

ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี

กลุ่มงานศัลยกรรมออร์โธปิดิกส์

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 28 สิงหาคม 2567

แผนก: กลุ่มงาน ศัลยกรรมออร์โธปิดิกส์

ผู้รับผิดชอบ: หัวหน้ากลุ่มงานศัลยกรรม, หัวหน้ากลุ่มงานการพยาบาลผู้ป่วยออร์โธปิดิกส์, IT nurse ประจำกลุ่มงานและหอผู้ป่วย

1. บทนำ

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

ปัญหา

ปัญหาที่ 1 ผู้ปฏิบัติไม่รู้ถึงผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้น

วิเคราะห์ปัญหา

- ขาดการสื่อสารจากผู้บริหารหรือศูนย์คอมพิวเตอร์ไม่ได้แจ้งข้อมูลเกี่ยวกับผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้นอย่างครบถ้วน ชัดเจน หรือทันเวลาที่
- โรงพยาบาลไม่มีแผนและเตรียมการซ้อมแผนนี้

แนวทางการแก้ปัญหา

- จัดทำแนวปฏิบัติอุบัติภัยทางไซเบอร์
- พัฒนาการสื่อสาร
 - แจ้งข้อมูลเกี่ยวกับผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้นอย่างครบถ้วน ชัดเจน ทันเวลาที่ และเข้าใจง่าย
 - ใช้ช่องทางการสื่อสารที่หลากหลายและเข้าถึงผู้ปฏิบัติได้ครบถ้วน
 - จัดกิจกรรมทบทวนความรู้เกี่ยวกับการใช้คอมพิวเตอร์และโปรแกรมต่างๆ รวมถึงถาม-ตอบ

ข้อสงสัยของผู้ปฏิบัติหน้างาน

- ซ้อมแผนอุบัติภัยทางไซเบอร์

ปัญหาที่ 2 ศูนย์คอมพิวเตอร์ไม่แจ้งปัญหาที่แท้จริงเมื่อได้รับแจ้งปัญหาในการใช้งานระบบ

วิเคราะห์ปัญหา

- ปัญหาทางเทคนิค
 - ศูนย์คอมพิวเตอร์อาจไม่มีเครื่องมือหรือความเชี่ยวชาญเพียงพอในการวินิจฉัยปัญหาที่แท้จริง
 - ระบบการตรวจสอบอาจมีข้อบกพร่อง ทำให้ไม่สามารถระบุสาเหตุของปัญหาได้
- ปัญหาการสื่อสาร
 - ศูนย์คอมพิวเตอร์ไม่ได้แจ้งข้อมูลเกี่ยวกับปัญหาที่เกิดขึ้นให้ผู้ใช้ทราบอย่างครบถ้วน
- ปัญหาด้านนโยบาย
 - ศูนย์คอมพิวเตอร์อาจมีนโยบายไม่แจ้งรายละเอียดเกี่ยวกับปัญหาที่แท้จริงแก่ผู้ใช้
 - ศูนย์คอมพิวเตอร์อาจกังวลว่าการแจ้งปัญหาที่แท้จริงอาจสร้างความตื่นตระหนกให้กับผู้ใช้
- ศูนย์คอมพิวเตอร์อาจขาดแคลนบุคลากรที่มีสมรรถนะ

แนวทางการแก้ปัญหา

1. เพิ่มจำนวนและพัฒนาสมรรถนะบุคลากรด้าน IT อย่างต่อเนื่อง
2. ควรมีระบบการแจ้งภาวะฉุกเฉินที่เกิดขึ้น ให้ผู้ปฏิบัติงานได้รับทราบอย่างรวดเร็วและบอกแนวทางการปฏิบัติอย่างชัดเจน เช่น งดการใช้งานคอมพิวเตอร์ ถอดสาย Lan เป็นต้น
3. จัดทำแผนงานและขั้นตอนเพื่อรองรับหรือเรียกอัตราค่าจ้างเสริมเพื่อการดำเนินให้กลับสภาวะปกติ พร้อมมีแผนสำรองระหว่างรอเรียกอัตราค่าจ้างตามแผนหลัก

ปัญหาที่ 3 เครื่องคอมพิวเตอร์ไม่เพียงพอ บางหน่วยงานต้องใช้ระบบ Internet ในการปฏิบัติงาน

วิเคราะห์ปัญหา

1. งบประมาณจำกัด: หน่วยงานอาจไม่มีงบประมาณเพียงพอที่จะจัดซื้อเครื่องคอมพิวเตอร์ใหม่หรืออัปเกรดเครื่องเก่า
2. การขาดการวางแผน: หน่วยงานอาจไม่ได้วางแผนการจัดซื้อคอมพิวเตอร์ล่วงหน้า
3. ประสิทธิภาพการทำงานลดลงเครื่องคอมพิวเตอร์ที่เก่าอาจมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์

แนวทางการแก้ปัญหา

1. ศูนย์คอมพิวเตอร์จัดทำแผนการจัดซื้อคอมพิวเตอร์ล่วงหน้า โดยพิจารณาถึงจำนวนผู้ใช้งาน งบประมาณ และประเภทของงาน
2. จัดสรรงบประมาณ: หน่วยงานควรจัดสรรงบประมาณให้เพียงพอสำหรับการจัดซื้อคอมพิวเตอร์ใหม่หรืออัปเกรดเครื่องเก่า
3. มีแผนการบำรุงรักษาและอัปเดตโปรแกรมเครื่องเก่าอย่างต่อเนื่อง

ปัญหาที่ 4 ไม่มีการสำรองข้อมูลเมื่อเกิดปัญหากรณีคอมพิวเตอร์ทำงานไม่ได้

วิเคราะห์ปัญหา

1. ไม่มีแผนสำรองเอกสารแบบ manual ไว้

แนวทางการแก้ไข้ปัญหา

1. มีการสำรองเอกสารแบบฟอร์มที่ต้องใช้ในการปฏิบัติงานของแต่ละหน่วยงาน
2. หน่วยงานมีการสำรองข้อมูลในระบบ on cloud/Stand alone หรือจัดทำสมุดเวชระเบียนผู้ป่วย

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ไม่สามารถดูประวัติการรักษาผู้ป่วยย้อนหลังได้
- การสืบค้นข้อมูลผู้ป่วยมียุ่งยาก ซับซ้อน หลายขั้นตอน
- ผู้ปฏิบัติยังไม่เคยพบสถานการณ์ทำให้การปรับตัวเข้ากับสถานการณ์ดังกล่าวเกิดความล่าช้า
- ระบบ logistics เกิดความล่าช้า ต้องใช้บุคลากรในการเชื่อมต่อในการทำงานระหว่างหน่วยงาน

2.2 กลยุทธ์

กลยุทธ์รับมือกับ Ransomware Attack

1. การป้องกัน

- สำรองข้อมูล: สำรองข้อมูลสำคัญอย่างสม่ำเสมอ โดยใช้ระบบสำรองข้อมูลแบบออฟไลน์ (Offline Backup)
- อัปเดตซอฟต์แวร์: อัปเดตซอฟต์แวร์และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัส: ติดตั้งโปรแกรมป้องกันไวรัสและไฟร์วอลล์ที่มีประสิทธิภาพ
- ฝึกอบรมพนักงาน: ฝึกอบรมพนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกัน

Ransomware Attack

- ใช้การยืนยันตัวตนแบบหลายชั้น: ใช้การยืนยันตัวตนแบบหลายชั้น (MFA) เพื่อเพิ่มความปลอดภัย

2. การตรวจจับ

- ใช้เครื่องมือตรวจจับ: ใช้เครื่องมือตรวจจับ Ransomware เฉพาะทางอย่างสม่ำเสมอ

3. การตอบสนอง

- แยกระบบที่ติดเชื้อ: แยกระบบที่ติดเชื้อออกจากเครือข่าย

4. การฟื้นฟู

- อัปเดตระบบ: อัปเดตระบบปฏิบัติการ ซอฟต์แวร์และโปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ
- เปลี่ยนรหัสผ่าน: เปลี่ยนรหัสผ่านทุกเดือนหรือทุกครั้งที่ไม่มีความปลอดภัย
- ฝึกอบรมพนักงาน: ฝึกอบรมพนักงานเกี่ยวกับวิธีการป้องกัน Ransomware Attack

วิธีการรักษางานบริการและลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร

1. มีการสำรองเอกสารแบบฟอร์มที่ต้องใช้ในการปฏิบัติงานของแต่ละหน่วยงาน
2. หน่วยงานมีการสำรองข้อมูลในระบบ on cloud หรือจัดทำสมุดเวชระเบียนผู้ป่วย

2.3 แผนปฏิบัติการ

เป้าหมาย	วัตถุประสงค์	กิจกรรม/ขั้นตอน	ผู้รับผิดชอบ	ระยะเวลา
เพื่อให้ระบบสามารถดำเนินได้เมื่อเกิดปัญหา Ransomware attack	1. เพื่อให้เจ้าหน้าที่สามารถ ปฏิบัติงานได้อย่างต่อเนื่อง เมื่อเกิด Ransomwareattack 2. เพื่อให้ผู้ป่วยได้รับการรักษา ที่ปลอดภัย และต่อเนื่อง	ระบุและแยกตัวเครื่องที่ติดเชื้อ	ทีม IT	ภายใน 1 ชั่วโมง
		สำรองข้อมูล	ผู้ใช้, ทีม IT	ภายใน 1 ชั่วโมง
		แจ้งหน่วยงานไอทีภายในองค์กร	ผู้ใช้	ภายใน 1 ชั่วโมง
		วิเคราะห์สายพันธุ์ของ ransomware	ทีม IT	ภายใน 1 ชั่วโมง
		กู้คืนระบบจากสำเนาสำรอง	ทีม IT	ภายใน 24 ชั่วโมง
		แจ้งหน่วยงานด้านความปลอดภัยทางไซเบอร์	ผู้บริหาร	ภายใน 24 ชั่วโมง
		หาวิธีแก้ไขเพิ่มเติม	ทีม IT	ภายใน 24 ชั่วโมง
		กู้คืนข้อมูล	ทีม IT	ภายใน 1 สัปดาห์
		ป้องกันการโจมตีในอนาคต	ทีม IT,ผู้ใช้	ภายใน 1 สัปดาห์
		แจ้งหน่วยงานบังคับใช้กฎหมาย	ผู้บริหาร	ภายใน 1 สัปดาห์

3. เอกสารแนบ

-

4. การอนุมัติ

หัวหน้าแผนก: _____

(นายสมภู นรนนันท์)

นายแพทย์เชี่ยวชาญ

หัวหน้ากลุ่มงานศัลยกรรมออร์โธปิดิกส์

วันที่ 28 สิงหาคม 2567

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน 1. แจ้งศูนย์คอมพิวเตอร์ให้รับทราบว่ามีปัญหาเกิดขึ้นที่หน่วยงาน 2. ไม่ใช้คอมพิวเตอร์ระบบ Lan ร่วมกับ Internet 3. ใช้เอกสารแบบ manual มาใช้ในการปฏิบัติงานแทนโปรแกรมที่ใช้ไม่ได้	/		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุหน่วยงาน มีการจัดเตรียมเอกสาร แบบ manual ให้พร้อมใช้กรณีที่เกิดภาวะฉุกเฉินทาง cyber	/		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินงานต่อไปได้ IT ควรมีหน่วยกลางเก็บเอกสารฟอร์ม manual ของทุกกลุ่มงานเป็นต้นฉบับ แยกไฟล์ไว้ ต่างหากกับโปรแกรมที่ปริ้นท์ จากคอมพิวเตอร์			/
การปฏิบัติหลังระบบกลับสู่ปกติ 1. ทบทวนการใช้งานคอมพิวเตอร์ในการปฏิบัติงานอย่างสม่ำเสมอ 2. หัวหน้างาน / หัวหน้าหอ ควบคุมกำกับ นิเทศติดตาม การใช้งานคอมพิวเตอร์ของ ผู้ปฏิบัติงาน 3. มีการสื่อสารนโยบายลงสู่ผู้ปฏิบัติ 100%	/	/	/

U = ดำเนินการได้เองระดับหน่วยงาน, S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน, I = ต้องได้รับการสนับสนุนจาก IT

แผนปฏิบัติการรับมือเหตุภัยคุกคามทางไฟเบอร์
กลุ่มงานศัลยกรรมออร์โธปิดิกส์ โรงพยาบาลอุดรธานี

