



แผนรับมือเหตุการณ์คุกคามทางไซเบอร์ โรงพยาบาลสกลนคร

(Cyber Incident Response Plan)

งานเทคโนโลยีสารสนเทศ

โรงพยาบาลสกลนคร

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ โรงพยาบาลสระบัวอ้อย (Cyber Incident Response Plan)

๑. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์โดยจะระบุขั้นตอนที่จำเป็นผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหายการกำจัดสาเหตุของภัยคุกคามและการกักกัน (Containment ,Eradication & Recovery) และการดำเนินการภายหลังการรับมือ และตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ต่อหน่วยงานในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เหมาะสมกับขนาด ความซับซ้อน ความเสี่ยงและรูปแบบในการดำเนินงานของหน่วยงาน

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคาม การจัดทำแผนนี้เป็นส่วนหนึ่งของแผนรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งประกอบด้วย

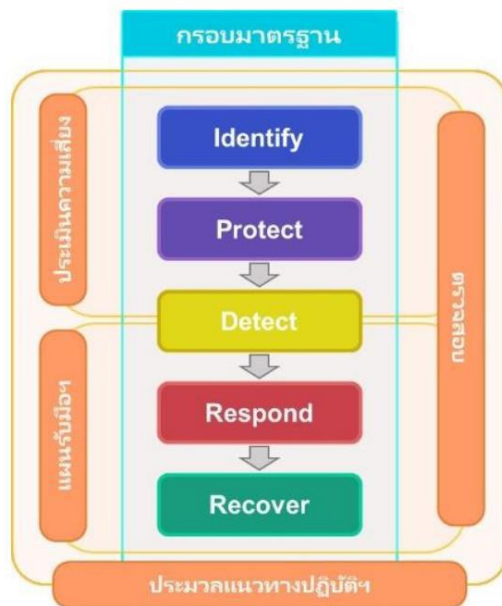
แผนดำเนินการอย่างต่อเนื่อง Business Continuity Plan (BCP)

แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan : CIRP)

แผนฟื้นฟูระบบ (Business Recovery Plan : BRP)

แผนป้องกันและเผชิญเหตุภัยพิบัติ (Disaster Recovery Plan (DRP)

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)



รูปที่ ๑ แสดงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์

- ๒.๑. เพื่อสร้างความเชื่อมั่นให้ผู้ใช้งานระบบเครือข่ายโรงพยาบาลสบาย้อยได้รับการปกป้องต่อภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ
- ๒.๒. เพื่อกำหนดมาตรการ นโยบาย และกลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการรับมือในภาวะฉุกเฉินเพื่อแก้ไขปัญหาอย่างทันท่วงที
- ๒.๓. เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงานภายในโรงพยาบาลให้สามารถป้องกันตนเองจากภัยคุกคามต่างๆ สามารถรายงานเหตุภัยคุกคามทางไซเบอร์และทราบขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตที่กำหนดไว้
- ๒.๔. เพื่อสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาลสบาย้อย

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของโรงพยาบาลสบาย้อย รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

คณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโรงพยาบาลสบาย้อยมีหน้าที่ทบทวนและขออนุมัติแผนฉบับนี้ต่อคณะกรรมการบริหารความเสี่ยงโรงพยาบาลและคณะกรรมการบริหารโรงพยาบาล

๕. หน้าที่ในการดำเนินการตามแผน

หน่วยงานที่ดูแลด้านระบบสารสนเทศของโรงพยาบาล ประกอบด้วย กลุ่มงานเทคโนโลยีสารสนเทศ กลุ่มงานสุขภาพดิจิทัลกลุ่มงานเวชระเบียนและข้อมูลทางการแพทย์คณะกรรมการคณะกรรมการรักษาความมั่นคงปลอดภัย ทางไซเบอร์คณะกรรมการสุขภาพดิจิทัลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการสารสนเทศโรงพยาบาลสบาย้อย มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนฉบับนี้

๖. ความเกี่ยวข้องกับเอกสารอื่น

- ๖.๑ ประกาศโรงพยาบาลสบาย้อย เรื่อง นโยบายเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๗
- ๖.๒ ประกาศโรงพยาบาลสบาย้อย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๗
- ๖.๓ ประกาศโรงพยาบาลสบาย้อย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
- ๖.๔ ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับผู้ใช้งานทั่วไป) พ.ศ. ๒๕๖๗

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่ายสภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้เหตุภัยคุกคามทางไซเบอร์ (Cyberincident) หมายความว่าเหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนิน

การใดโดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นอันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อ ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อ ให้เกิด ความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

