คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)

แนวปฏิบัติ
เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย พ.ศ. ๒๕๖๓

สารบัญ

บทนำ

ในปี ๒๕๕๕ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ได้ออกแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) ของบริษัทประกันภัย โดยแนวทางปฏิบัติฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อมูลและให้แนวทางในเบื้องต้นแก่บริษัทประกันภัยเกี่ยวกับการกำหนดนโยบายและมาตรฐานในการดำเนินธุรกิจอย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งระบบงานที่สำคัญต่างๆ (Critical Business Functions) ที่ต้องกลับมาดำเนินการได้ภายในระยะเวลาที่เหมาะสม เพื่อให้บริษัทสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และปฏิบัติตามภาระผูกพันที่มีต่อผู้เอาประกันภัยได้หากเกิดเหตุการณ์ที่ทำให้ธุรกิจไม่สามารถดำเนินงานได้ตามปกติ เช่น เหตุการณ์ความไม่สงบทางการเมือง ภัยธรรมชาติ อุทกภัย อัคคีภัย โรคระบาด เป็นต้น

ปัจจุบันสภาพแวดล้อมในการดำเนินธุรกิจได้มีการเปลี่ยนแปลงไปจากอดีตเป็นอย่างมาก ธุรกิจประกันภัยต้องเผชิญความท้าทายจากสภาวะการแข่งขันที่เพิ่มสูงขึ้น และเทคโนโลยีที่เติบโตรวดเร็วแบบก้าวกระโดด ทำให้บริษัทต้องปรับตัวให้ทันต่อการเปลี่ยนแปลง และสามารถดำเนินธุรกิจต่อไปได้ หลายบริษัทได้นำเทคโนโลยีเข้ามาช่วยในการดำเนินงานทั้งในส่วนของ Front Office และ Back Office เพื่อเป็นการลดต้นทุนในการดำเนินงาน รวมทั้งเพิ่มประสิทธิภาพในการดำเนินงาน ทั้งในด้านความรวดเร็วของการให้บริการ การพัฒนาผลิตภัณฑ์ และบริการลูกค้า เช่น การขายผลิตภัณฑ์ประกันภัยผ่านสื่ออิเล็กทรอนิกส์ ระบบการจัดเก็บข้อมูลลูกค้า ระบบการพิจารณารับประกันภัย ระบบการเงินและบัญชี ระบบการจ่ายค่าสินไหมทดแทน และการจ่ายผลประโยชน์ตามกรมธรรม์ประกันชีวิต ซึ่งการนำเทคโนโลยีเข้ามามีบทบาทในการดำเนินธุรกิจมากขึ้นนั้นย่อมมีความเสี่ยงแฝงมาด้วย **ไม่ว่าจะเป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์**ที่ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมากซึ่งอาจก่อให้เกิดความเสียหายและมีผลกระทบต่อความเชื่อมั่นของลูกค้า ส่งผลให้การดำเนินธุรกิจในปัจจุบันต้องเผชิญกับความเสี่ยงทั้งทางตรงและทางอ้อมที่สำคัญในหลายด้าน แม้บริษัทจะมีการควบคุมหรือการบริหารจัดการความเสี่ยงที่ดีเพื่อป้องกันหรือลดโอกาสและผลกระทบที่อาจจะเกิดขึ้น อย่างไรก็ตามยังคงมีความเสี่ยงที่ไม่สามารถป้องกันหรือหลีกเลี่ยงได้ ดังนั้น การปรับตัวเพื่อให้มีความพร้อมและสามารถรับมือกับสถานการณ์ที่อาจจะเกิดขึ้นโดยที่ธุรกิจยังสามารถดำเนินงานได้อย่างต่อเนื่องและลูกค้าหรือผู้มีส่วนได้เสียได้รับผลกระทบน้อยที่สุดจึงนับเป็นความท้าทายที่สำคัญประการหนึ่งในการดำเนินงาน

ในการนี้ เพื่อให้แนวทางในการกำกับดูแล เรื่อง การบริหารความต่อเนื่องทางธุรกิจของบริษัทประกันภัยเหมาะสมสอดคล้องกับบริบท รูปแบบในการดำเนินธุรกิจ และความเสี่ยงที่บริษัทต้องเผชิญในปัจจุบัน รวมทั้งเป็นแนวทางให้บริษัทสามารถกำหนดแนวทางในการรับมือ หรือตอบสนองต่อเหตุการณ์ที่เกิดขึ้นแล้วส่งผลให้การดำเนินงานหยุดชะงักได้อย่างมีประสิทธิภาพเหมาะสมกับความเสี่ยงของแต่ละบริษัท สำนักงาน คปภ. จึงได้มีการทบทวนแนวปฏิบัติ BCM และ BCP ของบริษัทประกันภัย ฉบับปี ๒๕๕๕ **โดยประเด็นหลักสำคัญในการทบทวนสำนักงานจะให้ความสำคัญกับความเสี่ยงด้านภัยคุกคามทางไซเบอร์ เป็นความเสี่ยงสำคัญที่ทุกบริษัทควรมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และครอบคลุมถึงแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan)** ซึ่งแนวปฏิบัติแบบนี้มุ่งเน้นที่จะให้มุมมองที่เป็นประโยชน์ในด้านการเตรียมความพร้อม การพัฒนาบุคลากร การกำหนดแผนในการตอบสนองหรือรับมือของบริษัทประกันภัย เพื่อช่วยบรรเทาความรุนแรงและผลกระทบที่จะเกิดขึ้นกับบริษัท อีกทั้งยังช่วยให้บริษัทสามารถตัดสินใจได้อย่างรวดเร็ว และถูกต้อง เมื่ออยู่ในสภาวะวิกฤต โดยไม่ทำให้การดำเนินธุรกิจเกิดการหยุดชะงัก รวมถึงกระทบต่อผู้ที่มีส่วนได้เสียของบริษัทน้อยที่สุด

วัตถุประสงค์

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ได้จัดทำแนวทางปฏิบัตินี้ขึ้นเพื่อเป็นข้อมูลและให้แนวทางในเบื้องต้นเกี่ยวกับการกำหนดนโยบายและมาตรฐานในการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัย โดยเฉพาะอย่างยิ่งระบบงานที่สำคัญต่างๆ (Critical Business Functions) ของบริษัทที่ต้องกลับมาดำเนินการได้ภายในระยะเวลาที่เหมาะสม รวมถึงเป็นข้อมูลและให้แนวในเบื้องต้นเกี่ยวกับการกำหนดนโยบายและมาตรฐานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ของบริษัทประกันภัย เพื่อให้บริษัทป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และปฏิบัติตามภาระผูกพันที่มีต่อผู้เอาประกันภัยได้หากเกิดเหตุการณ์ที่ทำให้ธุรกิจไม่สามารถดำเนินงานได้ตามปกติ

นิยามคำศัพท์

การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)	หมายถึง แนวทางในการกำหนดนโยบาย มาตรฐาน และกระบวนการทำงานของบริษัทเพื่อให้มั่นใจว่ากรณีที่มีเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติเกิดการหยุดชะงัก ระบบงานที่สำคัญจะยังสามารถดำเนินการได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม
แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)	หมายถึง แผนงานที่เป็นลายลักษณ์อักษรที่กำหนดขั้นตอน และกระบวนการทำงานในการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ เพื่อช่วยให้ธุรกิจสามารถดำเนินงานได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก
แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP)	หมายถึง แผนงานที่เป็นลายลักษณ์อักษรที่กำหนดถึงวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์
ระบบงานที่สำคัญ (Critical Business Function: CBF)	หมายถึง ระบบงานซึ่งหากเกิดการหยุดชะงัก จะส่งผลกระทบต่อการให้บริการผู้เอาประกันภัย ผู้มีส่วนได้เสีย การดำเนินธุรกิจ ชื่อเสียงฐานะและผลการดำเนินงานของบริษัทประกันภัยอย่าง มีนัยสำคัญ
การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	หมายถึง การวิเคราะห์และวัดผลกระทบทางธุรกิจหรือความสูญเสียทางธุรกิจที่เกิดจากการหยุดชะงักของการดำเนินธุรกิจ
ระยะเวลาการหยุดชะงักที่ยอมได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD)	หมายถึง ระยะเวลาที่ระบบงานหยุดชะงักที่ยอมรับได้สูงสุดหากเกินกำหนดเวลานี้แล้วจะไม่สามารถทำให้ธุรกิจกลับคืนสู่สภาพปกติได้
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives: RTO)	หมายถึง ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้กระบวนการกลับคืนสู่สภาพปกติหลังเกิดเหตุการณ์
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)	หมายถึงจุดเวลาเป้าหมายที่ข้อมูลจะได้รับการกู้กลับคืนมา เพื่อให้กิจกรรมเดินหน้าต่อไปได้ หรือ สามารถยอมรับการสูญหายของข้อมูลได้นานที่สุดเท่าไหร่
กลยุทธ์การเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Recovery Strategy)	หมายถึง แนวทางในการตอบสนองต่อการหยุดชะงักการดำเนินงานของระบบงานที่สำคัญ
แผนการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Business Recovery Plan: BRP)	หมายถึง แผนงานที่เป็นลายลักษณ์อักษร ที่เตรียมไว้ในการฟื้นฟูกระบวนการทางธุรกิจหลังจากที่มีเหตุฉุกเฉินเกิดขึ้น ช่วยให้การดำเนินธุรกิจกลับมากลับคืนสู่ปกติ
แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP)	หมายถึง แผนงานที่เป็นลายลักษณ์อักษร ที่เตรียมไว้ในการกู้ระบบในกรณีที่ระบบงานล่ม ช่วยให้สามารถกู้คืนระบบและการทำงานกลับคืนสู่ปกติ
ศูนย์ปฏิบัติงานสำรอง (Alternate Sites)	หมายถึง สถานที่ปฏิบัติงานทดแทน และดำเนินธุรกิจเมื่อเกิดการหยุดชะงักการดำเนินงาน เมื่อสถานที่ปฏิบัติงานหลักไม่สามารถดำเนินการได้ตามปกติ ซึ่งควรจะอยู่ห่างจากสำนักงานใหญ่พอที่จะไม่ได้รับผลกระทบเดียวกันและไม่ควรใช้สาธารณูปโภคจากแหล่งเดียวกัน โดยศูนย์ปฏิบัติงานสำรองควรจะรองรับสถานการณ์ได้ในระยะยาวและพร้อมใช้งาน

ภัยคุกคามทางไซเบอร์	หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือ ระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือ ส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง
ไซเบอร์	หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่าย คอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และ ระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

ภาพรวมกรอบแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ

การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)

๑. หน้าที่และความรับผิดชอบของคณะกรรมการของบริษัทประกันภัย

๒. นโยบายที่เกี่ยวข้องกับการบริหารความต่อเนื่องทางธุรกิจ

สำหรับกรณีเกิดเหตุการณ์ที่ไม่ใช่ภัยคุกคามทางไซเบอร์ที่ทำให้การดำเนินงานของบริษัทหยุดชะงัก

๒.๑ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)

- ขั้นตอนการปฏิบัติงานและผู้รับผิดชอบ
- ทรัพยากรที่จำเป็นสำหรับการปฏิบัติงาน
- การจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site)
- การกำหนดแนวทางในการสำรองข้อมูล (Backup System)
- การกำหนดผู้ที่มีอำนาจตัดสินใจหรืออนุมัติประกาศใช้แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

สำหรับเหตุการณ์ภัยคุกคามทางไซเบอร์

๒.๒ แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP)

- การเตรียมความพร้อม (Preparation)
- การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)
- การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์
- การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Post Cyber Incident Activity)

๓. กระบวนการที่เกี่ยวข้องในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

๓.๑ การวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักการดำเนินงานที่สำคัญ

๓.๒ การกำหนดเป้าหมายการเรียกคืนการดำเนินงานให้กลับสู่สภาพการดำเนินงานปกติ (Recovery Objectives)

๓.๓ แผนการติดต่อสื่อสาร (Communications)

๓.๔ การฝึกอบรม (Trainings)

๓.๕ การทดสอบและทบทวนแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Testing and Reviewing)

๔. การรายงานต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.)

