การพัฒนาแนวทางในการจัดการความมั่นคงความปลอดภัยระบบสารสนเทศที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร

A Development of Appropriate Approaches for Managing Information Systems Security of Private Hospitals in Bangkok

จิตตกานต์ บุญศิริทิวัตถ์ [1]

โกวิท รพีพิศาล [2]

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาระดับความถี่ของการเกิดภัยคุกคามต่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโรงพยาบาลเอกชนในกรุงเทพมหานคร ภายใต้การควบคุมที่เพิ่มเข้ามาใหม่ใน ISO 27001:2013 จาก ISO 27001:2005 ทั้งในมุมมองของผู้ใช้ระบบและนักพัฒนาระบบ เพื่อพัฒนาแนวทางในการควบคุมความปลอดภัยของระบบสารสนเทศในโรงพยาบาล ประชากรคือบุคลากรของโรงพยาบาลเอกชนในกรุงเทพมหานครทั้งผู้ใช้ระบบ เช่น แพทย์ พยาบาล พนักงาน และผู้พัฒนาระบบทั้งหมด 82 โรงพยาบาล เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถามที่สร้างขึ้นมาตามกรอบแนวคิดของมาตรฐาน ISO 27001:2013 มี 3 ส่วน 1) ลักษณะโดยทั่วไปของโรงพยาบาล 2) ลักษณะโดยทั่วไปของผู้ตอบแบบสอบถาม 3) ตัวแปรความมั่นคงปลอดภัยของระบบสารสนเทศ กลุ่มตัวอย่างเป็นผู้ใช้งานทั่วไป 362 คน และนักพัฒนาระบบ 20 คน ผลการวิจัยพบว่า ภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล, ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และเทคโนโลยีล้าสมัย ผู้วิจัยได้นำเสนอแนวทาง

---

[1] นักศึกษาปริญญาโท, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต, E-mail: mister.aaron@yahoo.com

[2] ผู้ช่วยศาสตราจารย์, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิชาการจัดการเทคโนโลยีสารสนเทศ วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต, E-mail: kowit.r@rsu.ac.th

แนวทางปฏิบัติสำหรับโรงพยาบาลทั้ง 11 ด้าน โดยการกำหนดกรอบนโยบาย และการนำไปปฏิบัติที่ชัดเจนตามความเหมาะสมของทรัพยากรและความสอดคล้องกับขอบเขตของโรงพยาบาล

คำสำคัญ: การจัดการความมั่นคงปลอดภัย ระบบสารสนเทศ การควบคุมความปลอดภัย ISO27001:2013 โรงพยาบาลเอกชน

Abstract

This research aims to study the frequency of threats occurrence in private hospitals in Bangkok towards the maintaining of hospital information systems security under controls as per the standard ISO 27001: 2013 and in perspective of users and developers for developing the guideline for security control management in hospitals in term of threat management. The target population of this research are both general users and developers of private hospitals in Bangkok total 82 hospitals. The instrumentation used in this research was a questionnaire created by the standard ISO 27001: 2013. There are 3 parts in the survey: Part one is general hospital's characteristic. The second part is general respondent's characteristics and the third part is the variable security of information systems based on the new controls added to the ISO 27001: 2013 from ISO 27001: 2005 by the online and paper questionnaires. The sample 362 users and 20 developers were explored. The research found that most of the threats caused by acts of human error or failure, technical hardware and software failures or errors and technological obsolescence. The researcher has presented the guidelines for 11 hospitals by setting the policy framework and the implementation of the resources as appropriate and consistent with the scope of the hospital.

Keywords: Hospital IT Security Management Approaches, Information System, Security Control, ISO27001:2013 Private Hospital

ความเป็นมาและความสำคัญของปัญหาการวิจัย

ปัจจุบันการดำเนินธุรกิจได้มีการนำระบบสารสนเทศเข้ามาใช้งานเพื่อเพิ่มประสิทธิภาพการทำงาน ความรวดเร็วในการให้บริการ รวมถึงความถูกต้องแม่นยำของข้อมูลต่างๆ แต่ในการใช้เทคโนโลยีสารสนเทศนั้นมักพบปัญหาต่างๆ หลายด้าน ไม่ว่าจะด้านความมั่นคงปลอดภัยของระบบที่ทำให้องค์กรได้รับความเสียหาย ดังนั้น การกำหนดนโยบายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจึงมีความสำคัญอย่างยิ่ง การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี การจัดการความเสี่ยงของระบบสารสนเทศได้มีการนำมาใช้ในหน่วยงานธุรกิจของภาครัฐและเอกชน มาตรฐาน ISO ถูกกำหนดและควบคุมโดยองค์การนานาชาติเพื่อเป็นระบบมาตรฐานสากล มาตรฐาน ISO 27001 เป็นแนวทางหรือวิธีการเกี่ยวกับเรื่องความเสี่ยงด้านสารสนเทศเพื่อการกำหนดนโยบายและกระบวนการทำงาน รวมทั้งเพื่อเลือกการควบคุมที่เหมาะสมในการบริหารความเสี่ยง (International Organization for Standardization, 2014)

ในอุตสาหกรรมโรงพยาบาล ระบบสารสนเทศนั้นถูกพัฒนาขึ้นเพื่อรวบรวมและจัดเก็บข้อมูลจากแหล่งต่างๆทั้งภายในและภายนอก โรงพยาบาลเอกชนหลายแห่งได้มีการนำระบบสารสนเทศทางการแพทย์ (Electronics Medical Records) เข้ามาประยุกต์ใช้ เพื่อเพิ่มขีดความสามารถในการแข่งขัน โดยมีการเชื่อมโยงฐานข้อมูลต่างๆเข้าด้วยกัน ไม่ว่าจะเป็น เวชระเบียนผู้ป่วย ประวัติการรักษา ดังนั้นข้อมูลระบบสารสนเทศของโรงพยาบาลจึงสำคัญอย่างยิ่ง ผู้วิจัยได้เล็งเห็นถึงปัญหาว่าควรมีการศึกษาระดับความถี่ของเหตุการณ์การเกิดภัยคุกคามและจัดทำแนวแนวทางในการจัดการการควบคุมความปลอดภัยระบบสารสนเทศที่สามารถนำไปประยุกต์ใช้ในอุตสาหกรรมโรงพยาบาล เพื่อให้ระบบมีเสถียรภาพด้านความมั่นคงปลอดภัยของข้อมูล และมีกรอบนโยบายด้านความมั่นคงปลอดภัย โดยใช้มาตรฐาน ISO 27001:2013 มาเป็นวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยให้มีประสิทธิภาพมากขึ้น

ขอบเขตของการวิจัย

1) ด้านประชากรงานวิจัย

ประชากรกลุ่มเป้าหมายของวิจัยนี้คือบุคลากรโรงพยาบาลเอกชนในกรุงเทพมหานครในฐานะใช้ระบบสารสนเทศ จำนวน 362 คน และผู้พัฒนาระบบ (Developer) จำนวน 20 คน จาก 82 โรงพยาบาล

2) ด้านตัวแปรงานวิจัย

2.1) ตัวแปรต้น

- จำนวนปีที่ดำเนินกิจการ (0-10 ปี, 11-30 ปี และ 31 ปีขึ้นไป)
- ขนาดของโรงพยาบาล (1-100 เตียง, 101-300 เตียง และ 301 เตียงขึ้นไป)
- จำนวนผู้ใช้งานระบบ (1-200 คน, 201-500 คน และ 501 คนขึ้นไป)
- เพศ (ชาย และ หญิง)
- อายุการทำงาน (0-5 ปี, 6-10 ปี และ 11 ปีขึ้นไป)
- ลักษณะงาน มี 3 กลุ่ม คือ แพทย์และผู้ช่วยแพทย์, พยาบาลและผู้สนับสนุนทางการแพทย์ (เภสัช นักเทคนิคการแพทย์) และ พนักงานหลังบ้าน

2.2) ตัวแปรตาม

ระดับความถี่ของภัยคุกคาม (ระดับความถี่, บ่อยมาก, บ่อย, บางครั้ง, น้อยครั้งและไม่เคย) ภัยคุกคาม 12 ข้อประกอบไปด้วย 1) ข้อผิดพลาดจากการกระทำของมนุษย์ 2) การละเมิดทรัพย์สินทางปัญญา 3) การบุกรุก 4) การกรรโชกข้อมูลสารสนเทศ 5) การก่อวินาศกรรมหรือการทำลาย 6) การโจรกรรม 7) การโจมตีซอฟต์แวร์ 8) ภัยธรรมชาติ 9) คุณภาพของบริการ 10) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ 11) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ 12) เทคโนโลยีล้าสมัย,

การควบคุมความมั่นคงปลอดภัยที่เพิ่มเข้ามาใหม่ใน ISO 27001:2013 จาก ISO 27001:2005 1) การควบคุมความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการ 2) การควบคุมการจำกัดการติดตั้งซอฟต์แวร์ 3) การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ 4) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก 5) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ 6) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 7) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ 8) การควบคุมนโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย 9) การควบคุมลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย 10) การควบคุมสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย 11) การควบคุมการทดสอบด้านความมั่นคงปลอดภัยของระบบ

กรอบแนวคิดและทฤษฎี

ผู้วิจัยได้กำหนดกรอบแนวคิดและทฤษฎีด้านเนื้อหาตามหัวข้อข้างล่างดังนี้

1) ความเสี่ยงของระบบสารสนเทศ

เป็นความเสี่ยงที่เกิดจากองค์กรมีการนำเทคโนโลยีสารสนเทศมาใช้ในการขับเคลื่อน และดำเนินงานอย่างกว้างขวาง ระบบสารสนเทศจึงกลายเป็นโครงสร้างพื้นฐานของการดำเนินธุรกิจและธุรกรรมต่างๆ ขององค์กรที่จะขาดเสียมิได้ดังนั้นการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร จึงมีความสำคัญต่อองค์กรอย่างมาก จนอาจกล่าวได้ IT Risk คือ Business Risk นั่นเอง (ISSACA, 2014)

2) ภัยคุกคามระบบสารสนเทศ

คือสิ่งที่ก่อให้เกิดอันตรายต่อทรัพยากรคอมพิวเตอร์ ผู้ใช้คอมพิวเตอร์เป็นสิ่งที่ทำให้เกิดความเสียหายของข้อมูล ไม่ว่าจะเป็นส่วนใดส่วนหนึ่งของข้อมูล เมื่อข้อมูลนั้นการคุกคาม โดยภัยคุกคามนี้ถ้าไม่ได้มีการป้องกันที่รัดกุมแล้วนั้น ก็จะเป็นสาเหตุที่จะทำให้ข้อมูลนั้นเกิดการเสียหายได้ โดยการโจมตีของกลุ่มที่ไม่หวังดีเช่นจากบุคคลภายในองค์กรเอง หรือกลุ่มเจาะระบบ (Hacker) อย่างไรก็ได้ ถ้ามีการจัดการที่ดีต่อข้อมูล ทำให้ข้อมูลนั้นปลอดภัยรัดกุมอยู่เสมอ ภัยต่างๆ ก็ไม่สามารถที่จะทำให้ข้อมูลเสียหายได้ (ศราวุฒิ จันทะคัด, 2554) และ (University of South Carolina Board of Trustees, 2014)

3) การจัดการความเสี่ยงของระบบสารสนเทศในโรงพยาบาล

การจัดการความเสี่ยงของระบบสารสนเทศ หน่วยงานธุรกิจ และหน่วยงานของรัฐจำนวนมาก มองข้ามถึงการจัดการปัญหาเรื่องความปลอดภัยของข้อมูล ด้วยเหตุว่าเป็นงานที่มีเทคนิคซับซ้อนในปัจจุบันข้อมูลข่าวสารที่มีความสำคัญต่อองค์กรและบุคคลเป็นหลัก ดังนั้นต้องสร้างความมั่นคงปลอดภัยในระบบสารสนเทศให้มีความเสี่ยงน้อยที่สุด โดยกำหนดมาตรการรักษาความปลอดภัยขององค์การโดยเฉพาะอย่างยิ่งองค์กรต่างๆที่ต้องสามารถปรับตัวและรับกับสภาพปัจจุบันที่มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่เสมอ หากระบบสารสนเทศขององค์กรถูกโจมตีไม่ว่าทางตรงหรือทางอ้อม จะทำให้เกิดผลเสียต่อองค์กรและการดำเนินงานต่างๆ ได้ เนื่องจากการที่ตัดสินใจจากข้อมูลที่ผิดพลาดหรือไม่สามารถหาข้อมูลเหล่านั้นไปใช้ได้ทันเวลา ยิ่งสถานการณ์ในปัจจุบันความถูกต้องและความรวดเร็วของข้อมูลข่าวสารมีความสำคัญมากสำหรับการบริการทางการแพทย์ เพื่อที่จะสนองความต้องการของผู้มารับบริการได้

อย่างรวดเร็วมากขึ้น ดังนั้นเพื่อให้มีความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร จึงควรมีนโยบายรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรนำมาใช้ในการบริหารงาน เพื่อให้เกิดเสถียรภาพและภาพลักษณ์ความเชื่อมั่นที่ดีต่อองค์การรักษาความปลอดภัยข้อมูลของธุรกิจ ซึ่งมีผลกระทบกับค่าใช้จ่ายหากธุรกิจต้องหยุดชะงัก จึงจำเป็นต้องเน้นเรื่องความปลอดภัย เช่น การแก้ปัญหาทางเทคนิค เป็นต้น

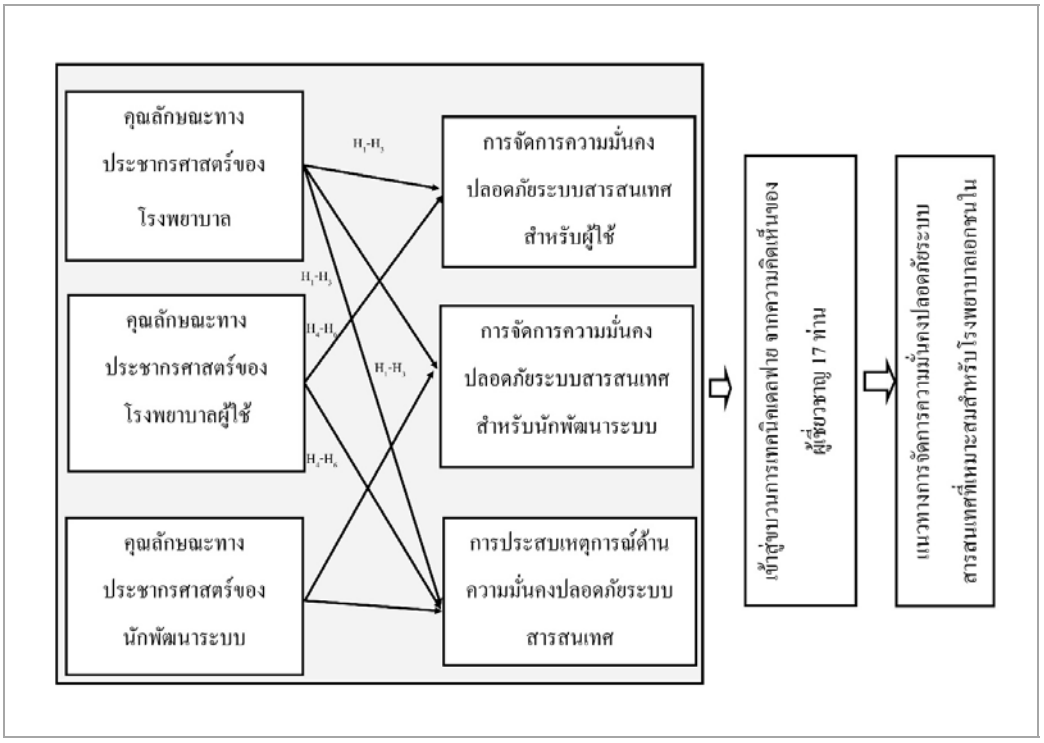
ระบบสารสนเทศโรงพยาบาล ถูกพัฒนาขึ้นเพื่อรวบรวมและจัดเก็บข้อมูลจากแหล่งข้อมูลต่างๆ ทั้งภายในและภายนอกโรงพยาบาลอย่าง มีหลักเกณฑ์ ตามกฎ ระเบียบ ข้อบังคับและมาตรฐานของระบบรับรองคุณภาพต่างๆ เพื่อนำมาประกอบผลและจัดรูปแบบให้ได้สารสนเทศที่ช่วยสนับสนุนการทำงานและการตัดสินใจในด้านต่างๆ ของผู้บริหาร เพื่อให้การดำเนินงานของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพทำให้บุคลากร ปฏิบัติงานได้สะดวกและรวดเร็ว ทำให้มีเวลาในการให้บริการแก่ผู้ป่วยมากขึ้น มีเวลามาพัฒนาคุณภาพบริการให้ดีขึ้น

4) มาตรฐาน ISO/IEC27001

เป็นแนวทางหรือวิธีการเกี่ยวกับเรื่องความเสี่ยงด้านสารสนเทศเพื่อการกำหนด นโยบายและกระบวนการทำงาน รวมทั้งเพื่อเลือกการควบคุมที่เหมาะสมในการบริหารความเสี่ยงด้วย กล่าวได้ว่าเป็นมาตรฐานเชิงระบบที่เน้นการปฏิบัติ จึงสามารถนำไปใช้อ้างอิงเพื่อการประเมินและขอรับการรับรองมาตรฐานได้ ซึ่งแน่นอนว่าระบบต่างๆ ในโรงพยาบาลที่มีการนำเทคโนโลยีสารสนเทศเข้ามาประยุกต์ใช้ย่อมเกี่ยวโยงกับระบบสารสนเทศอย่างไม่มีทางเลี่ยงได้ ดังนั้นองค์กรต่างๆ ควรจะจัดให้การจัดการความเสี่ยงที่เหมาะสม โดยการนำกรอบ

นโยบายมาตรฐานต่างๆ ที่กำหนดมาประยุกต์ใช้ในองค์กรให้เหมาะสมตามรูปแบบในแต่ละการดำเนินธุรกิจหลังจากที่ได้ดำเนินการเปรียบเทียบระบบรักษาความมั่นคงปลอดภัยในปัจจุบันกับ มาตรฐาน ISO ที่เลือกใช้ และมีการจัดการประเมินความเสี่ยงที่เกิดขึ้นกับระบบสารสนเทศขององค์กร ทำให้เราได้ทราบถึงปัญหาที่เกิดขึ้น และหาแนวทางในการจัดทำเป็นนโยบายรักษาความมั่นคง ปลอดภัยสารสนเทศขององค์กรเพื่อเป็นแนวทางในการปฏิบัติ

กรอบการวิจัย



วัตถุประสงค์การวิจัย

1. ศึกษามุมมองของผู้ใช้และผู้พัฒนาระบบสารสนเทศของโรงพยาบาลเอกชนในกรุงเทพมหานครต่อการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ
2. ศึกษาการประสบเหตุการณ์ด้านความมั่นคงปลอดภัยของโรงพยาบาล และบุคลากรโรงพยาบาลทั้งในส่วนของผู้ใช้และผู้พัฒนาระบบ
3. พัฒนาแนวทางในการจัดการการควบคุมความปลอดภัยระบบสารสนเทศที่เหมาะสมสำหรับโรงพยาบาลเอกชนในกรุงเทพมหานคร

สมมติฐาน

H_1 โรงพยาบาลที่มีจำนวนปีในการดำเนินงานต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

H_2 โรงพยาบาลที่มีขนาดต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

H_3 โรงพยาบาลที่มีผู้ใช้งานระบบต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

H_4 ผู้ใช้ระบบที่มีเพศสภาพที่ต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

H_5 ผู้ใช้ระบบที่มีอายุการทำงานที่ต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

H_6 ผู้ใช้ระบบที่มีลักษณะงานที่ต่างกันมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศในส่วนผู้ใช้แตกต่างกัน

การเก็บรวบรวมข้อมูล

การศึกษาครั้งนี้เป็นการศึกษาประชากร คือ ผู้ใช้งานระบบในโรงพยาบาลเอกชน จำนวน 82 โรงพยาบาล การสุ่มโรงพยาบาลผู้วิจัยใช้วิธีการสุ่มแบบสุ่มตัวอย่างแบบบังเอิญหรือตามความสะดวก (Convenience Sampling) เป็นการสุ่มแบบรายสะดวกโดยการแจกแบบสอบถามออนไลน์และแบบสอบถามในรูปแบบกระดาษ โดยกำหนดกลุ่มตัวอย่างจากผู้ใช้ระบบและนักพัฒนาระบบของโรงพยาบาลเอกชนในกรุงเทพมหานคร ทั้งหมด 82 โรงพยาบาล แบบสอบถามสำหรับผู้ใช้งานระบบคิดเป็นจำนวน 400 คน ได้แบบสอบถามคืนมา 362 ชุด คิดเป็นร้อยละ 90.5 ส่วนแบบสอบถามสำหรับผู้พัฒนาระบบคิดเป็นจำนวน 20 คน ได้แบบสอบถามคืนมา 20 ชุด คิดเป็นร้อยละ 100

เครื่องมือและวิธีดำเนินการวิจัย

1) เครื่องมือวิจัย

1.1) แบบสอบถามงานวิจัย ผู้วิจัยได้สร้างแบบสอบถามตามวัตถุประสงค์ในการศึกษา ที่ได้กำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการรวบรวมข้อมูลโดยเนื้อหาของแบบสอบถามแบ่งเป็น 3 ส่วน ดังนี้ ส่วนที่หนึ่ง คือ ลักษณะโดยทั่วไปของโรงพยาบาล ข้อมูล ประกอบด้วย จำนวนปีที่ดำเนินกิจการ ขนาดของโรงพยาบาล และจำนวนผู้ใช้ระบบ ส่วนที่สองคือลักษณะโดยทั่วไปของผู้ตอบแบบสอบถาม ข้อมูล ประกอบด้วย เพศ อายุการทำงาน และลักษณะงาน และส่วนที่สามคือ ตัวแปรความมั่นคงปลอดภัยของระบบสารสนเทศโดยยึดเกณฑ์การควบคุมที่เพิ่มเข้ามาใหม่ใน ISO 27001:2013 จาก ISO 27001:2005 โดยการควบคุมสำหรับผู้ใช้งานระบบมีจำนวน 7 ข้อประกอบไปด้วย 1) การควบคุมความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ 2) การควบคุมการจำกัดการติดตั้งซอฟต์แวร์ 3) การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก 4) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก 5) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ 6) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ 7) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ และผู้ใช้งานระบบจำนวน 4 ข้อ ประกอบไปด้วย 1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย 2) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย 3) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย และ 4) การทดสอบด้านความมั่นคงปลอดภัยของระบบ ประชากรกลุ่มเป้าหมายของวิจัยนี้คือบุคลากร ทั้งผู้ใช้ระบบและนักพัฒนาระบบของโรงพยาบาลเอกชนในกรุงเทพมหานคร ทั้งหมด 82 โรงพยาบาล การสุ่มโรงพยาบาลผู้วิจัยใช้วิธีการสุ่มแบบสุ่มตัวอย่างแบบบังเอิญหรือตามความสะดวก (Convenience Sampling) เป็นการสุ่มแบบรายสะดวกโดยการแจกแบบสอบถามออนไลน์และแบบสอบถามในรูปแบบกระดาษ การหาขนาดกลุ่มตัวอย่าง ผู้ใช้งานระบบและนักพัฒนาระบบ ผู้ใช้ระบบทั่วไปคือบุคลากรของโรงพยาบาล เนื่องจากผู้ใช้งานระบบและนักพัฒนาระบบนั้นผู้วิจัยไม่สามารถทราบจำนวนที่แน่นอนได้ จึงใช้วิธีการสุ่มตัวอย่าง โดยใช้สูตร ไม่ทราบจำนวนประชากรของ W.G. Cochran ผู้วิจัยจึงใช้ขนาดกลุ่มตัวอย่าง 330 คน

