แผนรับมือ Business Continuity Plan (BCP)

กลุ่มงานพยาธิวิทยากายวิภาค โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินงานได้ เมื่อวันที่ 9 ธันวาคม 2566

ผู้รับผิดชอบ: หัวหน้ากลุ่มงาน, หัวหน้างาน

1. บทนำ

จากการโดน ransomware attack ในวันที่ 9 ธันวาคม 2566 กลุ่มงานพยาธิวิทยากายวิภาค ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้

ปัญหา

- จากเหตุการณ์ ransomware attack มีผลให้ไม่สามารถทำงานในระบบคอมพิวเตอร์ได้ ตั้งแต่การบันทึกข้อมูล ค้นผลการตรวจทางพยาธิวิทยา และการออกผลการตรวจได้ เมื่อผู้ป่วยมาพบแพทย์ตามนัด ก็ไม่สามารถดูผลการตรวจในระบบของโรงพยาบาลได้
- เมื่อผู้ป่วยมาตามผลการตรวจ กลุ่มงานพยาธิวิทยากายวิภาค ไม่สามารถค้นข้อมูลจากระบบคอมพิวเตอร์ได้ จะต้องค้นจากทะเบียนรายชื่อผู้ป่วยที่พิมพ์เก็บไว้รายวัน ซึ่งมีเพียงชุดเดียว เมื่อผู้ป่วยมาตามผลจำนวนมาก จะไม่สามารถค้นหาได้ทัน ประกอบกับข้อมูลจากผู้ป่วยที่แจ้งวันที่ผ่าตัด ไม่แน่นอนชัดเจน ทำให้การค้นหาไม่พบ เสียเวลาและผู้ป่วยท่านอื่นๆต้องรอนานมากเนื่องจากข้อมูลการตรวจทางพยาธิวิทยาทั้งหมดที่เก็บไว้ในระบบของโรงพยาบาลได้หายไป
- การติดต่อกับหน่วยงานอื่นๆนอกโรงพยาบาลในการรับผลการตรวจหรือส่งสิ่งส่งตรวจ ไม่สามารถทำได้ เนื่องจากไม่มีสัญญาณอินเทอร์เนท ทำให้การรับผลการตรวจพิเศษต่างๆไม่สามารถทำได้ รวมทั้งการสั่งตรวจพิเศษทาง Molecular ก็ทำไม่ได้

วิเคราะห์สาเหตุของปัญหา: เนื่องจากข้อมูลทั้งหมดของการตรวจทางพยาธิวิทยาอยู่ในระบบของโรงพยาบาลเมื่อระบบมีปัญหาจึงทำให้ข้อมูลที่บันทึกไว้หายไปทั้งหมด

- ระบุแนวทางการแก้ไขปัญหา:
    1. จัดระบบการ Back up ข้อมูล แยกออกมาจากระบบของโรงพยาบาล ทั้งไฟล์สแกนและระบบการลงผลทางคอมพิวเตอร์ ซึ่งต้องลงข้อมูลแยกในเครื่องคอมพิวเตอร์ แบบ Stand alone
    2. จัดระบบการเก็บเอกสารการส่งตรวจ ใบส่งตรวจและใบรายงานผลให้ค้นหาง่าย และป้องกันการสูญหาย
    3. สแกนใบขอตรวจ Request form ทุกรายและจัดเก็บเรียงตามหมายเลขทางพยาธิวิทยาเป็นรายวัน ทุกวัน
    4. ในกรณีของการค้นชื่อผู้ป่วยเพื่อค้นหาผลการตรวจที่หายไปทั้งหมด จากการค้นหาจากทะเบียนที่พิมพ์เก็บไว้ ซึ่งมีเพียงชุดเดียวและการค้นหาด้วยมืออาจผิดพลาด หาไม่พบ จัดให้นำทะเบียนที่เก็บไว้มาพิมพ์ข้อมูลลงในโปรแกรมในคอมพิวเตอร์ เพื่อใช้ Search หาชื่อโดยคอมพิวเตอร์ ซึ่งใช้เวลาไม่นานและค้นหาง่าย
    5. การติดต่อกับหน่วยงานภายนอก จะต้องใช้สัญญาณอินเทอร์เนท ซึ่งควรเป็นเครื่องที่ไม่อยู่ในระบบ Land ของโรงพยาบาล เพื่อป้องกันการติดไวรัสและป้องกันข้อมูลสำคัญจากการโจมตีทางไซเบอร์ ซึ่งจะต้องหาเครื่องคอมพิวเตอร์ Stand alone และสัญญาณอินเทอร์เนทแยกออกมาจากระบบโรงพยาบาล

อุปสรรค

- ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack: ขาดเครื่องมือและอุปกรณ์ในการบันทึกข้อมูลทั้งในส่วนของการดำเนินงานไปข้างหน้า การบันทึกข้อมูลใหม่และ การค้นผลการตรวจเก่าที่หายไปและการบันทึกข้อมูลเก่าทดแทนที่หายไปทั้งหมด ซึ่งต้องใช้ทั้งคนทำงาน และเครื่องมือที่ใช้ คอมพิวเตอร์ เครื่องพิมพ์ สแกนเนอร์ อินเทอร์เนท ไม่เพียงพอ

- วิเคราะห์สาเหตุของอุปสรรค: คนทำงานไม่พอ เพราะต้องทำงานหน้างานที่เป็นงานปกติ และต้องทำงานย้อนหลังเพื่อเก็บข้อมูลที่หายไปทั้งหมดกลับคืนเข้าระบบ ต้องใช้บุคลากรจำนวนมากตั้งแต่การบันทึกข้อมูลเข้าระบบจนถึงการอ่านสไลด์โดยพยาธิแพทย์เพื่อให้ได้ผลการตรวจมาลงระบบใหม่

ระบุแนวทางการแก้ไขอุปสรรค: จัดหาเครื่องมือในการบันทึกข้อมูลให้พอเพียง และจัดเวลาการทำงานเพิ่มนอกเวลาเพื่อให้สามารถทำงานทั้งงานปัจจุบัน และการเก็บข้อมูลเก่าที่หายไปได้

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ระบุผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก: การค้นผลการตรวจไม่สามารถค้นได้จากระบบคอมพิวเตอร์ ต้องค้นจากทะเบียนที่พิมพ์เก็บไว้รายวัน ซึ่งการค้นหาจะประสบผลสำเร็จหรือไม่อยู่ที่ข้อมูลที่คนไข้ให้ซึ่งมักไม่ตรงกับความจริงจึงทำให้ต้องค้นหาสุ่มเพิ่มจำนวนข้อมูลมากขึ้นและเสียเวลานาน
- การบันทึกข้อมูลเก่าลงระบบใหม่ ในช่วงHN ของผู้ป่วยที่ข้อมูลเสียหายต้องสร้าง HN ใหม่ไม่สามารถลงข้อมูลได้หากยังเป็น HN เก่า การจะสร้างHN ใหม่ ต้องใช้ข้อมูลส่วนตัวของผู้ป่วย และต้องอยู่ในสถานะ Register ซึ่งไม่สามรถทำได้หากผู้ป่วยไม่มาโรงพยาบาล
- ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร: ผู้ป่วยได้ผลการตรวจช้า หรือไม่ได้ หากข้อมูลที่ให้ไม่ชัดเจน ถูกต้อง เช่น บอกวันเวลาการส่งตรวจผิดไป ข้ามเดือน ข้ามปี จะไม่สามารถหาเจอทำให้แพทย์ผู้รักษาไม่ได้ข้อมูลที่ควรทราบ

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack: การ Back up ข้อมูลไว้นอกระบบ Land ของโรงพยาบาล และบันทึกข้อมูลแยกออกจากระบบที่ลงข้อมูลปกติ รวมทั้งการสแกนเอกสารสำคัญในการตรวจแยกออกจากระบบ Land เพื่อให้สามารถค้นหาและบันทึกได้โดยอิสระในกรณีที่เกิดวิกฤติ ข้อมูลหาย ยังมีแหล่งสำรอง
- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น: ทำงานแบบ Stand alone เก็บข้อมูลควบคู่ไปกับระบบ Land ของโรงพยาบาล
- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร: จัดระบบการเก็บไฟล์สแกนเอกสารต่างๆให้ค้นหาง่าย และระบบจัดเก็บเอกสารให้เป็นระเบียบเพื่อให้สามารถค้นหาได้รวดเร็ว

2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack: เมื่อระบบข้อมูลโรงพยาบาลล่ม
    1. แจ้งเหตุกับผู้บังคับบัญชาตามลำดับชั้น
    2. กรณีที่ไม่สามารถเข้าดูข้อมูลในระบบได้เลย ให้ทำงานด้วยระบบ Manual
    3. ในส่วนของการรับสิ่งส่งตรวจเข้า หลังจากตรวจสอบความถูกต้องครบถ้วนแล้ว ให้ลงทะเบียนรับเข้าในคอมพิวเตอร์ Stand alone ซึ่งไม่ได้ต่อเชื่อมกับระบบฐานข้อมูลโรงพยาบาล โดยใช้โปรแกรม Microsoft Access เก็บข้อมูลเบื้องต้นที่สำคัญ เช่น ชื่อ สกุล HN วันที่รับเข้า และหมายเลขทางพยาธิวิทยา ทั้งนี้เพื่อเก็บบันทึกข้อมูลไว้เพื่อใช้เป็นฐานข้อมูลสำรองในการค้นหาข้อมูลทางพยาธิวิทยาของผู้ป่วยเมื่อเกิดเหตุการณ์โดนโจมตีซ้ำ จะสามารถหาข้อมูลของผู้ป่วยได้ และใช้ในการค้นหาชั่วคราว โดยไม่ต้องค้นมือจากทะเบียนกระดาษ
    4. ในส่วนของการค้นผลการตรวจให้ปฏิบัติดังนี้
        1. คีย์ชื่อ สกุล ผู้ป่วยค้นหาในโปรแกรมแยกซึ่งบันทึกข้อมูลเหมือนทะเบียนรับเข้ารายวันที่เป็นเอกสาร
        2. เมื่อค้นหาพบแล้ว จดหมายเลขทางพยาธิวิทยา นำมาค้นหาใบ Request ที่จัดเก็บไว้ในตู้เอกสาร ซึ่งจะแนบใบรายงานผลการตรวจไว้ นำผลการตรวจที่แนบไว้ออกมาถ่ายเอกสารและสแกนเข้าระบบ DocScanของโรงพยาบาลเพื่อส่งผลให้แพทย์ดูใน OPservหากระบบคอมพิวเตอร์ยังใช้ไม่ได้ ให้ผู้ป่วยถือผลไปห้องตรวจ
        3. ในกรณีที่ผลเก่ามาก หลายปี ไม่มีผลแนบ ให้ค้นสไลด์ออกมาให้พยาธิแพทย์อ่านออกผลใหม่
        4. กรณีที่หาใบ Request ไม่พบ ให้ค้นหาจากไฟล์สแกนที่สแกนเก็บไว้และพิมพ์ออกมาแนบสไลด์ให้พยาธิแพทย์อ่านออกผลใหม่

5. ในส่วนของการบันทึกข้อมูลใหม่ (New case) หากคอมพิวเตอร์ในระบบยังใช้ไม่ได้ ให้บันทึกข้อมูลแยกในโปรแกรมพิมพ์ทะเบียน เพื่อเก็บข้อมูลผู้ป่วย HN และเลขที่ทางพยาธิวิทยา เก็บไว้ ในส่วนของพยาธิแพทย์เมื่ออ่านสไลด์แล้วการออกรายงานผลให้พิมพ์ผลลงในTemplate แบบฟอร์มรายงานผลการตรวจและพิมพ์รายงานออกมา สแกนลงระบบเพื่อให้แพทย์ดูผ่าน OPserv หากระบบLand ยังใช้ไม่ได้ ให้พิมพ์ผลออกมา 2 ชุด ชุดแรกแนบเก็บไว้คู่กับใบ Request และชุดสองให้ผู้ป่วยถือไปพบแพทย์

- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน: งานธุรการ, หัวหน้างาน, พยาธิแพทย์, หัวหน้ากลุ่มงาน

ผู้รับผิดชอบสาหรับแต่ละขั้นตอน ลำดับ ผู้เกี่ยวข้อง	**หน้าที่**
ผู้ปฏิบัติงาน ณ ขณะเกิดเหตุการณ์	แจ้งเหตุ หรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบ หรือสงสัยว่ามีภัยคุกคามเกิดขึ้น
หัวหน้ากลุ่มงาน, หัวหน้างาน	รับแจ้งเหตุ หรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์ และรายงานแจ้งเหตุไปยังหัวหน้ากลุ่มงานสารสนเทศทางการแพทย์และรองผู้อำนวยการด้านเทคโนโลยีสารสนเทศและการสื่อสารโรงพยาบาลอุดรธานีเพื่อเร่งดำเนินการแก้ไขให้ทัน ให้คำแนะนำ ให้คำปรึกษากับเจ้าหน้าที่ผู้ปฏิบัติงาน ในด้านการทำงาน การแก้ปัญหาเฉพาะหน้า การเฝ้าระวังป้องกันไม่ให้เกิดภัยคุกคามซ้ำ
ผู้รับแจ้งเหตุ	รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
คณะกรรมการสารสนเทศ -หน่วยงาน IT ของโรงพยาบาล -หน่วยงานภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ	เฝ้าระวัง และวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
ผู้บริหารของโรงพยาบาล	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยทางไซเบอร์

หมายเหตุ คณะกรรมการสารสนเทศ ควรเป็นบุคลากรที่มีความรู้ ความสามารถ ประสบการณ์ ผ่านการอบรมด้าน Cyber security และผ่านการรับรอง Certification และมีความเชี่ยวชาญเฉพาะด้าน เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์

- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน:
  - การค้นหาผล-การออกผลใหม่ 1-2 ชั่วโมง
  - การค้นสไลด์ พยาธิแพทย์อ่านออกผลใหม่ 2-3 ชั่วโมง
  - การตัดบล็อกชิ้นเนื้อใหม่ ทำสไลด์ใหม่ ให้พยาธิแพทย์อ่านออกผลใหม่ 3-5 วัน

2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP: คอมพิวเตอร์, External hard disc, เครื่องสแกนเอกสาร, โปรแกรมที่ช่วยจัดระเบียบเอกสาร
- ระบุแหล่งที่มาของทรัพยากร: ศูนย์คอมพิวเตอร์

2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP: ทดลองการทำงานโดยไม่ใช้ระบบ Land ตามวิธีการปฏิบัติที่กำหนดไว้ ดูผลการทำงาน สามารถทำได้ภายในเวลาที่กำหนด
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้: จัดทำคู่มือปฏิบัติงานภายใต้สถานการณ์ถูกจู่โจมทางไซเบอร์ และสื่อสารให้ผู้ปฏิบัติรับทราบถึงแนวทางการปฏิบัติงานและผลกระทบที่จะเกิดขึ้นกับผู้ป่วยและเจ้าหน้าที่หากเกิดเหตุการณ์ขึ้น

รายชื่อผู้ติดต่อ

1. นายแพทย์ นิพันธ์ ทองบ่อ รองผู้อานวยการด้านเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลอุดรธานี

2. นายธนพล ธนอำพนสกุล หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์ โรงพยาบาลอุดรธานี

3. พญ.พัชรีย์ สุวรรณสนธิ์ หัวหน้ากลุ่มงานพยาธิวิทยากายวิภาค โรงพยาบาลอุดรธานี

4. นางสาวชุตินธร จังสถิตย์กุล นักวิทยาศาสตร์การแพทย์ชานาญการพิเศษ หัวหน้างานพยาธิวิทยา กลุ่มงานพยาธิวิทยากายวิภาค โรงพยาบาลอุดรธานี

5. นายวัชระ ชื่นชมน้อย เจ้าพนักงานวิทยาศาสตร์การแพทย์ชานาญงาน หัวหน้างานเซลล์วิทยา กลุ่มงานพยาธิวิทยากายวิภาค โรงพยาบาลอุดรธานี

แบบฟอร์มที่จำเป็น

ไม่มี

4. การอนุมัติ

หัวหน้ากลุ่มงานพยาธิวิทยากายวิภาค: พญ.พัชรีย์ สุวรรณสนธิ์

วันที่: 8 มีนาคม 2567 ทบทวนแผน 13 กันยายน 2567

5. บทสรุป

แผน BCP นี้เป็นแนวทางสำหรับปฏิบัติงานเมื่อเกิดกรณีถูกโจมตีทางไซเบอร์ เพื่อให้สามารถทำงานให้บริการตรวจวินิจฉัยทางพยาธิวิทยาและออกรายงานผลการตรวจได้ตามปกติ ทำให้ผู้ป่วยได้รับการวินิจฉัยและรับการรักษาได้ทันท่วงทีและจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่นๆ ได้อย่างมีประสิทธิภาพ

หมายเหตุ: แผน BCP ที่ใช้ มีการทบทวนปรับปรุงทุก 3 เดือน

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
Back up ข้อมูลไว้ในคอมพิวเตอร์ Stand alone แยกออกจาก ระบบ Land ของโรงพยาบาลและจัดระบบการเก็บเอกสาร ใบนำส่งสิ่งส่งตรวจให้เป็นระบบ ค้นหาง่าย	/		
ให้ผู้เชียวชาญทางด้าน IT วางระบบป้องกันที่แน่นหนา รัดกุม			/
จัดระบบการทำงานบันทึกข้อมูลกับคอมพิวเตอร์ แยกออกมาจากระบบของโรงพยาบาลไว้ใช้เป็นระบบสำรองหากเจอเหตุการณ์ อีก			/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
ซ้อมแผนปฏิบัติการณ์เพื่อรับมือเหตุการณ์เป็นประจำ เพื่อสร้างความชำนาญในการแก้ปัญหาในสถานการณ์จริง	/		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
ดำเนินการตามแนวทางการปฏิบัติเมื่อเกิดสถานการณ์ไม่ปกติ	/		
การปฏิบัติหลังระบบกลับสู่ปรกติ			
บันทึกข้อมูลที่เสียหายไปกลับเข้าสู่ระบบของโรงพยาบาล	/		

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT