ศูนย์คอมพิวเตอร์สำรองกรณีเกิดภัยฉุกเฉินกับการให้บริการผู้ป่วยในยุคดิจิทัล

Disaster Recovery Site and Patient Services in the Digital Age

กรรณิกา ละมั่งทอง[1] และ นภสินธุ์ บุญมาก[1]

Kannika Lamungthong[1] and Naphasin Boonmak[1]

[1]ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล 10700

[1] Information Technology Department Faculty of Medicine Siriraj Hospital, Mahidol University 10700

*Corresponding Author: kannika.lam@mahidol.edu

Received 27 พฤศจิกายน 2567; Revised 20 มีนาคม 2568; Accepted 24 เมษายน 2568

บทคัดย่อ

ความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้นและเข้ามามีบทบาทในเกือบจะทุกกิจกรรมภายในองค์กรและหน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชน ปัจจุบันมีเหตุการณ์ต่าง ๆ เกิดขึ้นในรูปแบบที่หลากหลาย อาทิ การโจมตีทางไซเบอร์ อุบัติภัยทางธรรมชาติ การชุมนุมประท้วง การเกิดอัคคีภัย ซึ่งสิ่งต่าง ๆ เหล่านี้หากเกิดขึ้นจะส่งกระทบต่อกิจกรรมทางธุรกิจต่าง ๆ ขององค์กรทั้งในด้านภาพลักษณ์ ชื่อเสียง ความเชื่อมั่น รวมไปถึงรายได้หลักขององค์กร ดังนั้นองค์กรจึงควรจัดทำกระบวนการบริหารความต่อเนื่องทางธุรกิจ เพื่อให้มั่นใจได้ว่าหากเกิดเหตุการณ์ฉุกเฉิน องค์กรจะยังสามารถดำเนินกิจกรรมทางธุรกิจได้ โดยใช้แผนการความต่อเนื่องทางธุรกิจที่ได้กำหนดไว้

การบริหารจัดการความต่อเนื่องทางธุรกิจมีคำแนะนำและแนวทางในการบริหารจัดการที่หลากหลาย โดยองค์กรสามารถนำไปใช้ให้เหมาะสมกับบริบทขององค์กร สำหรับพื้นฐานของการบริหารความต่อเนื่องทางธุรกิจจะประกอบด้วยกิจกรรมหลัก ๆ อาทิ การจัดทำแผนความต่อเนื่องทางธุรกิจภายใต้สถานการณ์ต่าง ๆ การสำรองและการกู้คืนข้อมูล ซึ่งสิ่งต่าง ๆ เหล่านี้หากองค์กรนำมาพิจารณา จัดทำ ทบทวน และปรับปรุงเป็นประจำอย่างสม่ำเสมอ ก็จะช่วยลดผลกระทบต่าง ๆ ที่อาจเกิดขึ้นกับองค์กรและช่วยให้องค์กรสามารถบริหารความต่อเนื่องทางธุรกิจได้อย่างมีประสิทธิภาพ

บทความนี้รวบรวมมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ การสำรองข้อมูล การกู้คืนข้อมูล และศูนย์คอมพิวเตอร์สำรองกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉิน พร้อมยกตัวอย่างการนำสิ่งต่าง ๆ เหล่านี้ไปประยุกต์ใช้ภายในองค์กรเพื่อให้เห็นภาพการนำไปเชื่อมโยงกับการบริหารจัดการและการปฏิบัติงานของบุคลากรภายในองค์กรต่อไป

คำหลัก: *การบริหารความต่อเนื่องทางธุรกิจ; การสำรองและการกู้คืนข้อมูล; ศูนย์คอมพิวเตอร์สำรองกรณีเกิดภัยฉุกเฉิน*

Abstract

The advancement of information technology has increased and played a role in almost every activity within organizations and agencies in both the public and private sectors. Currently, there are various incidents occurring in various forms, such as cyber-attacks, natural disasters, protests, and fires. If these things happen, they will affect the organization's business activities in terms of image, reputation, confidence, and the organization's main income. Therefore, the organization should establish a business continuity management process to ensure that if an emergency occurs, the organization can still conduct business activities using the specified business continuity plan.

Business continuity management has various recommendations and management guidelines that organizations can use appropriately in their context. The basics of business continuity management include main activities such as creating a business continuity plan under various situations, data backup and recovery. If the organization considers, creates, reviews, and improves these things regularly, it will help reduce the impacts that may occur to the organization and help the organization manage business continuity effectively.

This article compiles business continuity management standards, data backup, data recovery, and backup computer centers in case of crises or emergencies. Along with providing examples of how these things can be applied within an organization to illustrate how they can be linked to the management and operations of personnel within the organization.

Keyword: *Business Continuity Management; Data Backup and Recovery; Disaster Recovery Site, DR Site*

1. บทนำ

ระบบสารสนเทศกลายเป็นหัวใจหลักของการดำเนินธุรกิจในยุคดิจิทัล องค์กรหรือหน่วยงานส่วนใหญ่ทั้งภาครัฐและเอกชนล้วนนำระบบสารสนเทศมาใช้ในองค์กรอย่างกว้างขวาง อาทิ ระบบ Web Site ขององค์กร ระบบไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail) หรือ ระบบเฉพาะทางต่าง ๆ เช่น ระบบการวางแผนทรัพยากรในองค์กร (Enterprise Resource Planning: ERP) ระบบการจัดการห่วงโซ่อุปทาน (Supply Chain Management: SCM) และระบบการบริหารจัดการความสัมพันธ์ลูกค้า (Customer Relationship Management: CRM) เป็นต้น ทำให้การใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศในการเข้าถึงข้อมูลขององค์กรจึงกลายเป็นเรื่องที่บุคลากรในองค์กรทุกคนคุ้นเคยและใช้ปฏิบัติงานอยู่ในชีวิตประจำวัน โดยอาศัยระบบสารสนเทศและระบบเครือข่ายเป็นโครงสร้างพื้นฐานในการทำงานของระบบต่าง ๆ ดังกล่าว แน่นอนว่าระบบสารสนเทศจะสามารถใช้งานได้จำเป็นต้องมีโครงสร้างพื้นฐานและอุปกรณ์ทางกายภาพสนับสนุน ตัวอย่างเช่น เครื่องคอมพิวเตอร์แม่ข่าย (Computer Server) ที่ใช้สำหรับติดตั้งซอฟต์แวร์ระบบและจัดเก็บข้อมูลที่ได้จากการใช้งานสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ทำหน้าที่ในการเชื่อมต่อระบบให้สามารถทำงานในหลาย ๆ จุดหรือเป็นเส้นทางในการแลกเปลี่ยนข้อมูลสารสนเทศ ระบบปรับอากาศทำหน้าที่รักษาอุณหภูมิไม่ให้เครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายคอมพิวเตอร์เกิดความร้อน และระบบไฟฟ้า ที่สนับสนุนการทำงานของระบบเครื่องแม่ข่าย เครือข่าย และระบบปรับอากาศ ซึ่งสิ่งเหล่านี้เป็นอุปกรณ์ทางกายภาพย่อมมีโอกาสเสื่อมสภาพและหยุดทำงานได้ ส่งผลให้ระบบสารสนเทศหยุดชะงักได้ หรือหากเกิดเหตุการณ์ไม่คาดคิด เช่น ไฟไหม้ น้ำท่วม ตึกถล่มบริเวณที่ติดตั้งระบบสารสนเทศ ล้วนเป็นเหตุให้ระบบสารสนเทศหยุดชะงักได้ เมื่อระบบสารสนเทศที่มีความสำคัญและถือเป็นหัวใจหลักที่ใช้ในการปฏิบัติงานเกิดการหยุดชะงักย่อมทำให้การดำเนินการทางธุรกิจขององค์กรเกิดความล่าช้าหรือหยุดชะงักได้ ซึ่งความล่าช้าหรือการหยุดชะงักของการให้บริการขององค์กรย่อมทำให้เกิดความเสียหายขององค์กรทั้งทางด้านภาพลักษณ์ ความพึงพอใจของผู้รับบริการที่มีต่อองค์กรตลอดจนรายได้ขององค์กร ดังนั้น เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กรเมื่อระบบสารสนเทศและเทคโนโลยีสารสนเทศหยุดชะงัก องค์กรจึงต้องให้ความสำคัญในการบริหารจัดการให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องภายใต้ภาวะวิกฤต

2. การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)

การบริหารความต่อเนื่องทางธุรกิจเป็นกระบวนการบริหารจัดการแบบองค์รวม (Holistic Management Process) ซึ่งองค์กรสามารถกำหนดปัจจัยเสี่ยงและผลกระทบที่อาจเกิดขึ้นได้จากปัจจัยเสี่ยงดังกล่าวว่ามีผลเสียหายต่อองค์กรมากน้อยเพียงใด หรือที่เรียกว่า “การวิเคราะห์ผลกระทบของปัจจัยเสี่ยงและเหตุการณ์ที่ไม่พึงประสงค์ต่อธุรกิจ (Business Impact Analysis: BIA)” และนำมาใช้ในการกำหนดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning: BCP) เพื่อองค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดภาวะฉุกเฉินหรือภาวะวิกฤต ตลอดจนลดผลกระทบจากการที่ระบบสารสนเทศไม่

