คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)

คู่มือการตอบสนองภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย

(Cyber Incident Response Plan Handbook)

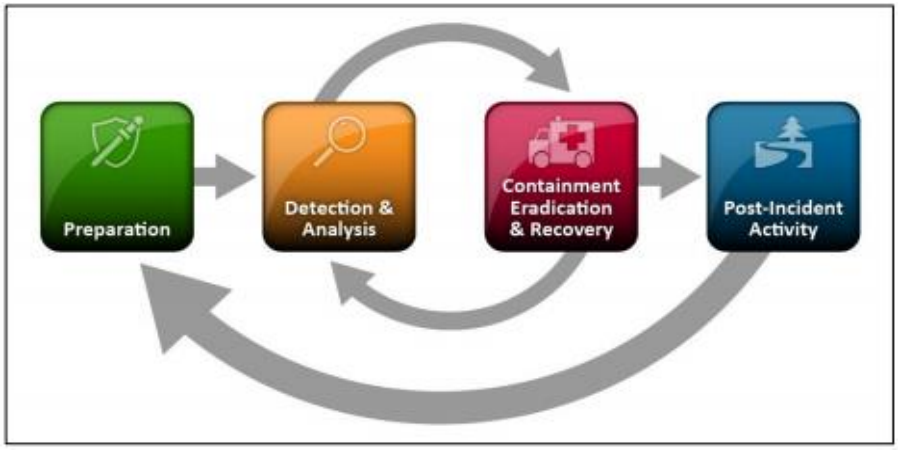
พ.ศ. ๒๕๖๔

(เผยแพร่ เดือนธันวาคม ๒๕๖๔)

สารบัญ

บทนำ

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ได้จัดทำ **"คู่มือ Cyber Incident Response Plan Handbook สำหรับบริษัทประกันภัย"** เพื่อเป็นคู่มือที่ใช้อ้างอิงและให้แนวทางแก่บริษัทในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งการจัดทำแผนการตอบสนองต่อภัยคุกคามทาง ไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับและวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และ การดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post-Incident Activity) มุ่งหวังให้เป็นประโยชน์ต่อบริษัทในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เหมาะสมกับขนาด ความซับซ้อน ความเสี่ยง และรูปแบบในการดำเนินธุรกิจ โดยคู่มือฉบับนี้ได้อ้างอิงหลักการและขั้นตอนตามมาตรฐานของเอกสาร "Computer Security Incident Handling Guide"Special Publication 800-61 Revision 2 ซึ่งจัดทำโดย Nation Institute of Standards and Technology (NIST)



รูปที่ ๑ NIST Incident Response Life

ทั้งนี้ แนวทางหรือคำแนะนำในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ในฉบับนี้ บริษัทสามารถพิจารณาประยุกต์ใช้ควบคู่กับ "**แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP) ในแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓**"

นอกจากนี้ ในแต่ละขั้นตอนของการรับมือและตอบสนอง จะประกอบด้วยหัวข้อที่จะใช้เป็นแนวทางในการวางแผนเพื่อให้บรรลุผลในแต่ละขั้นตอนตามที่ปรากฏใน Life Cycle ดังต่อไปนี้

- ✓ ผลลัพธ์ที่สำคัญ (Key Results)
- ✓ กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities)
- ✓ ข้อควรคำนึงถึงในการวางแผน (Cautions)

เหตุผลความจำเป็นของการกำหนดแนวทางการรับมือภัยคุกคามทางไซเบอร์

ปัจจุบันสภาพแวดล้อมในการดำเนินธุรกิจได้มีการเปลี่ยนแปลงไปจากอดีตเป็นอย่างมาก เนื่องจากเทคโนโลยีที่เติบโตรวดเร็วแบบก้าวกระโดด ทำให้บริษัท ต้องปรับตัวให้ทันต่อการเปลี่ยนแปลง และสามารถดำเนินธุรกิจต่อไปได้ จึงได้นำเทคโนโลยีเข้ามามีบทบาทในการดำเนินธุรกิจมากขึ้น ซึ่งย่อมมีความเสี่ยงแฝงมาด้วย ไม่ว่าจะเป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมากซึ่งอาจก่อให้เกิดความเสียหายและมีผลกระทบต่อการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้ (Availability) ของข้อมูลตลอดเวลา แม้บริษัทจะมีแนวทางป้องกันความมั่นคงปลอดภัยทางสารสนเทศ (Information Security) อย่างไรก็ตามแนวทางดังกล่าวสามารถครอบคลุมความมั่นคงปลอดภัยได้เฉพาะความเสี่ยงและภัยคุกคามที่เป็นที่รู้จักอยู่แล้ว ในขณะที่ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามที่มีการเปลี่ยนแปลงและพัฒนาตัวเองอยู่ตลอดเวลา จึงเป็นที่มาของ**ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)** และ**การรับมือภัยคุกคามทางไซเบอร์ (Incident Response)** เพื่อใช้ในการบริหารจัดการความเสี่ยงดังกล่าว รวมถึงตอบสนองต่อเหตุการณ์ที่เกิดขึ้นเพื่อให้บริษัทสามารถดำเนินการด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง พร้อมทั้งลดผลกระทบที่มีต่อข้อมูลสารสนเทศ และเครือข่ายทางสารสนเทศให้น้อยที่สุด เพื่อให้ธุรกิจยังสามารถดำเนินงานได้อย่างต่อเนื่องและสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้มีส่วนได้เสียตลอดเวลา

การกำหนดโครงสร้างการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Organizing a Cyber Incident Response Capability)

บริษัทควรมีการจัดเตรียมเพื่อรองรับขีดความสามารถในการรับมือตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ โดยคำนึงถึงเรื่องสำคัญดังต่อไปนี้

๑. คำจำกัดความ “Events” และ “Incidents”

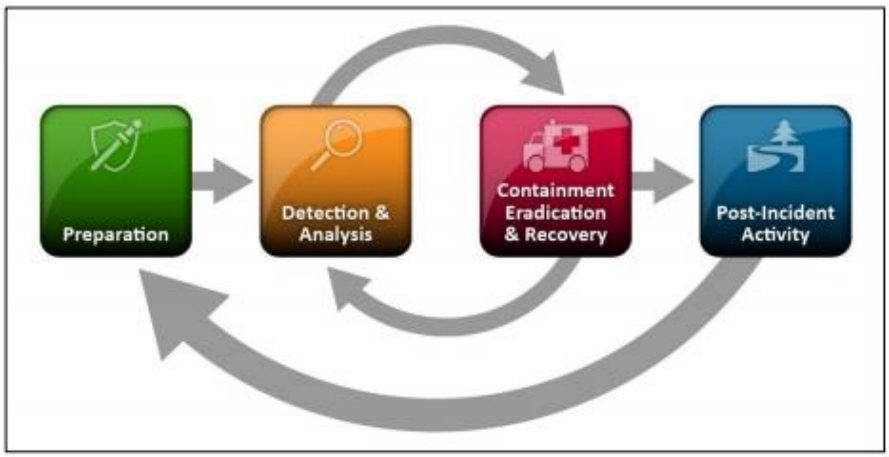
เหตุการณ์ (Events) คือ เหตุการณ์ปกติในการเข้าใช้งานระบบ ซึ่งจะมีความแตกต่างจากเหตุการณ์ที่เป็นภัยคุกคาม (Computer security incident) ซึ่งละเมิดนโยบายความมั่นคงปลอดภัย ข้อตกลงในการใช้งาน และหลักปฏิบัติโดยทั่วไปในด้านการรักษาความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ (baseline) เช่น ความพยายามเข้าใช้งานระบบในเวลาที่ผิดปกติไปจากเวลาทำงานประจำวันของผู้ใช้งาน เป็นต้น

ดังนั้น จึงควรพิจารณาให้ชัดเจนว่าเหตุการณ์ใดเป็นเหตุการณ์ปกติ หรือเป็นเหตุการณ์ที่เป็นภัยคุกคาม และมีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสามารถบริหารจัดการความเสี่ยง และทำการปิดช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการโจมตี

๒. การจัดทำนโยบาย แผนการดำเนินงาน และขั้นตอนการปฏิบัติด้านการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Policy)

เพื่อให้ขอบเขตและเป้าหมายของของการดำเนินงานมีความชัดเจน และสามารถจัดสรรทรัพยากรที่จำเป็นต่อการรับมือภัยคุกคามทางไซเบอร์ รวมถึงกำหนดโครงสร้าง บทบาทหน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ ควรพิจารณากำหนดให้ครอบคลุมในเรื่องดังต่อไปนี้

องค์ประกอบของนโยบาย แผน และขั้นตอนการปฏิบัติ	
นโยบาย จะกำหนดแนวทาง กลยุทธ์ และผลลัพธ์ที่คาดหวัง ซึ่งมีผลกับรายละเอียดในการวางแผน และการเลือกวิธีการในการรับมือที่สอดคล้องกับความต้องการของผู้บริหาร	- ภารกิจและความมุ่งมั่นของฝ่ายบริหาร (Statement of management commitment) - วัตถุประสงค์และเป้าหมายของนโยบาย - ขอบเขตของนโยบาย - คำนิยามที่เกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์ - การกำหนดโครงสร้างองค์กร บทบาทหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ของบุคลากรที่เกี่ยวข้อง เช่น ทีมหรือผู้ทำหน้าที่ในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response Team : IRT) เป็นต้น - การมอบอำนาจให้แก่ทีมรับมือเหตุการณ์ภัยคุกคามในการยึดหรือตัดสิทธิ์การเข้าถึงเครื่องมือด้านเทคโนโลยีสารสนเทศของผู้ใช้งานทั่วไป รวมถึงอำนาจในการติดตามตรวจสอบกิจกรรมที่น่าสงสัยที่เกิดขึ้นภายในองค์กร - การจัดทำข้อกำหนดสำหรับการรายงานเหตุการณ์ภัยคุกคามแต่ละประเภท - การจัดทำข้อกำหนด และแนวทางการสื่อสารและแบ่งปันข้อมูลข่าวสารสู่ภายนอกองค์กร - การกำหนดระดับความรุนแรงของเหตุการณ์ภัยคุกคามทางไซเบอร์ - การกำหนดแบบฟอร์มในการติดต่อและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์
แผนงานอย่างน้อยควรกำหนดขั้นตอนและทรัพยากรที่จะใช้ในการตอบสนอง	เพื่อกำหนดแนวทางการรับมือตอบสนองภัยคุกคามทางไซเบอร์เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อลดผลกระทบที่มีต่อข้อมูลสารสนเทศ และเครือข่ายทางสารสนเทศให้น้อยที่สุด และสามารถทำให้ธุรกิจสามารถดำเนินงานได้อย่างต่อเนื่อง โดยสามารถแบ่งได้เป็น แผนการรับมือทั่วไป และแผนการรับมือภัยคุกคามแบบเฉพาะเจาะจงตามรูปแบบของภัยคุกคาม และการดำเนินการควรสอดคล้อง และเป็นส่วนหนึ่งกับกระบวนการที่เกี่ยวข้องต่างๆ ภายในองค์กร เช่น แผน BCP เป็นต้น นอกจากนี้ ควรมีแนวทาง (Roadmap) ในการพัฒนาทักษะและศักยภาพในการตอบสนองเพื่อเพิ่มขีดความสามารถให้แก่บุคลากร แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ควรระบุขั้นตอนการรับมือและตอบสนองเหตุการณ์ที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยอย่างน้อยควรครอบคลุม ๑) ชื่อแผน วัตถุประสงค์ และขอบเขต ๒) โครงสร้างของการบังคับบัญชาในการดำเนินการตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ และผู้ปฏิบัติหน้าที่แทนในกรณีผู้ปฏิบัติหน้าที่หลักที่ได้รับมอบหมายไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน ๓) รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม เครือข่าย เป็นต้น ๔) ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ และแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ ๕) ขั้นตอนการกู้คืนระบบ โดยจัดทำเป็นเอกสารหรือ คู่มือ หรือ Checklist เพื่อควบคุมกระบวนการให้เป็นไปตามขั้นตอนที่กำหนดไว้ **ตัวอย่าง แนวทางที่ควรกำหนดในแผนงานให้สอดคล้องกับนโยบาย และสามารถประเมินผลตามที่นโยบายกำหนดได้ เช่น** ● ต้องตรวจจับภัยคุกคามให้ได้โดยใช้ระยะเวลาไม่เกิน ๑ วันเมื่อเกิดการโจมตีสำเร็จ