๑. หน้าที่และความรับผิดชอบของคณะกรรมการบริษัท

คณะกรรมการบริษัท เป็นผู้รับผิดชอบในการกำหนดนโยบายในการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) พร้อมทั้งจัดสรรทรัพยากรและงบประมาณเพื่อรองรับการดำเนินงานแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอ โดยการบริหารความต่อเนื่องทางธุรกิจถือเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงแบบองค์รวมของบริษัท สอดคล้องกับประกาศว่าด้วย หลักเกณฑ์ วิธีการ และเงื่อนไขในการกำกับการบริหารความเสี่ยงแบบองค์รวม และการประเมินความเสี่ยงและความมั่นคงทางการเงินของบริษัทประกันชีวิต/ประกันวินาศภัย และ ประกาศว่าด้วย หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย นอกจากนี้ ควรจัดให้มีการติดตามการปฏิบัติงานให้เป็นไปตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และ แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan : CIRP)

คณะกรรมการบริษัท มีหน้าที่และความรับผิดชอบในการกำกับดูแลการบริหารความต่อเนื่องทางธุรกิจ อย่างน้อยดังต่อไปนี้

(๑) กำกับดูแลให้มีการกำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM) และเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวมของบริษัท (Enterprise Risk Management: ERM) เป็นลายลักษณ์อักษร โดยต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๒) กำกับดูแลให้มีการนำนโยบายการบริหารความต่อเนื่องทางธุรกิจที่ผ่านการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความต่อเนื่องทางธุรกิจ และการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพของนโยบายดังกล่าวอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๓) กำกับดูแลให้มีการกำหนดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ รวมทั้งแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (CIRP) ที่อาจเกิดขึ้น และควรพิจารณาให้เหมาะสมสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยี ความเสี่ยงที่เกี่ยวข้อง และภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น

(๔) กำกับดูแลให้มีการรายงานต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายอย่างน้อยปีละ ๑ ครั้ง ในเรื่องดังต่อไปนี้

- ผลการบริหารความต่อเนื่องทางธุรกิจของบริษัท ที่บรรจุแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ รวมทั้งแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (CIRP)
- ผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
- ข้อมูลหรือปัญหาที่เกี่ยวข้องกับปัญหาหรือเหตุการณ์ที่ทำให้การดำเนินธุรกิจหยุดชะงัก รวมถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริษัท

(๕) กำกับดูแลให้มีการจัดอบรมให้ความรู้แก่ คณะกรรมการบริษัท ผู้บริหาร และบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านการบริหารความต่อเนื่องทางธุรกิจ และการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้มีความรู้ความเข้าใจและทักษะที่เพียงพอต่อการกำกับดูแลหรือปฏิบัติงานในส่วนที่เกี่ยวข้อง

ทั้งนี้ คณะกรรมการบริษัทสามารถมอบหมายคณะกรรมการชุดย่อยหรือคณะทำงาน เป็นผู้รับผิดชอบงานในการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านการบริหารความต่อเนื่องทางธุรกิจ และด้านการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดย**คณะกรรมการชุดย่อยหรือคณะทำงานที่ได้รับมอบหมาย บริษัทควรพิจารณาให้มีผู้บริหารที่มีความรู้ หรือมีประสบการณ์ที่เกี่ยวข้อง ด้านใดด้านหนึ่งดังต่อไปนี้**

(๑) ด้านการบริหารความต่อเนื่องทางธุรกิจ เช่น หัวหน้าหน่วยงานบริหารความเสี่ยง เป็นต้น

(๒) ด้านการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ เช่น หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ และหัวหน้าหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศหรือที่เกี่ยวข้อง เป็นต้น

๒. นโยบายที่เกี่ยวข้องกับการบริหารความต่อเนื่องทางธุรกิจ

บริษัทประกันภัย ควรกำหนด**นโยบายการบริหารความต่อเนื่องทางธุรกิจ** ซึ่งประกอบด้วย **แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง** ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ รวมทั้งมี**แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์** ให้เหมาะสมสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ รวมทั้งความเสี่ยงที่เกี่ยวข้องและการใช้บริการจากผู้ให้บริการภายนอก ทั้งนี้ บริษัทควรพิจารณาความสอดคล้องในการกำหนดแผนกับผลการวิเคราะห์และประเมินความเสี่ยงของเหตุการณ์ภัยคุกคามที่อาจส่งผลกระทบให้การดำเนินงานหยุดชะงักเป็นสำคัญ

นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy) สอดคล้องกับนโยบายการบริหารความเสี่ยงแบบองค์รวมของบริษัท โดยนโยบายดังกล่าวต้องแสดงให้เห็นถึงโครงสร้างองค์กร หน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารความต่อเนื่องทางธุรกิจ และแนวทางในการบริหารความต่อเนื่องทางธุรกิจ <u>ทั้งนี้ นโยบายการบริหารความต่อเนื่องทางธุรกิจอย่างน้อยควรครอบคลุมในเรื่องดังต่อไปนี้</u>

- **การกำหนดหน้าที่และความรับผิดชอบในการบริหารความต่อเนื่องทางธุรกิจ ที่ครอบคลุมทั้งในด้านการบริหารความต่อเนื่องในการดำเนินงาน (Operation) และในด้านการรับมือภัยคุกคาม (Cyber Incident) และตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์**
- **การวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักการดำเนินงานที่สำคัญ**
- **การกำหนดเป้าหมายสำหรับการเรียกคืนการดำเนินงานให้กลับสู่สภาพการดำเนินงานปกติ**
- **การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)**
- **การจัดทำแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP)**

โดยการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP) มีรายละเอียดอย่างน้อย ดังต่อไปนี้

<u>๒.๑ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)</u>

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หมายถึง แผนงานที่กำหนดเป็นลายลักษณ์อักษร แสดงถึงขั้นตอนการดำเนินการเพื่อรองรับเหตุการณ์ที่ทำให้การดำเนินงานตามปกติของบริษัทหยุดชะงัก ครอบคลุมทุกงานและระบบงานที่สำคัญของบริษัท ตลอดจนงานที่ใช้บริการจากผู้ให้บริการภายนอก (Service Provider) โดยควรพิจารณาให้ครอบคลุมเหตุการณ์ที่อาจส่งผลกระทบให้การดำเนินงานหยุดชะงัก ซึ่งรวมถึงกรณีเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยแผน BCP ควรได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย รวมทั้งทบทวนหรือปรับปรุงให้เป็นปัจจุบันเสมอ โดยควรทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ หลังจากบริษัทได้ประกาศใช้แผน BCP แล้ว **<u>ศูนย์รับแจ้งเหตุเคลม หรือ ศูนย์บริการลูกค้า</u>**ของบริษัทต้องสามารถดำเนินการได้อย่างต่อเนื่อง

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ควรมีรายละเอียดอย่างน้อย ดังนี้

๑) ขั้นตอนการปฏิบัติงานและผู้รับผิดชอบ เพื่อให้บริษัทสามารถกลับมาดำเนินงานสำคัญได้ตามระยะเวลาที่กำหนดหลังจากที่การดำเนินงานหยุดชะงัก บริษัทต้องกำหนดหน้าที่และความรับผิดชอบของผู้ปฏิบัติงานแต่ละรายอย่างชัดเจน และจัดให้มีการสื่อสารและซักซ้อมความเข้าใจถึงหน้าที่ที่ต้องปฏิบัติ ตลอดจนกำหนดรายละเอียดวิธีปฏิบัติงานที่สามารถเข้าใจและปฏิบัติตามได้

๒) ทรัพยากรที่จำเป็นสำหรับการปฏิบัติงาน บริษัทควรจัดสรรทรัพยากรที่จำเป็นต่อการปฏิบัติงาน เช่น การจัดหาหรือกำหนดบุคลากรที่จะปฏิบัติงานแทนทั้งระดับพนักงานและผู้บริหาร แหล่งเงินทุน อุปกรณ์สำนักงาน คอมพิวเตอร์ เครื่องใช้สำนักงาน ระบบเทคโนโลยีสารสนเทศ เป็นต้น

๓) การจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site) เพื่อป้องกันผลกระทบจากเหตุฉุกเฉินที่เกิดขึ้นในบริเวณกว้าง บริษัทควรจัดให้มีศูนย์ปฏิบัติงานสำรองเพื่อรองรับการดำเนินการอย่างต่อเนื่อง โดยที่ศูนย์ปฏิบัติงานสำรองดังกล่าวไม่ควรใช้สาธารณูปโภคจากแหล่งเดียวกันกับสถานที่ปฏิบัติงานหลัก และควรมีระยะที่ตั้งห่างจากสถานที่ปฏิบัติงานหลัก รวมทั้งควรจัดให้สามารถรองรับปริมาณงานสำคัญหรือการเกิดเหตุฉุกเฉินเป็นระยะเวลานานได้ นอกจากนี้ ศูนย์ปฏิบัติงานสำรองควรมีความพร้อมที่จะปฏิบัติงานทันทีที่เกิดเหตุฉุกเฉินหรือภายในระยะเวลาที่กำหนดไว้ (Recovery Time Objectives: RTO) **<u>ในกรณีที่บริษัทไม่สามารถจัดให้มีศูนย์ปฏิบัติงานสำรองได้ บริษัทควรมีแนวทางการปฏิบัติงานอื่นทดแทนที่สามารถรองรับการดำเนินงานอย่างต่อเนื่องได้</u>** เพื่อให้มั่นใจว่าศูนย์ปฏิบัติงานสำรองหรือแนวทางการปฏิบัติงานอื่นที่ทดแทนนั้นสามารถรองรับการดำเนินงานอย่างต่อเนื่องได้ในระบบงานที่สำคัญ โดยควรพิจารณาผลจากการวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักการดำเนินงานที่สำคัญ เพื่อให้มั่นใจว่าศูนย์ปฏิบัติงานสำรองสามารถรองรับการดำเนินงานอย่างต่อเนื่องได้ในระบบงานที่สำคัญ

