์ หัวหน้าส่วนฝึกเตรียมการ ชี้แจงร่างหัวข้อสำหรับการฝึกเตรียมการ ประกอบด้วย หัวข้อการอบรม วันและเวลาการอบรม คุณสมบัติและข้อจำกัดในแต่ละหัวข้อการอบรม และแจ้งให้ที่ประชุมทราบว่า สกมช. จะทำหนังสือถึงหน่วยงาน เพื่อขอให้พิจารณาส่งรายชื่อผู้ที่สนใจเข้ารับการอบรมในหัวข้อต่าง ๆ

(๔) พันตรี ปวิช บูรพาชลทิศน์ หัวหน้าส่วนประเมินผล ชี้แจงร่างแนวทางการทำงานส่วนประเมินผล โดยแบบประเมินผลการฝึกจะจัดทำตามแนวทางของ MITRE Cyber Exercise Playbook ซึ่งแบบประเมินผลดังกล่าว จะถูกจัดทำขึ้นให้เหมาะสมกับแต่ละ Sector โดยแต่ละชุดจะเชื่อมโยงกับโจทย์ฝึก (Inject) แต่ละข้อ ที่จัดทำโดยส่วนควบคุมการฝึก (ECG) ทั้งนี้ ผู้ที่ทำหน้าที่ประเมิน คือ ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล และเพื่อทำให้แบบประเมินสมบูรณ์ได้ประสานขอความร่วมมือผู้แทนหน่วยงานในส่วนประเมินผล ให้เข้าร่วมจัดทำแบบประเมินอย่างต่อเนื่อง

(๕) นางพัชญ์ชิชา ไกรแสงศรี รองหัวหน้าศูนย์การข่าว ชี้แจงร่างพิธีเปิดและพิธีปิดการฝึก โดยจะมีพิธีเปิดการฝึกในวันที่ ๒๒ ธันวาคม พ.ศ. ๒๕๖๔ เวลา ๐๘.๓๐ - ๑๑.๓๐ น. และพิธีปิดในวันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๔ เวลา ๑๖.๓๐ - ๑๗.๑๕ น.

๒.๓.๖ ผลผลิตจากการประชุม

ผู้แทนหน่วยงานที่เข้าร่วมประชุม ยืนยันตามหัวข้อ ๒.๓.๕.๑ และ ๒.๓.๕.๒

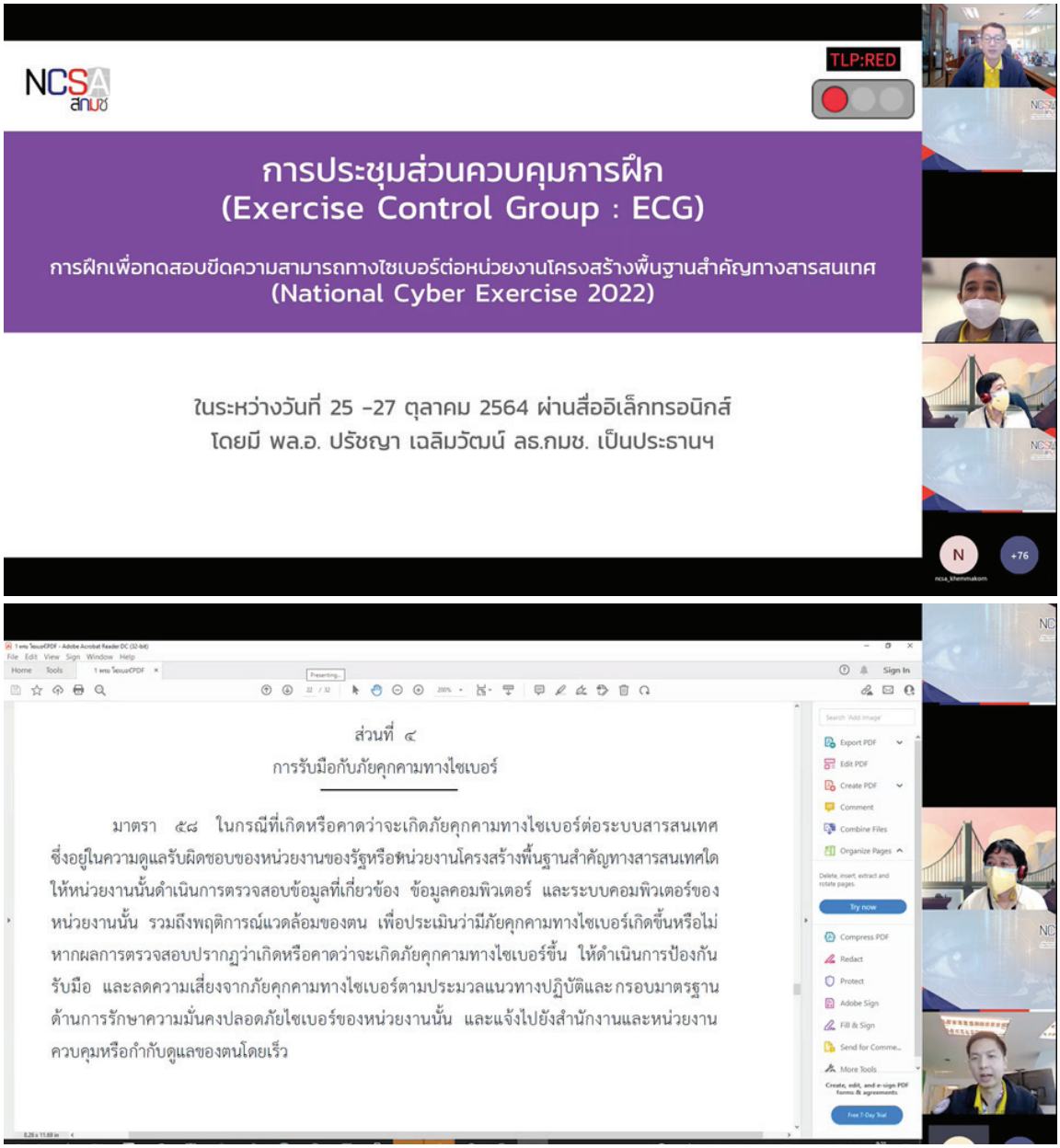
๒.๓.๗ สรุปประเด็นการหารือและข้อเสนอแนะจากผู้แทนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ดังนี้

๒.๓.๗.๑ ขอปรับเพิ่ม/ลด จำนวนผู้เข้ารับการฝึก และแจ้งรายชื่อภายหลังการประชุมวางแผนขั้นสุดท้าย

๒.๓.๗.๒ ข้อจำกัดและเงื่อนไขในการส่งรายชื่อเข้าร่วมการอบรมในหัวข้อต่าง ๆ

๒.๓.๗.๓ ตารางการเข้าร่วมทำหน้าที่ในส่วนควบคุมการฝึกและในส่วนประเมินผล มีการประชุมค่อนข้างบ่อย อาจเข้าร่วมไม่ได้หรืออาจไม่เต็มเวลาการประชุมทุกครั้ง

๒.๔ การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)



รูปที่ ๒-๕ การประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)

๒.๔.๑ วัตถุประสงค์การประชุม

เพื่อให้ผู้แทนหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ร่วมกันจัดทำสถานการณ์และโจทย์ฝึก ให้สอดคล้องกับวัตถุประสงค์การฝึกตามที่ บก.กอ.ฝึก กำหนด รวมทั้งใช้เป็นโจทย์ฝึกในห้วงดำเนินการฝึกด้วย

๒.๔.๒ วันและเวลาการประชุม

๒.๔.๒.๑ วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔ เวลา ๑๐.๓๐ - ๑๒.๐๐ น.

๒.๔.๒.๒ วันที่ ๒๐ ตุลาคม พ.ศ. ๒๕๖๔ เวลา ๑๐.๓๐ - ๑๒.๐๐ น.

๒.๔.๒.๓ วันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ - ๑๖.๐๐ น.

๒.๔.๓ สถานที่การประชุม

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๒.๔.๔ ผู้เข้าร่วมการประชุม

๒.๔.๔.๑ ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล จำนวน ๑๙ หน่วยงาน

๒.๔.๔.๒ ผู้แทนจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน๔๓ หน่วยงาน

๒.๔.๔.๓ ผู้แทนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน ๒ หน่วยงาน

๒.๔.๔.๔ ผู้แทนจากหน่วยงานอื่น ๆ ที่เกี่ยวข้อง จำนวน ๒ หน่วยงาน

สรุปเป็นจำนวนผู้เข้าร่วมการประชุมจัดทำสถานการณ์และโจทย์ฝึก ได้ดังนี้

- วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๔๒ คน
- วันที่ ๒๐ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๒๕ คน
- วันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๗๐ คน

๒.๔.๕ สาระสำคัญของการประชุม

๒.๔.๕.๑ แนวทางการจัดทำสถานการณ์และโจทย์ฝึก

(๑) ทบทวนวัตถุประสงค์การฝึก

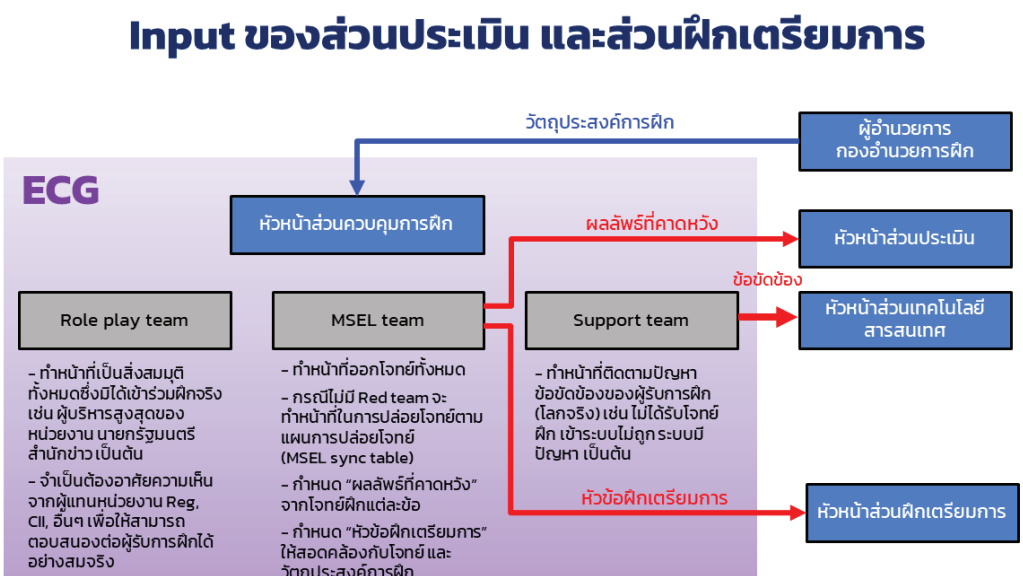
(๒) ทบทวนสถานการณ์ฝึก C-MEX 21

รูปที่ ๒-๖ ข้อตกลงเรื่องการแลกเปลี่ยนข้อมูล (Traffic Light Protocol : TLP)

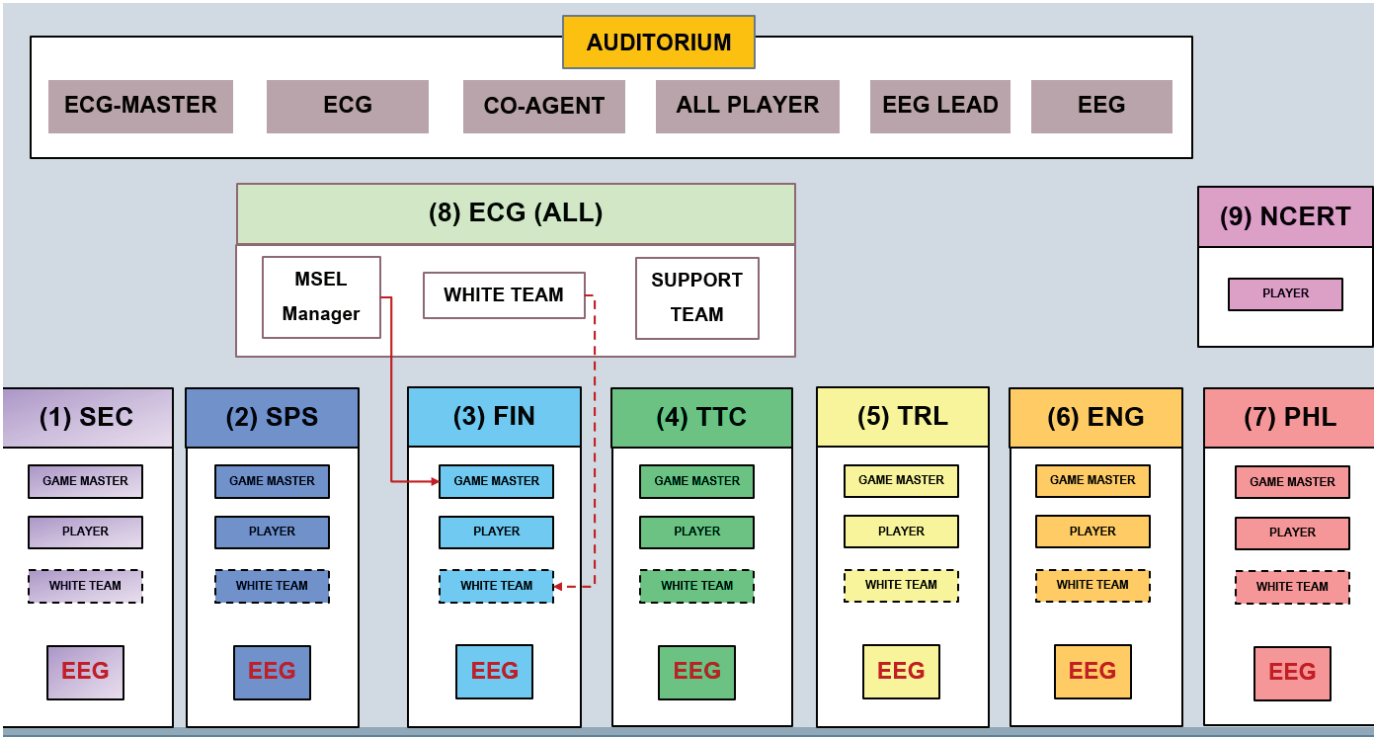
(๓) แนวทางการดำเนินการ

(๓.๑) ข้อตกลงเรื่องการแลกเปลี่ยนข้อมูล (Traffic Light Protocol : TLP) โดยในส่วนควบคุมการฝึก ได้รับทราบและตกลงร่วมกันว่า จะใช้ TLP : RED คือ ห้ามเปิดเผยข้อมูลออกไปนอกส่วนควบคุมการฝึก และจำกัดการเปิดเผยข้อมูลเฉพาะผู้ที่เกี่ยวข้องเท่านั้น

(๓.๒) โครงสร้างและการจัด



รูปที่ ๒-๗ โครงสร้างของส่วนควบคุมการฝึก



รูปที่ ๒-๗ โครงสร้างของส่วนควบคุมการฝึก

(๓.๒.๑) ECG Master ทำหน้าที่กำกับดูแล และควบคุมการดำเนินการทั้งหมดของส่วนควบคุมการฝึก เพื่อให้เป็นไปตามรายการโจทย์ฝึก (MSEL) ที่กำหนดไว้

(๓.๒.๒) MSEL Team ทำหน้าที่ออกแบบและปล่อยโจทย์โดยกำหนด “ผลลัพธ์ที่คาดหวัง” ให้กับโจทย์ฝึกแต่ละข้อ และกำหนด “หัวข้อฝึกเตรียมการ” ให้สอดคล้องกับโจทย์ฝึกรวมถึงวัตถุประสงค์การฝึก ทั้งนี้ MSEL Team จะประกอบด้วย

(๓.๒.๒.๑) MSEL Manager รับผิดชอบการส่งโจทย์ฝึกตามรายการโจทย์ฝึก (MSEL) ที่กำหนดไว้ ไปยัง Game Master

(๓.๒.๒.๒) Game Master รับผิดชอบการส่งโจทย์ฝึกที่ได้รับจาก MSEL Manager ไปยัง Players รวมถึงเรื่องการกระตุ้น Players ให้มีความกระตือรือร้น การอธิบายโจทย์ฝึกให้เกิดความชัดเจนมากขึ้น และการยืนยันผลการส่งโจทย์ฝึกกลับไปยัง MSEL Manager ด้วย

(๓.๒.๓) White Team หรือ Role Play Team ทำหน้าที่เป็นสิ่งสมมุติทั้งหมดซึ่งมิได้เข้าร่วมฝึกจริง เช่น นายกรัฐมนตรี ผู้บริหารสูงสุดของหน่วยงาน สำนักข่าว เป็นต้น

(๓.๒.๔) Support Team ทำหน้าที่ติดตามปัญหาข้อขัดข้องของผู้รับการฝึก (โลกจริง) เช่น ไม่ได้รับโจทย์ฝึก เข้าระบบไม่ถูก ระบบมีปัญหา เป็นต้น

(๓.๒.๕) Co-Agent ทำหน้าที่สนับสนุน Game Master และ MSEL Manager รวมถึงการประสานงานโดยใกล้ชิด ระหว่าง สกมช. และ ECG ด้วย

(๓.๒.๖) หน้าที่ของส่วนควบคุมการฝึก ประกอบด้วย

(๓.๒.๖.๑) ออกแบบสถานการณ์และโจทย์ฝึก (Scenario & Inject Development)

(๓.๒.๖.๒) จัดทำรายการโจทย์ฝึก (MSEL)

(๓.๒.๖.๓) ดำเนินการฝึก (Exercise Execution)

(๓.๒.๖.๔) ผลการฝึก (Daily Hotwash)

(๓.๒.๖.๕) เป็นผู้สอนในช่วงการฝึกเตรียมการ (Pre-exercise)

(๓.๒.๖.๖) รวบรวมหลักฐานประกอบการรายงาน (Global Cybersecurity Index : GCI)

(๔) กรอบอัตรา ประกอบด้วย ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง หน่วยงานละ ๑ คน

(๕) แนวทางการจัดทำสถานการณ์และโจทย์ฝึก ดังนี้

(๕.๑) วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๔ กำหนดสมาชิกลงในทีมย่อย (White Team/MSEL Team/Support Team) รวมถึงทบทวนวัตถุประสงค์ สถานการณ์ทั่วไป/เฉพาะ และผลลัพธ์ที่คาดหวัง

(๕.๒) วันที่ ๒๐ ตุลาคม พ.ศ. ๒๕๖๔ จัดทำลำดับสถานการณ์ (Road to Crisis) กำหนดประเภทโจทย์ฝึก (MSEL Type) และจัดทำตารางประสานสอดคล้อง (MSEL Sync Table)

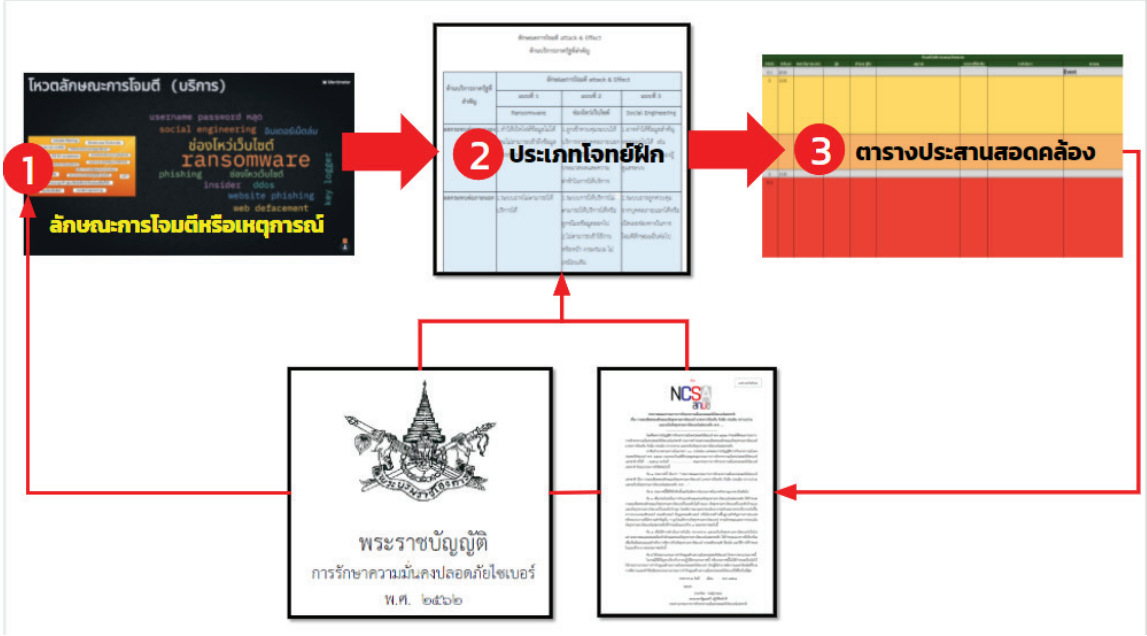
(๕.๓) วันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ พัฒนาเนื้อหา (Develop Content) รวมถึงการเตรียมการและทดสอบการส่ง (Prepare Response Handling)

๒.๔.๖ ผลผลิตจากการประชุม (วันที่ ๒๕ - ๒๗ ตุลาคม พ.ศ. ๒๕๖๔)

๒.๔.๖.๑ กิจกรรมสร้างความคุ้นเคย

รูปที่ ๒-๘ กิจกรรมสร้างความคุ้นเคย

๒.๔.๖.๒ กิจกรรมทบทวนหลักการที่สำคัญ ประกอบด้วย



รูปที่ ๒-๙ กิจกรรมทบทวนหลักการที่สำคัญ

(๑) แนวทางการจัดทำสถานการณ์ ตามแนวทางของ MITRE Cyber Exercise Playbook

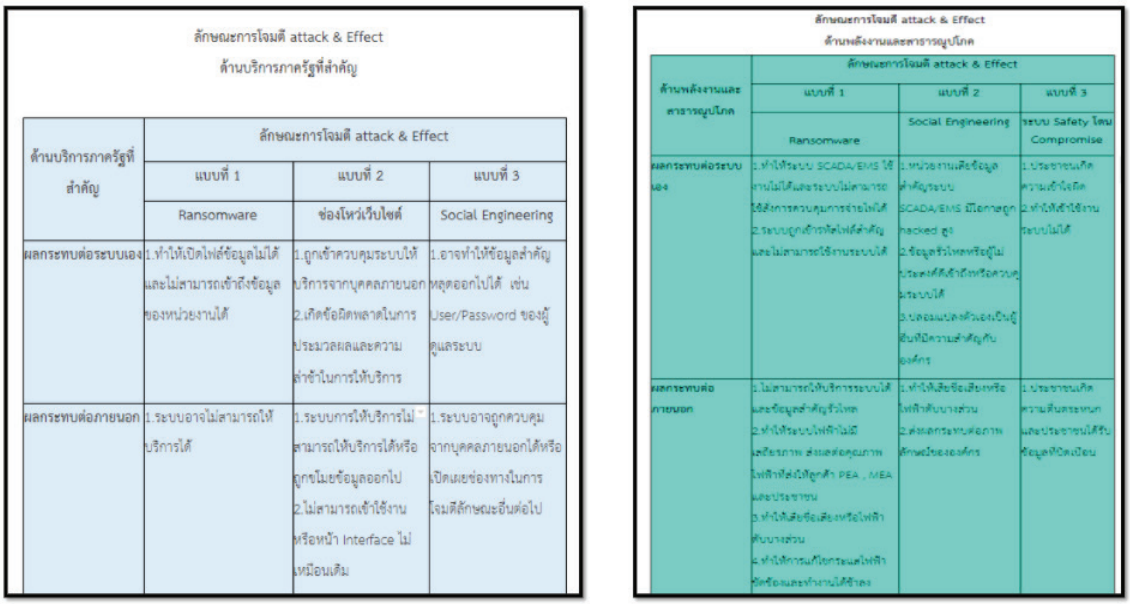
(๒) สถิติภัยคุกคามทางไซเบอร์ระหว่างปี พ.ศ. ๒๕๖๑ - ๒๕๖๔ และระดับความรุนแรงของเหตุการณ์

(๓) เน้นย้ำเรื่องประเภทของโจทย์ฝึก จะต้องสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และ (ร่าง) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ....

๒.๔.๖.๓ ผลการกำหนดประเภทโจทย์ฝึก

รูปที่ ๒-๑๐ ผลการกำหนดประเภทโจทย์ฝึก

๒.๔.๖.๔ ผลการกำหนดลักษณะการโจมตีและผลกระทบ



ลักษณะการโจมตี attack & Effect
ด้านบริการภาครัฐที่สำคัญ

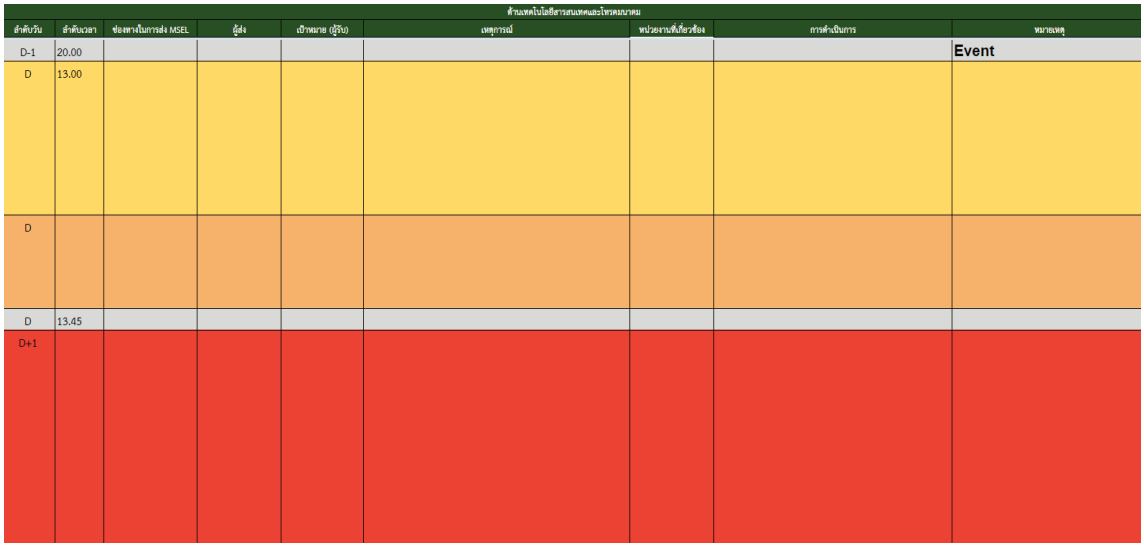
ด้านบริการภาครัฐที่สำคัญ	ลักษณะการโจมตี attack & Effect		
	แบบที่ 1	แบบที่ 2	แบบที่ 3
	Ransomware	ช่องโหว่เว็บไซต์	Social Engineering
ผลกระทบต่อระบบเอง	1.ทำให้เปิดไฟล์ข้อมูลไม่ได้ และไม่สามารถเข้าถึงข้อมูลของหน่วยงานได้	1.ถูกเข้าควบคุมระบบให้บริการจากบุคคลภายนอก 2.เกิดข้อผิดพลาดในการประมวลผลและความล่าช้าในการให้บริการ	1.อาจทำให้ข้อมูลสำคัญหลุดออกไปได้ เช่น User/Password ของผู้ดูแลระบบ
ผลกระทบต่อภายนอก	1.ระบบอาจไม่สามารถให้บริการได้	1.ระบบการให้บริการไม่สามารถให้บริการได้หรือถูกขโมยข้อมูลออกไป 2.ไม่สามารถเข้าใช้งานหรือหน้า Interface ไม่เหมือนเดิม	1.ระบบอาจถูกควบคุมจากบุคคลภายนอกได้หรือเปิดเผยช่องทางในการโจมตีลักษณะอื่นต่อไป

ลักษณะการโจมตี attack & Effect
ด้านพลังงานและสาธารณูปโภค

ด้านพลังงานและสาธารณูปโภค	ลักษณะการโจมตี attack & Effect		
	แบบที่ 1	แบบที่ 2	แบบที่ 3
	Ransomware	Social Engineering	ระบบ Safety โดน Compromise
ผลกระทบต่อระบบเอง	1.ทำให้ระบบ SCADA/EMS ใช้งานไม่ได้และระบบไม่สามารถใช้สำหรับการควบคุมการจ่ายไฟได้ 2.ระบบถูกเข้าทำลายไฟล์สำคัญและไม่สามารถใช้งานระบบได้	1.หน่วยงานเสียข้อมูลสำคัญระบบ SCADA/EMS มีโอกาสถูก hacked สูง 2.ข้อมูลรั่วไหลหรือผู้ไม่ประสงค์ดีเข้าถึงหรือควบคุมระบบได้ 3.บอลแบลคตัวเองเป็นผู้ที่มีความสำคัญกับองค์กร	1.ประชาชนเกิดความเข้าใจผิด 2.ทำให้เข้าใช้งานระบบไม่ได้
ผลกระทบต่อภายนอก	1.ไม่สามารถให้บริการระบบได้และข้อมูลสำคัญรั่วไหล 2.ทำให้ระบบไฟฟ้าไม่มีเสถียรภาพ ส่งผลต่อคุณภาพไฟฟ้าที่ส่งให้ลูกค้า PEA , MEA และประชาชน 3.ทำให้เสียชื่อเสียงหรือไฟฟ้าดับบางส่วน 4.ทำให้การผลิตไฮดรอลไฟฟ้าขัดข้องและทำงานได้ช้าลง	1.ทำให้เสียชื่อเสียงหรือไฟฟ้าดับบางส่วน 2.ส่งผลกระทบต่อภาพลักษณ์ขององค์กร	1.ประชาชนเกิดความตื่นตระหนกและประชาชนได้รับข้อมูลที่ผิดเบือน

รูปที่ ๒-๑๑ ผลการกำหนดลักษณะการโจมตีและผลกระทบ

๒.๔.๖.๕ ตารางประสานสอดคล้อง (MSEL Sync Table)



ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม								
ลำดับวัน	ลำดับเวลา	ช่องทางในการส่ง MSEL	ผู้ส่ง	เป้าหมาย (ผู้รับ)	เหตุการณ์	หน่วยงานที่เกี่ยวข้อง	การดำเนินการ	หมายเหตุ
D-1	20.00							Event
D	13.00							
D								
D	13.45							
D+1								

รูปที่ ๒-๑๒ ตารางประสานสอดคล้อง (MSEL Sync Table)

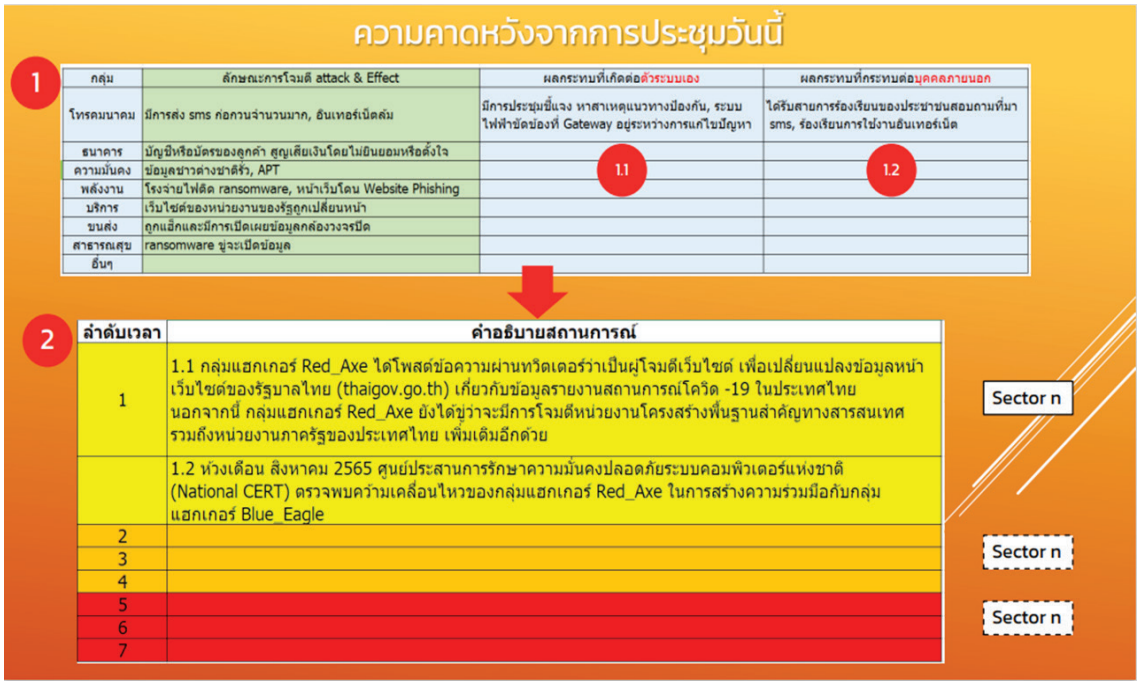
๒.๔.๗ การจัดทำสถานการณ์และโจทย์ฝึก (เพิ่มเติม)

เนื่องจากระยะเวลาที่ไม่เพียงพอต่อการจัดทำสถานการณ์และโจทย์ฝึกในวันที่ ๑๕, ๒๐, ๒๕- ๒๗ ตุลาคม พ.ศ. ๒๕๖๔ ประกอบกับการจัดทำโจทย์ฝึกที่แตกต่างกันในแต่ละ Sector ซึ่งมีความจำเป็นต้องอาศัยผู้เชี่ยวชาญขั้นสูงจากแต่ละ Sector เข้ามาออกแบบและจัดทำโจทย์ฝึกอย่างต่อเนื่อง ทำให้ส่วนควบคุมการฝึกดำเนินการปรับแผนการทำงาน ดังนี้

อาทิตย์	จันทร์	อังคาร	พุธ	พฤหัสบดี	ศุกร์	เสาร์
					๑๕ ๑๐.๓๐ – ๑๒.๐๐ น. จำนวน ๑๔๒ คน	๑๖
๑๗	๑๘	๑๙	๒๐ ๑๐.๓๐ – ๑๒.๐๐ น. จำนวน ๑๒๕ คน	๒๑	๒๒	๒๓
๒๔	๒๕	๒๖ ๐๙.๐๐ – ๑๖.๐๐ น. จำนวน ๗๐ คน	๒๗	๒๘	๒๙	๓๐
๓๑	๑	๒	๓ ๑๒.๐๐ – ๑๖.๓๐ น. จำนวน ๔๐ คน	๔	๕ ๑๓.๓๐ – ๑๖.๓๐ น. จำนวน ๔๓ คน	๖
๗	๘ ๑๒.๓๐ – ๑๗.๓๐ น. จำนวน ๕๐ คน	๙	๑๐ ๑๓.๐๐ – ๑๗.๓๐ น. จำนวน ๕๕ คน	๑๑	๑๒ ๑๓.๐๐ – ๑๗.๓๐ น. จำนวน ๕๒ คน	๑๓
๑๔	๑๕ ๑๓.๐๐ – ๑๗.๓๕ น. จำนวน ๖๐ คน	๑๖	๑๗ ๑๓.๐๐ – ๑๖.๓๐ น. จำนวน ๔๗ คน	๑๘	๑๙ ๑๓.๐๐ – ๑๗.๐๐ น. จำนวน ๓๖ คน	๒๐
๒๑	๒๒ ๑๓.๐๐ – ๑๖.๓๐ น. จำนวน ๔๓ คน	๒๓	๒๔ ๑๒.๔๕ – ๑๗.๐๐ น. จำนวน ๓๘ คน	๒๕	๒๖ ๑๒.๓๐ – ๑๗.๓๐ น. จำนวน ๓๘ คน	๒๗
๒๘	๒๙ ๑๓.๐๐ – ๑๗.๐๐ น. จำนวน ๕๖ คน	๓๐	๑ ๑๓.๑๕ – ๑๗.๑๕ น. จำนวน ๕๓ คน	๒	๓ ๑๓.๒๐ – ๑๖.๓๐ น. จำนวน ๔๖ คน	๔
๕	๖	๗ ๑๓.๓๐ – ๑๗.๐๐ น. จำนวน ๔๕ คน	๘	๙ ๑๓.๓๐ – ๑๗.๐๐ น. จำนวน ๖๓ คน	๑๐	๑๑
๑๒	๑๓ ๑๓.๐๐ – ๑๖.๒๐ น. จำนวน ๖๕ คน	๑๔	๑๕ ๑๓.๐๐ – ๑๗.๔๕ น. จำนวน ๗๐ คน	๑๖	๑๗ ๑๒.๒๓ – ๑๖.๔๖ น. จำนวน ๖๘ คน	๑๘
๑๙	๒๐ ๑๒.๐๖ – ๑๖.๔๙ จำนวน ๙๒ คน					

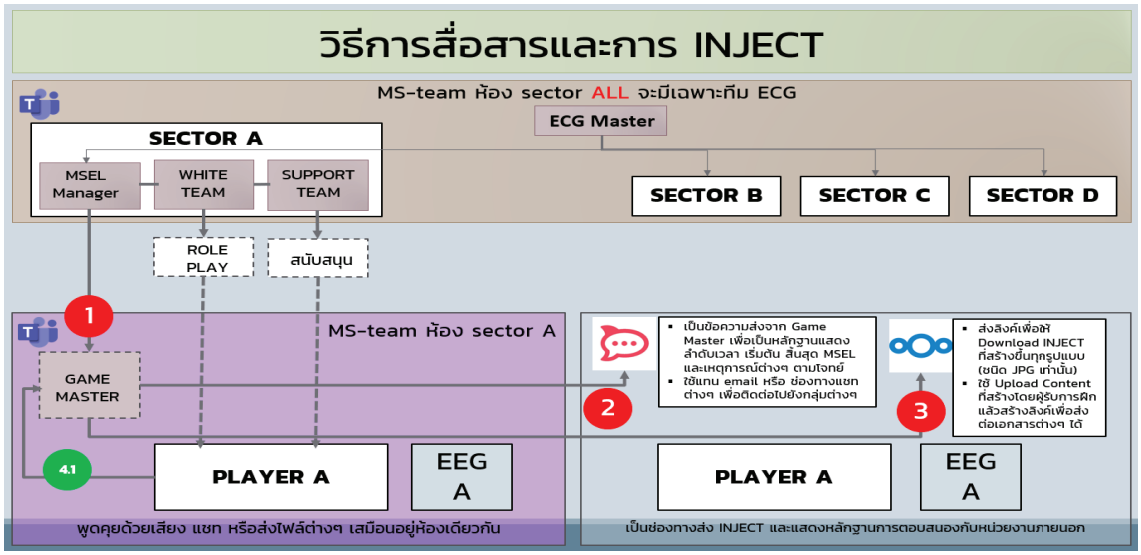
รูปที่ ๒-๑๓ การจัดทำสถานการณ์และโจทย์ฝึก (เพิ่มเติม)

