แผนเผชิญเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)

โรงพยาบาลทุ่งฝน จังหวัดอุดรธานี

1. วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติสำหรับเจ้าหน้าที่ศูนย์คอมพิวเตอร์และหน่วยงานที่เกี่ยวข้อง เมื่อตรวจพบการบุกรุกระบบเครือข่าย หรือถูกโจมตีทางไซเบอร์จนระบบหลัก (HOSxP) ไม่สามารถใช้งานได้ เพื่อลดความเสียหายและกู้คืนระบบให้กลับมาบริการได้โดยเร็วที่สุด

2. ขั้นตอนปฏิบัติเมื่อตรวจพบเหตุการณ์ (Action Steps)

ขั้นที่ 1 การจำกัดวงความเสียหาย (Containment) - [ทำทันที]

- ตัดการเชื่อมต่อ: ให้เจ้าหน้าที่ IT ทำการถอดสาย LAN หรือปิดการเชื่อมต่อเครือข่าย (Isolate) ของเครื่อง Server ที่ต้องสงสัยทันที
- หยุดการกระจาย: หากเป็น Ransomware ให้ปิดเครื่องคอมพิวเตอร์ (Shutdown) ในกลุ่มเสี่ยง เพื่อไม่ให้ไวรัสแพร่กระจายผ่านระบบ Network
- แจ้งสถานะ: แจ้งผู้บริหารและหัวหน้าแผนกผ่านช่องทางด่วน (Line Group/วิทยุสื่อสาร) เพื่อประกาศใช้ แผนสำรองกรณีระบบล่ม (Downtime Plan)

ขั้นที่ 2 การแก้ไขสถานการณ์หน้างาน (Downtime Procedure)

- เปลี่ยนสู่ระบบ Manual: ให้หน่วยงานบริการ (OPD, IPD, ER, ห้องยา) เปลี่ยนไปใช้เวชระเบียนกระดาษและแบบฟอร์มบันทึกการรักษาฉุกเฉิน
- คัดกรองสิทธิ: ใช้ระบบตรวจสอบสิทธิล่วงหน้า (Offline) หรือบันทึกข้อมูลเพื่อตรวจสอบย้อนหลัง

ขั้นที่ 3 การวิเคราะห์และกู้คืนระบบ (Analysis & Recovery)

- ตรวจสอบช่องโหว่: ค้นหาจุดที่ถูกเจาะ (Entry Point) และทำการปิดพอร์ตหรือล้างมัลแวร์ออกจากระบบ
- กู้คืนข้อมูล (Restore): ดำเนินการกู้คืนฐานข้อมูลจาก Backup ล่าสุด ที่ตรวจสอบแล้วว่าปลอดภัย (Clean Backup)
- ทดสอบระบบ: ตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ก่อนเปิดให้ใช้งานตามปกติ

3. ตารางลำดับการปฏิบัติงาน (Responsibility Matrix)

ระยะเวลา	ขั้นตอนปฏิบัติ	ผู้รับผิดชอบ
0 - 15 นาที	ตรวจพบเหตุ/ตัดการเชื่อมต่อเครือข่าย	เจ้าหน้าที่ IT (นวก.คอมพิวเตอร์)
15 - 30 นาที	ประกาศใช้ระบบ Downtime (กระดาษ)	ผู้บริหาร / หัวหน้าพยาบาล
1 - 4 ชั่วโมง	วิเคราะห์สาเหตุและเริ่มกู้คืนข้อมูล	เจ้าหน้าที่ IT / Vendor
ภายใน 72 ชม.	รายงานเหตุละเมิดข้อมูล (PDPA) ต่อ สคส.	คณะกรรมการบริหารข้อมูลฯ

4. การรายงานเหตุการณ์ (Reporting)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พ.ร.บ. ไซเบอร์ฯ โรงพยาบาลจะต้องบันทึกรายละเอียดดังนี้

1. วันและเวลา ที่พบเหตุการณ์
2. ลักษณะการถูกโจมตี (เช่น ถูกแฮกหน้าเว็บ, ข้อมูลถูกเข้ารหัส)
3. ขอบเขตความเสียหาย (เช่น ข้อมูลผู้ป่วยถูกเข้าถึงจำนวนกี่ราย)
4. แนวทางการแก้ไข และการป้องกันในอนาคต

บันทึกรายงานสถานการณ์จำลอง: เหตุการณ์ระบบ HOSxP ขัดข้องจากการถูกโจมตีทางไซเบอร์

1. ลำดับเหตุการณ์ (Timeline Simulation)