๔) การกำหนดแนวทางในการสำรองข้อมูล (Backup System) เพื่อทำให้สามารถกู้คืนข้อมูลได้ถูกต้องและรวดเร็ว สอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) โดยต้องกำหนดความถี่ในการสำรองข้อมูลให้เป็นไปตามนโยบายที่กำหนดใน BCP

๕) การกำหนดผู้ที่มีอำนาจตัดสินใจหรืออนุมัติประกาศใช้แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ผู้ที่ทำหน้าที่ตัดสินใจหรืออนุมัติประกาศใช้แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ควรเป็นคณะกรรมการบริษัท หรือ กรรมการผู้จัดการ (CEO) หรือ เป็นผู้ที่ได้รับมอบอำนาจจากคณะกรรมการหรือกรรมการผู้จัดการให้ปฏิบัติหน้าที่แทน

<u>๒.๒ แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP)</u>

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ เป็นแผนงานที่กำหนดเป็นลายลักษณ์อักษร แสดงถึงวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ โดยควรสอดคล้องและเชื่อมโยงกับแผน BCP ของบริษัท ครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญ โดยได้รับอนุมัติจากคณะกรรมการของบริษัท หรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ นอกจากนี้ แผน CIRP ควรครอบคลุมตั้งแต่กระบวนการจัดการการเตรียมความพร้อมในการรับมือและการตอบสนองต่อเหตุการณ์ และการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ทั้งนี้ บริษัทควรพิจารณา**<u>จัดให้มีบุคลากรหรือทีมงาน</u>**ที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Team) โดยอย่างน้อย **ทีมรับมือและตอบสนองฯ ควรประกอบด้วยบุคลากรดังต่อไปนี้**

๑) บุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้นภายในองค์กร โดยควรจัดให้มีช่องทางในการรายงาน เช่น ช่องทางอีเมล โทรศัพท์ โทรสาร แบบฟอร์มบนเว็บไซต์ ระบบที่รวบรวมข้อมูลอัตโนมัติ และการสื่อสารทางตรง เป็นต้น

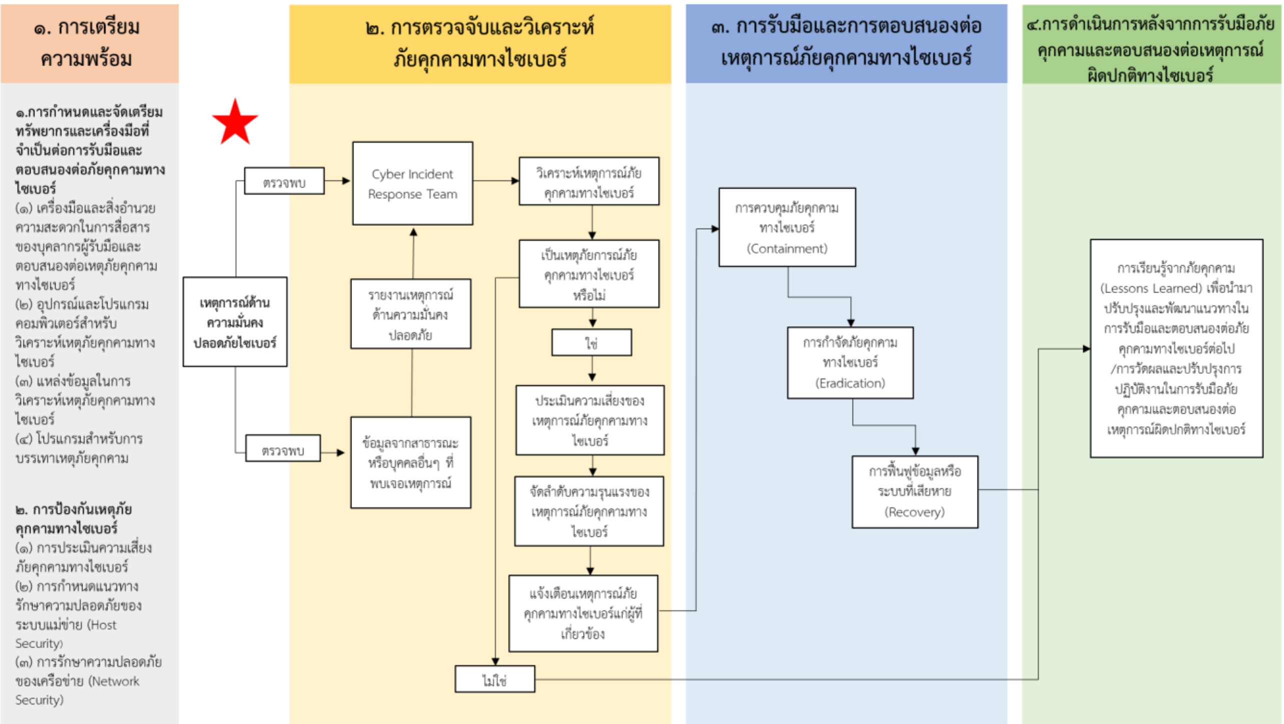
๒) บุคลากรที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ทั้งนี้ บริษัทอาจพิจารณาเพิ่มจำนวนบุคลากรที่มีความเชี่ยวชาญตามความเหมาะสมของความเสี่ยงและระดับความรุนแรงของภัยคุกคามที่อาจเกิดขึ้น โดยอาจจัดหาบุคลากรที่มีทักษะทางเทคนิคที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ เช่น การตรวจจับภัยคุกคาม การวิเคราะห์โปรแกรมไม่ประสงค์ดี (Malware) การบริหารจัดการระบบและเครือข่าย การสนับสนุนทางเทคนิค เป็นต้น

ทั้งนี้ บริษัทสามารถดำเนินการใช้บริการ Security Operation Center (SOC) จากผู้ให้บริการภายนอกได้ ในการปฏิบัติงานดังกล่าวได้ โดยบริษัทควรกำหนดเงื่อนไขให้ผู้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัยของบริษัท พร้อมทั้งมีการประเมินความความเสี่ยงจากการใช้ผู้ให้บริการภายนอก รวมถึงตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ควรระบุขั้นตอนการรับมือและตอบสนองเหตุการณ์ที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยอย่างน้อยควรครอบคลุม

- ชื่อแผน วัตถุประสงค์ และขอบเขต
- โครงสร้างของการบังคับบัญชาในการดำเนินการตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ และผู้ปฏิบัติหน้าที่แทนในกรณีผู้ปฏิบัติหน้าที่หลักที่ได้รับมอบหมายไม่สามารถปฏิบัติงานได้ รวมถึงบันทึกการบันทึกการเปลี่ยนแปลงของแผน
- รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรมเครือข่าย เป็นต้น
- ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ และแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ
- ขั้นตอนการกู้คืนระบบ โดยจัดทำเป็นเอกสารหรือ คู่มือ หรือ Checklist เพื่อควบคุมกระบวนการให้เป็นไปตามขั้นตอนที่กำหนดไว้

แผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์



ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

บริษัทควรกำหนดขั้นตอนการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ สามารถแบ่งได้เป็น ๔ ขั้นตอนอย่างน้อย ดังนี้

๑. การเตรียมความพร้อม (Preparation)

๑.๑ การกำหนดและจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกำหนดแนวทางการติดต่อสื่อสารอย่างเป็นระบบ บริษัทควรมีเครื่องมือสำหรับทำการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ และมีการกำหนดแนวทางรักษาความปลอดภัยของระบบแม่ข่าย (Host Security) ควรติดตั้งโปรแกรม (Software) เพื่อตรวจจับและยับยั้งโปรแกรมไม่ประสงค์ดี (Malware) ภายในระบบเทคโนโลยีสารสนเทศขององค์กร ระบบปฏิบัติการ ระบบโปรแกรมที่ใช้งาน (Application) และระบบโปรแกรมงานสำหรับลูกค้า (Application Clients) รวมถึงมีกระบวนการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและระบบงานที่สำคัญขององค์กร โดยอย่างน้อยเครื่องมือและทรัพยากรที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ควรครอบคลุม ดังนี้

(๑) เครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์

(๑.๑) รายชื่อและช่องทางการติดต่อสำหรับสมาชิกภายในทีมรับมือภัยคุกคามทางไซเบอร์ รวมถึงหน่วยงานอื่นๆ ที่จำเป็นต่อการรับมือเหตุทั้งภายในและภายนอกองค์กร (รายชื่อผู้รับผิดชอบหลักและรายชื่อสำรอง) เช่น ฝ่ายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ฝ่ายบริหารความเสี่ยง ฝ่ายสื่อสารองค์กร ฝ่ายทรัพยากรบุคคล และคู่ค้าของบริษัท เป็นต้น

(๑.๒) รายชื่อและช่องทางการติดต่อสำหรับทีมหรือหน่วยงานภายในองค์กรในกรณีที่มีการยกระดับความรุนแรงของเหตุการณ์ โดยสามารถให้ความช่วยเหลือหรือรับช่วงต่อในการรับมือได้ทันท่วงทีหลังได้รับการแจ้ง

(๑.๓) ช่องทางการรายงานเหตุการณ์ เช่น หมายเลขโทรศัพท์ อีเมล แบบรายงานออนไลน์ และระบบการส่งข้อความทันทีที่มีเหตุการณ์กระทบต่อความมั่นคงปลอดภัย เพื่อให้ผู้ใช้งานทั่วไปสามารถใช้ในการรายงานเหตุการณ์ที่เข้าข่ายจะเป็นภัยคุกคามทางไซเบอร์

(๑.๔) ระบบในการรายงานและติดตามข้อมูล สถานะการดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(๑.๕) โปรแกรมเข้ารหัส (Encryption Software) เพื่อเพิ่มความปลอดภัยในการสื่อสารทั้งระหว่างภายในและภายนอกองค์กร

(๑.๖) ห้องประชุม (War Room) สำหรับการสื่อสารและประสานงานระหว่างส่วนกลางและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจเป็นห้องประชุมที่ใช้งานชั่วคราวเพื่อการรับมือภัยคุกคามทางไซเบอร์ก็ได้

(๑.๗) สถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการจัดเก็บหลักฐาน ข้อมูลและพยานวัตถุอื่นๆ ที่สำคัญ

(๒) อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๒.๑) เครื่องคอมพิวเตอร์ หรืออุปกรณ์สำรองข้อมูล ที่ใช้งานเพื่อการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log Files) หรือสร้าง Disk Image หรือบันทึกข้อมูลเหตุการณ์ที่เกี่ยวข้องอื่นๆ โดยเฉพาะ

(๒.๒) เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ (Packet Sniffers and Protocol Analyzers) เพื่อเก็บข้อมูลและวิเคราะห์การดักจับข้อมูลที่ผ่านไปมาระหว่างเครือข่าย

(๒.๓) เครื่องคอมพิวเตอร์สำรอง เซิร์ฟเวอร์ และอุปกรณ์เครือข่ายที่สามารถใช้ทดแทนเครื่องคอมพิวเตอร์หรืออุปกรณ์หลักได้ ซึ่งสามารถใช้เพื่อสำหรับสนับสนุนการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๒.๔) อุปกรณ์ที่ใช้ในการรวบรวมหลักฐาน เช่น โน้ตบุ๊ก กล้องดิจิตอล เครื่องบันทึกเสียง แบบบันทึกข้อมูลผู้ครอบครองพยานหลักฐาน เป็นต้น เพื่อเก็บหลักฐานสำหรับการดำเนินการทางกฎหมาย

(๓) แหล่งข้อมูลในการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Analysis Resources)

(๓.๑) รายการพอร์ตช่องทางการแลกเปลี่ยนข้อมูลผ่านอินเตอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ (Port Lists) ตั้งแต่พอร์ตที่ใช้งานทั่วไปจนถึงพอร์ตที่เสี่ยงต่อการถูกโจมตี

(๓.๒) เอกสารหรือคู่มือการใช้งานของระบบปฏิบัติการ แอพพลิเคชั่น โปรโตคอลที่ใช้ในการสื่อสารระหว่างเครื่องคอมพิวเตอร์ ซอฟต์แวร์สำหรับตรวจจับการบุกรุก และซอฟต์แวร์ป้องกันไวรัส

(๓.๓) แผนผังเครือข่ายและรายการทรัพย์สินทางสารสนเทศที่สำคัญ เช่น ฐานข้อมูล เป็นต้น

(๓.๔) ค่าปกติ (Current Baseline) ของระบบ เครือข่าย และแอพพลิเคชั่น

(๓.๕) ค่า hash ของไฟล์ที่มีความสำคัญ เพื่อเพิ่มความเร็วในการวิเคราะห์ การตรวจสอบ และกำจัดภัยคุกคามที่เกิดขึ้น

(๔) ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม

ไฟล์ disk image ของระบบปฏิบัติการ (OS) และแอพพลิเคชั่น (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ

๑.๒ การป้องกันเหตุภัยคุกคามทางไซเบอร์ (เครือข่าย ระบบ และแอพพลิเคชั่น)

สิ่งสำคัญที่สุดในการป้องกันเหตุภัยคุกคามทางไซเบอร์ คือ การลดจำนวนเหตุภัยคุกคามให้เหลือน้อยที่สุด เพื่อลดผลกระทบต่อการดำเนินงานของบริษัท หากบริษัทมีมาตรการการรักษาความมั่นคงปลอดภัยที่ไม่เพียงพออาจทำให้เกิดเหตุภัยคุกคามมากจนเกินขีดความสามารถในการจัดการของบริษัท ซึ่งส่งผลให้การรับมือและตอบสนองกับเหตุภัยคุกคามที่เกิดขึ้นล่าช้าและไม่มีประสิทธิภาพ อาจส่งผลกระทบทางธุรกิจที่รุนแรงต่อบริษัทได้

การป้องกันเหตุภัยคุกคามทางไซเบอร์ ควรครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) การประเมินความเสี่ยงภัยคุกคามทางไซเบอร์

บริษัทควรทำการประเมินความเสี่ยง เพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัย โดยควรระบุเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบหรือสร้างความเสียหายต่อระบบงาน ข้อมูลสำคัญ และการดำเนินงานขององค์กร

ทั้งนี้ ควรประเมินความเสี่ยงรวมทั้งผลกระทบที่เกิดขึ้นจริงในระหว่างการเกิดเหตุอย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินผลกระทบและมูลค่าความเสียหายที่แท้จริง และเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามทางไซเบอร์ต่อไป

(๒) การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Host Security)

ระบบแม่ข่าย (Host) ควรกำหนดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีมาตรฐาน รวมทั้งการปิดช่องโหว่และทำการแพตช์ระบบอย่างเหมาะสม นอกจากนี้ ควรมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น รวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของบริษัท และได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ

(๓) การรักษาความปลอดภัยของเครือข่าย (Network Security)

ระบบการรักษาความมั่นคงปลอดภัยของเครือข่ายควรตั้งค่าให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาต รวมทั้งอุปกรณ์เครือข่ายทั้งหมดของบริษัทที่เชื่อมต่อกับเครือข่ายภายนอก

<u>๒. การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)</u>

การรวบรวมข้อมูลและตรวจวิเคราะห์จากระบบงานที่มีช่องโหว่จากการโจมตีทางไซเบอร์ภายในองค์กร ควรมีเครื่องมือในการชี้วัดและเฝ้าระวังภัยคุกคามทางไซเบอร์จากหลายแหล่งที่มา โดยอย่างน้อยต้องมีการจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (Access Log) และบันทึกการดำเนินงาน (Activity Log) และทำการแจ้งเตือนแก่ผู้เกี่ยวข้องเมื่อพบเหตุการณ์ภัยคุกคามทางไซเบอร์

(๑) รูปแบบของการโจมตีหรือภัยคุกคามที่มีโอกาสเกิดขึ้นหรือพบเห็นบ่อยครั้ง

(๑.๑) การโจมตีหรือภัยคุกคามที่เกิดจากสื่อบันทึกข้อมูลที่สามารถถอดหรือเคลื่อนย้ายได้หรืออุปกรณ์ต่อพ่วง เช่น มัลแวร์ที่แพร่กระจายเข้าระบบงานจากแฟลชไดรฟ์ USB ที่ติดมัลแวร์

(๑.๒) การโจมตีเพื่อทำให้ระบบประสิทธิภาพลดลง เช่น การโจมตีแบบ DDoS เพื่อทำให้ไม่สามารถให้บริการได้ เป็นต้น

(๑.๓) การโจมตีผ่านเว็บไซต์หรือระบบงานบนเว็บไซต์ เช่น การโจมตีด้วยวิธี Cross Site Scripting เพื่อขโมยข้อมูล หรือ การเปลี่ยนเส้นทางไปยังเว็บไซต์ที่มีการโจมตีผ่านช่องโหว่ของ Web Browser และติดตั้งมัลแวร์ไว้ และการโจมตีผ่านทางข้อความหรือเอกสารแนบในอีเมล เป็นต้น

(๑.๔) การโจมตีที่เข้าข่ายการปลอมแปลงตัวตน เช่น การปลอมตัว (Spoofing) เพื่อหลอกลวงและควบคุมระบบ การโจมตีโดยการปลอมตัวเป็นบุคคลอื่นเพื่อแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้งานระบบ (Man in the Middle Attack) และการโจมตีโดยส่งคำสั่ง SQL ผ่านทางระบบงานบนเว็บไซต์เพื่อไปโจมตีระบบฐานข้อมูล (SQL Injection) เป็นต้น

(๑.๕) ภัยคุกคามที่เกิดจากผู้ใช้งานละเมิดนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร เช่น การติดตั้งโปรแกรมที่นำไปสู่การรั่วไหลข้อมูลสำคัญของบริษัท หรือผู้ใช้งานทำกิจกรรมที่ผิดกฎหมายผ่านระบบงานเทคโนโลยีสารสนเทศของบริษัท เป็นต้น

(๑.๖) อุปกรณ์คอมพิวเตอร์หรือสื่อต่างๆ สูญหาย เช่น เครื่องโน้ตบุค แทบเล็ต โทรศัพท์มือถือหรือสิ่งที่ใช้ยืนยันตัวตนซึ่งเป็นทรัพย์สินของบริษัทที่สูญหายหรือถูกขโมย

(๒) <u>สัญญาณการเกิดเหตุภัยคุกคาม</u> สามารถติดตามได้จากช่องทางอย่างน้อยดังต่อไปนี้

(๒.๑) สัญญาณแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์ สามารถตรวจสอบได้จากระบบดังต่อไปนี้

• ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) ใช้ในการระบุเหตุการณ์ที่น่าสงสัยว่าอาจเป็นภัยคุกคามและบันทึกข้อมูลที่เกี่ยวข้อง รวมถึง

วันที่และเวลาที่ตรวจพบการโจมตี ประเภทของการโจมตี ที่อยู่ IP ต้นทางและปลายทาง และชื่อผู้ใช้งาน โดยส่วนใหญ่ระบบ IDPS จะระบุกิจกรรมที่เป็นอันตรายโดยใช้ลักษณะเฉพาะของการโจมตี (attack signature) ดังนั้น ข้อมูลลักษณะเฉพาะของการโจมตีจะต้องได้รับการอัพเดตอย่างสม่ำเสมอ เพื่อให้สามารถตรวจพบการโจมตีรูปแบบใหม่ได้ ทั้งนี้ ระบบ IDPS สามารถเกิดการแจ้งเตือนที่ผิดพลาดได้ (false positive) โดยแจ้งว่ามีกิจกรรมที่เป็นอันตรายกำลังเกิดขึ้น แต่ในความจริงยังไม่เกิด ดังนั้น นักวิเคราะห์ระบบจึงควรตรวจสอบข้อมูลแจ้งเตือนจาก IDPS ด้วยตนเอง และทบทวนรายละเอียดหรือรวมรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลอื่นๆ ประกอบการวิเคราะห์

• ระบบบริหารจัดการข้อมูลและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) ช่วยในการตรวจจับและทำการแจ้งเตือนจากการวิเคราะห์ที่ได้จากข้อมูลบันทึกเหตุการณ์ (Log data)

• ซอฟแวร์ป้องกันไวรัส (Antivirus Software) เพื่อป้องกันและตรวจจับไวรัสหรือมัลแวร์ในรูปแบบต่างๆ แล้วแจ้งเตือนและป้องกันไม่ให้เกิดการแพร่กระจายที่ระบบแม่ข่าย รวมทั้งเพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพในการป้องกันควรมีการอัพเดตลักษณะเฉพาะของการโจมตีอยู่เสมอ

