แผนรับมือเหตุภัยคุกคามทางไซเบอร์

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์

๒. วัตถุประสงค์

๒.๑ เพื่อสร้างความเชื่อมั่นให้ผู้ใช้งานระบบเครือข่าย สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ได้รับการปกป้องต่อภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ

๒.๒ เพื่อกำหนดมาตรการ นโยบาย และกลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการรับมือในภาวะฉุกเฉินเพื่อแก้ไขปัญหา

๒.๓ เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงานภายในสถาบัน ที่เกี่ยวข้องในการปรับปรุงพัฒนาระบบสารสนเทศ และการให้ความรู้แก่บุคคลากรทางไซเบอร์และผู้ใช้งานระบบเครือข่ายของสถาบัน ให้มีความรู้ในภัยคุกคามทางไซเบอร์ เพื่อสามารถป้องกันตนเองจากภัยคุกคามต่างๆ การรายงานเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

คณะกรรมการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้

๕. หน้าที่ในการดำเนินการตามแผน

หน่วยงานที่ดูแลด้านระบบสารสนเทศของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ ประกาศสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖

๖.๒ ประกาศสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อ

ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

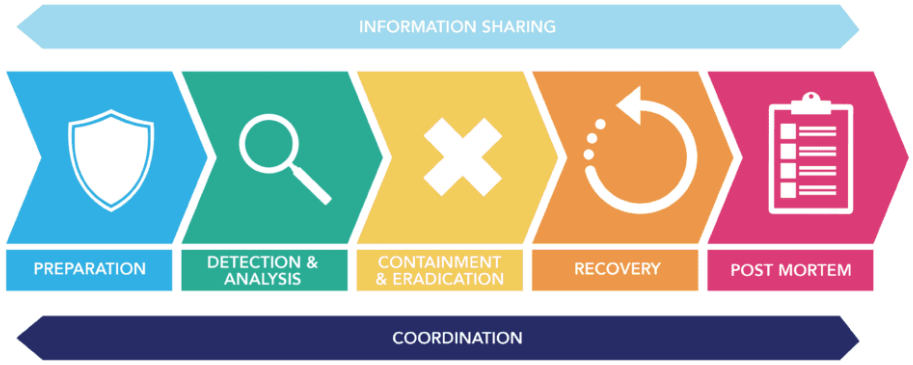
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (รายละเอียดตามผนวก ๑) ประกอบด้วย

ลำดับ	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นางสาวสุชาดา จังรัสสะ	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	- ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้ -ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๓	นายปวิธ ดวงสนิท	เจ้าหน้าที่รับมือฯ (Incident lead)	-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๔	นายสาธิต แก้วรัศมี	เจ้าหน้าที่รับมือฯ (Incident lead)	-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ -ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	นางสาวเสาวลักษณ์ เขียวผุด	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่รายงานเหตุภัยคุกคามทางไซเบอร์

๖	นางสาวรุ่งนภา โรจน์เจริญงาม	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ประเมินผลกระทบ-ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๙. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงประกาศสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖ ดังนี้



๙.๑ ขั้นการเตรียมการ เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (รายละเอียดตามผนวก ๒)

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำปนที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๙.๒.๑. การกำหนดวิธีการที่จะใช้ในการตรวจจับ Incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกใน การปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๙.๒.๑.๑. ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM (จะจัดหา ในปีงบประมาณ 2567)

๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๙.๒.๑.๒. ประเภท Log

๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์

๙.๒.๑.๓. ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้

๙.๒.๑.๔. บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๙.๒.๒. การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ ความผิดปกติเมื่อได้รับแจ้งดังนี้

๙.๒.๒.๑. log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐาน ทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๙.๒.๒.๒. Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๙.๒.๒.๓. Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ ข้อมูล

๙.๒.๒.๔. Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุ ที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

๙.๒.๓. การบันทึกภัยคุกคาม

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดตามภาคผนวก ๓)

๙.๒.๔. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจ เชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่ อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๙.๒.๔.๑. ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการและการ ดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาส เกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ

- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์

- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายในและภายนอก

- High ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

๙.๒.๔.๒. ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล ควรพิจารณา 3 ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อม ใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูล สำคัญ (Sensitive Information)อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับ อนุญาตเป็นต้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต

- Privacy Breach ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้ รับอนุญาต

- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้ รับอนุญาต

๙.๒.๔.๓. ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุ ภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญ ในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้โดยใช้ทรัพยากรที่มี

- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม

- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก

- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้วเป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๙.๒.๕. การติดต่อประสานงานและแจ้งข้อมูล

ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้อง เพื่อให้ ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้อง โครงสร้างการรับมือ ภัยคุกคามทางไซเบอร์(ตามภาคผนวก) รายละเอียดมีดังนี้

ลำดับ	ผู้เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้รับผลกระทบจาก incident	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามเกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือและตอบสนองต่อ Incident	1. รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ 2. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน 3. มีส่วนร่วมกับหน่วยงานภายนอกสถาบัน เช่น ThaiCERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน Incident	1. เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ 2. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน 3. มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น ThaiCERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม

		กำกับ ดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์

หมายเหตุ ทีมรับมือและตอบสนองต่อ Incident และทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน Incident ควรเป็น บุคลากรที่มีความรู้ ความสามารถ มีประสบการณ์ ผ่านการอบรมด้าน Cybersecurity ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้าน เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์

๙.๒.๖. การฝึกฝนและการทดสอบ

ผู้ทำหน้าที่รับมือและตอบสนองต่อ Incident ควรได้รับการอบรมฝึกฝนและทดสอบการรับมือ และตอบสนองต่อ Incident เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ และควรจัดให้มีการทดสอบแผนเป็นประจำ เพื่อประเมินและทราบถึงประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนา และเพิ่มความชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอ

๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกูคืนทรัพยสินสำคัญทางสารสนเทศใหกลับมาดำเนินงานหรือใหบริการได้ตามปกติ

๙.๓.๑. วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)

- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อ สำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)

- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย

๙.๓.๒. การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อย ที่สุด (Minimizing Impact to the Business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการ ตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล

- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) (ภาคผนวก) 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

๙.๓.๓. การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ

- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

- การลบโปรแกรมประเภท Backdoor ออกจากระบบ

- การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่ กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควร เตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย

- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ตองเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกขหรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น 12 ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปใน ระหว่างที่ตองระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน และกำนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะ ดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

๑. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
๒. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ 1. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker 2. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น 3. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด 4. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
๓. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธีCryptographic Hash เช่น MD5, SHA1, SHA256
๔. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident
๕. Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการ เคลื่อนย้าย

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

- NIST SP 800-61r2 Computer Security Incident Handling Guide

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๘
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๒) ผนวก ๑
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ ๙.๑ (๓)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๑)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๒)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๓)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๔)
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	ข้อที่ ๙.๓ (๕)
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔

ภาคผนวก ๑

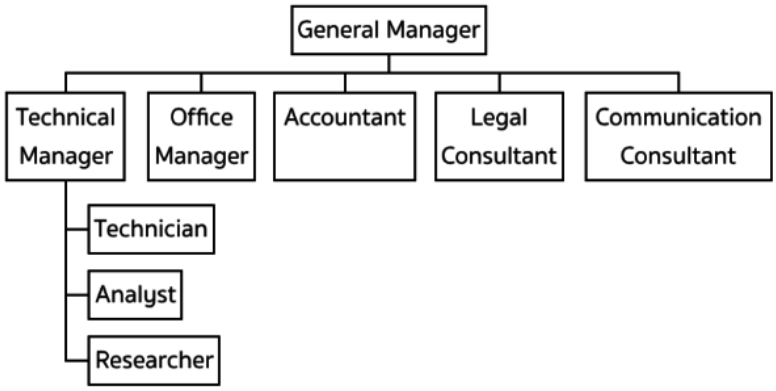
โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(Cyber Incident Response Team: CIRT)

ทีมตอบสนองต่อเหตุการณ์ซึ่งเรียกอีกอย่างว่าทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ (CSIRT), ทีมตอบสนองต่อเหตุการณ์ไซเบอร์ (CIRT), หรือทีมตอบสนองต่อเหตุฉุกเฉินเกี่ยวกับคอมพิวเตอร์ (CERT) ประกอบด้วยกลุ่มบุคลากรข้ามสายงานในองค์กรที่มีหน้าที่รับผิดชอบในการดำเนินการตามแผนตอบสนองต่อเหตุการณ์ ซึ่งไม่เพียงรวมถึงบุคคลที่กำจัดภัยคุกคามเท่านั้น แต่ยังรวมถึงบุคคลที่ตัดสินใจทางธุรกิจหรือทางกฎหมายที่เกี่ยวข้องกับเหตุการณ์ด้วย ทีมโดยทั่วไปประกอบด้วยสมาชิกดังต่อไปนี้:

- ผู้จัดการการตอบสนองต่อเหตุการณ์ซึ่งมักจะเป็นผู้อำนวยการฝ่ายไอที จะกำกับดูแลการตอบสนองทุกขั้นและแจ้งให้ผู้เกี่ยวข้องภายในรับทราบ
- นักวิเคราะห์ด้านการรักษาความปลอดภัยจะศึกษาเหตุการณ์ดังกล่าวเพื่อพยายามทำความเข้าใจถึงสิ่งที่เกิดขึ้น พร้อมทั้งบันทึกการค้นพบและรวบรวมหลักฐานการพิสูจน์อีกด้วย
- นักวิจัยด้านภัยคุกคามจะศึกษาข้อมูลภายนอกองค์กรเพื่อรวบรวมข่าวกรองที่ให้บริบทเพิ่มเติม
- บุคคลจากคณะผู้บริหาร เช่น ประธานเจ้าหน้าที่บริหารฝ่ายการรักษาความปลอดภัยของข้อมูลหรือประธานเจ้าหน้าที่บริหารฝ่ายสารสนเทศ ให้คำแนะนำและทำหน้าที่เป็นผู้ประสานงานกับผู้บริหารคนอื่นๆ
- ผู้เชี่ยวชาญด้านทรัพยากรบุคคลจะช่วยจัดการภัยคุกคามจากภายใน
- ที่ปรึกษาทั่วไปจะช่วยทีมสำรวจปัญหาด้านการรับผิดและตรวจสอบให้แน่ใจว่ามีการรวบรวมหลักฐานการพิสูจน์
- ผู้เชี่ยวชาญด้านการประชาสัมพันธ์จะประสานงานในการสื่อสารภายนอกที่ถูกต้องกับสื่อ ลูกค้า และผู้เกี่ยวข้องรายอื่นๆ

ทีมตอบสนองต่อเหตุการณ์อาจเป็นชุดย่อยของศูนย์การดำเนินการรักษาความปลอดภัย (SOC) ซึ่งจัดการการดำเนินการรักษาความปลอดภัยนอกเหนือจากการตอบสนองต่อเหตุการณ์



คุณสมบัติและทักษะ ประกอบด้วย

- ศักยภาพด้านบุคคล

ยืดหยุ่น มีความคิดสร้างสรรค์ และทำงานเป็นทีม
มีทักษะการวิเคราะห์ที่ดีเยี่ยม
สามารถอธิบายข้อมูลเชิงเทคนิคให้ผู้อื่นเข้าใจได้ง่าย
มีความมั่นใจสูงและทำงานอย่างเป็นระบบ
อดทนต่อความกดดัน
มีทักษะด้านการติดต่อสื่อสารและการเขียนดีเยี่ยม
เปิดใจและพร้อมที่เรียนรู้สิ่งใหม่

- ศักยภาพด้านเทคนิค

มีความรู้ทางด้านเทคโนโลยีอินเทอร์เน็ตและโปรโตคอลอย่างกว้างขวาง
มีความรู้ทางด้านระบบ Linux, Unix และ Windows
มีความรู้ทางด้านอุปกรณ์โครงสร้างเครือข่าย
มีความรู้ทางด้านแอพพลิเคชันและบริการบนอินเทอร์เน็ต เช่น SMTP, HTTP(s), Social Media และอื่นๆ
มีความรู้ทางด้านภัยคุกคาม เช่น DDoS, Phishing, Deafacing, Malware และอื่นๆ
มีความรู้ทางด้านการประเมินความเสี่ยงและการวางระบบ
มีความรู้ทางด้านการวิเคราะห์ข้อมูลแบบ Big Data และ Malware

- ศักยภาพด้านอื่นๆ

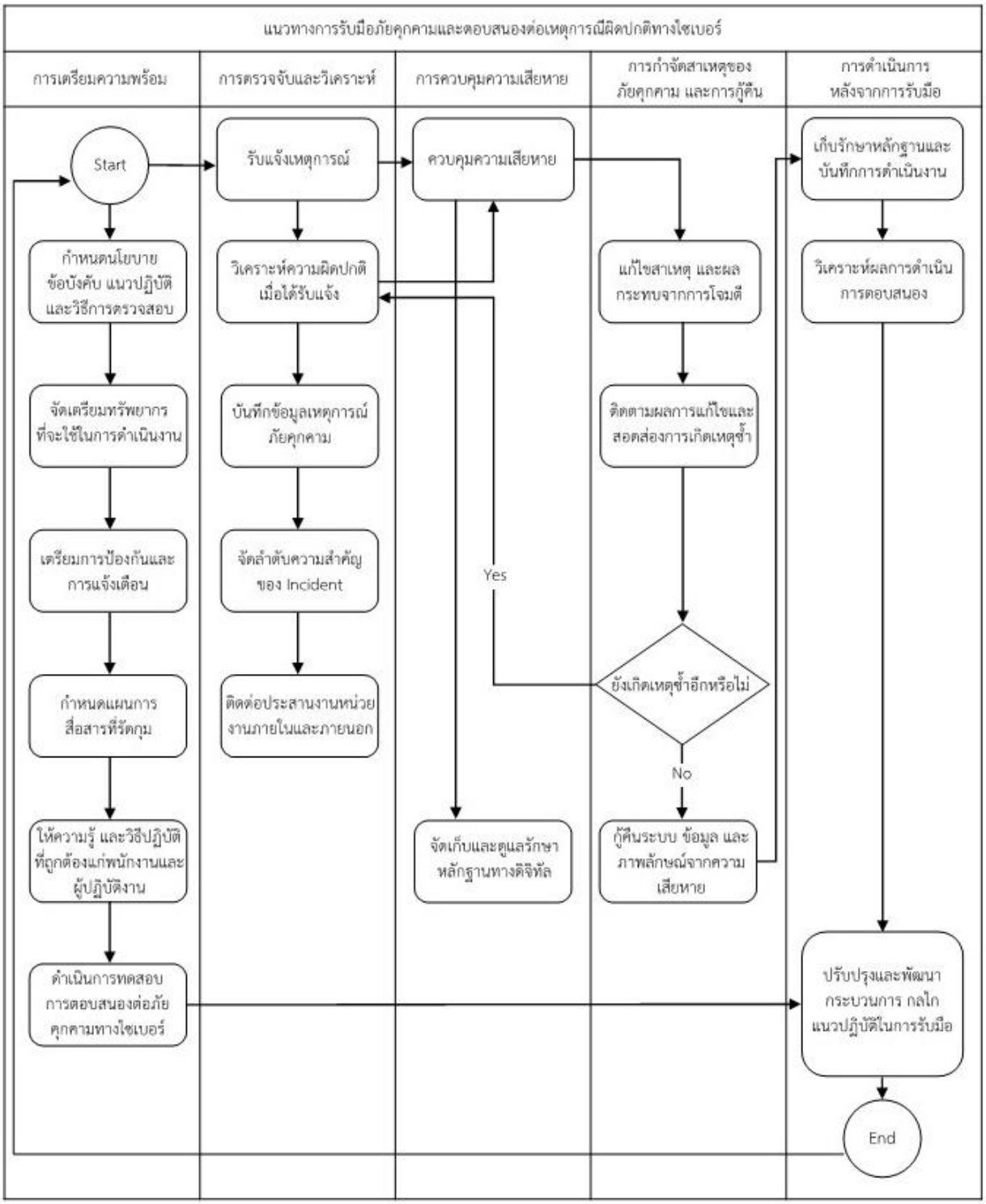
พร้อมทำงานแบบ 7/24 หรือพร้อมรับการติดต่อตลอดเวลา
สามารถทำงานต่างจังหวัดหรือระยะไกลได้
มีประสบการณ์การทำงานในสาย IT Security

ภาคผนวก ๒ โครงสร้างการรับมือภัยคุกคามทางไซเบอร์

รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์มีดังนี้

ขั้นตอน	ผู้รับผิดชอบ
๑.การแจ้งเหตุ	ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก Incident
๒. ขั้นการเตรียมการ (Preparation) ๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน ๒.๓ เตรียมการป้องกันและแจ้งเตือน ๒.๔ เตรียมรายละเอียดช่องทางการ ติดต่อสื่อสาร ๒.๕ การให้ความรู้ และวิธีปฏิบัติ ๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทาง ไซเบอร์	ทีมรับมือและตอบสนองต่อ Incident และเจ้าของระบบฯ
๓. ขั้นการตรวจจับ และวิเคราะห์ภัยคุกคาม (Detection & Analysis) ๓.๑ รับแจ้งเหตุ ๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง ๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม ๓.๔ จัดลำดับความสำคัญของ Incident ๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และภายนอก	ผู้รับแจ้งเหตุ ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ ผู้รับแจ้งเหตุ ทีมรับมือและตอบสนองต่อ Incident ทีมรับมือและตอบสนองต่อ Incident
๔. การระงับภัยคุกคามทางไซเบอร์ (Containment) ๔.๑ ควบคุมความเสียหาย ๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล	ทีมรับมือและตอบสนองต่อ Incident
๕. การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟู (Eradication & Recovery) ๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี ๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จาก ความเสียหาย	ทีมรับมือและตอบสนองต่อ Incident
๖. การดำเนินการภายหลังการแก้ปัญหาภัยคุกคาม (Post - Incident) ๖.๑ เก็บรักษาหลักฐานและบันทึกการ ดำเนินงาน ๖.๒ ปรับปรุงและพัฒนากระบวนการ กลไก แนวปฏิบัติในการรับมือ	ทีมรับมือและตอบสนองต่อ Incident

Cyber Incident Response Flow Chart



ภาคผนวก ๓ แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

๑. ชื่อเหตุการณ์ ..... ๒. หมายเลขของเหตุการณ์.....