๒.๔.๗.๑ กิจกรรมการกำหนดผลกระทบข้ามหน่วยงาน



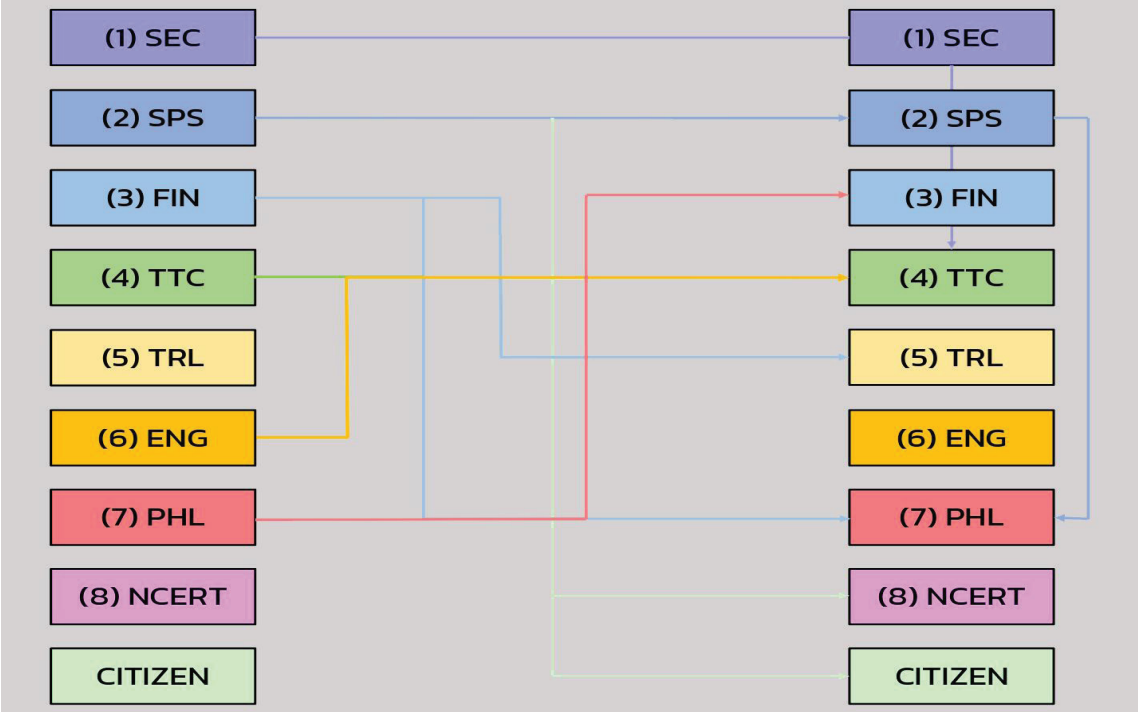
รูปที่ ๒-๑๔ กิจกรรมการกำหนดผลกระทบข้ามหน่วยงาน

๒.๔.๗.๒ วิธีการสื่อสารและการส่งโจทย์ฝึก (Inject)



รูปที่ ๒-๑๕ วิธีการสื่อสารและการส่งโจทย์ฝึก (Inject)

๒.๔.๗.๓ ผลกระทบข้าม Sector



รูปที่ ๒-๑๖ ผลกระทบข้าม Sector

๒.๔.๘ ผลผลิตจากการประชุม (เพิ่มเติม)

ลำดับ	DAY	TIME	แล้วเสร็จ	(1) SEC	(2) SPS	(3) FIN	(4) TTC	(5) TRL			(6) ENG	(7) PHL	(8) NCERT
								สปค.	รฟท.	รฟม.			
1	1 ช	10.30 - 11.00		SEC1.1 SEC1.2	SPS1.1	FIN1.1	TTC-1.1-1 | TTC-1.1-2 | TTC-1.1-3 | TTC-1.1-4	TRL1.1		TRL1.0M TRL1.1M	ENG1.1	PHL1.1	
2	1 ช	11.00 – 11.30		SEC1.3	SPS1.2	FIN1.1	TTC-1.1-1 | TTC-1.1-2 | TTC-1.1-3 | TTC-1.1-4 | TTC-1.2	TRL1.2		TRL1.2M	ENG1.1	PHL1.2	
3	1 ช	11.30 - 12.00		SEC1.4	SPS1.2	FIN1.2	TTC-1.2	TRL1.3		TRL1.3M TRL1.4M	ENG2.1	PHL1.3	
4	1 บ	13.00 – 13.30		SEC1.5	-	FIN1.3	TTC-1.2		TRL1.4	TRL1.5M	ENG2.1	PHL1.4	
5	1 บ	13.30 – 14.00		SEC1.6	SPS1.3	FIN1.4	TTC-1.3		TRL1.5	TRL1.6M TRL1.7M	ENG2.2	PHL1.5	
6	1 บ	14.00 – 14.30		SEC1.7	-	FIN1.5	TTC-1.3		TRL1.6	TRL2.0M TRL2.1M - TRL 2.1.1M	ENG2.2	PHL1.6	
7	1 บ	14.30 - 15.00		SEC1.8	SPS1.4	FIN1.5			TRL1.7	TRL2.2M	ENG2.2	-	
8	2 ช	09.00 – 09.30		SEC2.1	-	FIN2.1	TTC-2.1		TRL2.1	FIN2.1	ENG2.3	FIN2.1	
9	2 ช	09.30 – 10.00		SEC2.2	SPS2.1	FIN2.1	TTC-2.1		TRL2.2	TRL 3.0M - 3.0.1	ENG2.3	PHL2.1	
10	2 ช	10.00 -10.30		SEC2.3	SPS2.1	FIN2.1	TTC-2.2-2		TRL2.3	TRL 3.1M	ENG2.4	PHL2.2	
11	2 ช	10.30 - 11.00		SEC2.3	SPS2.2	FIN2.2	TTC-2.2-2		TRL2.4	TRL 3.2M	ENG2.4	PHL2.3	
12	2 ช	11.00 – 11.30		SEC2.4	SPS2.2	FIN2.3	TTC-2.2-2		TRL2.5	ENG2.5	ENG2.5	-	
13	2 ช	11.30 - 12.00		SEC2.4	SPS2.3	FIN2.3	TTC-2.2-2		TRL3.1		ENG2.5	-	
14	2 บ	13.00 – 13.30		SEC2.5	-	FIN2.4	TTC-2.3-1.1 | TTC-2.3-1.2 | TTC-2.3-1.3 | TTC-2.3-1.4 | TTC-2.3-2		TRL 3.2 TRL3.3 TRL3.4		ENG2.6	PHL2.4	

รูปที่ ๒-๑๗ รายการโจทย์ฝึก (MSEL Sync Table)

๒.๔.๘.๑ รายการโจทย์ฝึก (MSEL Sync Table) สรุปได้ดังนี้

(๑) ด้านความมั่นคงของรัฐ มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๗ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวงผ่านทางเว็บไซต์ (Web Phishing)
- ข้อมูลรั่วไหล (Data Leak)
- การหลอกลวงโดยใช้อีเมล (Email Phishing)
- การโจมตีโดยปฏิเสธการให้บริการ (Distributed Denial-of-Service : DDoS)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๒) ด้านบริการภาครัฐที่สำคัญ มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๓ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การถูกโจมตีหน้าเว็บ (Web Defacement)
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๓) ด้านการเงินการธนาคาร มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๕ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวงโดยใช้อีเมล (Email Phishing)
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๔ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวง (Phishing) โดยใช้ MalDoc หรือ Malicious URL
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๕) ด้านการขนส่งและโลจิสติกส์ มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๕ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวงโดยใช้อีเมล (Email Phishing)
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๖) ด้านพลังงานและสาธารณูปโภค มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๐ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวง (Phishing) โดยใช้ MalDoc หรือ Malicious URL
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

(๗) ด้านสาธารณสุข มีจำนวนโจทย์ฝึกที่ใช้ในห้วงการฝึกทั้งสิ้น ๑๗ ข้อ ประกอบด้วยลักษณะของโจทย์ฝึก (Inject Type) ดังนี้

- การหลอกลวง (Phishing) โดยใช้ MalDoc หรือ Malicious URL
- ข้อมูลรั่วไหล (Data Leak)
- มัลแวร์เรียกค่าไถ่ (Ransomware)

๒.๔.๘.๒ ตาราง MSEL log

ลำดับ	DAY	TIME	แล้วเสร็จ	(1) SEC	(2) SPS	(3) FIN	(4) TTC	(5) TRL			(6) ENG	(7) PHL	(8) NCERT
								สป.ค.	รพท.	รพช.			
1	1 ช	10.30 - 11.00		SEC1.1 SEC1.2	SPS1.1	FIN1.1	TTC-1.1-1 | TTC-1.1-2 | TTC-1.1-3 | TTC-1.1-4	TRL1.1		TRL1.0M TRL1.1M	ENG1.1	PHL1.1	
2	1 ช	11.00 – 11.30		SEC1.3	SPS1.2	FIN1.1	TTC-1.1-1 | TTC-1.1-2 | TTC-1.1-3 | TTC-1.1-4 | TTC-1.2	TRL1.2		TRL1.2M	ENG1.1	PHL1.2	
3	1 ช	11.30 - 12.00		SEC1.4	SPS1.2	FIN1.2	TTC-1.2	TRL1.3		TRL1.3M TRL1.4M	ENG2.1	PHL1.3	
4	1 บ	13.00 – 13.30		SEC1.5	-	FIN1.3	TTC-1.2		TRL1.4	TRL1.5M	ENG2.1	PHL1.4	
5	1 บ	13.30 – 14.00		SEC1.6	SPS1.3	FIN1.4	TTC-1.3		TRL1.5	TRL1.6M TRL1.7M	ENG2.2	PHL1.5	
6	1 บ	14.00 – 14.30		SEC1.7	-	FIN1.5	TTC-1.3		TRL1.6	TRL2.0M TRL2.1M - TRL 2.1.1M	ENG2.2	PHL1.6	
7	1 บ	14.30 - 15.00		SEC1.8	SPS1.4	FIN1.5			TRL1.7	TRL2.2M	ENG2.2	-	
8	2 ช	09.00 – 09.30		SEC2.1	-	FIN2.1	TTC-2.1		TRL2.1	FIN2.1	ENG2.3	FIN2.1	
9	2 ช	09.30 – 10.00		SEC2.2	SPS2.1	FIN2.1	TTC-2.1		TRL2.2	TRL 3.0M - 3.0.1	ENG2.3	PHL2.1	
10	2 ช	10.00 -10.30		SEC2.3	SPS2.1	FIN2.1	TTC-2.2-2		TRL2.3	TRL 3.1M	ENG2.4	PHL2.2	
11	2 ช	10.30 - 11.00		SEC2.3	SPS2.2	FIN2.2	TTC-2.2-2		TRL2.4	TRL 3.2M	ENG2.4	PHL2.3	
12	2 ช	11.00 – 11.30		SEC2.4	SPS2.2	FIN2.3	TTC-2.2-2		TRL2.5	ENG2.5	ENG2.5	-	
13	2 ช	11.30 - 12.00		SEC2.4	SPS2.3	FIN2.3	TTC-2.2-2		TRL3.1		ENG2.5	-	
14	2 บ	13.00 – 13.30		SEC2.5	-	FIN2.4	TTC-2.3-1.1 | TTC-2.3-1.2 | TTC-2.3-1.3 | TTC-2.3-1.4 | TTC-2.3-2			TRL 3.2 TRL3.3 TRL3.4		PHL2.4	
15	2 บ	13.30 – 14.00		SEC2.5	SPS2.4	FIN2.4	TTC-2.3-1.1 | TTC-2.3-1.2 | TTC-2.3-1.3 | TTC-2.3-1.4 | TTC-2.3-2 | TTC-2.3-3 | TTC-2.3-4					PHL2.5	
16	2 บ	14.00 – 14.30		SEC2.6	SPS2.4	FIN2.5	TTC-2.4 | TTC-2.5-1 | TTC-2.5-2 | TTC-2.5-3 | TTC-2.5-4 | TTC-2.6 | TTC-2.7					PHL2.6	
17	2 บ	14.30 - 15.00		SEC2.6	SPS2.5	FIN2.5 FIN2.6	TTC-2.4 | TTC-2.5-1 | TTC-2.5-2 | TTC-2.5-3 | TTC-2.5-4 | TTC-2.6 | TTC-2.7		TRL 2.6			PHL2.7	
18	3 ช	09.00 – 09.30		SEC3.1	SPS3.1	FIN3.1.1	TTC-3.1-1 | TTC-3.1-2 | TTC-3.2 | TTC-3.4-1.1 | TTC-3.4-1.2 | TTC-3.4-2			TRL3.1		PHL3.1	

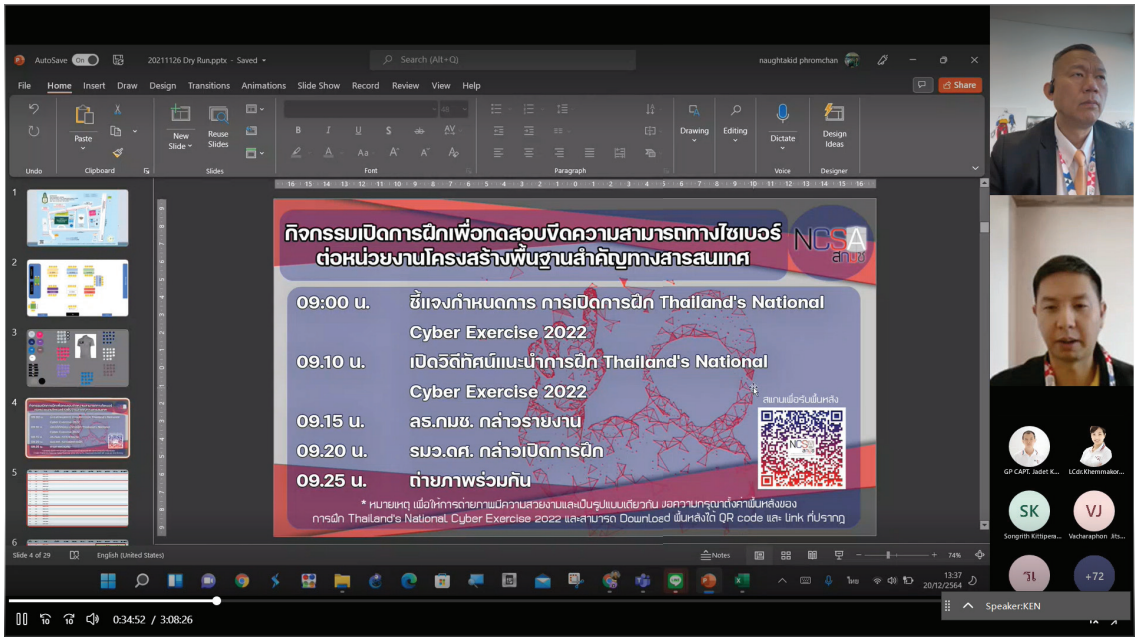
รูปที่ ๒-๑๘ ตาราง MSEL log

๒.๔.๘.๓ คาบการปล่อยโจทย์ฝึก

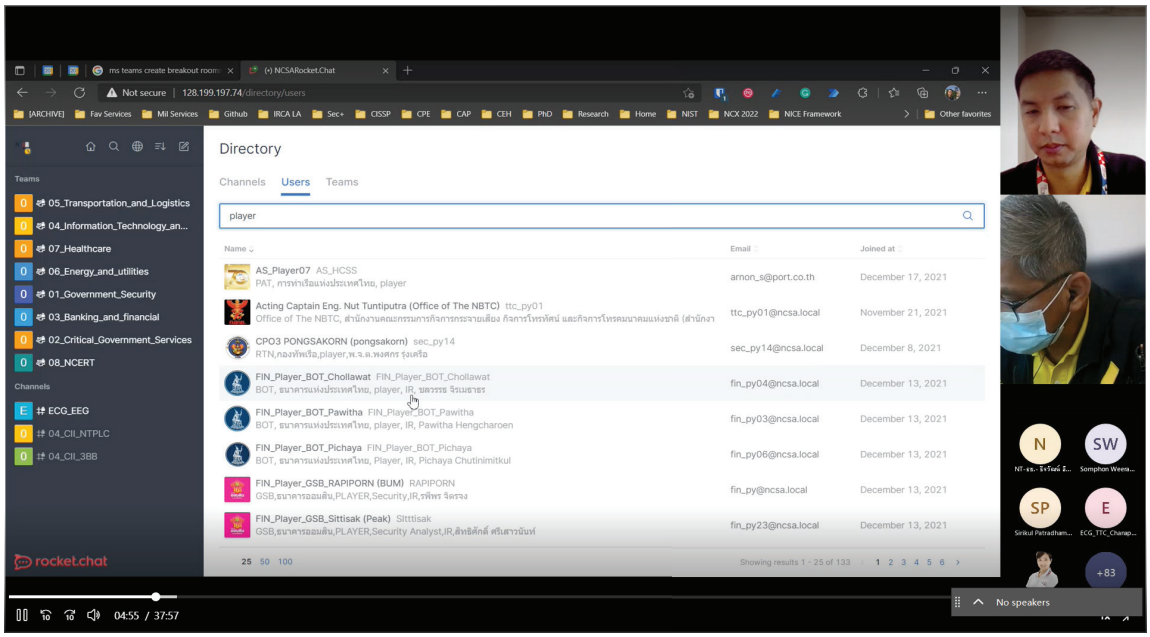
ลำดับ	DAY	TIME	แล้วเสร็จ	(1) SEC	(2) SPS	(3) FIN	(4) TTC	(5) TRL	(6) ENG	(7) PHL	(8) NCERT
1	1 ช	1030 - 1100						พุธ 22 ธ.ค.64			
2	1 ช	1100 – 1130									
3	1 ช	1130 - 1200									
4	1 บ	1300 – 1330									
5	1 บ	1330 – 1400						พุธ 22 ธ.ค.64			
6	1 บ	1400 – 1430									
7	1 บ	1430 - 1500									
8	2 ช	0900 – 0930									
9	2 ช	0930 – 1000									
10	2 ช	1000 -1030						พฤหัสบดี 23 ธ.ค.64			
11	2 ช	1030 - 1100									
12	2 ช	1100 – 1130									
13	2 ช	1130 - 1200									
14	2 บ	1300 – 1330									
15	2 บ	1330 – 1400						พฤหัสบดี 23 ธ.ค.64			
16	2 บ	1400 – 1430									
17	2 บ	1430 - 1500									
18	2 ช	0900 – 0930									
19	2 ช	0930 – 1000						ศุกร์ 24 ธ.ค.64			
20	2 ช	1000 -1030									
21	2 ช	1030 - 1100									

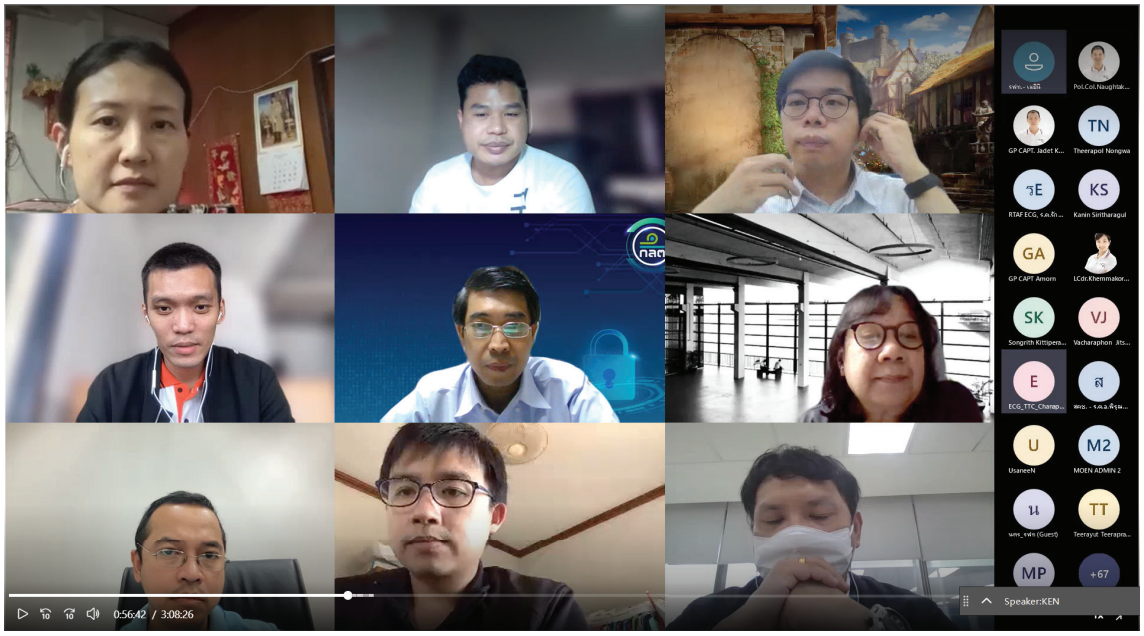
รูปที่ ๒-๑๙ คาบการปล่อยโจทย์ฝึก

๒.๔.๘.๔ การทดสอบก่อนการฝึก (Dry Run)



รูปที่ ๒-๒๐ การทดสอบก่อนการฝึก (Dry Run)





รูปที่ ๒-๒๐ การทดสอบก่อนการฝึก (Dry Run)

๒.๔.๘.๕ ลำดับสถานการณ์ประจำวัน รายละเอียดตามบทที่ ๔ ประกอบด้วย

(๑) สถานการณ์ประจำวันที่ ๒๒ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

(๒) สถานการณ์ประจำวันที่ ๒๓ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

(๓) สถานการณ์ประจำวันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

๒.๔.๘.๖ จำนวนผู้แทนหน่วยงานเข้าร่วมเป็นส่วนควบคุมการฝึก (ECG) สามารถจำแนกได้ตามบทบาทหน้าที่ รายละเอียดตามผนวก ง ๓ สรุปได้ ดังนี้

บทบาทหน้าที่	จำนวน (คน)
Game Master	๑๙
MSEL Manager	๓๑
White Team	๓๗
Support Team	๒๖
Co - Agent	๘

ตารางที่ ๒-๔ ตารางจำนวนผู้แทนหน่วยงานเข้าร่วมเป็นส่วนควบคุมการฝึก (ECG)

๒.๔.๙ การประชุมส่วนประเมินผล (Exercise Evaluation Group : EEG)

รูปที่ ๒-๒๑ การประชุมส่วนประเมินผล (Exercise Evaluation Group : EEG)

๒.๔.๙.๑ วัตถุประสงค์การประชุม

เพื่อจัดทำแนวทางการประเมินและแบบประเมิน (Checklist) ซึ่งจะทำให้ผู้เข้ารับการฝึกได้รับทราบถึงผลการประเมินพร้อมข้อเสนอแนะในการปรับปรุงแก้ไข ภายหลังจากการแก้ไขปัญหาตามโจทย์ฝึกเรียบร้อยแล้ว

๒.๔.๙.๒ วันและเวลาการประชุม

(๑) วันที่ ๔ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ - ๑๒.๐๐ น.

(๒) วันที่ ๑๑ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ - ๑๒.๐๐ น.

(๓) วันที่ ๑๘ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ - ๑๒.๐๐ น.

๒.๔.๙.๓ สถานที่การประชุม

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๒.๔.๙.๔ ผู้เข้าร่วมการประชุม

ผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแล ๑๙ หน่วยงาน รายชื่อตามผนวก ง ๓

๒.๔.๙.๕ สาระสำคัญของการประชุม

(๑) ข้อตกลงเรื่องการแลกเปลี่ยนข้อมูล (Traffic Light Protocol : TLP) ส่วนประเมินผลได้รับทราบและตกลงร่วมกันว่า จะมีระดับ TLP : RED คือ ห้ามเปิดเผยข้อมูลออกไปนอกส่วนประเมินผลและจำกัดการเปิดเผยข้อมูลเฉพาะผู้ที่เกี่ยวข้องเท่านั้น

(๒) แนวทางการจัดทำและพัฒนาแบบประเมิน (Checklist) ตามแนวทางของ MITRE Cyber Exercise Playbook ดังนี้

(๒.๑) กำหนดทีมประเมิน โดยแบ่งกลุ่มผู้แทนหน่วยงานควบคุมหรือกำกับดูแลตาม Sector จำนวน ๗ Sector ทั้งนี้ ผู้ประเมินไม่ควรน้อยกว่า ๓ คน/Sector

(๒.๒) จัดทำและพัฒนาแบบประเมิน (Checklist) ตามแนวทางของ MITRE Cyber Exercise Playbook

(๒.๓) ทดสอบแบบประเมินร่วมกับส่วนควบคุมการฝึก (ECG) เนื่องจากแบบประเมินแต่ละชุดจะเชื่อมโยงกับโจทย์ฝึก (Inject) แต่ละข้อ ที่จัดทำโดยส่วนควบคุมการฝึก (ECG)

(๒.๔) ทดสอบแบบประเมินร่วมกับผู้ประเมินจากหน่วยงานควบคุมหรือกำกับดูแล

(๒.๕) ดำเนินการประเมินผลให้มีความสอดคล้องกับวัตถุประสงค์การฝึก

(๒.๖) ตัวแทนจากหน่วยงานควบคุมหรือกำกับดูแลที่มาจาก Sector ใดจะเข้าสังเกตการณ์เฉพาะผู้รับการฝึกใน Sector นั้น เท่านั้น

(๒.๗) ช่วง Daily Hotwash กำหนดให้ผู้ประเมินแสดงความเห็นตามผลการประเมินใน Checklist

Cyber Exercise Playbook

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.
Approved for Public Release; Distribution Unlimited. 14-3929
This technical data was produced for the U.S. Government under Contract No. W15P7T-13-C-A802, and is subject to the Rights in Technical Data-Noncommercial Items clause at DFARS 252.227-7013 (NOV 1995).

©2014 The MITRE Corporation. All rights reserved.

Jason Kick

November 2014

MP140714
Wiesbaden, Germany

MITRE

Appendix H: Sample Inject Observation Form

This appendix shows a sample observation form outlining the important types of information to collect for each event/inject executed during an exercise. These are created prior to the exercise and utilized during the exercise to assist observers in accurately assessing the training audience's responses to exercise injects.

INJECT OBSERVER FORM[1] CONTROL AND OBSERVER EYES ONLY

Inject Number: IA-2
Inject Title: NETWORK VIRUS
Inject Date: 25JUN2014
START TIME (Local): _____
COMPLETE TIME (Local) _____

Observer Name: Jane Doe | Inject Delivered Via: CARD or ELECTRONIC | Target Group/Unit/Position: Unit A

Inject description, ASSUMPTIONS and references:
Your antivirus SW has just alerted a virus. Take appropriate actions in accordance with standard policies and procedures. Notify the Exercise Observer when you have completed all required actions.

Assumptions: Simulated virus triggers user anti virus software on device

References: (Source or document that states required actions)
Cyber Ops & IA; Cyber Incident Management Guide; (page 27-28)

Expectation:
"(e) Each virus incident must be reported as soon as possible to Cyber Security Team. The Cyber Security Team will then issue a virus warning to the other units the unit's appointed senior communications officers if necessary.

Assessment of training audience response: *CIRCLE ONE*

COMPLETED: (3) PART COMPLETE: (2) INCOMPLETE: (1) N/A (Explain Below):____

Was event documented in Master station log? Yes / No
Was incident response form completed? Yes / No

Observation and notes:

[1] Inject observer form adapted from the Africa Endeavor 2013 Handbook

34

SAMPLE

รูปที่ ๒-๒๒ การจัดทำแบบประเมิน

๒.๔.๑๐ การประชุมส่วนประเมินผล (เพิ่มเติม)

เนื่องจากระยะเวลาที่ไม่เพียงพอต่อการจัดทำแบบประเมินการฝึก ในวันที่ ๔, ๑๑ และ ๑๘ พฤศจิกายน พ.ศ. ๒๕๖๔ เนื่องจากแบบประเมินแต่ละชุดจะเชื่อมโยงกับโจทย์ฝึก (Inject) แต่ละข้อที่จัดทำโดยส่วนควบคุมการฝึก (ECG) ส่งผลให้ส่วนประเมินผลดำเนินการปรับแผนการทำงาน ดังนี้

อาทิตย์	จันทร์	อังคาร	พุธ	พฤหัสบดี	ศุกร์	เสาร์
	๑	๒	๓	๔ ๐๙.๐๐ – ๑๒.๐๐ น. จำนวน ๑๒ คน	๕	๖
๗	๘	๙	๑๐	๑๑ ๐๙.๐๐ – ๑๑.๓๐ น. จำนวน ๑๕ คน	๑๒	๑๓
๑๔	๑๕	๑๖	๑๗	๑๘ ๐๙.๓๐ – ๑๑.๓๐ น. จำนวน ๑๒ คน	๑๙ ๑๓.๐๐ – ๑๗.๐๐ น. จำนวน ๑๔ คน	๒๐
๒๑	๒๒ ๑๓.๐๐ – ๑๖.๓๐ น. จำนวน ๑๒ คน	๒๓	๒๔ ๑๒.๔๕ – ๑๗.๐๐ น. จำนวน ๑๓ คน	๒๕	๒๖ ๑๒.๓๐ – ๑๗.๓๐ น. จำนวน ๑๕ คน	๒๗
๒๘	๒๙ ๑๓.๐๐ – ๑๗.๐๐ น. จำนวน ๑๐ คน	๓๐	๑ ๑๓.๑๕ – ๑๗.๑๕ น. จำนวน ๑๒ คน	๒	๓ ๑๓.๒๐ – ๑๖.๓๐ น. จำนวน ๑๔ คน	๔
๕	๖	๗ ๑๓.๓๐ – ๑๗.๐๐ น. จำนวน ๑๕ คน	๘	๙ ๑๓.๓๐ – ๑๗.๐๐ น. จำนวน ๑๒ คน	๑๐	๑๑
๑๒	๑๓ ๑๓.๐๐ – ๑๖.๒๐ น. จำนวน ๑๐ คน	๑๔	๑๕ ๑๓.๐๐ – ๑๗.๔๕ น. จำนวน ๑๘ คน	๑๖	๑๗ ๑๒.๒๓ – ๑๖.๔๖ น. จำนวน ๒๒ คน	๑๘
๑๙	๒๐ ๑๒.๐๖ – ๑๖.๔๙ จำนวน ๒๓ คน					

รูปที่ ๒-๒๓ การประชุมส่วนประเมินผล (เพิ่มเติม)

๒.๔.๑๐.๑ ผลผลิตจากการประชุม

(๑) แบบประเมิน (Checklist)

แบบฟอร์มผู้สังเกตการณ์ Inject **สำหรับควบคุมและเฝ้าสังเกตการณ์เท่านั้น**

หมายเลข Inject:_____ วันที่ Inject:_____
ชื่อ Inject: _____ เริ่มเวลา: _____
สิ้นสุดเวลา: _____

ชื่อผู้สังเกตการณ์:_____ Inject ผ่าน:_____
เป้าหมาย (กลุ่ม/หน่วย/ตำแหน่ง):
_____ _____

รายละเอียด, เอกสารอ้างอิง และผลที่คาดหวัง :

รายละเอียด_____
_____
_____
_____
_____

เอกสารอ้างอิง: (แหล่งที่มาหรือเอกสารที่ระบุการดำเนินการที่จำเป็น)_____
_____

ผลที่คาดหวัง:_____
_____

การประเมินผู้เข้าอบรม: ***เลือก 1 หัวข้อ***

☐ **สำเร็จ : (3)** ☐ **สำเร็จเพียงบางส่วน: (2)** ☐ **ไม่สำเร็จ: (1)**

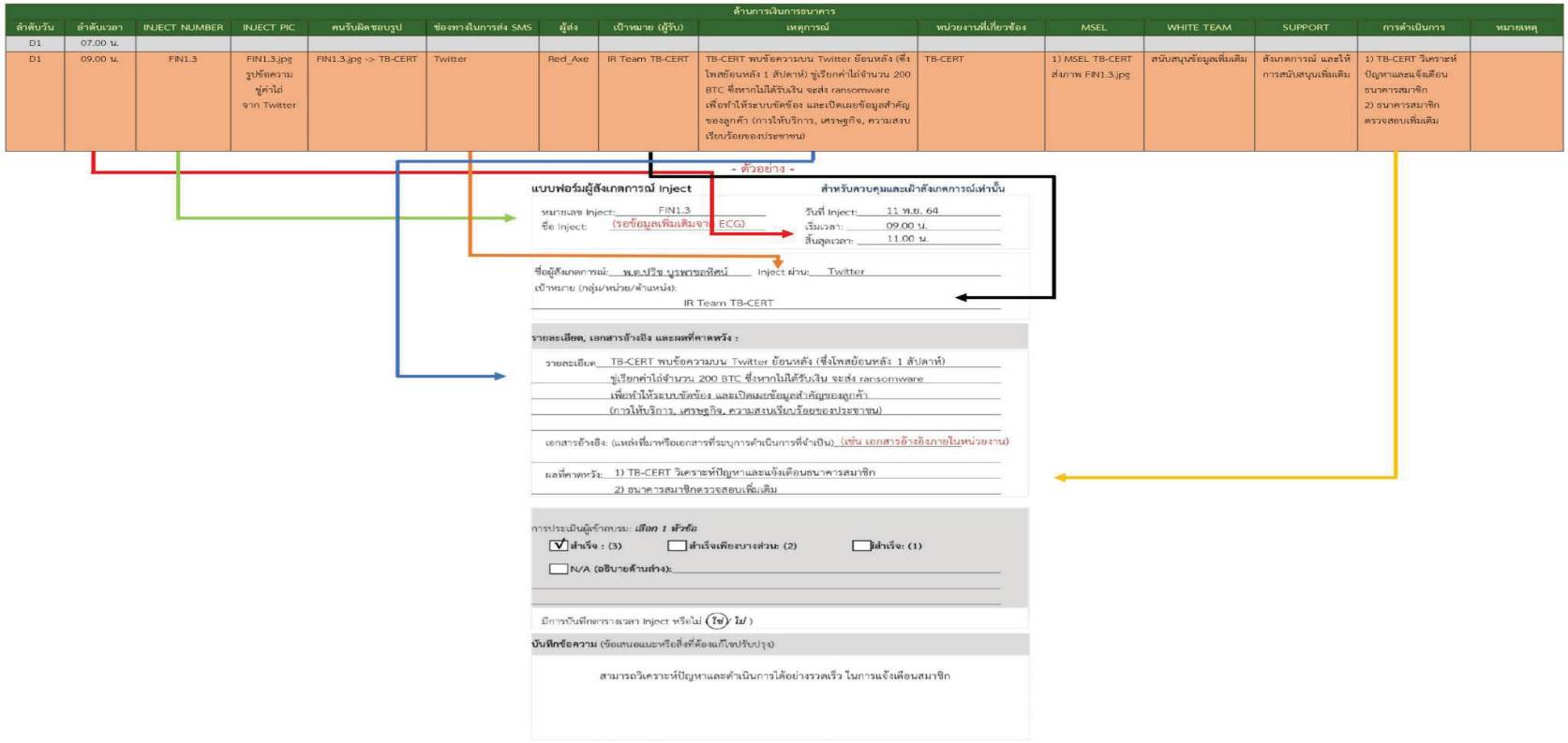
☐ **N/A (อธิบายด้านล่าง):**_____
_____
_____

มีการบันทึกตารางเวลา Inject หรือไม่ (***ใช่*** / ***ไม่***)

บันทึกข้อความ (ข้อเสนอแนะหรือสิ่งที่ต้องแก้ไขปรับปรุง)

รูปที่ ๒-๒๔ แบบประเมิน (Checklist)

(๒) การตรวจสอบแบบประเมินกับทีม ECG



ด้านการเงินการธนาคาร														
ลำดับวัน	ลำดับเวลา	INJECT NUMBER	INJECT PIC	คนรับผิดชอบรูป	ช่องทางในการส่ง SMS	ผู้ส่ง	เป้าหมาย (ผู้รับ)	เหตุการณ์	หน่วยงานที่เกี่ยวข้อง	MSEL	WHITE TEAM	SUPPORT	การดำเนินการ	หมายเหตุ
D1	07.00 น.													
D1	09.00 น.	FIN1.3	FIN1.3.jpg รูปข้อความขู่ค่าไถ่ จาก Twitter	FIN1.3.jpg -> TB-CERT	Twitter	Red_Axe	IR Team TB-CERT	TB-CERT พบข้อความบน Twitter ย้อนหลัง (ซึ่งโพสย้อนหลัง 1 สัปดาห์) ขู่เรียกค่าไถ่จำนวน 200 BTC ซึ่งหากไม่ได้รับเงิน จะส่ง ransomware เพื่อทำให้ระบบขัดข้อง และเปิดเผยข้อมูลสำคัญของลูกค้า (การให้บริการ, เศรษฐกิจ, ความสงบเรียบร้อยของประชาชน)	TB-CERT	1) MSEL TB-CERT ส่งภาพ FIN1.3.jpg	สนับสนุนข้อมูลเพิ่มเติม	สังเกตการณ์ และให้การสนับสนุนเพิ่มเติม	1) TB-CERT วิเคราะห์ปัญหาและแจ้งเตือนธนาคารสมาชิก 2) ธนาคารสมาชิกตรวจสอบเพิ่มเติม	

รูปที่ ๒-๒๕ การตรวจสอบแบบประเมินกับทีม ECG

บทที่ ๓
การฝึกเตรียมการ

บทที่ ๓
การฝึกเตรียมการ

การฝึกเตรียมการ (Pre-exercise) เป็นกิจกรรมการอบรมเพื่อเตรียมความพร้อมให้กับผู้เข้ารับการฝึกก่อนที่จะเข้าสู่กิจกรรมการดำเนินการฝึก (Exercise Execution) ซึ่งมีสภาพแวดล้อมที่แตกต่างจากสภาพแวดล้อมในหน่วยงานของผู้เข้ารับการฝึก จนอาจทำให้เกิดความไม่คุ้นเคยหรือความไม่เข้าใจอย่างเพียงพอ จนอาจส่งผลกระทบให้ผู้รับการฝึกไม่สามารถได้รับประโยชน์จากการดำเนินการฝึกอย่างเต็มที่ตามผลลัพธ์ที่คาดหวัง

๓.๑ วัตถุประสงค์การฝึกเตรียมการ

เพื่อให้ผู้เข้ารับการฝึกจาก หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความพร้อมในด้านความรู้และทักษะพื้นฐาน ที่จำเป็นต้องใช้ในกิจกรรมการดำเนินการฝึก (Exercise Execution) ซึ่งจะทำให้ผู้รับการฝึกได้รับประโยชน์จากการดำเนินการฝึกอย่างเต็มที่

๓.๒ สถานที่การฝึกเตรียมการ

จัดการประชุมแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

๓.๓ ผู้เข้าร่วมการฝึกเตรียมการ

ประกอบด้วย ผู้แทนจากหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง (รายละเอียดตามข้อ ๓.๔)

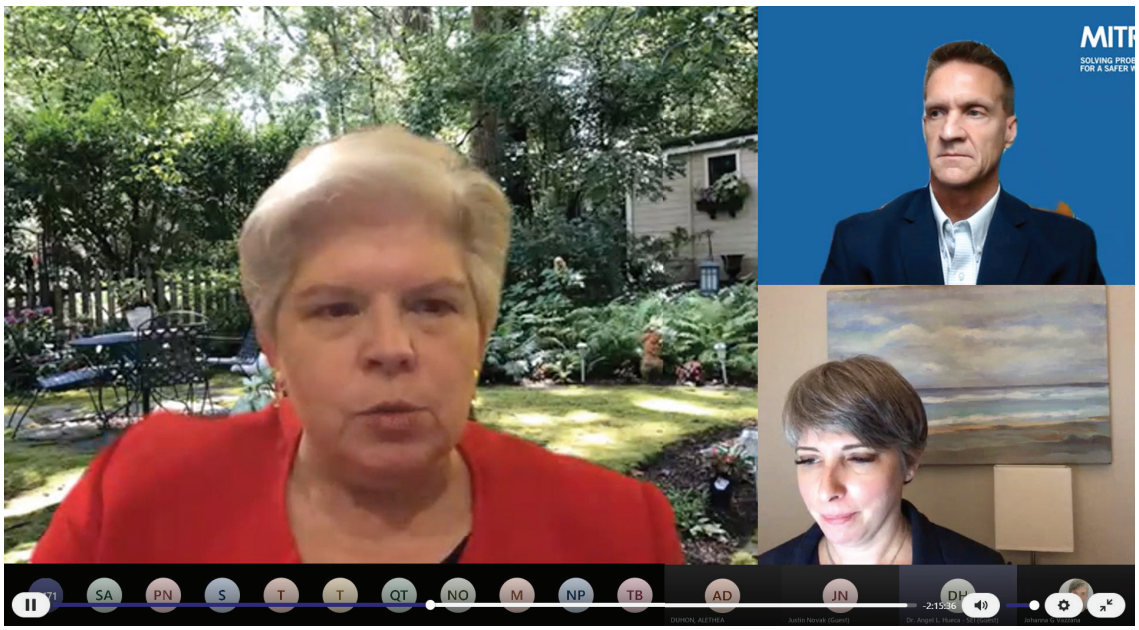
๓.๔ หัวข้อการฝึกเตรียมการ

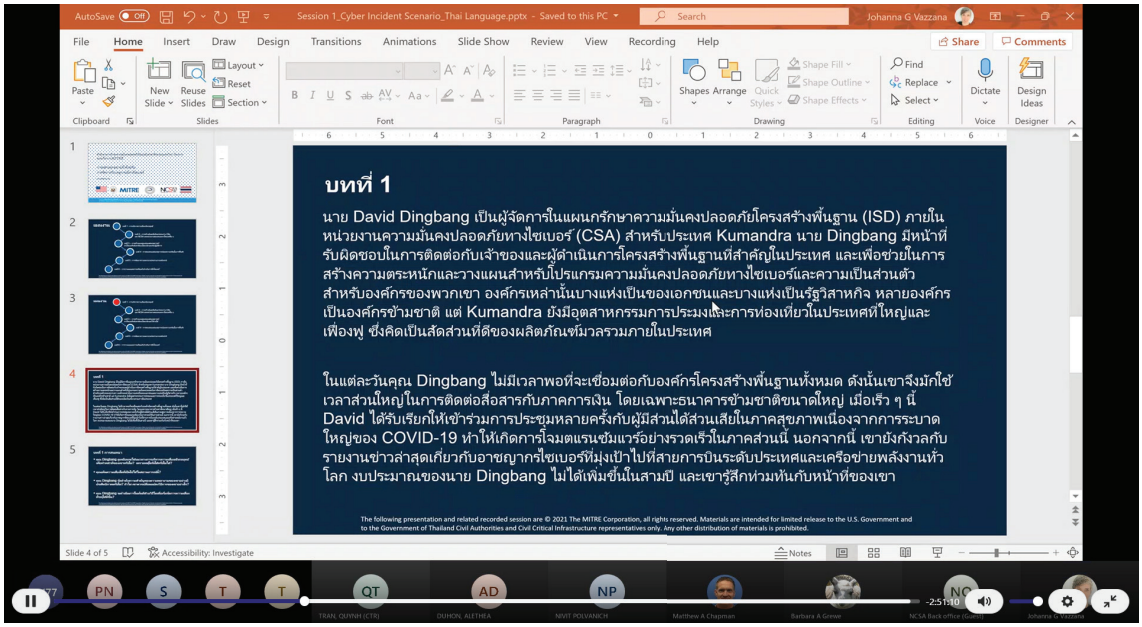
ประกอบด้วย ๗ หัวข้อการอบรม ดังนี้

รูปที่ ๓-๑ หัวข้อการฝึกเตรียมการ

๓.๔.๑ World Class Cyber Security Practices by MITRE/CISA/SEI โดย Barbara Grewe/ Joanna Vazzana/ Matthew Chapman/ Selam Kidane/ Robert Briggs

รูปที่ ๓-๒ การอบรม World Class Cyber Security Practices by MITRE/CISA/SEI





รูปที่ ๓-๒ การอบรม World Class Cyber Security Practices by MITRE/CISA/SEI

๓.๔.๑.๑ เนื้อหาการอบรม ประกอบด้วย

(๑) Strategic risk management

(๒) Building strong bonds between CII and NCSA and other cyber response entities

(๓) Creating a dynamic and functional national cyber incident response plan

(๔) Incident response and resiliency readiness

(๕) Development of a national coordination center

(๖) The cyber exercise playbook-planning and preparing for cyber exercises

๓.๔.๑.๒ วันและเวลาการอบรม

วันที่ ๙ - ๑๑ และ ๑๖ - ๑๘ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ - ๑๒.๐๐ น.