• ซอฟแวร์ตรวจสอบความถูกต้องของไฟล์เพื่อตรวจสอบการเปลี่ยนแปลง หรือการแก้ไขที่เกิดขึ้นกับไฟล์ที่มีความสำคัญในระหว่างเกิดเหตุภัยคุกคาม (File Integrity Checking Software)

• การใช้บริการเฝ้าระวังภัยคุกคามจากผู้ให้บริการภายนอก (Third-Party Monitoring Services)

(๒.๒) ข้อมูลบันทึกเหตุการณ์ ควรจัดเก็บข้อมูลดังต่อไปนี้เป็นอย่างน้อย

• ข้อมูลบันทึกเหตุการณ์ของระบบปฏิบัติการ การบริการ และแอพพลิเคชั่น (Operating System, Service and Application Logs)

• ข้อมูลบันทึกเหตุการณ์ของอุปกรณ์เครือข่าย (Network Device Logs)

• ข้อมูลบันทึกการเคลื่อนไหวของข้อมูลในเครือข่าย (Network Flow Logs)

(๒.๓) ข้อมูลสาธารณะ (Publicly Available Information)

• ข้อมูลของช่องโหว่หรือจุดอ่อนใหม่ จากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น TI-CERT National-CERT หรือช่องทางอื่นๆ ที่มีการอัพเดตและเผยแพร่ข้อมูลภัยคุกคามสู่สาธารณะ เป็นต้น

(๒.๔) บุคคล (People)

• บุคลากรภายในบริษัท เช่น ผู้ใช้งานระบบ ผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย เจ้าหน้าที่ด้านความมั่นคงปลอดภัย เป็นต้น ซึ่งเมื่อได้รับรายงานแล้วจะต้องมีการตรวจสอบข้อเท็จจริงหรือยืนยันข้อมูลทุกครั้ง

• บุคคลภายนอกบริษัท เช่น รายงานจากผู้ใช้งานภายนอกถึงหน้าเว็บไซต์ที่ไม่สามารถใช้งานได้ เป็นต้น โดยบริษัทควรมีขั้นตอนในการรับรายงานและตรวจสอบข้อมูลอย่างละเอียดถี่ถ้วน

(๓) การวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ ควรครอบคลุมอย่างน้อยดังต่อไปนี้

(๓.๑) การจัดทำข้อมูลเครือข่ายและระบบ (Profile Network and System) เพื่อให้สามารถระบุการเปลี่ยนแปลงที่เกิดขึ้นจากการเข้าถึงหรือใช้งานเครือข่ายและระบบงานจากปกติได้ เช่น การวัดปริมาณการใช้งาน bandwidth ของเครือข่ายและบันทึกข้อมูลระดับการใช้งานเฉลี่ยและระดับสูงสุดในแต่ละช่วงเวลาเพื่อตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติของเครือข่าย

(๓.๒) การศึกษาและเข้าใจพฤติกรรมตามปกติของระบบ เครือข่าย และแอพพลิเคชั่น เพื่อช่วยในการสังเกตพฤติกรรมที่ผิดปกติ โดยการตรวจสอบบันทึกเหตุการณ์ และการแจ้งเตือนด้านความมั่นคงปลอดภัย เพื่อให้มีความคุ้นเคยและจะช่วยให้การสังเกตเหตุการณ์และการแจ้งเตือนที่ผิดปกติได้เร็วและแม่นยำมากยิ่งขึ้น

(๓.๓) การจัดทำนโยบายการเก็บรักษาบันทึกเหตุการณ์ (Log Retention Policy)

(๓.๔) การตรวจสอบความสัมพันธ์ของเหตุการณ์ภัยคุกคาม (Event Correlation) โดยการตรวจสอบข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่ายเพื่อหาความเชื่อมโยง เพื่อนำประกอบการพิจารณาว่ามีเหตุภัยคุกคามเกิดขึ้นจริงหรือไม่

(๓.๕) การตั้งเวลาเครื่องแม่ข่ายให้เป็นมาตรฐานเดียวกัน

(๓.๖) การจัดทำเอกสาร หรือฐานข้อมูล ที่ใช้เพื่ออ้างอิงสำหรับการดำเนินการวิเคราะห์ข้อมูลภัยคุกคาม

(๓.๗) การเปิดใช้งานโปรแกรมสำหรับดักจับภัยคุกคาม (Packet Sniffer) เพื่อบันทึกหรือเก็บข้อมูลการจราจรภายในเครือข่ายของบริษัทเพิ่มเติม

(๔) การลงบันทึกข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident Documentation)

การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม จะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น หน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม โดยการบันทึกข้อมูลเกี่ยวกับสถานะของเหตุการณ์ภัยคุกคามและข้อมูลที่เกี่ยวข้อง อาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูล เช่น ระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์ ขั้นตอนการจัดการ และแก้ไขเหตุภัยคุกคามเพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม

ในการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- ชื่อเหตุการณ์ภัยคุกคาม
- วันที่บันทึกเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้
- ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม
- ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม
- ข้อมูลติดต่อสำหรับผู้ที่เกี่ยวข้องอื่นๆ เช่น เจ้าของระบบงาน ผู้ดูแลระบบงาน เป็นต้น
- ประเภทของเหตุการณ์ภัยคุกคาม
- วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม
- วันที่และเวลาพบเหตุภัยการณ์คุกคาม
- วันที่และเวลารายงานเหตุภัยคุกคาม
- รายละเอียดเหตุการณ์ภัยคุกคาม
    - สิ่งที่เกิดขึ้น
    - เกิดขึ้นอย่างไร
    - ทำไมจึงเกิดขึ้น
    - การประเมินทรัพย์สินสารสนเทศที่เสียหาย
    - ผลกระทบทางธุรกิจ
    - ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม
- การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ
- รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม
- สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม

โดยมีตัวอย่างของแบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ดังนี้

<table>
<tr><th colspan="6">แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="2">ชื่อเหตุการณ์ภัยคุกคาม</td><td colspan="2"></td><td>หมายเลขของเหตุการณ์ภัยคุกคาม</td><td></td></tr>
<tr><td colspan="2">วันที่บันทึกเหตุการณ์ภัยคุกคาม</td><td colspan="2"></td><td>หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้</td><td></td></tr>
<tr><th colspan="4">ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม</th><th colspan="2">ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="2">ชื่อ – นามสกุล</td><td colspan="2"></td><td>ชื่อ – นามสกุล</td><td></td></tr>
<tr><td colspan="2">หน่วยงาน</td><td colspan="2"></td><td>โทรศัพท์</td><td></td></tr>
<tr><td>โทรศัพท์</td><td></td><td>อีเมล</td><td></td><td>อีเมล</td><td></td></tr>
<tr><td colspan="4">วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม</td><td colspan="2"></td></tr>
<tr><td colspan="4">วันที่และเวลาพบเหตุภัยการณ์คุกคาม</td><td colspan="2"></td></tr>
<tr><td colspan="4">วันที่และเวลารายงานเหตุภัยคุกคาม</td><td colspan="2"></td></tr>
<tr><th colspan="6">รายละเอียดเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="6">- สิ่งที่เกิดขึ้น
- เกิดขึ้นอย่างไร
- ทำไมจึงเกิดขึ้น
- การประเมินทรัพย์สินสารสนเทศที่เสียหาย
- ผลกระทบทางธุรกิจ
- ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม</td></tr>
<tr><th colspan="4">การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้</th><th colspan="2">การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้</th></tr>
<tr><td colspan="4"></td><td colspan="2"></td></tr>
<tr><th colspan="4">ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ</th><th colspan="2">รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="4"></td><td colspan="2"></td></tr>
<tr><th colspan="6">สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="6"></td></tr>
</table>

(๕) การจัดลำดับความรุนแรงของเหตุการณ์ภัยคุกคามทางไซเบอร์ ควรคำนึงปัจจัยดังต่อไปนี้

• **ผลกระทบต่อการให้บริการ** และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม โดยควรพิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที

• **ผลกระทบต่อข้อมูล** ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมของบริษัทอย่างไร และส่งผลต่อข้อมูลสำคัญของบริษัท (Sensitive Information) อย่างไร

• **ความสามารถในการฟื้นฟูระบบ** ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถในการฟื้นฟูระบบ

(๖) การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง

ทีมรับมือและตอบสนองฯ ควรดำเนินการแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ ทั้งนี้ บริษัทควรมีข้อกำหนดเกี่ยวกับการแจ้งข้อมูลเหตุภัยคุกคาม ข้อมูลอะไรบ้างที่ต้องรายงาน รายงานต่อใคร และเมื่อใด โดยอย่างน้อยควรกำหนดบุคคลผู้รับรายงาน ข้อมูลที่ต้องรายงาน และเวลาที่ต้องรายงาน รวมถึงหน่วยงานต่างๆ ทั้งภายในและภายนอกที่ต้องได้รับแจ้ง

บุคลากรหรือหน่วยงานที่ควรได้รับการแจ้งเหตุภัยคุกคาม มีดังต่อไปนี้

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือเทียบเท่า (กรณีไม่มีตำแหน่ง CIO)
- ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือเทียบเท่า (กรณีไม่มีตำแหน่ง CISO)
- ทีมรับมือและตอบสนองต่อเหตุการณ์อื่นๆ ของบริษัท
- ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอกบริษัท (ตามความเหมาะสม)
- เจ้าของระบบงาน
- ฝ่ายทรัพยากรบุคคล (สำหรับกรณีที่เกี่ยวข้องกับพนักงาน เช่น การล่วงละเมิดทางอีเมล)
- ฝ่ายสื่อสารองค์กร (สำหรับเหตุการณ์ที่จำเป็นต้องให้การประชาสัมพันธ์)
- ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย)
- TI-CERT

<u>๓. การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์</u>

ประกอบด้วย ๓ ขั้นตอน ได้แก่ การควบคุมภัยคุกคามและจำกัดความเสียหาย (Containment) การกำจัดภัยคุกคาม (Eradication) และการฟื้นฟูระบบ (Recovery) โดยมีรายละเอียดดังนี้

(๑) กำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหายที่เกิดขึ้นจากเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งจะมีความแตกต่างกันไปขึ้นกับลักษณะ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

เกณฑ์ประกอบการพิจารณากำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหายควรพิจารณาอย่างน้อยในเรื่องดังต่อไปนี้