1.2) แบบสอบถามข้อค้นพบ เพื่อรวบรวมข้อมูลสำหรับความคิดเห็นของสภาพปัจจุบันในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลเอกชนในกรุงเทพมหานคร โดยเป็นแบบคำถามปลายเปิดเพื่อถามถึงสาเหตุของภัยคุกคามและการจัดการความมั่นคงปลอดภัยในระบบสารสนเทศในส่วนของผู้ใช้งานและผู้พัฒนาระบบ โดยแบบสอบถามเป็นการแจกแบบออนไลน์และสัมภาษณ์

เชิงลึกจากผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในหน่วยงานแผนก Information Technology (IT) ของ โรงพยาบาล

1.3) แบบสอบถามสำหรับการทำเทคนิคเดลฟายรอบที่ 1 เป็นแบบสอบถามแบบปลายเปิดรอบที่ 1 ที่ให้ผู้เชี่ยวชาญแสดงความคิดเห็นอย่างอิสระที่เกี่ยวกับแนวทางการปฏิบัติในการจัดการคุกคามระบบสารสนเทศในโรงพยาบาลเอกชนในกรุงเทพมหานคร โดยนำคำตอบที่ได้มาประมวลตัดข้อความที่ซ้ำซ้อนหรือส่วนเกินไปจากขอบข่ายที่กำหนดไว้ ทำการวิเคราะห์เนื้อหา (Content Analysis) และนำผลที่ได้ไปสร้างแบบสอบถามในรอบที่ 2

1.4) แบบสอบถามสำหรับการทำเทคนิคเดลฟายรอบที่ 2 เป็นแบบสอบถามแบบมาตราส่วนประมาณค่า 5 ระดับ ที่ให้ผู้เชี่ยวชาญจัดอันดับความสำคัญของข้อความแต่ละข้อที่ผู้เชี่ยวชาญเห็นว่ามีในการจัดการคุกคามระบบสารสนเทศในโรงพยาบาลเอกชนในกรุงเทพมหานคร โดยนำคำตอบที่ได้มาวิเคราะห์หาค่ามัธยฐาน ฐานและค่าพิสัยระหว่างควอไทล์ของคำถามแต่ละข้อ แล้วจึงนำผลที่ได้ไปสร้างแบบสอบถามรอบที่ 3 ที่มีการเพิ่มค่ามัธยฐาน ช่วงพิสัยระหว่างควอไทล์ และน้ำหนักคะแนนที่ผู้เชี่ยวชาญท่านนั้นๆ ตอบในรอบที่ผ่านมา

1.5) แบบสอบถามสำหรับการทำเทคนิคเดลฟายรอบที่ 3 เป็นแบบสอบถามซึ่งมีคำถามเหมือนแบบสอบถามรอบที่ 2 ที่ให้ผู้เชี่ยวชาญกลุ่มเดิมพิจารณาทบทวนคำตอบของตน แล้วนำคำตอบมาทำการวิเคราะห์หาค่ามัธยฐาน ฐานนิยม ความแตกต่างระหว่างมัธยฐานกับฐานนิยม และค่าพิสัยระหว่างควอไทล์

2) สถิติที่ใช้ในการวิจัย

การวิเคราะห์ข้อมูลโดยใช้สถิติพรรณนาด้วยโดยการใช้ความถี่ ค่าร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน สถิติอ้างอิงโดยใช้ t-test กับตัวแปรเพศสภาพของผู้ใช้ระบบ ANOVA F-test ใช้กับคุณลักษณะทางประชากรศาสตร์ของโรงพยาบาล จำนวนผู้ใช้ระบบ และลักษณะงานของผู้ใช้ระบบ

การทดสอบคุณภาพของแบบสอบถามโดยใช้การทดสอบความเที่ยงตรง สำหรับการนำเสนอนั้นเป็นการนำแบบสัมภาษณ์ไปทดลองใช้กับผู้ที่เกี่ยวข้องกับแผนก IT ของโรงพยาบาลที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่าง จำนวน 25 ท่าน โดยให้ผู้ที่ถูกสัมภาษณ์ตอบแบบสัมภาษณ์ เพื่อให้ผู้ถูกสัมภาษณ์ประเมินว่าเข้าใจข้อคำถาม วัตถุประสงค์ และเนื้อหาของแบบสัมภาษณ์หรือไม่ สรุปค่าดัชนีความสอดคล้องระหว่างแบบสอบถามกับตัวชี้วัด หลังจากนั้นให้ผู้เชี่ยวชาญทั้ง 3 ท่าน ตรวจ IOC ได้ค่าความสอดคล้องทั้งฉบับเท่ากับ 0.98 และทดสอบความน่าเชื่อถือด้วยค่าสัมประสิทธิ์แอลฟา (Cronbach Alpha) ได้ค่าเท่ากับ 0.82

ค่ามัธยฐาน (Median) จากแบบสอบถามมาตราส่วนประมาณค่า ที่ผู้วิจัยได้กำหนดน้ำหนักของคะแนนเป็น 5 ระดับ ตามเกณฑ์ของลิเคริ์ท (Likert Scale)

Delphi (Median & Interquartile) ค่าพิสัยระหว่างควอไทล์ (Interquartile Range) ผู้วิจัยคำนวณหาค่าพิสัยระหว่างควอไทล์จากค่าความแตกต่างระหว่างควอไทล์ที่ 3 กับควอไทล์ที่ 1 ค่าพิสัยระหว่างควอไทล์ของข้อความใดที่มีค่าน้อยกว่าหรือเท่ากับ 1.50 แสดงว่าความคิดเห็นของกลุ่มผู้เชี่ยวชาญที่มีต่อข้อความนั้นสอดคล้องกัน แต่ถ้าค่าพิสัยระหว่างควอไทล์ของข้อความนั้นมีค่ามากกว่า 1.50 แสดงว่าความคิดเห็นของกลุ่มผู้เชี่ยวชาญที่มีต่อข้อความนั้นไม่สอดคล้องกัน

ผลการศึกษา

ส่วนที่ 1 ภูมิหลังของลักษณะโดยทั่วไปของโรงพยาบาล

จากการวิจัยพบว่าจำนวนปีที่ดำเนินกิจการของโรงพยาบาลส่วนใหญ่จำนวนปีที่ดำเนินกิจการ 0-10 ปี (ร้อยละ 49.72) โดยส่วนใหญ่มีจำนวนเตียงโรงพยาบาล 101-300 เตียง (ร้อยละ 45.85) ส่วนใหญ่มีจำนวนผู้ใช้งานระบบ 201-500 คน (ร้อยละ 43.37)

ตารางที่ 1 ความถี่และร้อยละของภูมิหลังของลักษณะโดยทั่วไปของโรงพยาบาล

จำนวนปีที่ดำเนินกิจการ	จำนวนตัวอย่าง (โรงพยาบาล)	ร้อยละ
0-10 ปี	180	49.72
11-30 ปี	106	29.28
31 ปีขึ้นไป	76	20.99
รวม	362	100.0

จำนวนเตียงโรงพยาบาล	จำนวนตัวอย่าง (โรงพยาบาล)	ร้อยละ
1-100 เตียง	144	39.77
101-300 เตียง	166	45.85
301 เตียงขึ้นไป	52	14.36
รวม	362	100.00

