ประเด็นคำถาม – คำตอบ แนบท้าย คู่มือการตอบสนองภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย (Cyber Incident Response Plan Handbook) พ.ศ. ๒๕๖๔

ประเด็นคำถาม	ความเห็น / คำตอบ
ผู้ทำหน้าที่รับผิดชอบควรได้รับการอบรมเพื่อฝึกฝนและทดสอบการดำเนินงานจะมีการสอบทานและวัดผลอย่างไร ตามมาตรฐาน Exercise Programs for IT Plans and Capabilities Special Publication ๘๐๐-๘๔ ของ Nation Institute of Standards and Technology (NIST) หรือระบุ มาตรฐานที่เทียบเท่า หรือที่ได้เห็นชอบตาม OIC หรือสากล	บริษัทสามารถพัฒนาและกำหนดเกณฑ์การวัดผลเพื่อประเมินหรือทดสอบระดับความสามารถหรือประสิทธิภาพของทีมรับมือได้เป็นการภายในตามความเหมาะสม อย่างไรก็ตาม บริษัทสามารถพิจารณาแนวทางในการประเมินผลหรือสอบทานทีมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ตามแนวทางดังต่อไปนี้ 1. Exercise Programs for IT Plans and Capabilities Special Publication 800-84 ของ Nation Institute of Standards and Technology (NIST) ซึ่งจะแนะนำให้ใช้ตาราง Master Scenario Events List (MSEL) เพื่อประเมินการดำเนินการเพื่อรับมือและตอบสนองที่คาดหวังกับการดำเนินการจริง <u>ตัวอย่าง</u> **Master Scenario Events List** | Event # | MSEL Key Event Description | Expected Actions Resulting from MSEL Event | Objectives | | --- | --- | --- | --- | | 1 | ***Example*** The [*insert organization name*] experiences electronic intrusions on critical information systems. | ***Example*** Supporting Injects: Day 1, 0900 - 1700 ■ Activate cyber incident response team ■ Implement Cyber Intrusion Response Plan ■ Notify and coordinate with customers and other stakeholders ■ Take actions to clean infected systems | ***Example*** ■ Familiarize staff with responsibilities under Cyber Intrusion Response Plan ■ Validate Cyber Intrusion Response Plan ■ Coordinate with Federal cyber entities, customers, and key stakeholders | | 2 | ***Example*** The Homeland Security Advisory System threat level has been raised from an Orange "High" to a Red "Severe" risk of terrorist attack. | ***Example*** Supporting Injects: Day 1, 1000 - 1200 ■ Activate emergency response teams ■ Initiate backup procedures for all mission critical IT systems ■ Relocate essential personnel to alternate facilities ■ Coordinate with the White House and other departments and agencies to inform them of decision to relocate operations | ***Example*** ■ Familiarize staff with emergency activation and notification procedures ■ Validate IT contingency plans and procedures ■ Validate relocation plans and procedures ■ Validate coordination and communications processes with key stakeholders | | 3 | ***Example*** A large explosion occurs outside the Office Building. | ***Example*** Supporting Injects: Day 1, 1200-1700 ■ All commercial power to building has been cut ■ The site reports that some data communications links have failed ■ Facility managers report the building cannot be repaired | ***Example*** ■ Validate IT contingency plans and procedures ■ Identify whether additional contingency plans need to be developed ■ Examine plans to restore data center operations | | 4 | ***Example*** Possible threat of terrorism to alternate facility. | ***Example*** Supporting Injects: Day 2, 1000-1200 ■ Explore options if alternate facility is disabled ■ Prioritize IT system recovery | ***Example*** ■ Identify whether additional contingency plans should be developed for alternate facility | 2. Computer Security Incident Handling Guide Special Publication 800-61 Revision 2 ซึ่งกล่าวถึงในหัวข้อ Post-Incident Activity ซึ่งทั้งใน "แนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓" และ "คู่มือการตอบสนองภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย (Cyber Incident Response Plan Handbook)" พ.