

แผนรับมือ Business Continuity Plan (BCP)
กลุ่มงานสังคมสงเคราะห์ โรงพยาบาลอุดรธานี

เหตุการณ์ โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้
วันที่ 27 กันยายน 2567
แผนก กลุ่มงานสังคมสงเคราะห์
ผู้รับผิดชอบ นางไขศรี สิรินบุญทวี

1. บทนำ

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

1.1 ปัญหา

1. ปัญหาจากเหตุการณ์ ransomware attack ส่งผลให้ข้อมูลสำคัญของผู้ที่มารับบริการ โดยอาศัยข้อมูลในระบบฐานข้อมูลของโรงพยาบาล มีผลกระทบโดยตรงผู้รับบริการและเจ้าหน้าที่ผู้ปฏิบัติงานสังคมสงเคราะห์ ทำให้ไม่สามารถบันทึกประวัติของกลุ่ม OSCC ได้ แพทย์เฉพาะทางไม่สามารถดูประวัติเดิมของผู้ป่วยได้

2. การสืบค้นประวัติผู้ป่วยเก่า ประวัติการนัด เป็นไปได้ยากเนื่องจากฐานข้อมูลเชื่อมต่อกับ HIS ทำให้การประสานงาน ประสานติดตามญาติ เป็นไปอย่างล่าช้า

3. ระบบส่งปรึกษาออนไลน์ ไม่สามารถใช้งานได้ ทำให้การให้บริการล่าช้าลง

4. การเข้าถึงเครือข่ายอินเทอร์เน็ตที่โดนปิดกั้น ส่งผลกระทบต่อการประสานงาน

วิเคราะห์สาเหตุของปัญหา

1. เมื่อโดน Ransomware attack ทำให้ระบบ HIS ของทางโรงพยาบาลล่ม จึงไม่สามารถใช้โปรแกรมต่าง ๆ ได้ ไม่มีโปรแกรมสำรองในกรณีที่ระบบ HIS และ LIS ล่ม

2. ควรจะมีโปรแกรมที่สามารถทำงานได้ตามปกติ เช่น โปรแกรมค้นประวัติผู้รับบริการสังคมสงเคราะห์ จากฐานข้อมูลของกระทรวงสาธารณสุข (สค.1)

3. ไม่มีระบบสัญญาณอินเทอร์เน็ตที่แยกจาก ระบบ LAN

ระบุแนวทางการแก้ไขปัญหา

1. รายงานให้ผู้บังคับบัญชาทราบ เพื่อดำเนินการแจ้งคณะกรรมการบริหารโรงพยาบาลอุดรธานี

2. สำรองข้อมูลที่สำคัญ ติดตั้งโปรแกรม antivirus

3. หมั่นตรวจสอบหรือมีความผิดปกติตรงไหนบ้าง

อุปสรรค

ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack การสื่อสารภายในโรงพยาบาล เหตุที่เกิดขึ้นจริง เพื่อให้เจ้าหน้าที่ได้รับทราบข่าวสารที่ถูกต้อง ให้ทุกคนได้ตื่นตระหนก และเตรียมพร้อมรับมือกับสถานการณ์ที่เกิดขึ้น

สาเหตุของอุปสรรค

การสั่งการในสถานการณ์ช่วงแรก เจ้าหน้าที่ที่มีความสับสน เพราะการไม่ได้รับข้อมูลที่ชัดเจนว่าเกิดอะไรขึ้นกับโรงพยาบาล จึงทำให้ทุกคนเรียกร้องอยากได้เครื่องอำนวยความสะดวกในการทำงาน อีกทั้งผู้มารับบริการที่โรงพยาบาลอุดรธานีในแต่ละวันมีจำนวนมาก การรับมือในการให้บริการผู้ป่วยในช่วงแรก จึงทำให้ขาดแคลนทั้งอุปกรณ์คอมพิวเตอร์ และ การสื่อสาร การสั่งการที่เป็นจุดรวมเพียงหนึ่ง ทำให้ทุกหน่วยงานเข้าใจสถานการณ์ ที่เกิดขึ้นและร่วมกันทำงานให้สถานการณ์ดีขึ้น

ระบุแนวทางการแก้ไขอุปสรรค

การสั่งการในสถานการณ์ฉุกเฉิน

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

ระบุผลกระทบของ ransomware attack ที่มีต่องานบริการของกลุ่มงานสังคมสงเคราะห์

1. ภาระงานของผู้ปฏิบัติงานเพิ่มขึ้น เช่น การให้บริการกลุ่มผู้ป่วย OSCC ต้องเก็บเอกสารแยกจากประวัติผู้ป่วยทั่วไป และต้องลงทะเบียนแบบ manual เพื่อป้องกันเอกสารสูญหาย
2. ผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้เต็มประสิทธิภาพ เช่น ไม่สามารถค้นประวัติ หรือนัดเดิมของผู้ป่วยได้ ทำให้เกิดการทำงานที่ซ้ำซ้อน
3. การปฏิบัติงานล่าช้า และเพิ่มภาระงานให้กับเจ้าหน้าที่

ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร

1. ผู้ป่วยได้รับบริการล่าช้า เนื่องจากต้องใช้วิธีปฏิบัติงานแบบ manual
2. โรงพยาบาลได้มีการกำหนดใช้เลขที่โรงพยาบาลใหม่ (HN ใหม่) ทำให้การค้นประวัติเดิมของผู้ป่วยเป็นไปได้ยาก ถึงแม้จะมีฐานข้อมูลเดิมของคนไข้อยู่แล้วก็ตามไม่สามารถดึงเลขที่โรงพยาบาลเดิมมาใช้ได้ จึงทำให้เกิดความล่าช้าในการปฏิบัติงาน
3. เนื่องจากมีภาระงานเพิ่มมากขึ้น ทำให้บุคลากรเกิดความเหนื่อยล้าในการปฏิบัติงาน

2.2 กลยุทธ์

ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack

1. จัดให้มีการ back up ข้อมูล และมีการมอบหมายให้คณะกรรมการสารสนเทศทางการแพทย์ มีการตรวจสอบการ back up ข้อมูลร่วมกับกลุ่มงานสารสนเทศทางการแพทย์ของโรงพยาบาลอย่างสม่ำเสมอ
2. ลักษณะแบ่งกลุ่มการใช้งานสารสนเทศตามนโยบายกลุ่มที่ 2 ที่จำเป็นต้องใช้ทั้ง LAN และ website ที่ได้รับอนุญาต ต้องมีการกำหนดสิทธิการเข้าใช้งานและเข้าถึงข้อมูล โดยควรมีจุดให้สามารถใช้งานได้เฉพาะเครื่องที่กำหนดไว้ให้เท่านั้น
3. ให้ความรู้กับผู้ปฏิบัติงานให้สามารถปฏิบัติงานได้เมื่อเกิดปัญหา และต้องปฏิบัติตาม Flow หรือตามแนวทางที่กำหนดร่วมกันอย่างเคร่งครัด

ระบุวิธีการที่จะรักษางานบริการที่จำเป็น

1. อัปเดตโปรแกรมต่าง ๆ ที่ใช้ในระบบของโรงพยาบาลให้ทันสมัย และปลอดภัยต่อการโดน ransomware รวมทั้งมีโปรแกรมสำรอง เพื่อกรณีฉุกเฉินต่าง ๆ ที่อาจจะเกิดขึ้นในอนาคต

ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร

1. ผู้ปฏิบัติทุกหน่วยงานควรอธิบายผู้ป่วย และญาติผู้ป่วยให้เข้าใจถึงสถานการณ์ ransomware attack ที่เกิดขึ้น
2. มีช่องทางสื่อสารที่มีประสิทธิภาพเพื่อให้ผู้ปฏิบัติงานทุกหน่วยงาน ทั้งแพทย์ พยาบาล หอผู้ป่วยทราบถึงสถานการณ์ และปัญหาที่กำลังเกิดขึ้น ทำให้เข้าใจปัญหาร่วมกัน เพื่อลดแรงปะทะในการติดตามผล

2.3 แผนปฏิบัติการ

ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack

ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน

ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน

ตารางที่ 1. ผู้ปฏิบัติงานกลุ่มงานสังคมสงเคราะห์และบทบาทหน้าที่

ลำดับ	ชื่อ	บทบาทหน้าที่
1.	หัวหน้ากลุ่มงาน นางไขศรี สิริบุณยทวี 0862185811	- ประเมินสถานการณ์ที่เกิดขึ้นว่ามีผลกระทบและความรุนแรงในระดับใด - ประสานหน่วยงานที่เกี่ยวข้องในด้านผลกระทบที่เกิดขึ้นกับกลุ่มงานสังคมสงเคราะห์ - การสื่อสารกับผู้ปฏิบัติในกลุ่มงานสังคมสงเคราะห์
2.	ผู้ปฏิบัติงานกลุ่มงานสังคมสงเคราะห์ นายไอสุรีย์ ปุยละเทิม 092-4741333 นางสาวนิภาธร โพธิ์เงิน 093-3418158 นางสาวโสธญา หงษ์ทอง 064-0621825 นางสาวณัฐพร แคนเสาร์ 080-2395665 นางสาวเพ็ญพรรณ ไชยสวาง 085-7786369 นายพงศกร สารีรูป 061-0057003 นางสาววรารพร พานะกำจาย 093-5587869	- การสื่อสารภายในองค์กร กรณีมีความจำเป็นต้องติดต่อบุคลากรหรือหน่วยงานภายในต่าง ๆ ให้ดูข้อมูลสำหรับการติดต่อได้ในตารางข้อมูลสำหรับการติดต่อหน่วยงานภายใน - การสื่อสารภายนอกองค์กร หน่วยงานภายนอกที่ทีมกู้คืนบริการจำเป็นต้องติดต่อสื่อสารด้วยได้แก่ ผู้มารับบริการในโรงพยาบาล, ทีมสหวิชาชีพที่เกี่ยวข้อง - หมั่นตรวจสอบระบบคอมพิวเตอร์หากมีความผิดปกติให้รายงานหัวหน้ากลุ่มงาน

2.4 ทรัพยากร

ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP ผู้บริหารทุกท่าน สร้างความตระหนักแก่เจ้าหน้าที่คอมพิวเตอร์ เจ้าหน้าที่โรงพยาบาลอุดรธานีทุกท่าน ให้ความสำคัญกับการโดนภัยคุกคาม Ransomware เพื่อป้องกันการเกิดซ้ำ

3. สรุปประเด็นที่ควรดำเนินการ
 ตารางที่ 2 สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน 1. มอบหมายให้คณะกรรมการสารสนเทศ ตรวจสอบการ Back up ข้อมูลของโรงพยาบาลอย่างสม่ำเสมอ 2. การใช้งานสารสนเทศที่จำเป็นต้องใช้ LAN และเว็บไซต์ต้องกำหนดหรือจำกัดสิทธิการใช้งานและเข้าถึงข้อมูล	✓		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ 1. ให้ความรู้กับผู้ปฏิบัติงานได้เมื่อเกิดปัญหา สามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างเคร่งครัด	✓		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้ 1. กำหนดช่องทางการสื่อสารเพื่อให้ผู้รับบริการรับทราบโดยทั่วกัน และสร้างความรู้ความเข้าใจถึงสถานการณ์ที่จะเกิดขึ้น	✓		

หมายเหตุ : U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคอยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT