การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศในองค์กร

Contingency Support Planning for Organization Information Assurance

ณัฐวี อุตกฤษฎ์ (Nattavee Utakrit)*

บทคัดย่อ

การวางแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงของสารสนเทศในองค์กรคือการเตรียมการรับเหตุการณ์ฉุกเฉินที่คุกคามต่อสารสนเทศ ซึ่งองค์กรควรให้ความสำคัญ เพราะบางครั้งองค์กรอาจอยู่ในสภาวะที่ไม่สามารถรองรับและตอบสนองเหตุการณ์ดังกล่าวได้ด้วยการปฏิบัติตามแผนปกติ บทความนี้จึงมุ่งเน้นให้เห็นถึงความสำคัญของการวางแผนรองรับสำหรับเหตุการณ์ฉุกเฉินในองค์กร และยังอธิบายถึงขั้นตอนของการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินโดยพิจารณาตามแนวทางปฏิบัติของ NIST SP 800-34 และส่วนประกอบหลัก 4 ประการของแผนรองรับเหตุการณ์ฉุกเฉินได้แก่ 1) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 2) การวางแผนเพื่อตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด (Incident Response Plan: IRP) 3) การวางแผนฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง (Disaster Recovery Plan: DRP) และ 4) การวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง (Business Continuity Plan: BCP) นอกจากนี้ยังกล่าวถึงประเด็นแนวทางการทดสอบแผนรองรับเหตุการณ์ฉุกเฉิน และในตอนท้ายของบทความนี้ยังได้ยกตัวอย่างการใช้แผนสำหรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศ ขององค์กรต่างๆ ทั้งในประเทศไทยและต่างประเทศอีกด้วย

คำสำคัญ: ความมั่นคงสารสนเทศ, แผนรองรับเหตุการณ์ฉุกเฉิน

Abstract

Contingency planning to support organization information assurance is the preparation for unexpected events that might threaten the security of information resources and assets of an organization. It is important for organizations to consider different scenarios as particular plans in place may not respond effectively to certain problems. This article focuses on the essential areas of information assurance contingency planning and possible solutions. Moreover, it also explains steps of planning derived from NIST SP 800-34 and describes components of this particular planning technique, which are 1) Business Impact Analysis: BIA, 2) Incident Response Plan: IRP, 3) Disaster Recovery Plan: DRP, and 4) Business Continuity Plan: BCP. In addition, possible testing processes of this contingency plan are also described in detail. Finally, examples of real scenarios set in both Thailand and abroad combined with this technique are presented.

Keywords: Information Assurance, Contingency Planning.

1. บทนำ

ทุกวันนี้เราคงไม่อาจปฏิเสธได้ว่าสารสนเทศเป็นทรัพย์สินที่มีค่า มีความสำคัญต่อมนุษย์และต่อองค์กรแทบทุกภาคส่วน การบริหารจัดการสารสนเทศขององค์กรในปัจจุบันได้เปลี่ยนแปลงไปมากจากอดีต มีแผนงานและกิจกรรมหลายอย่างต้องอาศัยคนที่มีทักษะความสามารถคอมพิวเตอร์ เทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่เข้ามามีส่วนร่วมไม่ว่าสารสนเทศนั้นจะอยู่ในรูปของเอกสารทั่วไป หรืออยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ก็ตาม [1] อาทิ การออกแบบโพรโทคอลการเข้ารหัสข้อมูลสารสนเทศที่ปลอดภัย ผู้ออกแบบจะต้องรู้หลักการหรือแนวทางที่ถูกต้องเพื่อให้ระบบมีประสิทธิภาพการรักษาความปลอดภัย [2] ดังนั้นความสัมพันธ์ระหว่าง คอมพิวเตอร์ เทคโนโลยีสมัยใหม่ คน และสารสนเทศ เปรียบเสมือนหุ้นส่วนของการทำงานใน

* คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ทุกๆ องค์กร และธุรกิจ ตั้งแต่การออกแบบ เก็บรวบรวม การดำเนินการ การถ่ายทอด หรือการเก็บรักษา [1] แต่หากมีเหตุการณ์ใด ๆ ก็ตามที่ส่งผลกระทบต่อสิ่งที่กล่าวมาแล้วในลักษณะที่ไม่สามารถให้บริการหรือดำเนินงานในการบริหารจัดการสารสนเทศและธุรกิจต่างๆ ได้ตามปกตินั้น เช่น การเกิดอุทกภัย แผ่นดินไหว หรือไฟไหม้ เป็นต้น สิ่งเหล่านี้ย่อมส่งผลกระทบต่อข้อมูลสารสนเทศเช่นกัน หากเป็นเช่นนี้องค์กรควรจะปฏิบัติตัวอย่างไร

การวางแผนรองรับเหตุการณ์ฉุกเฉิน หรือในบางครั้งมักจะเรียกว่าแผนฉุกเฉิน จึงเป็นการเตรียมจัดทำแผนประเภทหนึ่งขึ้นมาเพื่อรักษาความมั่นคงต่อสารสนเทศ ในสภาวะการทำงาน และเหตุการณ์ที่ไม่เป็นปกติ

“มากกว่าร้อยละ 40 ของธุรกิจที่ไม่มีแผนรองรับเหตุการณ์ร้ายแรง หรือความพินาศ มักจะต้องเลิกธุรกิจไปหลังจากการสูญเสียครั้งใหญ่เกิดขึ้น” [3]