๓.๔.๑.๓ กลุ่มเป้าหมาย

ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐาน ทั้งในระดับบริหาร และระดับปฏิบัติ

๓.๔.๑.๔ รายละเอียดหลักสูตร

ระดับปานกลาง (Intermediate) เนื้อหาเป็นแบบ ๑ หัวข้อ ต่อ ๑ วัน

๓.๔.๑.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ

(๑) วันที่ ๙ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๓ คน

(๒) วันที่ ๑๐ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๔ คน

(๓) วันที่ ๑๑ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๒ คน

(๔) วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๕ คน

(๕) วันที่ ๑๗ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๓ คน

(๖) วันที่ ๑๘ ตุลาคม พ.ศ. ๒๕๖๔ จำนวน ๑๕๒ คน

๓.๔.๑.๖ ความรู้และทักษะที่จำเป็น

(๑) มีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อาทิ การบริหารความเสี่ยงด้านไซเบอร์ การรับมือกับภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ เป็นต้น

(๒) มีความรู้และความสามารถทางด้านภาษาอังกฤษในระดับพื้นฐาน

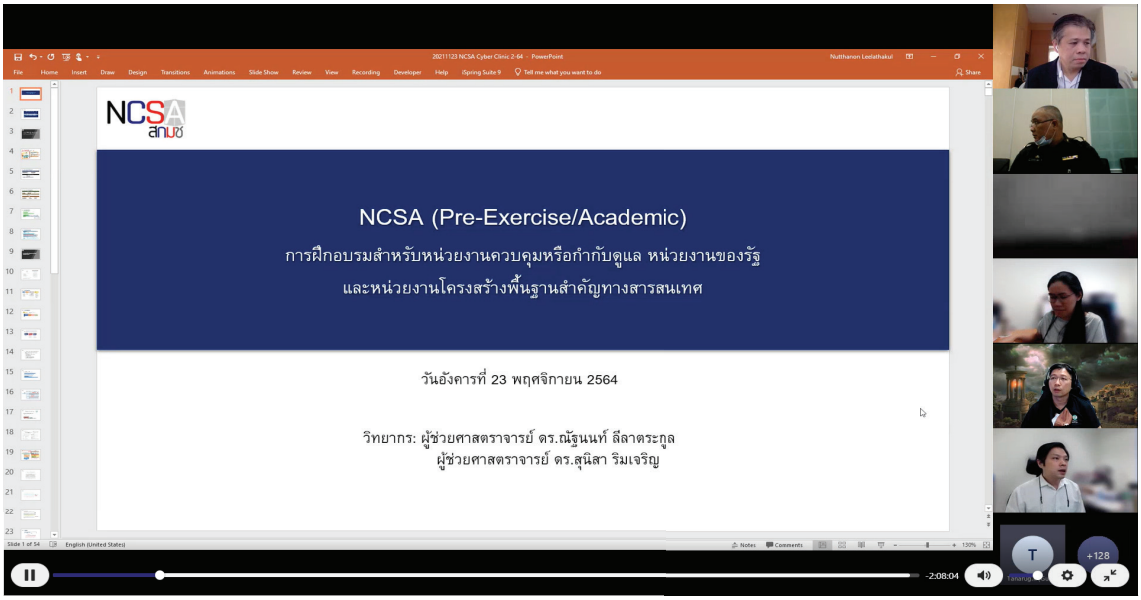
๓.๔.๑.๗ เครื่องมือที่ต้องใช้

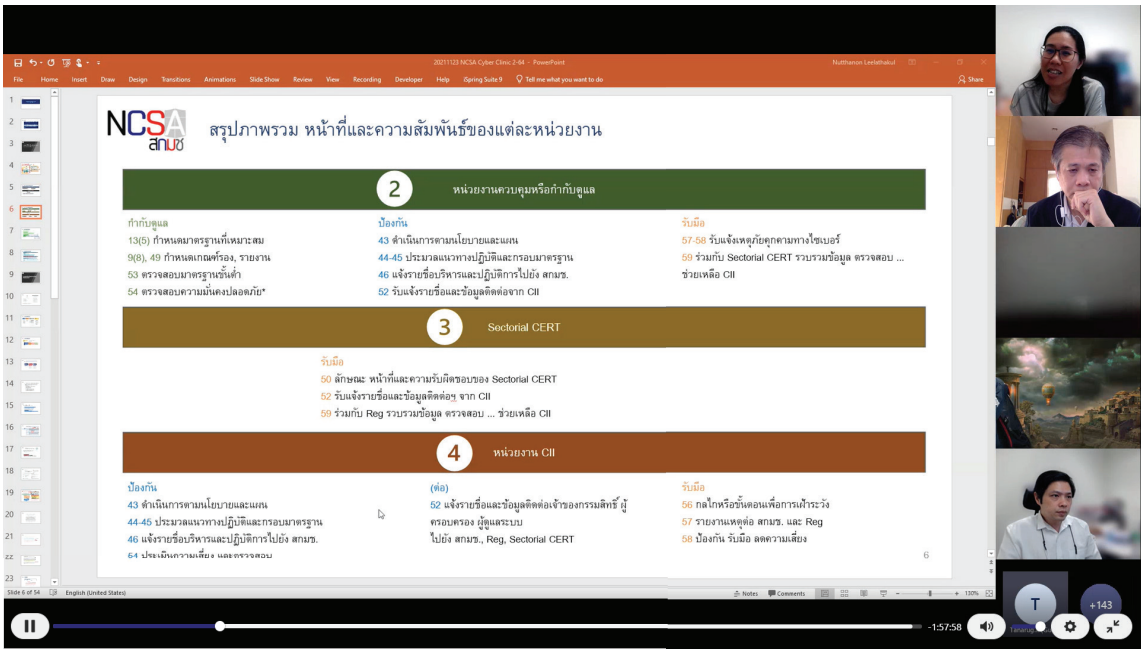
เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๑.๘ เงื่อนไขการอบรม

ด้วยข้อจำกัดทางด้านกฎหมายของ MITRE ทำให้หน่วยงานทางทหาร หน่วยงานบังคับใช้กฎหมาย และหน่วยงานด้านข่าวกรอง ไม่สามารถเข้าร่วมการอบรมได้

๓.๔.๒ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดย ผู้ช่วยศาสตราจารย์ ดร.ณัฐนนท์ ลีลาตระกูล และผู้ช่วยศาสตราจารย์ ดร.สุนิสา ริมเจริญ





รูปที่ ๓-๓ การอบรม บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๔.๒.๑ เนื้อหาการอบรม

(๑) ภาพรวมของประกาศคณะกรรมการการศึกษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

(๒) การมอบหมายการควบคุมหรือกำกับดูแล

(๓) ประกาศคณะกรรมการการศึกษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือบริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

๓.๔.๒.๒ วันและเวลาการอบรม

วันที่ ๒๓ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ – ๑๕.๐๐ น.

๓.๔.๒.๓ กลุ่มเป้าหมาย

(๑) ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐาน ระดับบริหาร และระดับปฏิบัติ

(๒) เหมาะกับผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief of Information Security Officer : CISO) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ผู้ปฏิบัติงานด้านไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เหมาะกับผู้ปฏิบัติงานที่เกี่ยวข้องกับการกำหนดมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควบคุมหรือกำกับดูแล

๓.๔.๒.๔ รายละเอียดหลักสูตร

ระดับพื้นฐาน (Basic) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๒.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๗๓ คน

๓.๔.๒.๖ ความรู้และทักษะที่จำเป็น

มีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๔.๒.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๓ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan) โดย พันตำรวจเอก ณัทกฤช พรหมจันทร์

รูปที่ ๓-๔ การอบรม บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan)

๓.๔.๓.๑ เนื้อหาการอบรม

(๑) บทบาทและหน้าที่ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๒) การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan)

(๓) (ร่าง) ประกาศคณะกรรมการการศึกษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ...

๓.๔.๓.๒ วันและเวลาการอบรม

วันที่ ๒๕ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ – ๑๖.๐๐ น.

๓.๔.๓.๓ กลุ่มเป้าหมาย

(๑) ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐาน ระดับบริหารและระดับปฏิบัติ

(๒) เหมาะกับผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief of Information Security Officer : CISO) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ผู้ปฏิบัติงานด้านไซเบอร์ โดยเฉพาะ SOC Manager, Incident Responder ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เหมาะกับผู้ปฏิบัติงานที่เกี่ยวข้องกับการกำหนดมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานควบคุมหรือกำกับดูแล

๓.๔.๓.๔ รายละเอียดหลักสูตร

ระดับปานกลาง (Intermediate) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๓.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๘๓ คน

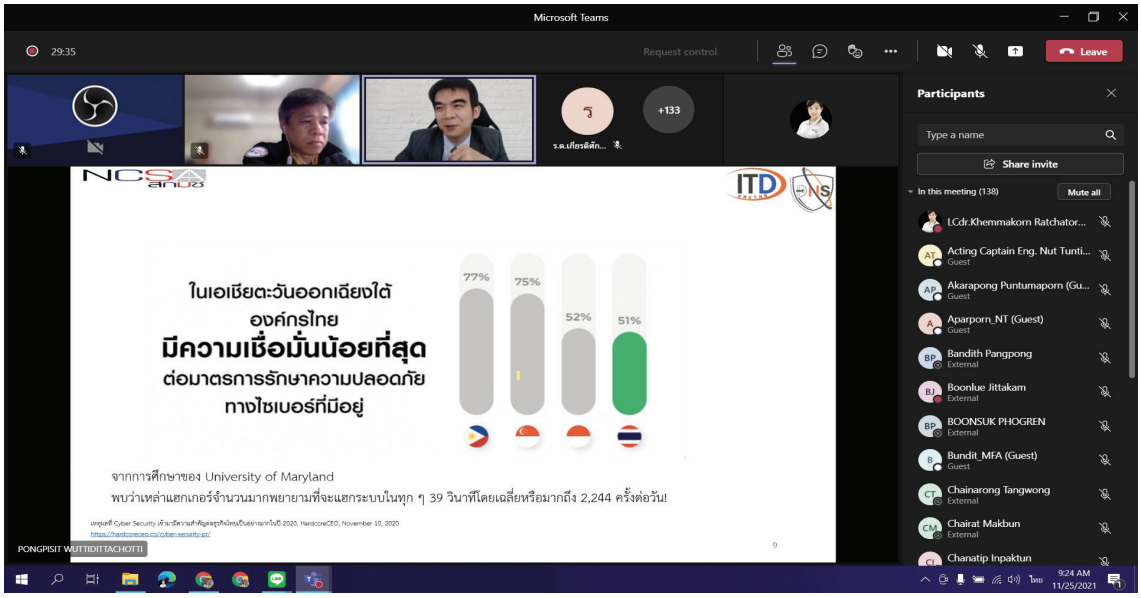
๓.๔.๓.๖ ความรู้และทักษะที่จำเป็น

มีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อาทิ การรับมือกับภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๔.๓.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๔ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดย รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ



รูปที่ ๓-๕ การอบรม ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๔.๔.๑ เนื้อหาการอบรม

(๑) ภาพรวมของร่างนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๒) ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงและปลอดภัยทางไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๓.๔.๔.๒ วันและเวลาการอบรม

วันที่ ๒๕ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ – ๑๒.๐๐ น.

๓.๔.๔.๓ กลุ่มเป้าหมาย

(๑) ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐาน ระดับบริหารและระดับปฏิบัติ

(๒) เหมาะกับผู้ปฏิบัติงานด้านไซเบอร์ ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เหมาะกับผู้ปฏิบัติงานที่เกี่ยวข้องกับการกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของหน่วยงานควบคุมหรือกำกับดูแล

๓.๔.๔.๔ รายละเอียดหลักสูตร

ระดับพื้นฐาน (Basic) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๔.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๖๓ คน

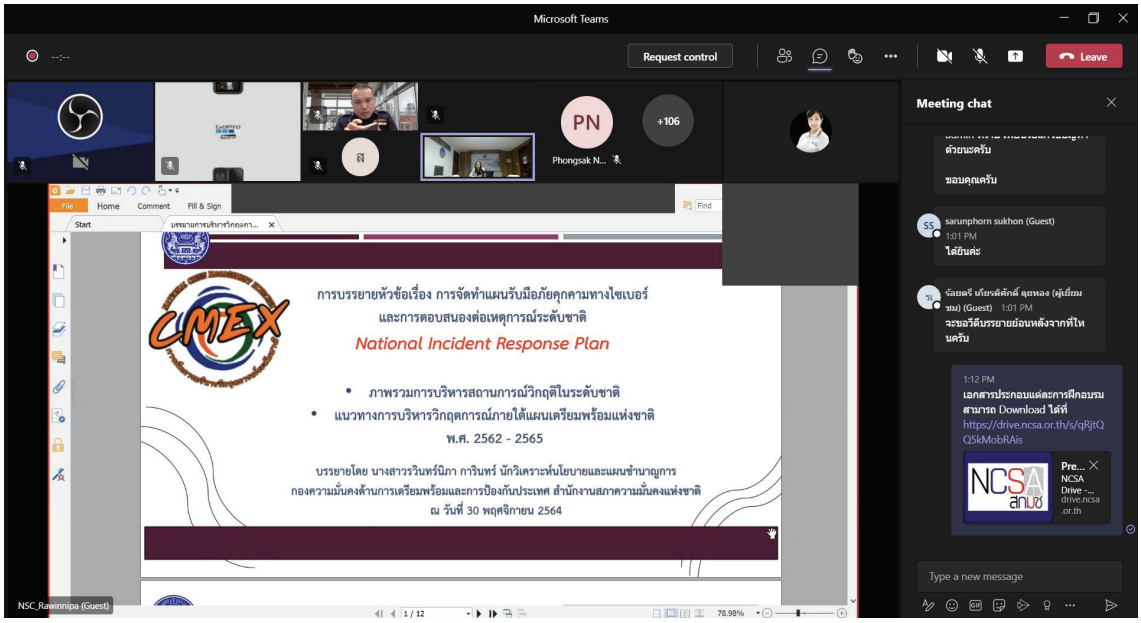
๓.๔.๔.๖ ความรู้และทักษะที่จำเป็น

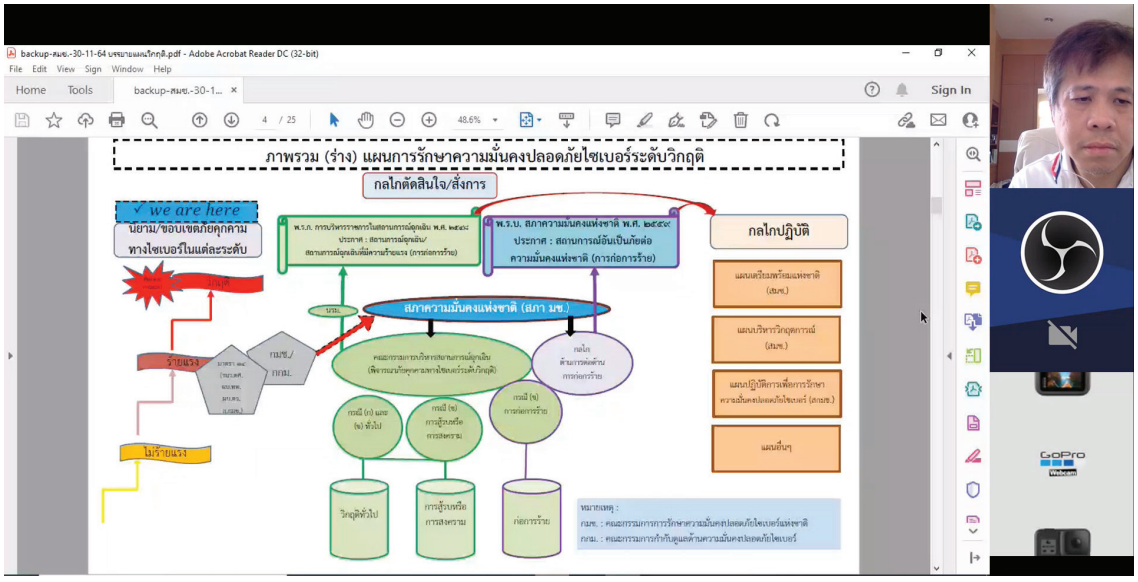
มีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๔.๔.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๕ การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan) โดย นางสาววรินทร์นิภา การินทร์ และนายสมเกียรติ บุญชู





รูปที่ ๓-๖ การอบรม การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์

ระดับชาติ (National Incident Response Plan)

๓.๔.๕.๑ เนื้อหาการอบรม ประกอบด้วย

(๑) ภาพรวมการบริหารสถานการณ์วิกฤติในระดับชาติ

(๒) แนวทางการจัดทำแผนบริหารสถานการณ์วิกฤติด้านไซเบอร์ ประกอบแผนเตรียมพร้อมแห่งชาติ

(๓) การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan)

๓.๔.๕.๒ วันและเวลาการอบรม

วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ – ๑๕.๐๐ น.

๓.๔.๕.๓ กลุ่มเป้าหมาย

(๑) ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐานระดับบริหาร

(๒) เหมาะกับผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief of Information Security Officer : CISO) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เหมาะกับผู้ปฏิบัติงานที่เกี่ยวข้องกับการกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานควบคุมหรือกำกับดูแล

๓.๔.๕.๔ รายละเอียดหลักสูตร

ระดับพื้นฐาน (Basic) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๕.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๖๓ คน

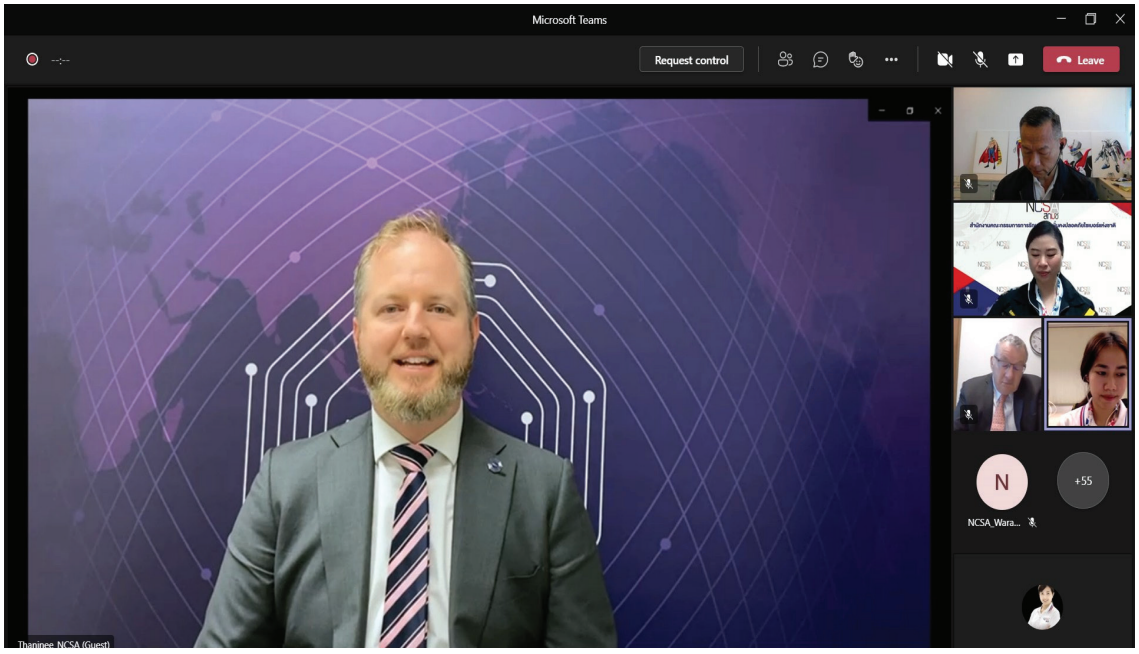
๓.๔.๕.๖ ความรู้และทักษะที่จำเป็น

มีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อาทิ การรับมือกับภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และแผนเตรียมพร้อมแห่งชาติ

๓.๔.๕.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๖ Incident Response Fundamental โดย Mr.Kawin Boonyapredee



รูปที่ ๓-๗ การอบรม Incident Response Fundamental

๓.๔.๖.๑ เนื้อหาการอบรม

(๑) Incident Response Plans

(๒) Operational Security

(๓) Tactics, Techniques, and Procedures (TTPs)

(๔) Frameworks (NIST, MITRE ATT&CK)

(๕) Common Tooling used in Incident Response (IR)

(๖) Case Management

(๗) Remediation

(๘) A Case Study

๓.๔.๖.๒ วันและเวลาการอบรม

วันที่ ๗ - ๙ ธันวาคม พ.ศ. ๒๕๖๔ เวลา ๑๐.๐๐ – ๑๒.๐๐ น.

๓.๔.๖.๓ กลุ่มเป้าหมาย

ผู้ปฏิบัติงานทั่วไป ทั้งในระดับบริหารและระดับปฏิบัติ

๓.๔.๖.๔ รายละเอียดหลักสูตร

ระดับพื้นฐาน (Basic) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๖.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๗๗ คน

๓.๔.๖.๖ ความรู้และทักษะที่จำเป็น

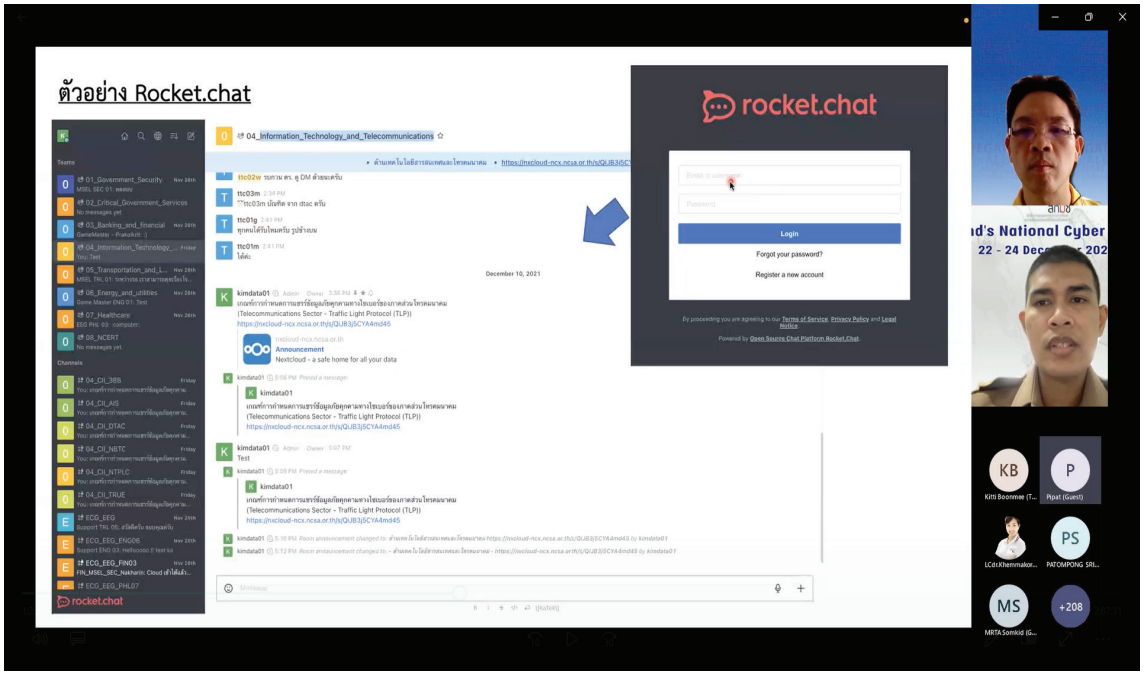
(๑) ไม่จำเป็นต้องมีความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) มีความรู้และความสามารถทางภาษาอังกฤษในระดับพื้นฐาน

๓.๔.๖.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๔.๗ วิธีการใช้งานเครื่องมือสนับสนุนการฝึก โดย เรือตรี ธีระวัฒน์ พูนวิเชียร



รูปที่ ๓-๘ การอบรม วิธีการใช้งานเครื่องมือสนับสนุนการฝึก

๓.๔.๗.๑ เนื้อหาการอบรม

(๑) เครื่องมือประชุม

(๒) เครื่องมือแชร์ไฟล์ (Shared Drive)

(๓) เครื่องมือรับส่งข้อความ (Chat)

๓.๔.๗.๒ วันและเวลาการอบรม

วันที่ ๑๓ ธันวาคม พ.ศ. ๒๕๖๔ เวลา ๐๙.๐๐ – ๑๒.๐๐ น.

๓.๔.๗.๓ กลุ่มเป้าหมาย

ผู้ปฏิบัติงานที่มีความรู้และทักษะด้านไซเบอร์ขั้นพื้นฐาน ระดับบริหาร และระดับปฏิบัติที่จะเข้าร่วมการฝึกและจำเป็นที่จะต้องใช้งานเครื่องมือสนับสนุนการฝึก

๓.๔.๗.๔ รายละเอียดหลักสูตร

ระดับพื้นฐาน (Basic) เนื้อหาเป็นแบบจบใน ๑ วัน

๓.๔.๗.๕ จำนวนผู้เข้าร่วมการฝึกเตรียมการ ๑๘๘ คน

๓.๔.๗.๖ ความรู้และทักษะที่จำเป็น

มีความรู้พื้นฐานด้านคอมพิวเตอร์

๓.๔.๗.๗ เครื่องมือที่ต้องใช้

เครื่องคอมพิวเตอร์พื้นฐาน

๓.๕ ผลของการฝึกเตรียมการ

๓.๕.๑ ผลการอบรมในหัวข้อ World Class Cyber Security Practices by MITRE/CISA/SEI มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๑๐๕ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๗.๑๘ มีค่าเฉลี่ยเท่ากับ ๔.๓๙ อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๒ ผลการอบรมในหัวข้อ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๖๖ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๔.๘๕ มีค่าเฉลี่ยเท่ากับ ๔.๒๔ อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๓ ผลการอบรมในหัวข้อ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๑๖ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๒.๕๐ มีค่าเฉลี่ยเท่ากับ ๔.๑๓

อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๔ ผลการอบรมในหัวข้อ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan) มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๔๑ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๔.๓๙ มีค่าเฉลี่ยเท่ากับ ๔.๒๒ อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๕ ผลการอบรมในหัวข้อการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan) มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๒๘ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๔.๘๕ มีค่าเฉลี่ยเท่ากับ ๔.๒๔ อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๖ ผลการอบรมในหัวข้อ Incident Response Fundamental มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๗๖ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรม คิดเป็นร้อยละ ๘๔.๒๑ มีค่าเฉลี่ยเท่ากับ ๔.๒๑ อยู่ในเกณฑ์ประเมินระดับดี

๓.๕.๗ ผลการอบรมในหัวข้อ วิธีการใช้งานเครื่องมือสนับสนุนการฝึก มีผู้เข้ารับการอบรมตอบแบบประเมินความพึงพอใจและความคิดเห็น จำนวน ๓๙ คน พบว่า ผู้ที่เข้าร่วมอบรมส่วนใหญ่มีความพึงพอใจในภาพรวมของการจัดอบรมคิดเป็นร้อยละ ๘๐.๐๐ มีค่าเฉลี่ยเท่ากับ ๔.๐๐ อยู่ในเกณฑ์ประเมินระดับดี

๓.๖ ความคิดเห็นและข้อเสนอแนะจากผู้ที่เข้ารับการฝึกเตรียมการ

๓.๖.๑ ด้านเนื้อหาการฝึกเตรียมการ

๓.๖.๑.๑ หัวข้อ World Class Cybersecurity Practices by MITRE/CISA/SEI มีเนื้อหาที่ดี วิทยากรและทีมงานมีความตั้งใจอย่างมาก ทั้งนี้ ในส่วนของสถานการณ์ประกอบการอบรม (Mr.Dingbang) สามารถส่งมาเป็นภาษาอังกฤษได้เลยโดยไม่จำเป็นต้องแปลเป็นภาษาไทย ควรมีภาคปฏิบัติ (Workshop) เพิ่มเติมระหว่างหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และควรลงรายละเอียดของ Topic 5 : Development of a National Coordination Center ให้มากยิ่งขึ้น

๓.๖.๑.๒ หัวข้อ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ

ทางสารสนเทศ เนื้อหาหลักสูตรดี

๓.๖.๑.๓ หัวข้อ บทบาทและหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan) ควรเพิ่มเนื้อหาในเรื่องของมาตรฐานหรือแนวทางการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) ให้มากขึ้น

๓.๖.๑.๔ หัวข้อ การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan) ควรเพิ่มเนื้อหาในเรื่องแนวคิดในการจัดทำ และแนวทางการจัดทำแผน ว่าในการทำแผนควรคำนึงถึงอะไรบ้าง ปัจจัยความสำเร็จในการจัดทำแผนคืออะไร

๓.๖.๑.๕ หัวข้อ Incident Response Fundamental ควรจัดให้มีหลักสูตรต่อเนื่องที่มีเนื้อหาเชิงลึก (Advanced) เพิ่มมากขึ้น

๓.๖.๑.๖ หัวข้อ วิธีการใช้งานเครื่องมือสนับสนุนการฝึก ควรมีการปรับปรุงในเรื่องการนำเสนอเนื้อหาให้สอดคล้องกับผู้รับการอบรมมากขึ้น เช่น การสาธิตการใช้งานระบบควรเข้าสู่ระบบด้วยมุมมองของผู้ใช้งาน (User) แทนที่มุมมองของผู้ดูแลระบบ (Admin) รวมถึงเรื่องจำนวนและความพร้อมใช้งานของบัญชีผู้ใช้ เป็นต้น

๓.๖.๒ ด้านการบริหารหลักสูตร

๓.๖.๒.๑ ควรเพิ่มช่องทางติดต่อในเว็บไซต์สำหรับการลงทะเบียนกรณีเกิดปัญหาในการเข้าฟังการอบรม

๓.๖.๒.๒ ควรปรับปรุงในเรื่องของการประสานงาน เพราะบางครั้งได้รับข้อมูลไม่ครบถ้วน หรือบางท่านไม่ได้รับข้อมูล

๓.๖.๒.๓ ควรเริ่มการอบรมให้ตรงต่อเวลาตามที่ได้แจ้งไว้

๓.๖.๒.๔ ควรกำหนดวันเวลาการอบรมมิให้มีการจัดอบรมหลายเนื้อหาในเวลาที่ใกล้ ๆ กัน

๓.๖.๒.๕ ควรมีการแจกเอกสารประกอบการอบรมล่วงหน้า จะทำให้มีโอกาสได้ทำความเข้าใจก่อนเข้ารับการอบรมมากยิ่งขึ้น

บทที่ ๔
การดำเนินการ
และผลการฝึก

บทที่ ๔
การดำเนินการฝึก และผลการฝึก

การดำเนินการฝึก (Exercise Execution) เป็นกระบวนการที่รับผิดชอบโดยส่วนควบคุมการฝึกในการส่งโจทย์ฝึก (Inject Releases) การมีปฏิสัมพันธ์กับผู้รับการฝึก (Training Audience Interactions) รวมถึงการติดตามการดำเนินการให้เป็นไปตามแผนการฝึก (Exercise Plan) และสังเกตการณ์ผู้รับการฝึกผ่านผู้สังเกตุการณ์ (Exercise Observers) [๙]

อย่างไรก็ตาม สกมช. ได้มีการประยุกต์หลักการดังกล่าว เพื่อให้สอดคล้องกับบริบทของประเทศไทย และทำให้สามารถจัดการฝึกได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยได้กำหนดให้ส่วนควบคุมการฝึก รับผิดชอบการส่งโจทย์ฝึก (Inject Releases) และการมีปฏิสัมพันธ์กับผู้รับการฝึก (Training Audience Interactions) ส่วน บก.กอ.ฝึก รับผิดชอบการติดตามการดำเนินการให้เป็นไปตามแผนการฝึก (Exercise Plan) และส่วนประเมินผลการฝึก รับผิดชอบเรื่องการสังเกตการณ์ผู้รับการฝึก

๔.๑ วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกสามารถตอบสนองต่อสถานการณ์และโจทย์ฝึกตามบทบาทที่ได้รับได้อย่างสอดคล้องกับผลลัพธ์ที่คาดหวัง ตามที่กำหนดไว้ในรายการโจทย์ฝึก (MSEL)

๔.๒ วันและเวลา

วันที่ ๒๒ - ๒๔ ธันวาคม พ.ศ. ๒๕๖๔

๔.๓ สถานที่ฝึก

ดำเนินการฝึกแบบผสมผสาน (Hybrid Event) โดยมีผู้แทนจากหน่วยงานที่รับผิดชอบเป็นส่วนควบคุมการฝึกมายังสถานที่จัดการฝึก ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร และในส่วนของผู้รับการฝึกจะเข้ารับการฝึกในรูปแบบออนไลน์ผ่านระบบ Microsoft Teams

[๙] Exercise Execution, MITRE Cyber Exercise Playbook

๔.๔ ผู้เข้าร่วมการฝึก รายละเอียดตามผนวก ง ๒ และ ง ๓ สรุปได้ดังนี้

๔.๔.๑ ผู้ทำหน้าที่ในส่วนควบคุมการฝึกและส่วนประเมินผลการฝึก จำนวน ๑๓๖ คน

๔.๔.๒ ผู้เข้ารับการฝึก จำนวน ๒๗๐ คน

๔.๕ สาระสำคัญของการฝึก

๔.๕.๑ แนวทางการดำเนินการฝึก

๔.๕.๑.๑ การชี้แจงก่อนการฝึก เมื่อวันที่ ๗ ธันวาคม พ.ศ. ๒๕๖๔ เวลา ๑๓.๐๐ - ๑๖.๐๐ น. ดังนี้