ศ. ๒๕๖๔ ได้ให้ตัวอย่างการประเมินผลหรือสอบทานการดำเนินการทีมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ซึ่งอ้างอิงจากเอกสาร Computer Security Incident Handling Guide Special Publication 800-61 Revision 2 โดยจะเป็นลักษณะให้ดำเนินการ

ประเด็นคำถาม	ความเห็น / คำตอบ
	จัดประชุมฝ่ายหรือหน่วยงานที่มีความเกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เพื่อให้ทุกหน่วยงานที่เกี่ยวข้องได้มีการแลกเปลี่ยนข้อมูล รวมทั้งทบทวนเหตุภัยคุกคาม และวิธีการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น เพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งจัดสรรทรัพยากร และเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต ทั้งนี้ ในเอกสารทั้งสองฉบับดังกล่าวข้างต้น ได้ให้ตัวอย่างประเด็นคำถามที่บริษัทสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
จากแผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ขั้นตอนจากกล่อง “รับแจ้งเหตุการณ์” ไม่ ควรมีลูกศรวิ่งต่อที่ไปกล่อง “ควบคุม ความเสียหาย” เนื่องจากยังไม่ได้ผ่าน การวิเคราะห์ความผิดปกติ	Flow การดำเนินการเพื่อรับมือตามแผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ บริษัทสามารถดำเนินการในบางขั้นตอนควบคู่กันไปได้ โดยควรพิจารณาตามความเหมาะสมของสถานการณ์ที่เกิดขึ้น เช่น เมื่อได้รับแจ้งเหตุการณ์ที่เกิดขึ้นแล้วพิจารณาอาการในเบื้องต้นอาจสามารถเข้าควบคุมความเสียหายในเบื้องต้นก่อนได้ โดยไม่จำเป็นต้องรอผลวิเคราะห์ความผิดปกติซึ่งอาจจะใช้เวลานาน ดังนั้น เพื่อจำกัดความเสียหายและผลกระทบจึงสามารถพิจารณาเข้าระงับเหตุและควบคุมความเสียหายได้ในเบื้องต้น หรือในบางกรณี Incident ที่เกิดขึ้นอาจจะไม่ได้มีเหตุการณ์เดียว บริษัทอาจจะต้องเร่งรีบในการดำเนินการรับมือและควบคุมความเสียหายในเบื้องต้นก่อน โดยหลังจากได้รับการแจ้งเหตุและดำเนินการวิเคราะห์ อาจจะต้องพิจารณาจัดลำดับความสำคัญให้สอดคล้องตามความต้องการของธุรกิจก่อน ซึ่งอาจจะไม่ได้รอบันทึกข้อมูลภัยคุกคามแล้วเสร็จแล้วจึงเข้าดำเนินการควบคุมความเสียหาย เป็นต้น
กิจกรรมหลักเพื่อให้บรรลุผลลัพธ์ (Key Activities) ในหัวข้อที่ ๑) การจัดเตรียมเครื่องมือ และสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ “โปรแกรมเข้ารหัส (Encryption Software)” ไม่น่าจะเกี่ยวข้องในขั้นตอนนี้ หรือช่วยขยายความในเอกสารให้ ชัดเจนว่าใช้โปรแกรมเข้ารหัสเพื่อวัตถุประสงค์ใด	โปรแกรมเข้ารหัส (Encryption Software) มีวัตถุประสงค์เพื่อปกป้องข้อมูลความลับ และการยืนยันความถูกต้องของข้อมูล โดยมีรายละเอียดดังนี้ ๑.ข้อมูลเกี่ยวกับ Incident บางครั้งถูกเข้ารหัส ซึ่งอาจมีความจำเป็นต้องใช้ Encryption Software ในการ Decrypt ข้อมูลเพื่อดำเนินการตรวจสอบ ๒. ใช้เพื่อยืนยันความถูกต้องของข้อมูล เช่น ใช้คำนวณค่า hashing ข้อมูลต้นทาง - ปลายทางเพื่อตรวจสอบความถูกต้องของข้อมูล ๓. ใช้เวลาที่มีความจำเป็นต้องส่งข้อมูลเกี่ยวกับ Incident ให้กับหน่วยงานภายนอก เช่น หน่วยงานบังคับใช้กฎหมาย เป็นต้น จึงมีความจำเป็นต้องเข้ารหัสข้อมูล อย่างไรก็ตาม การจัดเตรียมเครื่องมือและสิ่งอำนวยความสะดวกอื่นๆ เพื่อรับมือและตอบสนองต่อเหตุภัยคุกคาม

ประเด็นคำถาม	ความเห็น / คำตอบ
	ทางไซเบอร์ขึ้นอยู่กับการพิจารณาความเหมาะสมและความจำเป็นที่สอดคล้องกับระดับความเสี่ยงของบริษัท
แหล่งข้อมูลการแจ้งเตือน ทางบริษัทอาจไม่ได้มีทั้งหมดตามตัวอย่าง	แหล่งข้อมูลการแจ้งเตือนที่ปรากฏใน Handbook เป็นเพียงตัวอย่างเพื่อให้บริษัทพิจารณานำไปปรับใช้ในการตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่าย ไม่ได้เป็นข้อกำหนดหรือบังคับว่าต้องมีเครื่องมือตรวจจับทุกอย่างตามที่กำหนดใน Handbook อย่างไรก็ตาม ข้อแนะนำ หรือตัวอย่างที่ปรากฏใน Handbook ฉบับนี้ บริษัทสามารถนำไปพิจารณาปรับใช้ได้ตามความเหมาะสม สำนักงานมุ่งหวังให้เนื้อหา ข้อมูลต่างๆ หรือตัวอย่างใน Handbook เป็นประโยชน์ในการนำไปปรับใช้
เพิ่มตัวอย่างรายการทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งในตัวอย่างในคู่มือเป็นข้อมูลเกี่ยวกับ log ซึ่งเกี่ยวข้องกับ IT เท่านั้น ไม่แน่ใจว่ารายการทรัพย์สินควรครอบคลุมมากกว่าในส่วนงาน IT หรือไม่	บริษัทสามารถพิจารณาตัวอย่างเพิ่มเติมได้ตามแนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. ๒๕๖๔ ซึ่งจะมีตัวอย่างตารางทะเบียนทรัพย์สินสารสนเทศทั้ง Hardware Software และ Data ทั้งนี้ ทรัพย์สินสารสนเทศประเภทข้อมูลนอกจากข้อมูล Log ตามตัวอย่างแล้ว สามารถพิจารณาข้อมูลที่จัดเก็บในรูปอิเล็กทรอนิกส์อื่นๆ เพิ่มเติมได้ เช่น ข้อมูลการพัฒนาผลิตภัณฑ์ ข้อมูลแผนธุรกิจ ข้อมูลการลงทุน ข้อมูลลูกค้า ข้อมูลคู่ค้า ข้อมูลทางการเงิน ข้อมูลการฉ้อฉล ข้อมูลผลการทดสอบสภาวะวิกฤต ข้อมูลการบริหารจัดการค่าสินไหมทดแทน ข้อมูลการร้องเรียน ข้อมูลการรับประกันภัย ข้อมูลเกี่ยวกับความเสี่ยงของบริษัท ข้อมูลแผนประกันภัยต่อ เป็นต้น เพื่อให้บริษัททราบและระบุได้ว่าข้อมูลที่มีความสำคัญของบริษัทถูกจัดเก็บอยู่ที่ใดบ้าง และ flow ของข้อมูลในการเข้าถึงหรือใช้ข้อมูลเพื่อให้สามารถดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูลเหมาะสมสอดคล้องกับระดับความสำคัญของข้อมูลในแต่ละประเภท
เสนอให้มีการจัด session และ lesson leant เพื่อป้องกันหรือเพิ่มเติมในส่วนที่ action ในการรับมือภัยคุกคามต่อไป	เห็นด้วยตามเสนอ ซึ่งใน Handbook ฉบับนี้ ได้กำหนดขั้นตอน Post-Incident Activity อย่างชัดเจน โดยหัวใจสำคัญเพื่อให้เกิดการเรียนรู้เพื่อปรับปรุงการดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ทั้งนี้ ในคู่มือการตอบสนองภัยคุกคามทางไซเบอร์ สำหรับบริษัทประกันภัย (Cyber Incident Response Plan Handbook) และแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓ ได้ให้ตัวอย่างประเด็น

ประเด็นคำถาม	ความเห็น / คำตอบ
	คำถามที่บริษัทสามารถปรับใช้เพื่อประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
ขั้นตอนเพิ่มเติม : การดูแลรักษาหลักฐานทางดิจิทัล (Digital Evidence Handling Guide) บริษัทสามารถพิจารณาในเรื่องดังกล่าวหรือไม่ก็ได้ใช่หรือไม่ (เป็น optional ไม่ได้บังคับว่าต้องทำ)	การดูแลรักษาหลักฐานทางดิจิทัล จะครอบคลุมในเรื่อง การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ Incident การจัดเก็บหลักฐานด้วยเครื่องมือที่เหมาะสม และข้อควรระวัง การตรวจสอบความถูกต้องของหลักฐาน การวิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident และการจัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย โดยมุ่งหวังให้บริษัทมีความระมัดระวังตั้งแต่ขั้นตอนการจัดเก็บจนถึงการวิเคราะห์ และนำเสนอผลการวิเคราะห์เพื่อให้มั่นใจได้ว่า ข้อเท็จจริงที่ได้จากการวิเคราะห์มีความถูกต้องแม่นยำ รวมถึงการที่หลักฐานทางดิจิทัลจะสามารถถูกนำไปใช้ได้ในชั้นศาลหากมีความจำเป็น อย่างไรก็ตาม ขั้นตอนนี้ยังคงเป็นส่วนหนึ่งในการดำเนินการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ เพื่อเป็นประโยชน์ในการค้นหาสาเหตุที่แท้จริงของภัยคุกคามที่เกิดขึ้น และการนำหลักฐานไปใช้ในทางด้านกฎหมายต่อไป โดยสำนักงานมุ่งหวังให้บริษัทมีการพิจารณาดำเนินการตามความจำเป็น