จำนวนผู้ใช้งานระบบ	จำนวนตัวอย่าง (โรงพยาบาล)	ร้อยละ
1-200 คน	156	43.09
201-500 คน	157	43.37
501 คนขึ้นไป	49	13.53
รวม	362	100.00

ส่วนที่ 2 ภูมิหลังของบุคลากรทั้งผู้ใช้ระบบและนักพัฒนาระบบของโรงพยาบาล

จากการวิจัยพบว่าบุคลากรผู้ใช้ระบบของโรงพยาบาลเอกชนในกรุงเทพมหานคร ส่วนใหญ่เป็นเพศหญิง (ร้อยละ 66.85) ส่วนใหญ่มีอายุการทำงาน 0-5 ปี (ร้อยละ 58.56) และ ส่วนใหญ่ลักษณะงานคือพยาบาล (ร้อยละ 21.54) สำหรับนักพัฒนาระบบ ส่วนใหญ่เป็นเพศชาย (ร้อยละ 70.00) ส่วนใหญ่มีอายุการทำงาน 6-10 ปี (ร้อยละ 50.00)

ตารางที่ 2 ความถี่และร้อยละของภูมิหลังของบุคลากรทั้งผู้ใช้ระบบและนักพัฒนาระบบของโรงพยาบาล

เพศ	จำนวนตัวอย่าง (คน)	ร้อยละ
ชาย	120	33.14
หญิง	242	66.85
รวม	362	100.00

จำนวนปีอายุการทำงาน	จำนวนตัวอย่าง (คน)	ร้อยละ
0-5 ปี	212	58.56
6-10 ปี	100	27.62
11 ปีขึ้นไป	50	13.81
รวม	362	100.00

ลักษณะงาน	จำนวนตัวอย่าง(คน)	ร้อยละ
แพทย์และผู้ช่วยแพทย์	120	33.16
พยาบาลและผู้สนับสนุนทางการแพทย์	122	33.68
พนักงานหลังบ้านและอื่นๆ	120	33.16
รวม	362	100.00

ตารางที่ 3 แสดงสัดส่วนของ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของระดับภัยคุกคามของผลรวม ระดับประเภทของภัยคุกคามภายใต้การควบคุมที่เพิ่มเข้ามาใหม่ 11 ข้อตามมาตรฐาน (7 ข้อสำหรับผู้ใช้งานทั่วไป)

มาตรฐานการควบคุมภัยคุกคาม	$\bar{X}$	SD	**ระดับความถี่ของภัยคุกคาม**
1) การควบคุมความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ	1.99	0.53	น้อยครั้ง
2) การควบคุมการจำกัดการติดตั้งซอฟต์แวร์	1.68	0.43	ไม่เคย
3) การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก	1.65	0.37	ไม่เคย
4) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก	1.66	0.34	ไม่เคย
5) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ	2.22	0.47	น้อยครั้ง
6) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	1.68	0.51	ไม่เคย
7). สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ	2.35	0.64	น้อยครั้ง
การประสบเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ	1.89	0.47	น้อยครั้ง

ตารางที่ 4 แสดงสัดส่วนของ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของระดับภัยคุกคามของผลรวมระดับประเภทของภัยคุกคามภายใต้การควบคุมที่เพิ่มเข้ามาใหม่ 11 ข้อตามมาตรฐาน (4 ข้อสำหรับผู้พัฒนาระบบ)

มาตรฐานการควบคุมภัยคุกคาม	$\bar{X}$	SD	ระดับความถี่ของภัยคุกคาม
1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)	2.90	0.95	บางครั้ง
2) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)	2.77	0.99	บางครั้ง
3) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)	2.77	0.95	บางครั้ง
4) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)	2.60	0.78	น้อยครั้ง
การประสบเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ	2.76	0.91	บางครั้ง

ผลการทดสอบสมมติฐาน

การทดสอบสมมติฐานมีทั้งหมด 42 ข้อ ได้รับการยอมรับ 17 ข้อ อย่างมีนัยยะสำคัญที่ระดับ 0.05 ได้แก่ $H_{1.1}$ (F = 8.040 และ p-value = 0.000), $H_{1.3}$ (F = 9.648 และ p-value = 0.000), $H_{1.4}$ (F 5.465 = และ p-value = 0.005), $H_{1.5}$ (F = 3.881 และ p-value = 0.021), $H_{1.6}$ (F = 4.914 และ p-value = 0.008), $H_{1.7}$ (F = 3.351 และ p-value = 0.036), $H_{2.2}$ (F = 8.434 และ p-value = 0.000), $H_{2.3}$ (F = 11.580 และ p-value = 0.000), $H_{3.2}$ (F = 5.931 และ p-value = 0.003), $H_{3.3}$ (F = 12.416 และ p-value = 0.000), $H_{3.6}$ (F = 5.311 และ p-value = 0.005), $H_{4.3}$ (t = 2.172 และ p-value = 0.030), $H_{6.2}$ (F = 7.313 และ p-value = 0.001), $H_{6.3}$ (F = 31.216 และ p-value = 0.000), $H_{6.4}$ (F = 15.899 และ p-value = 0.000) $H_{6.5}$

(F = 23.115 และ p-value = 0.000), $H_{6.6}$ (F = 3.673 และ p-value = 0.026) และมีการปฏิเสธทั้งหมด 25 ข้อ

สรุปผลการวิจัยและอภิปรายผลการวิจัย

จากตารางที่ 3 และ 4 พบกว่าตัวชี้วัดที่ใช้ในเรื่องการควบคุมภัยคุกคามมีอยู่ 4 ตัวชี้วัดที่ไม่เคยพบในโรงพยาบาลเลย ได้แต่ การควบคุมการจำกัดการติดตั้งซอฟต์แวร์, การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก และการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

เป็นที่น่าสังเกตว่าสมมติฐานในงานวิจัยนี้โดยส่วนใหญ่ได้รับการปฏิเสธมากกว่าการยอมรับ แม้ว่า เมื่อแยกเป็นรายข้อย่อยแล้วมีบางข้อที่ได้รับการยอมรับ แสดงให้เห็นว่า ความแตกต่างระหว่างเพศสภาพของผู้ใช้ ล้วนไม่มีผลของความแตกต่างต่อมีการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

ในการสัมภาษณ์ผู้ทรงคุณวุฒิที่เกี่ยวข้องในเรื่องของการวิเคราะห์หาข้อค้นพบและสาเหตุของภัยคุกคามพบว่า ข้อมูลคนไข้นั้นยิ่งมีมากเท่าไหร่ก็ยิ่งเสี่ยงต่อการถูกโจมตีมากขึ้นเท่านั้น ซึ่งข้อมูลการรักษาพยาบาล (Medical Records) มีความอ่อนไหวในข้อมูลส่วนตัวอย่างมาก เช่น ประวัติคนไข้ เลขที่บัตรประชาชน ที่อยู่ ยาที่แพ้ ประวัติการเจ็บป่วย ประวัติค่ารักษาพยาบาล เรียกได้ว่าข้อมูลทั้งหมดล้วนเป็นข้อมูลส่วนบุคคล หากมีการรั่วไหลแล้วจะสามารถนำไปเป็นหลักฐานในการพิสูจน์ตัวตน เช่น ทำธุรกรรมทางการเงินต่างๆ มีรายงานจากข่าวต่างประเทศพบว่าแฮกเกอร์ส่วนมากโจรกรรมข้อมูลโรงพยาบาลเพื่อเรียกค่าไถ่ (Forbes, 2016) ซึ่งสอดคล้องกับสมมติฐานในตัวแปรด้านคุณลักษณะประชากรศาสตร์ของโรงพยาบาล และอายุการทำงานของผู้ใช้ กล่าวคือ โรงพยาบาลที่มีจำนวนปีในการดำเนินงาน ผู้ใช้ระบบ ขนาดของโรงยาบาล จะมีข้อมูลคนไข้มากขึ้นตามจำนวนและขนาด