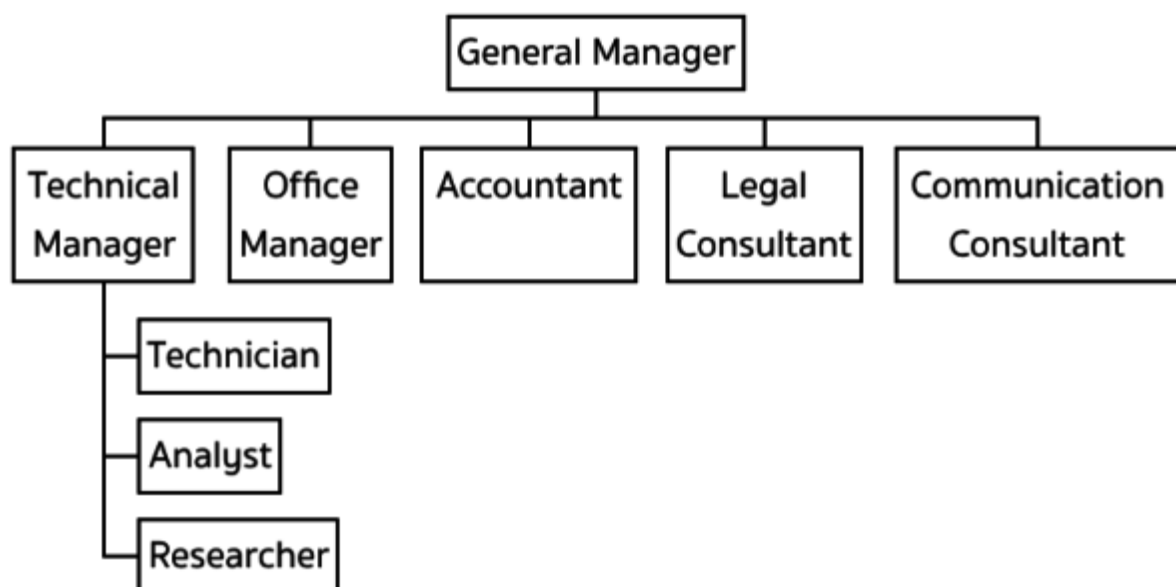
เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญหมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏ ต่อระบบสารสนเทศและเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่ง คณะกรรมการการ รักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทาง ไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

โรงพยาบาลสละบ้าย้อย ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ในลักษณะแบบรวมศูนย์ (รายละเอียดโครงสร้างเพิ่มเติมทีมดังภาคผนวก ๑) ประกอบด้วย

ทีมตอบสนองต่อเหตุการณ์อาจเป็นชุดย่อยของศูนย์การดำเนินการรักษาความปลอดภัย (SOC) ซึ่ง จัดการ การดำเนินการรักษาความปลอดภัยนอกเหนือจากการตอบสนองต่อเหตุการณ์

Team Manager (CIO)