เหตุการณ์ฉุกเฉินส่วนใหญ่เป็นเหตุการณ์ที่มักเกิดขึ้นมาโดยไม่คาดคิดมาก่อน และถึงแม้ว่าบางเหตุการณ์อาจจะพอรู้ตัวมาก่อนล่วงหน้าบ้างแล้วก็ตาม แต่เหตุการณ์ต่างๆ เหล่านี้ก็มักจะไม่ได้ถูกบรรจุไว้ในแผนการดำเนินงานทั่วไปขององค์กรที่จะต้องปฏิบัติเป็นประจำ ทั้งนี้เพื่อไม่ให้เกิดความสับสนหรือทำงานซ้ำซ้อนกับแผนทั่วไปอันจะทำให้เกิดความล่าช้าในระหว่างการดำเนินงานตามแผนยุทธศาสตร์หรือแผนปฏิบัติการทั่วไปขององค์กร ดังนั้นในทางปฏิบัติจึงมักแยกแผนทั้งสองประเภทออกจากกัน แผนฉุกเฉินจึงมีบทบาทต่อเหตุการณ์ฉุกเฉินตั้งแต่ความรุนแรงในระดับต่ำไปจนถึงความรุนแรงในระดับสูง และอาจถึงขั้นที่องค์กรไม่สามารถที่จะดำเนินธุรกิจต่อไปได้ภายในสถานที่ตั้งเดิม ณ ปัจจุบัน ซึ่งอาจจำแนกการเกิดได้เป็น 2 ลักษณะ 1) เกิดจากฝีมือมนุษย์ และ 2) เกิดจากภัยธรรมชาติ [4] ตัวอย่างเหตุการณ์ฉุกเฉินที่เคยเกิดขึ้นมาแล้วในอดีต เช่น เมื่อปี พ.ศ. 2544 เกิดเหตุการณ์ผู้ก่อการร้ายโจมตีอาคารเวิลด์เทรดเซ็นเตอร์ กลางมหานครนิวยอร์กและเหตุการณ์การโจมตีตึกบัญชาการของกระทรวงกลาโหมประเทศสหรัฐอเมริกาในช่วงเวลาไล่เลี่ยกัน [5] หรือเมื่อเดือนธันวาคม พ.ศ. 2555 ได้มีเหตุการณ์ที่รถเครนเกี่ยวสายไฟทำเสาไฟฟ้าหัก รวม 33 ต้น ระบบไฟฟ้าในบริเวณจุดเกิดเหตุถูกตัดขาดเป็นเวลานาน มีมูลค่าเสียหายทั้งสิ้นประมาณ 30 ล้านบาท [6] ซึ่งล้วนแต่เป็นเหตุการณ์ที่เกิดจากฝีมือมนุษย์ทั้งสิ้น

ภาพที่ 1 *ตัวอย่างการภาพเหตุการณ์รถเครนเกี่ยวสายไฟฟ้าทำเสาไฟฟ้าหัก 33 ต้นในกรุงเทพฯ [6]*

สำหรับเหตุการณ์ฉุกเฉินที่เกิดจากภัยธรรมชาติที่รุนแรง เช่น เหตุการณ์มหาอุทกภัยสึนามิในหลายประเทศในแถบเอเชีย ในปี พ.ศ.2544 รวมถึงวิกฤติมหาอุทกภัยของประเทศไทยในปี พ.ศ. 2554 ที่ผ่านมา ในประเด็นนี้ Zetlin [7] ได้เคยกล่าวไว้ว่าความสูญเสียที่เกิดขึ้นกับองค์กร ธุรกิจต่าง ๆ บางครั้งอาจมีสาเหตุจากเหตุการณ์บางเรื่องที่ไม่คาดคิด เช่น ท่อน้ำประปา ที่อยู่เหนือโต๊ะทำงานเกิดรั่วและมีน้ำไหลลงสู่โต๊ะเอกสารและโต๊ะทำงานก็สามารถทำให้เกิดความสูญเสียที่มีมูลค่ามหาศาลได้เช่นกัน ซึ่งทั้งนี้ความสูญเสียที่เกิดขึ้นจากเหตุการณ์คุกคามเล็กน้อยแต่ส่งผลร้ายแรงในเวลาต่อมาได้ ขึ้นอยู่กับมูลค่าของทรัพย์สินที่ถูกคุกคาม [8] เมื่อเหตุการณ์ฉุกเฉินดังตัวอย่างที่กล่าวมาแล้วเกิดขึ้นย่อมส่งผลเสียหายต่อการดำเนินงานขององค์กร และธุรกิจขององค์กร ทั้งในด้านชีวิต ทรัพย์สิน รายได้ และความเชื่อมั่นขององค์กร และความเสียหายนี้อาจส่งผลไปถึงการใช้คอมพิวเตอร์ เทคโนโลยีและการสื่อสารที่เกี่ยวข้องกับองค์กรต่างๆ ที่อาจจะเสียหายตามมาอีกด้วย ซึ่งจะทำให้เกิดปัญหาขึ้น และส่งผลกระทบต่อการจัดการสารสนเทศและการดำเนินธุรกิจจนอาจจะทำให้ธุรกิจขององค์กรหยุดชะงัก ดังนั้นกระบวนการที่จะช่วยทำให้องค์กรสามารถตอบสนองต่อเหตุการณ์ฉุกเฉินนี้ได้ทันท่วงที และมีประสิทธิภาพ เพื่อให้องค์กรสามารถดำเนินงานต่อไปจึงเป็นสิ่งที่สำคัญที่จะสร้างความมั่นคงให้แก่สารสนเทศขององค์กร และกระบวนการบริหารจัดการความมั่นคงสารสนเทศนั้นจะดำเนินการได้ก็ต้องเริ่มจากการวางแผน ซึ่งเป็นแผนที่จัดเตรียมขึ้นมาสำหรับเหตุการณ์ฉุกเฉิน นั่นคือการวางแผนรองรับเหตุการณ์ฉุกเฉิน

2. ส่วนประกอบสำคัญของการวางแผนรองรับเหตุการณ์ฉุกเฉิน

การวางแผนรองรับเหตุการณ์ฉุกเฉินมีชื่อเรียกในภาษาอังกฤษว่า Contingency Planning ในบางครั้งมักจะใช้คำย่อว่า "CP" Whitman และ Mattord [4] อธิบายว่าแผน CP คือ การวางแผนทั้งหมดเพื่อรองรับเหตุการณ์ที่ไม่ใช่เหตุการณ์ปกติทั่วไป โดยการวางแผนจะต้องมีผู้รับผิดชอบ ก็คือทีมงาน CP ที่อาจจะมาจากบุคลากรหลากหลายกลุ่มในองค์กร ซึ่งมีความรู้ ความเชี่ยวชาญมาร่วมกันทำหน้าที่วางแผนในการค้นหา การตรวจสอบ การตอบสนอง และการฟื้นฟูสภาวะการณ์จากเหตุการณ์ที่คุกคามต่อความมั่นคงของสารสนเทศขององค์กร และทรัพย์สินที่เกี่ยวข้อง ภายหลังจากเหตุการณ์ที่ไม่คาดคิดเกิดขึ้นให้กลับสู่สภาวะปกติ โดยเสียค่าใช้จ่ายน้อยที่สุด

แต่อย่างไรก็ตามบริบทหลักของแผนสำหรับเหตุการณ์ฉุกเฉินนั้นจะเป็นไปเพื่อการตอบสนองต่อเหตุการณ์ที่ไม่ปกติซึ่งอาจจะเป็นภัยคุกคามเมื่อเหตุการณ์นั้นเกิดแล้วหรือมีแนวโน้มจะเกิดขึ้นเท่านั้น ไม่ใช้เป็นมาตรการการป้องกันมิให้มีภัยคุกคามเกิดขึ้นได้เลย [4]

การวางแผนรองรับสำหรับเหตุการณ์ฉุกเฉินนั้นมีส่วนประกอบด้วยกัน 4 ประการคือ [4]

2.1 การวิเคราะห์ผลกระทบต่อธุรกิจ (Business Impact Analysis: BIA)

การวิเคราะห์ผลกระทบต่อธุรกิจ หรือจะใช้คำย่อว่า BIA เป็นองค์ประกอบที่สำคัญของการจัดทำทำแผน CP เพราะเป็นกิจกรรมในขั้นตอนแรกของการวางแผนรองรับเหตุการณ์ฉุกเฉิน ซึ่งก่อนจะมีการเลือกแผนรองรับเหตุการณ์ฉุกเฉินที่เหมาะสมควรมีการวิเคราะห์ผลกระทบทางธุรกิจก่อนเสมอ ทีมงาน CP จะต้องทำการวิเคราะห์ผลกระทบทางธุรกิจ แบ่งเป็น 5 ขั้นตอน มีรายละเอียดดังต่อไปนี้

1. การระบุและการจัดลำดับความเสี่ยงหรือภัยคุกคามที่จะส่งผลต่อองค์กรและความมั่นคงของสารสนเทศ

องค์กรที่ใช้กระบวนการจัดการความเสี่ยงจะมีการระบุการคุกคามและระดับความสำคัญของการคุกคามอยู่ในแผนการจัดการความเสี่ยง ซึ่งองค์กรเหล่านี้จะมีการปรับปรุงรายการของภัยคุกคามที่มักจะเกิดขึ้นให้ทันสมัย และมักจะมีการเพิ่มเติมข้อมูลสารสนเทศอื่นๆ อาทิ รายละเอียดของการจู่โจมในลักษณะต่างๆ เข้าไปด้วย ไม่ว่าจะเป็นลักษณะภัยคุกคามที่เกิดจากภัยธรรมชาติ หรือจากมนุษย์ เกิดจากความตั้งใจ หรือไม่ตั้งใจ ตัวอย่างเช่น ลักษณะของภัยคุกคามจากภายในที่เกิดจากการกระทำของมนุษย์ เกิดจากการกระทำที่ไม่ตั้งใจของบุคลากร หรือความประมาทเลินเล่อ เช่น การให้รหัสผ่านของตนเองให้กับบุคคลอื่น หรือการเข้าไปเปลี่ยนแปลงข้อมูลในระบบ [4]

2. การวิเคราะห์หน่วยงานธุรกิจ

การวิเคราะห์หน่วยงานธุรกิจเป็นงานหลักขั้นที่สองของกระบวนการ BIA โดยขั้นตอนนี้จะเป็นการวิเคราะห์หน้าที่การทำงานภายในองค์กรให้ครบถ้วนว่ามีความสัมพันธ์ มีเกี่ยวข้อง มีรายละเอียดเช่นใด และมีการควบคุมในลักษณะเช่นใดอยู่ในปัจจุบัน และต้องใช้เวลาเท่าใดในการกอบกู้ให้ดำเนินงานได้ตามปกติ หลังจากเกิดเหตุการณ์ฉุกเฉิน ซึ่ง BIA ทำได้ 3 วิธีหลัก คือ การทำแบบสอบถาม การสัมภาษณ์ การสนทนากลุ่ม (Focus Group)

3. การวิเคราะห์เหตุการณ์ฉุกเฉินที่เกิดขึ้น

การวิเคราะห์เหตุการณ์การฉุกเฉินนั้นจะเป็นขั้นตอนต่อมาที่ทีมงาน CP จะต้องปฏิบัติ โดยจะเป็นการออกแบบสถานการณ์จำลอง โดยลำดับเหตุการณ์ของการเกิดผลกระทบต่อการทำงานในแต่ละส่วนขององค์กร ซึ่งรายละเอียดของเหตุการณ์การนั้นควรประกอบไปด้วย วิธีการ ตัวบ่งชี้ และผลกระทบโดยรอบ

4. การประเมินความเสียหายที่อาจจะเกิดขึ้น

ข้อมูลจากสถานการณ์จำลองในขั้นตอนที่กล่าวมาแล้วนั้น ทีมงานที่ร่วมวางแผน CP ต้องประมาณค่าเสียหายที่คาดว่าจะเกิดขึ้นสูงสุด รวมทั้งโอกาสที่เกิด โดยประเมินจากกรณีของสถานการณ์จำลองต่างๆ ที่วางไว้ ขั้นตอนนี้จะช่วยให้ระบุสิ่งที่จะต้องกระทำในการฟื้นฟูจากเหตุการณ์ในกรณีต่างๆ ได้

5. การแบ่งแผนงานย่อย

เมื่อความเสียหายที่คาดว่าจะเกิดขึ้นได้ถูกประเมินค่าแล้ว จะต้องนำข้อมูลมาพิจารณาเพื่อจำแนก เหตุการณ์ สถานการณ์จำลอง และกรณีมีความเกี่ยวข้องกับแผนฉุกเฉินลักษณะต่างๆ อย่างไร รวมถึงการรับมือสำหรับการฉุกเฉินรูปแบบต่างๆ จะต้องได้รับการพัฒนา โดยอาจจะพิจารณาจากแผนเดิมที่เคยมีอยู่แล้วและนำมาปรับใช้ให้ถูกต้องตามสถานการณ์ของเหตุการณ์ฉุกเฉิน แต่ละกรณีจะถูกแบ่งกลุ่มตามความเสียหายที่ใกล้เคียงกัน รวมทั้งการจัดหาบุคลากรไว้เตรียม

ดำเนินการฟื้นฟูตามแผนที่วางไว้

2.2 การวางแผนตอบสนองต่อเหตุการณ์ที่ไม่คาดคิด (Incident Response Plan: IRP)