โดยสรุปแล้วจำเป็นต้องมีแนวทางการปฏิบัติในการจัดการคุกคามระบบสารสนเทศเพื่อความปลอดภัย และป้องกันสิ่งที่อาจจะเกิดขึ้นในอนาคต จึงจะเป็นการพัฒนาที่ก่อให้การป้องกันอย่างมีมาตรฐานและเป็นแบบสากลได้

ข้อค้นพบที่ได้ มีความสอดคล้องกับงานวิจัยเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศกรณีศึกษา ศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี (เฉลิม สุวรรณะ, 2554) ในด้านความเสี่ยงที่พบจากการประเมินความเสี่ยงของระบบของโรงพยาบาลตามมาตรฐาน ISO/IEC 27001

เช่น โรงพยาบาลยังไม่มีการจัดทำนโยบายความปลอดภัยสำหรับสารสนเทศขององค์กร อย่างเป็นลายลักษณ์อักษร หรือ ปัญหาความเสี่ยงจากการคุกคามของไวรัส เป็นต้น ทั้งนี้ผู้วิจัยได้นำข้อค้นพบที่น่าสนใจนำมาอภิปรายตามตารางที่ 7 ต่อไป

อนึ่งแนวทางการปฏิบัติที่นำเสนอไว้ในตารางที่ 7 นี้ เป็นบทสรุปจากผู้เชี่ยวชาญทั้ง 17 ท่าน โดยผู้วิจัยได้นำเสนอแนวทางในการควบคุมความปลอดภัยของระบบสารสนเทศในโรงพยาบาลจากการค้นพบในงานวิจัยนี้เป็นเบื้องต้นนำเสนอผู้เชี่ยวชาญก่อน หลังจากใช้เทคนิคการวิจัยแบบเดลฟายเพื่อให้ข้อเสนอแนวทางปฏิบัตินี้ขอความคิดเห็นเพิ่มเติม หาความสอดคล้องและคิดเห็นในแนวทางเดียวกันและเพื่อให้เกิดความน่าเชื่อถือและสามารถนำไปใช้ประโยชน์ได้จริง จึงได้ระดมความคิดเห็นจากผู้เชี่ยวชาญ 17 ท่าน (ซึ่งถือว่ามีความคลาดเคลื่อนน้อย ดูตารางที่ 5) ผู้เชี่ยวชาญประกอบไปด้วย อาจารย์สาขาวิชาเทคโนโลยีสารสนเทศ 3 ท่าน แพทย์ 2 ท่าน ผู้บริหารระดับสูง 2 ท่าน ผู้พัฒนาระบบ 3 ท่าน ผู้ดูแลระบบ network security 2 ท่าน และบุคลากรในโรงพยาบาลเอกชน 5 ท่าน โดยเครื่องมือที่ใช้เป็นคำถามปลายเปิดและแบบมาตราส่วนประมาณค่า (rating scale)

ตารางที่ 5 จำนวนผู้เชี่ยวชาญที่ใช้ในการวิจัยด้วยเทคนิคเดลฟาย

จำนวนผู้เชี่ยวชาญ	ช่วงของความคลาดเคลื่อน	ความคลาดเคลื่อนลดลง
1 – 5	1.02 – .70	0.5
5 – 9	.70 – .58	0.12
9 – 13	.58 – .54	0.04
13 - 17	.54 - .50	0.04
17 - 21	.50 - .48	0.02
21 - 25	.48 - .46	0.02
25 – 28	.46 - .44	0.02

ผู้วิจัยนำค่าพิสัยระหว่างควอไทล์ และค่าความแตกต่างระหว่างมัธยฐานกับฐานนิยมมาเป็นเกณฑ์ในการพิจารณาความสอดคล้องของแนวโน้มแต่ละข้อความ กล่าวคือ ข้อความใดมีค่าพิสัยระหว่างควอไทล์ไม่เกิน 1.50 และผลต่างระหว่างมัธยฐานกับฐานนิยม ไม่เกิน 1.00 แสดงว่าความคิดเห็นของกลุ่มผู้เชี่ยวชาญที่มีต่อข้อความนั้นมีความสอดคล้องกัน และสำหรับข้อความใดที่มีค่าพิสัยระหว่างควอไทล์

และผลต่างระหว่างมัธยฐานกับฐานนิยมไม่เป็นไปตามเกณฑ์ดังกล่าวข้างต้นแสดงว่าความคิดเห็นของกลุ่มผู้เชี่ยวชาญที่มีต่อข้อความนั้นไม่สอดคล้องกัน

การเสนอแนวทางปฏิบัติ

จากข้อค้นพบของงานวิจัยจากการสัมภาษณ์แบบสอบถามจากผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในหน่วยงานแผนก Information Technology (IT) ของ โรงพยาบาล เพื่อรวบรวมข้อมูลสำหรับความคิดเห็นของสภาพปัจจุบันในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลเอกชนในกรุงเทพมหานคร ผู้วิจัยได้เสนอทางการปฏิบัติในการจัดการคุกคามระบบสารสนเทศในโรงพยาบาลเอกชนในกรุงเทพมหานครไว้ในตารางที่ 6 ดังนี้

ตารางที่ 6 แนวทางการปฏิบัติในการจัดการคุกคามระบบสารสนเทศในโรงพยาบาลเอกชนในกรุงเทพมหานคร

ข้อค้นพบ	แนวทางการปฏิบัติ
1) การควบคุมความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และเทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากการบริหารโครงการในโรงพยาบาลนั้นไม่มีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้นๆ เช่นโรงพยาบาลไม่ตระหนักถึงการจัดการอุปกรณ์ฮาร์ดแวร์ของระบบสารสนเทศที่ล้าสมัย รวมถึงไม่มีการบำรุงรักษาและแก้ไข เป็นเหตุทำให้เกิดข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์และซอพท์แวร์ในระหว่างการบริหารจัดการโครงการ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก, ค่าฐานนิยม เท่ากับ 4 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติ กรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรให้มีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการในการตระหนักถึงนโยบายการบำรุงรักษาของฮาร์ดแวร์ และข้อผิดพลาดทางเทคนิคของซอฟต์แวร์, ควรกำหนดรอบปรับเปลี่ยนระบบฮาร์ดแวร์ และซอฟต์แวร์ตามต้องการของระบบและผู้ใช้ ซึ่งถ้าไม่มีการบำรุงรักษาที่ดี ระบบคอมพิวเตอร์อาจจะทำให้ผลวินิจฉัยจากการใช้โปรแกรมทำงานผิดพลาดได้ ส่งผลกระทบต่อการรักษาคนไข้ • ผู้บริหารควรเล็งเห็นความสำคัญในการกำหนดนโยบายเพื่อพัฒนาและปรับปรุงความมั่นคงสารสนเทศ, กำหนดแผนการทำงานที่ชัดเจน เช่น ในรูปแบบ checklist และขั้นตอน ผู้ทำ ผู้ตรวจสอบ ระยะเวลาให้ชัดเจน และต้องมีการวัดผล • ควรให้ความสำคัญในเรื่องของความแม่นยำและความเป็นส่วนตัวมากเป็นพิเศษ เพราะถ้าข้อมูลมีความคลาดเคลื่อนจะส่งผลให้เกิดการรักษาที่ผิดพลาด และข้อมูลการรักษาพยาบาลเป็นข้อมูลส่วนตัวที่จะต้องไม่มีการรั่วไหล หรือเปิดเผยให้แก่บุคคลภายนอกโดยไม่ได้รับการยินยอม • ควรมีการแต่งตั้งหรือจัดหาคนที่มีความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และให้บุคคล นั้นมีส่วนร่วมในทุกกระบวนการของโครงการ