องค์ประกอบของนโยบาย แผน และขั้นตอนการปฏิบัติ	
	• ต้องมีการตรวจจับและเฝ้าระวังแบบ ๒๔ x ๗ • การตั้งค่าอุปกรณ์ตรวจจับให้ครอบคลุมการใช้งานระบบ IT และ มีการประเมินความเปลี่ยนแปลงของระบบ และช่องทางการโจมตีอยู่เสมอ เพื่อให้ระบบตรวจจับทำงานได้ตามภารกิจ • ทีมตอบสนองต่อภัยคุกคามทางไซเบอร์ ต้องดำเนินการทำ Threat Hunting ในระบบที่มีความเสี่ยงสูงเสมอเพื่อป้องกันไม่ให้ภัยคุกคามที่มีความซับซ้อนสูงหลุดรอดการตรวจจับไปได้
ขั้นตอนการปฏิบัติ คือ รายละเอียดการดำเนินงานในแต่ละขั้นตอน เพื่อเพิ่มประสิทธิภาพ ความรวดเร็ว และลดความผิดพลาดที่อาจจะเกิดขึ้นได้	ขั้นตอนการปฏิบัติ หรือที่เรียกว่า Standard Operation Procedures (SOPs) จะกำหนดขั้นตอนการดำเนินงาน รวมทั้งการดำเนินงานด้านเทคนิคอย่างละเอียด เพื่อให้สามารถดำเนินงานตามแผน และได้ผลลัพธ์ตามที่กำหนด โดยต้องครอบคลุมในเรื่องดังต่อไปนี้  **๑. การเตรียมความพร้อม (Preparation)** **๒. การตรวจจับและวิเคราะห์ (Detection & Analysis)** **๓. การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)** **๔. การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)** ทั้งนี้ รายละเอียดสามารถพิจารณาได้จาก หัวข้อ “ขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์”

ทั้งนี้ วัตถุประสงค์หลักในการกำหนดนโยบาย และวางแผนการปฏิบัติงานเพื่อตอบสนองต่อภัยคุกคามทางไซเบอร์ คือ การลดผลกระทบและความเสียหายที่อาจจะเกิดขึ้นกับธุรกิจให้น้อยที่สุด (Minimizing the business impact) เป็นอันดับแรก

๓. โครงสร้างทีมรับมือเหตุการณ์ภัยคุกคาม (Incident Response Team Structure)

ทีมรับมือเหตุการณ์ภัยคุกคาม ควรมีความพร้อมในการจัดการกับภัยคุกคามเมื่อได้รับการแจ้งเหตุที่อาจกระทบต่อความมั่นคงปลอดภัยจากบุคคลภายในองค์กรเสมอ ควรมีการจัดโครงสร้างและขนาดของทีมรับมือเหตุการณ์ภัยคุกคามให้เหมาะสมกับลักษณะและขนาดขององค์กร และควรคำนึงถึงการประสานงานหรือขอความร่วมมือกับฝ่ายงานอื่นภายในองค์กรที่เกี่ยวข้องกับการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น

ทีมรับมือเหตุการณ์ภัยคุกคามสามารถแบ่งได้ ๓ ประเภท ดังนี้

๑. ทีมรับมือเหตุการณ์ภัยคุกคามที่เป็นบุคลากรภายในทั้งหมด (Insource)

๒. ทีมรับมือเหตุการณ์ภัยคุกคามที่มีทั้งบุคลากรภายใน และบุคลากรจากภายนอก (Co-Source)

๓. ทีมรับมือเหตุการณ์ภัยคุกคามที่เป็นบุคลากรจากภายนอกทั้งหมด (Fully Outsourced)

ทั้งนี้ ข้อควรระวัง สำหรับกรณีบริษัทเลือกใช้ทีมรับมือฯ ในรูปแบบ Fully Outsource เช่น คุณภาพของงานที่ได้รับการแบ่งหน้าที่ระหว่างผู้ประสานงานภายในกับผู้ให้บริการ Outsource ที่ชัดเจน การป้องกันข้อมูลความลับไม่ให้ถูกเปิดเผย การไม่ทราบข้อมูลหรือขั้นตอนบางอย่างที่จำเป็นภายในองค์กรซึ่งส่งผลให้เกิดความล่าช้าหรือเกิดปัญหาระหว่างการให้บริการได้ กรณีผู้ให้บริการ Outsource มีความจำเป็นที่จะต้องเข้าถึงระบบภายในด้วยสิทธิ์สูง (Privilege Account) ซึ่งอาจต้องใช้ทรัพยากรเพิ่มเติมในการบริหารจัดการ และอาจเกิดความล่าช้าเนื่องจากการเดินทางไปยังสถานที่บางจุดที่อาจอยู่ไกลจากผู้ให้บริการ ทำให้เกิดความล่าช้าและอาจไม่เป็นไปตามแผนที่วางไว้ เป็นต้น

<u>บุคลากรในส่วนงานอื่นที่ควรมีส่วนเกี่ยวข้องในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์</u>

ตามแนวทางที่แนะนำตาม BCP Guideline ที่ให้บริษัทมีการจัดบุคลากรหรือทีมงานที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Team) โดยอย่างน้อย **ทีมรับมือและตอบสนองฯ ควรประกอบด้วยบุคลากร ๑) บุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงาน**ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้นภายในองค์กร และ **๒) บุคลากรที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนอง**ต่อเหตุการณ์ผิดปกติทางไซเบอร์

นอกจากนี้ บริษัทควรพิจารณาบุคลากรในส่วนงานอื่นที่มีส่วนเกี่ยวข้องในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ที่อาจเกิดขึ้นและส่งผลกระทบในหลายด้านแก่บริษัทนอกเหนือจากด้านเทคนิค เช่น ด้านชื่อเสียงและภาพลักษณ์ ด้านกฎหมาย ด้านการดำเนินธุรกิจ เป็นต้น ดังนั้น การประสานงานเพื่อดำเนินการร่วมกับหน่วยงานอื่นทั้งภายในและภายนอกจึงเป็นสิ่งจำเป็นในการรับมือและตอบสนองต่อภัยคุกคาม โดยผู้ที่ควรเป็นส่วนหนึ่งของแผนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งได้รับการฝึกฝนทักษะที่จำเป็นตามตำแหน่ง และหน้าที่ในการรับมือและตอบสนอง ควรประกอบด้วยบุคคลอย่างน้อยดังต่อไปนี้

- ผู้บริหาร (Top Management)
- ฝ่ายงานเทคโนโลยีสารสนเทศ (IT)
- ฝ่ายงานกฎหมายและควบคุมการปฏิบัติตามกฎหมาย (Legal & Compliance Officer)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)
- ฝ่ายสื่อสารองค์กร (Public Affairs/Media Relations)
- ฝ่ายทรัพยากรบุคคล (Human resources)
- ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team)
- ฝ่ายรักษาความปลอดภัย (Physical Security)

<u>หน้าที่ความรับผิดชอบของทีมตอบสนองต่อภัยคุกคามทางไซเบอร์</u>

๑) การเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ (Intrusion Detection)

๒) ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับการใช้งานเทคโนโลยี (Advisory Distribution) เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง รวมทั้งแจ้งเตือนภัยคุกคามเกิดใหม่เพื่อให้ทุกคนในองค์กรมีความตระหนัก

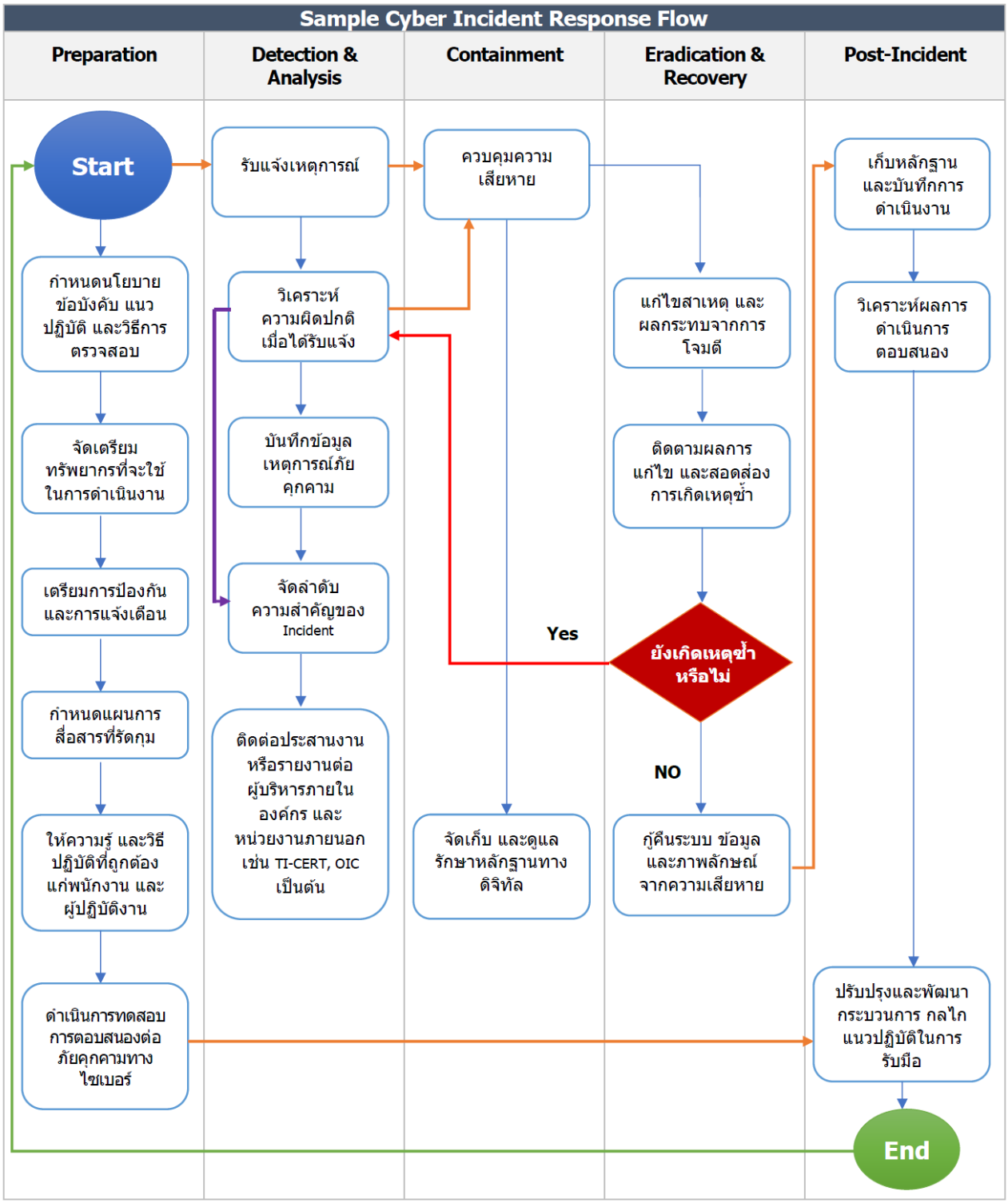
๓) การฝึกอบรมเพื่อสร้างความตระหนัก (Education and Awareness) เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับบุคลากรทุกระดับ เพื่อให้ทุกคนในองค์กรตระหนักรู้ถึงความผิดปกติและช่วยในการสอดส่องดูแลให้กับองค์กรในการตรวจจับและแจ้งเหตุการณ์ที่ผิดปกติ

๔) การมีส่วนร่วมกับหน่วยงานภายนอกองค์กร (Information Sharing) ควรกำหนดขั้นตอนการสื่อสารและประเภทข้อมูล ที่สามารถนำไปแบ่งปันได้กับบุคคลภายนอก ทั้งหน่วยงานบังคับใช้กฎหมาย หน่วยงานกำกับดูแล องค์กรอื่น หรือการติดต่อเพื่อขอความช่วยเหลือจากผู้เชี่ยวชาญจากภายนอกองค์กรที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์เช่น TI-CERT, TCM CERT, TB CERT และ Thai CERT เป็นต้น เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทาง ไซเบอร์ เพื่อช่วยให้การป้องกันและตอบสนองต่อภัยคุกคามได้เร็วยิ่งขึ้น

๔. การฝึกฝนและการทดสอบเป็นประจำ

ผู้ทำหน้าที่รับผิดชอบควรได้รับการอบรมเพื่อฝึกฝนและทดสอบการดำเนินงาน เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ นอกจากนี้ บริษัทควรจัดให้มีการทดสอบแผนเป็นประจำ เพื่อประเมินและทราบถึงประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนา และเพิ่มความชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอโดยที่ไม่ต้องรอให้เกิดการโจมตีจริง ทั้งนี้ บริษัทสามารถพิจารณาแนวทางการฝึกซ้อมและทดสอบแผนได้จากมาตรฐาน Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities Special Publication 800-84 ของ Nation Institute of Standards and Technology (NIST) หรือ สามารถเข้าร่วมการฝึกซ้อมตามที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) จัดเป็นประจำได้

แผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์



รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ในฉบับนี้ บริษัทสามารถพิจารณาแนวทางดำเนินการประยุกต์ใช้ควบคู่กับแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP) ในแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓

โดยมีรายละเอียดดังนี้

ขั้นตอนที่ ๑ : การเตรียมความพร้อม (Preparation)

๑. ผลลัพธ์ที่สำคัญในขั้นตอนนี้ (Key Results)

๑.๑. มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์

๑.๒. มีกระบวนการ และกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นทำหน้าที่ในการตรวจจับความพยายามในการบุกรุกได้อีกด้วย

๒. กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities)

๒.๑ ตามแนวทางที่แนะนำตาม BCP Guideline ที่กำหนดให้บริษัทควรมีการจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ที่ครอบคลุมทั้งในเรื่อง

๑) **การจัดเตรียมเครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์** เช่น รายชื่อและช่องทางการติดต่อผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ช่องทางการรายงานเหตุการณ์ ระบบในการรายงานและติดตามข้อมูล สถานะการดำเนินการของเหตุการณ์ที่ได้รับแจ้ง โปรแกรมเข้ารหัส (Encryption Software) ห้องประชุม (War Room) หรือ Virtual War Room และสถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการจัดเก็บหลักฐาน (Secure Storage Facility) ข้อมูลและพยานวัตถุอื่นๆ ที่สำคัญ โดยเฉพาะหลักฐานทางดิจิทัล เป็นต้น

๒) **อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์** เช่น เครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองข้อมูล (Backup Device) ที่ใช้งานเพื่อการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log Files) หรือสร้าง Disk Image เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ (Packet Sniffers and Protocol Analyzers) เพื่อใช้ศึกษาพฤติกรรมของ Malware หรือความผิดปกติของเครือข่าย เครื่องคอมพิวเตอร์สำรอง เซิร์ฟเวอร์ และอุปกรณ์เครือข่ายที่สามารถใช้ทดแทนอุปกรณ์หลักได้ และอุปกรณ์ที่ใช้ในการรวบรวมหลักฐาน เป็นต้น

๓) **แหล่งข้อมูลในการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Analysis Resources)** เช่น รายการพอร์ตช่องทางการแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ (Port Lists) เอกสารหรือคู่มือการใช้งานของระบบปฏิบัติการ แอปพลิเคชั่น โปรโตคอลที่ใช้ในการสื่อสารระหว่างเครื่องคอมพิวเตอร์ ซอฟต์แวร์สำหรับตรวจจับการบุกรุก และซอฟต์แวร์ป้องกันไวรัส แผนผังเครือข่ายและรายการทรัพย์สินทางสารสนเทศที่สำคัญ ค่าปกติ (Current Baseline) ของระบบ เครือข่าย และแอปพลิเคชั่น รวมทั้งค่า hash ของไฟล์ที่มีความสำคัญ เป็นต้น

๔) **ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม** เช่น ไฟล์ disk image ของระบบปฏิบัติการ (OS) และแอปพลิเคชั่น (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ เป็นต้น

ทั้งนี้ บริษัทสามารถพิจารณาเพิ่มเติมได้ในเรื่องดังต่อไปนี้

- คอมพิวเตอร์ที่ใช้สำหรับการวิเคราะห์หลักฐานทางดิจิทัล (Digital Forensic Workstation) ที่ต้องแยกจากการใช้งานอื่นๆ รวมถึงการเชื่อมต่อทางเครือข่าย และต้องได้รับการตั้งค่าเพื่อความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูลหลักฐานและการวิเคราะห์โดยมิชอบ และการปนเปื้อนของหลักฐาน (Cross-Contamination)
- Backup Device สำหรับใช้ในการเก็บข้อมูลต่างๆ ที่จำเป็นและเกี่ยวข้องกับ Incident เช่น log file, screen capture, บันทึกการสัมภาษณ์ผู้ใช้งาน เป็นต้น
- เครื่องคอมพิวเตอร์สำหรับใช้ในการวิเคราะห์ (Analyst Laptop) เพื่อใช้ในการวิเคราะห์ Malware, ดักจับ Live Packet

- Sanitized Removable Media สำหรับใช้ในการจัดเก็บข้อมูลที่ใช้ทำ Digital Forensic ก่อนที่จะนำไปถ่ายโอนเข้าสู่ Forensic Workstation โดยเฉพาะ เพื่อป้องกันการปนเปื้อนหรือเปลี่ยนแปลงหลักฐาน (Cross-Contamination) [อ้างอิงตามNIST SP 800-88 r1 Guidelines for Media Sanitization]

- เครื่องพิมพ์เคลื่อนที่ (Portable Printer) สำหรับกรณีที่มีความจำเป็นต้องพิมพ์ข้อมูลออกจากระบบปลายทางเป็นกระดาษ

- โปรแกรมสำหรับวิเคราะห์และกู้คืนข้อมูลหลักฐานทางดิจิทัล (Digital forensic software) เช่น Hard Disk Image เป็นต้น เพื่อใช้ในการหาข้อสรุปหรือสาเหตุของ Incident

- อุปกรณ์ในการเชื่อมต่อและเก็บข้อมูลหลักฐานจากแหล่งข้อมูลทางดิจิทัลต่างๆ (Evidence gathering accessories) เช่น Computer, Network Storage, Removable Media, Mobile Device เป็นต้น

- Threat Intelligence Information ที่ให้ข้อมูลภัยคุกคามที่เป็นที่รู้จัก เพื่อเพิ่มความรวดเร็วของกระบวนการตอบสนอง ให้ทราบถึงการมีอยู่ของภัยคุกคามภายในระบบได้อย่างรวดเร็ว ประกอบด้วย

  - เครื่องมือและวิธีการที่ภัยคุกคามใช้ (Threat Agent's Tools, Tactics, Procedure) เช่น Protocol ที่เป็นเป้าหมายของการโจมตี, Malware ที่ใช้ในการโจมตี เป็นต้น

  - ช่องโหว่ที่เกี่ยวข้องกับระบบในความดูแล (Vulnerability Databases) เพื่อใช้ประกอบการวิเคราะห์ความน่าจะเป็นรวมถึงร่องรอยที่เป็นไปได้หากเกิดการโจมตีขึ้น

  - Malware Indicator of Compromise (IoC) ข้อมูลที่บ่งชี้ว่าการถูกโจมตีสำเร็จ เช่น Cryptographic Hash, commonly used port lists : Network port ต่างๆ ที่ถูกใช้โดย Malware และ Channel ปลายทางที่ระบบที่ถูกโจมตีสำเร็จจะต้องติดต่อด้วยเพื่อรับคำสั่งจากผู้โจมตีหรือส่งข้อมูลที่จารกรรมได้ออกไป เป็นต้น

- รายการทรัพย์สินสารสนเทศที่สำคัญ โดยอย่างน้อยควรประกอบด้วย Hardware, Software, Data, Network Diagram, Data Flow Diagram

- การศึกษาและเข้าใจพฤติกรรมการทำงานปกติของระบบ เครือข่าย และแอปพลิเคชั่น (Baseline) เพื่อช่วยในการสังเกตพฤติกรรมที่ผิดปกติและสามารถตรวจจับได้เร็วขึ้น โดยการตรวจสอบบันทึกเหตุการณ์ และการแจ้งเตือนด้านความมั่นคงปลอดภัย เพื่อให้มีความคุ้นเคยและจะช่วยให้การสังเกตเหตุการณ์และการแจ้งเตือนที่ผิดปกติได้เร็วและแม่นยำมากยิ่งขึ้น เช่น Network, Operating System Software Whitelist, Application เป็นต้น

- **ตัวอย่างช่องทางการสื่อสาร**

  - สื่อหลักประเภทโทรทัศน์ วิทยุ Social Media และ Website สำหรับใช้กรณีสถานการณ์ที่ประชาชนส่วนใหญ่ได้รับผลกระทบ โดยสามารถเลือกใช้ช่องทางใดช่องทางหนึ่งหรือหลายๆ ช่องทางร่วมกัน

  - อีเมล (Email) สำหรับใช้ในการติดต่อประสานงานภายในหน่วยงาน หรือกับภาคธุรกิจที่เป็นทางการ เช่น การสรุปข้อมูลการโจมตีทางไซเบอร์ที่เกิดขึ้น การนัดประชุม หรือการปฏิบัติการร่วม เป็นต้น

  - Instant Messaging สำหรับใช้ในการติดต่อสื่อสารประสานงานภายในหน่วยงานหรือกับภาคธุรกิจกรณีเร่งด่วน และสามารถมีบันทึกการสื่อสารไว้อ้างอิงภายหลัง

  - โทรศัพท์มือถือ สำหรับใช้ในการติดต่อสื่อสารประสานงานภายในหน่วยงานหรือกับภาคธุรกิจ กรณีเร่งด่วน หรือใช้ในการยืนยันเมื่อมีการส่งข้อมูลเอกสารที่เป็นทางการไปแล้วอีกครั้งหนึ่ง

๒.๑. การดำเนินการป้องกันก่อนเกิดเหตุ (Preventing Incidents) ควรดำเนินการต่อไปนี้เป็นอย่างน้อย

๒.๑.๑. **การประเมินความเสี่ยง (Risk Assessment)** บริษัทควรทำการประเมินความเสี่ยง เพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัย และควรพิจารณาข้อมูลจากกระบวนการทางธุรกิจและข้อมูลรายการทรัพย์สินประกอบการประเมินความเสี่ยง เพื่อให้ทราบถึงระดับของความเสี่ยงทางไซเบอร์ที่อาจจะเกิดต่อทรัพย์สิน โดยอย่างน้อยควรระบุเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบหรือสร้างความเสียหายต่อระบบงาน ข้อมูลสำคัญ และการดำเนินงานขององค์กร

ทั้งนี้ ควรประเมินความเสี่ยงรวมทั้งผลกระทบที่เกิดขึ้นจริงในระหว่างการเกิดเหตุ เพื่อประเมินผลกระทบและมูลค่าความเสียหายที่แท้จริง และเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามทางไซเบอร์ต่อไป

๒.๑.๒. **การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Implement Host Security Control) และการควบคุมพื้นฐานในระดับ Endpoint ที่ควรมี** รวมทั้งควรกำหนดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีมาตรฐาน รวมทั้งการปิดช่องโหว่และทำการแพตช์ระบบอย่างเหมาะสม นอกจากนี้ ควรมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น รวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของบริษัท และได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ เช่น การทำ Hardening ตั้งค่าเพื่อความมั่นคงปลอดภัย และ Update Security Patch เป็นประจำ และ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention/Host-based Intrusion Prevention & Detection System เป็นต้น