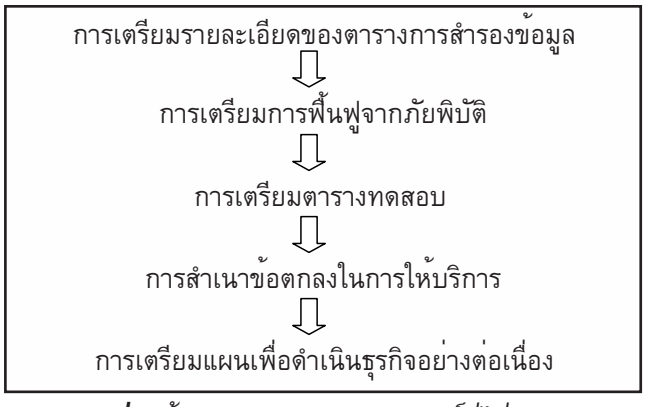
เป็นการวางแผนที่ระบุถึงรายละเอียดของกระบวนการและขั้นตอนที่คาดการณ์ ค้นหา และบรรเทาผลกระทบจากเหตุการณ์ไม่คาดคิดที่อาจทำความเสียหายแก่สินทรัพย์และทรัพยากรทางสารสนเทศแบบทันทีทันใด ซึ่งทีมงาน CP ที่ทำหน้าที่วางแผนตอบสนองเหตุการณ์ในลักษณะนี้จะถูกจัดตั้งขึ้น โดยเรียกเป็นคำย่อว่า ทีมงาน IR (Incident Response Team)

เมื่อเป็นที่แน่ชัดแล้วว่าความรุนแรงที่เกิดขึ้นนั้นมีแนวโน้มว่าจะก่อให้เกิดเป็นภัยคุกคามต่อความมั่นคงสารสนเทศ ทีมงาน IR จะต้องปรับเปลี่ยนกระบวนการจากการเฝ้าระวังตรวจสอบไปเป็นขั้นตอนการตอบสนองต่อเหตุการณ์ ซึ่งในกระบวนการตอบสนองนี้จะต้องทำอย่างรวดเร็วและทันทีทันใดเมื่อมีการค้นพบการเกิดเหตุการณ์คุกคามและเมื่อเหตุการณ์ดังกล่าวกลายเป็นการโจมตี ซึ่งสภาวะดังกล่าวจะถูกจัดเป็นเหตุการณ์ทางความมั่นคงสารสนเทศ ถ้าพบว่าการคุกคามนั้นมีโอกาสเป็นไปได้ที่จะส่งผลกระทบต่อสารสนเทศ

ขั้นตอนที่ทีมงาน IR ต้องเตรียมพร้อมและปฏิบัติต่อเหตุการณ์อาจแบ่งออกได้เป็น 3 ช่วง ได้แก่

1. ช่วงก่อนการเกิดเหตุการณ์

ทีมงาน IR จะต้องร่างกระบวนการขั้นตอนการตอบสนองต่อเหตุการณ์ไว้ล่วงหน้า ซึ่งมีขั้นตอนต่างๆ ดังนี้



***ภาพที่ 2** ขั้นการตอบสนองเหตุการณ์ที่ไม่คาดคิด*

2. ช่วงระหว่างการเกิดเหตุการณ์

ในช่วงระหว่างการเกิดเหตุการณ์นั้นทีมงาน IR จะต้องบันทึกเหตุการณ์ที่เกิดขึ้น และจัดทำเอกสารแสดงขั้นตอนการดำเนินงานที่จะต้องกระทำในระหว่างที่เกิดเหตุการณ์ไม่คาดคิดขึ้น โดยแบ่งขั้นตอนการดำเนินงานออกเป็นกลุ่มตามกลุ่มของผู้เกี่ยวข้อง เช่น ขั้นตอนที่ผู้ใช้ต้องกระทำ ขั้นตอนที่เจ้าหน้าที่ฝ่ายเทคนิคต้องกระทำ เป็นต้น

3. ช่วงหลังการเกิดเหตุการณ์

เมื่อมีการกระทำตามขั้นตอนเพื่อตอบสนองเหตุการณ์แล้ว ทีมงาน IR จะต้องจัดเอกสารขั้นตอนการจัดการเหตุการณ์ที่เกิดขึ้นไว้ ซึ่งจะต้องทำทันทีหลังเหตุการณ์สงบ ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้อ้างอิงเป็นหลักฐานหรือนำไปใช้ในการปรับปรุงในกระบวนการทำแผนครั้งต่อไปได้

2.3 การวางแผนการฟื้นฟูเหตุการณ์จากความเสียหายที่รุนแรง (Disaster Recovery Planning: DRP)

การวางแผนการฟื้นฟูจากความเสียหายที่รุนแรง หรือใช้คำย่อว่า DRP เป็นแผนเพื่อเตรียมการฟื้นฟูจากภัยพิบัติที่ร้ายแรง ที่องค์กรไม่สามารถยับยั้ง หรือควบคุมผลกระทบของเหตุการณ์ได เนื่องจากระดับของความเสียหาย หรือการทำลายจากเหตุการณ์มีมาก และองค์กรจะไม่สามารถฟื้นฟูได้อย่างเร็ว ดังนั้นบทบาทหลักของการวางแผนฟื้นฟูจากภัยพิบัติที่จะต้องปฏิบัติคือจะต้องวางแผนให้ได้ว่าจะเริ่มการปฏิบัติตอบสนองความรุนแรงได้อย่างไร

ในกระบวนการของ DRP นั้นจะพยายามแยกภัยพิบัติทางธรรมชาติ และภัยพิบัติที่เกิดจากคนออกจากกัน หรือพิจารณาจากความเร็วของการเกิดความเสียหาย เช่นเป็นภัยพิบัติที่เกิดอย่างรวดเร็ว หรือเกิดจากการสะสมความรุนแรง และส่งผลกระทบรุนแรงขึ้นอย่างช้าๆ ดังนั้นในการวางแผนเพื่อรองรับภัยพิบัติร้ายแรง ต้องคำนึงถึงการจำลองเหตุการณ์ที่ร้ายแรง และวิเคราะห์ผลกระทบ เพื่อใช้ในการแบ่งระดับของการคุกคามของภัยพิบัติแต่ละครั้ง ซึ่งประเด็นหลักของแผนฟื้นฟูจากภัยพิบัติ (DRP) ก็คือ

1) การกำหนดบทบาทและความรับผิดชอบของคณะบุคคลที่เกี่ยวข้องให้ชัดเจน

2) การกำหนดรายชื่อบุคคลรับผิดชอบที่เกี่ยวข้องพร้อมทั้งข้อมูลที่จะต้องติดต่อประสานงานได้เมื่อเกิดเหตุการณ์ดังกล่าวขึ้น (Alert Roster) และการแจ้งไปยังบุคคลหลักดังกล่าวนั้นให้ทราบ (Notification of Key Personnel)