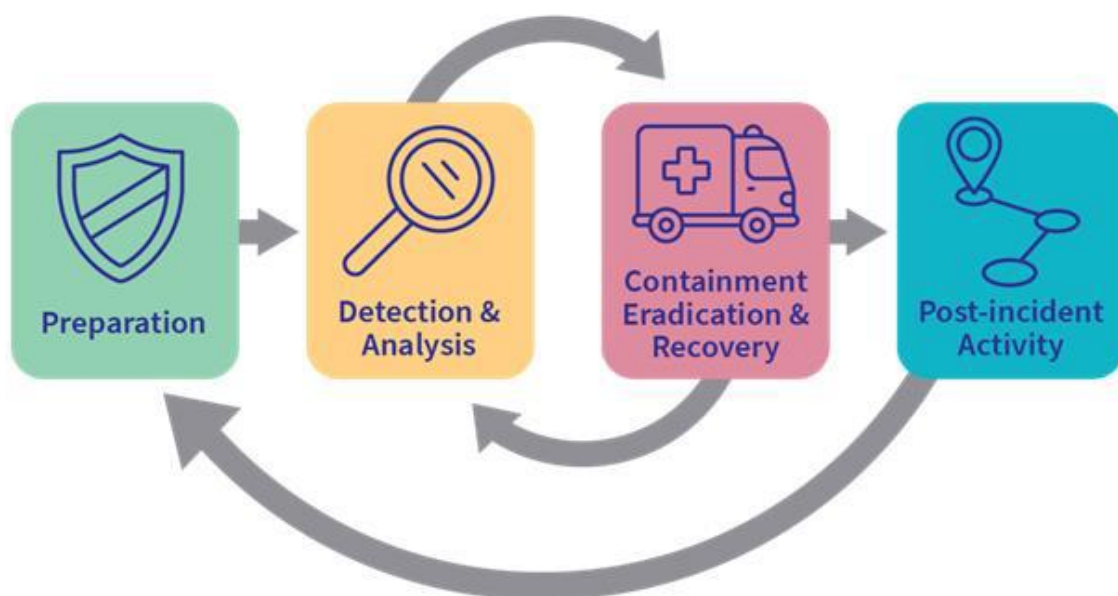


ลำดับ ที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	ภก.นิรุจน์ย์ รัตนประ พันธ์ (CIO)	หัวหน้าทีม (Team manager)	ทำหน้าที่บริหารจัดการทีมเพื่อ ควบคุม ระวัง เหตุจำกัดความเสียหายและสื่อสาร กับผู้บริหารของโรงพยาบาล
๒	นายรัชชัย ชატะพล หัวหน้ากลุ่มงานสุขภาพ ดิจิทัล	รองหัวหน้าทีม (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีม ไม่อยู่/ไม่ สามารถปฏิบัติงานได้
๓	นายรัชชัย มณี	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ประเมินความเสียหายจำกัด และ ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ (Control and Respond)
๔	นายมนตรี โดยหะ	เจ้าหน้าที่วิเคราะห์และสืบเหตุ (Investigate lead)	ทำหน้าที่ค้นหาสาเหตุ แหล่งที่มาของภัย คุกคามทางไซเบอร์ (Investigate)
๕	ผู้แทนจาก สกมช.	เจ้าหน้าที่ (Incident lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทาง ที่เหมาะสมในการควบคุมผลกระทบ จากภัยคุกคามทางไซเบอร์
๖	ผู้แทนจากบริษัทเอกชน ดูแลด้าน Cybersecurity Vender ของโรงพยาบาล	เจ้าหน้าที่ (Incident lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทาง ที่เหมาะสมในการจัดการและควบคุมภัย คุกคามทางไซเบอร์
๗	เจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคลประจำ โรงพยาบาลสະบ้ำย้อย	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทาง ที่เหมาะสมในการคุ้มครองข้อมูล ส่วนบุคคล ของรับบริการและประสานงาน กับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส)
๘	ผู้แทนส่วนสารบรรณนิติ การ	ผู้เชี่ยวชาญด้านกฎหมาย (Legal Consultant)	ทำหน้าที่ประเมินผลกระทบและ ความเสี่ยงที่ เกี่ยวกับกฎหมายความมั่นคง ปลอดภัยทางไซเบอร์ กฎหมาย PDPA
๙	พ.ญ.สุวารี ชูประดิษฐ์ นายแพทย์ชำนาญการ	ประธานกรรมการบริหารความ เสี่ยง (Risk Management)	ทำหน้าที่ประเมินผลกระทบความเสี่ยง ในภาพรวมของทั้งโรงพยาบาล
๑๐	ผู้แทนส่วน ประชาสัมพันธ์	ผู้รับผิดชอบด้านสื่อสารองค์กร (Communication Consult)	ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วน เสีย เกี่ยวกับความมั่นคงปลอดภัย ไซเบอร์

๙. ขั้นตอนการรับมือ

แผนฉบับนี้ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของ รัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงประกาศโรงพยาบาลสละบ้าย้อย เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลสละบ้าย้อย พ.ศ. ๒๕๖๗ ดังนี้

Cyber Incident Response Cycle



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

(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 ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

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

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตามแต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจ หลีกเลียงได้ การดำเนินการมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทัน ท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๙.๒.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายาม โจมตี และกลไกใน การปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึก ข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติและมีการปรับ Finetune เพื่อให้มีความเหมาะสมกับสภาพการใช้งาน ของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบ ที่ต้องการ ป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

ประเภท Alert

๑) Firewall ปัจจุบันโรงพยาบาลสละบ้าย้อย Forti Gate ๒๐๐ F

๒) Anti-Virus ปัจจุบันโรงพยาบาลใช้ ESET nod ๓๒ สำหรับเครื่องลูกข่าย และ Kaspersky สำหรับเครื่องแม่ข่ายระบบ E-office windows server ทำหน้าที่ตรวจจับโปรแกรม ประสงค์ร้าย

ประเภท Log

๑) Operating System and Application Log โดยอุปกรณ์ FortiGate ข้อมูลจาก Log ของ Hosxp และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถ ถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์ โดยสามารถเก็บข้อมูลได้สูงสุด ๗ วัน

๒) Network Access Control (NAC) อุปกรณ์เครือข่ายที่มีควบคุมและการบันทึก ข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์ ปัจจุบันโรงพยาบาลใช้ระบบ Fortinet

ประเภทข้อมูลอื่นๆ

ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้ เช่น เว็บไซต์ สกมช. Thai Health CERT ข่าวสารทางโทรทัศน์

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 ตรงกันอยู่เสมอเพื่อให้การ Correlate Event ทำได้ง่าย

๙.๒.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่าย เพื่อนำมาวิเคราะห์ ข้อมูล

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

๙.๒.๓ การบันทึกภัยคุกคาม

กรณีปฏิบัติงานปกติประจำวันจะต้องมีเจ้าหน้าที่สารสนเทศเข้ามาดู Alert และ Log ตามข้อ ๙.๒.๑ ทุกครั้งที่ขึ้นเวรเช้าและเวรบ่าย และเขียนรายงานสรุป ตามแบบฟอร์ม (รายละเอียดดังภาคผนวก ๓) และ CISO นำเหตุการณ์ที่สำคัญรายงานที่ประชุมกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทุกเดือน

หากมีเหตุการณ์ความเสี่ยงที่รุนแรงระดับกลางขึ้นไปต้องทำการบันทึกข้อมูล เหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพและเป็นระบบโดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดดังภาคผนวก 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) ผลกระทบต่อการให้บริการ และการ ดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาส เกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึง

ผลกระทบทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไข โดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ยังครบถ้วนสมบูรณ์
- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายใน และภายนอก
- High ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