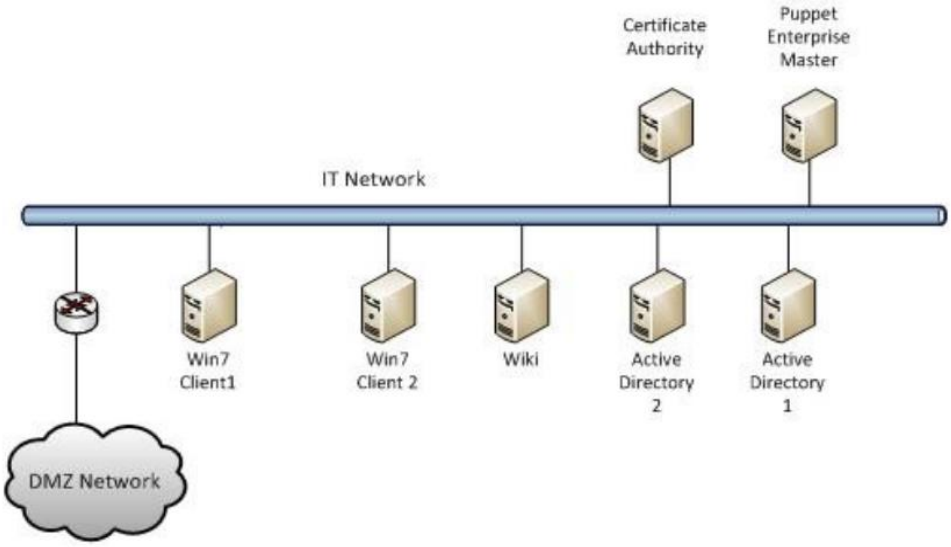
๒.๑.๓. **การรักษาความปลอดภัยของเครือข่าย (Network Security: Implement Network Security Control)** เป็นการตั้งค่าอุปกรณ์ทางเครือข่ายที่จำเป็น เช่น Router ACL, Firewall, IPDS เป็นต้น ให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาต รวมทั้งอุปกรณ์เครือข่ายทั้งหมดของบริษัทที่เชื่อมต่อกับเครือข่ายภายนอกเพื่อป้องกันและแจ้งเตือนการบุกรุก

๒.๑.๔. **การจัดให้มี User Awareness training** เพื่อให้ทุกคนในองค์กร มีความรู้ความเข้าใจ มีความระมัดระวังและเข้าใจถึงความผิดปกติที่เกิดขึ้นจากการโจมตีทางไซเบอร์ รวมทั้งเข้าใจวิธีการตอบสนองในเบื้องต้นและดำเนินการแจ้งให้หน่วยงานที่ทำหน้าที่ในการรับมือและตอบสนองรับทราบเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น

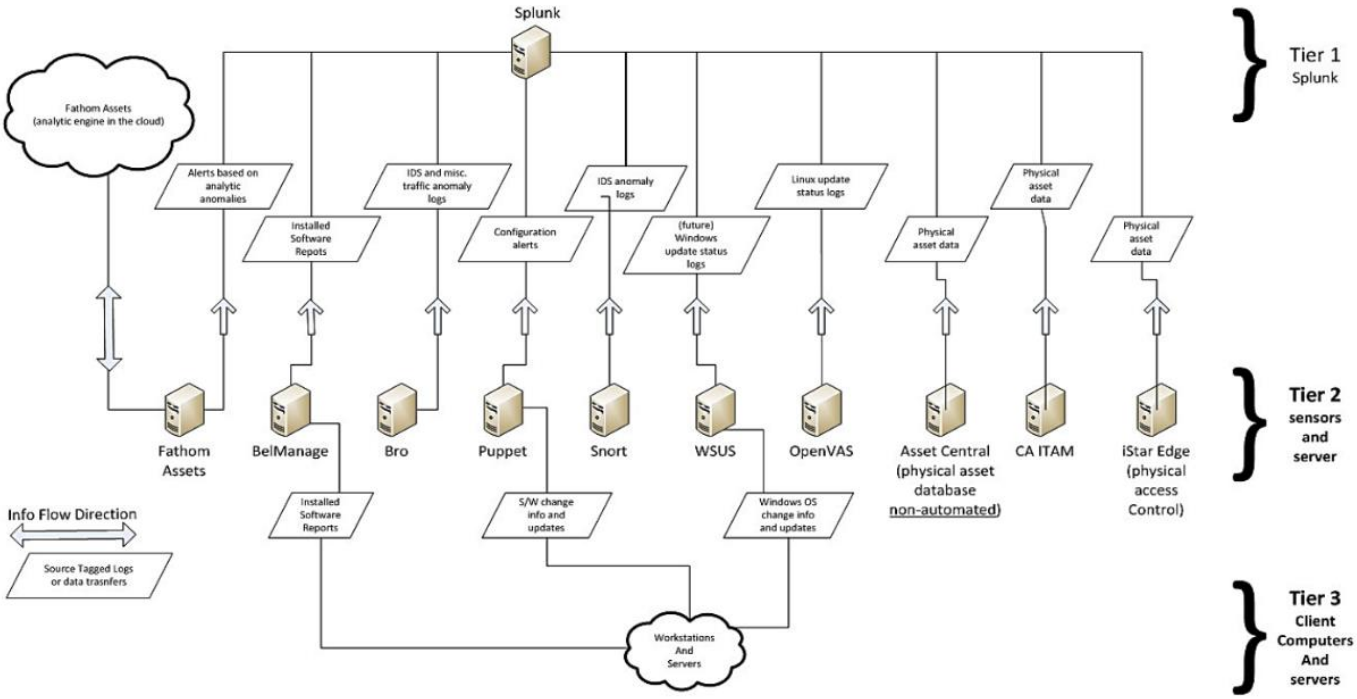
ตัวอย่างการจัดทำรายการทรัพย์สิน

Host	Product	Function	Internet Protocol Address	Operating System
Demilitarized Zone				
Bro	Bro	Network security monitor	172.16.0.20	Ubuntu 14.04
FathomSensor	RedJack Fathom	Network analysis	172.16.0.50	CentOS 7
OpenSwan	OpenSwan	Virtual Private Network (VPN)	172.16.0.67	Ubuntu 14.04
Router0	pfSense	Router/firewall	172.16.0.11 10.33.5.9	BSD pfSense appliance
Snort	Cisco/Sourcefire Snort	Intrusion Detection System	172.16.0.40	Ubuntu 14.04
Apt-cacher0	Ubuntu apt-cacher	Patch management	172.16.0.77	Ubuntu 14.04
WSUS	Microsoft WSUS	Patch management	172.16.0.45	Server 2012R2
IT Systems				
AD1	Microsoft Active Directory	Directory manager, AAA, DNS	172.16.1.20	Server 2012R2
AD2	Microsoft Active Directory	Directory manager, AAA, DNS	172.16.1.21	Server 2012R2
CA server	Microsoft Certifi-cate Authority	PKI certificate authority	172.16.1.41	Server 2012R2
Email Server	Postfix	Email server for the lab	172.16.1.50	Ubuntu 14.04
PE Master	Puppet Labs Puppet Enterprise	Configuration manage-ment	172.16.1.40	Ubuntu 14.04
Router1	pfSense	Router/firewall	172.16.0.12 172.16.1.1	BSD pfSense appliance
Ubuntu Client1	Ubuntu Desktop	Representative Linux client	DHCP	Ubuntu 14.04
Win7-Client1	Microsoft Windows7	Representative Windows client	DHCP	Windows 7 Enterprise
Win7-Client2	Microsoft Windows7	Representative Windows client	DHCP	Windows 7 Enterprise

รูปที่ ๒ ตัวอย่างรายการข้อมูล



รูปที่ ๓ ตัวอย่าง Network Diagram



รูปที่ ๔ ตัวอย่าง Data Flow Diagram

ตัวอย่างตารางทะเบียนทรัพย์สินสารสนเทศ ตามที่ระบุไว้ใน BCP Guideline ของสำนักงาน คปภ.

1. รายการทะเบียนทรัพย์สินสารสนเทศประเภทอุปกรณ์ (Hardware)								
เลขทะเบียนทรัพย์สินสารสนเทศ	ประเภทฮาร์ดแวร์	ลักษณะการใช้งาน	ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของฮาร์ดแวร์	ผู้ใช้งาน	ที่ตั้ง	วันที่เริ่มสัญญาบำรุงรักษา	หมายเหตุ
501232045	Switch	Switch NetApp Intercluster	ปานกลาง	นาย A	IT	IDC ชั้น 30 Rack A9 U40	1 มกราคม 2564	NS-OS 1.1.0.5
FXH19487	UCS Blade Server	Blade Server	สูง	นาย A	IT	ชั้น 30 Rack B1 U3 - U9	1 มกราคม 2564	UCSB-B200-M3

2. รายการทะเบียนทรัพย์สินสารสนเทศประเภทระบบ (Software)										
เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อซอฟต์แวร์	ชื่อบริษัทผู้พัฒนา	จำนวนลิขสิทธิ์	ประเภทซอฟต์แวร์	รายละเอียดซอฟต์แวร์	ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของซอฟต์แวร์	สถานที่จัดเก็บซอฟต์แวร์	วันที่ลงทะเบียนซอฟท์แวร์	เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)
VM55xx78	VMware vCenter	VMWare	1	Virtual Machine	Vmware Management	สูง	นาย B	IT Dept	1 ธันวาคม 2563	FXH19487

3. รายการทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล (Data)							
เลขทะเบียนทรัพย์สินสารสนเทศ	ประเภทของข้อมูล	รายละเอียดของสารสนเทศ	ระดับความลับ	ระดับความมั่นคงปลอดภัย (สูง/ ปานกลาง/ต่ำ)	ผู้เป็นเจ้าของสารสนเทศ	ที่จัดเก็บ (ชื่อสถานที่)	เลขทะเบียนทรัพย์สินซอฟต์แวร์ (เพื่อใช้อ้างอิง)
OIC-IT-017	Information	ข้อมูล Log ของระบบ	Confidential	สูง	IT	IDC ชั้น 10	85697604

ขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ (Detection & Analysis)

๑. ผลลัพธ์ที่สำคัญในขั้นตอนนี้ (Key Results)

๑.๑. กำหนดช่องทางที่จะใช้ในการตรวจจับความผิดปกติได้อย่างเหมาะสมกับสภาพแวดล้อมที่ดูแล โดยสามารถพิจารณาตามตัวอย่างในข้อ ๒.๑ “การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident” ของขั้นตอนที่ ๒

๑.๒. ดำเนินการวิเคราะห์ Incident ได้อย่างรวดเร็วและเหมาะสม

๒. กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities)

๒.๑. การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident

การตรวจจับ Incident จะขึ้นอยู่กับระบบที่ใช้งานอยู่ และรูปแบบของความพยายามในการโจมตี ประกอบกับกลไกต่างๆ ที่ทำการปกป้องระบบอยู่ เพราะโดยทั่วไประบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติด้วย

ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลที่บ่งบอกว่า Incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลที่บ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

การเลือกใช้อุปกรณ์ป้องกันและตรวจจับ นอกจากจะต้องพิจารณาความเหมาะสมกับระบบที่ต้องการจะป้องกันแล้ว ควรต้องมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้นๆ เป็นสำคัญ

ตัวอย่างแหล่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่าย

แหล่งข้อมูล	คำอธิบาย
ประเภท Alert	
IDPS	ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะ ทั้งในระดับเครือข่าย และ Endpoint วิธีการตรวจจับมีหลายแบบแตกต่างกันไป ระบบประเภทนี้จะมีการแจ้งเตือนเมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก
SIEM	ทำหน้าที่คล้าย IPDS แต่จะตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่นๆ เพื่อนำมาวิเคราะห์ โดยปกติ SIEM จะมีประสิทธิภาพได้ต้องมีการตั้งค่า Rule set ที่ดีโดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่ SIEM ดูแลอยู่
Anti-Malware Software	ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ปัจจุบันทำงานได้ทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งความพยายามในการโจมตีหรือการโจมตีได้สำเร็จลุล่วงแล้ว
File Integrity Monitoring	ระบบที่ทำหน้าที่สอดส่องดูแลการเปลี่ยนแปลงแก้ไขของไฟล์สำคัญๆ และจะแจ้งเตือนเมื่อมีการเปลี่ยนแปลงของไฟล์โดยไม่ได้รับอนุญาต