สามารถให้บริการได้อย่างมีประสิทธิภาพ ซึ่งแผนความต่อเนื่องทางธุรกิจประกอบด้วย 5 ขั้นตอนหลัก [1] ได้แก่

2.1 ขั้นตอนการวิเคราะห์ (Analysis Phase)

เป็นขั้นตอนการวิเคราะห์การปฏิบัติงานทางธุรกิจที่สำคัญ (Critical Function) และการปฏิบัติงานทางธุรกิจทั่วไป (Non-Critical Function) ขององค์กร เพื่อวิเคราะห์ผลกระทบของความเสี่ยงและเหตุการณ์ที่ไม่พึงประสงค์ต่อธุรกิจ (Business Impact Analysis) ซึ่งจะให้ผู้บริหารระดับสูงขององค์กรพิจารณาจากตัวเลข 2 ชุด ได้แก่

1) ช่วงเวลาการหยุดชะงักของระบบสารสนเทศที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) ที่หากระยะเวลาเกินไปกว่าค่าที่กำหนดแล้ว จะส่งผลกระทบกับการดำเนินธุรกิจ หรือผู้รับบริการขององค์กร เช่น ธุรกิจการจัดส่งอาหารสดหากระบบไม่สามาถส่งได้ระยะเวลาที่องค์กรได้ทำสัญญากับลูกค้าไว้อาจเกิดการฟ้องร้องเกิดขึ้นได้ในความเสียหายที่ได้รับสินค้าล่าช้า หรือธุรกิจท่าอากาศยานหากระบบหยุดชะงักไปอาจจะส่งผลกับความปลอดภัยในการขึ้นลงของเครื่องบินได้ โดยค่า MTPD จะถูกใช้ในการกำหนดค่า “ระยะเวลาเป้าหมายในการฟื้นคืนสภาพของระบบ (Recovery Time Objective: RTO)” ทั้งนี้ ระบบที่กลับมาจะยังไม่ได้สมบูรณ์ทั้งหมด แต่องค์กรก็สามารถดำเนินธุรกิจต่อได้ ระยะเวลาเป้าหมายในการฟื้นคืนสภาพของระบบ (Recovery Time Objective: RTO) ที่แท้จริงจะได้จากการทดสอบการกู้คืนระบบประจำปี ทั้งนี้ ค่า RTO จะมีค่าน้อยกว่าค่า MTPD เสมอ

2) ระยะเวลาของข้อมูลสูญหายจากระบบที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (Recovery Point Objective: RPO) โดย ตัวอย่างเช่น กำหนดให้ค่า MTPD 24 ชั่วโมง ค่า RTO ที่เคยผ่านการทดสอบ 2 ชั่วโมง และ RPO มีค่า 1 ชั่วโมง เมื่อเกิดสถานการณ์ฉุกเฉินระบบล่มไม่สามารถใช้งานได้เมื่อเวลา 15.30 น. และจากการตรวจสอบพบว่าองค์กรทำการสำรองข้อมูล (Backup Data) ไว้ล่าสุดเมื่อเวลา 15.00 น องค์กรจะทำการกู้คืนข้อมูล (Restore Data) ที่สำรองไว้เมื่อเวลา 15.00 น. ขึ้นมาใช้งาน ผู้ดูแลระบบสามารถกู้คืนขึ้นมาใช้งานได้ภายในเวลา 17.00 น. แล้วองค์กรจะมีค่าการดำเนินการ RTO 1.5 ชั่วโมง และระยะเวลาข้อมูลที่สูญหายจากระบบ RPO 30 นาที (ตั้งแต่เวลา 15.00 น. (เวลาข้อมูลที่สำรองล่าสุด) ถึง 15.30 น. (เวลาที่ระบบไม่สามารถใช้งานได้) จากตัวอย่างเราจะพบว่าระบบที่กลับมามีการสูญหายของข้อมูล ดังนั้น หลังจากที่ระบบกลับมาจะมีกระบวนการนำข้อมูลที่สูญหายจากระบบกลับเข้าสู่ระบบให้สมบูรณ์ให้มากที่สุด รวมถึงระบบงานต่างที่ยังกู้คืนไม่เสร็จแต่ธุรกิจขององค์กรณ์ดำเนินการต่อได้แบบไม่สมบูรณ์แบบเราจะต้องกู้คืนให้แล้วเสร็จ เราเรียกระยะเวลาการดำเนินการทั้งสองส่วนนี้ว่า Work Recovery Time: WRT ซึ่งจะต้องดำเนินการให้แล้วเสร็จภายใน 22.5 ชั่วโมง หรือกล่าวอีกนัยว่า ค่า MTPD = ค่า RTO + ค่า WRT

2.2 ขั้นตอนการออกแบบวิธีการ (Solution Design Phase)

เป็นขั้นตอนที่นำค่า MTPD RTO WRT และ RPO มาทำการออกแบบวิธี การสำเนาข้อมูล การสำรองข้อมูล และวิธีการกู้คืนระบบ ให้ดำเนินการได้สอดคล้องกับระยะเวลาต่าง ๆ ที่กำหนด

2.3 การทำแผนปฏิบัติการ (Implementation Phase)

เป็นขั้นตอนการนำวิธีการสำรองข้อมูลและวิธีการกู้ข้อมูลที่ออกแบบไว้มาทำเป็นแผนปฏิบัติการ โดยเขียนแผนความต่อเนื่องทางธุรกิจที่สามารถนำไปใช้ปฏิบัติงานได้จริง

2.4 ขั้นตอนการซ้อมแผน (Testing and Organization Acceptance Phase)

เป็นขั้นตอนการทดสอบแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า หากเกิดเหตุการณ์ไม่พึงประสงค์ ภาวะฉุกเฉินหรือภาวะวิกฤตขึ้นจริง จะสามารถนำแผนปฏิบัติการจากขั้นตอนการทำแผนปฏิบัติการมาใช้งานจริงได้หรือไม่

2.5 ขั้นตอนการปรับปรุงแผน (Maintenance Phase)

เป็นขั้นตอนการทบทวนแผนความต่อเนื่องทางธุรกิจตั้งแต่การสำเนาข้อมูล การสำรองข้อมูล การปฏิบัติตามขั้นตอนการซ้อมแผน จนถึงการกู้ข้อมูลที่องค์กรได้จัดทำขึ้นว่า พบประเด็น ปัญหา อุปสรรคหรือสิ่งที่ต้องดำเนินการปรับปรุงแก้ไขเพื่อนำไปปรับปรุงแผนความต่อเนื่องทางธุรกิจให้สามารถใช้งานได้อย่างมีประสิทธิภาพต่อไป นอกจากนี้ยังรวมถึงการฝึกอบรมบุคลากรให้มีความรู้ และความเข้าใจในการนำแผนความต่อเนื่องทางธุรกิจมาใช้งานได้เมื่อภาวะฉุกเฉินหรือภาวะวิกฤตเกิดขึ้นจริง

3. มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ

การบริหารความต่อเนื่องทางธุรกิจเป็นแนวทางปฏิบัติสำหรับองค์กรเพื่อให้มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กร และจัดทำแผนความต่อเนื่องทางธุรกิจสำหรับการรับมือกับสถานการณ์ฉุกเฉินหรือสถานการณ์วิกฤตที่อาจเกิดขึ้นจริง ทั้งนี้ เพื่อให้องค์กรสามารถดำเนินการและตอบสนองแก่ผู้มีส่วนได้ส่วนเสียได้อย่างต่อเนื่อง โดยมาตรฐานการบริหารความต่อเนื่องทาง

ธุรกิจเป็นเครื่องมือหนึ่งที่สำคัญซึ่งช่วยส่งเสริมให้องค์กรสามารถป้องกันธุรกิจ ลดผลกระทบ และฟื้นฟูธุรกิจได้อย่างรวดเร็วจากสภาวะวิกฤตหรือสภาวะฉุกเฉิน ซึ่งมาตรฐานการบริหารความต่อเนื่องทางธุรกิจที่เป็นที่ยอมรับในระดับสากล อาทิ ISO 22301 และ BS 25999

3.1 มาตรฐาน ISO 22301: 2019 Security and resilience – Business continuity management systems

เป็นมาตรฐานที่ระบุข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจ ซึ่งประกอบด้วย การวางแผนการดำเนินการ การติดตาม การทบทวน การฝึกซ้อม การรักษาไว้ และการปรับปรุงกระบวนการบริหารความต่อเนื่องทางธุรกิจที่ได้จัดการไว้เป็นลายลักษณ์อักษร เพื่อใช้ในการบริหารความเสี่ยงทางธุรกิจทั้งหมดขององค์กรโดยใช้ PDCA Model

3.2 มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Standard: BS 25999)

ประกาศใช้โดย The British Standards Institution (BSI) ประเทศอังกฤษ ประกอบด้วยมาตรฐาน 2 ฉบับ (กิตติพงศ์, 2555) คือ

- BS 25999- 1: 2006 – Part 1: Business Continuity Management. Code of Practices เป็นแนวปฏิบัติที่ดีและข้อแนะนำให้ปฏิบัติแต่ไม่บังคับ สำหรับองค์ที่ต้องการจะดำเนินการด้านการจัดการความต่อเนื่องทางธุรกิจตามข้อกำหนด
- BS 25999-2: 2007 – Part 2: Specification for Business Continuity Management เป็นข้อกำหนดภาคบังคับที่ต้องปฏิบัติและสามารถต่อยอดไปยังการรับรองมาตรฐานโดยหน่วยตรวจสอบและรับรองคุณภาพ (Certification Body: CB)

4. การสำรองข้อมูล (Data Backup) และการกู้ข้อมูล (Data Restore)

การสำรองข้อมูลเป็นสิ่งที่สำคัญสำหรับการบริหารความต่อเนื่องทางธุรกิจ ซึ่งการสำรองข้อมูล หมายถึง การคัดลอกข้อมูล เช่น ไฟล์ ฐานข้อมูล ระบบคอมพิวเตอร์ ระบบคอมพิวเตอร์เสมือน (Computer Virtualization) ในช่วงเวลาใดช่วงเวลาหนึ่งไปจัดเก็บไว้ยังสถานที่เก็บอื่น ๆ เพื่อการเก็บรักษาและกู้คืนข้อมูลขึ้นมาใช้งานในกรณีที่อุปกรณ์ขัดข้องหรือเกิดภัยพิบัติ กระบวนการสำรองข้อมูลที่ดีและถูกต้องมีความสำคัญต่อความสำเร็จของแผนการกู้คืนข้อมูลภายหลังจากการเกิดสถานการณ์ฉุกเฉินหรือสถานการณ์วิกฤต นอกจากนี้การสำรองข้อมูลยังช่วยลดความเสี่ยงที่เกิดจากซอฟต์แวร์มีปัญหา ข้อมูลเสียหาย ฮาร์ดแวร์เสีย การถูกแฮ็กระบบ และข้อผิดพลาดของผู้ใช้หรือเหตุการณ์ที่ไม่คาดคิดอื่น ๆ ซึ่งการสำรองข้อมูลมีหลากหลายรูปแบบ อาทิ การสำรองข้อมูลภายในองค์กร (On-Premises Backup) การสำรองข้อมูลภายนอกองค์กร (Off-Site Backup) การสำรองข้อมูลแบบ Appliance (Appliance Storage Backup) การสำรองข้อมูลแบบคลาวด์ (Cloud Backup) และการสำรองข้อมูลสำหรับเซิร์ฟเวอร์ (Physical Backup)

การกู้ข้อมูล เป็นกระบวนการที่ทำให้ข้อมูลที่สูญหาย ข้อมูลที่เสียหาย และข้อมูลที่ไม่สามารถใช้งานได้จากสื่อเทปสำรองข้อมูลหรืออุปกรณ์สำรองข้อมูลให้กลับมาใช้งานได้ตามปกติ ซึ่งผลสำเร็จในการกู้ข้อมูลจะมากหรือน้อยนั้นขึ้นอยู่กับสาเหตุที่ทำให้ ข้อมูลนั้นใช้การไม่ได้ และการกระทำกับข้อมูลหลังจากที่เกิดความเสียหาย

ปัจจุบันมีการพัฒนาเทคนิคและเทคโนโลยีของการสำรองข้อมูลอย่างต่อเนื่อง ส่งผลให้มีหลากหลายเทคนิคและเทคโนโลยีของการสำรองข้อมูล ซึ่งองค์กรสามารถนำเทคโนโลยีดังกล่าวมาประยุกต์ใช้ให้เหมาะสมกับข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และข้อกำหนดหรือความต้องการในส่วนของระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉินขึ้นและระยะเวลาของข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง ทั้งนี้ การพิจารณาเลือกเทคโนโลยีที่จะนำมาใช้ในการสำรองข้อมูลยังขึ้นอยู่กับความสามารถของแอปพลิเคชันสำรองข้อมูลอีกด้วย ซึ่งประเภทของการสำรองข้อมูล [4] มีดังนี้

4.1 Full Backup

เป็นการรวบรวมสำเนาของชุดข้อมูลทั้งหมดบันทึกใส่เทปสำรองข้อมูลหรืออุปกรณ์สำหรับสำรองข้อมูลอื่น ๆ ถือได้ว่าเป็นวิธีสำรองข้อมูลที่น่าเชื่อถือที่สุด แต่การสำรองข้อมูลทั้งหมดนั้นใช้เวลานานและต้องใช้เทปสำรองข้อมูลหรืออุปกรณ์สำรองข้อมูลเป็นจำนวนมาก องค์กรส่วนใหญ่เรียกใช้การสำรองข้อมูล Full Backup ทั้งหมดเป็นครั้ง ๆ คือ สัปดาห์ละ 1 ครั้ง หรือเดือนละ 1 ครั้ง

4.2 Incremental Backup

เป็นการสำรองข้อมูลเฉพาะส่วนเพิ่มหรือสำรองเฉพาะข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองข้อมูลจากครั้งล่าสุด ข้อเสียคือการกู้คืนข้อมูลทั้งหมดจะใช้เวลานาน เพราะต้องนำข้อมูลจากการสำรองข้อมูลแบบ Full Backup มาใช้ร่วมกับการสำรองข้อมูล Incremental ทั้งหมดที่มี

4.3 Differential Backup

เป็นการสำรองข้อมูลเฉพาะส่วนต่างจาก Full Backup โดยทำการคัดลอกข้อมูลที่เปลี่ยนแปลงไปจากการสำรองข้อมูลทั้งหมด Full Backup ครั้งล่าสุด ซึ่งช่วยให้การกู้คืนทั้งหมดเกิดขึ้นได้รวดเร็วยิ่งขึ้นโดยต้องการกู้คืนเฉพาะการสำรองข้อมูลแบบ Full Backup ล่าสุดและการสำรองข้อมูล Differential Backup ส่วนต่างล่าสุด ตัวอย่างเช่น หากคุณสร้างข้อมูลสำรองแบบ Full Backup ในวันจันทร์ ข้อมูลสำรอง Differential Backup ของวันอังคารจะคล้ายกับการสำรองข้อมูลส่วนเพิ่ม ณ จุดนั้น การสำรองข้อมูลของวันพุธจะสำรองข้อมูลส่วนต่างที่เปลี่ยนไปตั้งแต่การสำรองข้อมูล Full Backup ของวันจันทร์ ข้อเสียคือ การเพิ่มของข้อมูลของการสำรองข้อมูล Differential Backup ส่วนต่างมีแนวโน้มที่จะมากขึ้นและส่งผลเสียต่อระยะเวลาในการสำรองข้อมูล การกู้คืนข้อมูล จะนำข้อมูลจากการสำรองข้อมูลแบบ Full Backup มาใช้ร่วมกับการสำรองข้อมูล Differential Backup 1ชุด ที่เกิดจากการสำรองข้อมูลภายหลังการสำรองแบบ Full Backup

4.4 Synthetic full backup

เป็นการผสมผสานระหว่าง Full Backup และ Incremental Backup โดยระบบจะสร้างข้อมูลการรวบรวมสำเนาของชุดข้อมูลทั้งหมด (Full Backup) ก่อน จากนั้นระบบจะทำการสำรองข้อมูลเฉพาะส่วนเพิ่ม (Incremental Backup) และระบบการสำรองข้อมูลจะนำข้อมูลที่สำรองข้อมูลทั้งสองส่วนรวมเข้าด้วยกัน เพื่อทำเป็นสำเนาข้อมูลทั้งหมดอีกครั้ง จากนั้นก็จะทำการสำรองข้อมูลเฉพาะส่วนเพิ่ม (Incremental Backup) และทำการรวมข้อมูลซ้ำเช่นนี้ไปเรื่อย ๆ จะทำให้ได้เสมือนการสำรองข้อมุลแบบ Full Backup ในทุกๆครั้ง

4.5 Incremental-forever backup

เป็นการสำรองข้อมูลทั้งหมด (Full Backup) 1 ครั้ง หลังจากนั้นจะสำรองข้อมูลเฉพาะส่วนที่แตกต่าง (Incremental) ครั้งล่าสุด ทุกครั้งที่มีการสำรองข้อมูลเฉพาะส่วนที่แตกต่าง(Incremental) ระบบการสำรองข้อมูลจะดำเนินการรวบรวมข้อมูลส่วนต่างที่ถูกสำรองไว้ก่อนหน้ากับข้อมูลส่วนต่างที่สำรองข้อมูลครั้งล่าสุดเข้าด้วยกัน เพื่อให้มีชุดการการสำรองข้อมูลส่วนต่างเพียง 1ชุด การกู้คืนข้อมูลจะใช้การสำรองข้อมูลทั้งหมด (Full Backup) ร่วมกับ ชุดข้อมูลส่วนต่างที่ระบบสำรองข้อมูลมีการรวบรวมไว้ล่าสุด ซึ่งการสำรองแบบนี้จะลดระยะเวลาในการสำรองข้อมูล ในขณะเดียวกันก็ทำให้สามารถกู้คืนข้อมูลที่รวดเร็วยิ่งขึ้น

4.6 Reverse-incremental backups

เป็นการสำรองข้อมูลที่รวมส่วนแตกต่างที่เกิดขึ้นระหว่างสองชุดสำรองข้อมูล เมื่อทำการสำรองข้อมูล Full Backup ครั้งแรกเสร็จสิ้น การสำรองข้อมูลส่วน Incremental ครั้งถัดมาจะถูกรวมเข้าสู่ชุดสำรองข้อมูล Full Backup ก่อนหน้าเป็นการสร้างชุดข้อมูล Full Backup ใหม่ การสำรองข้อมูลแบบนี้จะได้ชุดข้อมูล Full Backup ล่าสุดตลอดเวลา และเมื่อมีการทำการสำรองข้อมูล Incremental ในครั้งถัดไป ก็จะได้ชุดข้อมูล Full Backup ใหม่อีกครั้ง และข้อมูลที่แตกต่างจะถูกจัดเก็บเป็นชุด Incremental ก่อนหน้า

การสำรองข้อมูลจะขึ้นอยู่กับความสำคัญของข้อมูลหรือแอปพลิเคชันสำหรับธุรกิจที่เกี่ยวข้อง กระบวนการนี้ควบคุมโดยนโยบายการสำรองข้อมูล (Backup Disaster Recovery Policy) ที่กำหนดไว้ล่วงหน้าขององค์กร ซึ่งการระบุความถี่ในการสำรองข้อมูลและจำนวนสำเนาที่ซ้ำกันเป็นสิ่งจำเป็นเช่นเดียวกับข้อตกลงระดับการให้บริการที่กำหนดว่าข้อมูลจะต้องสามารถกู้คืนได้ภายในระยะเวลาเท่าใด สำหรับแนวทางปฏิบัติที่ดีที่สุดควรมีการกำหนดเวลาสำรองข้อมูลทั้งหมด (Full Backup) อย่างน้อยสัปดาห์ละครั้ง โดยมากจะทำในช่วงสุดสัปดาห์หรือนอกเวลาทำการ นอกจากการสำรองข้อมูลทั้งหมดแบบรายสัปดาห์ องค์กรต้องกำหนดเวลาสำรองข้อมูลส่วนต่างหรือส่วนเพิ่มที่สำรองเฉพาะข้อมูลที่เปลี่ยนแปลงตั้งแต่มีการสำรองข้อมูลทั้งหมดตามระดับความสำคัญและความต้องการในการกู้คืนข้อมูลที่ระบุในนโยบาย ในส่วนของข้อแนะนำสำหรับการสำรองข้อมูลองค์กรอาจยึดกฎ 3-2-1 Backup Rule [5] ซึ่งมีหลักสำคัญ ดังนี้

- สำรองข้อมูลอย่างน้อย 3 ชุด ได้แก่ ข้อมูลหลักต้นฉบับ (Production Data) บนเครื่องคอมพิวเตอร์หลัก 1 ชุด และข้อมูลสำรอง (Backup) อีก 2 ชุด การมีข้อมูลสำรองหลายชุดจะช่วยลดความเสี่ยงที่ข้อมูลทั้งหมดจะเสียหายในคราวเดียว ยกตัวอย่างเช่น ถ้าอุปกรณ์ที่เก็บข้อมูลชุดใดชุดหนึ่งมีโอกาสเสียหายได้ 1% (1 ใน 100) เมื่อมีข้อมูลสำรอง 2 ชุด ความเสี่ยงที่ข้อมูลจะหายทั้งหมดจะลดลงเหลือเพียง 0.01% (1 ใน 10,000) และถ้ามีสำรองถึง 3 ชุด ความเสี่ยงก็จะยิ่งลดลงไปอีกเหลือ 0.0001% (1 ใน 1,000,000) เลยทีเดียว
- ใช้อุปกรณ์ 2 ชนิดในการสำรองข้อมูล (2 Different Media) เพื่อป้องกันความเสียหายหากอุปกรณ์ชนิดใดชนิดหนึ่งมีปัญหา เช่น ควรมีทั้ง Backup บน Internal Hard Disk, External Hard Disk, NAS (Network Attached Storage), Tape หรือ Cloud Storage เป็นต้น
- เก็บข้อมูลสำรองอย่างน้อย 1 ชุดไว้นอกสถานที่ (1 Offsite Backup) ป้องกันในกรณีที่เกิดเหตุการณ์ร้ายแรงใน

บริเวณกว้าง เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ฯลฯ ซึ่งอาจทำให้ข้อมูลสำรองที่เก็บในสถานที่เดียวกันเสียหายไปด้วย

ทั้งนี้ องค์กรสามารถกำหนดสถานที่สำหรับการจัดเก็บข้อมูลที่สำรองไว้ ณ สาขาต่าง ๆ ขององค์กร หรือจัดเก็บไว้ ณ ศูนย์คอมพิวเตอร์สำรองกรณีเกิดภัยฉุกเฉิน (Disaster Recovery Site) หรือบน Cloud ซึ่งไม่ได้อยู่ในพื้นที่เดียวกันเพื่อกระจายความเสี่ยง (ดิจิตอล ดิสทริบิวชั่น, 2565)

5. ศูนย์คอมพิวเตอร์สำรองกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉิน (Disaster Recovery Site: DR Site)

ในยุคดิจิทัลองค์กรและหน่วยงานต่าง ๆ ใช้เทคโนโลยีและระบบสารสนเทศในการดำเนินงานทางธุรกิจขององค์กรอย่างกว้างขวาง ความเสี่ยงสำคัญสำหรับองค์กรในยุคดิจิทัลนี้ คือ การที่ข้อมูลสูญหายหรือระบบไม่พร้อมใช้งานซึ่งอาจเกิดจากระบบหลักไม่สามารถใช้งานได้หรือเกิดความเสียหายจากภัยพิบัติตามธรรมชาติหรือจากฝีมือของมนุษย์ เหตุการณ์ดังกล่าวสามารถสร้างความเสียหายให้กับองค์กรได้อย่างมากมายทั้งในด้านมูลค่าความเสียหาย ภาพลักษณ์ขององค์กร ตลอดจนความเชื่อมั่นจากผู้มีส่วนได้ส่วนเสีย เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นแนวทางหนึ่งที่นิยมใช้ในปัจจุบัน คือ การสำรองข้อมูลที่สำคัญขององค์กรไว้ ณ “ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉิน (Disaster Recovery Site: DR Site)” หรือการทำระบบ Disaster Recovery ซึ่งสามารถทำได้หลายวิธีการและหลายสถานที่ ในกรณีที่ทำการสำรองข้อมูลไปยังในสถานที่ ๆ ไม่ใช่ที่เดียวกับศูนย์ข้อมูลหลัก (Data Center) โดยแบ่งประเภทของ DR Site ออกเป็น 3 ประเภท ได้แก่

5.1 Hot Site

ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินที่มีระบบทุกอย่างเหมือนศูนย์ข้อมูลหลักทุกประการ ไม่ว่าจะเป็นซอฟต์แวร์ (Software) หรือฮาร์ดแวร์ (Hardware) ซึ่ง Hot Site จะมีการสำรองข้อมูลของระบบหลักอยู่ตลอดเวลา ในกรณีที่ระบบหลักไม่สามารถใช้งานได้หรือหยุดทำงาน (Downtime) ฮาร์ดแวร์และซอฟต์แวร์ ณ Hot Site จะสามารถทำงานแทนได้ทันที เพื่อให้ผู้ใช้ได้รับผลกระทบน้อยที่สุด

5.2 Warm Site

ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินที่มีระบบการสำรองข้อมูลเป็นระยะ ๆ ไม่ได้มีการสำรองข้อมูลของระบบหลักอยู่ตลอดเวลาเช่นเดียวกับ Hot Site เมื่อเกิดเหตุการณ์ที่ระบบหลักไม่สามารถใช้งานได้หรือหยุดทำงาน ผู้รับผิดชอบ และ/หรือผู้เกี่ยวข้องจะต้องใช้เวลาในการดำเนินการติดตั้ง ตั้งค่า กู้ข้อมูล เพื่อเตรียมระบบให้พร้อมใช้งานก่อนที่จะเปิดใช้งานศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน

5.3 Cold Site

ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินที่มีการสำรองข้อมูลของระบบหลักไว้บ้างบางส่วน เช่น อาจเป็นเพียงการส่งเทปสำรองข้อมูลไปยังสถานที่ที่เตรียมไว้ เมื่อเกิดเหตุการณ์ที่ระบบหลักไม่สามารถใช้งานได้หรือหยุดทำงาน จำเป็นต้องมีผู้เชี่ยวชาญ ผู้รับผิดชอบ และ/หรือผู้เกี่ยวข้องเข้ามาดูแลและตั้งค่าก่อนเปิดใช้งาน จึงใช้เวลานานกว่าจะสามารถเปิดใช้งานศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินได้

ตารางที่ 1 เปรียบเทียบ DR site ในด้านต่าง ๆ

รูปแบบ DR Site	ความพร้อมด้าน Infrastructure	การสูญหายของข้อมูลเมื่อระบบเปิดใช้งานที่ DR site
Hot	มี	ไม่มี
Warm	มี	สูญหายตามระยะเวลาที่องค์กรยอมรับได้
Cold	ไม่มี	ขึ้นกับความสำเร็จของการสำรองข้อมูลระบบนั้น ๆ

หมายเหตุ: ปัจจัยที่ทำให้ระยะเวลาการสูญหายของข้อมูลเป็นไปตามที่กำหนดขึ้นกับความสามารถทางด้าน Infrastructure เช่น Speed Network ขนาดของเครื่องแม่ข่าย และความสามารถการเขียนข้อมูล Storage และปริมาณข้อมูลที่ต้องทำการสำรอง

ข้อเปรียบเทียบการมีศูนย์คอมพิวเตอร์สำรองกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉิน

ข้อดี

1) องค์กรมั่นใจได้ว่าเมื่อเกิดสถานการณ์ฉุกเฉินหรือสถานการณ์วิกฤต องค์กรสามารถดำเนินกิจการได้อย่างต่อเนื่อง

2) ข้อมูลสำคัญขององค์กรได้รับการปกป้องไว้ในระดับหนึ่งจากการสำรองข้อมูลและการกู้คืนข้อมูล

ข้อเสีย

1) ค่าใช้จ่ายในการเก็บรักษาข้อมูล ซึ่งองค์กรต้องพิจารณาความสำคัญของข้อมูล และงบประมาณขององค์กร

ที่จะใช้ลงทุนในส่วนของศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินเป็นปัจจัยสำคัญในการเลือก

2) องค์กรจำเป็นต้องวิเคราะห์และประเมินสถานการณ์ (Scenario) ต่างๆ ที่อาจเกิดขึ้นกับระบบสารสนเทศและระบบคอมพิวเตอร์ขององค์กร สถานการณ์ที่อาจเกิดขึ้น องค์กรต้องกำหนดระยะเวลาสำหรับการแก้ไขสถานการณ์นั้น ๆ และพิจารณากำหนดระยะเวลาการดำเนินธุรกิจขององค์กรว่าสามารถรอได้นานมากน้อยเพียงใด

6. การบริหารความต่อเนื่องของโรงพยาบาลศิริราชกับการให้บริการผู้ป่วยในยุคดิจิทัล

โรงพยาบาลศิริราช คณะแพทยศาสตร์ศิริราชพยาบาล นำระบบสารสนเทศและเทคโนโลยีสารสนเทศเข้ามาใช้ในการให้บริการผู้ป่วยในทุกกิจกรรมที่เกี่ยวข้องกับการรักษาผู้ป่วย อาทิ การลงทะเบียนผู้ป่วยใหม่ การเปิดสิทธิ์ที่ใช้ในการรักษา การจัดลำดับ (Queue) เข้ารับการรักษา การตรวจวิเคราะห์ทางห้องปฏิบัติการ การตรวจวินิจฉัยทางรังสีวิทยา การสั่ง-จ่ายยา และการชำระเงินค่ารักษา ทั้งนี้ การนำระบบสารสนเทศมาสนับสนุนการทำงานในกิจกรรมต่าง ๆ นั้นมีวัตถุประสงค์เพื่อให้การปฏิบัติงานและการบริการผู้ป่วยได้รับความสะดวก รวดเร็ว ลดความผิดพลาดในการประมวลผลจากบุคลากร ข้อมูลที่ได้จากการทำกิจกรรมต่าง ๆ ถูกจัดเก็บอย่างเป็นระเบียบ มีรูปแบบที่ชัดเจนมีมาตรฐานเดียวกัน สามารถเรียกดูย้อนหลังและสอบทานได้ รวมถึงสามารถใช้ข้อมูลร่วมกันเพื่อไม่ให้การทำงานเกิดความซ้ำซ้อน ตัวอย่างเช่น เมื่อมีการลงทะเบียนข้อมูลผู้ป่วยจากเวชระเบียนแล้ว ข้อมูลพื้นฐานของผู้ป่วย เช่น HN ชื่อ-นามสกุล และสิทธิการรักษา จะสามารถนำมาใช้ในระบบการสั่งตรวจวิเคราะห์ทางห้องปฏิบัติการ การสั่ง-จ่ายยา การรับชำระเงิน เป็นต้น

ข้อมูลสารสนเทศที่บันทึกเข้าระบบต่าง ๆ ในการให้บริการผู้ป่วย ตัวอย่างเช่น ใบต่อเวชระเบียนผู้ป่วย ใบสั่งยา ข้อมูลการสั่งตรวจวิเคราะห์ทางห้องปฏิบัติการ จะถูกจัดเก็บไว้ในเครื่องแม่ข่าย (Server) ณ ศูนย์ข้อมูลหลักของคณะฯ ส่งผลให้ศูนย์ข้อมูลหลักมีความสำคัญเป็นอย่างยิ่ง โดยภายในศูนย์ข้อมูลหลักประกอบด้วยอุปกรณ์ทางกายภาพที่ใช้สนับสนุนการทำงานของระบบสารสนเทศ อาทิ เครื่องแม่ข่ายสำหรับระบบงาน (Application Server) เครื่องแม่ข่ายสำหรับจัดเก็บข้อมูล (Database Server) ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ระบบปรับอากาศ ระบบไฟฟ้า ระบบดับเพลิง และระบบควบคุมความชื้น ซึ่งสิ่งต่าง ๆ เหล่านี้ต้องได้รับการดูแลและบำรุงรักษาอย่างต่อเนื่อง เพื่อสนับสนุนให้ระบบสารสนเทศทำงานได้อย่างเต็มประสิทธิภาพ อย่างไรก็ตามอุปกรณ์ทางกายภาพย่อมมีโอกาสเสื่อมสภาพและขัดข้องส่งผลให้ระบบสารสนเทศหยุดชะงักได้ หรือหากเกิดเหตุการณ์ไม่คาดคิด เช่น ไฟไหม้ น้ำท่วม ตึกถล่ม ณ บริเวณที่ติดตั้งของศูนย์ข้อมูลหลักก็ทำให้ระบบสารสนเทศหยุดชะงักได้เช่นกัน เมื่อระบบสารสนเทศที่ให้บริการเกิดการหยุดชะงักไป ย่อมทำให้การดำเนินการให้บริการตรวจรักษาผู้ป่วยเกิดความล่าช้าหรือหยุดชะงักได้ ส่งผลให้เกิดความเสียหายต่อโรงพยาบาลศิริราชทั้งทางด้านภาพลักษณ์ ความพึงพอใจของผู้รับบริการและรายได้ของโรงพยาบาลศิริราช

ด้วยเหตุนี้โรงพยาบาลศิริราช คณะแพทยศาสตร์ศิริราชพยาบาล จึงจัดตั้งศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน และได้กำหนดแผนความต่อเนื่องทางธุรกิจของระบบสารสนเทศสำหรับการให้บริการตรวจรักษาผู้ป่วย เพื่อบริหารจัดการให้โรงพยาบาลศิริราชสามารถดำเนินการให้บริการผู้ป่วยของโรงพยาบาลศิริราชได้อย่างต่อเนื่อง อีกทั้งยังลดผลกระทบที่ทำให้เกิดความเสียหายต่อโรงพยาบาลศิริราชในกรณีที่เกิดสภาวะวิกฤตหรือสภาวะฉุกเฉิน ในการดำเนินการดังกล่าวเริ่มต้นจากการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อให้ทราบว่าหากระบบสารสนเทศเกิดการหยุดชะงักกิจกรรมใดบ้างที่ได้รับผลกระทบ และระดับความรุนแรงของผลกระทบมากน้อยเพียงใด กิจกรรมใดไม่สามารถดำเนินการได้หากไม่มีระบบสารสนเทศหรือกิจกรรมใดสามารถดำเนินการได้ด้วยวิธีแบบดั้งเดิม (Manual) ตัวอย่างเช่น ปัจจุบันแพทย์สามารถเรียกดูข้อมูลประวัติการรักษาของผู้ป่วยผ่านระบบสารสนเทศของโรงพยาบาลศิริราชที่ชื่อ Si-iScan ซึ่งเมื่อระบบ Si-iScan หยุดชะงักไม่สามารถใช้งานได้ก็จะส่งผลให้แพทย์ไม่สามารถค้นหาหรือเรียกดูข้อมูลประวัติการรักษาของผู้ป่วยได้ จำเป็นจะต้องเรียกดูข้อมูลจากแฟ้มประวัติการรักษาของผู้ป่วยที่จัดเก็บในรูปแบบแฟ้มกระดาษ ดังนั้น กระบวนการที่งานเวชระเบียนจะนำแฟ้มประวัติการรักษาดังกล่าวไปส่งให้แพทย์ ณ ห้องตรวจต่าง ๆ จะต้องทำอย่างไร และมีขั้นตอนการดำเนินการอย่างไรต้องมีการกำหนดไว้ให้ชัดเจน

ทั้งนี้การทำงานระบบงานต่าง ๆ จะมีเงื่อนไขการยอมรับการหยุดชะงักของระบบสารสนเทศที่แตกต่างกัน เช่น ถ้าระบบการเรียกเก็บเงินต้นสังกัดจะต้องดำเนินการให้แล้วเสร็จภายในกี่วันหลังจากผู้ป่วยในออกจากโรงพยาบาล หรือการดำเนินการด้วยวิธีแบบดั้งเดิม (Manual) จะมีขีดความสามารถดำเนินการได้ในระยะช่วงเวลาหนึ่งก็จะทำให้ไม่สามารถให้บริการได้ทัน เช่นระบบการเงิน หากขณะที่ระบบทำงานได้ปกติสามารถออกใบเสร็จคิดค่าใช้จ่ายได้ภายใน 1 นาที เมื่อระบบสารสนเทศเกิดการหยุดชะงักไปจะต้องดำเนินการคิดค่าใช้จ่ายและใบเสร็จด้วยเจ้าหน้าที่การเงิน ซึ่งจะมีระยะเวลาการดำเนินการที่มากขึ้น ก็จะเกิดการรอคิวสะสม การคิดค่ารักษาพยาบาลจนไม่สามารถ

ดำเนินการให้แล้วเสร็จภายในวันได้ ระยะเวลาเช่นนี้จะถูกนำมาพิจารณาเป็นค่าระยะเวลาที่ระบบใช้งานไม่ได้ที่สามารถยอมรับได้ (MTPD)

สำหรับแนวทางการรับมือและการลดโอกาสเกิดกรณีที่เกิดสภาวะวิกฤตหรือสภาวะฉุกเฉินอันส่งผลให้ระบบสารสนเทศการให้บริการผู้ป่วย ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล ได้ดำเนินการจัดทำกระบวนการเพื่อรองรับกับสถานการณ์ ดังนี้

1) การสร้างกระบวนการดูแลและบำรุงรักษาศูนย์ข้อมูลหลักอย่างเป็นระบบ โดยอ้างอิงมาตรฐานสากลสำหรับระบบการจัดความมั่นคงปลอดภัยของข้อมูล (Information Security Management System: ISMS) ซึ่งกำหนดให้มีการควบคุมระบบไฟฟ้า อุณหภูมิ การควบคุมความชื้นและการระบายอากาศ ระบบดับเพลิง การควบคุมพื้นที่และการเข้า-ออก ตลอดจนกำหนดให้มีเจ้าหน้าที่เฝ้าระวังคอยตรวจสอบและควบคุมการทำงานของระบบต่าง ๆ ภายในศูนย์ข้อมูลหลัก

2) การดำเนินการสำรองข้อมูลอย่างเป็นระบบ คือ การจัดทำข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ของการสำรองข้อมูลของระบบงานต่าง ๆ โดยแบ่งระดับการสำรองข้อมูลระบบงานเป็น 5 ระดับ ดังนี้

ตารางที่ 2 ระดับการสำรองข้อมูลของระบบงาน

SLA	Disk			Tape		ระบบ
	Daily	Weekly	Monthly	Daily	Monthly	
	Retention Period			Retention Period		
L1 Critical	14D	1M	-	3M	1Y	ระบบ ERP (SAP), ระโรงพยาบาล
L2 High	7D	1M	-	3M	1Y	ระบบสำนักงาน , ระบบการศึกษา, ระบบ Web คณะฯลฯ
L3.1 Normal	-	1M	-	2M	-	ระบบ File server คณะ ระบบสำนักงานอื่นๆ
L3.2 Normal	-	1M	-	2M	-	เครื่องแม่ข่าย (VM)
L3.3 Normal	-	-	1M	2M		เครื่องแม่ข่ายของระบบงานที่อยู่ใน SLA L1,L2 ,L3.1 (VM)
L4 Low	-	1M	-	-	-	ฐานข้อมูล Test/UAT/Develop
L5 Lowest	-	-	1M	-	-	เครื่องแม่ข่าย Test/UAT/Develop (VM)

ตัวอย่างเช่น ระบบสแกนเอกสารเวชระเบียนของผู้ป่วย ซึ่งมีรูปแบบการทำงานของระบบแบบ Windows Application มีการจัดเก็บข้อมูลในรูปแบบฐานข้อมูล MS-SQL และมี Web API ในการแลกเปลี่ยนข้อมูล ดังนั้น การดำเนินการสำรองข้อมูลจะประกอบไปด้วย SLA L1, L3.2 และ L3.3 กล่าวคือ L1 เป็นฐานข้อมูล MS-SQL, L3.2 เครื่องแม่ข่าย (VM) สำหรับ Web service และ L3.3 เครื่องแม่ข่าย (VM) สำหรับติดตั้งฐานข้อมูล MS-SQL การสำรองข้อมูล SLA โดยที่ L1 จะทำการ Backup ทุก ๆ วัน โดยจัดทำเป็น Image Backup ในวันจันทร์-เสาร์ ให้เป็นการสำรองข้อมูลแบบรายวัน (Daily) และเก็บไว้บน Storage Appliance Deduplication หรือ Storage สำหรับเก็บข้อมูลการสำรองข้อมูลด้วยรูปแบบการจัดเก็บแบบหากพบ Image ใดที่มีรูปแบบที่ซ้ำกันจะเก็บเพียง Image เดียวและจัดทำดัชนีรายการกำกับไว้) และดำเนินการเก็บรักษา (Retention) ในส่วนของ Image Backup ไว้ทั้งสิ้น 14 วัน นับจาก Backup Success จะจัดทำเป็น Image Backup ในวันอาทิตย์ สัปดาห์ที่ 2-5 ให้เป็นการสำรองข้อมูลแบบรายสัปดาห์ (Weekly) และดำเนินการเก็บรักษา (Retention) ในส่วนของ Image Backup ไว้ทั้งสิ้น 1เดือน นับจาก Backup Success จากนั้นจะเข้าสู่กระบวนการเก็บข้อมูลของ Image Backup ในช่วงวันอาทิตย์ สัปดาห์แรกของเดือน ให้เป็นการสำรองข้อมูลแบบรายเดือน (Monthly) ซึ่งเป็นการจัดเก็บลงบน Physical tape จากนั้นเข้าสู่กระบวนการเก็บรักษาแบบราย 3 เดือน ต่อไป นอกจากนี้ทุก ๆ วันอาทิตย์ สัปดาห์แรกของปีระบบจะจัดเก็บข้อมูลในรูปแบบรายปี (Yearly) อีก 1 ครั้ง สำหรับการสำรองข้อมูลในส่วนของ SLA อื่น ๆ จะมีความถี่การสำรองข้อมูลและการเก็บรักษาที่แตกต่างกันดังตารางที่ 2 ส่วนประเภทการสำรองข้อมูลจะเป็น Full back up, Increase mental, Differential ขึ้นกับระยะเวลาในการสำรองข้อมูลแล้วเสร็จที่มีปัจจัยมาจาก ขนาดของข้อมูลที่ทำการสำรองข้อมูล ความสามารถในการทำ Deduplication ของ Storage ที่ใช้จัดเก็บImage backup ความสามารถของ Backup Software และความสามารถของเครือข่าย ทั้งนี้จะปรับให้เหมาะสมกับระบบนั้น ๆ โดยเน้นการสำรองข้อมูลแบบ Full backup เป็นอันดับแรกเพื่อประสิทธิภาพการกู้คืนข้อมูล

Job Policy	Elapsed Time	Kilobytes	KB/Sec	Job Schedule
02_L3.1_DD_Fileserv...	02:29:35	14,366,954,202	1,639,937	Daily_Sched
02_L3.1_DD_Fileserv...	02:36:36	14,366,932,905	1,554,347	Daily_Sched
02_L3.1_DD_Fileserv...	02:27:35	14,335,261,307	1,654,826	Daily_Sched
02_L3.1_DD_Fileserv...	02:27:12	14,335,195,479	1,656,148	Daily_Sched
02_L3.1_DD_Fileserv...	02:31:10	14,331,810,875	1,613,348	Daily_Sched
02_L3.1_DD_Fileserv...	13:23:48	14,313,866,356	297,104	Weekly_Sched_Force

รูปที่ 1 แสดงตัวอย่างผลการสำรองข้อมูลผ่าน NetBackup software

แสดงการสำรองข้อมูลแบบ Full Backup ของเครื่องแม่ข่ายเสมือน(Virtual Machine) ที่ทำหน้าที่เป็น File server มีขนาด 14 TB ใช้ระยะเวลาการสำรอง 2.5 ชั่วโมง และ 13.5 ชั่วโมง โดยประมาณ สาเหตุที่มีระยะเวลา 2 ค่า เพราะความสามารถของ Backup Software ที่สามารถ Backup ส่วนต่างแล้ว Merge เข้ากับ ข้อมูลที่มีการสำรองก่อนหน้าให้เป็นการสำรองข้อมูลเป็นแบบ Full Backup แต่ทั้งนี้เราต้องให้ระบบมีการสำรองข้อมูลแบบ Full Backup แบบอ่านข้อมูลต้นทางทั้งหมดอาทิตย์ละครั้งเพื่อเพิ่มความมั่นใจในข้อมูลที่ถูกสำรอง ข้อมูลที่ถูกสำรอง มีการเก็บทั้งใน Storge ที่ใช้สำรองข้อมูลภายใน Datacenter หลัก Tape สำรองข้อมูลที่จัดเก็บต่างอาคาร และ Storge ที่ใช้สำรองข้อมูล ที่ติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน มีสำหรับข้อมูลบางระบบงาน (phase เริ่มต้น)

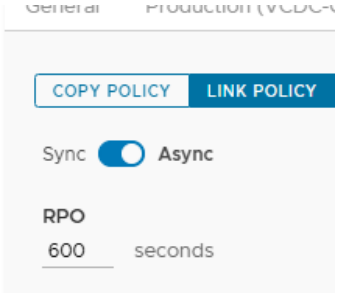
จากตาราง SLA เราจะพบว่า ค่า RPO (ระยะเวลาของข้อมูลสูญหายที่โรงพยาบาลศิริราชยอมรับได้ในช่วงเวลาหนึ่ง : Recovery Point Objective) ของระบบนั้น ๆ จะมีค่าเท่ากับความถี่ในการสำรองข้อมูล ตัวอย่างเช่น ถ้าเราสำรองข้อมูลทุกๆวันและมีการสำรองข้อมูลสำเร็จ นั่นหมายความว่า ค่า RPO จะมีค่ามากสุดคือ 24 ชั่วโมง ขึ้นกับเวลาที่เกิดเหตุระบบใช้งานไม่ได้ลบด้วยเวลาข้อมูลการสำรองข้อมูลครั้งล่าสุดที่สำเร็จ จะเป็นค่า RPO ที่ได้จากการกู้คืนข้อมูล ระยะเวลาการกู้คืนข้อมูลแปลผัน ตามขนาดข้อมูลที่ต้องการกู้คืน ความเร็วและความเสถียรของเครือข่าย ความสามารถและเทคนิคการกู้คืนที่ Backup Software สามารถดำเนินการได้สิ่งเหล่านี้จะต้องดำเนินการซักซ้อมเป็นประจำทุกปีเพื่อให้มั่นใจได้ว่าเมื่อเกิดเหตุระบบสามารถจะกู้คืนข้อมูลกลับมาได้ด้วยระยะเวลาเท่าไหร่

Job Id	Type	Elapsed ...	Kilobytes	KB/Sec
4001513	**Restore**	**02:49:10**		
40015	Restore	02:22:47	905,219,901	113,416
40021	Restore	00:00:18	108,000	92,703
40021	Restore	00:02:44	14,058,848	96,147
40022	Restore	00:00:23	539,744	110,286
40022	Restore	00:00:18	108,768	109,314
40022	Restore	00:00:19	128,224	107,932
40022	Restore	00:05:07	27,665,696	96,039
40022	Restore	00:00:33	1,515,168	113,623
40022	Restore	00:00:19	1,056	30,171
40022	Restore	00:00:17	18,528	61,554
40022	Restore	00:00:20	272,736	100,492
40022	Restore	00:00:17	4,768	103,652
40022	Restore	00:00:18	1,696	36,869
40022	Restore	00:00:17	34,464	77,972
40022	Restore	00:00:19	61,344	79,667
40022	Restore	00:00:17	8,416	125,611
40022	Restore	00:00:16	85,600	86,377
40022	Restore	00:00:18	70,240	104,213
40022	Restore	00:00:18	8,800	50,285
40022	Restore	00:00:18	17,248	68,717
40022	Restore	00:00:19	21,856	92,610

รูปที่ 2 แสดงตัวอย่างผลการกู้คืนข้อมูลผ่าน NetBackup software

ระยะเวลาการกู้คืนข้อมูลของระบบฐานข้อมูลที่มีขนาด 950 GB ผ่านการ สำรองข้อมูลแบบ Full Backup วันละหนึ่งครั้ง และมีการสำรองข้อมูล Transaction Log ทุก 1 ชั่วโมง ใช้ระยะเวลาในการดำเนินการ 2 ชั่วโมง 50 นาที นั่นแสดงให้เห็นว่า หากฐานข้อมูลชุดนี้เกิดความเสียหายไม่ว่ากรณีใด และต้องดำเนินการกู้คืนข้อมูล ระบบสารสนเทศที่มีการใช้ฐานข้อมูลชุดนี้จะการหยุดชะงักการให้บริการ อย่างน้อยที่สุด 2 ชั่วโมง 50 นาที ถ้ากระบบเสียหายเฉพาะตัวฐานข้อมูล

3) การจัดทำศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน ณ งานสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก เนื่องจากเป็นหน่วยงานภายใต้สังกัดเดียวกัน และเป็นหน่วยงานที่ได้รับมาตรฐาน มาตรฐานสากล ISO/IEC27001:2013 โดยการดำเนินการเริ่มต้นจากการประเมินและคัดเลือก Application จากการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อตอบสนองความสำคัญด้านบริการขององค์กร และความปลอดภัยของผู้ป่วย รวมถึงให้ผู้มีส่วนได้ส่วนเสียเป็นผู้กำหนดช่วงเวลาการหยุดชะงักของระบบสารสนเทศที่ยอมรับได้สูงสุด (MTPD) ซึ่งมีค่าเท่ากับ 1 ชม. และ ระยะข้อมูลการสูญหายของข้อมูลที่ยอมรับได้ (RPO) คือ 15 นาที ของแต่ระระบบงานที่กำหนดใน BIA และนำเสนอผู้บริหารเพื่อมีมติยอมรับค่าตัวเลขดังกล่าว หลังจากนั้นดำเนินการจัดหาระบบ ติดตั้งระบบ ดำเนินการผสานรวมข้อมูลและเชื่อมโยงข้อมูลระหว่างศูนย์ข้อมูลหลักและศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดเหตุภัยฉุกเฉิน และทดสอบระบบเพื่อให้แน่ใจว่าระบบสามารถให้บริการได้ตามข้อกำหนด



รูปที่ 3 การตั้งค่า RPO ของเครื่องแม่ข่ายผ่าน Recovery Point Software

4) การทดสอบศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน ปีละ 1 ครั้ง ซึ่งมี 2 จุดประสงค์ ได้แก่ จุดประสงค์แรกเป็นการตรวจสอบระยะเวลาที่ใช้ทดสอบการกู้คืนระบบสารสนเทศ ณ ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน โดยการกำหนดเวลาสำหรับการทดสอบการกู้คืนระบบสารสนเทศ 3 ชุด คือ ระยะเวลาสูงสุดที่ใช้ใน

การกู้คืนข้อมูล (Recovery Time Objective: RTO) โดยเป็นการกู้ข้อมูลชุดสุดท้ายที่ดำเนินการสำรองเอาไว้ขึ้นมาใช้งาน ระยะเวลาในการตั้งค่าระบบต่าง ๆ (Work Recovery Time: WRT) รวมถึงการตรวจสอบข้อมูลที่กู้คืนว่าถูกต้องหรือไม่ ก่อนที่จะเริ่มเปิดใช้งานระบบอีกครั้ง และระยะเวลารวมทั้งหมดในการกู้คืนระบบก่อนจะเริ่มใช้งานจริง (Maximum Tolerable Downtime: MTD) จุดประสงค์ที่สอง คือ ร้อยละของจำนวนระบบที่ผ่านการทดสอบการกู้คืนระบบสารสนเทศ ณ ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน โดยกำหนดจำนวนระบบที่ดำเนินการทดสอบเทียบกับระบบที่ผ่านการทดสอบ

5) การซ้อมแผนความต่อเนื่องทางธุรกิจในส่วนของระบบการให้บริการผู้ป่วย ปีละ 1 ครั้ง โดยการซ้อมแผนดังกล่าวเป็นการซักซ้อมขั้นตอนต่าง ๆ ตั้งแต่การพบเหตุการณ์ระบบสารสนเทศหยุดชะงัก การติดต่อประสานงานระหว่างผู้เกี่ยวข้องเพื่อตรวจสอบและประเมินสถานการณ์ การแจ้งผู้บริหารเพื่อสั่งการและเรียกใช้แผนความต่อเนื่องทางธุรกิจของโรงพยาบาลศิริราช รวมถึงการดำเนินการของบุคลากรฝ่ายสารสนเทศที่เกี่ยวข้องเพื่อเปิดใช้งานระบบสารสนเทศสำหรับการให้บริการผู้ป่วยที่ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน ณ ศูนย์การแพทย์กาญจนาภิเษก