ข้อค้นพบ	แนวทางการปฏิบัติ
2) การควบคุมการจำกัดการติดตั้งซอฟต์แวร์ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากโรงพยาบาลไม่มีกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม อีกทั้งยังมีการใช้ระบบปฏิบัติการที่ไม่ได้รับการสนับสนุนจากผู้ให้บริการ จึงส่งผลให้มีภัยคุกคามจากไวรัสและซอฟส์แวร์ไม่พึงประสงค์ เป็นสาเหตุทำให้เกิดข้อผิดพลาดทางเทคนิคของซอฟต์แวร์รวมถึงฮาร์ดแวร์ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 5 หมายถึง สามารถนำไปปฏิบัติได้มากที่สุด ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 0.5 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• การจำกัดการติดตั้งซอฟต์แวร์ (ไพศาล ลักขณานุรักษ์, 2555) ควรมีการจัดตั้งนโยบายการควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User privilege) โดยกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการติดตั้งซอฟต์แวร์บนคอมพิวเตอร์ ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอโดยนโยบายนั้น สามารถบังคับใช้ได้อย่างเห็นผลและรัดกุม เพื่อป้องกันผลกระทบโดยรวมของระบบในโรงพยาบาล • ซอฟต์แวร์ที่ดีต้องสามารถกำหนดสิทธิ์ได้อย่างชัดเจน ไม่จำเป็นจะต้องกำหนดในเอกสารหรือเป็นลายลักษณ์อักษรเสมอไป ซึ่งอาจจะส่งผลต่อการทำงานที่ล่าช้า ควรปรับไปใช้ตามสภาพแวดล้อมและการใช้งานของแต่ละโรงพยาบาล • ควรจะมีการ software ป้องกันไวรัส (Anti-Virus) ติดตั้งทั้งในเครื่องที่จะต้องมีการรับข้อมูลจากภายนอก และเครื่องที่ไม่มีการรับข้อมูลจากภายนอก เช่น เครื่องมือแพทย์ที่เชื่อมต่อกับระบบภายใน และควรอบรมผู้ใช้งานคอมพิวเตอร์ในการป้องกันไวรัสและสิ่งคุกคามอื่นๆอีกด้วย

ข้อค้นพบ	แนวทางการปฏิบัติ
3) การควบคุมนโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ คุณภาพของบริการ, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากโรงพยาบาลไม่มีการกำหนดและตกลงกับผู้ให้บริการภายนอก และการจัดทำเป็นลายลักษณ์อักษร ที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กร ผู้ให้บริการเข้าถึงระบบสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กรโดยไม่ต้องได้รับอนุญาต ซึ่งเป็นสาเหตุทำให้เกิดภัยคุกคามในด้านคุณภาพการให้ที่ไม่น่าไว้วางใจ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 5 หมายถึง สามารถนำไปปฏิบัติได้มากที่สุด ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรมีการกำหนดและตกลงกับผู้ให้บริการภายนอก และจัดทำเป็นลายลักษณ์อักษร ในด้านความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงระบบสารสนเทศของโรงพยาบาลโดยผู้ให้บริการภายนอก ควรกำหนดแนวทางปฏิบัติให้ชัดเจนและมีสื่อสารกับพนักงานและหน่วยงานที่เกี่ยวข้อง • ควรมีการจำกัดพื้นที่ที่บุคคลภายนอกเข้าถึง เช่น หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงอย่างรัดกุมของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ ในส่วนของเจ้าหน้าที่และผู้ให้บริการภายนอก ต้องติดบัตรประจำตัวตลอดเวลาขณะ ปฏิบัติหน้าที่ในบริเวณโรงพยาบาล • การเชื่อมต่อระยะไกลจากผู้ให้บริการภายนอก ควรมีการกำหนดรหัสผ่านและการเข้าถึงข้อมูลไว้อย่างชัดเจน มีระบบระบุตัวตนและรหัสผ่านในการเข้าถึง (VPN) รวมถึงการกำหนดสิทธิการเข้าถึงระบบ • ระบบปฏิบัติการของโรงพยาบาลควรมีการเปิดใช้รหัสผ่าน (User Credential) ที่ให้ใช้ล็อคอิน เพื่อเป็นการยืนยันตัวตนก่อนที่จะเข้าถึงระบบสารสนเทศ ป้องกันไม่ให้ผู้ให้บริการภายนอกรวมถึงคนไข้เข้าถึงข้อมูลของโรงพยาบาล และควรพิจารณาถึงความมั่นคงปลอดภัยของระบบสารสนเทศที่มีการใช้งานผ่านเครือข่ายอินเทอร์เน็ต เช่น Proxy อีกด้วย

ข้อค้นพบ	แนวทางการปฏิบัติ
4) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากในข้อตกลงกับผู้ให้บริการภายนอก ไม่มีการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอกที่ให้บริการต่างๆภายในโรพยาบาล อีกทั้งไม่มีมีการดำเนินการตามวิธีปฏิบัติที่เหมาะสมเพื่อจัดการความเสี่ยงหรือผลกระทบที่มี หรือที่อาจจะเกิดขึ้น, มาตรการและแนวทางการจัดการตอบสนองต่อภัยคุกคามต่างๆ ทั้งภายในและภายนอกองค์กร โดยให้ครอบคลุมถึงการบริหารความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationship) ในการจัดการตามวงจร Supply Chain ที่มีส่วนเกี่ยวข้อง ตัวอย่างเช่นโรงพยาบาลและผู้ให้บริการไม่มีข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) มาใช้เป็นเครื่องมือในการพัฒนาระบบงานด้านบรอดแบนด์เครือข่ายความเร็วสูง เพื่อเชื่อมต่อกับฐานข้อมูลภายนอก เป็นสาเหตุทำให้เกิดเหตุการณ์โทรคมนาคมล่มบ่อยครั้ง ส่งผลให้มีโอกาสเกิดข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์และซอฟต์แวร์ เนื่องจากอุปกรณ์ทางเครือข่าย (Network) ไม่สามารถเชื่อมต่อกับระบบฐานข้อมูล อีกทั้งยังมีการใช้เทคโนโลยีล้าสมัย ซึ่งทำให้ไม่ได้รับการสนับสนุนจากผู้ให้บริการเท่าที่ควร (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ4 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรมีข้อตกลงกับผู้ให้บริการภายนอกโดยระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก, การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยการสร้างขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement), มีการระบุถึงแผนการรับมือในกรณีที่คลาดเคลื่อน หรือระบบล่มอันเนื่องมาจากผู้ให้บริการภายนอก มีการกำหนดข้อตกลง และการกำหนดการชดใช้ค่าเสียหาย และการจัดทำเอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมเพื่อให้มั่นใจ ได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศ • ควรมีการกำหนดและแนวปฏิบัติในการควบคุมดูแลสินค้าและบริการ ตลอด supply chain เพื่อให้เกิดในเรื่องของ integrity และ reliability ของข้อมูลระบบสารสนเทศทางการแพทย์ และที่สำคัญต้องตรวจสอบได้ว่าถ้ามีปัญหาเกิดขึ้นเกิดที่จุดไหนของ supply chain • ควรมีการอบรมให้ความรู้ความเข้าใจกับ user เพื่อให้ตระหนักเห็นความสำคัญและปฏิบัติตามอย่างเคร่งครัดและเป็นไปในแนวทางเดียวกัน

ข้อค้นพบ	แนวทางการปฏิบัติ
5) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากตัวบุคคลผู้ใช้งานระบบของโรงพยาบาลไม่ตระหนักต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรมีการสร้างความตระหนักและพัฒนาบุคลากรโดยการ ให้ความรู้ ฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงาน เช่น ควรมีการอบรมเรื่อง Privacy ของข้อมูลการรักษา รวมถึงการจัดสัมมนาเพื่อเผยแพร่นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงมีการซ้อมในสถานการณ์ต่างๆ หรือการทดสอบ (Demonstration) ในกรณีเสมือนเหตุการณ์จริงๆ เพื่อให้เกิดความเข้าใจ รวมถึงกำหนดหน้าที่รับผิดชอบการเข้าร่วมการอบรมในแต่ละครั้งอย่างชัดเจน และควรทำอย่างสม่ำเสมอ เพื่อให้มีความพร้อมในการรับมือกับปัญหาที่จะเกิดขึ้นได้จริง • ควรมีการกำหนดแนวทางปฏิบัติหากผู้ใช้งานสามารถประเมินหรือระบุได้แล้วว่าเกิดภัยคุกคามจะตัดสินใจทำอย่างไรต่อ และควรมีระบบที่คอยแจ้งเตือนหรือช่วยให้ผู้ใช้งานรับรู้ถึงความผิดปกติเพื่อที่จะประเมินและตัดสินใจต่อว่าจะทำอย่างไร • ควรมีการซักซ้อมในเรื่องความปลอดภัยในระยะเวลาที่กำหนด เช่นประจำปีเป็นต้น