แหล่งข้อมูล	คำอธิบาย
Third-Party Monitoring Service	บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบของเรา โดยเฉพาะเมื่อระบบของเราถูกนำไปใช้โจมตีระบบอื่นๆ ภายนอกองค์กร ก็เป็นตัวบ่งชี้ได้ว่าระบบได้ถูกยึดครองโดยผู้ที่ไม่หวังดีและนำไปใช้ในการสร้างความเสียหาย
ประเภท Log	
Operating System and Application Log	ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยบันทึกเหตุการณ์หลากหลายประเภท สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
Network Device Log	อุปกรณ์เครือข่ายที่มีบันทึกข้อมูลที่ผ่านเข้าออกเครือข่ายก็สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้เช่นเดียวกัน ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
ข้อมูลจากแหล่งสาธารณะ	
Vulnerability and Exploit Database	ข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่ สามารถถูกใช้เป็นเครื่องบ่งชี้ภัยคุกคามได้ หากการโจมตีที่ออกมาใหม่นั้นสามารถโจมตีระบบที่เราดูแลอยู่ได้
บุคคลเป็นผู้แจ้งเตือน	
บุคคลภายในองค์กร	บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝนเพื่อช่วยสอดส่องดูแลความผิดปกติที่เกิดกับระบบเทคโนโลยีสารสนเทศได้
บุคคลภายนอกองค์กร	บุคคลภายนอก เช่น ลูกค้าก็สามารถเป็นแหล่งข้อมูลการทำงานผิดปกติของระบบได้ นอกจากนี้ยังมี CERT ต่างๆ รวมถึง White Hat Hacker

๒.๒. การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติ ควรมีความถูกต้องแม่นยำและมีประสิทธิภาพ เพื่อให้การดำเนินการในขั้นตอนต่อไปสามารถดำเนินการได้เร็วและถูกต้องมากยิ่งขึ้น

ตัวอย่างเทคนิคในการวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง มีดังต่อไปนี้

เทคนิค	คำอธิบาย
Profiling (Baselining) Networks and Systems & Understand Normal Behavior	ข้อมูลสถานะการทำงาน การตั้งค่า และการใช้งานปกติของระบบ จะทำให้ทราบได้เร็วขึ้นเมื่อมีพฤติกรรมผิดปกติเกิดขึ้นในระบบ
Log Retention Policy	Log จากอุปกรณ์ต่างๆ เช่น IPDS, Workstation, Servers, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาและป้องกันอย่างดี รวมถึงเก็บไว้เป็นระยะเวลาที่เหมาะสม ตอบโจทย์ในด้านของการตอบสนองและเป็นไปตามกฎหมายข้อบังคับ
Perform Event Correlation	การโจมตีโดยทั่วไปมักจะมีเส้นทางการเข้าถึงระบบเป้าหมายที่ผ่านอุปกรณ์ต่าง ๆ บนเครือข่าย ดังนั้นการวิเคราะห์ก็จำเป็นที่จะต้องใช้ข้อมูลจากทุกอุปกรณ์ที่คาดว่า

เทคนิค	คำอธิบาย
	จะเกี่ยวข้องร่วมกัน (Correlation) เพื่อให้เห็นถึงเส้นทางการโจมตี และสาเหตุที่แท้จริงที่ทำให้การบุกรุกประสบผลสำเร็จ
Clock Synchronization	อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอ ไม่เช่นนั้นแล้วการ Correlate Event จะทำได้ยากหรือไม่สามารถทำได้
Sniff and Analyze Network Data	ในหลาย ๆ กรณีการดักจับข้อมูลทางเครือข่ายขณะเกิดเหตุเพื่อนำมาร่วมการวิเคราะห์สามารถที่จะให้ข้อมูลเบาะแสที่สำคัญได้
Seek Assistance	เมื่อใดที่ทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ Incident เพื่อหาสาเหตุที่แท้จริงเพื่อกำจัดผู้บุรุกออกจากระบบได้ ก็สามารถใช้บริการให้คำแนะนำปรึกษาจากภายนอกตามสมควรได้ เช่น CERT ต่าง ๆ หรือบริการจากที่ปรึกษาภายนอก เป็นต้น

๒.๓. การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

ตามแนวทางที่แนะนำตาม BCP Guideline ที่กำหนดให้บริษัทมีการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ซึ่งจะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม ซึ่งการบันทึกข้อมูลอาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูล เช่น ระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์ ขั้นตอนการจัดการ และแก้ไขเหตุภัยคุกคามเพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม

ทั้งนี้ บริษัทสามารถพิจารณาประเด็นดังต่อไปนี้เพิ่มเติม นอกเหนือจากที่กำหนดไว้ใน BCP Guideline

- สถานะปัจจุบันของ Incident ต้องได้รับการอัพเดทตามจริงที่เป็นอยู่ เช่น New, In Progress, Forwarded for investigation, Resolved เป็นต้น
- สรุปเหตุการณ์ที่เกิดตั้งแต่การตรวจพบถึงการแก้ไขเสร็จเรียบร้อย
- สิ่งที่เป็นตัวบ่งชี้การมีอยู่ของ Incident เช่น การทำงานของระบบผิดไปจากเดิม มีการแสดงผลที่ผิดปกติทางหน้าจอคอมพิวเตอร์ ระดับการใช้งานทรัพยากร เช่น RAM มากขึ้นอย่างผิดสังเกต และการมีข้อความขู่กรรโชกทรัพย์ปรากฏบนหน้าจอคอมพิวเตอร์ เป็นต้น
- Incident อื่นที่อาจมีความเกี่ยวข้องกัน
- รายการกิจกรรมโดยละเอียดที่สุดที่ผู้ตอบสนองได้กระทำไปในระหว่างการรับมือ Incident
- ห่วงโซ่หลักฐาน (Chain of Custody) เพื่อคงไว้ซึ่งความถูกต้องน่าเชื่อถือของหลักฐาน
- รายการหลักฐานที่มีการจัดเก็บระหว่างการรับมือ Incident
- ความคิดเห็นจากผู้ที่ทำการรับมือ Incident
- การดำเนินการในลำดับถัดไป

ตัวอย่างฟอร์มการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ตามที่ระบุไว้ใน BCP Guideline ของสำนักงาน คปภ.

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม			
ชื่อเหตุการณ์ภัยคุกคาม		หมายเลขของเหตุการณ์ภัยคุกคาม	
วันที่บันทึกเหตุการณ์ภัยคุกคาม		หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้	
ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม		**ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม**	
ชื่อ – นามสกุล		ชื่อ – นามสกุล	
หน่วยงาน		โทรศัพท์	
โทรศัพท์	อีเมล	อีเมล	
วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม			
วันที่และเวลาพบเหตุภัยการณ์คุกคาม			
วันที่และเวลารายงานเหตุภัยคุกคาม			
รายละเอียดเหตุการณ์ภัยคุกคาม			
- สิ่งที่เกิดขึ้น - เกิดขึ้นอย่างไร - ทำไมจึงเกิดขึ้น - การประเมินทรัพย์สินสารสนเทศที่เสียหาย - ผลกระทบทางธุรกิจ - ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม			
การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้		**การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้**	
ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ		**รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม**	
สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม			

๒.๔. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของบริษัท และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด

ตัวอย่าง แนวทางการการกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้าน ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

ปัจจัยในการพิจารณา	คำอธิบาย
ผลกระทบต่อการให้บริการ (Functional Impact)	ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม โดยควรพิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที ซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบ IT ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น
ผลกระทบต่อข้อมูล (Information Impact)	ผลกระทบต่อข้อมูล ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมของบริษัทอย่างไร และส่งผลต่อข้อมูลสำคัญของบริษัท (Sensitive Information) อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น
ความสามารถในการฟื้นฟูระบบ (Recoverability)	ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศ เช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้

ตารางที่ ๑ คำอธิบายผลกระทบด้านต่างๆ

ระดับของ Functional Impact	คำนิยาม
None	ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
Low	มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้าง แต่ผลที่ได้ยังครบถ้วนสมบูรณ์
Medium	ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายในและภายนอก
High	ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

ตารางที่ ๒ ระดับของ Functional Impact

ระดับของ Information Impact	คำนิยาม
None	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
Privacy Breach	ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
Proprietary Breach	ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
Integrity Loss	ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาต

ตารางที่ ๓ ระดับของ Information Impact

ระดับของ Recoverability Effort	คำนิยาม
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจาย รวมถึงการเยียวยาผลกระทบ

ตารางที่ ๔ ระดับของ Recoverability Effort

๒.๕. การติดต่อประสานงานและแจ้งข้อมูลให้กับบุคลากรด้านอื่นๆ

ตามแนวทางที่แนะนำใน BCP Guideline ที่กำหนดให้ทีมรับมือและตอบสนองฯ ควรดำเนินการแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ ทั้งนี้ บริษัทควรมีข้อกำหนดเกี่ยวกับการแจ้งข้อมูลเหตุภัยคุกคาม ข้อมูลอะไรบ้างที่ต้องรายงาน รายงานต่อใคร และเมื่อใด โดยอย่างน้อยควรกำหนดบุคคลผู้รับรายงาน ข้อมูลที่ต้องรายงาน และเวลาที่ต้องรายงาน รวมถึงหน่วยงานต่างๆ ทั้งภายในและภายนอกที่ต้องได้รับแจ้งแล้ว ทั้งนี้ **บริษัทสามารถพิจารณาปัจจัยในเรื่องดังต่อไปนี้ประกอบการพิจารณาเพื่อกำหนดแนวทางในการติดต่อประสานงานและแจ้งข้อมูลให้กับผู้ที่เกี่ยวข้อง**

- เป็นผู้ได้รับผลกระทบจาก Incident
- เป็นผู้ที่มีหน้าที่ตัดสินใจในการดำเนินการที่เกี่ยวข้องกับ Incident
- เป็นผู้ที่มีหน้าที่รับผิดชอบกำหนดในนโยบายและแผน
- เป็นผู้ที่มีหน้าที่รับผิดชอบตามที่กฎหมายกำหนด

การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง บุคลากรหรือหน่วยงานที่ควรได้รับการแจ้งเหตุภัยคุกคาม มีดังต่อไปนี้

- ผู้บริหาร (Top Management)
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
- ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือ หัวหน้าหน่วยงานการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Head of Information Security)
- ทีมรับมือและตอบสนองต่อเหตุการณ์อื่นๆ ของบริษัท
- ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอกบริษัท (ตามความเหมาะสม)
- เจ้าของระบบงาน (System Owner)
- ฝ่ายทรัพยากรบุคคล (Human Resources)
- ฝ่ายสื่อสารองค์กร (สำหรับเหตุการณ์ที่จำเป็นต้องให้การประชาสัมพันธ์)
- ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย)
- ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team)
- ทีมรับมือและตอบสนองต่อเหตุการณ์วิกฤต (Crisis Management Team)
- หน่วยงานกำกับ (Regulators) / ทีม TI-CERT / สำนักงาน คปภ.
- หน่วยงาน CERT (Computer Emergency Response Team) เช่น Thai-CERT
- หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง (Law Enforcer)

๓. ข้อควรระวัง (Cautions)

การจัดลำดับความสำคัญของการตอบสนองต่อ Cyber Incident ควรให้ความสำคัญกับ Incident ที่มีผลต่อความอยู่รอดของธุรกิจก่อนเป็นอันดับแรก ที่ส่งผลกระทบในด้านเชื่อมั่นต่อภาพลักษณ์และชื่อเสียง

ขั้นตอนที่ ๓ : การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

๑. ผลลัพธ์ที่สำคัญในขั้นตอนนี้ (Key Results)

๑.๑. การเลือกวิธีการในการควบคุมความเสียหายที่เหมาะสม

๑.๒. การจัดเก็บและรักษาหลักฐานทางดิจิทัล

๑.๓. การกู้คืนระบบให้กลับมาทำงานปกติ

๒. กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities)

๒.๑. พิจารณาวิธีการในการควบคุมความเสียหาย

การควบคุมความเสียหายมีความจำเป็นอย่างยิ่งที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้าง สร้างผลกระทบต่อทรัพยากรในการดำเนินธุรกิจอื่นๆ และยังเป็นการเปิดพื้นที่ เพิ่มระยะเวลาให้ทีมที่รับมือ Incident มีเวลาในการคิดหาสาเหตุ และวิธีการแก้ปัญหาที่ถาวรได้

ข้อสำคัญของการควบคุมความเสียหาย คือ การตัดสินใจเลือกใช้วิธีการที่เหมาะสม โดยวิธีการทั่วไปมีดังต่อไปนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใดๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole / Sandbox / Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหาย จะขึ้นอยู่กับลักษณะสถานการณ์ที่บริษัทกำลังเผชิญประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย โดยบริษัทสามารถพิจารณาเกณฑ์เพื่อกำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหายได้ตามที่กำหนดใน “แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP) ในแนวปฏิบัติเรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓”