(๑) วัตถุประสงค์และบทบาทของผู้ที่จะเข้าร่วมการฝึก

(๒) กำหนดการฝึก

๒๒ ธันวาคม พ.ศ. ๒๕๖๔		๒๓ ธันวาคม พ.ศ. ๒๕๖๔		๒๔ ธันวาคม พ.ศ. ๒๕๖๔	
๐๘.๓๐ – ๐๘.๔๕ น.	เข้าสู่ระบบ	๐๘.๓๐ – ๐๘.๔๕ น.	เข้าสู่ระบบ	๐๘.๓๐ – ๐๘.๔๕ น.	เข้าสู่ระบบ
๐๘.๔๕ – ๐๙.๓๐ น.	พิธีเปิดการฝึก	๐๘.๔๕ – ๐๙.๐๐ น	บก.กอ.ฝึก ชี้แจง	๐๘.๔๕ – ๐๙.๐๐ น	บก.กอ.ฝึก ชี้แจง
๐๙.๓๐ – ๐๙.๔๕ น.	บก.กอ.ฝึก ชี้แจง	๐๙.๐๐ – ๑๒.๐๐ น.	สถานการณ์ฝึก	๐๙.๐๐ – ๑๒.๐๐ น.	สถานการณ์ฝึก
๐๙.๔๕ – ๑๒.๐๐ น.	สถานการณ์ฝึก	๑๒.๐๐ – ๑๓.๐๐ น.	รับประทานอาหารเที่ยง	๑๒.๐๐ – ๑๓.๐๐ น.	รับประทานอาหารเที่ยง
๑๒.๐๐ – ๑๓.๐๐ น.	รับประทานอาหารเที่ยง	๑๓.๐๐ – ๑๕.๐๐ น.	สถานการณ์ฝึก	๑๓.๐๐ – ๑๕.๐๐ น.	บก.กอ.ฝึก ชี้แจง
๑๓.๐๐ – ๑๕.๐๐ น.	สถานการณ์ฝึก	๑๕.๐๐ – ๑๕.๑๕ น.	บก.กอ.ฝึก ชี้แจง	๑๕.๐๐ – ๑๕.๑๕ น.	After Action Review (AAR)
๑๕.๐๐ – ๑๕.๑๕ น.	บก.กอ.ฝึก ชี้แจง	๑๕.๑๕ – ๑๗.๐๐ น.	Daily Hotwash	๑๕.๑๕ – ๑๗.๐๐ น.	พิธีปิดการฝึก
๑๕.๑๕ – ๑๗.๐๐ น.	Daily Hotwash				

ตารางที่ ๔-๑ กำหนดการฝึก

(๓) ข้อตกลงร่วม (Rules of Engagement : RoE)

(๓.๑) ยึดถือวัตถุประสงค์การฝึกอยู่เสมอ

(๓.๒) Nation-wide crisis, not a sector crisis

(๓.๓) เตรียมตัวล่วงหน้าก่อนเข้าร่วมการฝึก

(๓.๔) การคิดอย่างมีวิจารณญาณและมุ่งเน้นกระบวนการ (Critical thinking & Process focus, NO blame culture)

(๓.๕) มีความกระตือรือร้นในการแสดงความเห็นคิด (Active discussion)

(๔) แหล่งข้อมูลประกอบการฝึก ประกอบด้วย เอกสารประกอบการฝึกเตรียมการทั้ง ๗ หัวข้อ และเอกสารประกอบการชี้แจงก่อนการฝึกเมื่อวันที่ ๗ ธันวาคม พ.ศ. ๒๕๖๔

(๕) (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์

(๖) สถานการณ์ฝึก และลำดับสถานการณ์ประจำวัน

๔.๕.๑.๒ การชี้แจงก่อน Daily Hotwash

(๑) Daily Hotwash เป็นกิจกรรมการทบทวนการปฏิบัติภายหลังการจัดทำโจทย์ฝึก โดยมีวัตถุประสงค์เพื่อให้ผู้รับการฝึก ส่วนควบคุมการฝึก และส่วนประเมินผล ได้อธิบายเกี่ยวกับการแก้ไขปัญหาตามสถานการณ์และโจทย์ฝึกที่ได้รับ ซึ่งจะทำให้ผู้รับการฝึกมีความรู้ความเข้าใจเกี่ยวกับวิธีการปฏิบัติที่เหมาะสมในการรับมือกับเหตุการณ์ทางไซเบอร์ รวมถึงได้แลกเปลี่ยนมุมมองและประสบการณ์กับผู้รับการฝึกที่อยู่ในหน่วยงานอื่น ๆ ด้วย

(๒) บก.กอ.ฝึก ได้กำหนดลำดับการนำเสนอ Daily Hotwash โดยให้เวลา Sector ละ ๑๐ นาที (รวมเป็น ๗๐ นาที) และปิดท้ายด้วยหัวหน้าส่วนควบคุมการฝึก (ECG Master) ๕ นาที โดยมีลำดับการนำเสนอ ดังนี้

(๒.๑) ผู้เข้ารับการฝึก (Player) นำเสนอเกี่ยวกับโจทย์ฝึกที่ได้รับและวิธีการแก้ไขปัญหา (๕ นาที)

(๒.๒) Game Master (ECG) นำเสนอเกี่ยวกับโจทย์ฝึกที่ส่งและผลลัพธ์ที่คาดหวัง (๓ นาที)

(๒.๓) ผู้ประเมินผล (EEG) นำเสนอเกี่ยวกับผลจากการสังเกตการณ์และข้อเสนอแนะ (๒ นาที)

๔.๕.๑.๓ ลำดับสถานการณ์ประจำวัน

(๑) สถานการณ์ประจำวันที่ ๒๒ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

(๑.๑) กลุ่มแฮกเกอร์ Red_Axe ประกาศผ่าน Official Red_Axe Forum จะมีการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานของภาครัฐของประเทศไทย ในวันที่ ๒๓ ธันวาคม พ.ศ. ๒๕๖๔

(๑.๒) National CERT ได้รับรายงานจาก TTC – CERT พบความพยายามของกลุ่มแฮกเกอร์ Red_Axe ในการลาดตะเวนทางไซเบอร์ (Reconnaissance) ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านโทรคมนาคม เพิ่มสูงขึ้นอย่างมีนัยสำคัญ

(๑.๓) National CERT ได้รับรายงานจาก CERT ต่างประเทศ แจ้งเตือนเกี่ยวกับกิจกรรมทางไซเบอร์ของกลุ่มแฮกเกอร์ Blue_Eagle มีการแชร์เครื่องมือประเภท Downloader, Screenshot tool, Keylogger, Privilege Escalation, Lateral Movement, Ransomware เป็นต้น โดยมีความเป็นไปได้สูงที่จะสนับสนุนเครื่องมือดังกล่าวให้กับกลุ่มแฮกเกอร์ Red_Axe เพื่อปฏิบัติการในพื้นที่ประเทศไทยด้วย

(๑.๔) National CERT ได้รับรายงานจาก TB – CERT พบว่ามีเหตุการณ์ภัยคุกคามทางไซเบอร์ในลักษณะ Spear Phishing เพิ่มสูงขึ้นอย่างมาก รวมถึงสำนักข่าว ABC รายงานว่ากลุ่มแฮกเกอร์ Red_Axe ประกาศผ่าน Official Red_Axe forum จะโจมตีหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้วยวิธีการ DDOS และ Web Defacement

(๒) สถานการณ์ประจำวันที่ ๒๓ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

(๒.๑) กลุ่มแฮกเกอร์ Red_Axe ประกาศผ่าน Official Red_Axe Forum ว่าสามารถแฮ็กเข้าสู่ Cloud ของหน่วยงานของรัฐ และสามารถเข้าถึงรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทยได้ทั้งหมด

(๒.๒) กลุ่มแฮกเกอร์ Red_Axe ประกาศความร่วมมือกับกลุ่มแฮกเกอร์ Blue_Eagle ตั้ง Campaign การโจมตี OpThailand โดยจะระดมโจมตีทางไซเบอร์ขนาดใหญ่ต่อเนื่องตลอด ๒๔ ชั่วโมง ไปยังหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย

(๒.๓) กลุ่มแฮกเกอร์ Red_Axe ยื่นคำขาดว่าจะโจมตีทางไซเบอร์ต่อระบบไฟฟ้าของประเทศรวมถึงการโจมตีโรงพยาบาลโดยใช้ Ransomware หากรัฐบาลไทยยังคงจำกัดสิทธิในการแสดงความคิดเห็นในการประท้วงการทำงานของรัฐ และมีการจับกุมผู้เห็นต่างทางการเมือง

(๓) สถานการณ์ประจำวันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๔ (สิงหาคม ๒๕๖๕)

(๓.๑) กลุ่มแฮกเกอร์ Red_Axe ประกาศความสำเร็จในการโจมตีทางไซเบอร์ขนาดใหญ่ต่อเนื่องตลอด ๒๔ ชั่วโมง ไปยังหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย โดยขอให้มุ่งโจมตีระบบอินเตอร์เน็ตของประเทศไทยให้เสียหายและเกิดผลกระทบเป็นวงกว้างมากที่สุด

(๓.๒) กลุ่มแฮกเกอร์ Red_Axe โพสต์ข้อมูลที่ได้จากการแฮ็กหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย จำนวนมากกว่า ๓๐ หน่วยงาน ลงใน Dark Web โดยอ้างว่าเป็นข้อมูลของคนไทยที่ใช้บริการต่าง ๆ ครอบคลุมทั้ง ๗ Sector อาทิ ข้อมูลบัตรเครดิต ข้อมูลด้านสุขภาพ ข้อมูลการตั้งค่าที่สำคัญ ข้อมูลจากเครื่องแม่ข่าย เป็นต้น

(๓.๓) ประชาชนเริ่มมีการก่อตัวในบางพื้นที่ รวมถึงวิพากษ์วิจารณ์อย่างรุนแรงถึงความไร้ประสิทธิภาพของหน่วยงานด้านความมั่นคงของรัฐ และหน่วยงานของรัฐ เพื่อแสดงความไม่พอใจที่ได้รับผลกระทบต่อชีวิตและทรัพย์สินเพิ่มมากขึ้น

(๓.๔) นายกรัฐมนตรี ในฐานะประธาน กมช. สั่งการให้ สกมช. และ สมช. เตรียมใช้กฎหมายว่าด้วยความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง ในการดำเนินการรักษาความปลอดภัยไซเบอร์ขั้นสูงสุด

๔.๖ ผลการฝึก (Daily Hotwash)

ผลการฝึกเป็นช่วงเวลาที่สำคัญที่สุดในห้วงการฝึก โดยจะกำหนดให้ผู้รับการฝึก (Player) ได้ตอบคำถามตามโจทย์ฝึกที่ได้รับจากส่วนควบคุมการฝึก (ECG) ตามความรู้ ประสบการณ์ รวมถึงขั้นตอนการปฏิบัติงานของหน่วยงานนั้น ๆ และเพื่อเป็นการสะท้อนถึงความรู้และทักษะของผู้เข้ารับการฝึกในห้วงเวลานั้น สกมช. จึงได้คงแนวทางการตอบคำถามให้มีลักษณะใกล้เคียงกับคำตอบเดิมให้มากที่สุด ดังนี้

๔.๖.๑ ด้านความมั่นคงของรัฐ

๔.๖.๑.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีข้อมูลรั่วไหล (Data Leak) ไปยังดาร์กเว็บ (Dark Web) ประเมินสถานการณ์ พบว่าอยู่ในระดับร้ายแรง

(๑.๑) ตรวจสอบข้อมูลที่มีการเผยแพร่ออกไปว่าเป็นข้อมูลของหน่วยงานจริงหรือไม่ มีชั้นความลับหรือไม่ และผลกระทบของข้อมูลเป็นอย่างไร

(๑.๒) ปิดช่องการเชื่อมต่อจากภายนอก ปิดระบบ

(๑.๓) แจ้งให้หน่วยงานที่ได้รับผลกระทบ ทำการตรวจสอบการตั้งค่าและเปลี่ยนรหัสผ่าน (Password)

(๑.๔) ให้เจ้าของระบบและทีมสืบค้นข้อมูลทางดิจิทัล (Forensic) ทำการตรวจสอบ Log และวิเคราะห์หาสาเหตุ

(๑.๕) ทีมสืบค้นข้อมูลทางดิจิทัล (Forensic) เก็บพยานหลักฐานทางดิจิทัลเพื่อใช้ในการดำเนินคดีตามกฎหมาย

(๑.๖) รวบรวมข้อมูลข้อเท็จจริงที่เกิดขึ้นทั้งหมด นำเรียนผู้บังคับบัญชาตามลำดับชั้น

(๑.๗) ในส่วนการแถลงข่าว มอบให้โฆษกกองทัพเป็นผู้ชี้แจงรายละเอียดข้อเท็จจริงที่เกิดขึ้น รวมไปถึงแนวทางในการแก้ไข

(๑.๘) สร้างความตระหนักรู้ให้กับกำลังพลหรือผู้ใช้งาน

(๑.๙) แจ้งหน่วยงานควบคุมหรือกำกับดูแล และ สกมช. ให้ทราบ

(๒) กรณีตรวจพบและได้รับรายงานว่ามี Email Phishing ในหน่วยงานจำนวนมาก

(๒.๑) ประเมินสถานการณ์ พบว่า อยู่ในระดับ ไม่ร้ายแรง

(๒.๒) ตรวจสอบรูปแบบ Email Phishing ที่เกิดขึ้นว่าผู้ส่งเป็นใคร มาจากที่ไหน

(๒.๓) นำ Link หรือ File ที่แนบมาตรวจสอบที่ VirusTotal เพื่อตรวจสอบว่าไฟล์มีความอันตรายหรือไม่

(๒.๔) เพิ่มรูปแบบในการป้องกันที่ Email Security Gateway

(๒.๕) สร้างความตระหนักรู้แก่ กำลังพลและผู้ใช้งานระบบ เช่น ไม่เปิด E-mail จากแหล่งที่ไม่รู้จัก หรือ Link ที่ไม่น่าเชื่อถือ

(๒.๖) ติดตั้ง Antivirus

(๓) กรณีระบบควบคุมขัดข้อง ถูกโจมตีโดยปฏิเสธการให้บริการ (Distributed Denial-of-Service : DDoS)

(๓.๑) รายงานต่อผู้บังคับบัญชาสูงสุด เพื่อขอนโยบายแนวทางของผู้บังคับบัญชาสูงสุด เพื่อเปิดระบบบัญชาการสั่งการสำรองสำหรับสถานการณ์ฉุกเฉิน หากจำเป็น ให้จัดตั้งศูนย์การบังคับกลาง

(๓.๒) ผู้ดูแลระบบดำเนินการระงับผลกระทบของเหตุการณ์ตามแนวทางปฏิบัติของหน่วยงาน

(๓.๓) รายงานผู้บังคับบัญชาสูงสุดตามลำดับขั้น

(๓.๔) แจ้งหน่วยงานควบคุมหรือกำกับดูแล สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) และ สกมช. ตามมาตรา ๖๒ และมาตรา ๕๗ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้ข้อมูลแก่หน่วยงานควบคุมหรือกำกับดูแล และ National CERT ในการรวบรวม ตรวจสอบ วิเคราะห์และประเมินสถานการณ์ เพื่อแจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่น ๆ โดยเร็วต่อไป

(๔) กรณีถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ (Ransomware)

(๔.๑) รายงานผู้บังคับบัญชาสูงสุดเพราะเป็นเหตุการณ์โจมตีระดับวิกฤติและแจ้งไปยัง สกมช.

(๔.๒) ทำการตัดสัญญาณการเชื่อมต่อ และใช้ช่องทางสำรองไว้สำหรับการสื่อสาร หาวิธีการแก้ไขและทำการปิดช่องโหว่ แนะนำหน่วยงานอื่น ๆ ให้ทำการสำรองข้อมูล (Backup) ไว้ภายนอก

(๔.๓) ดำเนินการติดตามและรายงานให้กับผู้บังคับบัญชา ถ้าแก้ไขปัญหาไม่ได้ ให้แจ้งขอความช่วยเหลือมายัง สกมช. และเตรียมหาข้อมูลต่าง ๆ เพื่อดำเนินคดี

๔.๖.๑.๒ ผลลัพธ์ที่ความคาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ เมื่อได้รับ MSEL ผู้เข้ารับการฝึกจากหน่วยงานที่เกิดเหตุแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตน และแจ้ง สกมช. โดยให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทำการตรวจสอบสาเหตุของการโจมตี จากนั้นทำการแก้ไขปรับปรุงช่องโหว่ที่ตรวจพบ หากไม่สามารถแก้ไขได้ ให้ร้องขอทีม National CERT จาก สกมช. เพื่อให้การช่วยเหลือในการดำเนินการแก้ไข ขณะเดียวกัน ทีมสื่อสารองค์กรต้องดำเนินการจัดเตรียมข้อมูลและออกแถลงข่าวการถูกโจมตี, และในส่วนของทีมกฎหมาย ให้ดำเนินการรวบรวมพยานหลักฐานที่เกี่ยวข้องเพื่อดำเนินคดี

ต่อไป, ทำการแจ้งเตือนเหตุการณ์ให้หน่วยต่าง ๆ ใน Sector ความมั่นคงและหน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ พร้อมทั้งจัดทำการร่วมใช้ข้อมูลชุดเดียวกัน (Information Sharing) ผ่านตัวบ่งชี้ภัยคุกคาม (Indicator of Compromise : IOC) และเปลี่ยนมาใช้ระบบสำรองและเครือข่ายภายใน อีกทั้งยังคาดหวังว่าการปฏิบัติในการแก้ไขสถานการณ์จะเป็นไปอย่างมีประสิทธิภาพ

(๒) ผลการปฏิบัติในการฝึก พบว่า การติดต่อสื่อสารขัดข้องบ่อย ผู้เข้ารับการฝึกไม่ได้ใช้ White Team เนื่องจากข้อจำกัดด้านเวลา และแผนการรับมือภัยคุกคามแต่ละหน่วยงานไม่เหมือนกัน ทั้งนี้ ขึ้นอยู่กับบริบทและวัฒนธรรมองค์กร

๔.๖.๑.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้เล่นมีความกระตือรือร้น สามารถดำเนินการแก้ไขสถานการณ์ฝึกได้ดี แต่ขาดการมีส่วนร่วมของ White Team

(๒) ข้อเสนอแนะ White Team ควรมีบทบาทในการร่วมแก้ไขสถานการณ์ฝึกให้มากขึ้น

๔.๖.๒ ด้านบริการภาครัฐที่สำคัญ

๔.๖.๒.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณี AMI Sever หน่วยงานปลายทางล้มเหลว (Failed) ๕๐%

(๑.๑) ตรวจสอบหน่วยงานที่ Fail ๕๐% ว่าเป็นหน่วยงานไหน และตรวจสอบปัญหาที่เกิดจากระบบเครือข่ายหรือระบบศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ

(๑.๒) หากไม่ได้เกิดจากปัญหาเครือข่ายให้แจ้งผู้ดูแลระบบศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐเพื่อหาสาเหตุของปัญหา

(๑.๓) แจ้ง สกมช. และหน่วยงานควบคุมหรือกำกับดูแล ว่าตรวจสอบหน่วยงานใดเกิดปัญหาการใช้งานบ้าง

(๑.๔) แจ้งหน่วยงานที่ดูแลระบบสืบค้นข้อมูลของศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (Government Data Exchange Center : GPX) หาสาเหตุและแก้ไขปัญหา ถ้ายังไม่สามารถแก้ไขปัญหาได้ ในเบื้องต้นจะต้องดำเนินการจัดหาระบบสำรองเพื่อมาทดแทนชั่วคราว

(๑.๕) เมื่อระบบกลับมาใช้งานได้ตามปกติ แจ้งหน่วยงานที่เกิดปัญหาทดสอบใช้ระบบว่ากลับมาใช้งานได้ตามปกติหรือไม่ หากใช้งานได้ตามปกติแล้ว ให้แจ้งผู้ดูแลระบบให้ทราบและทำการปิดเคส

(๑.๖) แจ้งเจ้าของระบบทำการตรวจสอบและวิเคราะห์ไฟล์ข้อมูล (Log File)

(๒) ระบบสืบค้นข้อมูลของศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (Government Data Exchange Center : GPX) เกิดความล่าช้า

(๒.๑) ประเมินการเข้าใช้งานเครือข่าย (Network) ว่ามีการปริมาณการใช้งานมากกว่าปกติหรือไม่ ตรวจสอบไฟล์บันทึกข้อผิดพลาด (log error) ถ้ามีการแฮกข้อมูล ให้ร้องขอไปที่ สกมช. ให้ทำการตรวจสอบการเชื่อมโยงข้อมูล และจะจัดส่งให้กรมการปกครองช่วยตรวจสอบปัญหา

(๒.๒) ตรวจสอบหน่วยงานที่รับบริการว่าสามารถใช้บริการได้หรือไม่ พบปัญหาอะไรบ้าง โดยแจ้งให้ผู้ดูแลระบบตรวจสอบ และทำแผนแก้ไข ประเมินเหตุการณ์ที่เกิดขึ้นเพื่อรับมือและหาวิธีป้องกัน หากถูกโจมตีด้วย DDoS หน่วยงานจะทำการล็อคหมายเลขประจำเครื่องคอมพิวเตอร์ (Internet Protocol Address : IP Address) ที่โจมตีเข้ามา โดยตรวจสอบแก้ไขในส่วนที่เกิดปัญหา และแจ้ง สกมช. ผู้ควบคุมหรือกำกับดูแล กรณีเกิดปัญหาภายในจะแจ้งและรายงานผู้บังคับบัญชาภายในทราบ

(๓) กรณีการถูกโจมตีหน้าเว็บ (Web Defacement)

(๓.๑) ประเมินแล้วแจ้งไปยัง สกมช. หน่วยงานควบคุมหรือกำกับดูแล และประสานผู้ดูแลเว็บไซต์ (Website) แก้ไขหน้า Website โดยต่อไปจะทำการประเมิน และจัดทำแผนแก้ไขว่าถูกโจมตีถึงขั้นไหน ส่วนไหน และทำการเปลี่ยนรหัสผ่าน (Password) ทันที ซึ่งได้มีการสำรองข้อมูลเบื้องต้นตลอดการทำงาน

(๔) กรณีเกิดการรั่วไหลของข้อมูล (Data Leak) ไปยังดาร์กเว็บ (Dark Web)

(๔.๑) ประเมิน ระบุกระบวนการและงานเร่งด่วน ข้อมูลที่หลุดออกไปมีความสำคัญหรือไม่ ซึ่งเมื่อประเมินแล้วอยู่ในระดับวิกฤติ เนื่องจากกระทบกับระบบและผู้รับบริการ ทำการแจ้ง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลให้ทราบ ภายใน ๑๐ นาที ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และส่งรายงานให้กับหน่วยงานควบคุมหรือกำกับดูแลภายใน ๓๐ นาที และ สกมช. ภายใน ๑ ชั่วโมง

(๔.๒) แจ้งผู้ใช้งานที่ได้รับผลกระทบ และดำเนินการแจ้งความเพื่อดำเนินคดีตามกฎหมาย

(๔.๓) ดำเนินการตามแผนการกู้คืนระบบและเครือข่ายให้สามารถกลับมาใช้งานอย่างเร็วที่สุด

(๔.๔) การปรับปรุงมาตรการ เพื่อเตรียมพร้อมรับมือ ป้องกัน และระงับภัยคุกคามทางไซเบอร์

(๔.๕) จัดทำแผนการจัดการสภาวะวิกฤติ (Crisis Management) คือรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงาน เก็บหลักฐานตามนโยบายขององค์กร และเตรียมหลักฐานดำเนินคดีต่อไป

(๕) กรณีได้รับการร้องเรียนจากผู้ได้รับผลกระทบจากเหตุการณ์ข้อมูลรั่วไหล (Data Leak)

(๕.๑) ประเมินโอกาสและผลกระทบเชิงลบต่อองค์กร

(๕.๒) ดำเนินการเครื่องมือตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เช่น ระบุตัวตน กำหนดสิทธิ์การเข้าถึงข้อมูล การป้องกันคุ้มครองข้อมูล ป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์

(๕.๓) ดำเนินการตามแผนการจัดการภาวะวิกฤติ (Crisis Management) ที่องค์กรได้จัดทำไว้

(๕.๔) แต่งตั้งคณะทำงานเฉพาะกิจเพื่อรองรับสถานการณ์

(๕.๕) จัดการสภาวะวิกฤติ (Crisis Management) ในช่องทางโซเชียลมีเดีย (Social Media) ในระยะแรกให้หยุดการสื่อสารในช่องทางดังกล่าว

(๕.๖) แถลงการณ์ให้รับทราบถึงปัญหาและแนวทางการแก้ไข

(๕.๗) ตอบข้อความแสดงความคิดเห็นของผู้ได้รับผลกระทบ (Comment) เน้นการรับทราบถึงปัญหา และวิธีการแก้ไข

(๖) กรณีรองนายกรัฐมนตรีได้รับมอบหมายให้แถลงสรุปปัญหาและแนวทางในการแก้ไขปัญหา โดยให้การเยียวยาผู้ที่ได้รับผลกระทบต่อเหตุการณ์ที่เกิดขึ้น

(๖.๑) จัดตั้งการประชุมในภาวะที่เกิดเหตุการณ์ไม่ปกติ (War Room) ปฏิบัติการสำหรับการแก้ไขปัญหาที่เกิดขึ้น และจัดทำมาตรการป้องกันเหตุการณ์ที่อาจเกิดขึ้นอีก

(๖.๒) จัดให้มีมาตราการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในรูปแบบที่เหมาะสม เช่น ปรับระดับการรักษาความปลอดภัยให้เหมาะกับระดับความเสี่ยง

(๖.๓) มีคณะกรรมการเฉพาะกิจในการบริหารในภาวะวิกฤติ โดยทำหน้าที่กลั่นกรองข้อมูลที่ทันสมัยและทันเหตุการณ์ ร่วมพิจารณาให้ความเห็น จัดทำสรุปรายงานประจำวัน แต่งตั้งผู้ที่ทำหน้าที่แถลงข่าว และจัดทำข่าวประชาสัมพันธ์

(๖.๔) สื่อสารภายในองค์กรเพื่อให้พนักงานได้รับทราบ และให้แสดงความคิดเห็นเชิงบวก เพื่อให้องค์กรมีภาพลักษณ์ที่ดี

(๖.๕) ทำแผนผลิกฟื้นธุรกิจ (Disaster Recovery Plan : DRP) เพื่อให้ผ่านพ้นวิกฤติไปได้อย่างมีเสถียรภาพ

(๖.๖) คณะกรรมการบริหารความเสี่ยงระดับจัดการ จะต้องถอดบทเรียน (Lesson Learned) เพื่อสรุปประเด็นความเสี่ยง การควบคุม และข้อเสนอแนะ เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพมากยิ่งขึ้น และนำเสนอต่อคณะกรรมการบริหารความเสี่ยงขององค์กร รวมทั้งรายงานต่อบริษัทเพื่อพิจารณาต่อไป

๔.๖.๒.๒ ผลลัพธ์ที่ความคาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ เมื่อผู้เข้ารับการฝึก (Player) ได้รับ MSEL เช่น ระบบไม่สามารถใช้งานได้จะมีวิธีการในการประสานหรือตรวจสอบอย่างไร เช่น ต้องติดต่อหรือ

ประสานงานกับหน่วยงานใด และการประสานงานดังกล่าวได้ถูกต้องครบถ้วนหรือไม่ มีวิธีการรับมือกับแฮกเกอร์และแก้ไขสถานการณ์อย่างไร เริ่มการแก้ไขสถานการณ์จากการประเมินและขั้นตอนการปฏิบัติการภายในหน่วยงานหรือไม่

(๒) ผลการปฏิบัติในการฝึก พบว่า โดยรวมผู้เข้ารับการฝึก (Player) เริ่มมีการวางแผนและการรับมือได้ดีขึ้นตามลำดับ ตลอดจนสรุปผลจากเหตุการณ์ที่เกิดขึ้นได้ดี

๔.๖.๒.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้รับการฝึก (Player) มีความตั้งใจ กระตือรือร้นในแก้ไขปัญหา และให้ความร่วมมือระหว่างหน่วยงานได้ดี มีการคำนึงถึงด้านกฎหมาย และสามารถดำเนินการได้ตามความคาดหวัง อีกทั้ง ผู้เล่นเข้าใจในบริบทของ MSEL ที่ได้รับ มีประสบการณ์และขั้นตอนในการตรวจสอบ แต่ยังมีความสับสนในการใช้เครื่องมือในเรื่องของการสื่อสารที่ใช้ในระบบฝึก (แบบฟอร์ม, เครื่องมือ) และขาดทักษะในเรื่องการถูกโจมตี

(๒) ข้อเสนอแนะ ควรศึกษาและทำความเข้าใจขั้นตอนการปฏิบัติในการแจ้งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแล เมื่อเกิดเหตุการณ์

๔.๖.๓ ด้านการเงินการธนาคาร

๔.๖.๓.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีระบบภายในของระบบการชำระเงินและโอนเงินระหว่างธนาคาร (Interbank Transaction Management and Exchange : ITMX) ไม่สามารถให้บริการได้ ส่งผลกระทบต่อลูกค้าและประชาชน ซึ่งมีผลกระทบทั้ง Sector โดยได้รับการแจ้งระบบโอนเงินของ ITMX ขัดข้อง, ระบบพร้อมเพย์ถูกโจมตี ระบบให้บริการไม่ได้ เนื่องจากมีการทำธุรกรรมสูงขึ้นและได้รับ Email Phishing ซึ่งเป็นการส่ง Email หลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงิน หรือตำแหน่ง

(๑.๑) ปฏิบัติตามกฎเกณฑ์และขั้นตอนต่าง ๆ มีการตั้งคณะกรรมการ จัดการสภาวะวิกฤติ (Crisis Management)

(๑.๒) ITMX operation ดำเนินการตามกระบวนการต่าง ๆ เช่น ตรวจสอบระบบภายใน ITMX เร่งทำให้ระบบให้กลับคืนมาใช้งานได้เร็วที่สุด

(๑.๓) แจ้งธนาคารให้ทราบถึงผลกระทบที่ได้รับ

(๑.๔) ติดต่อประสานงานไปยังหน่วยงานที่เกี่ยวข้อง เพื่อเร่งทำให้ระบบให้กลับคืนมาใช้งานได้เร็วที่สุด

(๑.๕) หากไม่สามารถแก้ไขปัญหาได้ และประชาชนโอนเงินไม่ได้เกิดผลกระทบเป็นวงกว้าง หน่วยงานจะต้องทำการยกระดับ และแจ้งให้ธนาคารต่าง ๆ ที่เกี่ยวข้อง และแจ้งธนาคารแห่งประเทศไทย, TB-CERT และ สกมช. ให้ทราบถึงผลกระทบที่ได้รับ เพื่อให้ส่งผลกระทบต่อประชาชนให้น้อยที่สุด

(๑.๖) แบ่งปันความรู้และประสบการณ์ให้องค์กรต่าง ๆ ทราบ เพื่อให้มีแนวทางในการปัญหาเมื่อเผชิญเหตุการณ์

(๒) กรณีระบบโอนเงินถูกโจมตี ทำให้ระบบซื้อ-ขาย ขัดข้อง ไม่สามารถใช้งานได้ ส่งผลให้นักลงทุนต้องมีการปิดการซื้อ-ขาย หลายชั่วโมง

(๒.๑) การกอบกู้ระบบเป็นขั้นวิกฤติ มีการสั่งการกอบกู้ระบบที่ศูนย์สำรอง โดยตรวจสอบระบบจากศูนย์สำรองที่ไม่ได้รับผลกระทบและดำเนินการทันที หลังจากนั้นประกาศแจ้งการแก้ไขโดยมีมาตรการการป้องกันเรียบร้อยแล้วและเปิดการซื้อ-ขาย ในวันต่อไป

(๒.๒) การสื่อสาร ระหว่างช่วงแก้ไขหรือช่วงแก้ไขแล้ว จะแจ้งการแก้ปัญหาและคอยอัปเดตสถานการณ์ให้นักลงทุน และพิจารณาแถลงข่าว ตลอดจนดำเนินการทางด้านกฎหมาย

(๓) กรณีเกิดการรั่วไหลของข้อมูลบัตรเครดิต (Data Leak) ไปยังดาร์กเว็บ (Dark Web)

(๓.๑) Statement ควรใช้ภาษาที่สั้นและกระชับ และควรเขียนให้มีความชัดเจน เช่น การเยียวยาสำหรับผู้ที่เสียหาย ควรระบุว่า ผู้เสียหายจะได้รับเงินคืนเมื่อไหร่ มาตรการเยียวยามีอะไรบ้าง

(๓.๒) ทำการตรวจสอบออกมาตรการเพื่อเพิ่มความมั่นคงปลอดภัยให้กับหน่วยงานต่าง ๆ ต้องมีแผนสำรองในการทำงานที่ศูนย์ใหญ่

(๓.๓) หากมีการประท้วงและไม่สามารถเข้าปฏิบัติงานได้ จะใช้แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) โดยให้พนักงานไปปฏิบัติงานที่ศูนย์สำรองได้และสามารถให้บริการได้อย่างต่อเนื่อง

๔.๖.๓.๒ ผลลัพธ์ที่คาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ มีการสื่อสารและประสานงานร่วมกันอย่างไร แก้ไขปัญหาที่เกิดขึ้นได้อย่างไร ระหว่างออกแถลงการณ์จะต้องใช้คำพูดเพื่อเยียวยาและข้อมูลจะต้องตรงกัน หลังสถานการณ์คลี่คลายไป จะต้องติดตามดูแลลูกค้า และมีแนวทางในการรับมือได้อย่างทันท่วงที

(๒) ผลการปฏิบัติในการฝึก พบว่า สามารถรับมือได้อย่างดีเยี่ยม และสอดคล้องกับแนวปฏิบัติและแจ้งให้กับ สกมช. ทราบ สามารถใช้เวลาสรุปแนวทางปฏิบัติได้อย่างละเอียดในเวลาที่จำกัด และการประสานงานได้ครบถ้วน มีการสื่อสารต่อลูกค้าได้ทราบรวมถึงลดผลกระทบต่อภาคประชาชน

๔.๖.๓.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้เข้ารับการฝึก (Player) มีการแชร์ความรู้และแนวทางการปฏิบัติกันอย่างดี มีกระบวนการจัดการกับเหตุการณ์ (Incident Management) และแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ในการรับมือ มีการจัดตั้งการประชุมในภาวะที่เกิดเหตุการณ์ไม่ปกติ (War Room) มีแผนในการรับมือและ

ให้ความช่วยเหลือเยียวยาลูกค้า มีการรายงานเหตุการณ์ข้อมูลรั่วไหลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และสำนักงานตำรวจแห่งชาติครบถ้วน มีการ Monitor กระแสสังคม กำหนดกลยุทธ์ที่เหมาะสมในการสื่อสาร มีการตกลงกันใน Sector เพื่อให้ข้อมูลที่สื่อสารออกไปตรงกัน

(๒) ข้อเสนอแนะ หัวใจสำคัญ คือ การตอบสนองเหตุการณ์ที่รวดเร็วในการแจ้งหน่วยงานที่เกี่ยวข้องได้ครอบคลุมและครบถ้วน เพื่อให้ความช่วยเหลือให้การรับมือและการสื่อสารกับประชาชนเพื่อกอบกู้ความน่าเชื่อถือกลับมาให้เร็วที่สุด

๔.๖.๔ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

๔.๖.๔.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีได้รับ Email Phishing ซึ่งเป็นการส่ง Email หลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงิน หรือตำแหน่ง

(๑.๑) วิเคราะห์ข้อมูลของ Email Phishing จริงหรือไม่ พบว่าเป็น Email Phishing จริง และมีมัลแวร์ (Malicious file) แนบมาด้วย

(๑.๒) ตรวจสอบต้นทางของอีเมลว่าส่งมาจากที่ใด และตรวจสอบว่าเป็นไฟล์ลักษณะใด

(๑.๓) นำข้อมูลที่ได้จากการวิเคราะห์ไปสร้างตัวบ่งชี้ภัยคุกคาม Indicator of Compromise (IOC) และนำไปเพิ่มเติมในนโยบาย (Policy) ของ Control ตัวอื่น ๆ เช่น Firewall, อุปกรณ์ตรวจจับการบุกรุก (Intrusion Prevention System : IPS) เพื่อป้องกันการเกิดเหตุการณ์นี้ขึ้นอีก และจากตัวบ่งชี้ภัยคุกคาม (IOC) ที่วิเคราะห์ได้ นำไปใส่ในระบบที่ใช้กรองอีเมล (Mail Gateway) เพื่อให้รู้จัก Email Phishing และทำการปิดกันอีเมลนี้ไม่ให้เข้ามาใหม่ได้

(๑.๔) หากผู้ได้รับอีเมลทำการเปิดไฟล์ที่มีมัลแวร์ (Malicious file) แล้ว ให้ตรวจสอบว่า Malicious file ที่เข้ามา โปรแกรมตรวจจับไวรัส (Antivirus) สามารถตรวจจับหรือป้องกันได้หรือไม่ รวมถึงประเมินความเสี่ยงและผลกระทบ

(๑.๕) หาก Malicious file เป็นตัวใหม่ ป้องกันไม่ได้ ให้ทำการแยกเครื่องที่รัน Malicious file และใช้ซอฟต์แวร์โซลูชั่น Endpoint Detection and Response (EDR) หรือแจ้งให้หยุดใช้เครื่อง

(๑.๖) ส่งข้อมูลที่วิเคราะห์และข้อมูลตัวบ่งชี้ภัยคุกคาม (IOC) ไปยัง TTC-CERT โดยมี Traffic Light Protocol (TLP) เป็นสีส้ม (AMBER) เพื่อวิเคราะห์และประสานงานต่อไป

(๒) มีการโจมตีที่ผ่านทางข้อความในโทรศัพท์มือถือ (Short Message Service : SMS) ในโทรศัพท์มือถือ (Smishing) และเกิดการรั่วไหลของข้อมูล (Data Leak) ไปยังดาร์กเว็บ (Dark Web)

(๒.๑) จัดการประชุมในภาวะที่เกิดเหตุการณ์ไม่ปกติ (War Room) เนื่องจากข้อมูลลูกค้าเกิดการรั่วไหล ซึ่งถือว่าเป็นระดับวิกฤติ

(๒.๒) ทีมรักษาความมั่นคงปลอดภัย (Security) ทำการวิเคราะห์ข้อมูลที่หลุดออกไปว่า หลุดไปทางช่องทางไหน ติดมาจากเครื่องไหน (Server/Laptop) ข้อมูลที่หลุดออกไปเป็นข้อมูลที่ใช้ได้หรือไม่ วิเคราะห์ผลกระทบ ทำการกู้คืนระบบ และทำการ Takedown Service (นำข้อมูลที่รั่วไหลที่ถูกโพสต์ออก)