3) แจ้งลำดับความสำคัญเหตุการณ์ ปัญหา และขั้นตอนการตอบสนองให้ชัดเจน

4) การบันทึกข้อมูลเหตุการณ์ภัยพิบัติที่เกิดขึ้น

5) การกำหนดขั้นตอนปฏิบัติในการบรรเทาผลกระทบที่เกิดขึ้นจากเหตุการณ์ร้ายแรง

6) การจัดเตรียมทางเลือกอื่นๆ ในการดำเนินการไว้รองรับเหตุการณ์ที่ยากต่อการควบคุม

2.4 การวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง (Business Continuity Planning: BCP)

Hearnden [9] ได้ทำการศึกษาไปยังประเด็นสำคัญที่ส่งผลต่อกิจกรรมการดำเนินงานขององค์กรธุรกิจมากที่สุด พบว่า ประเด็นความสูญเสียด้านอาคารและสถานที่เป็นประเด็นที่มีค่าสูงสุด เท่ากับความเสียหายด้านการสื่อสาร ดังนั้นการวางแผนให้ธุรกิจดำเนินไปได้อย่างต่อเนื่องแม้เกิดสถานการณ์ฉุกเฉินที่รุนแรงที่ส่งผลไม่ให้สามารถใช้สถานที่ ณ ปัจจุบันขององค์กรหรือโครงสร้างพื้นฐานอื่นๆ ในการดำเนินงานต่อไปได้ เป็นสิ่งจำเป็น ดังนั้นการวางแผนเพื่อดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง หรือเรียกโดยย่อว่าการวางแผน BC เป็นกระบวนการสร้างความมั่นใจได้ว่าธุรกิจที่สำคัญจะยังสามารถดำเนินการต่อได้แม้ในเหตุการณ์ภัยพิบัติร้ายแรงก็ตาม การวางแผน BC จึงต้องดำเนินการโดยผู้บริหารขององค์กร โดยกำหนดให้มีการดำเนินงานจัดหาที่ตั้งสำรองเพื่อดำเนินธุรกิจ หรืองานขององค์กรต่อไปได้ ในขณะที่แผนการฟื้นฟูจากเหตุการณ์ความเสียหายที่รุนแรง (DRP) จะเน้นการวางแผนเพื่อตอบสนองเหตุการณ์ร้ายแรงโดยที่ยังอยู่ในสถานที่ทำงานหรือที่ตั้งเดิม

แผน BC นี้เป็นแผนประเภทหนึ่งที่ยอมรับกันอย่างกว้างขวางในองค์กรต่าง ๆ ว่าเป็นเครื่องมือในการจัดการ และเป็นกลยุทธ์ที่จำเป็นในการทำงาน Kash และ Darling [10] ได้ชี้ให้เห็นว่ากว่าร้อยละ 85 ขององค์กรทั่วไป ต่างยอมรับว่าแผน BC เป็นส่วนหนึ่งที่สำคัญของธุรกิจที่หลีกเลี่ยงไม่ได้ แต่กระนั้นก็ตามมีองค์กรอยู่จำนวนไม่มากที่มีการจัดเตรียมแผน BC นี้อย่างจริงจัง Harnden [9] ได้ระบุไว้ว่าเมื่อใดก็ตามที่องค์กรได้จัดทำแผน BC ส่วนใหญ่ก็มักจะมุ่งเน้นไปยังเรื่องของเทคโนโลยีสารสนเทศ แต่มีน้อยมากที่จะระบุถึงองค์ประกอบอื่นๆ ที่เกี่ยวข้อง เช่น คน กระบวนการ หรือ โครงสร้างพื้นฐานทั่วไป Harnden [9] ยังได้ระบุเพิ่มเติมไว้อีกว่าแผน BC ส่วนใหญ่มักจะขาดการทบทวนหรือทดสอบอย่างสม่ำเสมอ ซึ่งอาจจะส่งผลให้ประสิทธิภาพของแผนนั้นๆ ลดลง

รูปแบบในการวางแผน BC นั้นมีหลากหลายแหล่งที่ได้คิดค้น อ้างอิงได้จากรูปแบบของ Karakasidis [11], Hinks [12], Heng [13], Varcoe [14], DRI International [15] ซึ่งรูปแบบที่อ้างอิงมาดังกล่าวมีกระบวนการที่สอดคล้องกันพอสรุปรวมกันได้ดังนี้

การวางแผน BC ต้องเริ่มพิจารณาจาก 1) การริเริ่มการวางแผน 2) การประเมินความเสี่ยง/ BIA 3) การออกแบบและพัฒนาตัวแผน BC 4) การจัดทำแผน BC 5) การทดสอบแผน และการนำไปใช้ 6) การดูแลรักษาและปรับปรุงแผนให้ทันสมัย

นอกจากรูปแบบข้างต้นแล้วทีมงาน BC ยังอาจพิจารณามาตรฐาน BS 25999 เพื่อใช้สำหรับวางแผนการจัดการการนำไปปฏิบัติ และการปรับปรุงระบบบริหารความต่อเนื่องธุรกิจขององค์กรได้อีกด้วย BS 25999 เป็นมาตรฐานด้านการบริหารความต่อเนื่องธุรกิจ (Business Continuity Management: BCM) โดยข้อกำหนดต่างๆ ตามมาตรฐาน BS 25999 นี้มุ่งเน้นใน 1) ด้านการทำความเข้าใจในความต้องการของความต่อเนื่องทางธุรกิจ และการจัดทำนโยบายเพื่อสอดคล้องกับวัตถุประสงค์ในการสร้างความต่อเนื่องทางธุรกิจ 2) ด้านการนำไปปฏิบัติ และการควบคุม สำหรับการจัดการกับความเสี่ยงต่างๆ ที่มีต่อความต่อเนื่องในการดำเนินธุรกิจ 3) การติดตามผล และทบทวนผลการดำเนินงาน รวมทั้งความมีประสิทธิผลของระบบ และ 4) การปรับปรุงระบบอย่างต่อเนื่อง [16]

การจำแนกความแตกต่างของแผนเพื่อรองรับเหตุการณ์ฉุกเฉินทั้ง 3 ชนิด จะใช้เวลา ระดับความรุนแรง และความพร้อมของสถานที่ และโครงสร้างพื้นฐานในการปฏิบัติงาน งบประมาณ ค่าใช้จ่ายที่ต้องใช้ เป็นเงื่อนไขในการพิจารณา [4] สามารถสรุปได้ดังนี้