ทั้งนี้ จะเห็นได้ว่ากระบวนทั้ง 5 ข้อที่ฝ่ายสารสนเทศจัดทำขึ้นเพื่อให้มั่นใจว่าหากเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉินขึ้นกับระบบสารสนเทศสำหรับการให้บริการผู้ป่วย ณ ศูนย์ข้อมูลหลัก ฝ่ายสารสนเทศจะสามารถเปิดใช้งานระบบดังกล่าวให้ใช้งานได้ตามปกติ ตามข้อตกลงที่ให้ไว้กับผู้ใช้งานของโรงพยาบาลศิริราช นอกจากกระบวนการทั้ง 5 ข้อนี้ ยังมีรายละเอียดอื่น ๆ ที่ต้องดำเนินการเพื่อให้ความต่อเนื่องในการให้บริการผู้ป่วยของโรงพยาบาลศิริราชมีประสิทธิภาพสูงสุด อาทิ การทบทวนและปรับปรุงรายชื่อบุคลากรที่เกี่ยวข้องทั้งหมดรวมถึงหมายเลขโทรศัพท์ที่สามารถติดต่อได้ การกำหนดการสื่อสารตามช่องทางต่าง ๆ การแจ้งเหตุฉุกเฉินให้ผู้เกี่ยวข้องตามรายชื่อ (Call Tree) ที่ปรากฏในข้อมูลการบริหารความต่อเนื่องทางธุรกิจทราบทั้งก่อนและหลังจากการสั่งการและเรียกใช้แผนความต่อเนื่องทางธุรกิจของโรงพยาบาลศิริราช ตลอดจนการสรุปผลการทดสอบศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน และการซ้อมแผนความต่อเนื่องทางธุรกิจในส่วนของระบบการให้บริการผู้ป่วย เพื่อนำสิ่งที่พบจากการทดสอบและการซ้อมแผนดังกล่าวมาทบทวนและพิจารณาปรับปรุง แก้ไข หรือเพิ่มเติมให้กระบวนการครบถ้วนและสมบูรณ์มากขึ้นหากเกิดเหตุการณ์ขึ้นจริง หรือในการซ้อมครั้งต่อไป

7. บทสรุป

การให้บริการผู้ป่วยในยุคดิจิทัลนั้นระบบสารสนเทศและเทคโนโลยีสารสนเทศมีส่วนช่วยในการอำนวยความสะดวก รวดเร็วในการให้บริการผู้ป่วย ดังนั้น เพื่อให้การให้บริการได้อย่างต่อเนื่ององค์กรควรพิจารณากระบวนการปฏิบัติงานของบุคลากรที่เกี่ยวข้องและระบบเทคโนโลยีสารสนเทศให้มีความต่อเนื่อง ไม่หยุดชะงัก เพื่อควบคุมความเสียหายในมิติต่าง ๆ ที่อาจส่งผลกระทบกับองค์กร ซึ่งการสำรองข้อมูลและการมีศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉินเป็นอีกหนึ่งปัจจัยที่สามารถทำให้การดำเนินธุรกิจเป็นไปอย่างต่อเนื่องเมื่อเกิดสภาวะวิกฤติหรือสภาวะฉุกเฉิน การออกแบบศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉินให้เหมาะสมกับรูปแบบและกิจกรรมทางธุรกิจขององค์กรเป็นสิ่งที่องค์กรพึงกระทำ ทั้งนี้ องค์กรต้อง ประเมินระยะเวลาการยอมรับได้ของการหยุดชะงักระบบสารสนเทศและความคุ้มทุนในการลงทุนของศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดสภาวะวิกฤตหรือสภาวะฉุกเฉินให้เหมาะสมกับการให้บริการและบริบทขององค์กร

8. ข้อเสนอแนะ

8.1) องค์กรต้องให้ความสำคัญในการพิจารณาและทบทวนการวิเคราะห์ผลกระทบของปัจจัยเสี่ยงและเหตุการณ์ที่ไม่พึงประสงค์ต่อธุรกิจ (Business Impact Analysis: BIA) ขององค์กรเอง ทั้งนี้ เพื่อให้องค์กรสามารถเลือกดำเนินการได้ตรงตามเป้าหมายขององค์กรที่กำหนดไว้ (ระบบอะไร การให้บริการใดที่สามารถรอได้ และไม่สามารถรอได้)

8.2) การกำหนดตัวเลข 3 ชุด ได้แก่ ระยะเวลาของข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (Recovery Point Objective: RPO) ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉินขึ้น (Recovery Time Objective: RTO) และระยะเวลารวมทั้งหมดในการกู้คืนระบบก่อนจะเริ่มใช้งานจริง (Maximum Tolerable Downtime: MTD) ซึ่งจะเป็นสิ่งสำคัญที่นำไปกำหนดการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับความต่อเนื่องทางธุรกิจขององค์กร

8.3) งบประมาณและการลงทุนสำหรับความต่อเนื่องทางธุรกิจขององค์กร ตั้งแต่การจัดทำแผนการสำรองข้อมูล, เทคโนโลยีที่ใช้ในการสำรองข้อมูล และการกำหนดรูปแบบตลอดจนสถานที่สำหรับศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน

8.4) ข้อควรพิจารณาเพิ่มเติมสำหรับการทดสอบศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน

- ระบบสารสนเทศที่มีการเปลี่ยนแปลงระหว่างปี อาทิ การเพิ่มเส้นทางการเชื่อมต่อของระบบระหว่างปี และไม่ได้แจ้งให้ผู้เกี่ยวข้องทราบ ส่งผลให้สภาพแวดล้อมการทำงานของระบบสารสนเทศเปลี่ยนแปลงไปจากเดิมที่เคยตั้งค่าหรือกำหนดค่าไว้
- อัตราการเจริญเติบโตของพื้นที่จัดเก็บข้อมูลอันเนื่องจากมีการปรับปรุงความสามารถของระบบเพิ่มขึ้น หรือมีปริมาณการใช้งานเพิ่มขึ้น ควรพิจารณาจัดสรรพื้นที่ให้เพียงพอ
- การเชื่อมต่อเครือข่ายคอมพิวเตอร์ระหว่างศูนย์ข้อมูลหลักและศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉิน หากเกิดเหตุฉุกเฉินหรือสภาวะวิกฤตขึ้นบริเวณจุดเชื่อมต่อเครือข่ายคอมพิวเตอร์ภายในศูนย์ข้อมูลหลักส่งผลให้ไม่สามารถเชื่อมต่อหรือเปิดใช้งานศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินได้
- แหล่งจ่ายไฟที่ให้บริการเครื่องลูกข่าย (Client) หากไม่มีระบบไฟฟ้าสำรอง ถึงแม้จะสามารถเปิดใช้งานระบบสารสนเทศ ณ ศูนย์คอมพิวเตอร์สำรองสำหรับกรณีเกิดภัยฉุกเฉินได้ แต่จุดให้บริการผู้ป่วยจะไม่สามารถใช้งานได้และไม่สามารถให้บริการผู้ป่วยได้เช่นกัน

เอกสารอ้างอิง

[1] ปริญญา หอมอเนก. “*Standard จับกระแสมาตรฐานการบริหารจัดการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤติ*,” [ออนไลน์]. https://www.acisonline.net/?p=1780 (เข้าถึงเมื่อ: 2 กันยายน 2567).

[2] กิตติพงศ์ จิรวัสวงศ์. “*BS 25999 มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ*,” [ออนไลน์]. https://www.gotoknow.org/posts/283403 (เข้าถึงเมื่อ: 3 กันยายน 2567).

[3] บริษัทดิจิตอล ดิสทริบิวชั่น จำกัด. “*เทคนิคและเทคโนโลยีการสำรองข้อมูล (Backup)*,” [ออนไลน์]. https://www.digitaldistribution.co.th/th/news-articles/ประเภท-เทคนิค-backup (เข้าถึงเมื่อ: 3 กันยายน 2567).

[4] บริษัท Veritas (Thailand) จำกัด. “*วิธีการ Backup ในรูปแบบต่าง ๆ*,” [ออนไลน์]. https://www.veritasthailand.com/วิธีในการ-backup-ในรูปแบบต่าง (เข้าถึงเมื่อ: 6 กันยายน 2567).

[5] นิพนธ์ นาชิน. “*3-2-1 Backup Rule: กฎทองปกป้องข้อมูลธุรกิจจากภัยไซเบอร์*,” [ออนไลน์]. https://www.alphasec.co.th/post/3-2-1-backup-rule-กฎทองปกป้องข้อมูลธุรกิจจากภัยไซเบอร์ (เข้าถึงเมื่อ: 20 กันยายน 2567).