(๒.๓) ทีมกฎหมาย ประสานงานกับหน่วยงานภาครัฐที่เกี่ยวข้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA), ขอหมายศาลในการปิดกั้น IP Address ที่โจมตี

(๒.๔) ทีมผู้บริหาร จัดทำแผนการจัดการสภาวะวิกฤติ (Crisis Management) และข่าวประชาสัมพันธ์

(๒.๕) ฝ่ายสื่อสารองค์กร แจ้งนักข่าว และลูกค้าที่ได้รับผลกระทบ โดยให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) แถลงข่าว

(๒.๖) ประสานงานหน่วยงานที่เกี่ยวข้อง TTC-CERT, สกมช. และ กสทช. ต่อไป

(๓) กรณีถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ (Ransomware)

(๓.๑) ทีมศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center : SOC) จัดประชุมในภาวะที่เกิดเหตุการณ์ไม่ปกติ (War Room) เพื่อทำการวิเคราะห์ ตรวจสอบข้อมูล

(๓.๒) ทำการ Bypass ระบบ Online Charging เพื่อไม่กระทบกระเทือนต่อลูกค้า สามารถใช้งานต่อไปได้ แต่ Operator ไม่สามารถเก็บเงินได้

(๓.๓) เตรียมพร้อมสถานการณ์ฉุกเฉิน เช่น แผนรับมือ ผู้ดูแลระบบ ฝ่ายช่วยเหลือ (Helpdesk)

(๓.๔) รายงานสถานการณ์ให้กับผู้บริหารระดับสูง กสทช., สกมช. และ TTC-CERT

(๓.๕) ประชาสัมพันธ์ในประกาศกับผู้ใช้งาน หาสาเหตุว่าแฮกเกอร์มาจากไหน เพื่อหาสาเหตุและแก้ไขปัญหาต่อไป

(๓.๖) ทำกู้คืนระบบ คืนค่าระบบ (Restore) จากระบบสำรองข้อมูล (Backup)

(๓.๗) เมื่อมีการใช้งานได้ปกติก็จะประกาศไปช่องทางเดิมเพื่อแจ้งผู้ใช้งานระบบ และแจ้งผลกลับไปทาง กสทช., สกมช. TTC-CERT และจัดทำรายงานเพื่อรายงานต่อผู้บริหารระดับสูง แต่ละส่วนงานต้องทำงานขนานกันไปพร้อม ๆ กัน

(๔) กรณี Autonomous System Number (ASN) ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (National Telecom Public Company Limited : NT) หายไปจาก Internet

(๔.๑) เมื่อได้รับแจ้งว่า ลูกค้าไม่สามารถใช้งานอินเทอร์เน็ตได้จำนวนมาก ศูนย์ปฏิบัติการเครือข่าย (Network Operations Center : NOC) ของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) ทำการตรวจสอบระบบ Network ว่าล่มหรือไม่ หรือมีเหตุการณ์อะไรเกิดขึ้นบ้าง กระทบกับการให้บริการ (Service) ใดบ้าง จากนั้นทำการเปิด Ticket ตามกระบวนการจัดการเหตุการณ์ (Incident Management) ของผู้ให้บริการอินเทอร์เน็ต (ISP)

(๔.๒) ศูนย์ปฏิบัติการเครือข่าย (NOC) ของผู้ให้บริการอินเทอร์เน็ต (ISP) ประสานงานกับทีมเครือข่าย (Network) เพื่อทำการตรวจสอบและแก้ไข

(๔.๓) Network Team รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บริหารระดับสูง

(๔.๔) จัดตั้งการประชุมในภาวะที่เกิดเหตุการณ์ไม่ปกติ (War Room) และใช้แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)

(๔.๕) ศูนย์ปฏิบัติการเครือข่าย (NOC) ของ ผู้ให้บริการอินเทอร์เน็ต (ISP) ประกาศ Manager Breakdown ในระบบ NT ว่าเกิดเหตุอะไรขึ้น และรายงานเหตุกับจาก กสทช., สกมช. และ TTC-CERT

(๔.๖) หน่วยงานประชาสัมพันธ์ ประกาศแจ้งผู้ใช้งานผ่านทางเว็บไซต์และโซเชียลมีเดีย

(๔.๗) Network Team หาสาเหตุจาก Syslog, Core Network, ระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information Event Management : SIEM) เพื่อป้องกันการเกิดเหตุการณ์ซ้ำ พร้อมจัดทำรายงานผู้บริหาร และประสานบริษัทที่บริการดูแล และบำรุงรักษาระบบโปรแกรมให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา (Maintenance Service Agreement : MA) เพื่อทำการกู้คืนรหัสผ่าน (Recovery Password) อุปกรณ์ทั้งหมดที่โดนแฮกทำการกู้คืนค่า Config จากการสำรองข้อมูล (Recovery Backup Config) โดยจัดลำดับการกู้คืนระบบตามแผนบริหารความต่อเนื่อง (Business Continuity Plan : BCP) เมื่อพบช่องโหว่ของอุปกรณ์และแก้ไขปัญหาแล้วเสร็จ พร้อมทั้งทดสอบการเชื่อมต่อระบบ

(๔.๘) เมื่อมีการใช้งานได้ปกติ ทำการแจ้งผู้ใช้งานระบบ กสทช. สกมช. TTC-CERT และจัดทำรายงานเพื่อรายงานต่อผู้บริหารระดับสูง แต่ละส่วนงานต้องทำงานขนานกันไปพร้อม ๆ กัน และประกาศยกเลิกแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)

(๔.๙) ทำการเฝ้าสังเกต (Monitor) หลังจากการกู้คืน ๔ ชั่วโมง จัดทำรายงาน Incident Report Improvement Plan ต่อผู้บริหารตามลำดับต่อไป รวมถึง กสทช. สกมช. TTC-CERT

๔.๖.๔.๒ ผลลัพธ์ที่คาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ เมื่อเกิดเหตุการณ์ขึ้น แจ้งให้ประชาชน/ลูกค้า ที่ได้รับข้อความในโทรศัพท์มือถือ (Short Message Service : SMS) ในการแถลงข่าวมีการประสานงานกับ สกมช. และออกหนังสือแถลงการณ์ของ กสทช. โดยมีรายละเอียดขั้นตอนการแก้ไขปัญหา และมีการเปิดเผยข้อมูลอย่างรวดเร็วและต้องดำเนินการอย่างถูกต้องตามกฎหมาย, จะต้องดำเนินการให้เป็นไปตามแผนของบริษัท ตลอดจนคำนึงถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมายต่าง ๆ และระหว่างการฝึกมีการแชร์ข้อมูล

(๒) ผลการปฏิบัติในการฝึก พบว่า การแก้ไขปัญหาทำได้ค่อนข้างดี ผู้เข้ารับการฝึก (Player) ปฏิบัติได้ตามที่คาดหวังครบทุกข้อ แนะนำให้ใช้ White Team เพิ่มเติม

๔.๖.๔.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้เข้ารับการฝึก (Player) ไม่เข้าใจบทบาทของ White Team โดยภาพรวมค่อนข้างดี ได้ปฏิบัติตามขั้นตอนและแผนรับมือถูกต้องตามมาตรฐาน

(๒) ข้อเสนอแนะ ควรอบรมผู้เข้ารับการฝึก (Player) ในการสื่อสารกับ White Team เพื่อให้เข้าใจบทบาทของ White Team มากขึ้น

๔.๖.๕ ด้านการขนส่งและโลจิสติกส์

๔.๖.๕.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีมีการแจ้งเตือนจาก Firewall ว่าตรวจสอบพบการติดตั้งโปรแกรมที่ Backend เพื่อควบคุม Server และ Database โดย Firewall ได้แจ้งเตือนความผิดปกติกับผู้ดูแลระบบ (Administrator)

(๑.๑) ดำเนินการ Block Port และ IP ที่พยายามติดตั้งโปรแกรมที่ Backend

(๑.๒) ดำเนินการแจ้งผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย แจ้ง White Team (แสดงบทบาทผู้บริหาร) และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกระทรวง (Ministry Chief Information Officer : MCIO) ทราบ

(๒) เจ้าหน้าที่ Admin เปิดดูการตรวจสอบและแจ้งเตือนพบว่า มีข้อมูลสำคัญบางส่วนถูกสำเนาไปจาก Database เช่น อีเมลผู้บริหาร ชื่อผู้ใช้งานและรหัสผ่าน จากนั้นแฮกเกอร์ใช้อีเมลของผู้บริหารส่ง Phishing ไปยังหน่วยงานภายใต้สังกัด

(๒.๑) ดำเนินการเปลี่ยนรหัสของ ผู้ดูแลระบบ (Administrator) เพื่อ Login Database และแจ้ง Admin เพื่อตรวจสอบช่องทางแฮกเกอร์ที่เจาะเข้ามาในระบบ จากนั้นทำการ Block และดำเนินตามแผน IDP (Individual Development Plan) และประเมินสมรรถนะ

(๒.๒) ดำเนินการ แจ้งผู้ใช้งานเปลี่ยนรหัสผ่าน และประชาสัมพันธ์เรื่อง Email Phishing ให้ด้านขนส่งและโลจิสติกส์รับทราบของหน่วยงาน

(๓) กรณีแฮกเกอร์ส่งอีเมลปลอมไปยังผู้โดยสารของระบบ D -Ticket

(๓.๑) เกี่ยวข้องกับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้ครบถ้วน

(๓.๒) ทำการถอดบทเรียน (Lesson Learned) มาดำเนินการป้องกันและลดความเสี่ยง อาจนำเครื่องมือเข้ามาช่วย เช่น Two-Factor Authentication, สร้างความตระหนักในการใช้เทคโนโลยีสารสนเทศ (IT Awareness)

(๔) กรณีระบบควบคุมการเดินรถติดมัลแวร์เรียกค่าไถ่ (Ransomware)

(๔.๑) จัดระดับภัยคุกคามตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งพบว่า เป็นภัยคุกคามระดับร้ายแรง

(๔.๒) ตรวจสอบและบันทึกเหตุการณ์ (Incident) และแจ้งรายงานต่อผู้บริหาร

(๔.๓) ดำเนินตรวจสอบและประสานงานกับฝ่ายเทคโนโลยีสารสนเทศ (IT) เรื่อง มัลแวร์เรียกค่าไถ่ (Ransomware) เครื่องผู้ใช้งาน (Client)

(๔.๔) ประสานหาเครื่องสำรองหรืออุปกรณ์ที่สามารถนำมาเปลี่ยนทดแทนเพื่อให้ระบบสามารถใช้งานได้หรือไม่

(๔.๕) ประชาสัมพันธ์ไปยังผู้โดยสารในแต่ละสถานีถึงความล่าช้าของขบวนรถ และขออภัยในความไม่สะดวก

(๔.๖) ประสานไปยัง บริษัทผู้ดูแลระบบ Call Center เพื่อตอบคำถามผู้โดยสารดำเนินการเปลี่ยนเครื่องทดแทนที่ศูนย์การควบคุมการเดินรถที่เป็นส่วนกลาง โดยจะใช้เวลา ๑๐-๑๕ นาที ในการเปลี่ยนทดแทนระบบ เพื่อทำให้ศูนย์ควบคุมกลับมาใช้งานได้ ในระหว่างที่เปลี่ยนก็จะมีระบบที่สามารถโอนไปยังสถานีปลายทางให้สามารถควบคุมรถแทนศูนย์ควบคุมกลางได้ เพื่อไม่ให้เสียเวลาเดินรถมากขึ้น

(๔.๗) ทำการถอดบทเรียน (Lesson Learned) เพื่อรองรับสถานการณ์ดังกล่าวและลดปัญหาให้สามารถแก้ไขปัญหาได้เร็วขึ้น โดยการปรับแผนผลิกฟื้นธุรกิจ (Disaster Recovery Plan : DRP) และแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ต่อไป

(๕) กรณีระบบการชำระเงินที่สถานีได้รับ Email Phishing ซึ่งเป็นการส่ง Email หลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงิน หรือตำแหน่ง ซึ่งมีผลกระทบต่อการให้บริการ

(๕.๑) ตอบสนองต่อเหตุการณ์ (Response) ต่อหน่วยงานที่เกี่ยวข้อง คือ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ผู้โดยสาร และหน่วยงานบริหารจัดการภายในสถานี เพื่อลดผลกระทบตามแผนการจัดการเหตุการณ์ที่มี เช่น การใช้ตั๋วโดยสารทดแทนการจัด Gate ทดแทน

เพื่อให้การบริการดำเนินไปได้ และสื่อสารให้ผู้โดยสารหรือผู้ใช้บริการและ รฟม. ได้รับทราบเหตุการณ์ต่าง ๆ เป็นระยะ ๆ

(๕.๒) ดำเนินการกู้คืนระบบการชำระเงินตามแผนที่มี

(๖) กรณีเครื่องผู้ใช้งาน (Client) ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ (Ransomware)

(๖.๑) ตรวจสอบและวิเคราะห์ว่าเป็นภัยไซเบอร์หรือไม่ มีเหตุการณ์เกิดขึ้นและจะเข้าตรวจสอบสถานการณ์ว่าเป็นอย่างไร และแก้ไขสถานการณ์ถึงขั้นตอนใด เกิดขึ้นที่เครื่องใด กระทบเครื่องอื่นหรือไม่

(๖.๒) รับมือและลดความเสี่ยง ตามมาตรา ๖๐ โดยแก้ไขเครื่องที่มีปัญหาและตัดระบบเครือข่าย (Network) ก่อน เพื่อป้องกันไว้ก่อนเพื่อไม่ให้กระจายไปในส่วนอื่น และแจ้งให้ทราบเมื่อแก้ปัญหาเสร็จสิ้นแล้ว

(๖.๓) ทีมสื่อสารองค์กร ประสานงานไปยังผู้ดูแลระบบ และประเมินผลกระทบที่จะเกิดขึ้น และแจ้งหน่วยงานควบคุมหรือกำกับดูแล Sector ที่เกี่ยวข้อง และ National CERT เมื่อประเมินแล้วเป็นภัยคุกคามประเภทมัลแวร์เรียกค่าไถ่ (Ransomware) ให้ทำการตัดสัญญาณและดำเนินการสำรองข้อมูล (Backup) ทั้งหมดที่เกี่ยวข้อง โดยใช้เวลากู้คืนระบบ (Recovery) ๓ ชั่วโมง จากนั้นทำการรวบรวมข้อมูลเพื่อแจ้งความดำเนินการทางกฎหมายและประชาสัมพันธ์ให้กับประชาชนได้รับทราบ

(๗) กรณีมีประกาศ ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ (Ransomware) เครื่องแม่ข่ายของระบบจำหน่ายตั๋ว (D-Ticket) โดยมีสาเหตุมาจาก Email Phishing ทำให้ไม่สามารถใช้งานได้ทั้งระบบ

(๗.๑) ประสานงานกับบริษัท แอ็ดวานซ์อินฟอร์เมชั่นเทคโนโลยี จำกัด (มหาชน) (AIT) ซึ่งเป็นผู้ดูแลระบบ D-Ticket เพื่อดำเนินการตรวจสอบปัญหา และผลกระทบที่เกิดขึ้น

(๗.๒) ฝ่ายเทคโนโลยีสารสนเทศ (IT) แจ้งตามมาตรา ๕๘ และรายงานตามมาตรา ๕๗ ไปยังหน่วยงานควบคุมหรือกำกับดูแล และ National CERT

(๗.๓) ประเมินตามมาตรา ๖๐ และยืนยันโดยใช้เครื่องมือ cyberact60.ncsa.or.th ว่าเป็นภัยคุกคามระดับร้ายแรง เนื่องจากไม่สามารถใช้งานได้ทั้งระบบ

(๗.๔) รายงานผู้บริหาร และแจ้งประชาสัมพันธ์ไปยังผู้โดยสารให้รับทราบว่า ระบบ D-Ticket ขัดข้อง ไม่สามารถจองตั๋วแบบ Online ได้

(๗.๕) ประสานงานกับบริษัท AIT เพื่อทำการตัดระบบออกจากเครือข่าย

(๗.๖) ทำการเปลี่ยนรหัสผ่านระบบทั้งหมด โดยเฉพาะรหัสผ่านที่ใช้ซ้ำกับระบบที่พบมัลแวร์เรียกค่าไถ่ (Ransomware)

(๗.๗) ทำการสำรองข้อมูลที่ถูกเข้ารหัสไว้ ในกรณีที่อาจมีความเป็นไปได้ในการที่จะถอดรหัสไฟล์และข้อมูลที่ถูกเข้ารหัสในอนาคต

(๗.๘) ลบไฟล์ที่เกี่ยวข้องทั้งหมดแล้วกู้คืนจากสำเนาข้อมูลที่ไม่ติดเชื้อขึ้นระบบใหม่

(๗.๙) จัดเก็บหลักฐานดิจิตอลจากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อทำการตรวจสอบเพิ่มเติม

(๗.๑๐) ใช้เวลากู้คืนระบบ ๓ ชั่วโมง

(๗.๑๑) Switch ไปที่ DR-Site เพื่อแก้ปัญหามัลแวร์เรียกค่าไถ่ (Ransomware)

(๗.๑๒) ดำเนินการแจ้งสำนักงานตำรวจแห่งชาติ เนื่องจากเป็นความผิดทางอาญาในการใช้มัลแวร์เรียกค่าไถ่ (Ransomware) ประสานหน่วยงานผ่านทาง Website, Social Media, Call Center แจ้งว่าระบบสามารถใช้งานได้ตามปกติแล้ว

(๘) กรณีได้รับแจ้งจากทีมการเงินว่าผู้โดยสารไม่สามารถชำระเงินผ่านทางบัตรเครดิตได้

(๘.๑) ตรวจสอบการเชื่อมต่อเครือข่ายว่าผิดปกติหรือไม่

(๘.๒) แจ้งทีมสื่อสารองค์กร ประสาน Call Center ให้แจ้งผู้โดยสาร ขอรับการชำระเงินผ่านช่องทางการเงินที่เป็นเงินสดแทน ประสานธนาคารเพื่อแจ้งปัญหา

(๘.๓) เมื่อธนาคารแจ้งว่า สามารถชำระเงินผ่านทางบัตรเครดิตได้แล้ว ให้ทำการตรวจสอบกับเครือข่ายอีกครั้งว่าสามารถใช้งานได้หรือไม่ จึงได้พบว่า เครื่องทำรายการด้วยบัตรเครดิต ต้องมีการ Reset ก่อน ๑ ครั้ง ที่จะกลับมาใช้งานครั้งต่อไป จึงประสานไปยังเจ้าหน้าที่ประจำสถานีให้ทำการ Reset เพื่อใช้งานได้ตามปกติ

(๙) กรณีแฮกเกอร์ทำการโจมตีผ่านทางช่องโหว่ของอุปกรณ์ที่มี Public IP และพยายามเข้าถึง Backend Server ของระบบจำหน่ายตั๋ว (D-Ticket) เพื่อจารกรรมข้อมูล หรือทำให้ระบบไม่สามารถใช้งานได้

(๙.๑) ประสานงานกับบริษัท AIT ซึ่งเป็นผู้ดูแลระบบ D-Ticket เพื่อดำเนินการตรวจสอบปัญหา และผลกระทบที่เกิดขึ้น และแจ้งผู้เชี่ยวชาญทางเทคโนโลยีสารสนเทศ (IT Expert) เพื่อดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๙.๒) เมื่อประสานกับบริษัท AIT พบว่า ระบบยังใช้งานได้ แต่ตรวจพบ IP แปลกปลอมพยายามโจมตีผ่านช่องโหว่เพื่อต้องการเข้าถึง Backend Server

(๙.๓) ประเมินภัยคุกคามแล้ว อยู่ในระดับไม่ร้ายแรง เนื่องจากยังไม่ส่งผลกระทบต่อการให้บริการและไม่มีผลทางกฎหมาย

(๙.๔) แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล และ National CERT ตามมาตรา ๕๖ ผ่านแบบฟอร์มการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์

(๙.๕) รายงานหน่วยงานควบคุมหรือกำกับดูแล และ National CERT ตามมาตรา ๕๗ ผ่านแบบฟอร์ม Log Book

(๙.๖) ฝ่าย IT Expert แนะนำผู้ดูแลระบบจำหน่ายตั๋ว (D-Ticket) Update Patch ของอุปกรณ์ให้เป็น Version ล่าสุดและปิด Port ที่ไม่ใช้งานให้หมด

(๙.๗) บริษัท AIT ดำเนินการสแกนช่องโหว่และแก้ไขเรียบร้อยสมบูรณ์ เนื่องจาก ตรวจพบไม่เจอการโจมตีทาง Backend แล้ว

(๑๐) กรณีระบบไฟฟ้ามีปัญหา จะมีการตรวจสอบไปยังหน่วยงานที่เกี่ยวข้อง ว่าเกิดจากระบบหรือเกิดจากภัยคุกคาม เพื่อเตรียมการป้องกันและแก้ไข

(๑๐.๑) มีการตรวจสอบว่าระบบสำรองไฟฟ้าใช้งานได้นานเท่าไหร่ ใช้เวลาเท่าไหร่ ทางการไฟฟ้าถึงจะกู้ระบบคืนได้

(๑๐.๒) แจ้งทีมสื่อสารองค์กร ให้ติดต่อ Call Center และผู้โดยสารว่า ขณะนี้มีเหตุขัดข้อง ขอหยุดใช้บริการชั่วคราว และเมื่อระบบไฟฟ้าพร้อมใช้งานได้ปกติจะรีบแจ้งให้ทราบโดยเร็ว

(๑๐.๓) เมื่อระบบกลับมาปกติ ตรวจสอบระบบสำรองไฟฟ้าว่า ได้เปลี่ยนเป็นระบบปกติแล้วหรือไม่ แบตเตอรี่มีการชาร์จเหมือนเดิมหรือไม่ พร้อมแจ้งทีมสื่อสารองค์กร

(๑๑) กรณีภัยธรรมชาติ มีพายุหนักมาก ส่งผลให้แหล่งจ่ายไฟฟ้าของรถไฟฟ้าที่เสียหายทั้งหมด

(๑๑.๑) ทำการวิเคราะห์ว่าเป็นเคสระดับใด เมื่อวิเคราะห์แล้วว่าเป็นเคสที่วิกฤติรุนแรง ให้แจ้งหน่วยงานควบคุมหรือกำกับดูแล Sector ที่เกี่ยวข้อง หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้อง

(๑๑.๒) แจ้งทีมสื่อสารองค์กรให้ประสานไปที่ Call Center และผู้โดยสารในการหยุดการเดินทาง พร้อมทั้งเหตุผล จากนั้นทำการเคลื่อนย้ายผู้โดยสารไปยังจุดที่ปลอดภัย รถไฟฟ้าที่ยังไม่ได้เข้าศูนย์ซ่อม เพื่อรอการไฟฟ้าเข้ามาซ่อมแซม

(๑๑.๓) รายงานเหตุการณ์ (Incident Report) เสนอผู้บริหารต่อไป

๔.๖.๕.๒ ผลลัพธ์ที่คาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ ศึกษาและวิเคราะห์ รวมถึงเรียนรู้จากหน่วยงานใน Sector ได้อย่างดี และในส่วนของการโจรกรรมข้อมูล อาจจะเกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งจะต้องคำนึงถึงว่าจะต้องดำเนินคดีทางกฎหมายหรือไม่ จะเกิดการรั่วไหลของข้อมูลหรือไม่ แนวทางการปฏิบัติ Security Control Baseline เอามาใช้อ้างอิงได้อย่างครบถ้วน

(๒) ผลการปฏิบัติในการฝึก พบว่า ผู้เข้ารับการฝึก (Player) ดำเนินการได้ดีเกินความคาดหวังที่ตั้งไว้และมีการวิเคราะห์ได้ตรงประเด็นจากปัญหาร้ายแรงถึงร้ายแรงมาก, ข้อมูลที่ได้จัดทำ

มีการรับมือตามขั้นตอนที่ถูกต้อง, ผู้เข้ารับการฝึก (Player) มีความกระตือรือร้นและรับมือได้ดีมากยิ่งขึ้น รวมถึงการรายงานข้อมูลทุกขั้นตอนทำหน้าที่ได้พึงพอใจมากขึ้น

๔.๖.๕.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า โจทย์ฝึกมีความท้าท้าย ผู้เข้ารับการฝึก (Player) ตอบโจทย์และรับมือกับสถานการณ์ได้เป็นอย่างดี บางครั้งการตอบสนองต่อเหตุการณ์ล่าช้า โดยรวมทำได้ดีมาก

๔.๖.๖ ด้านพลังงานและสาธารณูปโภค

๔.๖.๖.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีได้รับการขู่ว่าจะทำการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญของภาครัฐ (Domain *go.th) ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) โดยขู่ผ่านช่องทาง Social Media ต่าง ๆ เช่น Facebook, Twitter, Website ต่าง ๆ ทำให้หน่วยงานภาครัฐทราบกันโดยทั่วไปว่าจะมีการโจมตี

(๑.๑) ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Response Team : CSIRT) ของหน่วยงาน ทำการตรวจสอบแหล่งที่มาของข่าวการโจมตีทางไซเบอร์โครงสร้างพื้นฐานของรัฐว่าจริงหรือไม่ ซึ่งต้องยืนยันจากหลายหน่วยงาน โดเมน *go.th

(๑.๒) ตรวจสอบยืนยันข่าว รายชื่อของหน่วยงาน Sector พลังงาน ที่ใช้โดเมน *go.th เพื่อยืนยันกลับไปยัง สกมช.

(๑.๓) ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ของหน่วยงานประเมินเหตุการณ์ว่ามีผลกระทบต่อระบบโครงสร้างที่สำคัญของประเทศระดับใด แจ้งทางผู้บริหารและผู้เกี่ยวข้องทราบ

(๑.๔) จัดประชุมผู้บริหารระดับสูงโดยด่วน ตามแผนรับมือเหตุการณ์ (Incident Response plan) ขององค์กร เพื่อยกระดับมาตรการการเฝ้าระวังภัยคุกคามทางไซเบอร์

(๑.๕) พิจารณาตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรณีนี้ส่งผลกระทบให้ต้องดำเนินการอย่างไร

(๑.๖) เตรียมความพร้อม ระบบสำรองข้อมูล (Backup) และวิธีการสำรองข้อมูลในกรณีที่ระบบหลักเกิดความเสียหาย จะสามารถใช้ข้อมูลที่สำรองไว้มาทำงานต่อได้ทันที (Disaster Recovery Site : DR Site)

(๒) กรณี โดยแนบ MalDoc หรือ Malicious Code มากับอีเมลเพื่อการโจมตีแบบ Phishing โดยมุ่งเป้าไปที่ผู้ปฏิบัติงานขององค์กร

(๒.๑) ทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ตรวจสอบความผิดปกติของ Email นี้ว่าผิดปกติจริงหรือไม่

(๒.๒) หากพบว่าผิดปกติ จึงดำเนินการค้นหา IP ต้นทาง แล้วทำการปิดกั้น IP (Block IP) ต้นทางนั้นที่ Mail Gateway และดำเนินการลบอีเมลในกล่องข้อความขาเข้า (Inbox) ของผู้ใช้งาน

(๒.๓) ตรวจสอบจำนวนผู้ใช้งานทั้งหมดที่ได้รับ Email Phishing แล้วส่งเมลแจ้งเตือนไปยังผู้ใช้งานที่ได้รับอีเมล หากมีผู้ใช้งานได้รับจำนวนมาก ให้ดำเนินการส่งเมลแจ้งเตือนทั้งองค์กรเพื่อสร้างความตระหนัก

(๒.๔) รายงานผู้บริหารเพื่อทราบ

(๓) กรณีพบฟังก์ชัน การทำงานหรือพฤติกรรมที่เป็นมัลแวร์เรียกค่าไถ่ (Ransomware) ชนิดแพร่ตัวเองได้โดยไม่ต้องพึ่ง Hacker ทำให้ Antivirus ขององค์กรไม่รู้จัก (Zero Day Situation)

(๓.๑) นำ IOC Hash หรือ File Hash ที่ได้ Update Signature ที่อุปกรณ์ Security ต่าง ๆ เช่น Firewall, อุปกรณ์ตรวจจับการบุกรุก (Intrusion Prevention System : IPS), ระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information Event Management : SIEM) หรือ ระบบที่ใช้กรองอีเมล (Mail Gateway) พร้อมแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคาม (IOC) ไปยังหน่วยงานภายใน Sector เพื่อทำการเฝ้าระวังต่อไป

(๓.๒) เร่งรัดบริษัทให้สร้าง Signature ออกมา แล้วส่งให้อัปเดตไปยัง Antivirus ทุกเครื่องในองค์กร

(๓.๓) ตรวจสอบช่องโหว่ของระบบ ประเมินผลกระทบและปิดช่องโหว่ที่มีอยู่ในองค์กร เช่น การประสานงานให้ Update Patch ล่าสุดของระบบปฏิบัติการ (OS) หรือเฟิร์มแวร์

(๓.๔) รายงานหน่วยงานควบคุมหรือกำกับดูแล ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

(๔) กรณีเครื่องได้เชื่อมต่อระบบควบคุมการจ่ายไฟฟ้า ติดมัลแวร์เรียกค่าไถ่ (Ransomware) และแพร่ไปยัง Server ของระบบควบคุมการจ่ายไฟฟ้า ส่งผลให้ระบบการจ่ายไฟฟ้าใช้งานไม่ได้บางส่วน

(๔.๑) แยกเครือข่ายใน DMZ (Demilitarized Zone) ออกมาจาก Production และอื่น ๆ

(๔.๒) ตรวจสอบเครื่องแม่ข่าย (Server) ทุกเครื่องว่าได้รับผลกระทบหรือไม่ แยกระบบสำรองข้อมูล (Backup) ออกมาเพื่อไม่ให้ได้รับผลกระทบ แจ้งผู้บังคับบัญชาเพื่อให้มีการประกาศใช้แผนตอบสนองต่อเหตุการณ์ (Incident Response plan) จากการประเมิน เห็นว่าเป็นเหตุการณ์ร้ายแรง จึงดำเนินการตามตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๕) กรณีผลกระทบต่อเนื่องจาก มัลแวร์เรียกค่าไถ่ (Ransomware) เข้าไปใน Production Zone ทำให้ระบบการควบคุมการจ่ายไฟใช้งานไม่ได้ ๑๐๐%

(๕.๑) แจ้งผู้บริหารอนุมัติสั่งการและขออนุมัติใช้แผนบริหารความต่อเนื่อง (Business Continuity Plan : BCP) เปิดช่องทางการสั่งการฉุกเฉิน กระจายอำนาจการสั่งการไปยังภูมิภาค เพื่อให้แต่ละภูมิภาคมีอำนาจให้การสั่งการดูแลการจ่ายไฟได้ด้วยตนเอง และแจ้งหน่วยงานการไฟฟ้า และ สกมช. ให้ทราบ

(๖) กรณีฟ้าผ่าลงมายังสายส่งไฟฟ้า ทำให้ไฟดับในบริเวณกว้าง

(๖.๑) ทีมปฏิบัติงาน รวบรวมข้อมูลว่า ไฟฟ้าดับที่ใดบ้าง ประเมินเวลาในการกู้ไฟฟ้ากลับมา แจ้งผู้บริหารเพื่อจัดทำแผน Backout Restoration Plan

(๖.๒) ทีม Security สอบสวนหาสาเหตุ เมื่อตรวจสอบพบว่าอยู่ในระดับวิกฤติ ให้แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล เพื่อรายงานไปยัง Sector ข้างเคียงที่ได้รับผลกระทบให้ทราบถึงสาเหตุ ประมาณการเวลาในการแก้ไข และแจ้ง สกมช. ทราบ อีกทั้ง เตรียมข้อมูลในการชี้แจงประชาชนและสื่อมวลชน

(๗) กรณีหลังจากผู้บริหารสูงสุดขององค์กรเรียกประชุมผู้บริหารภายในกรณีการรียกค่าไถ่ และมีมติว่าจะไม่จ่ายเงินค่าไถ่ ต่อมากลุ่ม Red_Axe และ Blue_Eagle ดำเนินการตอบโต้หรือแก้แค้น โดยการเผยแพร่เหตุการณ์การติดมัลแวร์เรียกค่าไถ่ (Ransomware) ทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบ SCADA/EMS/DMS ขององค์กรนี้ต่อสื่อมวลชน ทั้งในและต่างประเทศ เพื่อให้เสียชื่อเสียง

(๗.๑) นัดประชุมโดยประสานงานหน่วยควบคุมหรือกำกับดูแล

(๗.๒) การแชร์ข้อมูลระหว่าง ๓ หน่วยงาน ได้แก่ การไฟฟ้า, บริษัท ปตท. จำกัด (มหาชน) และหน่วยงานทางด้านสาธารณูปโภคอื่น ๆ ในเรื่องผลกระทบที่เกิดขึ้นจากการโจมตีครั้งนี้ และวิธีการที่ใช้รับมือ เพื่อให้ได้ข้อสรุปในทิศทางเดียวกัน

(๗.๓) เตรียมรายงานสรุปข้อมูลสำหรับการแถลงข่าว ให้กับผู้บริหารรับทราบ และรัฐมนตรีเพื่อแถลงข่าวกับสื่อมวลชน

(๗.๔) Monitor สื่อ Social ต่าง ๆ เพื่อเตรียมการรับมือ Fake News ที่อาจตามมา

(๘) กรณีผู้บริหารสูงสุดขององค์กรสั่งการให้ผู้บริหารหน่วยงานและทีมผู้ดูแลระบบ Cyber Security ของหน่วยงานให้ดำเนินการกู้คืนระบบ SCADA/EMS/DMS และเก็บหลักฐานการกระทำความผิดของผู้ประสงค์ร้าย

(๘.๑) พิจารณาประเมินแนวทางการจัดการการกู้คืนระบบ SCADA/EMS/DMS รวมถึงเครื่อง Sever ใน DMZ และการเก็บหลักฐานการกระทำผิดอาจเลือกได้แบบใดแบบหนึ่งแล้วแต่องค์กรจะพิจารณา ทำโดยทีมตอบโต้ภายในหรือภายนอกองค์กร

(๘.๒) พิจารณาการเก็บหลักฐานให้ได้มากที่สุดจากอุปกรณ์ Network ต่าง ๆ (Switch/Firewall) และระบบปฏิบัติการ (OS) ของ Server ต่าง ๆ ไว้ก่อน โดยการดำเนินการกู้คืนระบบ (Recovery) ที่เครื่อง Standby ให้กลับมา Active จะทำโดยผู้ดูแลระบบ (Administrator) ของระบบ SCADA/EM5 สำหรับการเก็บหลักฐานการกระทำความผิดจะทำที่เครื่อง Active โดย ผู้ดูแลระบบของระบบเทคโนโลยีสารสนเทศ (IT) ขององค์กร

(๘.๓) เก็บหลักฐานให้ได้มากที่สุดอย่างรวดเร็ว โดยระหว่างนั้นการดำเนินการใช้งานระบบแบบ Manual หรือระบบสำรองไปก่อน

(๘.๔) เก็บหลักฐานให้ได้มากที่สุดจากระบบหลักและระบบสำรองที่ถูกมัลแวร์เรียกค่าไถ่ (Ransomware) โจมตีทั้งสองระบบ ระหว่างนั้นนำระบบ Offline/Isolate System เป็นระบบที่ไม่ได้เชื่อมต่อเครือข่ายในภาวะปกติ (ใช้ในภาวะฉุกเฉินเท่านั้น) แทน

(๘.๕) แจ้ง Operator เพื่อนำระบบเข้าใช้งาน โดยต้องพิจารณดำเนินการ Update Patch หรือแก้ไขหาเพิ่มก่อน

(๘.๖) Monitor ระบบอย่างใกล้ชิดและต่อเนื่อง เพื่อเฝ้าระวังการเกิดเหตุการณ์ซ้ำ

(๘.๗) จัดทำรายงานสรุปเพื่อแจ้งผู้บริหารรับทราบ และนำเหตุการณ์ที่เกิดขึ้นมาทำ Lesson Learned ภายในองค์กรและเผยแพร่แก่หน่วยงานอื่นใน Section เดียวกันหรือ Section ที่เกี่ยวข้อง

๔.๖.๖.๒ ผลลัพธ์ความคาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ มีการแชร์ข้อมูลระหว่างหน่วยงานเพื่อให้ได้ข้อสรุปในทิศทางเดียวกัน และมีการถอดบทเรียน (Lesson Learned) ภายในองค์กรและเผยแพร่แก่หน่วยงานอื่น ๆ ใน Section เดียวกัน Monitor สื่อ Social ต่าง ๆ เพื่อเตรียมการรับมือกับ Fake News ที่อาจตามมา

(๒) ผลการปฏิบัติในการฝึก พบว่า บางครั้งผู้เข้ารับการฝึก (Player) ไม่เข้าใจในโจทย์ต้องพยายามอธิบายอีกครั้งเพื่อทำความเข้าใจ กรณีที่เป็นเหตุการณ์ระดับไม่ร้ายแรง เน้นทางเทคนิคมากไป ไม่ได้ใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เป็นแนวทางในการแก้ไขสถานการณ์ และไม่ค่อยใช้ประโยชน์จาก White Team

๔.๖.๖.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้เข้ารับการฝึก (Player) มีการประสานงานที่ดีและมีการส่งต่อข้อมูลอย่างเป็นระบบ มีการทำงานที่ดีเป็นการปรึกษากันภาพรวมดีขึ้น

(๒) ข้อเสนอแนะ ควรแจ้งระดับความรุนแรง โดยเปรียบเทียบภัยคุกคามตามหมวดหมู่ เช่น หมวดหมู่ไหนควรแจ้งทุก ๆ ๑๐ นาที เป็นต้น

๔.๖.๗ ด้านสาธารณสุข

๔.๖.๗.๑ ขั้นตอนการแก้ไขปัญหาของผู้เข้ารับการฝึก (Player) จาก MSEL ที่ได้รับ มีดังนี้

(๑) กรณีเกิดการรั่วไหล (Data Leak) ของข้อมูลสุขภาพ

(๑.๑) แจ้งเหตุการณ์ให้ทีมเทคโนโลยีสารสนเทศ (IT) ประสานงานกับส่วนที่เป็น Outsource และผู้เชี่ยวชาญภายในหน่วยงาน

(๑.๒) รายงานผู้บังคับบัญชาตามลำดับชั้น รวมทั้งรายงานไปยัง National CERT ให้รับทราบการดำเนินการ

(๑.๓) กู้คืนระบบให้กลับสู่สภาพเดิม รายงานความเสียหาย

(๑.๔) เครื่องคอมพิวเตอร์ที่ได้ถูกเข้ารหัส จะตัดการเชื่อมต่อ ส่วนอุปกรณ์จัดเก็บข้อมูล (Hard disk) ที่ถูกเข้ารหัส จะนำไปตรวจสอบ เพื่อกู้คืนและค้นหาสาเหตุ