1. แผนรับมือเหตุการณ์ไม่คาดคิด (IRP) นำไปใช้ทันทีที่พบเหตุการณ์ฉุกเฉินประเภทต่างๆ หากเหตุการณ์ไม่คาดคิดนั้นทำให้ระบบเสียหาย ให้นำแผนฟื้นฟูจากความเสียหายมาใช้

2. แผนฟื้นฟูจากความเสียหายที่รุนแรง (DRP) มีวัตถุประสงค์เพื่อการฟื้นฟูระบบให้กลับมาทางานได้ ตามปกติหลังจากที่ระบบมีความเสียหายเกิดขึ้น

3. แผนดำเนินธุรกิจต่อไปได้ในสถานการณ์ฉุกเฉินที่รุนแรง (BCP) นำมาใช้ควบคู่กับแผนฟื้นฟูจากความเสียหายที่รุนแรง หากพบว่าต้องใช้เวลานานหรือต้องใช้ความพยายามอย่างมากในการฟื้นฟูระบบ และองค์กรไม่สามารถใช้สถานที่เดิมในการปฏิบัติงานได้

3. ขั้นตอนของการจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน

แนวทางปฏิบัติของ NIST SP 800-34 (National Institute of Standards and Technology Special Publication 800-34) [17] ได้ระบุถึงกระบวนการจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน ซึ่งพอสรุปได้ดังนี้ โดยเริ่มจาก

1. เขียนนโยบายจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน
2. วิเคราะห์ผลกระทบทางธุรกิจ ประกอบด้วย
   - การประเมินความเสี่ยง (Risk Assessment)
   - การวิเคราะห์ผลกระทบทางธุรกิจ (BIA)
3. ระบุข้อกำหนดและมาตรการควบคุมเพื่อป้องกัน เพื่อลดผลกระทบที่อาจจะเกิดขึ้นในกรณีที่เกิดเหตุการณ์รุนแรงขึ้น
4. กำหนดกลยุทธ์การฟื้นฟูหลังจากเหตุการณ์ผ่านพ้นไป
5. จัดทำแผนรองรับเหตุการณ์ฉุกเฉิน
6. ทดสอบแผน การสร้างความตระหนักและฝึกอบรมการใช้แผน
7. บำรุงรักษาแผน ทบทวนและปรับปรุงข้อมูลในแผนงานให้เป็นปัจจุบัน

4. การทดสอบแผนรองรับเหตุการณ์ฉุกเฉิน

องค์กรควรมีการทดสอบแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง แต่อย่างไรก็ตามการทดสอบแผนฉุกเฉินจะต้องมีค่าใช้จ่ายที่เกิดขึ้นแน่นอน ดังนั้น 1 ใน 3 ของงบประมาณด้านระบบสารสนเทศขององค์กร ควรจะต้องจัดสรรไว้สำหรับการจัดทำแผนฉุกเฉิน และแน่นอนว่าเงินจำนวนนี้จะต้องเตรียมไว้สำหรับขั้นตอนการทดสอบแผนฉุกเฉินดังกล่าวด้วยเช่นกัน [18]

Pitt และ Goyal [19] ได้กล่าวเสริมไว้เช่นกันว่า กระบวนการวางแผนฉุกเฉินนั้นจะมีขั้นตอนสำคัญประการในตอนท้ายคือการทดสอบแผนฉุกเฉิน บำรุงรักษาแผน ซึ่งสอดคล้องกับขั้นตอนการจัดทำแผนข้อที่ 6 และ 7 ของ NIST SP 800-34 ที่ได้ระบุไว้ก่อนหน้านี้เช่นกัน เมื่อมีการพบปัญหาในระหว่างที่มีการทดสอบ องค์กรก็สามารถจะปรับปรุงแผนให้ดีขึ้นเพื่อให้แผนมีความเป็นปัจจุบันและพร้อมต่อการใช้งานได้เสมอ สำหรับวิธีการทดสอบแผนรองรับเหตุการณ์ฉุกเฉินนั้น Whitman และ Mattord [4] ได้เสนอไว้ 5 วิธีดังนี้

1. การทดสอบแบบ Desk Check

วิธีนี้ทำได้โดยการแจกจ่ายแผนให้ผู้ปฏิบัติงานที่ได้รับมอบหมายให้รับผิดชอบได้ทดลองปฏิบัติตามเพื่อตรวจสอบดูว่าหากเกิดเหตุการณ์ฉุกเฉินต่าง ๆ ในขั้นตอนของการปฏิบัติงาน พวกเขาจะสามารถแก้ไขปัญหาต่าง ๆ เหล่านั้นได้ทันทีทันใดโดยดูวิธีการแก้ไขจากแผนนี้ได้หรือไม่

2. การทดสอบ Structured Walk-Through

การทดสอบวิธีนี้ บุคลากรที่ได้รับมอบหมายจะทำการทดสอบแผนตามขั้นตอนต่าง ๆ ที่ระบุไว้ในแผน ผู้ทำการตรวจสอบจะเดินตรวจสอบไปตามโครงสร้างและขั้นตอนของการปฏิบัติงาน

3. การทดสอบแบบ Simulation

การทดสอบโดยวิธีนี้ บุคลากรได้รับมอบหมายในแผนงานจะต้องทำการทดสอบแผนงานโดยจำลองสถานการณ์การดำเนินงานของทุกกิจกรรมที่ได้รับมอบหมาย และบันทึกข้อผิดพลาดที่เกิดจากการทดสอบเพื่อปรับปรุงต่อไป แต่อย่างไรก็ตามบุคลากรในการทดสอบนี้จะรับผิดชอบเฉพาะงานที่ตัวได้รับมอบหมายเท่านั้น

4. การทดสอบแบบ Parallel

บุคลากรที่ได้รับมอบหมายให้ทำการทดสอบจะดำเนินการทดสอบโดยจะทำการทดสอบในรูปแบบคล้ายกับเหตุการณ์ทำงานจริง ไปคู่กันกับการทำงานจริงปกติ เพียงแต่ในการทดสอบนี้จะไม่รบกวนการดำเนินงานตามปกติของธุรกิจ

5. การขัดจังหวะแบบ Full Interruption

บุคลากรจะปฏิบัติหน้าที่เสมือนมีเหตุการณ์ฉุกเฉินที่รุนแรงขึ้นจริง กระบวนการทดสอบจะคล้ายกับ Parallel Testing แต่ต่างกันที่ การทดสอบแบบ Full Interruption จะทำการรบกวนการทำงานปกติของธุรกิจ วิธีนี้จะมีความเสี่ยง และมีค่าใช้จ่ายสูงมากกว่าวิธีอื่น

5. ตัวอย่างการใช้/ การซ้อมแผนรองรับเหตุการณ์ฉุกเฉินเพื่อความมั่นคงสารสนเทศขององค์กรต่าง ๆ

ตัวอย่างต่อไปนี้เป็นเหตุการณ์ที่เกิดขึ้นจริงที่องค์กรต่าง ๆ ได้มีการเตรียมความพร้อมต่อเหตุการณ์ฉุกเฉินร้ายแรงในลักษณะต่าง ๆ

ในช่วงวิกฤติสถานการณ์น้ำท่วมในปลายปี 2554 ที่ผ่านมา ได้ส่งผลต่อเนื่องในหลายจังหวัด โดยเฉพาะในเขตกรุงเทพมหานคร ซึ่งหลายฝ่ายคาดการณ์ว่ามีแนวโน้มที่น้ำจะไหลเข้าสู่พื้นที่กรุงเทพฯ ชั้นใน และมีระดับน้ำที่สูงขึ้นจนอาจเกิดอันตรายที่ส่งผลต่อการจ่ายกระแสไฟฟ้าของการไฟฟ้านครหลวง ดังนั้นหนังสือพิมพ์ไทยรัฐออนไลน์ [20]

(www.thairath.co.th) จึงได้ประกาศเตรียมความพร้อม ด้วยการเตรียมแผนรองรับเหตุการณ์ฉุกเฉินในลักษณะต่าง ๆ ซึ่งรวมไป ซึ่งทางไทยรัฐได้รับความร่วมมือจาก บมจ. ทีโอที ในการให้ใช้ศูนย์เซ็นเตอร์ไอดีซี ทีโอที ที่นิคมอุตสาหกรรมแหลมฉบัง จังหวัดชลบุรี เป็นศูนย์เซิร์ฟเวอร์สำรองเพื่อให้การบริการที่ไม่ขาดตอน ถึงแม้ที่กรุงเทพฯ จะไฟฟ้าดับก็ยังสามารถดำเนินธุรกิจการให้บริการข่าวสารต่อไปได้ [20]

Home Depot ร้านค้าปลีกอุปกรณ์ตกแต่งบ้านรายใหญ่ของโลก มีพนักงานทุกสาขารวมกันกว่า 3 แสนคน ได้มีการจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน และมีการทดสอบแผนดังกล่าวอยู่เสมอ Robbie Atabagi (Home Depot Disaster Recovery Coordinator) ได้ชี้แจงว่าทางบริษัทได้ทำการทดสอบแผนฉุกเฉินกว่า 2 ถึง 3 ครั้งในแต่ละปี เพื่อให้แผนยังคงไว้ซึ่งความพร้อมในการตอบสนองเหตุการณ์ที่ไม่คาดคิด ซึ่งในปี ค.ศ.1992 ทาง Home Depot ก็เคยประสบกับวิกฤติเหตุการณ์รุนแรงจากพายุเฮอร์ริเคนแอนดรู (Hurricane Andrew) สร้างความเสียหายแก่ Home Depot ที่มีสาขาอยู่ในรัฐฟอริดา แต่ทางบริษัทก็สามารถฟื้นฟูความเสียหายให้กลับคืนสู่สภาพเดิมได้อย่างรวดเร็วด้วยการปฏิบัติตามแผนรองรับเหตุกาณ์ฉุกเฉินนั่นเอง [21]

นิคมอุตสาหกรรมบ้านหว้าไฮเทค เป็นนิคมอุตสาหกรรมแห่งที่ 2 ที่การนิคมอุตสาหกรรมแห่งประเทศไทย (กนอ.) ทำการฝึกซ้อมแผนฉุกเฉิน กรณีเกิดเหตุอุทกภัยขึ้น เพื่อสร้างความมั่นใจให้กับนักลงทุน และซ้อมความพร้อมในการรับมือกับสถานการณ์ฉุกเฉิน ซึ่งตามแผนซักซ้อม กนอ. จะแจ้งให้ขนย้ายสิ่งของ วัตถุดิบ เครื่องจักร และอพยพคนออกจากพื้นที่ ไปยังศูนย์พักพิงชั่วคราวที่ได้เตรียมไว้ โดยให้ประเมินผล และติดตามสถานการณ์ 24 ชั่วโมง หลังการทดสอบ กนอ. ระบุว่า นิคมอุตสาหกรรมบ้านหว้า มีความพร้อมค่อนข้างดี [22]

บริษัทวิทยุการบินแห่งประเทศไทย ใช้แผนฉุกเฉินดำเนินการแก้ไขปัญหาไฟฟ้าดับที่เกาะสมุยในช่วงต้นเดือนธันวาคม 2555 ที่ผ่านมา โดยใช้เครื่องกำเนิดไฟฟ้าสำรองที่มีอยู่จ่ายไฟให้ระบบ/อุปกรณ์ สามารถทำงานได้ตามปกติ และได้สั่งการให้วิศวกรที่เชี่ยวชาญดูแลระบบไฟฟ้าอย่างใกล้ชิดตลอด 24 ชั่วโมง อีกทั้งประสานหน่วยงานที่เกี่ยวข้องช่วยสนับสนุน ซึ่งสามารถแก้ไขสถานการณ์เบื้องต้นได้ทั้งหมด และ ยังมีมาตรการควบคุมความเสี่ยงที่อาจจะเกิดขึ้นซ้ำ โดยสามารถให้บริการจราจรทางอากาศ ณ ท่าอากาศยานสมุยได้ตามปกติ ไม่เกิดปัญหาความล่าช้าของเที่ยวบินแต่อย่างใด [23]

ภาพที่ 3 *ตัวอย่างการซ้อมดับเพลิงบริษัท ปตท. เคมิคอล จำกัด (มหาชน) ตามตารางทดสอบแผนฉุกเฉินแบบ Full Interruption [24]*

6. บทสรุป

บทความนี้ได้พยายามชี้ให้เห็นถึงความสำคัญของการวางแผนเพื่อรองรับเหตุการณ์ฉุกเฉินกับการรักษาความมั่นคงสารสนเทศขององค์กร ที่ทั้งสองประเด็นมีความเกี่ยวพันกัน ซึ่งองค์กรไม่ควรมองข้าม เนื่องจากเหตุการณ์ฉุกเฉินอาจเกิดในเวลาที่ไม่คาดคิด และบางครั้งอาจมีสาเหตุจากเหตุการณ์ที่ไม่น่าจะส่งผลต่อสารสนเทศขององค์กรโดยตรง แต่ก็สามารถสร้างความเสียหายให้แก่ทรัพย์สินที่เป็นสารสนเทศดังกล่าวได้ถึงขั้นทำให้กระบวนการธุรกิจไม่สามารถดำเนินการต่อไปได้

เมื่อเป็นเช่นนี้แล้วลองสำรวจดูในองค์กรของท่านว่าได้มีการจัดทำแผนเพื่อรองรับสำหรับเหตุการณ์ฉุกเฉินที่มีประสิทธิภาพ พร้อมทั้งมีกระบวนการในการทดสอบแผนเหล่านั้นอย่างเป็นระบบแล้วหรือยัง ข้อแนะนำเพิ่มเติมสำหรับองค์กรที่กำลังจะเริ่มจัดทำแผนฉุกเฉินควรศึกษาแนวทางปฏิบัติที่ดีจากการใช้แผนหรือการทดสอบแผนฉุกเฉินที่มีความเหมาะสมเพื่อนำข้อมูลมาปรับใช้กับการวางแผนให้เข้ากับลักษณะขององค์กรตนเองต่อไป

7. เอกสารอ้างอิง

[1] M. R Stair, and W. G. Reynolds, *Principles of Information Systems*, 10th Ed. Cambridge : Course Technology, 2011.

[2] ศิรปัฐช์ บุญครอง, "การออกแบบโพรโทคอลการเข้ารหัส" *วารสารเทคโนโลยีสารสนเทศ*, ปีที่ 7 ฉบับที่ 13 มกราคม - มิถุนายน หน้า 52-56, 2554.

[3] E. Whitman Michael and J. Mattord Herbert, *Management of Information Security*, Thomson Learning , 2nd Edition , 2005. Cited in The Heartford Financial Services Group, Inc. Why you need a disaster Recovery Plan. Accessed 13 May 2003 from sb.theheartford.com/ reduce_risk/disater_recovery.asp.

[4] E. Whitman Michael and J. Mattord Herbert *Management of Information Security*, Thomson Learning , 2nd Edition , 2005.

[5] J. Michael Cerullo, R. Steve McDuffie, and L. Murphy Smith. "Planning for Disaster," *The CP A Journal*, Jun 64, 6. pp: 34, 1994.

[6] แอลซีไทยดอทคอม. "รถเครนเกี่ยวเสาไฟล้มนับสิบแยกนางลิ้นจี่ ถ.พระราม 3" วันที่ 22 ธันวาคม 2555 สืบค้นจาก http://news.tlcthai.com/ news/77680.html.

[7] M. Zetlin, "When technology fails." Getting Results for the Hands; on Manager, Mar 42. pp. 6, 1997.

[8] K. Davis, "Planning for the Unthinkable: IT Contingencies," *Information Management*; Fall 2004; Vol.17 No.3-4 pp. 2, 2004.

[9] K. Hearnden, "Business continuity planning," *Computer Audit Update*, 3-9 July, 1995.

[10] T. Kash, and J. Darling, "Crises management: prevention, diagnosis and intervention," *Leadership & Organizational Development Journal*, Vol. 19 No.4, pp. 179, 1998.

[11] Karakasidis, ?. "A project planning process for business continuity," *Information Management and Computer Security*, Vol. 5 No. 2, pp. 72, 1997.

[12] J. Hinks, "Facilities Management 1 – Course Notes, Heriot-Watt University, Edinburgh, 2001.

[13] Heng, "Developing a suitable business continuity planning methodology", *Information Management and Computer Security*, Vol. 4 No.2 pp. 11-13, 1996.

[14] B. Varcoe, "Not us surely? Disaster recovery planning for premises," *Facilities*, Vol.16 No.7/8, pp. 204, 1998.

[15] DRI International. "DRI international business continuity planning model", available online at www.dr.org/model (accessed 16 December 2012).

[16] wikipedia.org. "BS 25999 (Business Continuity Management)", Available online at http://en.wikipedia.org/wiki/BS_25999

[17] NIST.gov. "NIST SP 800-34 (National Institute of Standards and Technology Special Publication 800-34)" Available online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf (accessed 18 December 2012).

[18] K. Mead, "Staying alive: Business contingency planning" The Internal Auditor; 52, pp: 6 December 1995.Cited in Muecke, D. "Justifying Recovery Testing" Disaster Recovery Testing ed. Philip Jan Rothstein (Ossining, NY: Rothstein Associated Inc., pp. 7, 1994.

[19] M . Pitt, and S. Goyal, "Business continuity planning as a facilities management tool," *Facilities*, 22-3/4 pp. 87, 2004.

[20] ไทยรัฐออนไลน์. "ไทยรัฐออนไลน์ตายยาก ผุดไซต์สำรองที่แหลมฉบัง" *หนังสือพิมพ์ไทยรัฐออนไลน์* วันที่ 22 ตุลาคม 2554 สืบค้นจาก www.thairath.co.th/content/tech/211014.

[21] Home Depot. The Home Depot-Leadership in Crisis Management. Available online at http://www.studymode.com/essays/The-Home-Depot-Leadership-In-Crisis-Management-800330.html (accessed 18 December 2012).

[22] VoiceTV. “นิคมฯบ้านหว้าซ้อมแผนฉุกเฉิน” VoiceTV วันที่ 27 กันยายน 2555 สืบค้นจาก http://news.voicetv.co.th/thailand/51694.html.

[23] หนังสือพิมพ์โพสต์ทูเดย์. “วิทยุการบินฯ งัดใช้แผนฉุกเฉินแก้ไฟดับสมุย” หนังสือพิมพ์โพสต์ทูเดย์ หน้า B10 วันที่ 14 พฤศจิกายน 2555.

[24] ปราโมทย์ คล้ายเชย. “การจัดทำแผนฉุกเฉินสำหรับโรงงานอุตสาหกรรม กรณีศึกษา บริษัท ปตท. เคมิคอล จำกัด (มหาชน)” สำเนาเอกสารประกอบการนำเสนอ ณ วันที่ 13 ธันวาคม 2550.