- 08:30 น.: งานห้องบัตรและ OPD แจ้งว่าระบบ HOSxP ค้าง ไม่สามารถบันทึกข้อมูลได้
- 08:45 น.: ฝ่ายไอทีตรวจสอบ Server พบไฟล์ฐานข้อมูลมีนามสกุลผิดปกติ (ถูกเข้ารหัส) และมีไฟล์ข้อความเรียกค่าไถ่ (Ransomware Note) ปรากฏขึ้น
- 08:50 น.: [ขั้นตอนแจ้งข่าว] ไอทีแจ้งผู้อำนวยการและประสานงานประชาสัมพันธ์ เพื่อประกาศสถานการณ์ "ระบบเครือข่ายขัดข้องชั่วคราว" ให้ผู้รับบริการทราบและขออภัยในความไม่สะดวก
- 09:00 น.: ประกาศใช้ระบบ Downtime (Manual Paper) ทั่วทั้งโรงพยาบาล

2. การวิเคราะห์เหตุการณ์ (Incident Analysis)

จากการตรวจสอบย้อนหลัง (Forensics) พบปัจจัยที่ทำให้เกิดเหตุดังนี้:

- จุดเริ่มต้น (Entry Point): พบการบุกรุกผ่านเครื่องคอมพิวเตอร์ในหน่วยงานหนึ่ง เนื่องจากมีการใช้รหัสผ่านที่คาดเดาง่าย (Weak Password) และไม่มีการจำกัดสิทธิ์ Admin ในเครื่องลูกข่าย
- ช่องโหว่ (Vulnerability): ระบบปฏิบัติการ Windows ในบางจุดยังไม่ได้อัปเดต Patch ความปลอดภัยล่าสุด ทำให้มัลแวร์แพร่กระจายผ่านช่องทาง SMB ภายในเครือข่าย
- ความเสียหาย (Impact): ฐานข้อมูลหลักไม่สามารถเข้าถึงได้ ส่งผลกระทบต่อประวัติการรักษา การสั่งยา และการเบิกจ่ายสิทธิการรักษาของผู้ป่วยทั้งหมดที่มารับบริการในวันนั้น

3. การกู้คืนและแก้ไข (Recovery Action)

- การตัดการเชื่อมต่อ: ไอทีสั่งปิด Switch และ Isolation เซิร์ฟเวอร์หลักออกจากระบบเครือข่ายโรงพยาบาลทันทีเพื่อหยุดการแพร่กระจาย
- การกู้คืนข้อมูล: ดำเนินการล้างเซิร์ฟเวอร์ (Clean Install) และกู้คืนฐานข้อมูลจาก Backup ภายนอก (Offline Backup) ของเมื่อวานเวลา 24:00 น.
- การตรวจสอบ: ตรวจสอบความถูกต้องของข้อมูล (Data Integrity Check) ก่อนเปิดระบบให้ใช้งานได้อีกครั้งในเวลา 14:00 น.

4. สรุปผลและข้อเสนอแนะ (Conclusion & Lessons Learned)

สรุปผล: ระบบล่มเป็นเวลา 5 ชั่วโมง 30 นาที ข้อมูลสูญหายบางส่วน (เฉพาะข้อมูลที่บันทึกในช่วงเช้าก่อนกู้คืน)

ข้อเสนอแนะเชิงนโยบาย (เพื่อเขียนรายงานเสนอผู้บริหาร):

1. มาตรการรหัสผ่าน: บังคับเปลี่ยนรหัสผ่าน User ทุกคนให้มีความซับซ้อน และห้ามใช้รหัสซ้ำกัน
2. ระบบสำรองข้อมูล: พัฒนาระบบ Backup แบบ 3-2-1 (มีสำรอง 3 ชุด, เก็บในสื่อ 2 ชนิด, และ 1 ชุดต้องอยู่นอกเครือข่าย/Offline)
3. ความตระหนักรู้งานไอที (Cyber Awareness): จัดอบรมเจ้าหน้าที่หน้างานเรื่องการสังเกต Link หรือไฟล์แนบที่ผิดปกติในอีเมลและสื่อโซเชียล
4. ระบบเฝ้าระวัง: พิจารณาจัดหาเครื่องมือตรวจจับพฤติกรรมผิดปกติในระบบเครือข่าย (Endpoint Detection and Response)

ผังการฝึกซ้อมและทบทวนแผนรับมือภัยคุกคามทางไซเบอร์(Incident Response Plan – IRP)

ข้อที่ 1 การกำหนดสถานการณ์จำลอง (Scenario Setting)

เป็นการระบุภัยคุกคามที่จะนำมาซ้อม โดยต้องเลือกเหตุการณ์ที่มีความเสี่ยงสูงต่อโรงพยาบาล

- ตัวอย่าง: "จำลองสถานการณ์เซิร์ฟเวอร์หลัก HOSxP ถูกโจมตีด้วย Ransomware ทำให้ไฟล์ฐานข้อมูลถูกเข้ารหัสทั้งหมด และระบบหยุดทำงาน 100%"
- เป้าหมาย: เพื่อทดสอบว่าหากเกิดเหตุจริง ทีมงานจะตอบสนองได้รวดเร็วเพียงใด

ข้อที่ 2 การฝึกซ้อมบนโต๊ะประชุม (Tabletop Exercise)

การซ้อมเชิงบริหารและนโยบายโดยไม่ต้องปิดระบบจริง

- กิจกรรม: ประชุมร่วมกับผู้อำนวยการและหัวหน้าแผนก เพื่อซักซ้อมบทบาทการตัดสินใจ เช่น ใครจะเป็นผู้อนุมัติให้ปิดระบบเครือข่าย หรือใครจะเป็นผู้แถลงข่าวต่อสาธารณะ
- เป้าหมาย: ตรวจสอบความเข้าใจใน "สายบังคับบัญชา" (Chain of Command)

ข้อที่ 3 การฝึกซ้อมทางเทคนิคและการกู้ข้อมูล (Technical Drill)

การปฏิบัติงานจริงของฝ่ายไอทีในสภาพแวดล้อมจำลอง (Sandbox)

- กิจกรรม: ฝึกการถอดสาย LAN เพื่อ Isolate ระบบ, การตรวจสอบจุดที่ถูกเจาะ (Entry Point) และการทดสอบ Restore ฐานข้อมูลจาก Backup ลงในเครื่องสำรอง
- เป้าหมาย: วัดค่า RTO (ระยะเวลากู้ระบบ) ว่าทำได้ทันตามที่กำหนดไว้หรือไม่

ข้อที่ 4 การประกาศสถานะระบบขัดข้อง (Downtime Announcement)

ขั้นตอนการสื่อสารจากห้องคอมพิวเตอร์สู่ผู้รับบริการและเจ้าหน้าที่

- กิจกรรม: งานประชาสัมพันธ์ประกาศแจ้งสถานะระบบล่มผ่านเสียงตามสายและกลุ่ม Line, ส่วนแผนกบริการ (OPD/IPD) สลับไปใช้ระบบเวชระเบียนกระดาษทันทีตาม Flow แผนสำรอง
- เป้าหมาย: เพื่อให้การบริการผู้ป่วยดำเนินต่อไปได้โดยไม่หยุดชะงัก (Business Continuity)

ข้อที่ 5 การประเมินผลการซ้อม (Evaluation & Review)

การตรวจสอบความสำเร็จหลังเสร็จสิ้นการซ้อม

- กิจกรรม: ตรวจสอบความครบถ้วนของข้อมูลที่กู้คืนมาได้, ประเมินความพึงพอใจของหน่วยงานหน้างาน และตรวจสอบว่ามีขั้นตอนใดที่เกิดความสับสนหรือล่าช้า
- เป้าหมาย: หาจุดบกพร่อง (Gap Analysis) ก่อนเกิดเหตุการณ์จริง

ข้อที่ 6: การสรุปบทเรียนและผลลัพธ์ (Lessons Learned)

การนำปัญหาที่พบจากการประเมินมาวิเคราะห์เชิงลึก

- กิจกรรม: จัดประชุม After Action Review (AAR) เพื่อระบุว่า "อะไรที่ทำได้ดี" และ "อะไรที่ต้องแก้ไข" เช่น พบว่ารหัสผ่านแอดมินจำยากเกินไป หรือไฟล์ Backup ของบางวันเสียหาย
- เป้าหมาย: เพื่อสร้างองค์ความรู้ใหม่และป้องกันความผิดพลาดซ้ำเดิม

ข้อที่ 7: การปรับปรุงแผนเผชิญเหตุ (Plan Update & Maintenance)

การปรับเปลี่ยนเอกสารแผน IRP ให้เป็นฉบับปัจจุบัน (Update)

- กิจกรรม: แก้ไขขั้นตอนในเล่มแผนเผชิญเหตุตามผลสรุปในข้อ 6, ปรับปรุงรายชื่อผู้รับผิดชอบและเบอร์โทรศัพท์ติดต่อด่วนให้เป็นปัจจุบัน
- เป้าหมาย: เพื่อให้โรงพยาบาลมีแผนที่ "ใช้งานได้จริง" และพร้อมสำหรับการตรวจสอบมาตรฐาน HA หรือ Audit จากส่วนกลาง