(๒) ระบบบัญชีใช้งานไม่ได้

(๒.๑) แจ้งทีมเทคโนโลยีสารสนเทศ (IT) ให้ทำการตรวจสอบและวิเคราะห์สถานการณ์ พบว่า มีผลกระทบน้อยมากและได้แก้ไขปัญหาอย่างรวดเร็วและเรียบร้อย

(๓) ระบบ Internet Banking และ Mobile Banking ชำระเงินทางการแพทย์ไม่ได้

(๓.๑) แจ้งสื่อสารองค์กร ประกาศให้ประชาชนชำระเงินเป็นเงินสด เนื่องจากเกิดผลกระทบบางส่วนเท่านั้น ไม่ได้กระทบทั้งกระทรวงสาธารณสุข และยังคงให้บริการได้

(๔) หมายเลขประจำเครื่องคอมพิวเตอร์ (Internet Protocol Address : IP Address) ของกระทรวงสาธารณสุข พบช่องโหว่ Apache (Zero day)

(๔.๑) ตรวจสอบแล้วใช้งานได้ แต่มีความเสี่ยงในการถูกโจมตี ซึ่งเป็นภัยร้ายแรง

(๔.๒) แจ้งทาง National CERT ให้รับทราบ และทำการปิดช่องโหว่ในระบบ

(๔.๓) ประกาศให้ฝ่ายที่ใช้งานระบบที่มีการใช้งาน Apache ได้มีการอัปเดตแพตช์ (Patch)

(๕) กรณีเว็บไซต์ (Website) ถูกโจมตีโดย SQL Injection ด้วยการ Remote เข้ามายึดเครื่องของ Server ได้

(๕.๑) ตัดระบบการเชื่อมต่อ ทำการวิเคราะห์และตรวจสอบ Server รวมถึง Coding ต่าง ๆ ร่วมกับหน่วยงานควบคุมหรือกำกับดูแล และ National CERT เพื่อทำการแก้ไข

(๖) กรณีถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ (Ransomware)

(๖.๑) ตัดระบบออกไปให้ทางผู้พัฒนาระบบเทคโนโลยีสารสนเทศ (IT) เข้ามาบูรณาการการกู้คืนข้อมูล

(๖.๒) ประสานขอความช่วยเหลือจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกระทรวงสาธารณสุข และโรงพยาบาลที่ได้รับผลกระทบ แจ้งความไปทางสำนักงานตำรวจแห่งชาติและทำการกู้ข้อมูลคืน

(๖.๓) รายงานไปยัง National CERT และจัดประชุมระหว่างสื่อสารองค์กร National CERT ในการออกแถลงการณ์เกี่ยวกับเหตุการณ์ที่เกิดขึ้น

๔.๖.๗.๒ ผลลัพธ์ที่คาดหวังของ Game Master ต่อการแก้ไขปัญหาของผู้เข้ารับการฝึก

(๑) แนวทางดำเนินการที่คาดหวัง คือ ผู้เข้ารับการฝึก (Player) มีความตระหนักและการดำเนินการต่าง ๆ ตามกฎหมาย

(๒) ผลการปฏิบัติในการฝึก พบว่า หลังจากการกู้ระบบเสร็จสิ้น ยังขาดแนวทางการป้องกันว่าจะมีแผนรับมืออย่างไรหากถูกโจมตีอีกครั้ง และขาดการลงรายละเอียดในเรื่องของข้อกฎหมายให้มีความชัดเจน โดยภาพรวมเป็นที่น่าพอใจ มีการพัฒนา ปรึกษา และตอบโต้กันมากขึ้น

๔.๖.๗.๓ ผลการสังเกตการณ์และข้อเสนอแนะ จากผู้ประเมินการฝึก (EEG)

(๑) ผลจากการสังเกตการณ์ พบว่า ผู้เข้ารับการฝึก (Player) มีความกระตือรือร้นในการตอบคำถามเพิ่มขึ้น โดยภาพรวมค่อนข้างดีขึ้นมาก มีการดำเนินการแจ้งเหตุและประเมินเหตุการณ์

(๒) ข้อเสนอแนะ ควรมีส่วนในการดำเนินคดีทางกฎหมายด้วย

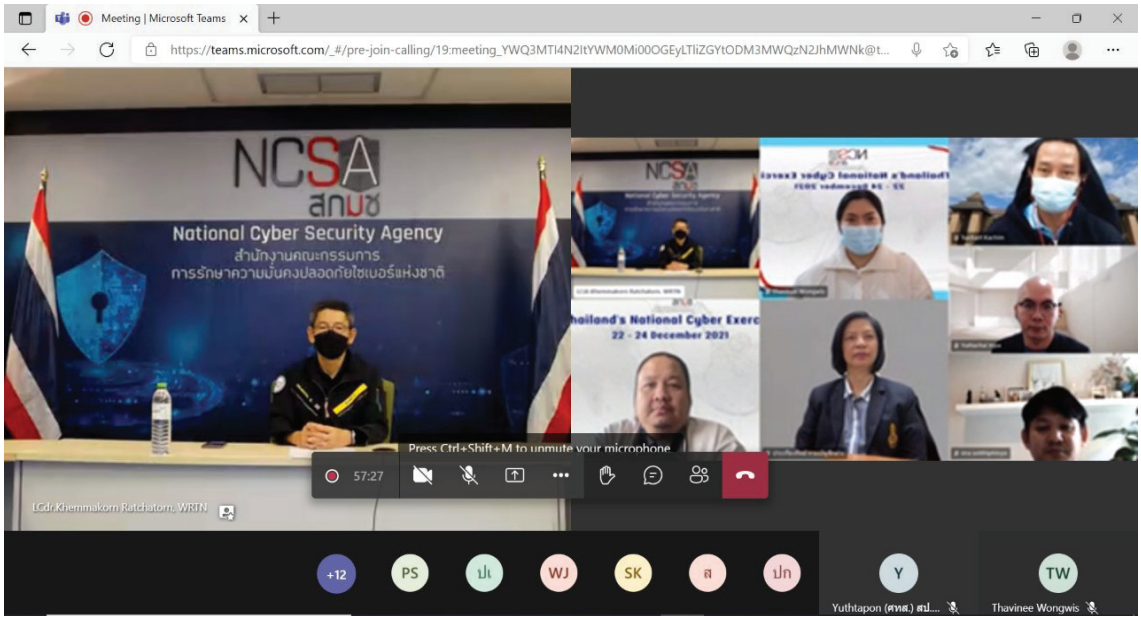
๔.๗ การตรวจเยี่ยมการฝึก

รูปที่ ๔-๑ การตรวจเยี่ยม ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร

รูปที่ ๔-๑ การตรวจเยี่ยม ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร

รูปที่ ๔-๑ การตรวจเยี่ยม ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร

รูปที่ ๔-๑ การตรวจเยี่ยม ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร



รูปที่ ๔-๒ การตรวจเยี่ยมในรูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

รูปที่ ๔-๒ การตรวจเยี่ยมในรูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์

ด้วยการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นการจัดขึ้นครั้งแรก จึงได้มีแนวคิดในการจัดให้มีการตรวจเยี่ยมการฝึกขึ้น เพื่อให้ผู้บริหาร หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีความเข้าใจบทบาทและหน้าที่เกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพิ่มมากขึ้น

๔.๗.๑ กำหนดการตรวจเยี่ยมการฝึก

การตรวจเยี่ยมการฝึก จัดขึ้นเมื่อระหว่างวันที่ ๒๓ - ๒๔ ธันวาคม พ.ศ. ๒๕๖๔ ซึ่งสามารถตรวจเยี่ยมการฝึกได้ ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า อาคารศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร หรือในรูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์ ทั้งนี้ การรับคณะตรวจเยี่ยมนั้น แบ่งเป็น ๒ ช่วงเวลา ได้แก่ ภาคเช้า เวลา ๑๐.๐๐ - ๑๑.๑๕ น. และภาคบ่าย เวลา ๑๓.๓๐ - ๑๔.๔๕ น. มีรายละเอียดดังนี้

ภาคเช้า	ภาคบ่าย	กำหนดการ
๑๐.๐๐ – ๑๐.๓๐ น.	๑๓.๓๐ – ๑๔.๐๐ น.	คณะตรวจเยี่ยมเดินทางมาถึง หรือเข้าสู่ระบบ
๑๐.๓๐ – ๑๐.๓๕ น.	๑๔.๐๐ – ๑๔.๐๕ น.	ลธ.กมช. หรือผู้แทน กล่าวต้อนรับ
๑๐.๓๕ – ๑๐.๕๐ น.	๑๔.๐๕ – ๑๔.๒๐ น.	บรรยายสรุป - หลักการและเหตุผล วัตถุประสงค์ และผลที่คาดหวัง - รายละเอียดการฝึก - ลำดับสถานการณ์ และประเภทโจทย์ฝึก - การประเมินผล
๑๐.๕๐ – ๑๑.๐๐ น.	๑๔.๒๐ – ๑๔.๓๐ น.	นำชม หรือถ่ายทอดบรรยากาศจริง ณ ห้องสัตมราชาธิราช ชั้น ๔ สถาบันพระปกเกล้า
๑๑.๐๐ – ๑๑.๑๕ น.	๑๔.๓๐ – ๑๔.๔๕ น.	ตอบข้อซักถาม
๑๑.๑๕ น.	๑๔.๔๕ น.	ลธ.กมช. หรือผู้แทน กล่าวขอบคุณ/เสร็จสิ้นการตรวจเยี่ยม

ตารางที่ ๔-๒ กำหนดการตรวจเยี่ยม

๔.๗.๒ รายชื่อหน่วยงานที่ตรวจเยี่ยมการฝึก

๔.๗.๒.๑ ภาคเช้า วันที่ ๒๓ ธันวาคม พ.ศ. ๒๕๖๔

รูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์ จำนวน ๘ หน่วยงาน ดังนี้

(๑) สำนักงานคณะกรรมการพัฒนาระบบราชการ

(๒) ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)

(๓) ธนาคารแห่งประเทศไทย

(๔) กรมบัญชีกลาง

(๕) สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

(๖) สำนักงานคณะกรรมการข้าราชการพลเรือน

(๗) ศูนย์บริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่ฟ้าหลวง

(๘) กระทรวงพลังงาน

รูปแบบตรวจเยี่ยม ณ สถานที่จริง จำนวน ๓ หน่วยงาน ดังนี้

(๑) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

(๒) สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

(๓) กระทรวงคมนาคม

๔.๗.๒.๒ ภาคบ่าย วันที่ ๒๓ ธันวาคม พ.ศ. ๒๕๖๔

รูปแบบออนไลน์ผ่านสื่ออิเล็กทรอนิกส์ จำนวน ๑ หน่วยงาน ดังนี้

(๑) กระทรวงพลังงาน

รูปแบบตรวจเยี่ยม ณ สถานที่จริง จำนวน ๖ หน่วยงาน ดังนี้

(๑) คณะอนุกรรมาธิการติดตาม เสนอแนะ และเร่งรัดการปฏิรูปประเทศและการจัดทำและดำเนินการตามยุทธศาสตร์ชาติด้านความมั่นคง ในคณะกรรมาธิการการทหารและความมั่นคงของรัฐ วุฒิสภา

(๒) สำนักงานปลัดกระทรวงยุติธรรม

(๓) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

(๔) คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

(๕) สำนักงานปลัดกระทรวงกลาโหม

(๖) กองบัญชาการกองทัพไทย

๔.๗.๒.๓ ภาคเช้า วันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๔

รูปแบบตรวจเยี่ยม ณ สถานที่จริง จำนวน ๒ หน่วยงาน ดังนี้

(๑) United State Embassy in Bangkok

(๒) British Embassy in Bangkok

บทที่ ๕
การสรุปบทเรียน
จากการฝึก

บทที่ ๕
การสรุปบทเรียนจากการฝึก

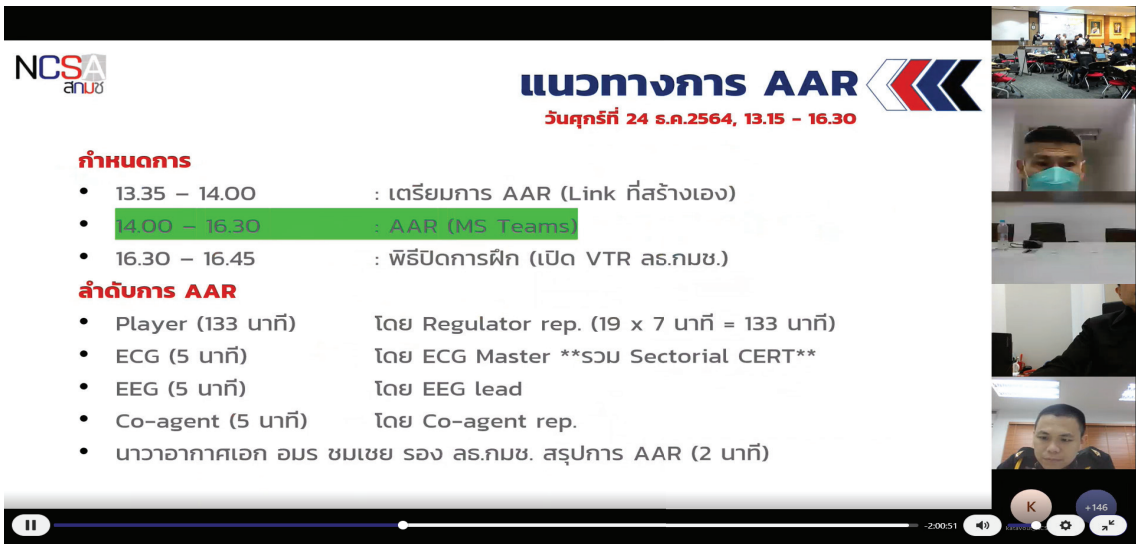
การสรุปบทเรียนจากการฝึก (After Action Review : AAR) เป็นหนึ่งในกิจกรรมสำคัญที่จะใช้ในการปรับปรุงการฝึกครั้งต่อ ๆ ไปให้มีคุณภาพมากยิ่งขึ้น ทั้งนี้ ส่วนที่รับผิดชอบในการวางแผนการฝึก (Exercise Planners) ควรจะจัดทำสรุปบทเรียนจากการฝึกให้แล้วเสร็จภายใน ๒๑ วัน โดยการทบทวนบทเรียนที่เกิดขึ้นในการฝึกที่ผ่านมา รวมถึงแนวทางที่เหมาะสมสำหรับการฝึกครั้งต่อ ๆ ไป ยกตัวอย่างเช่น หากพบว่าผู้รับการฝึกในครั้งนี้มีการตอบสนองต่อโจทย์ฝึกเร็วเกินไป การออกแบบโจทย์ฝึกในครั้งหน้าก็ควรจะเพิ่มความซับซ้อนมากยิ่งขึ้น รวมถึงส่วนข้าศึกสมมุติ (Red Team) ก็จะต้องใช้เทคนิคขั้นสูงมากยิ่งขึ้น[๕]

๕.๑ การประชุมสรุปบทเรียนจากการฝึก

๕.๑.๑ วัตถุประสงค์การประชุม

เพื่อให้ทราบถึงปัญหาข้อขัดข้อง สาเหตุ และข้อเสนอแนะเพื่อปรับปรุงให้การจัดการฝึกเพื่อให้ทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในครั้งต่อ ๆ ไปดียิ่งขึ้น

๕.๑.๒ กำหนดการและลำดับการนำเสนอ



รูปที่ ๕-๑ กำหนดการและลำดับการนำเสนอ

[๕] Post Exercise, MITRE Cyber Exercise Playbook

รูปที่ ๕-๑ กำหนดการและลำดับการนำเสนอ

เมื่อวันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๔ ได้มีการสรุปบทเรียนจากการฝึกโดยผู้แทนจากผู้เข้ารับการฝึก (Player) ส่วนควบคุมการฝึก (ECG) ส่วนประเมินผล (EEG) และผู้ช่วยส่วนควบคุมการฝึก (Co-agent) โดยมีลำดับการนำเสนอตามตารางที่ ๕-๑ ดังนี้

เวลา	เรื่อง
๑๓.๓๕ น. - ๑๔.๐๐ น.	**เตรียมการสรุปบทเรียนจากการฝึก**
๑๔.๐๐ น. - ๑๖.๓๐ น.	**ลำดับการสรุปบทเรียนจากการฝึก ดังนี้** - ผู้เข้ารับการฝึก (Player) โดยผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแลร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของตน (หน่วยงานละ ๗ นาที) - ส่วนควบคุมการฝึก (ECG) โดย ECG Master (๕ นาที) - ส่วนประเมินผล (EEG) โดย EEG Lead (๕ นาที) - ผู้ช่วยส่วนควบคุมการฝึก (Co-agent) โดยผู้แทน Co-agent (๕ นาที)
๑๖.๓๐ น. - ๑๖.๔๕ น.	**พิธีปิดการฝึก**

ตารางที่ ๕-๑ กำหนดการและลำดับการนำเสนอ

๕.๑.๓ หัวข้อการประชุม

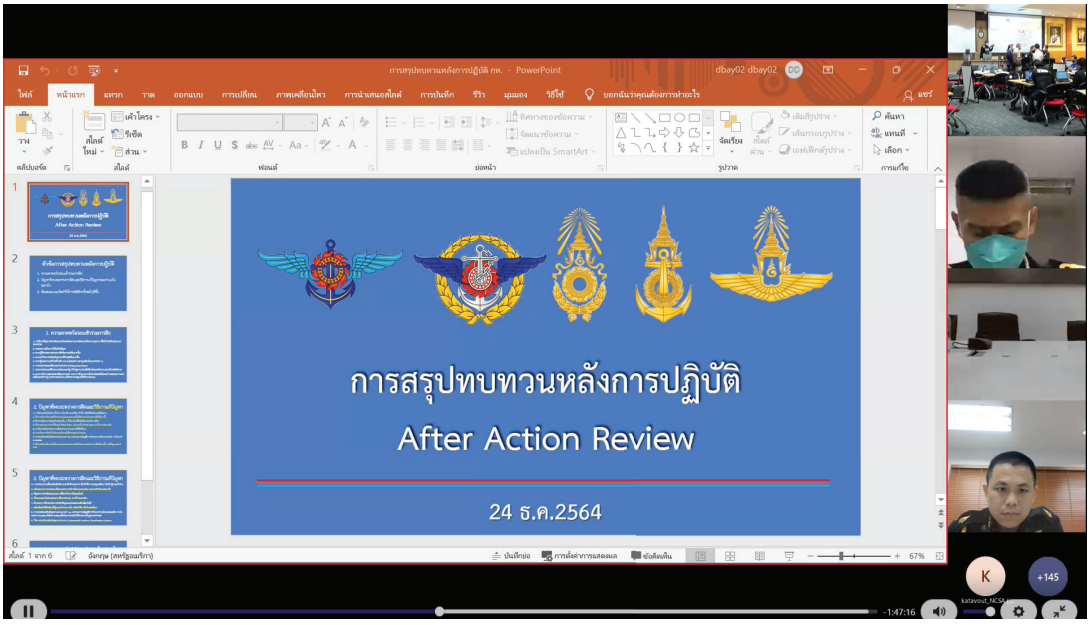
๕.๑.๓.๑ ความคาดหวังก่อนเข้าร่วมการฝึก

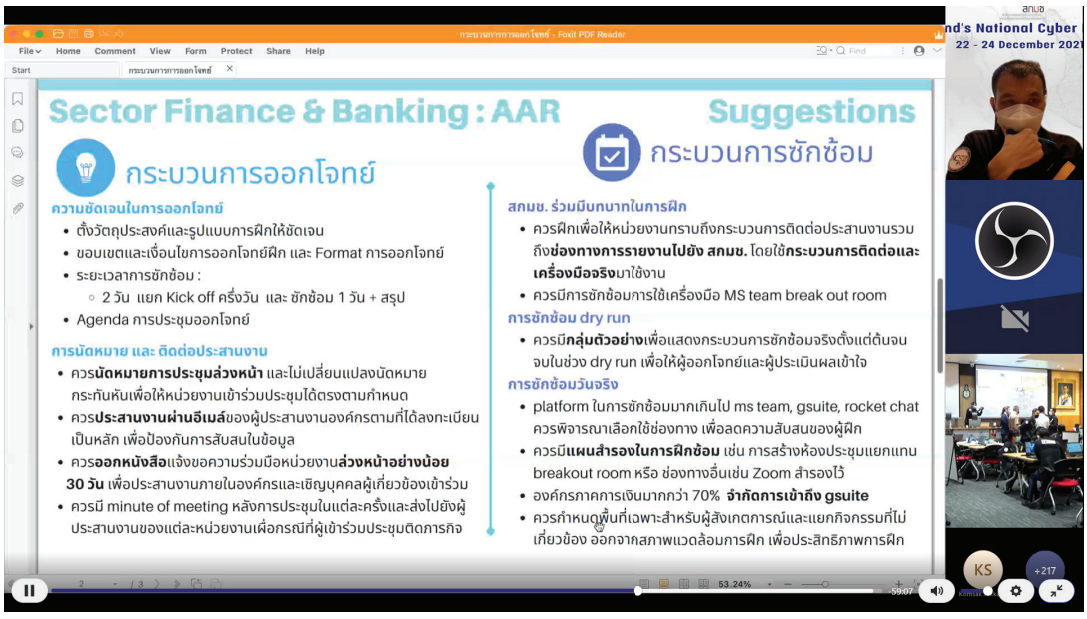
๕.๑.๓.๒ ปัญหาที่พบระหว่างการฝึก

๕.๑.๓.๓ วิธีการแก้ปัญหาของท่านเป็นอย่างไร

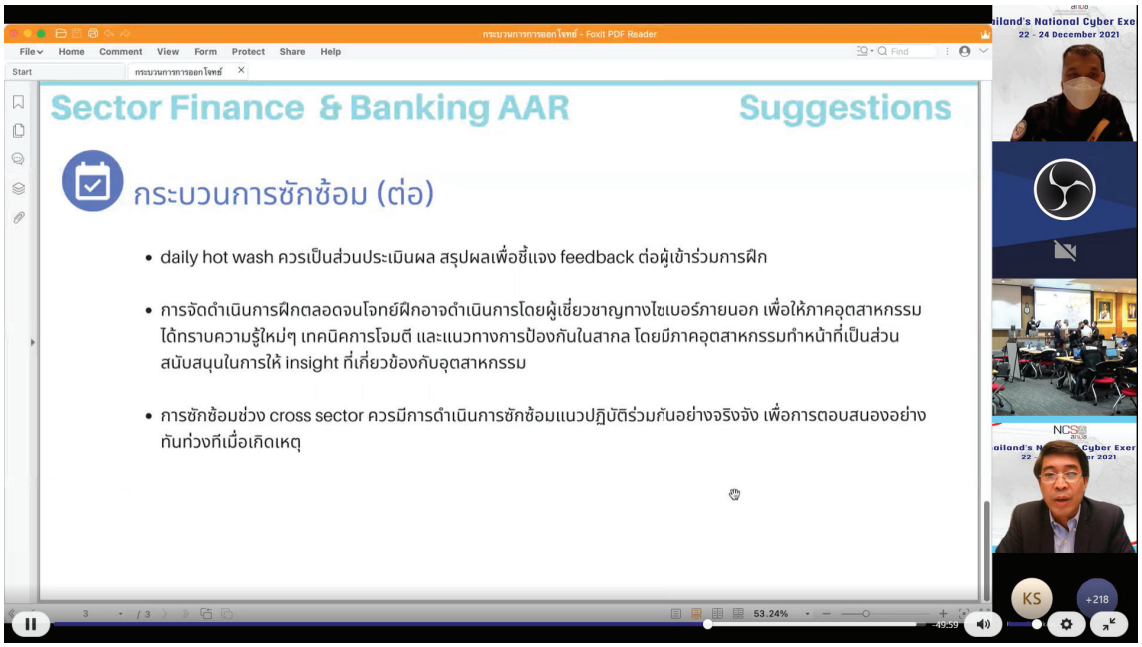
๕.๑.๓.๔ ข้อเสนอแนะเพื่อทำให้การจัดการฝึกครั้งต่อไปดียิ่งขึ้น

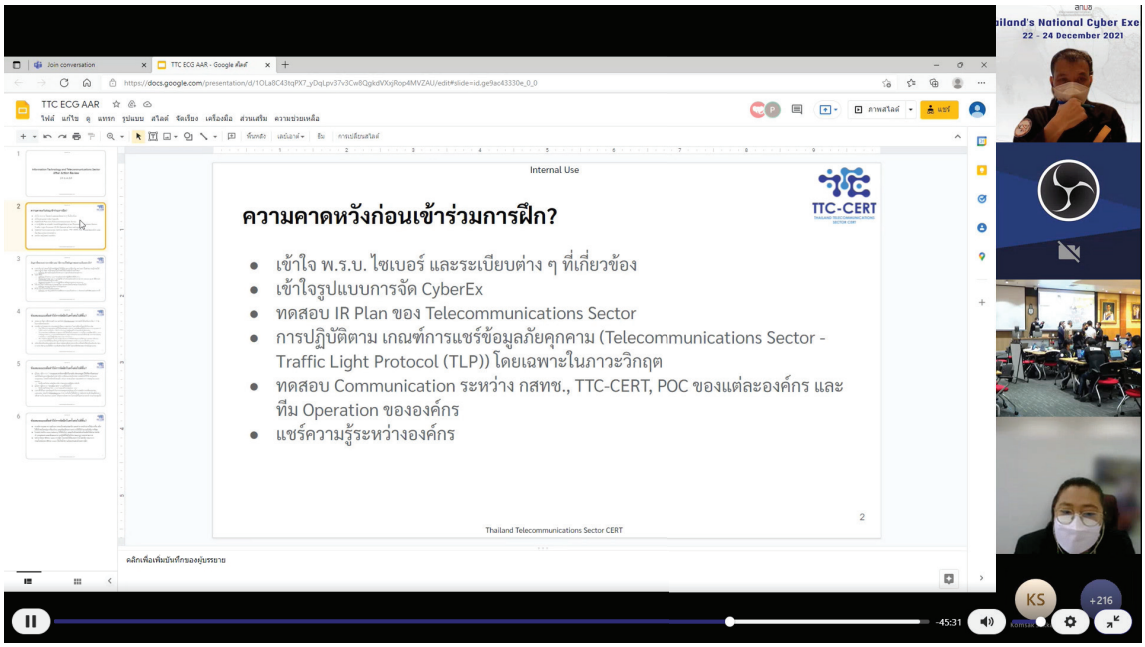
๕.๒ ผลการสรุปบทเรียน จากผู้เข้ารับการฝึก





รูปที่ ๕-๒ ผลการสรุปบทเรียน จากผู้เข้ารับการฝึก





รูปที่ ๕-๒ ผลการสรุปบทเรียน จากผู้เข้ารับการฝึก

๕.๒.๑ ความคาดหวังก่อนเข้าร่วมการฝึก

๕.๒.๑.๑ การฝึกจะทำให้มีความเข้าใจภัยคุกคามทางไซเบอร์เพิ่มมากขึ้น และสามารถแก้ปัญหาได้อย่างเป็นระบบในแต่ละสถานการณ์และระดับความรุนแรง เพื่อนำไปปรับปรุงแผนหรือกระบวนการภายในของหน่วยงานให้สามารถแก้ไขปัญหาได้อย่างทันท่วงที

๕.๒.๑.๒ ทำให้มีความรู้ ความเข้าใจ และมีแนวทางในการตอบสนองภัยคุกคามด้านไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อย่างถูกต้องในบทบาทต่าง ๆ ตลอดจนการแลกเปลี่ยนองค์ความรู้ระหว่างหน่วยงาน เพื่อนำมาประยุกต์ใช้กับหน่วยงานของผู้เข้าฝึก

๕.๒.๑.๓ ทำให้มีการประสานงานที่สอดคล้องกันระหว่างหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

๕.๒.๑.๔ ทำให้ได้รู้จัก เรียนรู้ และได้รับประโยชน์จากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมีความสัมพันธ์อันดีเกิดขึ้นระหว่างหน่วยงานต่าง ๆ ที่เข้าร่วมในการฝึก ซึ่งจะนำไปสู่การร่วมมือกันด้านไซเบอร์ และจัดตั้งเป็นประชาคมไซเบอร์ด้านต่าง ๆ ต่อไปในอนาคต

๕.๒.๑.๕ ทำให้หน่วยงานมีความรู้ความเข้าใจถึงบทบาทหน้าที่มากขึ้น และได้ทราบแนวทางการดำเนินการตามแผนรับมือของหน่วยงาน มีช่องทางการติดต่อสื่อสารกันระหว่างองค์กร

๕.๒.๒ ปัญหาที่พบระหว่างการฝึก

๕.๒.๒.๑ การฝึกแบบออนไลน์โดยผู้รับการฝึกอยู่ในสถานที่ทำงานของตนเอง ทำให้มีปัญหาเรื่องภารกิจแทรกซ้อน และปัญหาการประสานงานกับหน่วยงานอื่น ๆ ทำได้ยาก ส่งผลกระทบต่อการพิจารณาลำดับเหตุการณ์และการตอบคำถาม

๕.๒.๒.๒ การไม่ทราบถึงบทบาทสมมติของส่วนอื่น ๆ ที่เกี่ยวข้องในการรับมือและแก้ไขปัญหาจากเหตุการณ์ทางไซเบอร์ แก้ปัญหาโดยใช้บทบาทสมมติ (Role Play) แบ่งมอบให้ White Team ดำเนินการช่วยเหลือ

๕.๒.๒.๓ การประเมินระดับภัยคุกคามและการวิเคราะห์ผลกระทบตามประกาศมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ยังมีความคลุมเครือ

๕.๒.๒.๔ ปัญหาการประสานงานในช่วงเริ่มต้นมีความล่าช้าในด้านเอกสาร ทำให้การประชุมเตรียมการไม่มีผู้แทนเข้าร่วม

๕.๒.๒.๕ ปัญหาทางเทคนิค ระบบการสื่อสาร และระบบการประชุมผ่านสื่อออนไลน์

๕.๒.๒.๖ ปัญหาเรื่องห้วงเวลาการฝึกตรงกับภารกิจสำคัญของหน่วยงานอย่างหลีกเลี่ยงไม่ได้ ทำให้มีความจำเป็นต้องส่งผู้แทนเข้าร่วมการฝึก ส่งผลให้การฝึกไม่มีความต่อเนื่อง

๕.๒.๒.๗ ระยะเวลาการฝึกค่อนข้างยาวนาน ทำให้เกิดความขัดข้องในการให้ความร่วมมือกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการฝึก

๕.๒.๒.๘ โจทย์ฝึกเน้นไปทางเทคนิคมากเกินไป ควรเน้นไปที่การประสานงานข้ามหน่วยงาน การรายงานและแจ้งเตือน การยกระดับสถานการณ์ รวมถึงการทำงานร่วมกับ Sectorial CERT และ National CERT ให้มากขึ้น

๕.๒.๒.๙ ปัญหาความไม่คุ้นเคยกับเครื่องมือสนับสนุนการฝึกและเครื่องมือการสื่อสารผ่านออนไลน์

๕.๒.๒.๑๐ ปัญหาการเปลี่ยนแปลงกำหนดการฝึกอบรมกระทันหันทำให้ติดภารกิจไม่สามารถเข้าร่วมได้

๕.๒.๒.๑๑ การไม่มีผู้เข้ารับการฝึกด้านอื่นนอกจากทีมเทคโนโลยีสารสนเทศ (IT) ทำให้วิธีการมองปัญหาและการแก้ไขปัญหาได้ไม่ครอบคลุม เนื่องจากต้องใช้เวลานานในการอ่านเอกสาร

๕.๒.๓ วิธีการแก้ปัญหาของท่านเป็นอย่างไร

๕.๒.๓.๑ เพิ่มช่องทางในการประสาน/สื่อสาร มีการประสานงานทางอีเมลและออกหนังสือล่วงหน้าก่อนดำเนินการภายใน ๓๐ วัน เพื่อเพิ่มความรวดเร็ว

๕.๒.๓.๒ ใช้การบริหารจัดการลำดับความเร่งด่วนของงานเพื่อให้สามารถเข้าร่วมการฝึกได้มากขึ้น (แก้ปัญหาเฉพาะหน้า)

๕.๒.๓.๓ หน่วยงานไม่สามารถเข้าร่วมการฝึกได้ แก้ปัญหาโดยส่งผู้แทนเข้าร่วม

๕.๒.๔ ข้อเสนอแนะเพื่อทำให้การจัดฝึกครั้งต่อไปดีขึ้น

๕.๒.๔.๑ ควรจัดการฝึก ณ สถานที่จริง (Onsite) เพื่อแยกผู้เข้าร่วมการฝึกออกจากภาระงานและสิ่งรบกวนของแต่ละคน รวมทั้งทำให้สามารถพบหน้ากันและปรึกษาหารือกันได้อย่างมีประสิทธิภาพ

๕.๒.๔.๒ ควรเพิ่มการทดลองหรือซักซ้อมการใช้งานระบบฝึกให้มากขึ้น โดยอาจทำเป็นข้อมูลตัวอย่างเพื่อใช้แสดงกระบวนการซักซ้อม จะให้เข้าใจกระบวนการ ลำดับขั้นตอน และวิธีใช้งานก่อนการฝึกจริงเพิ่มมากขึ้น

๕.๒.๔.๓ ควรจัดให้มีการฝึกย่อยเฉพาะด้าน (Sector) ก่อน เพื่อทบทวนแผนรวมทั้งการประสานสอดคล้องภายใน Sector ก่อนที่จะเข้าร่วมการฝึกในระดับประเทศ

๕.๒.๔.๔ กรณีต้องฝึกแบบออนไลน์มีข้อดีในด้านความอ่อนตัวและความประหยัด แต่ควรมีการวางแผน ประสานงาน ซักซ้อมการฝึก และกำหนดห้วงเวลาที่เหมาะสมอย่างเป็นระบบให้มากขึ้น

๕.๒.๔.๕ ควรลดจำนวนคนและจำนวนโจทย์ฝึก แต่ขยายระยะเวลาในการตอบโจทย์ฝึกให้มากขึ้น เนื่องจากต้องใช้เวลาในการหาแนวทางแก้ไข ประเมินความเสี่ยง และกรอกแบบฟอร์มต่าง ๆ

๕.๒.๔.๖ ควรเพิ่มการหารือระหว่างหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละด้าน (Sector) และการเรียนรู้กระบวนการเฝ้าระวังตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อสร้างเครือข่ายด้านไซเบอร์ทั้งภาครัฐและภาคเอกชนให้มีความเข้มแข็ง ก่อนที่จะเข้าร่วมกิจกรรมการฝึก ซึ่งจะทำให้มีพื้นฐานและการประสานงานที่ดีก่อนเข้าร่วมการฝึกมากยิ่งขึ้น

๕.๒.๔.๗ ควรปรับรูปแบบการฝึกอบรมก่อนการฝึกจริง โดยให้มีการซ้อมในรูปแบบที่คล้ายกับการฝึกจริง

๕.๒.๔.๘ ควรจัดการอบรมตลอดหลักสูตรให้มีความต่อเนื่อง ไม่ควรเว้นระยะเวลานานเกินไป เพราะจะทำให้ขาดช่วงในการฝึกจริง

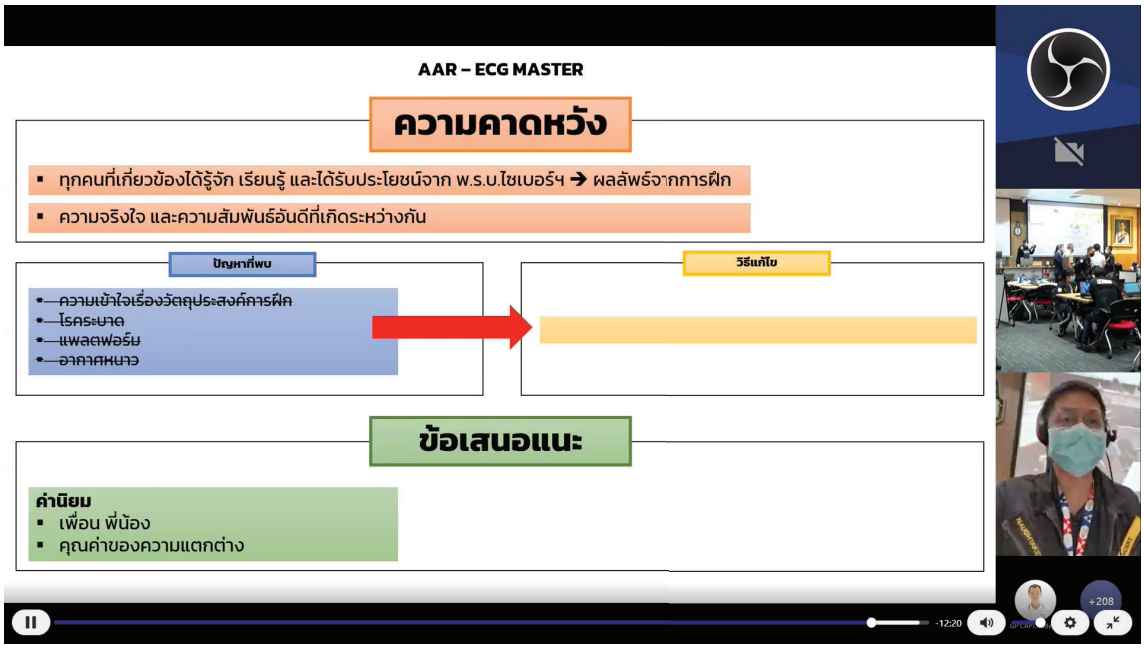
๕.๒.๔.๙ ระยะเวลาควรเหลือแค่ ๑ - ๒ วัน ควรกำหนดบทบาทหน้าที่ให้ชัดเจนมากขึ้น โดยเฉพาะบทบาทของ White Team ควรมีการตกลงให้ชัดเจน ควรใช้เครื่องมือที่สามารถใช้ได้ในชีวิตจริงด้วย เผื่อกรณีที่เกิดเหตุการณ์จริงในอนาคต ผู้จัดการฝึกควรวางแผนจัดการฝึกในระดับยุทธศาสตร์ (Strategic) ให้เรียบร้อยก่อน ควรตรงต่อเวลาตามที่นัดหมายไว้ และควรมีการเฉลยความต้องการของโจทย์แต่ละข้อด้วย

๕.๒.๔.๑๐ ควรมีวิดีทัศน์นำเสนอ สกมช. ว่ามีบทบาทอย่างไร โดยจัดเป็นกิจกรรมตอบคำถามเพื่อสร้างความคุ้นเคยกันก่อน

๕.๒.๔.๑๑ ควรมีการชี้แจงและแถลงข่าวเกี่ยวกับการจัดการฝึก เพื่อให้เกิดการรับรู้ต่อประชาชนทั่วไปให้มากขึ้น

๕.๒.๔.๑๒ ควรมีแพลตฟอร์ม (Platform) ในการแก้ไขปัญหาเพื่อการติดต่อสื่อสารได้ง่ายขึ้น ควรเพิ่มการประสานงานกับหน่วยงานย่อย ๆ ให้มากขึ้นเพื่อทำความเข้าใจเรื่องกฎหมาย โดยอาจใช้วิดีโอหรือคลิปสั้น ๆ อธิบายแทนเอกสาร จะทำให้เกิดความเข้าใจมากขึ้น ช่วงเวลาการฝึกควรมีเวลาที่ชัดเจน ควรควบคุมการนำเสนอให้มีความชัดเจนมากขึ้น แต่ละโจทย์ควรมีการเฉลยและแนวทางการปฏิบัติด้วย

๕.๓ ผลการสรุปบทเรียน จากส่วนควบคุมการฝึก



รูปที่ ๕-๓ ผลการสรุปบทเรียน จากส่วนควบคุมการฝึก

๕.๓.๑ ความคาดหวังก่อนเข้าร่วมการฝึก

ทุกคนที่เกี่ยวข้องได้รู้จัก เรียนรู้ และได้รับประโยชน์จากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมีความสัมพันธ์อันดีที่เกิดระหว่างกัน

๕.๓.๒ ปัญหาที่พบระหว่างการฝึก

ความเข้าใจในเรื่องวัตถุประสงค์การฝึก โรคระบาด แพลตฟอร์ม อากาศหนาว

๕.๓.๓ ศึกษาและทำความเข้าใจ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ วิธีการแก้ปัญหาของท่านเป็นอย่างไร

๕.๓.๔ ข้อเสนอแนะเพื่อทำให้การจัดฝึกครั้งต่อไปดีขึ้น

มีค่านิยมความเป็นเพื่อน พี่น้อง และเห็นคุณค่าของความแตกต่าง

๕.๔ ผลการสรุปบทเรียน จาก Co-Agent

รูปที่ ๕-๔ ผลการสรุปบทเรียน จาก Co-Agent

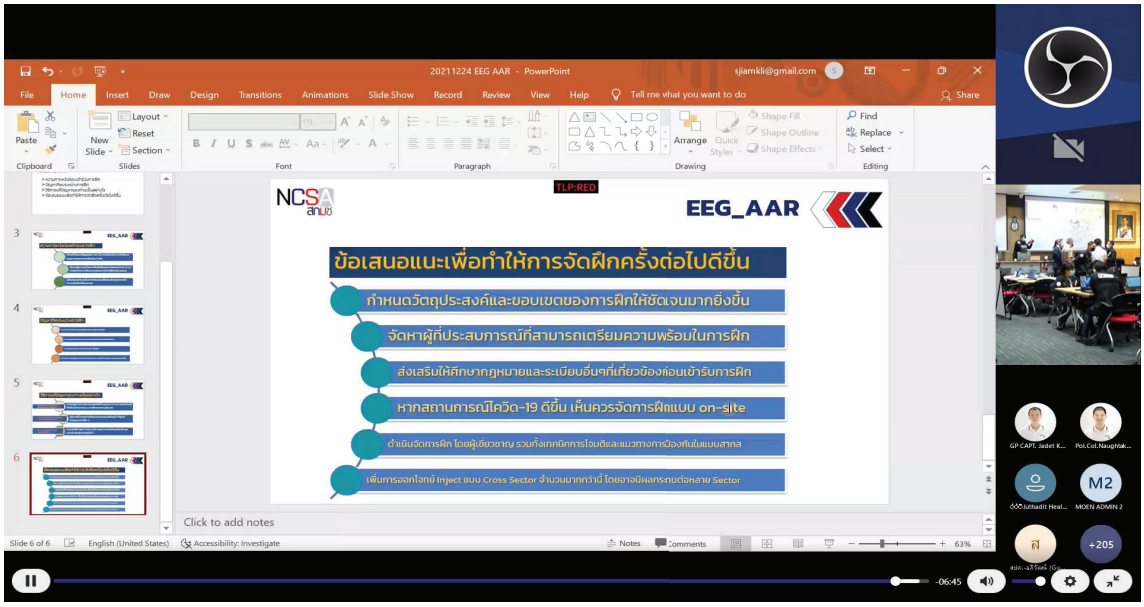
๕.๔.๑ ปัญหาที่พบระหว่างการฝึก

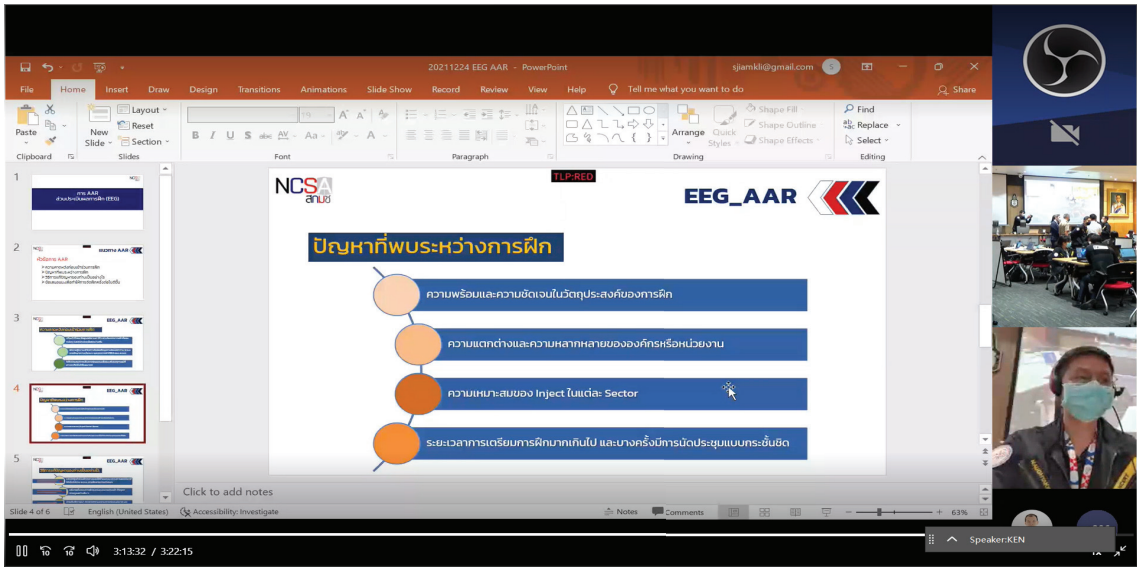
เครื่องมือ อุปกรณ์ต่าง ๆ ยังไม่อำนวยความสะดวกในการดำเนินการฝึกมากพอ

๕.๔.๒ ข้อเสนอแนะเพื่อทำให้การจัดฝึกครั้งต่อไปดีขึ้น

อยากเพิ่มมิตรภาพ อยากให้เกิดความสมจริงมากยิ่งขึ้น อยากให้มีการจัดฝึกนอกสถานที่

๕.๕ ผลการสรุปบทเรียน จากส่วนประเมินผล





รูปที่ ๕-๕ ผลการสรุปบทเรียน จากส่วนประเมินผล

๕.๕.๑ ความคาดหวังก่อนเข้าร่วมการฝึก

๕.๕.๑.๑ เจ้าหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล (Regulator) และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทราบถึงบทบาทหน้าที่ของตนเอง และความร่วมมือระหว่างกัน มีความรู้ความเข้าใจในการรับมือภัยคุกคามทางไซเบอร์ฯ และได้รับประสบการณ์ในการฝึกอบรม

๕.๕.๑.๒ ได้ซักซ้อมและทำความเข้าใจทั้งภายในหน่วยงาน และในภาคอุตสาหกรรมถึงแนวทางการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕.๕.๑.๓ ได้ซักซ้อมวิธีปฏิบัติร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ รวมทั้ง Cross Sector

๕.๕.๑.๔ ได้เรียนรู้ข้อมูล เทคนิค และรูปแบบการโจมตีทางไซเบอร์ในรูปแบบใหม่ ๆ เพื่อเตรียมการรับมือในภาคอุตสาหกรรม

๕.๕.๑.๕ ได้เรียนรู้แนววิธีปฏิบัติของหน่วยงานที่เกี่ยวข้อง (Give & Take) เพื่อนำมาปรับใช้ภายในภาคอุตสากรรม เพื่อยกระดับแนวปฏิบัติการตอบสนองต่อเหตุการณ์ทางไซเบอร์ในภาพรวม

๕.๕.๑.๖ อยากเห็นกระบวนการและวิธีการที่ใช้ในการรับมือกับโจทย์ฝึกของแต่ละหน่วยงานหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๕.๕.๑.๗ มีความรู้ความเข้าใจการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงประกาศ และแนวทางปฏิบัติของ สกมช.

๕.๕.๑.๘ มีการบูรณาการแผนแนวทางการปฏิบัติงานระหว่างหน่วยงานที่เกี่ยวข้องสอดคล้องกับกฎหมายที่ประกาศเป็นแบบแผนในการพัฒนาการฝึกของหน่วยงานระดับย่อย มีการนำแผนแนวทางไปสู่การปฏิบัติจริงในการจัดทำแผนเผชิญเหตุ แนวทางฟื้นฟู แก้ไข และแผนสำรองในการทำแผนบริหารความต่อเนื่องของหน่วยงาน

๕.๕.๒ ปัญหาที่พบระหว่างการฝึก

๕.๕.๒.๑ แต่ละหน่วยงานมีความพร้อมในการเข้าร่วมการฝึกแตกต่างกันมาก เช่น มีผู้ปฏิบัติงานด้านไซเบอร์น้อย ผู้เล่นบางท่านยังไม่มีประสบการณ์ในการใช้งานระบบต่าง ๆ มีความแตกต่างของแผนรับมือภัยไซเบอร์ของแต่ละหน่วยงาน ทำให้ไม่สามารถแก้ไขปัญหาตามโจทย์ฝึก (Inject) ในแต่ละด้าน (Sector) ได้ตามที่คาดหวัง

๕.๕.๒.๒ การจัดเตรียมโจทย์ฝึกค่อนข้างพึ่งพาผู้ออกโจทย์และผู้ประเมินจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแลมากเกินไป ทำให้การจัดสรรเวลาค่อนข้างยาก อาจจำเป็นต้องให้ สกมช. เข้ามามีส่วนร่วมมากขึ้น

๕.๕.๒.๓ ระบบจัดการฝึกและระบบสนับสนุนการฝึกค่อนข้างมีปัญหาเชิงเทคนิคในการรองรับการฝึกขนาดใหญ่แบบนี้

๕.๕.๒.๔ ระยะเวลาการฝึก ๓ วัน อาจใช้เวลานานเกินไป

๕.๕.๒.๕ ข้อจำกัดทางด้านสภาพแวดล้อม เช่น ข้อจำกัดเกี่ยวกับระบบและเครื่องมือสื่อสาร ความพร้อมของเครือข่ายอินเทอร์เน็ต มีกิจกรรมที่มิได้เกี่ยวข้องกับการฝึกเข้ามาแทรก มีภารกิจและงานจากหน่วยงานค่อนข้างมาก ส่งผลกระทบโดยตรงต่อผู้เข้าร่วมการฝึกทางออนไลน์

๕.๕.๒.๖ ผู้เข้าร่วมฝึกในทุกส่วนตอบ/ แก้โจทย์/ แก้ปัญหาโดยใช้ความรู้ของตนเอง ไม่ค่อยได้ปรึกษาหารือ/ แลกเปลี่ยนแนวความคิด/ ข้อเสนอแนะ กับผู้เข้าร่วมฝึกท่านอื่น ๆ

๕.๕.๒.๗ ผู้เล่นอยู่คนละสถานที่ทำให้มีปัญหาในการประสานงานหรือระดมสมอง

๕.๕.๓ วิธีการแก้ปัญหาของท่านเป็นอย่างไร

๕.๕.๓.๑ ผู้บริหารหน่วยงานควบคุมหรือกำกับดูแลเข้าใจและให้ความสำคัญกับกิจกรรมการฝึก จึงให้การสนับสนุนอย่างเต็มที่

๕.๕.๓.๒ ชี้แจงผู้รับการฝึกว่าสามารถสอบถาม White Team ตามบทบาทที่อยากให้เป็นได้

๕.๕.๓.๓ มอบหมายผู้แทนในผู้เล่นบางท่านที่มีความพร้อม ช่วยดำเนินการแทนผู้เล่นท่านอื่น ๆ

๕.๕.๓.๔ ผู้เข้าร่วมการฝึกในทุกส่วนต้องหาทางทำสิ่งต่าง ๆ ด้วยตนเอง เพื่อแก้ปัญหาเฉพาะหน้า

๕.๕.๓.๕ ใช้เครื่องคอมพิวเตอร์มากกว่า ๑ เครื่อง ในการทำการฝึก เพื่อป้องกันปัญหาเชิงเทคนิค

๕.๕.๔ ข้อเสนอแนะเพื่อทำให้การจัดฝึกครั้งต่อไปดีขึ้น

๕.๕.๔.๑ ควรมีผู้จัดงานมืออาชีพเข้ามาเตรียมความพร้อมในการจัดงาน สถานที่ เครื่องมือสนับสนุนการฝึก และการประสานงานต่าง ๆ

๕.๕.๔.๒ ควรจัดหาผู้มีประสบการณ์ที่สามารถเตรียมความพร้อมให้กับผู้รับการฝึกโดยเฉพาะในเรื่องกฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้อง

๕.๕.๔.๓ ควรมีผู้เชี่ยวชาญเข้ามาทำโจทย์ฝึกและดำเนินการฝึก เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละด้าน (Sector) ได้รับความรู้ใหม่ ๆ เทคนิคการโจมตี รวมถึงแนวทางการป้องกันในระดับสากล ทั้งนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละด้าน (Sector) ควรทำหน้าที่ให้ข้อมูลเชิงลึก (Insight) เพิ่มเติมด้วย

๕.๕.๔.๔ ควรปรับระยะเวลาดำเนินการฝึกให้เหมาะสม (๑-๒ วัน) และปรับสภาพแวดล้อมให้เอื้อต่อประสิทธิภาพการฝึกซ้อม รวมทั้งใช้ระบบเครื่องมือสื่อสารที่เหมาะสม และลดข้อจำกัดที่ผู้เข้าร่วมการฝึกอาจไม่สามารถใช้งานได้ เช่น ใช้เครื่องมือ Google G Suite แทน Nextcloud หรือ Rocket Chat เป็นต้น

๕.๕.๔.๕ ควรกำหนดให้ผู้ออกโจทย์ยึดแนวทางการออกโจทย์ โดยให้มีการรายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ และการปฏิบัติตามมาตรา ๕๘ หรือมาตราอื่น ๆ ที่เกี่ยวข้อง เพื่อให้สอดคล้องกับวัตถุประสงค์การฝึกได้ดียิ่งขึ้น

๕.๕.๔.๖ หากเป็นการฝึกในลักษณะเสมือน (Virtual) ควรแยกลิงค์ (Link) ห้องประชุมเป็นห้องหลักและห้องในแต่ละด้าน (Sector) หากต้องการถ่ายทอดสดในแต่ละห้องอาจใช้เทคโนโลยีเสริม อย่างเช่น Microsoft Teams จะเป็น Network Device Interface (NDI)

๕.๕.๔.๗ ควรมีผู้แทนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ทำหน้าที่ด้านมวลชนสัมพันธ์กับ สกมช.

๕.๕.๔.๘ ควรใช้แพลตฟอร์มการฝึกอบรมเพียงอย่างเดียว เพื่อลดความสับสนของผู้เข้ารับการอบรม

๕.๕.๔.๙ ควรจัดการฝึกแบบสถานที่จริง (OnSite) เพราะจะได้ทำงานร่วมกันและได้มีโอกาสเจอกับหน่วยงานอื่น ๆ ลดผลกระทบจากสภาพแวดล้อมและภารกิจแทรกซ้อน ทำให้บรรลุวัตถุประสงค์การฝึกมากยิ่งขึ้น

๕.๕.๔.๑๐ ควรประสานงานกับหน่วยงานต่าง ๆ เพื่อทำความเข้าใจในภาพรวมก่อนแล้วจึงรวมเป็นกลุ่ม Sector เพื่อทำความเข้าใจในส่วนที่แตกต่างกันอีกครั้ง

๕.๕.๔.๑๑ ผู้รับการฝึกควรต้องทำความเข้าใจเรื่องกฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้องก่อนเข้ารับการฝึก

๕.๕.๔.๑๒ ควรชี้แจงแนวทางการฝึกโดยนำเสนอเป็นคลิปวิดีโอสั้น ๆ แทนการอ่านเอกสาร

๕.๕.๔.๑๓ ควรมีการควบคุมเวลาในการนำเสนอของแต่ละกลุ่มให้มีความกระชับมากขึ้น

๕.๕.๔.๑๔ ควรมีการเฉลยโจทย์ฝึกเพื่อให้ผู้รับการฝึกมีความเข้าใจเพิ่มมากขึ้น

ภาคผนวก

ผนวก ก กฎหมายที่เกี่ยวข้อง

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๔. พระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘

๕. พระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑

๖. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้งหน้าที่ และอำนาจของศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

๗. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

๘. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่ และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

๙. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑๐. (ร่าง) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐

๑๑. (ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐

๑๒. (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ผนวก ข นิยามศัพท์ และบัญชีคำย่อ

ข ๑ นิยามศัพท์

โจทย์ฝึก (Event/ Inject) หมายถึง เหตุการณ์หรือกิจกรรมซึ่งมีลักษณะเฉพาะเจาะจงและเป็นส่วนหนึ่งของรายการโจทย์ฝึก (MSEL)

ส่วนควบคุมการฝึก (Exercise Control Group : ECG) หมายถึง กลุ่มบุคคลซึ่งมีหน้าที่จัดการและกำหนดทิศทางในห้วงดำเนินการฝึก (Execution Phase) ในทางปฏิบัติ ECG จะเป็นผู้ส่งโจทย์ฝึก (Inject) รวมถึงการดำเนินการเกี่ยวกับสถานการณ์ฝึก (Scenario) ด้วย

รายการโจทย์ฝึก (Master Scenario Event List : MSEL) หมายถึง รายการของเหตุการณ์หรือกิจกรรมซึ่งได้มีการกำหนดไว้ล่วงหน้า เพื่อใช้ในการกำหนดผลลัพธ์ที่เฉพาะเจาะจงของการฝึก

สถานการณ์ฝึก (Exercise Scenario) หมายถึง การอธิบายสภาพแวดล้อมการปฏิบัติการ (Operating Environment) หรือสภาพแวดล้อมเชิงยุทธศาสตร์ (Strategic Environment) เพื่อกำหนดรายละเอียดรวมถึงขอบเขตของการฝึกให้สอดคล้องกับวัตถุประสงค์การฝึกที่ตั้งไว้ ในทางปฏิบัติ Exercise Scenario จะกำหนดเป็นลำดับสถานการณ์ (Storyline) หรือพล็อตเรื่องเกี่ยวกับการฝึก เพื่อให้ผู้วางแผน (Planner) รวมถึงผู้รับการฝึก (Participant) นำไปใช้ตลอดห้วงการฝึก

การสรุปสถานการณ์ประจำวัน (Daily Hotwash) หมายถึง กิจกรรมการแถลงผลการแก้ไขสถานการณ์ฝึกในแต่ละวัน เพื่อให้ผู้รับการฝึก ส่วนผู้ควบคุมการฝึก และส่วนประเมินผล ได้วิเคราะห์ร่วมกันเกี่ยวกับการแก้ไขปัญหาตามรายการโจทย์ฝึก ซึ่งจะทำให้เกิดความเข้าใจเกี่ยวกับโจทย์ฝึกต่าง ๆ มากยิ่งขึ้น

ข้อตกลงร่วม (Rules of Engagement : RoE) หมายถึง แนวปฏิบัติ (Guideline) หรือเงื่อนไข (Constraint) ที่จะต้องปฏิบัติในห้วงการทดสอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Testing) ทั้งนี้ ข้อตกลงร่วมจะต้องกำหนดขึ้นก่อนที่จะเริ่มการทดสอบ ซึ่งจะทำให้ทีมทดสอบได้รับอนุญาตให้สามารถดำเนินการได้ (ในบริบทของการฝึก ข้อตกลงร่วมจะหมายถึงแนวปฏิบัติหรือเงื่อนไขที่จะกำหนดขึ้นให้กับผู้รับการฝึกก่อนที่จะเริ่มดำเนินการฝึก)

White Team หรือ Role Play Team หมายถึง ผู้ทำหน้าที่เป็นสิ่งสมมุติซึ่งมิได้เข้าร่วมในห้วงดำเนินการฝึก

ผู้ช่วยส่วนควบคุมการฝึก (Co - Agent) หมายถึง ผู้ทำหน้าที่สนับสนุนหัวหน้าส่วนควบคุมการฝึกในด้านการประสานงานและสนับสนุนให้ทีมย่อยภายในส่วนควบคุมการฝึกสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้ ผู้ช่วยส่วนควบคุมการฝึก จะกำหนดจากผู้ปฏิบัติงานในสกมช. เป็นหลัก

การวางแผนบริหารความต่อเนื่อง (Business Continuity Planning : BCP) หมายถึง กระบวนการในการสร้างระบบการทำงานเพื่อการป้องกันและฟื้นฟู จากภาวะคุกคามต่าง ๆ ที่ส่งผลกระทบต่อธุรกิจ โดยการวางแผนนั้นต้องมั่นใจว่าบุคลากรรวมไปถึงทรัพยากรและสินทรัพย์ต่าง ๆ จะได้รับการปกป้องเป็นอย่างดี และพร้อมใช้งานได้อย่างดีในทุก ๆ สถานการณ์

การจัดการภาวะวิกฤติ (Crisis Management) หมายถึง การจัดการในลักษณะที่ลดความเสียหายให้น้อยที่สุดและช่วยให้องค์กรที่ได้รับผลกระทบสามารถฟื้นตัวได้อย่างรวดเร็ว

Traffic Light Protocol (TLP) หมายถึง การจัดระดับชั้นความลับและความละเอียดอ่อนของข่าวสารที่ใช้แบ่งปัน โดยมักแบ่งตามลำดับชั้นของสี

Web Defacement หมายถึง การโจมตีเว็บไซต์ที่เปลี่ยนรูปลักษณ์ของเว็บไซต์หรือหน้าเว็บซึ่งเจาะเข้าไปในเว็บเซิร์ฟเวอร์และแทนที่เว็บไซต์ที่โฮสต์ด้วยเว็บไซต์ของตนเอง

ข ๒ บัญชีคำย่อ

คำย่อ	**หน่วยงาน**
กมช.	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม.	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส.	คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
สกมช.	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำย่อ	**ภาษาอังกฤษ**
National CERT	National Computer Emergency Response Team ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
TB-CERT	Thailand Banking Sector Computer Emergency Response Team ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
TTC-CERT	Thailand Telecommunication Computer Emergency Response Team ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม
AAR	After Action Review การสรุปบทเรียนจากการฝึก
C-MEX	National Crisis Management Exercise การฝึกการบริหารวิกฤตการณ์ระดับชาติ
NCSA	National Cyber Security Agency สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CDC	Concept Development Conference การประชุมพัฒนาแนวคิดการฝึก
IPC	Initial Planning Conference การประชุมวางแผนขั้นต้น
FPC	Final Planning Conference การประชุมวางแผนขั้นสุดท้าย
ECG	Exercise Control Group ส่วนควบคุมการฝึก
EEG	Exercise Evaluation Group ส่วนประเมินผล
TTX	Table Top Exercise การฝึกซ้อมแผนบนโต๊ะ
CERT	Computer Emergency Response Team ทีมสำหรับรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์
SIEM	Security Information & Event Management ระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร
IOC	Indicator of Compromise ตัวบ่งชี้ภัยคุกคาม
SOC	Security Operations Center ศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย
PDPA	Personal Data Protection Act พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
DRP	Disaster Recovery Plan แผนผลิกฟื้นธุรกิจ

ผนวก ค รายชื่อคณะทำงาน

กองบัญชาการ กองอำนวยการฝึก	
๑. ผู้อำนวยการฝึก	พลเอก ดร.ปรัชญา เฉลิมวัฒน์
๒. รองผู้อำนวยการฝึก ๑	นาวาอากาศเอก อมร ชมเชย
๓. รองผู้อำนวยการฝึก ๒	นางกิ่งนภา บางชวด
๔. ผู้ช่วยผู้อำนวยการฝึก ๑	นาวาอากาศเอก จเด็ด คูหะก้องกิจ
๕. ผู้ช่วยผู้อำนวยการฝึก ๒	นาวาตรีหญิง เขมกร รัชธร
ส่วนควบคุมการฝึก	
๖. หัวหน้าส่วนควบคุมการฝึก	พันเอก ธีรวุฒิ วิทยากรณ์
๗. รองหัวหน้าส่วนควบคุมการฝึก ๑	นาวาเอก ณัฐพนธ์ ชาติปรีชากุล
๘. รองหัวหน้าส่วนควบคุมการฝึก ๒	พันตำรวจเอก ณัทกฤช พรหมจันทร์
๙. รองหัวหน้าส่วนควบคุมการฝึก ๓	นางสาวดรุณี พิกุลทอง
ส่วนประเมินผล	
๑๐. หัวหน้าส่วนประเมินผล	พันตรี ปวิช บูรพาชลทิศน์
ส่วนเทคโนโลยีสารสนเทศ	
๑๑. หัวหน้าส่วนเทคโนโลยีสารสนเทศ	นาวาเอก ณัฐพนธ์ ชาติปรีชากุล
ศูนย์การข่าว	
๑๒. หัวหน้าศูนย์การข่าว	ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ พรหมวิกร
๑๓. รองหัวหน้าศูนย์การข่าว	นางพัชญ์ชิชา ไกรแสงศรี
ส่วนการฝึกเตรียมการ	
๑๔. หัวหน้าส่วนฝึกเตรียมการ	นาวาเอกหญิง ศิริเนตร รักษ์วงศ์
๑๕. รองหัวหน้าส่วนฝึกเตรียมการ	นายจตุรงค์ บุญเรือง
ส่วนธุรการและสนับสนุน	
๑๖. หัวหน้าส่วนธุรการและสนับสนุน	ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ พรหมวิกร
๑๗. รองหัวหน้าส่วนธุรการและสนับสนุน	นางพัชญ์ชิชา ไกรแสงศรี
ที่ปรึกษาคณะทำงาน	
๑๘. พลโท ปริญญา ฉายดิลก	ผู้เชี่ยวชาญด้านนโยบายและยุทธศาสตร์ สกมช.
๑๙. ดร.กิตติ โฆษะวิสุทธิ์	ประธานกรรมการ TB-CERT

ผนวก ง รายชื่อผู้ที่เข้าร่วมการฝึก

ง ๑ รายชื่อหน่วยงานที่เข้าร่วมการฝึก

ลำดับ	หน่วยงาน
๑	กรมการขนส่งทางราง
๒	กรมการปกครอง
๓ - ๔	กรมชลประทาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน
๕	กรมธุรกิจพลังงาน
๖	กรมป้องกันและบรรเทาสาธารณภัย
๗	กรมศุลกากร
๘	กระทรวงการคลัง
๙	กระทรวงการต่างประเทศ
๑๐	กระทรวงพลังงาน
๑๑	กองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ
๑๒	กองทัพบก
๑๓	กองทัพเรือ
๑๔	กองทัพอากาศ
๑๕	กองบังคับการตำรวจจราจร กองบัญชาการตำรวจนครบาล สำนักงานตำรวจแห่งชาติ
๑๖	กองบัญชาการกองทัพไทย
๑๗	การท่าเรือแห่งประเทศไทย
๑๘	การประปาส่วนภูมิภาค
๑๙	การไฟฟ้านครหลวง
๒๐	การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
๒๑	การไฟฟ้าส่วนภูมิภาค
๒๒	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
๒๓	การรถไฟแห่งประเทศไทย

ลำดับ	หน่วยงาน
๒๔ - ๒๗	ตลาดหลักทรัพย์แห่งประเทศไทย บริษัท ตลาดสัญญาซื้อขายล่วงหน้า (ประเทศไทย) จำกัด (มหาชน) บริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด บริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด
๒๘	ธนาคารกรุงเทพ จำกัด (มหาชน)
๒๙	ธนาคารกรุงไทย จำกัด (มหาชน)
๓๐	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)
๓๑	ธนาคารกสิกรไทย จำกัด (มหาชน)
๓๒	ธนาคารทหารไทยธนชาต จำกัด (มหาชน)
๓๓	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
๓๔	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
๓๕	ธนาคารแห่งประเทศไทย
๓๖	ธนาคารออมสิน
๓๗	บริษัท ดีแทค ไตรเน็ต จำกัด
๓๘	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)
๓๙	บริษัท ทรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด
๔๐	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด
๔๑	บริษัท ทางด่วนและรถไฟฟ้ากรุงเทพ จำกัด (มหาชน)
๔๒	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๔๓	บริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด
๔๔	บริษัท ปตท. จำกัด (มหาชน)
๔๕	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด
๔๖	บริษัท ระบบขนส่งมวลชน กรุงเทพ จำกัด (มหาชน)
๔๗	ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ
๔๘	ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)
๔๙	ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ลำดับ	หน่วยงาน
๕๐	สำนักข่าวกรองแห่งชาติ
๕๑	สำนักงานการบินพลเรือนแห่งประเทศไทย
๕๒	สำนักงานคณะกรรมการกำกับกิจการพลังงาน
๕๓	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
๕๔	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
๕๕	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
๕๖	สำนักงานคณะกรรมการอาหารและยา
๕๗	สำนักงานตรวจคนเข้าเมือง
๕๘	สำนักงานตำรวจแห่งชาติ
๕๙	สำนักงานปรมาณูเพื่อสันติ
๖๐	สำนักงานปลัดกระทรวงกลาโหม
๖๑	สำนักงานปลัดกระทรวงการคลัง
๖๒	สำนักงานปลัดกระทรวงคมนาคม
๖๓	สำนักงานปลัดกระทรวงสาธารณสุข
๖๔	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
๖๕	สำนักงานสภาความมั่นคงแห่งชาติ
๖๖	องค์การเภสัชกรรม

ง ๒ รายชื่อผู้แทนหน่วยงานที่เข้าร่วมการประชุมวางแผนการฝึก

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๑	กรมการขนส่งทางราง	๑	คุณภูวิศ รักษาแก้ว
๒	กรมการปกครอง	๒	คุณวรวิทย์ จิรังคสกุลเดช
๓	กรมชลประทาน	๓	คุณราชพล หิรัญรักษ์
		๔	คุณศุภชัย คะชาถา
		๕	คุณสาธิต บุญหลง

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๔	กรมธุรกิจพลังงาน	๖	นายถิร เกียรติวิวัฒน์
		๗	คุณอดินันท์ ดิษฐเกษร
		๘	คุณณัฐวดี คำภิรานนท์
๕	กรมป้องกันและบรรเทาสาธารณภัย	๙	คุณสุไลลักษณ์ แบ่งลาภ
๖	กรมศุลกากร	๑๐	คุณสโรชา ต้อยมาเมือง
๗	กระทรวงการคลัง	๑๑	คุณประทีป สร้อยนาค
		๑๒	คุณบุญลือ จิตตคาม
		๑๓	คุณเฉลิมศักดิ์ เลิศวงศ์เสถียร
๘	กระทรวงการต่างประเทศ	๑๔	คุณสุดาภรณ์ แต้เจริญผล
		๑๕	คุณพิชญะ ลภัสธำรง
		๑๖	คุณจุฑาเกียรติ มันตภาณีวัฒน์
		๑๗	คุณชูเกียรติ ประเสริฐสุข
		๑๘	คุณธีรวุฒิ มงคลสหกุล
๙	กระทรวงพลังงาน	๑๙	คุณอรอนุตตร์ สุทธิ์เสงี่ยม
		๒๐	คุณธวัชชัย สุขสาย
		๒๑	คุณจรัสพงษ์ จำนงทอง
		๒๒	คุณภาณุพงศ์ ปรึกษา
		๒๓	คุณธนพล ศรีเมือง
		๒๔	คุณพรพนิต บุญส่ง
๑๐	กองทัพบก	๒๕	พันเอก อธิกร เอกชัยฤดี
		๒๖	พันโท จิระเดช ปานพรหมมาศ
		๒๗	พันโท ฉัตร เนินลพ
๑๑	กองทัพเรือ	๒๘	นาวาโท คณิน ศิริธรากูล
		๒๙	นาวาตรี รัตนะ เต้นปักษี
		๓๐	เรือตรี สุธี กับกระโทก

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๑๒	กองทัพอากาศ	๓๑	นาวาอากาศเอก พรชัย ภัควันต์
		๓๒	นาวาอากาศเอก สุรงกานต์ ท้าวสัน
		๓๓	นาวาอากาศเอก วิพุธ อนันทนุพงศ์
		๓๔	นาวาอากาศเอก เอกชัย สิงห์ทอง
		๓๕	นาวาอากาศโท กำพล โหมดเอี่ยม
๑๓	กองบัญชาการกองทัพไทย	๓๖	นาวาอากาศเอก ประทีป ขุมทอง
		๓๗	พันโท ชวลิต เชียงปิ๋ว
		๓๘	นาวาโทหญิง สุภาพร แสงสว่าง
		๓๙	ร้อยตรี ชนพล ประสพจำรูญภิญโญ
		๔๐	เรือตรี ธีระวัฒน์ พูนวิเชียร
		๔๑	คุณวรธน เจริญผล
๑๔	การท่าเรือแห่งประเทศไทย	๔๒	คุณพยุงเกียรติ เจริญลือชัย
		๔๓	คุณเชาวลิต อินทร์จันทร์
๑๕	การประปาส่วนภูมิภาค	๔๔	คุณวีรศักดิ์ เหย่ากุลบดี
		๔๕	คุณรัฐกร ทองเรือง
		๔๖	คุณทรงพล เมืองรอด
๑๖	การไฟฟ้านครหลวง	๔๗	คุณธนะพล สกุลธนะ
		๔๘	คุณสาธิต บุญหลง
		๔๙	คุณชัยชนะ สารสินธร
		๕๐	คุณจิรัชญา กาญจนกุญชร
		๕๑	คุณณรงค์ศักดิ์ เรืองโฉม
		๕๒	คุณพลวัต ชุ่มอินทร์
		๕๓	คุณณัฐพงศ์ รังสิมันตุชาติ
		๕๔	คุณสิริรักษ์ ไทยมีสุข
๑๗	การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย	๕๕	คุณสมพล วีระดำรงพันธุ์
		๕๖	คุณภูริทัต พุ่มพฤกษ์
		๕๗	คุณจิตสถา ธาตวากร

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๑๘	การไฟฟ้าส่วนภูมิภาค	๕๘	คุณอลิสา ส่งพุทธิพงศ์
		๕๙	คุณศึกษิต ศรีพิชญพันธ์
		๖๐	คุณวสันต์ ชัยพร
๑๙	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	๖๑	ว่าที่ร้อยตรีหญิง ภานุมาศ พระพินิจ
		๖๒	คุณธนากานต์ ส่งสุข
		๖๓	คุณวรรณดี โอฬาร์ผล
		๖๔	คุณอำพล ฤกษ์สมผุส
		๖๕	คุณสุพพัต พิพัฒนกุล
๒๐	การรถไฟแห่งประเทศไทย	๖๖	คุณเมธินี คัมภิรานนท์
		๖๗	คุณนคร ปรุงเลิศบัวทอง
๒๑	ตลาดหลักทรัพย์แห่งประเทศไทย	๖๘	คุณวิทวัส ชุติโสวรรณ
		๖๙	คุณราตรี วงษ์สุวรรณ
๒๒	ธนาคารกรุงเทพ จำกัด (มหาชน)	๗๐	คุณธัญญรัตน์ ทองเพชร
๒๓	ธนาคารกรุงไทย จำกัด (มหาชน)	๗๑	คุณปริญญา เสริมอนุพงษ์
๒๔	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	๗๒	คุณสิทธิกร แสงรัตนพิทักษ์
		๗๓	คุณศิริชัย ปาระสี
		๗๔	คุณปกป้อง รังสิมันตุชาต
		๗๕	คุณกรวิชญ์ ปิ่นทอง
		๗๖	คุณกัณณิกา วรคามิน
๒๕	ธนาคารกสิกรไทย จำกัด (มหาชน)	๗๗	คุณกิติศักดิ์ จิรวรรณกูล
๒๖	ธนาคารทหารไทยธนชาต จำกัด (มหาชน)	๗๘	คุณเพิ่มยศ ภูมิวสนะ
		๗๙	คุณชนะชัย พาขุนทด
		๘๐	คุณชญานุช ธนวงศ์สุวรรณ
		๘๑	คุณธนลักษณ์ สร้อยทอง
๒๗	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)	๘๒	คุณภกร กังพิศดาร
		๘๓	คุณพาวิต ศักดิ์สูง

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๒๘	ธนาคารแห่งประเทศไทย	๘๔	คุณจิรโรจน์ โสอุดร
		๘๕	คุณคมศักดิ์ สุขเกษม
		๘๖	คุณอนุภาค มาตรมูล
		๘๗	คุณภาวิตา เฮงเจริญ
		๘๘	คุณประพนธ์ พันธ์มานะเจริญผล
		๘๙	คุณธนเดช ตะรุโณทัย
		๙๐	คุณณรัฐ วีรทองประเสริฐ
		๙๑	คุณศรัณยา เมฆราตรี
		๙๒	คุณภิญโญ ตรีเพชราภรณ์
		๙๓	คุณสมภพ สุรัตนกวีกุล
๒๙	ธนาคารออมสิน	๙๔	คุณรพีพร จิตรจง
		๙๕	คุณปิยณัฐ ธนะสมบัติ
		๙๖	คุณสิทธิศักดิ์ ศรีเสาวนันท์
๓๐	บริษัท ดีแทค ไตรเน็ต จำกัด	๙๗	คุณอภิชัย วงศ์จินดาคุณ
		๙๘	คุณบัณฑิต แพงป้อง
		๙๙	คุณปกรสิน พรทรัพย์ไพศาล
๓๑	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	๑๐๐	คุณวิชยุตม์ แท่งทองคำ
๓๒	บริษัท ทรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด	๑๐๑	คุณวีณา จ่างเจริญ
๓๓	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	๑๐๒	คุณปุณยนุช คุณนิธิวุฒิ
		๑๐๓	คุณกิตติพงษ์ ธีระเรืองไชยศรี
		๑๐๔	คุณจุลินทร์ อภิบุญ
		๑๐๕	คุณกิตติ บุญมี
		๑๐๖	ดร.ไกรสิน ส่งวัฒนะ