๙.๒.๔.๒ ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล ควรพิจารณา ๓ 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 หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาต

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

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือ จากภายนอก
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะ แล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๙.๒.๕ การติดต่อประสานงานและแจ้งข้อมูล

ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้อง โครงสร้างการรับมือ ภัยคุกคามทางไซเบอร์(ตามภาคผนวก) รายละเอียดดังนี้

ลำดับที่	ผู้เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้รับผลกระทบจาก incident	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบ หรือ สงสัยว่ามีภัยคุกคามเกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือและตอบสนองต่อ incident	๑.รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดขึ้นใหม่ให้เจ้าหน้าที่ ในหน่วยงาน ๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident	๑.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ ตรวจจับ ทุกวันและทำบันทึกประจำวัน ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดขึ้นใหม่ให้เจ้าหน้าที่ ในหน่วยงาน ๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดทำ และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยไซเบอร์

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

๙.๒.๖ การฝึกฝนและการทดสอบ

ผู้ทำหน้าที่รับมือและตอบสนองต่อ incident ควรได้รับการอบรมฝึกฝนและทดสอบ การรับมือ และตอบสนองต่อ incident เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่ กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผน ได้อย่างมีประสิทธิภาพ และควรจัดให้มี การทดสอบแผนเป็นประจำ เพื่อประเมินและทราบถึง

ประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนา และเพิ่มความชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอ

๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมา ดำเนินงานหรือให้บริการได้ตามปกติ

๙.๓.๑ วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมีข้อยกเว้นการเชื่อมต่อ สำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบ และตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลา และทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย โดย CIO เป็นผู้ตัดสินใจเลือกแนวที่รวดเร็วและจำกัดความเสียหายให้ได้อย่างจำกัดมากที่สุด

๙.๓.๒ การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

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

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวข้องกับหลักฐานดิจิทัล 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 และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่าง การรับมือ Incident

๓) สถานที่จัดเก็บหลักฐาน

๙.๓.๓ การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ ๒ เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อยแล้ว 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 จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่งและควร เตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าสู่ระบบจาก Back Up Storage

๙.๔ ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามให้ใช้ แผนดังกล่าว และแผนฟื้นฟูระบบ (Business Recovery Plan : BRP) และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น ๑๒ ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไป ในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว โดยการดูแลรักษาหลักฐานทางดิจิทัลที่ต้องดำเนินการดังนี้

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 ๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware

	Write Blocker ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น ๓. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติ อย่างละเอียด ๔. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
๓. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธีCryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖
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 และการ จัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในชั้นศาล หลักฐานเหล่านี้จึง จะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่า เป็นหลักฐานที่ปลอมหรือทำขึ้นมา

แหล่งที่มา

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

NIST SP ๘๐๐-๖๑๒ Computer Security Incident Handling Guide
แนวทางการดำเนินงาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ พ.ศ. ๒๕๖๗ (HAIT plus)

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	ข้อที่ ๘
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๙.๑ (๒) ผนวก ๑
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๓)
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT	ข้อที่ ๙.๓ (๑)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๒)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๓)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๔)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๕)

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนฉบับนี้
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือ แนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้ กฎหมายเพื่อดำเนินคดี และ (ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔

ภาคผนวก ๑

โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

ทีมตอบสนองต่อเหตุการณ์ซึ่งเรียกอีกอย่างว่าทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ (CSIRT), ทีมตอบสนองต่อเหตุการณ์ไซเบอร์ (CIRT), หรือทีมตอบสนองต่อเหตุฉุกเฉินเกี่ยวกับคอมพิวเตอร์ (CERT) ประกอบด้วยกลุ่มบุคลากรข้ามสายงานในองค์กรที่มีหน้าที่รับผิดชอบในการดำเนินการตามแผนตอบสนองต่อเหตุการณ์ ซึ่งไม่เพียงรวมถึงบุคคลที่กำจัดการคุกคามเท่านั้น แต่ยังรวมถึงบุคคลที่ตัดสินใจทางธุรกิจหรือทางกฎหมายที่เกี่ยวข้องกับเหตุการณ์ด้วย ทีมโดยประกอบด้วยสมาชิกดังต่อไปนี้

ผู้จัดการการตอบสนองต่อเหตุการณ์ จะกำกับดูแลการตอบสนองทุกชั้นและแจ้งให้ผู้เกี่ยวข้องภายในรับทราบ ตำแหน่งคือรองผู้อำนวยการด้านสุขภาพดิจิทัล

นักวิเคราะห์ด้านการรักษาความปลอดภัยจะศึกษาเหตุการณ์ดังกล่าวเพื่อพยายามทำความเข้าใจถึงสิ่งที่เกิดขึ้น พร้อมทั้งบันทึกการค้นพบและรวบรวมหลักฐานการพิสูจน์อีกด้วย ตำแหน่งคือหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

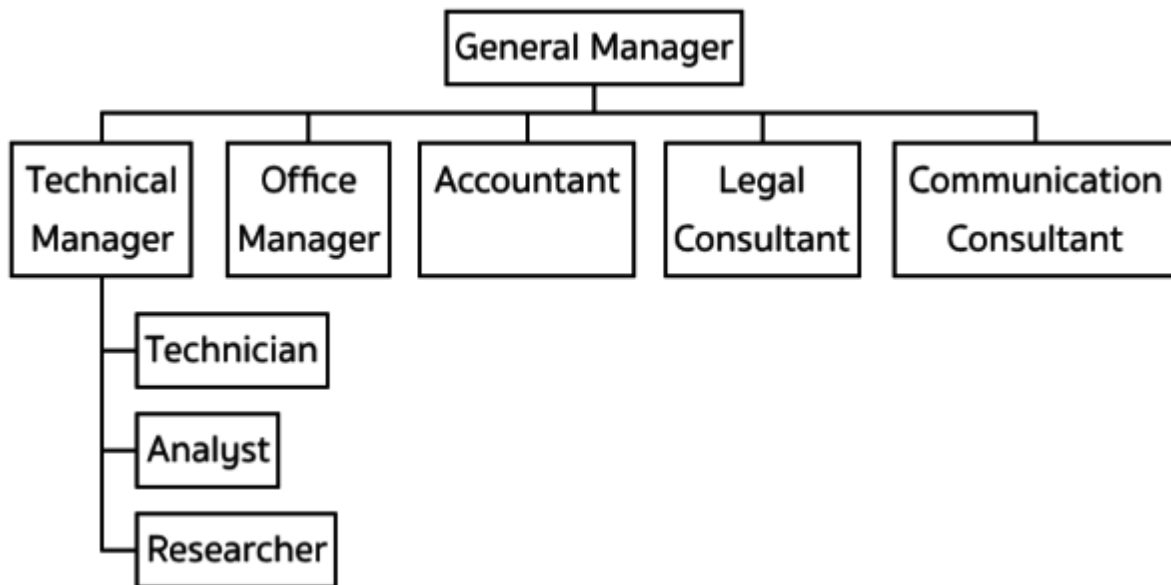
นักวิจัยด้านภัยคุกคามจะศึกษาข้อมูลภายนอกองค์กรเพื่อรวบรวมข่าวกรองที่ให้บริบทเพิ่มเติม ตำแหน่งคือหัวหน้างาน Infrastructure - Cybersecurity

บุคคลจากคณะผู้บริหาร ได้แก่ คณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์ระดับโรงพยาบาล

ผู้เชี่ยวชาญด้านทรัพยากรบุคคลจะช่วยจัดการภัยคุกคามจากภายใน

ที่ปรึกษาภายนอกที่จะช่วยทีมสำรวจปัญหาด้านการรับมือและตรวจสอบให้แน่ใจว่ามีการรวบรวมหลักฐานการพิสูจน์ ได้แก่ สกมช. สคส.

ทีมประชาสัมพันธ์จะประสานงานในการสื่อสารภายนอกที่ถูกต้องกับสื่อ ลูกค้า และผู้เกี่ยวข้องรายอื่นๆ



คุณสมบัติและทักษะ Technician ที่พึงมี ประกอบด้วย

- ศักยภาพด้านบุคคล
- ยืดหยุ่น มีความคิดสร้างสรรค์ และทำงานเป็นทีม
- มีทักษะการวิเคราะห์ที่ดีเยี่ยม
- สามารถอธิบายข้อมูลเชิงเทคนิคให้ผู้อื่นเข้าใจได้ง่าย
- มีความมั่นใจสูงและทำงานอย่างเป็นระบบ
- อดทนต่อความกดดัน
- มีทักษะด้านการติดต่อสื่อสารและการเขียนดีเยี่ยม
- เปิดใจและพร้อมที่เรียนรู้สิ่งใหม่
- ศักยภาพด้านเทคนิค
- มีความรู้ทางด้านเทคโนโลยีอินเทอร์เน็ตและโปรโตคอลอย่างกว้างขวาง
- มีความรู้ทางด้านระบบ Linux, Unix และ Windows
- มีความรู้ทางด้านอุปกรณ์โครงสร้างเครือข่าย
- มีความรู้ทางด้านแอปพลิเคชันและบริการบนอินเทอร์เน็ต เช่น SMTP, HTTP(s), Social Media และอื่นๆ
- มีความรู้ทางด้านภัยคุกคาม เช่น DDoS, Phishing, Defacing, Malware และอื่นๆ
- มีความรู้ทางการประเมินความเสี่ยงและการวางระบบ
- มีความรู้ทางการวิเคราะห์ข้อมูลแบบ Big Data และ Malware
- ศักยภาพด้านอื่นๆ
- พร้อมทำงานแบบ ๗/๒๔ หรือพร้อมรับการติดต่อตลอดเวลา
- สามารถทำงานต่างจังหวัดหรือระยะไกลได้
- มีประสบการณ์การทำงานในสาย IT Security

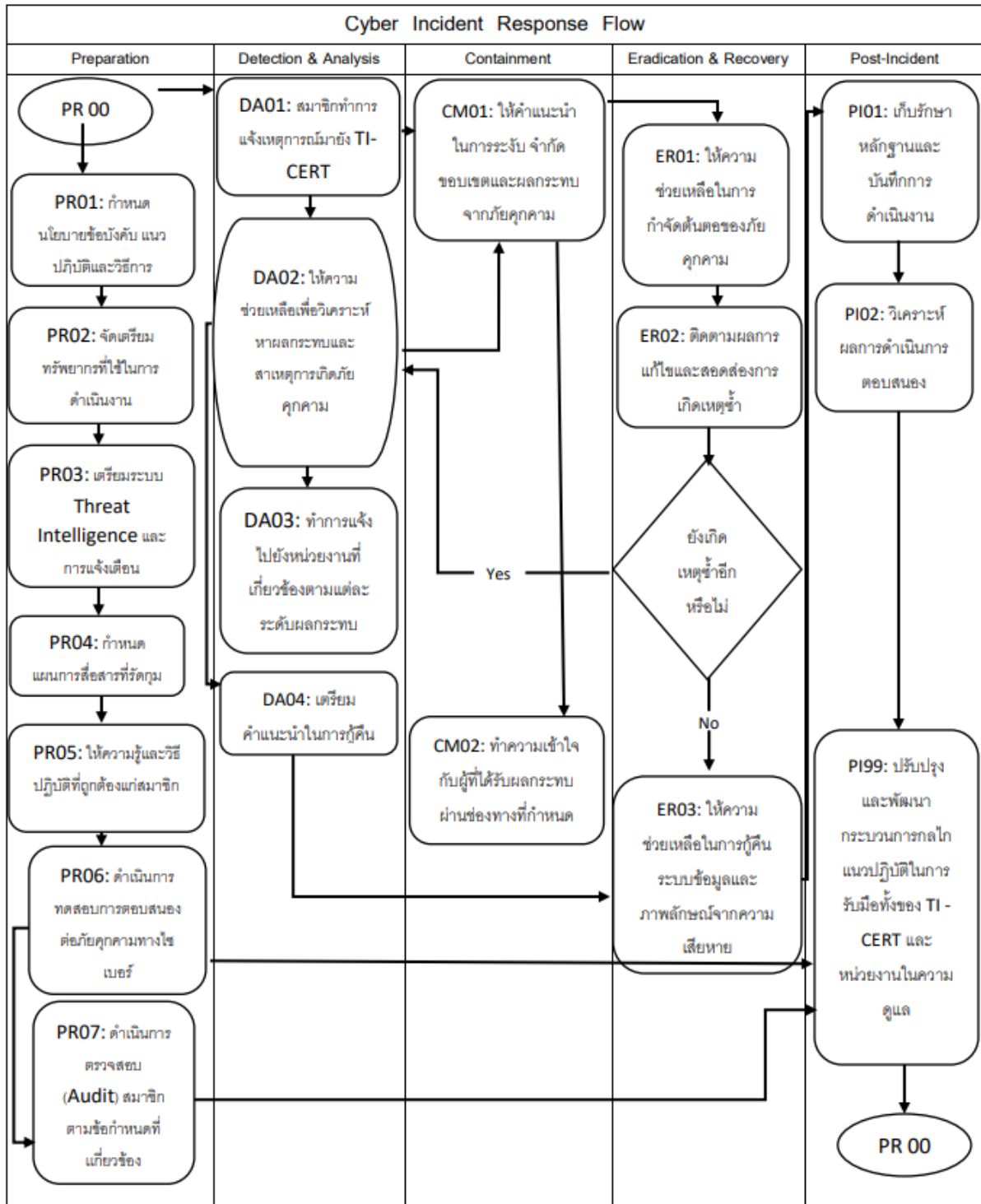
ภาคผนวก ๒

โครงสร้างการรับมือภัยคุกคามทางไซเบอร์ และ Call Tree เมื่อเกิดเหตุการณ์คุกคามทางไซเบอร์
โรงพยาบาลสะบ้าย้อย ๒๕๖๘ ประเภทรุนแรง

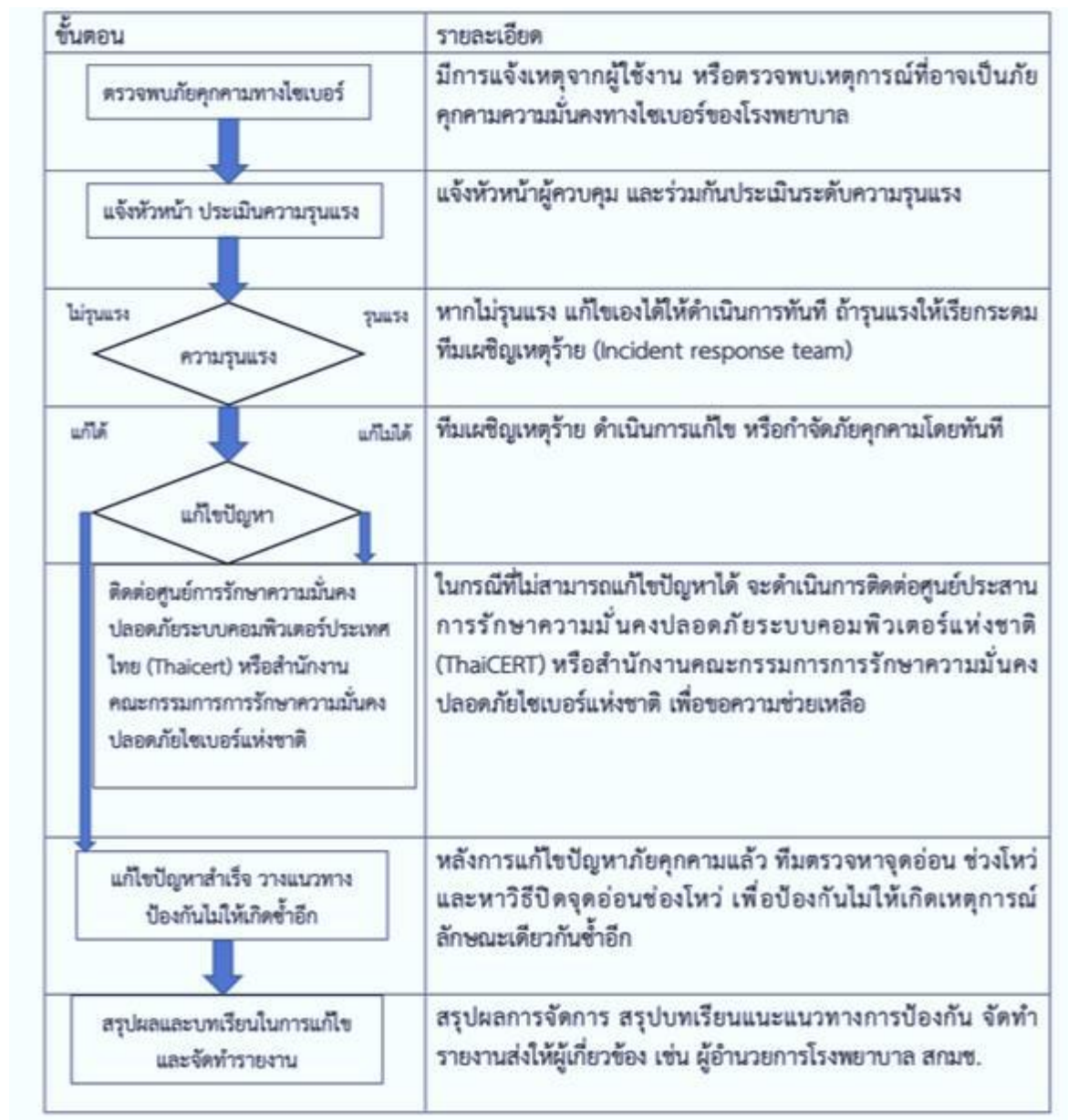
รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์มีดังนี้

ขั้นตอน	ผู้รับผิดชอบ/ผู้ประสานงาน
๑.การแจ้งเหตุ	ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก incident เจ้าหน้าที่เวรไอที (๐๗๔-๓๗๗๑๐๐-๑) ต่อ ๑๒๙-๑๒๓
๒. ขั้นตอนการเตรียมการ (Preparation) ๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน ๒.๓ เตรียมการป้องกันและแจ้งเตือน ๒.๔ เตรียมรายละเอียดช่องทางการติดต่อสื่อสาร ๒.๕ การให้ความรู้ และวิธีปฏิบัติ ๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทาง ไซเบอร์	นายธวัชชัย มณี (PR ๐๑-๐๗) โทร ๐๘๙๒๙๙๓๖๓๗  แจ้งผู้อำนวยการโรงพยาบาลสะบ้าย้อย โทร ๐๘๑๗๖๖๔๕๑๒
๓.ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection & Analysis) ๓.๑ รับแจ้งเหตุ ๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง ๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม ๓.๔ จัดลำดับความสำคัญของ incident ๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และ ภายนอก	นายธวัชชัย ชาทะพล DA ๐๑-๐๔) โทร ๐๘๘๗๘๔๔๔๔๐
๔. การระงับภัยคุกคามทางไซเบอร์ (Containment) ๔.๑ ควบคุมความเสียหาย ๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล	นายธวัชชัย มณี (CM-๐๑) โทร ๐๘๙๒๙๙๓๖๓๗
๕.การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟู (Eradication & Recovery) ๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี ๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จาก ความ เสียหาย	นายมนตรี โดยหะ (ER-๐๑) โทร ๐๙๘๖๙๘๙๙๒๙
๖.การดำเนินการภายหลังการแก้ปัญหาภัยคุกคาม (Post-incident) ๖.๑ เก็บรักษาหลักฐานและบันทึกการ ดำเนินงาน ๖.๒ ปรับปรุงและพัฒนากระบวนการ กลไก แนว ปฏิบัติในการรับมือ	นายธวัชชัย มณี (PI ๐๑-๐๒) นายมนตรี โดยหะ (PI ๙๙)

Cyber Incident Response Flow Sabayoi Hospital



สรุปขั้นตอนการเผชิญเหตุ และแก้ไข เมื่อเกิดภัยคุกคามทางไซเบอร์โรงพยาบาลสະบ้ำย้อย ๒๕๖๘



ภาคผนวก ๓

รายการตรวจสอบ เหตุการณ์ที่อาจเป็นร่องรอยของการละเมิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาล

เหตุการณ์	วันเวลาที่รายงานขึ้นไป
1. การจราจรใน network ของโรงพยาบาลหนาแน่นผิดปกติ ☐ ไม่พบ ☐ พบ	
2. พื้นที่ว่างใน hard disk ของเครื่องแม่ข่าย หายไปผิดปกติ ☐ ไม่พบ ☐ พบ	
3. CPU Usage สูงผิดปกติ ☐ ไม่พบ ☐ พบ	
4. พบการสร้างบัญชี user ใหม่ โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
5. พบการใช้บัญชีผู้ดูแลระบบ โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
6. พบการปิดบัญชีผู้ใช้งาน โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
7. พบการใช้บัญชีผู้ใช้งานโดยเจ้าของบัญชีลาพักผ่อน ลาศึกษาต่อ ไม่อยู่ ☐ ไม่พบ ☐ พบ	
8. log files ถูกลบทิ้งไป ☐ ไม่พบ ☐ พบ	
9. log files เพิ่ม มีเหตุการณ์ไม่ธรรมดาบันทึกไว้ใน log file จำนวนมาก ☐ ไม่พบ ☐ พบ	
10. การแจ้งเตือนจาก antivirus หรือระบบตรวจจับการบุกรุก ☐ ไม่พบ ☐ พบ	
11. ระบบ antivirus หรือระบบป้องกันอื่น ๆ ถูกปิดไป ☐ ไม่พบ ☐ พบ	
12. มีการเปลี่ยนแปลงใน patch โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
13. พบการเชื่อมโยงเครื่องมือแพทย์ใน network ของโรงพยาบาลไปยัง IP ภายนอก ☐ ไม่พบ ☐ พบ	
14. พบคำสั่งขอรายละเอียดเครื่องแม่ข่ายเข้ามาในระบบ ☐ ไม่พบ ☐ พบ	
15. ความเร็วของการส่งข้อมูลในระบบเครือข่ายลดลงมากเห็นได้ชัด ☐ ไม่พบ ☐ พบ	
16. เกิดหน้าจอแสดงผล error ในหน้า web, เครื่องแม่ข่าย หรือ ฐานข้อมูล ☐ ไม่พบ ☐ พบ	
17. ชื่อไฟล์หรือโคเร็กทอรีถูกเปลี่ยน แทรกด้วยอักขระผิดปกติ ☐ ไม่พบ ☐ พบ	
18. ค่าของระบบที่ตั้งไว้ (system configuration) เปลี่ยนแปลงไป ☐ ไม่พบ ☐ พบ	
19. มี email จำนวนมากส่งเข้ามา มีลักษณะเนื้อหาไม่ปกติ ☐ ไม่พบ ☐ พบ	
20. พบการส่งข้อมูลในเส้นทางที่ไม่เคยใช้ ☐ ไม่พบ ☐ พบ	
21. เครื่องคอมพิวเตอร์หรืออุปกรณ์เกิดอาการผิดปกติพร้อมกันจำนวนมาก ☐ ไม่พบ ☐ พบ	
22. พบการข้ามขั้นตอนการมาตรฐานการทำงานที่ตั้งไว้ ด้านการสำรองข้อมูล หรือ การ fail over ☐ ไม่พบ ☐ พบ	
23. มีเครื่องที่ส่งข้อมูลจำนวนมากผ่านเครือข่าย โดยผู้ใช้ไม่ได้ทำงานที่แปลกไป ☐ ไม่พบ ☐ พบ	
24. พบการใช้พลังงานจาก data center มากกว่าปกติ ☐ ไม่พบ ☐ พบ	
25. พบการแจ้งปัญหาขัดข้องในระบบจากผู้ใช้งานจำนวนมากพร้อม ๆ กัน ☐ ไม่พบ ☐ พบ	

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคามกรณีมีความเสี่ยงระดับปานกลางขึ้นไป

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.ค่าใช้จ่ายในการฟื้นฟูคืนสู่สภาพปกติ.....

.....

.....

๑๔.รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์.....

.....

.....

๑๕.สรุปสาระสำคัญของเหตุการณ์.....

.....

.....

ทั้งนี้เพื่อให้เกิดความต่อเนื่องของการปฏิบัติงาน ในสภาวะวิกฤต และ สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ และไม่ให้เกิดผลกระทบต่อ ด้านต่าง ๆ กับหน่วยงานภายในโรงพยาบาล เช่น การให้บริการผู้ป่วย เป็นต้น จึงให้หน่วยงานต่างๆ ปฏิบัติตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ โรงพยาบาลสะบ้าย้อย (Cyber Incident Response Plan) ในกรณีที่เกิดสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ

ประกาศ ณ วันที่ ๖ กุมภาพันธ์ ๒๕๖๘



(นายสุภัทร ฮาสุวรรณกิจ)
ผู้อำนวยการโรงพยาบาลสะบ้าย้อย