แผนรับมือ Business Continuity Plan (BCP)
โรงพยาบาลอุดรธานี

เหตุการณ์ : โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้
วันที่ : 9 ธันวาคม 2566
แผนก : วิสัญญี กลุ่มงานวิสัญญี)วิทยา , งานการพยาบาลวิสัญญี
ผู้รับผิดชอบ : กลุ่มงานวิสัญญีวิทยา , งานการพยาบาลวิสัญญี

1. บทนำ

จากการโดน ransomware attack ในวันที่ 9 ธันวาคม 2566 แผนก วิสัญญี ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้

ปัญหา

บทเรียนปัญหาจากเหตุการณ์ ransomware attack : ผู้ป่วยได้รับความล่าช้าในการให้บริการ เช่นการรับส่งผู้ป่วย การ set ผ่าตัด การสื่อสาร เพิ่มภาระงานบุคลากร (มีจำนวนจำกัด)

วิเคราะห์สาเหตุของปัญหา : อิสระต่อการเข้าถึงข้อมูล การไม่เข้าใจการใช้ (การใช้การเข้าถึงข้อมูลง่ายและมีบุคลากรที่หลากหลาย) งานระบบ It ผิดประเภท ผิด การนำเข้าออกข้อมูลผ่านตัวเก็บข้อมูล site web การลงโปรแกรมการป้องกันไวรัส การเข้าถึงการตรวจสอบเครื่องไม่ครบทุกเครื่องในขณะที่มีการใช้เครื่องกระจายตามจุดต่างๆ(การควบคุมกำกับติดตาม)

ระบุแนวทางการแก้ไขปัญหา แยกวงกลุ่มผู้ใช้งาน ตามความเหมาะสมกับหน้างานนั้นๆ การเข้าถึงให้ยากขึ้น การให้ความรู้ด้านการใช้งาน ให้ความรู้ด้านผลกระทบวงกว้างหากเกิดการเข้าจู่โจมอีก จัดระบบการรับส่งผู้ป่วย รูปแบบฉุกเฉิน กับไม่ฉุกเฉิน จัดช่องทางการสื่อสารระหว่างวิสัญญีกับหน่วยงานที่เกี่ยวข้องที่เกี่ยวกับการใช้ระบบคอมพิวเตอร์ แจ้งพบเห็นความผิดปกติในการใช้งานให้รีบแจ้งเบาะแสต่อผู้ที่มีความรับผิดชอบโดยตรง พร้อมเบอร์เพื่อติดต่อด้วยความรวดเร็ว

อุปสรรค

อุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack : เป็นการรับทราบหลังการถูกโจมตีไปในวงกว้างแล้ว

วิเคราะห์สาเหตุของอุปสรรค : ไม่ทราบผู้ดูแลที่ชัดเจนว่าต้องแจ้งใครและเข้าถึงใครได้เป็นคนแรกความไม่รู้เพราะไม่เคยเกิดและไม่ทราบผลกระทบหากเกิด

แนวทางการแก้ไขอุปสรรค :

- ให้ความรู้ ให้ความเป็นผู้สังเกต
- แจ้งระบุผู้มีหน้าที่รับผิดชอบโดยตรงให้ผู้ปฏิบัติงานที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์รับทราบ พร้อมเบอร์ติดต่อได้หากเกิดข้อสงสัย ด้วยไวรัสบางชนิดจะระบาดเร็วมากฟอร์มนี้จัดทำขึ้นเพื่อให้แต่ละแผนกในโรงพยาบาลอุดรธานีสามารถจัดทำแผนรับมือ Business Continuity Plan (BCP) กรณีเกิดเหตุการณ์ ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้แผน BCP นี้จะช่วยให้แต่ละแผนกสามารถดำเนินงานต่อเนื่องได้อย่างมีประสิทธิภาพแม้จะเผชิญกับเหตุการณ์วิกฤต

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

ผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก ; การทำงานล่าช้า เพิ่มบุคลากรทำงาน การลงข้อมูลเวชระเบียนผลกระทบต่อผู้ป่วยญาติและบุคลากร ; ความล่าช้า จากการขาดข้อมูลในการสืบค้น ต่อการรักษา ต่อการ Identification ผู้ป่วย เสี่ยงต่อความผิดพลาดคลาดเคลื่อน เพิ่มภาระงานการทำงานของบุคลากรที่มีจำนวนจำกัด โรงพยาบาลสูญเสียรายได้

2.2 กลยุทธ์

กลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack ; การให้ความรู้กับบุคลากรในองค์กรทุกคน การแจ้งข้อมูลข่าวสารการสื่อสาร ความตระหนักรู้ถึงภัยร้ายแรงต่อการเข้าถึงของไวรัส การให้ทุกคนมีความรู้วิธีการป้องกันภัยการมาเยือนของไวรัส เมื่อใช้คอมพิวเตอร์เบื้องต้น สอนการเข้าดูโปรแกรมการป้องกันไวรัส

วิธีการที่จะรักษางานบริการที่จำเป็น ; การ กับ emergency รูปแบบ ผ่าตัด case set elective case การลงข้อมูลเวชระเบียน การคิดค่าบริการ

วิธีการที่จะลดผลกระทบต่อผู้ป่วยญาติและบุคลากร ; ด้านผู้ป่วยและญาติ ชี้แจง อธิบายต่อเหตุการณ์ที่เกิดขึ้น พร้อมขอความร่วมมือ ด้านบุคลากร เพิ่มอัตรากำลังช่วยเสริมในด้านการช่วยลงลงข้อมูล ลดการเดินทางส่งเอกสารโดยเพิ่มช่องทางการส่งต่อข้อมูล เช่น การนำกระสวยอวกาศมาเป็นทางเลือก

2.3 แผนปฏิบัติการ

ขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack

ขั้นตอนในการรับมือกับ ransomware attack 7 ขั้นตอน ผู้รับผิดชอบ และ ระยะเวลา สำหรับแต่ละขั้นตอน

การรับมือ	ผู้รับผิดชอบ	ระยะเวลา
1 ใช้โปรแกรมป้องกันไวรัส	ผู้ที่ได้รับมอบหมายทางศูนย์คอมฯโรงพยาบาลอุดรธานี	1-2 ต่อปี
2 รับ ให้ ความรู้การใช้โปรแกรมป้องกันไวรัสที่เหมาะสมกับตัวเอง	บุคลากรทุกคนในโรงพยาบาล ผู้ที่ได้รับมอบหมายทางศูนย์คอมฯ	ทุก1ปี
3 ใช้โปรแกรมให้เป็น	บุคลากรทุกคนในโรงพยาบาล	ต่อเนื่อง
4 อัพเดทฐานข้อมูลไวรัส (definition) อยู่เสมอ	ผู้ที่ได้รับมอบหมายทางศูนย์คอมฯ	ทุกปี
5 เปลี่ยนversionใหม่ทันทีที่มีการรับแจ้ง หรือตามรอบเวลา	ผู้ที่ได้รับมอบหมายทางศูนย์คอมฯ	ตามรอบระยะเวลา
6 อย่ารับ fileแปลกหน้า และติดตามข้อข่าวเสมอ	บุคลากรทุกคนในโรงพยาบาล	ต่อเนื่อง
7 หากเครื่องติดไวรัสแล้ว อย่ากลัว รีบแจ้งผู้รับผิดชอบของศูนย์คอม โรงพยาบาลทันที	บุคลากรทุกคนในโรงพยาบาล ผู้ที่ได้รับมอบหมายทางศูนย์คอมฯ	ต่อเนื่อง

2.4 ทรัพยากร

ทรัพยากรที่จำเป็นในการดำเนินการแผน BCP ; บุคลากรที่รับผิดชอบในการดำเนินงาน และบุคลากรของโรงพยาบาลทุกคน

แหล่งที่มาของทรัพยากร ; นโยบาย คน เงิน ของ

2.5 การทดสอบและฝึกอบรม

วิธีการทดสอบแผน BCP ; จัดทำโครงการฝึกอบรมเรียนรู้การใช้คอมพิวเตอร์เบื้องต้นด้าน การป้องกัน การใช้โปรแกรมไวรัส-ผลกระทบต่อการสูญเสีย

วิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้; ภาคทฤษฎีและปฏิบัติ

3. เอกสารแนบ

แผนงาน ; ตามแผนยุทธศาสตร์ของโรงพยาบาลอุดรธานี

4. การอนุมัติ

หัวหน้าแผนก : พญ ปิยะฉัตร วรรณาสุนทรไชย

วันที่ : ล้อตามแผนนโยบายของโรงพยาบาลอุดรธานี

5. บทสรุป

ฟอร์มนี้เป็นแนวทางสำหรับแต่ละแผนกในการจัดทำแผน BCP แผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่นๆได้อย่างมีประสิทธิภาพ

หมายเหตุ:

ฟอร์มนี้สามารถปรับแต่งให้เหมาะกับแต่ละแผนกได้

แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

แหล่งข้อมูล

คำแนะนำ

ควรจัดทำแผน BCP ร่วมกับผู้เชี่ยวชาญด้านไอที

ควรทดสอบแผน BCP เป็นประจำ

ควรฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U)/(	S)/(	I)/(
การป้องกัน	/		/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ	/	/	
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้	/	/	/
การปฏิบัติหลังระบบกลับสู่ปกติ	/		/

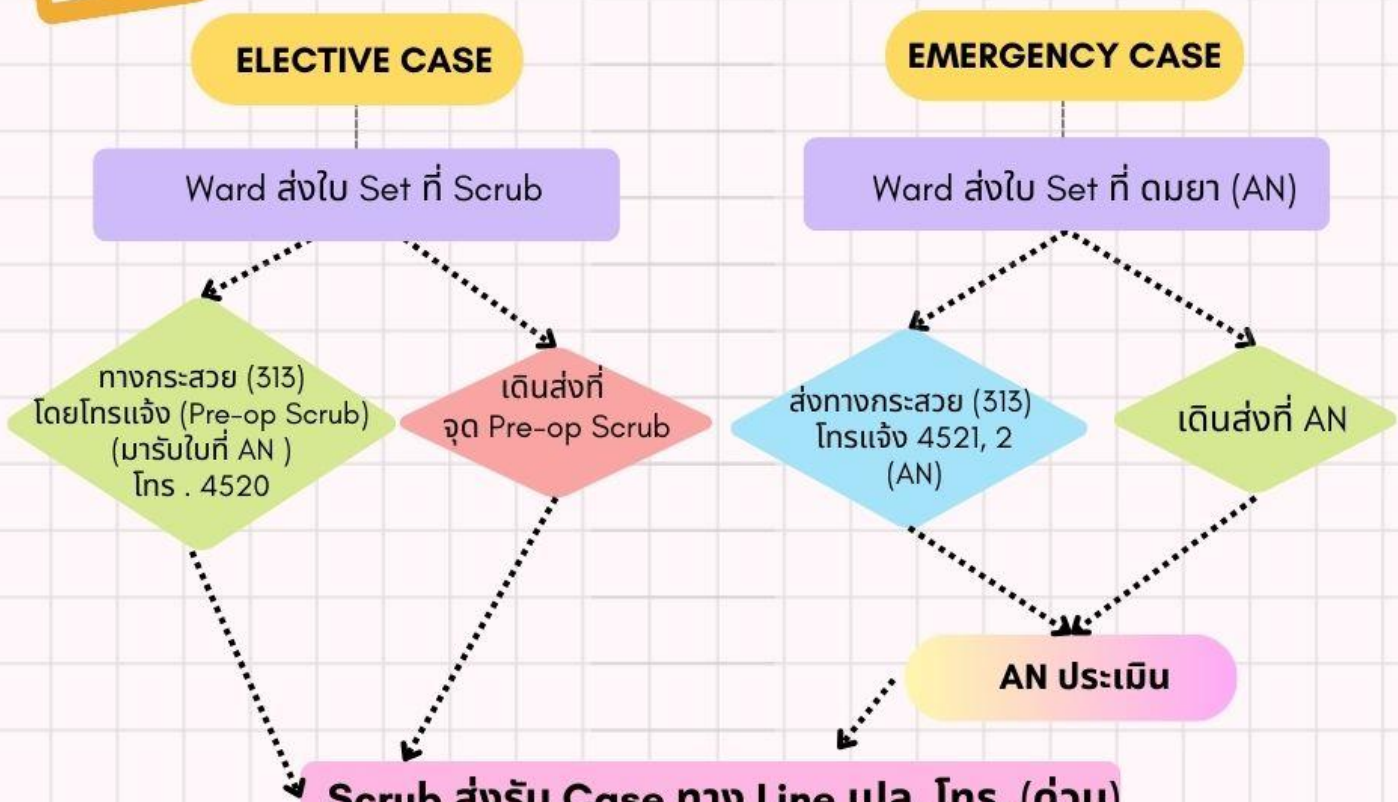
U =ดำเนินการได้เองระดับหน่วยงาน

S= ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT

การ SET CASE ห้องผ่าตัด

กรณี ระบบ IT ขัดข้อง



พ.ปิยะฉัตร วรรณสุนทรไชย/หน.กลุ่มงานวิสัญญีวิทยา
10 ธันวาคม 2566

แนวทางการประเมินผู้ป่วยก่อนผ่าตัด

กรณี ระบบ IT ขัดข้อง

1. จากใบ SET CASE
2. จากการซักประวัติผู้ป่วยและญาติ
3. ดูผล LAB ที่ WARD ส่งมา (ครบถ้วน)
4. ดู X-RAY จากเครื่องคอมพิวเตอร์ตำแหน่ง SCRUB

พ.ปิยะฉัตร วรรณสุนทรไชย/หน.กลุ่มงานวิสัญญีวิทยา
10 ธันวาคม 2566

แนวทางการคิดค่าบริการทางวิสัญญี

กรณี ระบบ IT ขัดข้อง

- คิดเงินตามใบสีฟ้าพร้อมสรุปยอดเงิน (MANUAL) และถ่ายเอกสารเก็บไว้ 1 ชุด
- ส่งใบสีฟ้ากลับไปที่ WARD เพื่อให้การเงิน WARD คิดค่าบริการทางวิสัญญี
- ใบถ่ายเอกสารเก็บไว้ เพื่อลงข้อมูลในระบบภายหลัง ระบบใช้งานได้ปกติ

พ.ปิยะฉัตร วรรณสุนทรไชย/หน.กลุ่มงานวิสัญญีวิทยา
10 ธันวาคม 2566