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๓๔	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	๑๐๗	ดร.ผดุงกฤษณ์ แพรกทอง
		๑๐๘	ดร.ธีรวัฒน์ อิสสริยะกุล
		๑๐๙	ดร.ชยพล ตันวงศ์วาล
		๑๑๐	คุณอาภาภร อ่อนเปรี้ยว
		๑๑๑	คุณจารุณี กัมพลาวลี
		๑๑๒	คุณเบญจวรรณ อาภัสรพรหม
		๑๑๓	คุณสุรเชษฐ์ ศรีพลกรัง
		๑๑๔	คุณนรเศรษฐ์ ศรีโพธิ์ทอง
		๑๑๕	คุณกัณณิกา วรคามิน
		๑๑๖	คุณธเชษฐ หอมเกตุ
		๑๑๗	คุณพงษ์ศักดิ์ แน่งน้อย
		๑๑๘	คุณดิษฐวัฒน์ ทรงรัฐเศรษฐ์
		๑๑๙	คุณชนกานต์ รุญเจริญ
		๑๒๐	คุณคมชัย ปวโรภาส
๓๕	บริษัท ปตท. จำกัด (มหาชน)	๑๒๑	คุณนิวิฏฐ์ ผลวานิชย์
๓๖	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	๑๒๒	คุณกอปรยศ บุณยธาดา
		๑๒๓	คุณพลพัฒน์ อัศวสันติ
		๑๒๔	คุณวิเทศน์ เชนธนากิจ
		๑๒๕	คุณภาสุ เสริมศรีสุวรรณ
๓๗	บริษัทระบบขนส่งมวลชน กรุงเทพ จำกัด (มหาชน)	๑๒๖	คุณอุษณีย์ นามศิริ
		๑๒๗	คุณปิยชัย ชูเอม
๓๘	ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร	๑๒๘	คุณศิริพร เภรีฤกษ์
๓๙	ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)	๑๒๙	คุณพิศุทธิ์ ม่วงสมัย
		๑๓๐	ว่าที่ร้อยตรี สมาน ทาโคตร

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๔๐	สำนักข่าวกรองแห่งชาติ	๑๓๑	คุณธีระยุทธ ธีรประถัมภ์
		๑๓๒	คุณนันทพงษ์ นามแก้ว
		๑๓๓	คุณวันชัย แผ่นทอง
		๑๓๔	คุณอัศวิน ศรีสวัสดิ์
		๑๓๕	คุณนฤทธิ์ พาพินิจ
๔๑	สำนักงานการบินพลเรือนแห่งประเทศไทย	๑๓๖	คุณวีระ ระบายศรี
		๑๓๗	คุณอรวรรณ ใจเอื้อ
		๑๓๘	คุณลัคนัย นิติวัฒนวิจารณ์
		๑๓๙	คุณศิวพร รัตนสุวรรณ
๔๒	สำนักงานคณะกรรมการกำกับกิจการพลังงาน	๑๔๐	คุณธีระ ศรีขำ
๔๓	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์	๑๔๑	คุณเจษฎา ปรมาภรณ์พิลาส
๔๔	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	๑๔๒	คุณรติ เพิ่มพูล
		๑๔๓	คุณพัชราภรณ์ ลี้ธนะรุ่ง
		๑๔๔	คุณขวัญชัย คงสุข
		๑๔๕	คุณณรงค์เดช วัชระภาสร
๔๕	สำนักงานคณะกรรมการอาหารและยา	๑๔๖	คุณชาญณรงค์ ปวนปินตา
		๑๔๗	คุณนพดล เสาร์สุวรรณ์
๔๖	สำนักงานตรวจคนเข้าเมือง	๑๔๘	ร้อยตำรวจเอก วรกร ทองสุข
๔๗	สำนักงานตำรวจแห่งชาติ	๑๔๙	พันตำรวจเอก พรชัย โฆษิตสุรังคกุล
		๑๕๐	พันตำรวจตรี ร่มไทร ไทรงาม
		๑๕๑	ร้อยตำรวจเอก ชญาน์ แหวนหล่อ
		๑๕๒	ร้อยตำรวจเอก พิรุณ ศุภฤทธิธำรง
๔๘	สำนักงานปรมาณูเพื่อสันติ	๑๕๓	คุณกฤษฎา ถิ่นทับปุด
		๑๕๔	คุณนวภัทร์ ขันธ์ต้นธง

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๔๙	สำนักงานปลัดกระทรวงคมนาคม	๑๕๕	คุณสรัลพร สุคนธ์พานิช
		๑๕๖	คุณประธาน จิ๋วจู
		๑๕๗	คุณชัยอนันต์ คำรักษ์
		๑๕๘	คุณถิรายุ เพชระบูรณิน
๕๐	สำนักงานปลัดกระทรวงสาธารณสุข	๑๕๙	คุณสมภพ ลายา
		๑๖๐	คุณฐิติภรณ์ สุวรรณหงส์
		๑๖๑	คุณสรายุทธ ภูตาสืบ
		๑๖๒	คุณราชิ ปาลือชา
		๑๖๓	คุณชวลิต รัตนโกสีย์กิจ
		๑๖๔	คุณสุวันต์นา เสมอเนตร
๕๑	สำนักงานสภาความมั่นคงแห่งชาติ	๑๖๕	คุณศิรประภา แก่นดี
		๑๖๖	คุณฐิติรัตน์ เชื้อพุทธ

ง ๓ รายชื่อผู้ทำหน้าที่ในส่วนควบคุมการฝึกและส่วนประเมินผล

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๑	กรมการขนส่งทางราง	๑	คุณโสภิดา อำนวยศิลป์
		๒	คุณภูวิศ รักษาแก้ว
		๓	คุณพลากร กลัดเจริญ
		๔	คุณปัณณพัทธ์ สมหวัง
๒	กรมการปกครอง	๕	คุณวรวิทย์ จิรังคสกุลเดช
๓	กรมชลประทาน	๖	คุณราชพล หิรัญรักษ์
		๗	คุณอัจฉรา ดาวัน
๔	กรมธุรกิจพลังงาน	๘	คุณณัฐวดี คำภิรานนท์
๕	กรมป้องกันและบรรเทาสาธารณภัย	๙	คุณสุไลลักษณ์ แบ่งลาภ
๖	กรมศุลกากร	๑๐	คุณกำชัย จัตตานนท์
		๑๑	คุณบวร เรืองแรงสกุล

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๗	กระทรวงการคลัง	๑๒	คุณบุญลือ จิตตคาม
		๑๓	คุณเฉลิมศักดิ์ เลิศวงศ์เสถียร
๘	กระทรวงการต่างประเทศ	๑๔	คุณชูเกียรติ ประเสริฐสุข
		๑๕	คุณสุดาภรณ์ แต้เจริญผล
๙	กระทรวงพลังงาน	๑๖	คุณธวัชชัย สุขสาย
		๑๗	คุณอรอนุตตร์ สุทธิ์เสงี่ยม
		๑๘	คุณภาณุพงศ์ ปรึกษา
๑๐	กองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ	๑๙	พันตำรวจเอกหญิง สุทิศา รัตนเทวมาตย์
๑๑	กองทัพบก	๒๐	พันโท พรสวรรค์ พรหมอินทร์
๑๒	กองทัพเรือ	๒๑	นาวาเอก ทรงฤทธิ์ กิตติพีรชล (Co-Agent)
		๒๒	นาวาโท คณิน ศิริธรากูล (Game Master)
		๒๓	เรือโท ธีรพล หนองหว้า (Co-Agent)
๑๓	กองทัพอากาศ	๒๔	นาวาอากาศเอก วิพุธ อนันทนุพงศ์
		๒๕	เรืออากาศตรี รักพงศ์ วงศ์ปัญญาดี
๑๔	กองบังคับการตำรวจจราจร กองบัญชาการตำรวจนครบาล สำนักงานตำรวจแห่งชาติ	๒๖	พันตำรวจตรี ร่มไทร ไทรงาม
		๒๗	ร้อยตำรวจตรี นพรุจ โตงิ้ว
๑๕	กองบัญชาการกองทัพไทย	๒๘	ร้อยเอก พงศ์พัฒน์ เพ็ชรไชย (Co-Agent)
		๒๙	เรือตรี ธีระวัฒน์ พูนวิเชียร
		๓๐	เรืออากาศตรี ชนพล ประสพจำรูญภิญโญ (Co-Agent)
๑๖	การประปาส่วนภูมิภาค	๓๑	คุณรัฐกร ทองเรือง
		๓๒	คุณวีรศักดิ์ เหย่ากุลบดี
๑๗	การไฟฟ้านครหลวง	๓๓	คุณสาธิต บุญหลง (Game Master)
		๓๔	คุณณรงค์ศักดิ์ เรืองโฉม

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๑๘	การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย	๓๕	คุณสมพล วีระดำรงพันธุ์ (Game Master)
		๓๖	คุณจิตสถา ธาตวากร
		๓๗	คุณภูริทัต พุ่มพฤกษ์
๑๙	การไฟฟ้าส่วนภูมิภาค	๓๘	คุณอลิสา ส่งพุทธิพงศ์
		๓๙	คุณศึกษิต ศรีพิชญพันธ์ (Game Master)
๒๐	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	๔๐	ว่าที่ร้อยตรีหญิง ภานุมาศ พระพินิจ (Game Master)
		๔๑	คุณสุพพัต พิพัฒนกุล
		๔๒	คุณสมคิด ลีลิตธรรม
		๔๓	คุณวรรณดี โอฬาร์ผล
		๔๔	คุณธนากานต์ ส่งสุข
		๔๕	คุณอำพล ฤกษ์สมผุส (Game Master)
๒๑	การรถไฟแห่งประเทศไทย	๔๖	คุณเมธินี คัมภิรานนท์ (Game Master)
		๔๗	คุณนคร ปรุงเลิศบัวทอง
๒๒	ตลาดหลักทรัพย์แห่งประเทศไทย	๔๘	คุณวิทวัส ชุติโสวรรณ
๒๓	ธนาคารกรุงไทย จำกัด (มหาชน)	๔๙	คุณจริยา อัตต์สินทอง
๒๔	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	๕๐	คุณกมลวรรณ ทิพยวรานันท์
		๕๑	คุณศุภฤกษ์ กิรณโสภณ
๒๕	ธนาคารทหารไทยธนชาต จำกัด (มหาชน)	๕๒	คุณประกลกฤษ แสงชูวงศ์ (Game Master)

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๒๖	ธนาคารแห่งประเทศไทย	๕๓	คุณคมศักดิ์ สุขเกษม (Game Master)
		๕๔	คุณจิรโรจน์ โสอุดร
		๕๕	คุณพชรวรรณ ทองเอี่ยม
		๕๖	คุณณรัฐ วีรทองประเสริฐ
		๕๗	คุณธนเดช ตะรุโณทัย
		๕๘	คุณสิริกุล ภัทรธรรมกุล
		๕๙	คุณกฤติมา เกรียงวัฒนศิริ
		๖๐	คุณพงศ์รวี เตชะวีรพงศ์
๒๗	ธนาคารออมสิน	๖๑	คุณปิยณัฐ ธนะสมบัติ
๒๘	บริษัท ดีแทค ไตรเน็ต จำกัด	๖๒	คุณบัณฑิต แพงป้อง
		๖๓	คุณอภิชัย วงศ์จินดาคุณ
๒๙	บริษัท ตลาดสัญญาซื้อขายล่วงหน้า (ประเทศไทย) จำกัด (มหาชน)	๖๔	คุณวิทวัส ชุติโสวรรณ
๓๐	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	๖๕	คุณวรวิทย์ กิตติกุศล
๓๑	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	๖๖	คุณณฐกร เทศสอาด
๓๒	บริษัท ทางด่วนและรถไฟฟ้า กรุงเทพ จำกัด (มหาชน)	๖๗	คุณประชา อุดมชัยพร
๓๓	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	๖๘	ดร.ผดุงกฤษณ์ แพรกทอง
		๖๙	ดร.ธีรวัฒน์ อิสสริยะกุล
		๗๐	คุณนรเศรษฐ์ ศรีโพธิ์ทอง
		๗๑	คุณอาภาภร อ่อนเปรี้ยว
		๗๒	คุณอุบลรัตน์ โรจน์พจนานาวิน
		๗๓	คุณชนกานต์ รุญเจริญ
		๗๔	คุณดิษฐวัฒน์ ทรงรัฐเศรษฐ์
		๗๕	คุณปัทมา พุ่มชูศักดิ์
๓๔	บริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด	๗๖	คุณอัศนัย จุลกิจวัฒน์

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๓๕	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	๗๗	คุณพลพัฒน์ อัศวส้นติ
		๗๘	คุณภาสุ เสริมศรีสุวรรณ
		๗๙	คุณวีรยุทธ สิทธิ์สกนธ์กุล
๓๖	บริษัทระบบขนส่งมวลชน กรุงเทพ จำกัด (มหาชน)	๘๐	คุณอุษณีย์ นามศิริ (Game Master)
		๘๑	คุณปิยชัย ชูเอม
๓๗	ศูนย์ประสานงานด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)	๘๒	คุณปรมินทร์ ช่วงมณี
		๘๓	คุณปิลัญญา เชิญถนอมวงศ์
๓๘	ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)	๘๔	คุณพิศุทธิ์ ม่วงสมัย (Game Master)
		๘๕	ว่าที่ร้อยตรี สมาน ทาโคตร
๓๙	สำนักข่าวกรองแห่งชาติ	๘๖	คุณธีระยุทธ ธีรประถัมภ์
๔๐	สำนักงานการบินพลเรือนแห่งประเทศไทย	๘๗	คุณวีระ ระบายศรี
		๘๘	คุณธนเสฏฐ์ เลื่อมนรินทร์
		๘๙	คุณลัคนัย นิติวัฒนวิจารณ์
๔๑	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์	๙๐	คุณนครินทร์ ลิ้มรังษี
		๙๑	คุณเจษฎา ปรมาภรณ์พิลาส
		๙๒	คุณฉัตร ทองสง (Game Master)
		๙๓	คุณวรนาถ หมื่นวิชิต
๔๒	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ	๙๔	คุณกนกอร ฉวาง
๔๓	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	๙๕	คุณรติ เพิ่มพูล
		๙๖	คุณพัชราภรณ์ ลี้ธนะรุ่ง
๔๔	สำนักงานคณะกรรมการอาหารและยา	๙๗	คุณนพดล เสาร์สุวรรณ์
		๙๘	คุณชาญณรงค์ ปวนปินตา
๔๕	สำนักงานตรวจคนเข้าเมือง	๙๙	พันตำรวจตรีหญิง ปุณยวีร์ ดอกคำ

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๔๖	สำนักงานตำรวจแห่งชาติ	๑๐๐	พันตำรวจตรี ร่มไทร ไทรงาม
		๑๐๑	ร้อยตำรวจโท นพรุจ โตงิ้ว
๔๗	สำนักงานปรมาณูเพื่อสันติ	๑๐๒	คุณกฤษฎา ถิ่นทับปุด (Game Master)
		๑๐๓	คุณนวภัทร์ ขันธ์ต้นธง
๔๘	สำนักงานปลัดกระทรวงกลาโหม	๑๐๔	พันเอก พีระ สกุลรัตนศักดิ์
		๑๐๕	พันเอก สุขธนา พงษ์มา
		๑๐๖	พันโท ปริญญา วีระกุลพิริยะ
		๑๐๗	พันโท จารุกฤษณ์ เรืองสุวรรณ
		๑๐๘	ร้อยโท สันติสุข เทพทอง (Co-Agent)
๔๙	สำนักงานปลัดกระทรวงการคลัง	๑๐๙	คุณมานพ เณรสูงเนิน
๕๐	สำนักงานปลัดกระทรวงคมนาคม	๑๑๐	คุณอาภรณ์ ขวัญสุด
		๑๑๑	คุณสรัลพร สุคนธ์พานิช (Game Master)
		๑๑๒	คุณประธาน จิ๋วจู
		๑๑๓	คุณชัยอนันต์ คำรักษ์
๕๑	สำนักงานปลัดกระทรวงสาธารณสุข	๑๑๔	คุณอนันต์ กนกศิลป์
		๑๑๕	คุณปนิสภ์ วณิชชานนท์ (Game Master)
		๑๑๖	คุณพีระวิทย์ สิงห์สูง
		๑๑๗	คุณสรายุทธ ภูตาสืบ
		๑๑๘	คุณราชิ ปาลือชา (Game Master)
๕๒	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	๑๑๙	คุณคมกริช คำสวัสดิ์ (Game Master)
		๑๒๐	คุณศรีสุดา แซ่เฮ้ง (Game Master)
		๑๒๑	คุณพลากร ลาภอลงกรณ์ (Game Master)
๕๓	องค์การเภสัชกรรม	๑๒๒	คุณยงยุทธ เกตุสำเภา
		๑๒๓	คุณยงยุทธ ไข่เจริญ

ลำดับ	หน่วยงาน	ลำดับที่	รายชื่อ
๕๔	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	๑๒๔	พันเอก คทาวุธ ขจรกิตติยุทธ (Co-Agent)
		๑๒๕	นางมัตติกา จงพิริยะอนันต์ (Co-Agent)
		๑๒๖	นายทานตะวัน เรืองไทย (Co-Agent)

ง ๔ รายชื่อผู้เข้ารับการฝึก

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๑	กรมการขนส่งทางราง	๑	คุณพงศธร ศิริจันทร์เพ็ญ
		๒	คุณธนินท์ธร วาศพุฒิสิทธิ์
๒	กรมชลประทาน	๓	ว่าที่ร้อยตรี ฉัตรณรงค์ กัณหรัตน์
		๔	คุณสิริวัฒน์ หญีตสอน
		๕	คุณพิชิต ขุมทรัพย์
		๖	คุณณัฐวงษ์ พรอโนทัย
		๗	คุณศุภชัย คะชาถา
		๘	คุณภาณุวัฒน์ ฤทธิสิทธิ์
		๙	คุณชัยวัฒน์ เกิดธีระพงศ์
๓	กรมธุรกิจพลังงาน	๑๐	คุณอดินันท์ ดิษฐเกษร
		๑๑	คุณจุฑารัตน์ คงมี
		๑๒	คุณภัคจิรา ปรีเปรม
		๑๓	คุณสุมาลี สีสุข
๔	กรมป้องกันและบรรเทาสาธารณภัย	๑๔	คุณณรัณภัช แสงทอง
		๑๕	คุณปรัชญา สนิทมัจโร
๕	กระทรวงการคลัง	๑๖	คุณประทีป สร้อยนาค
๖	กระทรวงการต่างประเทศ	๑๗	คุณธีรวุฒิ มงคลสหกุล
		๑๘	คุณบัณฑิต บุญนิธิ
		๑๙	คุณกฤษฎา โพธิ์แดง
		๒๐	คุณนันทวัฒน์ ทองมวน

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๗	กระทรวงพลังงาน	๒๑	คุณจรัสพงษ์ จำนงทอง
		๒๒	คุณธนพล ศรีเมือง
		๒๓	คุณธีรวัฒน์ จุฑาวิจิตรธรรม
		๒๔	คุณนิธินาถ สุดปัญญา
		๒๕	คุณฐิติญาภรณ์ วีระพงษ์
๘	กองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ	๒๖	ร้อยตำรวจเอก บดินทร์ แสงทองล้วน
		๒๗	ว่าที่ร้อยตำรวจโท วุฒิพงษ์ วิรติกุล
		๒๘	ว่าที่ร้อยตำรวจโท กิตติภัค วรรณพานิช
		๒๙	ว่าที่ร้อยตำรวจโท ประจักษ์ โฉมงาม
		๓๐	ว่าที่ร้อยตำรวจตรีหญิง นภัสสร อนุเอกจิตร
๙	กองทัพบก	๓๑	พันเอกหญิง เครือวัลย์ ไพรวัน
		๓๒	พันโท จิระเดช ปานพรหมมาศ
		๓๓	ร้อยโท มนตรี อินบุญส่ง
		๓๔	ร้อยโท ศุภวัชร์ คีรีรัตน์
		๓๕	ร้อยตรี เกียรติศักดิ์ ลุยทอง
๑๐	กองทัพเรือ	๓๖	นาวาโท นุวัฒน์ สุขแสง
		๓๗	นาวาโท วิโรจน์ วงษ์เวียน
		๓๘	ว่าที่นาวาตรีหญิง กิตติวรรณ เอมสุข
		๓๙	เรือโทหญิง สุพิชญา เย็นสมุทร
		๔๐	พันจ่าตรี พงศกร รุ่งเครือ
๑๑	กองทัพอากาศ	๔๑	นาวาอากาศโท ชัชชัย บุตรสอน
		๔๒	เรืออากาศโท สมบูรณ์ อุดนัน
		๔๓	เรืออากาศโท ดำรงค์เดช ศิลายศ
		๔๔	เรืออากาศโท พัทธกรณ์ ทรัพย์เจริญ
		๔๕	เรืออากาศตรี ศุภชัย พันธุ์สุข

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๑๒	กองบังคับการตำรวจจราจร กองบัญชาการตำรวจนครบาล สำนักงานตำรวจแห่งชาติ	๔๖	สิบตำรวจเอก ไพโรจน์ เขียวอิ่ม
๑๓	กองบัญชาการกองทัพไทย	๔๗	นาวาอากาศโท สมศักดิ์ เมาลีทอง
		๔๘	คุณวรธน เจริญผล
๑๔	การท่าเรือแห่งประเทศไทย	๔๙	คุณชาญณรงค์ ศิริสุขโภคา
		๕๐	คุณวุฒิภูมิ ประทีปกิจไพศาล
		๕๑	คุณอานนท์ แสงเมฆ
		๕๒	คุณอิสระ ฟ้าสาง
		๕๓	คุณเปรมรัชต์ กรัสพงษ์
๑๕	การประปาส่วนภูมิภาค	๕๔	คุณวชิระ กลั่นจัตุรัส
		๕๕	คุณพชร เจริญดี
		๕๖	คุณสุริยกมล ศรีสุนทรไท
		๕๗	คุณอิสฬาณุรักษ์ ชูพงศ์
๑๖	การไฟฟ้านครหลวง	๕๘	คุณสิริรักษ์ ไทยมีสุข
		๕๙	คุณพลวัต ชุ่มอินทร์
		๖๐	คุณณัฐพงศ์ รังสิมันตุชาติ
		๖๑	คุณจิรัชญา กาญจนกุญชร
		๖๒	คุณชัยชนะ สารสินธร
		๖๓	คุณธนะพล สกุลธนะ
		๖๔	คุณกิตติศักดิ์ จัดเจนนาวี
		๖๕	คุณวีรพล ภู่พันธ์

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๑๗	การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย	๖๖	คุณเอก เจียมวงษา
		๖๗	คุณกมล ทองขาว
		๖๘	คุณธนา พงษ์กิตติหล้า
		๖๙	คุณเรืองศักดิ์ แก้วอยู่
		๗๐	คุณกฤชพงศ์ ธรรมานุกรศรี
		๗๑	คุณพงศภัค จันทร์นาค
		๗๒	คุณรภัสสิทธิ์ ตั้งเอี่ยมอมร
		๗๓	คุณไพรวัลย์ จรวงษ์
๑๘	การไฟฟ้าส่วนภูมิภาค	๗๔	คุณวสันต์ ชัยพร
		๗๕	คุณจารุวัชร์ ดวงจิโน
		๗๖	คุณกฤติกา ชอบชื่นชม
		๗๗	คุณกนกวรรณ รบมีชัย
		๗๘	คุณอภิรดา ธีรลีกุล
๑๙	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	๗๙	คุณกฤษฎิ์ธิวัฒน์ ขจรพันธ์
		๘๐	คุณพิสิทธิ์ นพคุณพงศ์
		๘๑	คุณชนนิกานต์ จินดาศรี
		๘๒	คุณสิรินาถ แสงสุวรรณ
		๘๓	คุณภัทรสุดา หวานแหลม
		๘๔	คุณณัฐพล ศุภนิมิตรเจริญพร
๒๐	การรถไฟแห่งประเทศไทย	๘๕	คุณสุจิตรา พงศ์พิศุทธิ์โสภา
		๘๖	คุณกิตติทัต กองคำ
		๘๗	คุณชัยทัต ขุมเงิน
		๘๘	คุณเรือนชาย หวัดเพ็ชร
		๘๙	คุณเมธาพัฒน์ สุนทรวราภาส
		๙๐	คุณชาญณรงค์ จันทโพธิ์
		๙๑	คุณชาคริต อัตถจรรยา
		๙๒	คุณพงศ์พศวัต สังข์ทอง

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๒๑-๒๔	ตลาดหลักทรัพย์แห่งประเทศไทย	๙๓	คุณถิรพันธุ์ สรรพกิจ
		๙๔	คุณประจักษ์ ชาญชัยฤกษ์
	บริษัท ตลาดสัญญาซื้อขายล่วงหน้า (ประเทศไทย) จำกัด (มหาชน)	๙๕	คุณไพลิน วัฒนะรัตน์
		๙๖	คุณกนกวรรณ เข็มมาลัย
	บริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด	๙๗	คุณพันธุ์วศิน พงศ์เพชรดิถ
		๙๘	คุณราตรี วงษ์สุวรรณ
	บริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด	๙๙	คุณสาริศ งามเสงี่ยม
		๑๐๐	คุณอดิศร โรจนพันธุ์
๒๕	ธนาคารกรุงเทพ จำกัด (มหาชน)	๑๐๑	คุณธัญญรัตน์ ทองเพชร
		๑๐๒	คุณสุวิทย์ วศินวงศ์
		๑๐๓	คุณครองสิญจ์ สมประสงค์
๒๖	ธนาคารกรุงไทย จำกัด (มหาชน)	๑๐๔	คุณนิโรจน์ ผิวพรรณ
		๑๐๕	คุณธีระ ธนากรปิ่นทอง
		๑๐๖	คุณสมพัฒน์ มงคลพิไลสกุล
		๑๐๗	คุณศันสนะ วอแสวง
		๑๐๘	คุณปทิตตา ไทยเมืองทอง
		๑๐๙	คุณปริญญา เสริมอนุพงษ์
		๑๑๐	คุณชลาลัย มกุลพานิช
๒๗	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	๑๑๑	คุณกรวิชญ์ ปิ่นทอง
		๑๑๒	คุณปกป้อง รังสิมันตุชาต
		๑๑๓	คุณสิทธิกร แสงรัตนพิทักษ์
		๑๑๔	คุณศิริชัย ปาระสี
		๑๑๕	คุณวิเชียร ศิริศรีมังกร
๒๘	ธนาคารกสิกรไทย จำกัด (มหาชน)	๑๑๖	คุณชัชวัฒน์ อัศวรักวงศ์
		๑๑๗	คุณสุทธิพันธ์ ภัสสร
		๑๑๘	คุณกิติศักดิ์ จิรวรรณกูล
		๑๑๙	คุณสาธินี ศรีรัตนพงษ์
		๑๒๐	คุณแก้วกานต์ ปิ่นจินดา

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๒๙	ธนาคารทหารไทยธนชาต จำกัด (มหาชน)	๑๒๑	คุณธนลักษณ์ สร้อยทอง
		๑๒๒	คุณภะคะ หวังประกอบสุข
		๑๒๓	คุณประภาส พูลศรี
		๑๒๔	คุณเกศนี กฤตยากีรณ
๓๐	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)	๑๒๕	ดร.ศุภกร กังพิศดาร
		๑๒๖	คุณพาวิต ศักดิ์สูง
		๑๒๗	คุณวราลี วัฒนวิบูลย์
		๑๒๘	คุณวัฒนี สมจิตต์
		๑๒๙	คุณพูนชัย สิทธิกรเมธากุล
๓๑	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร	๑๓๐	คุณพงษ์เทพ พรหมศิริ
		๑๓๑	คุณสัณห์ชัย เตียธสิทธิ์
		๑๓๒	คุณพีระปกรณ์ ปิงแก้ว
		๑๓๓	คุณศิริรัตน์ วงศ์สถิตย์พร
		๑๓๔	คุณพรพรหม เหล่ากิจไพศาล
		๑๓๕	คุณปนัสย์ มั่งประยูร
		๑๓๖	คุณสมรัฐ เชตนุช
		๑๓๗	คุณประวีณ เลิศล้ำ
		๑๓๘	คุณปิยะพล ปิยะกิจ
		๑๓๙	คุณปัณณ์พัฒน์ เบญญาพรพงศ์
		๑๔๐	คุณกิจติพงษ์ ทะนงค์ลักณ์
		๑๔๑	คุณอัฏฐพร พลอินทร์
๓๒	ธนาคารแห่งประเทศไทย	๑๔๒	คุณประพนธ์ พันธ์มานะเจริญผล
		๑๔๓	คุณปัณชญาพิชญ์ ธำรงค์คูสกุล
		๑๔๔	คุณพิชญา ชุตินิมิตกุล
		๑๔๕	คุณอนุภาค มาตรมูล
		๑๔๖	คุณภาวิตา เฮงเจริญ
		๑๔๗	คุณชลวรรธ จิรเมธาธร

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๓๓	ธนาคารออมสิน	๑๔๘	คุณวชิราวัชร์ มหาทัพกฤษ
		๑๔๙	คุณรพีพร จิตรจง
		๑๕๐	คุณธนัตถ์นันท์ แก้วทอง
		๑๕๑	คุณสิทธิศักดิ์ ศรีเสาวนันท์
		๑๕๒	คุณประวุธ หมัดยะลาน
๓๔	บริษัท ดีแทค ไตรเน็ต จำกัด	๑๕๓	คุณอภิณัฐ กณะวงศ์
		๑๕๔	คุณกศิณ นุตาลัย
		๑๕๕	คุณปกรสิน พรทรัพย์ไพศาล
		๑๕๖	คุณทักพงศ์ บุญทั่ง
		๑๕๗	คุณธีรยุทธ กระจ่างโพธิ์
๓๕	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	๑๕๘	คุณมนัสชัย ใจเอื้อ
		๑๕๙	คุณอัครพงศ์ พันธุมาภรณ์
		๑๖๐	คุณณัฐพงษ์ ทองรังษี
		๑๖๑	คุณวิชยุตม์ แท่งทองคำ
		๑๖๒	คุณเนติวุธ สุดหนองบัว
๓๖	บริษัท ทรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด	๑๖๓	คุณกิตติพงษ์ ธีระเรืองไชยศรี
		๑๖๔	คุณมัณฑนี เนื่องตุลยศักดิ์
		๑๖๕	คุณสมพล เอี่ยมจิตกุศล
๓๗	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	๑๖๖	คุณจุลินทร์ อภิบุญ
		๑๖๗	คุณกิตติ บุญมี

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๓๘	บริษัท ทางด่วนและรถไฟฟ้ากรุงเทพ จำกัด	๑๖๘	คุณประชา อุดมชัยพร
		๑๖๙	คุณกิติพัฒน์ สุภัคลีลากุล
		๑๗๐	คุณประสงค์ มโนมยางกูร
		๑๗๑	คุณรักข์ษิตา โพธิ์พิทักษ์กุล
		๑๗๒	คุณนิษา น้อยศรี
		๑๗๓	คุณณัฐวุฒิ์ กุตัน
		๑๗๔	คุณนิตยา แก้วทรายขาว
		๑๗๕	คุณสมิทธิ์ สุขเจริญ
		๑๗๖	คุณสุวินันท์ ศรีสิทธิประภา
		๑๗๗	คุณศุภชัย ชุ่มเสนา
		๑๗๘	คุณศุภกร พวงเพชร
		๑๗๙	คุณชวิศ แย้มศิริ
		๑๘๐	คุณพิพัฒน์ เรืองสวัสดิ์
		๑๘๑	คุณสิริชัย สมบูรณ์ดี
		๑๘๒	คุณธราธร มิตรภาพจิต
๓๙	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	๑๘๓	คุณพิมพ์พินิต ศรีมุกข์
		๑๘๔	คุณคมชัย ปวโรภาส
		๑๘๕	คุณจารุณี กัมพลาวลี
		๑๘๖	คุณรัตน์ติกา พรมหนู
		๑๘๗	คุณยอดเพชร บุบผา
		๑๘๘	คุณเบญจวรรณ อาภัสรพรหม
๔๐	บริษัท เนชั่นแนล ไอทีเอ็มเอ๊กซ์ จำกัด	๑๘๙	คุณอิทธิวัฒน์ จารุศรีวรกุล
		๑๙๐	คุณจิตติมาศ เรืองอร่าม
		๑๙๑	คุณชูเกียรติ โพธิวราพรรณ
		๑๙๒	คุณเจตพล พุ่มวัฒนกุล
		๑๙๓	คุณวิไลลักษณ์ พันชน
		๑๙๔	คุณสุทธิพงศ์ แก้วคุณากร

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๔๑	บริษัท ปตท. จำกัด (มหาชน)	๑๙๕	คุณนิวิฏฐ์ ผลวานิชย์
		๑๙๖	คุณวรรธนัย เกิดสมบัติ
๔๒	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	๑๙๗	คุณกอปรยศ บุณยธาดา
		๑๙๘	คุณวิเทศน์ เชนธนากิจ
		๑๙๙	คุณวราลี จิรชัยศรี
		๒๐๐	คุณณฤดี คอศิริ
		๒๐๑	คุณวิสิฐศักดิ์ เจริญไชย
๔๓	บริษัทระบบขนส่งมวลชน กรุงเทพ จำกัด (มหาชน)	๒๐๒	คุณปรมินทร์ พิสิฐอรรถกุล
		๒๐๓	คุณชนนิกานต์ กตเวทิตานนท์
		๒๐๔	คุณกานดา แซ่อึ้ง
		๒๐๕	คุณบุรินทร์ พิศเพ็ง
		๒๐๖	คุณธีรศาสตร์ ทิพย์กมลแสง
๔๔	ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ	๒๐๗	พันตำรวจตรี ชัยณรงค์ เอ่งฉ้วน
๔๕	สำนักข่าวกรองแห่งชาติ	๒๐๘	คุณณัฐนรี ศรีไชย
		๒๐๙	คุณรณกร ถ้อยสุนทร
		๒๑๐	คุณอัศวิน ศรีสวัสดิ์
		๒๑๑	คุณนฤทธิ์ พาพินิจ
		๒๑๒	คุณณัฐพงศ์ บุญฤทธิ์
๔๖	สำนักงานการบินพลเรือนแห่งประเทศไทย	๒๑๓	คุณอรวรรณ ใจเอื้อ
		๒๑๔	คุณสราวุฒิ ล่วงเขตต์
		๒๑๕	คุณวัลภา เรือนขันทร์
		๒๑๖	คุณประมุข นิภารักษ์
		๒๑๗	คุณศิวพร รัตนสุวรรณ
๔๗	สำนักงานคณะกรรมการกำกับกิจการพลังงาน	๒๑๘	คุณคุณธีระ ศรีขำ
		๒๑๙	คุณภัสสร์อร เรืองจันทร์

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๔๘	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์	๒๒๐	คุณพชร แก้ววิเศษ
		๒๒๑	คุณธรรมนูญ เพลิดเพลิน
๔๙	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ	๒๒๒	ว่าที่ร้อยเอก ณัฐ ตันติบุตร
		๒๒๓	คุณจักรกฤษณ์ ศรีอรุณ
๕๐	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	๒๒๔	คุณทวีสิทธิ์ เพ็ญรัศมีพูนสุข
		๒๒๕	คุณขวัญชัย คงสุข
๕๑	สำนักงานคณะกรรมการอาหารและยา	๒๒๖	คุณเทวะ แก้วปลั่ง
		๒๒๗	คุณธัญญลักษณ์ เฉลิมทรง
๕๒	สำนักงานตรวจคนเข้าเมือง	๒๒๘	ร้อยตำรวจเอก วรกร ทองสุข
๕๓	สำนักงานตำรวจแห่งชาติ	๒๒๙	สิบตำรวจโทธนัท โรจน์สัตตรัตน์
		๒๓๐	สิบตำรวจโทวันเฉลิม ดีวิญญา
๕๔	สำนักงานปรมาณูเพื่อสันติ	๒๓๑	คุณพงศ์พันธ์ นาคแก้ว
		๒๓๒	คุณอัฉรารัตน์ ฉายเหมือนวงศ์
		๒๓๓	คุณไชยยศ สุนทราภา
		๒๓๔	คุณศันสนีย์ บริรักษ์
		๒๓๕	คุณเอกลักษณ์ ไชยวัฒน์
		๒๓๖	คุณชนาธิป คำเพ็ญ
๕๕	สำนักงานปลัดกระทรวงกลาโหม	๒๓๗	พันเอก ธนภัทร บุญเดช
		๒๓๘	นาวาตรี วัลลภ บุญณรงค์
		๒๓๙	พันตรี ญาณินทร์ สุรพันธ์ไพโรจน์
		๒๔๐	เรือเอก พงศ์ปณต ทรัยพ์วิไล
		๒๔๑	เรืออากาศโท นิติพัฒน์ วานิกร
		๒๔๒	ร้อยตรี ชนาธิป อินพักทัน

ลำดับ	หน่วยงาน	ลำดับที่	ชื่อ-สกุล
๕๖	สำนักงานปลัดกระทรวงการคลัง	๒๔๓	คุณปริญญา ปรีดียานนท์
		๒๔๔	คุณมาฆฤกษ์ เกียรติก้อง
		๒๔๕	คุณจิรวัฒน์ อิ่มนุกูลกิจ
		๒๔๖	คุณมนตรพล ลาชะเกตุ
		๒๔๗	คุณอนุวัฒน์ บัวไสว
๕๗	สำนักงานปลัดกระทรวงคมนาคม	๒๔๘	คุณถิรายุ เพชระบูรณิน
๕๘	สำนักงานปลัดกระทรวงสาธารณสุข	๒๔๙	ดร.สิริพรรณ แสงอรุณ
		๒๕๐	สิบเอกจุฑาทิตย์ แสนสะอาด
		๒๕๑	คุณสุวันต์นา เสมอเนตร
		๒๕๒	คุณชุติมา โพธิ์ป้อม
		๒๕๓	คุณฐิติภรณ์ สุวรรณหงส์
		๒๕๔	คุณสมภพ ลายา
		๒๕๕	คุณชัยยศ อินติยะ
		๒๕๖	คุณชวลิต รัตนโกสีย์กิจ
		๒๕๗	คุณอริณญา พงศธรพิศุทธิ์
๕๙	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	๒๕๘	คุณสุรัชนา รัตนเปรมใจ
		๒๕๙	คุณสกุลวัล ประเดิมวงศ์
		๒๖๐	คุณนฤเทพ ฉัตรวนิชกุล
		๒๖๑	คุณธนากร สังข์อ้น
		๒๖๒	คุณพงศ์ระพี นาคมณี
๖๐	สำนักงานสภาความมั่นคงแห่งชาติ	๒๖๓	คุณปรียาภรณ์ อยู่คง
		๒๖๔	คุณลักษิกา สงวนสุข
		๒๖๕	คุณฐิติรัตน์ เชื้อพุทธ
		๒๖๖	คุณศิรประภา แก่นดี
		๒๖๗	คุณวิลาวัณย์ ศิลปเดช
๖๑	องค์การเภสัชกรรม	๒๖๘	คุณฤทธิรงค์ ศรีสมานุวัตร
		๒๖๙	คุณอาทิตยา ศรีพิมพ์
		๒๗๐	คุณวศินี คุ้มไพร

NCSA
สกมช
สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