- ความเสียหายที่อาจเกิดขึ้นและการโจรกรรมข้อมูล
- ความจำเป็นในการเก็บรักษาหลักฐาน
- ความพร้อมให้บริการ เช่น การเชื่อมต่อเครือข่าย การให้บริการกับบุคคลภายนอก เป็นต้น
- เวลาและทรัพยากรที่จำเป็นในการดำเนินการ

- ประสิทธิผลของแนวทางในการควบคุมและจำกัดความเสียหาย เช่น การควบคุมบางส่วน หรือการควบคุมทั้งหมด
- ระยะเวลาในการแก้ปัญหา เช่น การแก้ไขปัญหาแบบฉุกเฉินภายใน ๔ ชั่วโมง การแก้ไขปัญหาแบบชั่วคราวภายใน ๒ สัปดาห์ และการแก้ไขปัญหาแบบถาวร เป็นต้น

นอกจากนี้ บริษัทควรเก็บรวบรวมหลักฐานที่เกิดขึ้นระหว่างเกิดเหตุการณ์ภัยคุกคาม เพื่อใช้ในการแก้ไขปัญหาและจัดการเหตุภัยคุกคาม รวมทั้งเพื่อใช้ในกระบวนการทางกฎหมายหากจำเป็น บริษัทควรจัดทำเอกสารรวบรวมหลักฐานทั้งหมดที่ได้ถูกบุกรุกโจมตี รวมถึงระบุขั้นตอนการเก็บรักษาหลักฐานที่เป็นไปตามกฎหมายและระเบียบข้อบังคับ เพื่อให้สามารถใช้เป็นพยานหลักฐานได้ในชั้นศาล นอกจากนี้ ควรมีการบันทึกหลักฐานทุกครั้งหากมีการถ่ายโอนหลักฐานจากบุคคลหนึ่งสู่อีกคน และลงลายมือชื่อกำกับของแต่ละฝ่าย

การจัดทำเอกสารรายละเอียดหลักฐานควรครอบคลุมอย่างน้อยดังนี้

- ข้อมูลระบุพยานหลักฐาน เช่น สถานที่ตั้ง หมายเลขซีเรียล (Serial Number) หมายเลขรุ่น (Model Number) ชื่อเครื่องแม่ข่าย ที่อยู่สำหรับควบคุมการเข้าใช้งานสื่อกลาง (Media Access Control Addresses) และที่อยู่ IP ของคอมพิวเตอร์ เป็นต้น
- ชื่อ-สกุล และหมายเลขโทรศัพท์ของบุคคลที่เก็บรวบรวมหรือดูแลพยานหลักฐานในระหว่างการสอบสวน
- วันที่และเวลาที่มีการดำเนินการกับพยานหลักฐานในแต่ละครั้ง
- สถานที่เก็บหลักฐาน

(๒) การกำจัดภัยคุกคามทางไซเบอร์ (Eradication)

บริษัทควรกำจัดต้นเหตุของเหตุการณ์ที่เป็นอันตรายต่อเครือข่าย ระบบ หรือแอพพลิเคชั่น รวมถึงการกำจัดไฟล์ที่เกี่ยวข้องกับการโจมตีและการปิดช่องโหว่ที่ถูกใช้ในการโจมตี ทั้งนี้ การกำจัดภัยคุกคามมีวิธีที่แตกต่างกันโดยขึ้นกับประเภทของเหตุภัยคุกคาม

ตัวอย่างของวิธีการกำจัดภัยคุกคาม ดังนี้

(๒.๑) การลบมัลแวร์ (Malware) คือ การกักกัน ลบ แทนที่ หรือกู้คืนไฟล์ที่ติดมัลแวร์ ซึ่งโดยส่วนใหญ่ หน่วยงานจะต้องกู้คืนระบบสารสนเทศใหม่โดยการติดตั้งระบบปฏิบัติการ ระบบงาน และข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้ และอาจรวมถึงการอัพเดตข้อมูลคุณลักษณะเฉพาะของโปรแกรมป้องกันไวรัส (antivirus signature) ให้เป็นปัจจุบัน

(๒.๒) การแก้ไขหรือลดผลกระทบจากช่องโหว่ การแก้ไขช่องโหว่สามารถทำได้ด้วยการติดตั้งแพตช์ (Patch) รุ่นล่าสุดของระบบปฏิบัติการและระบบงาน เพื่อป้องกันการใช้งานช่องโหว่ที่เป็นช่องทางการโจมตี ทั้งนี้ หากระบบสารสนเทศไม่สามารถติดตั้งแพตช์ ได้ด้วยเหตุผลทางเทคนิคหรือเหตุผลในการปฏิบัติงาน ให้ลดผลกระทบจากช่องโหว่โดยปรับปรุงการตั้งค่า (configuration) ของระบบสารสนเทศให้สามารถป้องกันหรือจำกัดความเสียหายจากเครื่องแม่ข่ายที่ติดมัลแวร์ หากกรณียังไม่มี patch ให้ใช้วิธีแก้ไขปัญหาหรือลดผลกระทบชั่วคราว

(๒.๓) การปรับปรุงการควบคุมการเข้าถึงผู้ใช้งานและเครือข่าย เช่น การลบบัญชีผู้ใช้งานหรือผู้ดูแลระบบที่ถูกบุกรุก การปรับปรุงการควบคุมการเข้าถึงเครือข่าย เช่น การตั้งค่าของระบบตรวจจับและป้องกันการบุกรุก (IDPS) ไฟร์วอลล์ (firewall) เป็นต้น การปรับปรุงการกำหนดค่าพื้นฐาน (baseline configuration) และการลบกลไกการเข้าถึงอื่นๆ ที่ถูกใช้โดยผู้โจมตี

(๓) การฟื้นฟูระบบ (Recovery)

การฟื้นฟูระบบ เป็นการกู้คืนข้อมูลหรือระบบ เพื่อทำให้ระบบสารสนเทศ ข้อมูล ความมั่นคงปลอดภัยของระบบและเครือข่ายกลับสู่สถานะปกติ ด้วยการติดตั้งระบบปฏิบัติการ ระบบงาน และข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้ พร้อมทั้งมีกลไกติดตามการดำเนินการเพื่อป้องกันการเกิดเหตุภัยคุกคามที่มีความคล้ายคลึงกันขึ้นอีกในอนาคต การฟื้นฟูระบบมีวิธีการที่แตกต่างกันขึ้นอยู่กับประเภทของเหตุภัยคุกคาม เช่น การติดตั้งระบบใหม่จากต้นฉบับหรือติดตั้งจากข้อมูลที่สำรองที่เชื่อถือได้ การเปลี่ยนรหัสผ่านของระบบ การติดตั้งแพตซ์ (Patch) ให้เป็นเวอร์ชั่นปัจจุบัน และการปรับปรุงความมั่นคงปลอดภัยของเครือข่าย เป็นต้น ทั้งนี้ ในกรณีที่การกู้คืนข้อมูลและระบบที่เสียหายเสร็จสิ้น ผู้ดูแลระบบควรทำการยืนยันว่าระบบสามารถกลับมาทำงานได้ตามปกติให้ผู้ที่เกี่ยวข้องทราบ

<u>๔. การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Post Cyber Incident Activity)</u>

๔.๑ การเรียนรู้จากภัยคุกคาม (Lessons Learned)

บริษัทควรมีการเรียนรู้จากเหตุภัยคุกคามที่เกิดขึ้น เพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งจัดสรรทรัพยากรและเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต นอกจากนี้ บริษัทควรจัดให้มีการประชุมของฝ่ายหรือหน่วยงานที่มีความเกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยวัตถุประสงค์ของการประชุมเพื่อให้ทุกหน่วยงานที่เกี่ยวข้องได้มีการแลกเปลี่ยนข้อมูล รวมทั้งทบทวนเหตุภัยคุกคาม และวิธีการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น

ตัวอย่างประเด็นคำถามที่บริษัทสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ เช่น

- เหตุภัยคุกคามที่เกิดขึ้นคืออะไร เกิดขึ้นเมื่อเวลาใดบ้าง
- เจ้าหน้าที่และฝ่ายบริหารสามารถรับมือภัยคุกคามได้ดีเพียงใด การดำเนินการเป็นไปตามขั้นตอนการปฏิบัติงานที่กำหนดไว้หรือไม่
- ข้อมูลอะไรบ้างที่จำเป็นต้องได้รับรายงานภายในระยะเวลาอันสั้น เพื่อเพิ่มประสิทธิภาพในการรับมือและตอบสนองต่อเหตุการณ์
- มีขั้นตอนหรือการดำเนินการใดๆ ที่อาจเป็นอุปสรรคหรือไม่สอดคล้องกับขั้นตอนของการฟื้นฟูระบบหรือไม่
- เจ้าหน้าที่และฝ่ายบริหาร มีแนวทางดำเนินการเพิ่มเติมหรือแตกต่างไปจากเดิม หากเกิดภัยคุกคามที่มีรูปแบบคล้ายคลึงกันเกิดขึ้นในครั้งต่อไป
- การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ สามารถปรับปรุงให้ดีขึ้นได้อย่างไร
- แนวทางการดำเนินการแก้ไข (corrective action) ที่สามารถเพิ่มเติมเพื่อป้องกันภัยคุกคามที่คล้ายคลึงกันในอนาคตได้
- สัญญาณอะไรบ้างที่สามารถนำมาใช้เพื่อตรวจจับภัยคุกคามที่มีลักษณะคล้ายคลึงกันซึ่งอาจเกิดขึ้นในอนาคต
- เครื่องมือหรือทรัพยากรที่มีความจำเป็นต้องได้รับการจัดสรรเพิ่มเติม เพื่อใช้ดำเนินการในการตรวจจับ วิเคราะห์ และบรรเทาเหตุภัยคุกคามที่อาจเกิดขึ้นในอนาคต

๔.๒ การวัดผลและปรับปรุงการปฏิบัติงานในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

(๑) จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่รับมือต่อเดือน/ไตรมาส/ปี

(๒) ระยะเวลาในการรับมือและตอบสนองต่อเหตุการณ์ สามารถวัดได้หลายวิธี เช่น

๑) ระยะเวลาทั้งหมดที่ใช้ในการรับมือและตอบสนอง

๒) ระยะเวลาที่ใช้ในการดำเนินการในแต่ละช่วงของกระบวนการรับมือและตอบสนองในแต่ละขั้นตอน

๓) ระยะเวลาที่ทีมรับมือฯ ใช้ในการตอบสนองหลังจากที่ได้รับรายงานภัยคุกคาม

๔) ระยะเวลาที่ทีมรับมือฯ ใช้ในการรายงานภัยคุกคามต่อผู้บริหาร หรือหน่วยงานภายนอกที่เกี่ยวข้อง เช่น TI-CERT เป็นต้น