๓. วันที่บันทึกเหตุการณ์ .....

๔. หมายเลขของเหตุการณ์อื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้.....

๕. ข้อมูลของผู้แจ้งเหตุการณ์ ๖.ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์

ชื่อ-นามสกุล	ชื่อ-นามสกุล .....
หน่วยงาน	หน่วยงาน .....
โทรศัพท์	โทรศัพท์ .....
อีเมล	อีเมล .....

๗. วันที่และเวลาเกิดเหตุการณ์

.....

๘. วันที่และเวลาพบเหตุการณ์

.....

๙. วันที่และเวลารายงานเหตุการณ์

.....

๑๐. รายละเอียดเหตุการณ์

.....

.....

.....

๑๑. การดำเนินการทั้งหมดของทีมรับมือและตอบสนอง

.....

.....

๑๒. การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนอง

.....

.....

๑๓. ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ

.....

๑๔. รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์

.....

.....

๑๕. สรุปสาระสำคัญของเหตุการณ์

.....

.....

แผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐	
๑.	ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือภายนอก						
๒.	ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย cyber ด้านระบบเครือข่าย /ระบบสารสนเทศ/ ระบบดิจิทัล						
๓.	จัดทำและทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ของระบบเครือข่าย/ระบบสารสนเทศ/ระบบดิจิทัล						
๔.	จัดทำและปรับปรุงคู่มือ/แผนงาน/กระบวนการที่เกี่ยวข้องในการป้องกันภัย คุกคามทาง cyber แต่ละระบบสำรสนเทศหรือฐานข้อมูล						
๕.	ขั้นตอนที่๑ : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์						
๖.	จัดทำรายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสอบต่อภัยคุกคามทางไซเบอร์						
๗.	จัดทำรูปแบบ/แบบฟอร์มการรายงานเหตุการณ์ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์						

๘.	จัดทำแบบฟอร์มการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตการณ์ที่ได้รับแจ้ง						
๙.	จัดเตรียมสถานที่จัดเก็บ ที่มีความมั่นคงปลอดภัย เพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูล และพยานวัตถุอื่น ๆ ที่สำคัญ (ใช้ห้อง data center)						
๑๐.	จัดหาอุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์						
๑๑.	จัดหาระบบตรวจจับและป้องกันภัยคุกคามไซเบอร์ ของเครื่องคอมพิวเตอร์แม่ข่าย (Server EndPoint Detection & Response) ทำการติดตั้งและทำการปรับ Fine Tune						
๑๒.	จัดตั้งทีมรับมือภัยคุกคามทาง Cyber						
๑๓.	ส่งบุคลากรเพื่อเข้ารับการฝึกอบรมด้าน Cyber Security						
๑๔.	ตั้งค่าระบบต่าง ๆ ที่ใช้งานอยู่ในปัจจุบันให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS และระบบสารสนเทศที่พัฒนาขึ้น การ MA ระบบอย่างต่อเนื่อง)						
๑๕.	ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์						

๑๖.	ขั้นตอนที่๓: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ						
๑๗.	จัดทำคู่มือหรือวิธิการควบคุมความเสียหาย การจัดเก็บและดูแลหลักฐานทางดิจิทัล ของระบบสารสนเทศในแต่ละระบบ						
๑๘.	จัดทำแนวทางการจำกัดสาเหตุและการกู้คืน ระบบสารสนเทศในแต่ละระบบ หรือแต่ละ เหตการณ์ที่สามารถเกิดขึ้นได้						
๑๙.	ขั้นตอนที่๔ : การดำเนินการภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์						
๒๐.	จัดทำบันทึกข้อมูลสถติ ภัยคุกคามทางไซเบอร์เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับ ผิดชอบภายในหน่วยงาน						
๒๑.	จัดทำแนวทางปฏิบัติในการดูแลรักษาหลักฐานทางดิจิทัลของระบบสารสนเทศแต่ละระบบ						