๒.๒. การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัล บริษัทสามารถดำเนินการโดยพิจารณาตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในชั้นศาล
- เมื่อหลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody)

รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๑) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น

๒) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

๓) สถานที่จัดเก็บหลักฐาน

ทั้งนี้ บริษัทสามารถศึกษาเพิ่มเติมได้ที่เอกสาร National Institute of Standards and Technology (NIST) Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response

๒.๓. การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

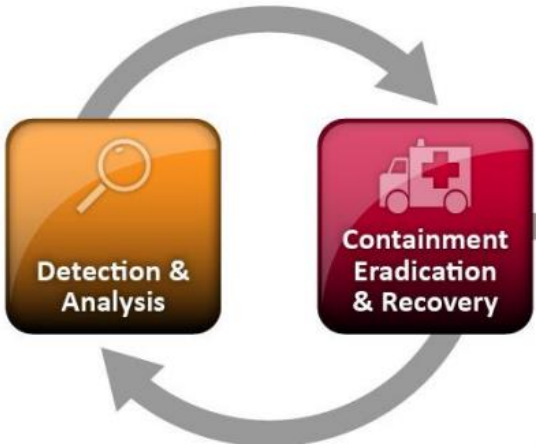
หากพิจารณาแผนภาพ Incident Response Life Cycle จะพบว่า เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้ว ข้อมูลทั้งหมดจะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ ๒ เรื่อง การตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย

ตัวอย่างของการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ เช่น

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล IoC ในการสแกนหา Malware หรือร่องรอยอื่นๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว บริษัทจึงจะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่างๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage



รูปที่ ๕ Incident Response Life Cycle Revisit

๓. ข้อควรระวัง (Cautions)

๓.๑. การควบคุมความเสียหายโดยการ Redirect ผู้บุกรุกไปยัง Sandbox/Honeypot โดยที่ไม่ได้ตัดการเชื่อมต่อของผู้บุกรุกออกไปในทันที แต่ปล่อยให้ทำการโจมตีต่อไปในระบบ Sandbox เพื่อศึกษาเทคนิค พฤติกรรม พร้อมทั้งเก็บไว้เป็นหลักฐานไปก่อนนั้น ควรทำการปรึกษาขอความเห็นจากทีมกฎหมายก่อนรวมทั้งไม่ควรใช้วิธีการนี้กับอุปกรณ์อื่นๆ นอกเหนือจากระบบที่เป็น Sandbox/Honeypot เนื่องจากการที่ปล่อยให้ผู้บุกรุกอยู่ในระบบต่อไปหลังจากทราบว่าเป็นการโจมตีแล้ว และเกิดความเสียหายอื่นๆ ตามมาภายหลังโดยเฉพาะกับบุคคลที่สาม องค์กรอาจมีส่วนที่จะต้องรับผิดชอบเพิ่มเติมในทางกฎหมายโดยไม่จำเป็น

๓.๒. การนำหลักฐานดิจิทัลออกมาวิเคราะห์ควรกระทำบนสำเนา (Digital Copy) ของหลักฐานชิ้นนั้น และการจัดทำสำเนาหลักฐานควรกระทำโดยมีเครื่องมือประเภท Write Blocker เพื่อป้องกันการเปลี่ยนแปลงต่อหลักฐานต้นฉบับ สุดท้ายก่อนนำมาวิเคราะห์ให้ทำการเปรียบเทียบ Cryptographic Hash ของหลักฐานทั้งสองชิ้นให้ตรงกันก่อน

๓.๓. ขั้นตอนการ Recover Operating System หรือ Application หาก Master Image มีช่องโหว่ควรทำการแก้ไขและ Update Master Image ก่อนที่จะมีการ Restore

๓.๔. เมื่อระบบเข้าสู่สภาวะปกติแล้วต้องมีการ Monitor เหตุการณ์ว่ายังเกิดการโจมตีหรือสิ่งผิดปกติอยู่อีกหรือไม่อย่างต่อเนื่อง เช่น ๔๘ ชั่วโมง เป็นต้น

ขั้นตอนที่ ๔ : การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)

๑. ผลลัพธ์ที่สำคัญในขั้นตอนนี้ (Key Results)

๑.๑. การปรับปรุงพัฒนาแผนการรับมือหรือความพร้อมด้านอื่น ๆ จากข้อมูลที่ได้จากการรับมือ

๒. กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities)

การเรียนรู้เพื่อปรับปรุงการดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity) ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลจาก Issue Tracking System เพื่อประกอบการพิจารณาปรับปรุงและพัฒนา

ตัวอย่างประเด็นคำถาม ที่บริษัทสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยบริษัทสามารถพิจารณา**เพิ่มเติมได้จากตัวอย่างที่ระบุไว้ใน BCP Guideline เช่น**

- การดำเนินงานเสร็จสิ้นตามกำหนด และได้ผลลัพธ์ตามที่ระบุไว้หรือไม่
- ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ได้ดำเนินการครบถ้วนถูกต้องตามที่กำหนดหรือไม่
- การใช้ทรัพยากรเพื่อรับมือและตอบสนองเป็นไปตามที่วางแผนไว้หรือไม่ มีส่วนใดบ้างที่ต้องได้รับการจัดสรรเพิ่มเติม
- ข้อมูลที่จำเป็นต้องใช้ในการตอบสนอง มีข้อมูลจากส่วนใดบ้างที่ทีมรับมือฯ คิดว่ายังได้รับช้าไป
- การปฏิบัติงานในขั้นตอนใดที่ทำให้การกู้คืนข้อมูลหรือระบบช้าลง
- การติดต่อสื่อสารระหว่างการรับมือและตอบสนองต่อเหตุการณ์ทั้งภายในและภายนอกองค์กร มีประเด็นปัญหาอุปสรรคอะไรบ้าง ที่ต้องได้รับการทบทวนเพื่อนำไปพัฒนาและปรับปรุงต่อไป
- เหตุการณ์ภัยคุกคามลักษณะนี้ มีแนวทางในการป้องกันไม่ให้เกิดซ้ำในอนาคตได้อย่างไรบ้าง
- สัญญาณตรวจจับทั้ง Precursor และ Indicator ใดบ้างที่ควรเพิ่มเติมเพื่อเพิ่มประสิทธิภาพและความเร็วในการรับมือและตอบสนอง
- การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น มีประเด็นปัญหาหรืออุปสรรคอะไรบ้าง และสามารถปรับปรุงให้ดีขึ้นอย่างไร

๓. ข้อควรระวัง (Cautions)

การรับมือ Incident ได้สำเร็จมากในช่วงเวลาหนึ่ง อาจไม่ได้เป็นการบ่งชี้ว่ามีความพร้อมในการรับมือได้ดีเสมอไป เพราะจากข้อเท็จจริงที่ว่ามี Incident เกิดขึ้นได้จำนวนมากเป็นตัวบ่งชี้การป้องกันที่หละหลวมหรือไร้ประสิทธิผล และไม่ได้รับการปรับปรุงเลยแม้จะผ่านการรับมือมาหลายครั้งแล้วก็ตาม

การดูแลรักษาหลักฐานทางดิจิทัล (Digital Evidence Handling Guide)

หลักฐานทางดิจิทัล จะมีความอ่อนไหวต่อความเปลี่ยนแปลงสูง ดังนั้น จึงจำเป็นต้องระมัดระวังตั้งแต่ขั้นตอนการจัดเก็บจนถึงการวิเคราะห์และนำเสนอผลการวิเคราะห์ เพื่อให้มั่นใจได้ว่า ข้อเท็จจริงที่ได้จากการวิเคราะห์มีความถูกต้องแม่นยำ รวมถึงการที่หลักฐานจะสามารถถูกนำไปใช้ได้ในชั้นศาลหากมีความจำเป็น ทั้งนี้ หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมี ๕ ข้อดังนี้

1. Assessment	การประเมินเพื่อหาจุดที่ต้องมีดำเนินการจัดเก็บหลักฐานของ Incident ที่เรากำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น เพื่อดำเนินการจัดเตรียมเครื่องมือและวิธีการที่เหมาะสมในการเก็บข้อมูลหลักฐาน
2. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ ๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐาน ด้วยการใช้งาน Hardware Write Blocker ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น ๓. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด ๔. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
3. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256
4. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident
5. Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

ตัวอย่างการประยุกต์ใช้ขั้นตอนการรับมือ

กรณีตัวอย่างที่ ๑ : Ransomware และ Data Leakage จากภายในองค์กร

Preparation		
Objective	๑. มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ ๒. มีกระบวนการ และกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นทำหน้าที่ในการตรวจจับความพยายามในการบุกรุกได้อีกด้วย	
Activity	Description	Stakeholders
จัดเตรียมทรัพยากร	อ้างอิงข้อ ๒.๑ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)”	CEO / CFO / CIO / CISO / CRO / CCO
ดำเนินการป้องกันก่อนเกิดเหตุ	อ้างอิงข้อ ๒.๒ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)” สำหรับการรับมือ Ransomware ในปัจจุบันให้มุ่งเน้นไปที่เรื่องของการ Backup ระบบ และข้อมูลการจัดการเรื่องของข้อมูลที่รั่วไหลโดยเฉพาะเรื่องของการ Take Down แหล่งที่รั่วไหลของข้อมูล การมีมาตรการในการเยียวยาผู้ที่ได้รับผลกระทบจากการรั่วไหลของข้อมูล รวมทั้งควรมีความพร้อมในการดำเนินการ Personal Information usage Monitoring สำหรับบุคคลที่ข้อมูลรั่วไหล ว่าจะมีการถูกนำไปใช้ที่ใดได้บ้าง และกิจกรรมใดบ้าง	CISO / CRO / IRT
Detection & Analysis		
Objective	๑. รับแจ้งเหตุการณ์การโจมตี ๒. การระบุความเสียหายเบื้องต้น ๓. การระบุสาเหตุที่การโจมตีสำเร็จ ๔. การระบุความสามารถของผู้บุกรุกและเครื่องมือที่ใช้รวมถึง Malware	
Activity	Description	Stakeholders
รับแจ้งเหตุ	ส่วนใหญ่เมื่อการโจมตีประเภท Ransomware เกิดขึ้นจะรับทราบได้จากการที่ผู้ใช้งานระบบเป็นผู้แจ้ง	Users / SOC / IRT
วิเคราะห์การโจมตีและขอบเขตเสียหาย	ผลกระทบเบื้องต้นสามารถสอบถามได้จากผู้ใช้งานระบบ รวมถึงกิจกรรมก่อนหน้าที่กระทำไป และเป็นผลให้การโจมตีสำเร็จ รวมทั้ง ใช้ข้อมูลจากการสอบถามเป็นข้อมูลเบื้องต้นในการจัดการภัยคุกคามและค้นหาระบบอื่นๆ ที่อาจจะได้รับผลกระทบในลักษณะเดียวกัน	IRT
จัดเก็บหลักฐานทางดิจิทัลที่จำเป็นรวมถึงตัวอย่าง (Specimen) Malware	การโจมตีที่สำเร็จ หมายถึง การโจมตีที่สามารถผ่านกลไกการป้องกันมาได้ ซึ่งเป็นการโจมตีที่มีความซับซ้อน ซึ่งการจะทราบถึงเทคนิควิธีการโจมตี ลักษณะที่ใช้ และผลกระทบที่เป็นไปได้ทั้งหมด ต้องอาศัยการเก็บข้อมูลและการวิเคราะห์ชั้นสูง การเก็บข้อมูลจากจุดต่างๆ ของเครื่องคอมพิวเตอร์ที่โดนโจมตีและอุปกรณ์เครือข่ายที่ทำงานร่วมกันจึงเป็นสิ่งจำเป็น โดยที่ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้า ประกอบด้วย	Users / IRT / System Admins

	- RAM - Network Connection - Running Processes - Opened Files - Swap Memory - Hard Disk Image - System Log - Network Log - External Media ข้อมูลที่อ่อนไหวต่อการสูญเสียกระแสไฟฟ้า คือ ข้อมูลที่จะหายไปหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM เป็นต้น ดังนั้นเพื่อให้หลักฐานที่กล่าวมาคงอยู่ครบถ้วน ในบางกรณี การเก็บข้อมูลจึงต้องกระทำอย่างรวดเร็ว โดยผู้เชี่ยวชาญ และก่อนที่จะมีการปิดเครื่องคอมพิวเตอร์ และหากการตอบสนองเกิดขึ้นเร็วพอ โอกาสที่จะได้ตัวอย่างของ Malware ที่เป็น Ransomware มาวิเคราะห์จะมีโอกาสสูงขึ้น การดำเนินการทั้งหมดจะต้องถูกบันทึกอย่างละเอียดเพื่อการอ้างอิงถึงในภายหลังโดยเฉพาะการขึ้นสู่ชั้นศาล (หากจำเป็น)	
วิเคราะห์ข้อมูลหลักฐานทางดิจิทัลเพื่อหาข้อสรุปจากการโจมตีและความเสียหายที่เกิดจาก Malware	ข้อมูลจากขั้นตอนก่อนหน้า จะต้องถูกนำมาหาข้อสรุปให้ได้ ๓ เรื่อง ดังต่อไปนี้ ๑. สาเหตุที่การโจมตีประสบผลสำเร็จ เพื่อการแก้ไขที่ตรงจุด ซึ่งต้องวิเคราะห์จากข้อมูลการสัมภาษณ์ และข้อมูลที่จัดเก็บได้ในขั้นตอนก่อนหน้า โดยเฉพาะการทำ Data Correlation และ Timeline Analysis ๒. โอกาสและรูปแบบของผลกระทบที่อาจจะขยายวงกว้างออกไปได้ โดยเฉพาะความสามารถของภัยคุกคามและ Malware ที่ใช้งาน เพื่อที่จะได้ค้นหาและหยุดการแพร่กระจายของภัยคุกคาม ซึ่งต้องพิจารณาจากข้อมูลที่จัดเก็บได้ในขั้นตอนก่อนหน้าเช่นเดียวกัน ที่ได้จากการทำ Malware Analysis ๓. การจัดทำ Indicator of Compromise (IoC) จากผลการวิเคราะห์ที่ได้เพื่อใช้ในการ Scan ระบบอื่นๆ ในเครือข่ายเดียวกัน และ/หรือ เครือข่ายใกล้เคียง เพื่อระบุขอบเขตของการแพร่กระจายของ Malware และภัยคุกคาม *** ขั้นตอนการวิเคราะห์อาจจะต้องมีการทำซ้ำ ในกรณีพบข้อมูลใหม่ เช่น พบ Malware อีกประเภทหนึ่งในระบบอื่นที่ไม่เหมือนกับระบบที่โดนโจมตีในครั้งแรก	IRT
ขยายผลการวิเคราะห์ความเสียหายที่เกิดจากข้อมูลรั่วไหล	เมื่อทราบว่ามีข้อมูลรั่วไหล ต้องทำการเตรียมความพร้อมและตรวจสอบความเป็นไปได้ของข้อมูลที่รั่วไหลว่าสามารถไปปรากฏอยู่ในแหล่งใดบ้าง โดยสามารถพิจารณาจากระบบที่ได้รับผลกระทบ	IRT / CMT / System Admins
ติดต่อประสานงานกับหน่วยงานภายในและภายนอก	ข้อมูลที่ได้จากการวิเคราะห์จำเป็นที่จะต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้อง โดยขึ้นอยู่กับเหตุการณ์และความจำเป็น โดยในกรณีของ Ransomware และ	IRT / CMT / Regulators / Customers /

	Data Leakage จากภายในองค์กร ควรมีหน่วยงานที่ต้องติดต่อสื่อสาร อย่างน้อยดังต่อไปนี้ ๑. การแจ้งผลการวิเคราะห์ให้กับทีมผู้ดูแลระบบ เพื่อทำการแก้ไขจุดอ่อนและความเสียหายที่เกิดขึ้นกับระบบ ๒. กรณีระบบไม่สามารถให้บริการตามปกติได้ ต้องติดต่อประสานงานกับทีม BCP ซึ่งอาจเป็นการติดต่อโดยตรง หรือผ่าน Crisis Management Team ได้ ทั้งนี้จะขึ้นอยู่กับโครงสร้างขององค์กร ๓. การแจ้งหน่วยงานกำกับดูแลตามเกณฑ์ที่กำหนด ๔. การแจ้งเจ้าของข้อมูลที่รั่วไหล ตามเงื่อนไขของกฎหมายที่เกี่ยวข้อง หรือตามความเหมาะสมและความจำเป็น	Employees /
Containment, Eradication & Recovery		
Objective	๑. การค้นหา กำจัด และควบคุมการแพร่กระจายของ Malware ๒. การค้นหาและควบคุมการรั่วไหลของข้อมูล ๓. การกู้คืนระบบให้กลับมาทำงานปกติ	
Activity	Description	Stakeholders
นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัดภัยคุกคามออกจากระบบ	ขั้นตอนที่สามารถดำเนินการควบคู่กับการวิเคราะห์ข้อมูล คือ การจำกัดความเสียหายเบื้องต้น ซึ่งปกติจะดำเนินการตัดการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่โดนโจมตีออกจากเครือข่าย และ/หรือ ทำการปิดการทำงานของอุปกรณ์ลงโดยวิธี Shutdown หรือถอดสายไฟโดยทันที ทั้งนี้ วิธีที่เลือกใช้ควรคำนึงถึงความเสียหายที่จะเกิดกับข้อมูลหลักฐานทางดิจิทัลเสมอ และควรมีการเก็บข้อมูลออกจากอุปกรณ์นั้นๆ ด้วยวิธีที่ถูกต้องก่อนที่จะมีการปิดการทำงาน ผลการวิเคราะห์ข้อมูลหลักฐานทางดิจิทัลจะทำให้ได้ข้อสรุปของการโจมตี ตั้งแต่ช่องโหว่ที่ใช้ ความเสียหายที่เกิดขึ้น และร่องรอยที่เกี่ยวข้อง (เช่น การเข้าถึง/เปลี่ยนแปลง File, Registry, Networking Resource, Network Storage เป็นต้น) ซึ่งทั้งหมดนี้สามารถใช้ในการแก้ไข Incident ได้ นอกจากนี้ การ Scan เพื่อค้นหา Indicator of Compromise (IoC) เป็นหนึ่งวิธีที่ช่วยให้การค้นหา และกำจัดภัยคุกคามสามารถดำเนินการได้เร็วขึ้น	IRT / System Admins
เรียกใช้งาน BCP หากมีความจำเป็น	ในระหว่างการรับมือและตอบสนองภัยคุกคาม หากความเสียหายที่เกิดขึ้น อยู่ในระดับที่ทำให้ระบบหลักไม่สามารถให้บริการได้ บริษัทต้องดำเนินการ Activate Disaster Recovery Site/System ตามที่กำหนดใน Business Continuity Plan	IRT / CMT / BCT / System Admins
ควบคุมและเยียวยาความเสียหายจากการรั่วไหลของข้อมูล	การรั่วไหลของข้อมูลถึงแม้จะไม่สามารถถูกแก้ไขได้อย่างสิ้นเชิง แต่ควรมีการตอบสนองที่สำคัญเพื่อช่วยบรรเทาความเสียหาย และลดหรือ กำจัดผลกระทบจากการรั่วไหลนั้นได้ คือ การระบุจุดที่ข้อมูลรั่วไหลถูกเปิดเผย เช่น Website, Bit torrent เป็นต้น และควรมีขั้นตอนหรือแนวทางในการดำเนินการ Take Down แหล่งข้อมูลเหล่านั้นเท่าที่ทำได้ และควรมีมาตรการเยียวยาเจ้าของข้อมูลและผู้ที่ได้รับผลกระทบตามที่กฎหมายกำหนด	IRT / CMT / Regulators

	นอกจากนี้ ควรร่วมมือกับหน่วยงานที่เกี่ยวข้อง เพื่อจัดทำ Information Marking และ Personal Information usage Monitoring เพื่อให้รู้ได้ทันทีเมื่อข้อมูลชุดที่รั่วไหลถูกนำไปใช้งาน (คล้ายคลึงกับการทำ Credit Monitoring ของข้อมูลทางการเงินที่เกิดการรั่วไหล)	
กู้คืนระบบ และ ข้อมูลหากมีความเสียหาย	เมื่อแก้ไขและกำจัดภัยคุกคามออกจากระบบได้แล้ว หากจำเป็นต้องมีการกู้คืนระบบ และ/หรือ ข้อมูลที่ได้รับความเสียหายกลับมาจาก Backup System Image และ Backup Data และควรระมัดระวังช่องโหว่หรือจุดอ่อนใดที่ปรากฏอยู่ใน Backup System Image ซึ่งหากตรวจพบ ควรดำเนินการแก้ไขก่อนนำมาใช้งาน	IRT / System Admins
สอดส่องดูแลความผิดปกติอย่างต่อเนื่อง	การสอดส่องดูแลความผิดปกติ ต้องเริ่มตั้งแต่เมื่อมีการนำอุปกรณ์ที่โดนโจมตีออกจากเครือข่าย จนถึงการกู้คืนระบบเรียบร้อยแล้ว รวมทั้งหลังจากกลับมาปฏิบัติงานตามปกติอีกสักระยะหนึ่ง โดยการกำหนดระยะเวลาจะขึ้นอยู่กับแต่ละองค์กรซึ่งอย่างน้อยไม่ควรต่ำกว่า ๔๘ ชั่วโมง ทั้งนี้ หากพบเจอความผิดปกติให้กลับไปดำเนินการในขั้นตอน Detection & Analysis อีกครั้ง	IRT / CMT
Post-Incident Activity		
Objective	การปรับปรุงพัฒนาแผนการรับมือหรือความพร้อมด้านอื่นๆ จากข้อมูลที่ได้จากการรับมือ	
Activity	Description	Stakeholders
การเรียนรู้เพื่อปรับปรุง	อ้างอิงข้อ ๒.๑ ใน “ขั้นตอนที่ ๔: การปฏิบัติภายหลังการตอบสนองเสร็จสิ้น (Post-Incident Activity)”	ทุกคนที่มีส่วนร่วมในขั้นตอนการตอบสนองทั้งภายนอกและภายใน

กรณีตัวอย่างที่ ๒ : Data Leakage จาก Third-Party ที่ให้บริการ

Preparation		
Objective	๑. มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ ๒. มีกระบวนการ และกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นทำหน้าที่ในการตรวจจับความพยายามในการบุกรุกได้อีกด้วย	
Activity	Description	Stakeholders
จัดเตรียมทรัพยากร	อ้างอิงข้อ ๒.๑ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)”	CEO / CFO / CIO / CISO / CRO / CCO
ดำเนินการป้องกันก่อนเกิดเหตุ	อ้างอิงข้อ ๒.๒ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)” ๑. สำหรับการเตรียมพร้อมรับมือ Data Leakage จาก Third-Party ให้มุ่งเน้นไปที่เรื่องของ - กระบวนการคัดเลือก Third-Party (Selection) - ความสามารถในการให้บริการตามกำหนด	CISO / CRO / IRT / Third-Party

	- ความสามารถในการดำเนินการตาม Security Policy ขององค์กร ๒. การดำเนินงานระหว่างผู้ให้บริการกับบริษัท (Orientation & Integration) ควรแบ่งหน้าที่ความรับผิดชอบในการดำเนินการตามนโยบาย Security Policy ให้ชัดเจน อย่างน้อยในเรื่องดังต่อไปนี้ - กำหนดขั้นตอนการดำเนินงานในแต่ละเรื่อง - มีการอบรมและฝึกฝนร่วมกันอย่างสม่ำเสมอ - มีกระบวนการตรวจสอบ และต้องกำหนดสิทธิในการตรวจสอบสัญญาการให้บริการ มีการตรวจสอบด้วยมาตรฐานระดับเดียวกับองค์กร - มีการติดตามและปรับปรุงอย่างสม่ำเสมอ - มีกระบวนการยกเลิกการใช้บริการ - สามารถอำนวยความสะดวกเมื่อต้องมีการเปลี่ยนแปลงผู้ให้บริการ - ข้อกำหนดในการทำลายข้อมูลสำคัญออกจากระบบ	
Detection & Analysis		
Objective	๑. รับแจ้งเหตุการณ์การโจมตี ๒. การระบุความเสียหายเบื้องต้น ๓. การระบุสาเหตุที่การโจมตีสำเร็จ ๔. การระบุความสามารถของผู้บุกรุกและเครื่องมือที่ใช้รวมถึง Malware	
Activity	Description	Stakeholders
รับแจ้งเหตุ	เมื่อมีการรั่วไหลของข้อมูลเกิดขึ้น Third-Party จะต้องแจ้งให้กับองค์กรทราบตามเงื่อนไขและวิธีการที่ได้ชี้แจงและฝึกฝนไว้ และต้องสอดคล้องกับ Security Policy ขององค์กรทั้งหมด	Third-Party / SOC / IRT
วิเคราะห์การโจมตีและความขอบเขตเสียหาย	๑. IRT ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ข้อมูลความเสียหายเบื้องต้นสำหรับการพิจารณามาตรการในส่วนที่องค์กรเองจะต้องดำเนินการ ๒. การรายงานความคืบหน้าและผลลัพธ์ควรกระทำเป็นระยะ และมีข้อมูลชัดเจน ๓. ทีม IRT อาจจะพิจารณาให้ความช่วยเหลือได้ ตามที่กำหนดไว้ตอนเริ่มสัญญา หรือ ตามสถานการณ์	IRT / Third-Party
จัดเก็บหลักฐานทางดิจิทัลที่จำเป็นรวมถึงตัวอย่าง (Specimen) Malware	ทีม IRT ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ผลลัพธ์เช่นเดียวกับ ภาคผนวก จ. ขั้นตอน “Detection & Analysis” ส่วน Activity “จัดเก็บหลักฐานทางดิจิทัลที่จำเป็นรวมถึงตัวอย่าง (Specimen) Malware”	Third-Party / IRT
วิเคราะห์ข้อมูลหลักฐานทางดิจิทัลเพื่อหาข้อสรุปจากการโจมตีและความเสียหายที่เกิดจาก Malware	ทีม IRT ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ ผลลัพธ์เช่นเดียวกับภาคผนวก จ. ขั้นตอน “Detection & Analysis” ส่วน Activity “วิเคราะห์ข้อมูลหลักฐานทางดิจิทัลเพื่อหาข้อสรุปจากการโจมตีและความเสียหายที่เกิดจาก Malware”	IRT / Third-Party

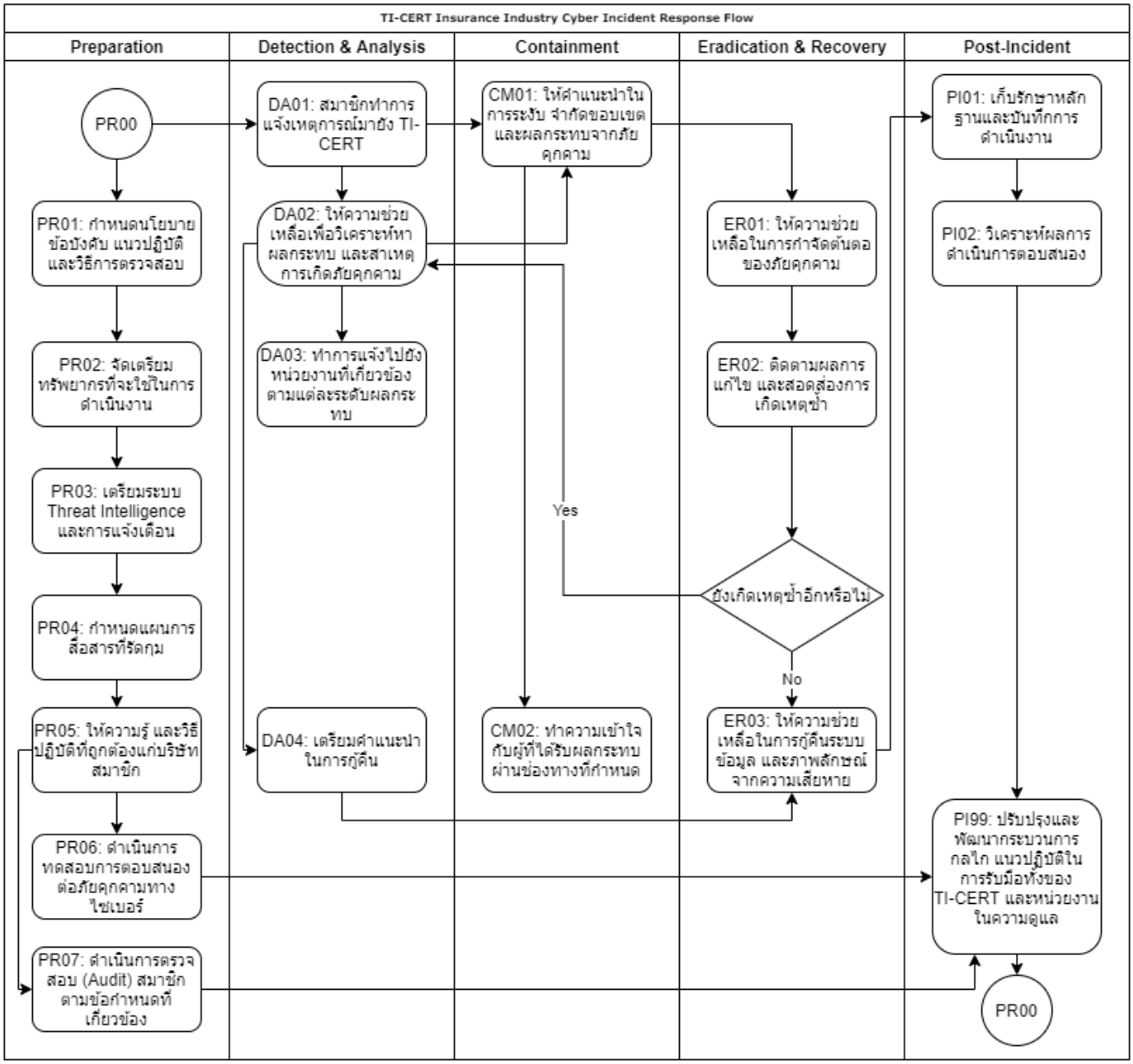
ขยายผลการวิเคราะห์ความเสียหายที่เกิดจากข้อมูลรั่วไหล	ต้องได้ข้อมูลการรั่วไหลที่ชัดเจนจากผู้ให้บริการ เพื่อให้มีความพร้อมในการสอดส่องเสาะหาข้อมูลที่รั่วไหลว่าไปปรากฏอยู่ในที่ใดบ้าง	IRT / CMT / Third-Party
ติดต่อประสานงานกับหน่วยงานภายในและภายนอก	ข้อมูลที่ได้จากการวิเคราะห์จำเป็นที่จะต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้องต่างๆ ขึ้นอยู่กับเหตุการณ์และความจำเป็น ในกรณี Data Leakage ขององค์กรมีหน่วยงานที่ต้องติดต่อสื่อสาร ดังนี้เป็นอย่างน้อย ๑. การแจ้งผลการวิเคราะห์ให้กับทีมผู้ดูแลระบบ เพื่อทำการแก้ไขจุดอ่อนและความเสียหายที่เกิดขึ้นกับระบบ ๒. การแจ้งหน่วยงานกำกับดูแลตามเกณฑ์ที่กำหนด ๓. การแจ้งเจ้าของข้อมูลที่รั่วไหล ตามเงื่อนไขของกฎหมายที่เกี่ยวข้อง หรือตามความเหมาะสมและความจำเป็น	IRT / CMT / Regulators / Customers / Employees
Containment, Eradication & Recovery		
Objective	๑. การค้นหา กำจัด และควบคุมการแพร่กระจายของ Malware ๒. การค้นหาและควบคุมการรั่วไหลของข้อมูล ๓. การกู้คืนระบบให้กลับมาทำงานปกติ	
Activity	Description	Stakeholders
นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัดภัยคุกคามออกจากระบบ	IRT ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ผลลัพธ์เช่นเดียวกับภาคผนวก จ. ขั้นตอน “Containment, Eradication & Recovery” ส่วน Activity “นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัดภัยคุกคามออกจากระบบ”	IRT / Third-Party
ควบคุมและเยียวยาความเสียหายจากการรั่วไหลของข้อมูล	การรั่วไหลของข้อมูลถึงแม้จะไม่สามารถถูกแก้ไขได้อย่างสิ้นเชิง แต่ควรมีการตอบสนองที่สำคัญเพื่อช่วยบรรเทาความเสียหาย และลดหรือกำจัดผลกระทบจากการรั่วไหลนั้นได้ คือ การระบุจุดที่ข้อมูลรั่วไหลถูกเปิดเผย เช่น Website, Bit torrent เป็นต้น และควรมีขั้นตอนหรือแนวทางในการดำเนินการ Take Down แหล่งข้อมูลเหล่านั้นเท่าที่ทำได้ และควรมีมาตรการเยียวยาเจ้าของข้อมูลและผู้ที่ได้รับผลกระทบตามที่กฎหมายกำหนด นอกจากนี้ ควรร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อจัดทำ Information Marking และ Personal Information usage Monitoring เพื่อให้รู้ได้ทันทีเมื่อข้อมูลชุดที่รั่วไหลถูกนำไปใช้งาน (คล้ายคลึงกับการทำ Credit Monitoring ของข้อมูลทางการเงินที่เกิดการรั่วไหล)	IRT / CMT / Regulators
สอดส่องดูแลความผิดปกติอย่างต่อเนื่อง	การสอดส่องดูแลความผิดปกติ ต้องเริ่มตั้งแต่เมื่อมีการนำอุปกรณ์ที่โดนโจมตีออกจากเครือข่าย จนถึงการกู้คืนระบบเรียบร้อยแล้ว รวมทั้งหลังจากกลับมาปฏิบัติงานตามปกติอีกสักระยะหนึ่ง โดยการกำหนดระยะเวลาจะขึ้นอยู่กับแต่ละองค์กรซึ่งอย่างน้อยไม่ควรต่ำกว่า ๔๘ ชั่วโมง ทั้งนี้ หากพบเจอความผิดปกติให้กลับไปดำเนินการในขั้นตอน Detection & Analysis อีกครั้ง	IRT / CMT / Third-Party

Post-Incident Activity		
Objective	การปรับปรุงพัฒนาแผนการรับมือหรือความพร้อมด้านอื่น ๆ จากข้อมูลที่ได้จากการรับมือ	
Activity	Description	Stakeholders
การเรียนรู้เพื่อปรับปรุง	อ้างอิงข้อ ๒.๑ ใน “ขั้นตอนที่ ๔: การปฏิบัติภายหลังการตอบสนองเสร็จสิ้น (Post-Incident Activity)”	ทุกคนที่มีส่วนร่วมในขั้นตอนการตอบสนองทั้งภายนอกและภายใน

ภาคผนวก ก. เอกสารที่เกี่ยวข้อง

ลำดับที่	ชื่อเอกสาร
๑	แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP) ในแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓
๒	National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide
๓	National Institute of Standards and Technology (NIST) Special Publication 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
๔	National Institute of Standards and Technology (NIST) Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response

ภาคผนวก ข. ตัวอย่าง Incident Response Flow ของ TI-CERT ที่ปรับใช้วิธีการใน Handbook ฉบับนี้



ภาคผนวก ค. ตัวอย่างแบบฟอร์ม Chain of Custody

EVIDENCE / PROPERTY CHAIN OF CUSTODY			
REFERENCE NO.	DESCRIPTION		
ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES (If physical device, include manufacturer, model, and serial number)	
Date/ Time	From	To	PURPOSE OF CHANGE OF CUSTODY
	Name Organization Signature	Name Organization Signature	
Date/ Time	From	To	PURPOSE OF CHANGE OF CUSTODY
	Name Organization Signature	Name Organization Signature	
Date/ Time	From	To	PURPOSE OF CHANGE OF CUSTODY
	Name Organization Signature	Name Organization Signature	

ที่มา : https://www.sans.org/media/score/incident-forms/ChainOfCustody.pdf

ภาคผนวก ง. ตัวอย่าง Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

ที่มา: Incident Handling Checklist (NIST 800-61 r2)

คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)