(๓) การประเมินกระบวนการรับมือในแต่ละเหตุการณ์ (Objective Assessment) ตัวอย่างของการประเมิน เช่น

- การตรวจทานบันทึกเหตุการณ์ (log) แบบฟอร์ม รายงาน และเอกสารอื่นๆ ที่เกี่ยวข้องกับภัยคุกคาม เพื่อให้การปฏิบัติงานเป็นไปตามขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดไว้
- การระบุว่าสัญญาณการเกิดเหตุภัยคุกคามอะไรบ้างที่บันทึกไว้ เพื่อพิจารณาว่าการบันทึกเหตุการณ์และระบุเหตุภัยคุกคามมีประสิทธิภาพเพียงใด
- การพิจารณาว่าภัยคุกคามที่เกิดขึ้นก่อให้เกิดความเสียหายก่อนที่จะตรวจพบหรือไม่
- การพิจารณาว่ามีการระบุสาเหตุที่แท้จริงของภัยคุกคามไว้หรือไม่ และการระบุช่องทางการโจมตี ช่องโหว่ที่เปิดเผย และลักษณะของระบบ เครือข่าย และแอพพลิเคชั่นที่เป็นถูกโจมตี
- การพิจารณาว่าภัยคุกคามเป็นการเกิดขึ้นอีกครั้งของภัยคุกคามก่อนหน้าหรือไม่
- การประเมินความเสียหายทางการเงินจากภัยคุกคามที่เกิดขึ้น เช่น ข้อมูลและกระบวนการทางธุรกิจที่สำคัญที่ได้รับผลกระทบจากภัยคุกคาม

(๔) การประเมินประสิทธิภาพของทีมรับมือและตอบสนองฯ (Subjective Assessment) บริษัทอาจกำหนดให้มีการประเมินผลการปฏิบัติงานของทีมรับมือและตอบสนองฯ ทั้งในรูปแบบรายบุคคล หรือทั้งทีม รวมทั้งอาจให้เจ้าของระบบงานที่ระบบถูกโจมตีเป็นผู้ทำการประเมินการปฏิบัติหน้าที่ของทีมรับมือและตอบสนองฯ ก็ได้ เพื่อประกอบการพิจารณาว่าประสิทธิภาพของการรับมือให้ผลลัพธ์เป็นที่น่าพอใจหรือไม่

๓. กระบวนการที่เกี่ยวข้องในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

๓.๑ การวิเคราะห์และประเมินผลกระทบต่อการหยุดชะงักการดำเนินงานที่สำคัญ

บริษัทต้องจัดให้มีการประเมินความเสี่ยง และโอกาสที่งานสำคัญจะหยุดชะงักจากเหตุฉุกเฉินที่อาจเกิดขึ้น รวมทั้งวิเคราะห์ผลกระทบทางธุรกิจและประเมินความเสียหายจากการหยุดชะงักของการดำเนินงานที่สำคัญ (Major Operational Disruptions) เพื่อให้บริษัทสามารถกำหนดลำดับความสำคัญของงาน และจัดสรรทรัพยากรในการบริหารการดำเนินธุรกิจอย่างต่อเนื่องได้อย่างมีประสิทธิภาพ โดยบริษัทต้องทำการประเมินความเสี่ยงและวิเคราะห์ผลกระทบทางธุรกิจดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่ส่งผลต่อความเสี่ยงและผลกระทบที่จะเกิดขึ้นนั้น โดยควรครอบคลุมประเด็นดังต่อไปนี้

๑) การระบุระบบงานที่สำคัญต่าง ๆ (Critical Business Function: CBF) บริษัทควรเลือกงานสำคัญที่พิจารณาว่าหากเกิดเหตุการณ์ฉุกเฉินแล้วงานดังกล่าวหยุดชะงัก จะส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการลูกค้า การดำเนินธุรกิจ ผู้มีส่วนได้เสีย สถานะการเงิน ผลการดำเนินงาน หรือชื่อเสียงของบริษัท โดยบริษัทควรกำหนดหลักเกณฑ์ที่ชัดเจนในการพิจารณาความสำคัญของแต่ละระบบงานที่สำคัญ ซึ่งอย่างน้อยควรครอบคลุมถึงการระบุภัยคุกคาม (Threats) ที่อาจจะเกิดขึ้น และช่องโหว่ (Vulnerabilities) ของระบบงานที่สำคัญ

นอกจากนี้ บริษัทควรระบุทรัพยากรที่จำเป็นสำหรับระบบงานที่สำคัญที่จำเป็นต้องใช้สำหรับระบบงานที่สำคัญต่างๆ ในข้อ ๓.๑) เพื่อให้ตอบสนองต่อการหยุดชะงักการดำเนินงานได้ เช่น บุคลากร

เครื่องมืออุปกรณ์ต่างๆ ระบบเทคโนโลยีสารสนเทศ ระบบที่ใช้ในการปฏิบัติงาน (Systems) ข้อมูลและบันทึกต่างๆ (Records & Data) เป็นต้น

๒) การประเมินความเสี่ยง (Risk Assessment) บริษัทต้องทำการประเมินความเสี่ยงและโอกาสที่อาจทำให้งานสำคัญหยุดชะงักอย่างน้อยปีละ ๑ ครั้ง โดยควรประเมินเหตุการณ์ฉุกเฉินที่ทำให้เกิดการหยุดชะงักและก่อให้เกิดความเสียหายต่อธุรกิจหรือการดำเนินงานทางธุรกิจ โดยต้องครอบคลุมถึงเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งอาจส่งผลกระทบทางธุรกิจทั้งในระยะสั้น ระยะปานกลาง และระยะยาว ทั้งนี้ อาจมีการกำหนดสถานการณ์จำลองที่อาจเกิดขึ้นในระดับความรุนแรงและรูปแบบความเสียหายที่แตกต่างกัน และควรกำหนดสถานการณ์วิกฤตร้ายแรง (Worst Case Scenario) ที่อาจเกิดขึ้น เพื่อใช้ในการจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่อง รวมทั้งทำการประเมินข้อจำกัดต่าง ๆ ที่อาจเกิดขึ้นเมื่อเกิดเหตุการณ์ความเสียหายด้วย

นอกจากนี้ บริษัทควรวิเคราะห์กระบวนการควบคุมความเสี่ยงที่มีอยู่ และทำการปรับปรุงกระบวนการรวมถึงจัดหาทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงที่จะทำให้เกิดเหตุการณ์หยุดชะงัก

๓) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) บริษัทควรวิเคราะห์ผลกระทบทางธุรกิจจากเหตุการณ์ที่อาจเกิดขึ้นกับทุกธุรกรรมงานที่สำคัญ เพื่อให้ทราบถึงความสัมพันธ์ของธุรกรรมงานที่สำคัญและผลกระทบจากการหยุดชะงักของระบบงานที่สำคัญนั้น ซึ่งจะทำให้บริษัทสามารถกำหนดระยะเวลาการหยุดชะงักที่ยอมได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) ของแต่ละระบบงาน และลำดับความสำคัญของการดำเนินงานเพื่อให้สามารถจัดสรรทรัพยากรในการเรียกคืนการดำเนินงานได้อย่างมีประสิทธิภาพ โดยวิเคราะห์ผลกระทบทางธุรกิจและควรพิจารณาถึงผลกระทบต่อผู้มีส่วนได้เสียของบริษัททั้งในเชิงปริมาณและเชิงคุณภาพ

ทั้งนี้ การวิเคราะห์ผลกระทบทางธุรกิจ ถือเป็นกิจกรรมที่มีความสำคัญในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP) ควรจัดสรรทรัพยากรและให้เวลาในการวิเคราะห์ และพิจารณาให้ครอบคลุมถึงภัยคุกคามทางไซเบอร์ โดยที่คณะกรรมการบริษัทและผู้บริหารระดับสูงควรให้ความสำคัญ รวมถึงได้รับรายงานผลการวิเคราะห์ผลกระทบทางธุรกิจ

๓.๒ การกำหนดเป้าหมายการเรียกคืนการดำเนินงานให้กลับสู่สภาพการดำเนินงานปกติ (Recovery Objectives)

๑) บริษัทควรกำหนดระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) ของแต่ละระบบงานที่สำคัญ เพื่อจัดลำดับความสำคัญของระบบงานที่สำคัญ และกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives: RTO) โดยระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย และระยะเวลาเป้าหมายในการฟื้นคืนสภาพต้องได้รับความเห็นชอบจากต้องได้รับความเห็นชอบจากคณะกรรมการบริษัท หรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงของบริษัท

๒) บริษัทควรนำผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) มาพิจารณาในการกำหนดกลยุทธ์การเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Recovery Strategy) ที่เหมาะสมเพื่อให้บรรลุเป้าหมายที่ได้กำหนดไว้ โดยต้องจัดสรรทรัพยากรและงบประมาณแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอต่อการดำเนินกลยุทธ์ดังกล่าว

๓.๓ แผนการติดต่อสื่อสาร (Communications)

๑) บริษัทควรกำหนดวิธีการและช่องทางการติดต่อสื่อสารกับผู้ที่เกี่ยวข้องทั้งภายในและภายนอกบริษัท ผู้รับผิดชอบในการสื่อสาร รวมทั้งรายละเอียดข้อมูลที่จะเปิดเผยแก่ผู้เกี่ยวข้องอย่างชัดเจน บริษัทควรจัดทำผังการติดต่อพนักงาน (Call Tree) และผู้เกี่ยวข้องอื่น ๆ รวมถึงข้อมูลที่สามารถใช้ในการติดต่อ โดยบริษัทต้องทำการปรับปรุงรายชื่อและข้อมูลที่ใช้ในการติดต่อให้เป็นปัจจุบันเสมอ นอกจากนี้บริษัทอาจจะเพิ่มช่องทางในการติดต่อสื่อสารในช่องทางอื่น ๆ ได้ เช่น อีเมล โทรศัพท์ Call Center หรือการเผยแพร่ผ่านสื่อต่าง ๆ เป็นต้น

๒) บริษัทควรมีการวางแผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัทให้สอดคล้องกับผลกระทบที่จะเกิด เพื่อสามารถแจ้งเหตุได้ทันท่วงทีและป้องกันไม่ให้เกิดความตื่นตระหนกต่อผู้เอาประกันภัยและผู้ที่มีส่วนเกี่ยวข้อง หากสถานการณ์ที่เกิดขึ้นส่งผลกระทบอย่างมีนัยสำคัญต่อผู้เอาประกันภัยหรือผู้เกี่ยวข้อง บริษัทต้องแจ้งหรือทำการประชาสัมพันธ์ให้ผู้เอาประกันภัยหรือผู้เกี่ยวข้องทราบถึงสถานการณ์ฉุกเฉิน ผลกระทบที่จะเกิดขึ้น ช่องทางที่ลูกค้าหรือผู้เกี่ยวข้องจะสามารถติดต่อใช้บริการหรือสื่อสารกับบริษัทได้ตลอดระยะเวลาที่เกิดสถานการณ์ฉุกเฉิน และมาตรการดำเนินการของบริษัท

๓.๔ การฝึกอบรม (Trainings)

การสื่อสารและการฝึกอบรมเพื่อให้พนักงานทุกคนมีความเข้าใจ และรับทราบแนวทางในการปฏิบัติภายใต้สถานการณ์ฉุกเฉิน บริษัทควรจัดให้มีการฝึกอบรมแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องแก่พนักงาน และผู้ที่มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างสม่ำเสมอ โดยแผนการฝึกอบรมควรครอบคลุมแผนการฝึกอบรมของระบบงานที่สำคัญและโดยรวม รวมถึงความรู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อให้มั่นใจว่าพนักงานและผู้ที่มีส่วนเกี่ยวข้องทุกคนสามารถเข้าใจและรับทราบถึงบทบาทความรับผิดชอบของตนหากเกิดเหตุการณ์หยุดชะงักการดำเนินงาน นอกจากนี้ บริษัทควรจัดให้มีการประชาสัมพันธ์แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยระบุขั้นตอนและวิธีการประชาสัมพันธ์ที่ชัดเจน เพื่อให้พนักงานที่เกี่ยวข้องได้รับทราบ และเพื่อสร้างความเชื่อมั่นให้แก่ผู้เอาประกันภัยและผู้ที่มีส่วนได้เสียว่าบริษัทยังคงดำเนินธุรกิจได้อย่างต่อเนื่อง

ทั้งนี้ บริษัทควรจัดอบรมให้ความรู้เกี่ยวกับ การบริหารความต่อเนื่องทางธุรกิจ และการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง แก่กรรมการบริษัท ผู้บริหารระดับสูงและบุคลากรภายในบริษัท เพื่อสร้างความตระหนัก ความรู้และความเข้าใจ ในการดำเนินการดังกล่าว

๓.๕ การทดสอบและทบทวนแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Testing and Reviewing)

๑) บริษัทควรทบทวนและกำหนดให้มีการทดสอบทั้งแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์อย่างชัดเจน สอดคล้องกับสถานการณ์ในปัจจุบัน นโยบายและกลยุทธ์ของบริษัท และจัดให้มีการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับระบบงานที่สำคัญ และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยงในการเกิดการหยุดชะงักของการดำเนินงานที่มีนัยสำคัญในการดำเนินธุรกิจเกิดขึ้น เพื่อให้มั่นใจว่าแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์มีประสิทธิภาพและสามารถนำไปใช้ปฏิบัติได้จริง บริษัทควรให้ผู้ที่เกี่ยวข้องในทุกระดับมีส่วนร่วมในการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยบริษัทควรจัดให้มีการประเมินประสิทธิภาพจากผู้ประเมินภายนอกที่มีความเชี่ยวชาญ หรือผู้ประเมินภายในที่มีความรู้ความสามารถ และสามารถให้ความเห็นได้อย่างอิสระ ทำหน้าที่ประเมินประสิทธิภาพ และผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องหรือแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ว่าการทดสอบดังกล่าวบรรลุเป้าหมายตามที่บริษัทกำหนดไว้ รวมทั้งผู้เกี่ยวข้องปฏิบัติตามแผนได้อย่างครบถ้วนถูกต้อง และรายงานผลการประเมินต่อคณะกรรมการบริษัทหรือคณะทำงานที่ได้รับมอบหมาย

นอกจากนี้ บริษัทควรจัดให้มีการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ร่วมกับผู้ให้บริการหลัก หากระบบงานที่สำคัญของบริษัทต้องพึ่งพิงบริการจากผู้ให้บริการภายนอกเป็นหลัก ในกรณีที่ไม่สามารถทดสอบแผนร่วมกับ

ผู้ให้บริการหลักได้ บริษัทต้องมั่นใจว่าผู้ให้บริการหลักสามารถให้บริการเมื่อเกิดเหตุการณ์หยุดชะงักได้ หรือบริษัทควรมีแผนแก้ปัญหารองรับทดแทน

๒) การทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ควรครอบคลุมอย่างน้อยในประเด็นดังต่อไปนี้

(๑) วัตถุประสงค์และขอบเขตของการทดสอบ

(๒) สถานการณ์จำลองที่ใช้ทดสอบ

(๓) ระยะเวลาในการทดสอบ

(๔) ขั้นตอนการอพยพพนักงาน (สำหรับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง)

(๕) แผนการสื่อสาร

(๖) การสำรองและการเรียกคืนข้อมูลที่สำคัญ

(๗) ความพร้อมของอาคารสถานที่ และทรัพยากรที่จำเป็นในการดำเนินงาน

(๘) ความพร้อมของศูนย์ปฏิบัติงานสำรองในการดำเนินการได้ภายในเวลาที่กำหนด (สำหรับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง)

๔. การรายงานต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.)

หากระบบงานที่สำคัญมีการหยุดให้บริการเกินกว่าระยะเวลาหยุดดำเนินงานที่ยอมรับได้ (Recovery Time Objective: RTO) ซึ่งบริษัทกำหนดไว้ และส่งผลกระทบต่อการให้บริการผู้เอาประกันภัยและผู้มีส่วนได้เสียกับบริษัทอย่างมีนัยสำคัญ บริษัทต้องแจ้งต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยในโอกาสแรกที่ทำได้และไม่เกิน ๒๔ ชั่วโมง นับแต่ระบบงานที่สำคัญหยุดให้บริการเกินกว่าระยะเวลาหยุดดำเนินงานที่ยอมรับได้ พร้อมทั้งแจ้งรายละเอียดของเหตุการณ์ที่เกิดขึ้น ทั้งนี้ เมื่อระบบงานที่สำคัญดังกล่าวสามารถกลับมาดำเนินการได้ตามปกติแล้ว ให้บริษัทแจ้งสำนักงาน คปภ.รับทราบด้วย โดยแจ้งมาที่ ITRiskMgt@oic.or.th

ทั้งนี้ หากการหยุดชะงักของระบบงาน มีสาเหตุมาจากภัยคุกคามทางไซเบอร์ ให้บริษัทปฏิบัติตามประกาศสำนักงาน คปภ. ว่าด้วย หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย เรื่องการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

Frequently asked Questions: FAQs

คำถาม	คำอธิบาย
๑. บริษัทสามารถแยกนโยบายการบริหารความต่อเนื่องทางธุรกิจออกจากนโยบายการบริหารจัดการความเสี่ยงแบบองค์รวมของบริษัทได้หรือไม่	นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM) ควรเป็นส่วนหนึ่งหรือสอดคล้องกับการบริหารความเสี่ยงแบบองค์รวมของบริษัท ทั้งนี้ แนวปฏิบัติฉบับนี้ไม่ได้ระบุให้นโยบายดังกล่าวต้องปรากฏอยู่ในนโยบายการบริหารความเสี่ยงแบบองค์รวมของบริษัท โดยบริษัทสามารถจัดทำนโยบายแยกกันได้ แต่เนื้อหาต้องมีความสอดคล้องและเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม
๒. การรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ของบริษัท ควรจะรับมือเฉพาะภัยคุกคามทางไซเบอร์ที่ส่งผลต่อความต่อเนื่องทางธุรกิจเท่านั้นหรือไม่	บริษัทควรมีแนวทางการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ทั้งที่ส่งผลหรือไม่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ เนื่องจากไม่มีสิ่งใดที่จะยืนยันได้ว่าภัยคุกคามประเภทหนึ่ง จะไม่สร้างผลกระทบต่อความต่อเนื่องทางธุรกิจ อีกทั้งภัยคุกคามทางไซเบอร์มีในลักษณะการโจมตี และช่องโหว่ที่หลากหลาย บริษัทควรจะมีแนวทางการวิเคราะห์และตอบสนองภัยคุกคามในเบื้องต้น เพื่อจำกัดความเสียหายไม่ให้ลุกลามเกินกว่าจะควบคุมได้
๓. ถ้าบริษัทมี BCM/BCP policy แยก ใน ERM policy สามารถอ้างอิงถึงนโยบายนี้ได้หรือไม่	นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCM) ควรเป็นส่วนหนึ่งหรือสอดคล้องกับการบริหารความเสี่ยงแบบองค์รวมของบริษัท ทั้งนี้ แนวปฏิบัติฉบับนี้ไม่ได้ระบุให้นโยบายดังกล่าวต้องปรากฏอยู่ในนโยบายการบริหารความเสี่ยงแบบองค์รวมของบริษัท โดยบริษัทสามารถจัดทำนโยบายแยกกันได้ แต่เนื้อหาต้องมีความสอดคล้องและเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม
๔. บริษัทจำเป็นต้องมีเครื่องมือในการรับมือภัยคุกคามทางไซเบอร์ตามที่แนวปฏิบัติเสนอแนะมาหรือไม่	ในแนวปฏิบัติฉบับนี้ สำนักงาน คปภ. ได้เสนอแนะเครื่องมือและอุปกรณ์ที่ควรจะมีสำหรับการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ให้แก่ทางบริษัท อย่างไรก็ตาม บริษัทควรพิจารณาจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ให้เหมาะสมสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยี ความเสี่ยงที่เกี่ยวข้อง และภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น
๕. ควรกำหนดให้มีการจัดอบรม กรรมการบริษัทด้วยหรือไม่ เพราะการจัดอบรมเป็นไปค่อนข้างยาก อีกทั้ง กรรมการบริษัท เป็นผู้มีส่วนร่วมในการอนุมัตินโยบาย แต่ไม่ได้เป็นผู้ปฏิบัติตามแผน	คณะกรรมการบริษัทและผู้บริหารระดับสูง ควรได้รับการอบรมให้ความรู้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มีความรู้ความเข้าใจที่เพียงพอต่อการกำกับดูแลทั้งในด้านการบริหารความต่อเนื่องทางธุรกิจ และการรับมือและตอบสนองต่อภัยคุกคาม

คำถาม	คำอธิบาย
BCP หรือดำเนินงานดังกล่าว	ทางไซเบอร์ เพื่อที่จะสามารถกำหนดทิศทางการบริหารความต่อเนื่องทางธุรกิจของบริษัท พร้อมทั้งจัดสรรทรัพยากรและงบประมาณเพื่อรองรับการดำเนินงานแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอ รวมถึงเป็นการสร้างวัฒนธรรมในการบริหารความต่อเนื่องทางธุรกิจให้กับทุกระดับขององค์กร