ข้อค้นพบ	แนวทางการปฏิบัติ
6) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศไม่ได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร ซึ่งทำให้เกิดติดมัลแวร์หรือไวรัสภายในเครือข่าย เป็นสาเหตุของการเกิดข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์และซอฟต์แวร์ รวมถึงไม่ได้รับการสนับสนุนซอฟต์แวร์แอนติไวรัสเวอร์ชันที่ล้าสมัยจากเจ้าของผลิตภัณฑ์ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญค่อนข้างสอดคล้องกัน)	• โรงพยาบาลควรมีการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษร กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว และกำหนดให้มีระบบป้องกันผู้บุกรุก โดยดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก ระบบไฟร์วอลล์ และระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์(Malware) ประกอบด้วย ไวรัส โทรจัน รวมถึงสปายแวร์ • รายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศควรส่งไปยังหน่วยงานที่รับผิดชอบอย่างสม่ำเสมอ เพื่อทำการทบทวน และจัดทำ Business Continuity Plan อันเนื่องมาจากสาเหตุของภัยคุกคามต่างๆที่มีผลกระทบต่อระบบสารสนเทศ มีการอบรม สื่อสาร เพื่อเพิ่มความรู้ความเข้าใจให้กับผู้ใช้งานมากขึ้น • เมื่อตอบสนองหรือจัดการกับเหตุการณ์ที่เกิดขึ้นได้แล้ว ควรพิจารณากับการรับมือกับช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ หรือ ภัยคุกคามนั้นนั้นมีผลกระทบไปยังส่วนอื่นๆ ต่อหรือไม่ และกรณีที่จัดการได้ครบถ้วนแล้วก็ควรบันทึกสรุปเหตุการณ์ว่าเกิดขึ้นเพราะอะไร มีผลกระทบอย่างไร ดำเนินการแก้ไขอย่างไร เพื่อเป็นข้อมูลที่เอาไว้ใช้ในอนาคต

ข้อค้นพบ	แนวทางการปฏิบัติ
7) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล, ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ และ เทคโนโลยีล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจากอุปกรณ์ประมวลผลสารสนเทศไม่มีมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้ ผู้ใช้งานระบบไม่ตระหนักต่อความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ หรือการไม่ตรวจเช็คอุปกรณ์คอมพิวเตอร์หรือระบบปฏิบัติการให้ทันสมัย เช่น การทำงานของระบบคอมพิวเตอร์ ซึ่งบางครั้งทำให้เกิดข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• โรงพยาบาลควรมีการเตรียมอุปกรณ์ประมวลผลสารสนเทศอย่างเพียงพอต่อตามต้องการด้านสภาพการพร้อมใช้ที่กำหนดไว้, กำหนดอายุการใช้งาน และการบำรุงรักษาของอุปกรณ์คอมพิวเตอร์ ฮาร์ดแวร์, ซอฟต์แวร์ , ระบบปฏิบัติการ ระบบเครือข่าย เช่น Cloud Computing จะต้องไม่ออกแบบเครือข่ายในลักษณะที่ เกิดข้อผิดพลาดในจุดเดียว ส่งผลกระทบกับส่วนอื่นๆ ในวงกว้าง และต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศต่างๆ, ระบบสำรอง เช่น ระบบสำรองไฟในห้องผ่าตัดและจุดสำคัญต่างๆในโรงพยาบาล ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง (แผนประจำปี) หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ (กระทรวงสาธารณสุข, 2556)

ข้อค้นพบ	แนวทางการปฏิบัติ
8) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ เทคโนโลยีล้าสมัย ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ คุณภาพของบริการ และการโจมตีซอฟต์แวร์ จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจาก ไม่มีกฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบของโรงพยาบาล เนื่องจากมีการใช้เทคโนโลยีล้าสมัย และ คุณภาพของบริการ เช่นระบบไฟฟ้า, โทรคมนาคม เกิดขึ้นบ่อยครั้ง จึงทำให้ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ในช่วงการพัฒนาระบบของโรงพยาบาล (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1.5 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน	• ควรมีกฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบของโรงพยาบาล ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง และควรมีแผนสำรองในการรองรับกรณีเกิดเหตุการณ์ที่มีผลกระทบต่อระบบเกิดขึ้น • มีนโยบายให้ความสำคัญในการประยุกต์ใช้วงจรการพัฒนาระบบ (SDLC) สำหรับการวางแผนความปลอดภัย ประชาสัมพันธ์และให้ความรู้เกี่ยวกับ Secure Software Development Life Cycle ให้นักพัฒนาระบบทราบ ในขั้นตอนของการพัฒนาระบบสำหรับการสร้างระบบ และในขั้นตอนของการปฏิบัติงานสำหรับการพัฒนาซอฟต์แวร์ให้มีรูปแบบความปลอดภัย (เศรษฐพงศ์ มะลิสุวรรณ, 2552) เช่น ควรระบุรายละเอียดว่าต้องทำอะไร เช่น penetration testing, code review เป็นต้น • ควรมีการจัดหานิติบุคลที่มีความชำนาญในการให้คำปรึกษาในการลดความเสี่ยงที่จะเกิดขึ้นในซอฟต์แวร์ที่พัฒนาขึ้นในโรงพยาบาล

ข้อค้นพบ	แนวทางการปฏิบัติ
9) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย สำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล, ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ล้าสมัย จากการทบทวนวรรณกรรมส่วนมากสาเหตุเกิดจาก หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยไม่มีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ รวมถึงผู้พัฒนาระบบไม่ตระหนัก จึงทำให้เกิด ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์และฮาร์ดแวร์ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 4 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรมีการกำหนดหลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยขึ้นมาเป็นลายลักษณ์อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ เช่น ภาษาคอมพิวเตอร์มีความยืดหยุ่น มีส่วนประกอบพร้อมสำหรับการสร้างความสามารถในการเปลี่ยนแปลงรูปแบบตลอดเวลาที่ต้องการผลลัพธ์ รูปแบบโครงสร้างเป็นทางการคือ รูปแบบที่ใช้กำหนดลักษณะการรับข้อมูล เป็นสิ่งที่หลีกเลี่ยงยากบางครั้งในการพัฒนาโปรแกรมอาจจะใช้ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ, ผู้พัฒนาโปรแกรมใช้ระบบรักษาความปลอดภัยของข้อมูล (SSL) ในการที่จะส่งข้อมูลที่ละเอียดอ่อนรวมถึงหมายเลขบัตรเครดิต เช่น ควรคำนึงถึงความปลอดภัยของข้อมูลด้านการเงินของโรงพยาบาล, ข้อมูลประกันสุขภาพกับบริษัทประกันภัย และข้อมูลส่วนบุคคลอื่นๆ, ควรนำระบบงานที่สำคัญไปอยู่หลัง Firewall, ปิดช่องโหว่ของระบบให้เหลือน้อยที่สุด หรือการออกแบบด้านความปลอดภัยต้องให้ง่ายสำหรับการทำความเข้าใจ (เศรษฐพงศ์ มะลิสุวรรณ, 2552)

ข้อค้นพบ	แนวทางการปฏิบัติ
10) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล, เทคโนโลยีล้าสมัย และคุณภาพของบริการ จากการทบทวนวรรณกรรม ส่วนมากสาเหตุเกิดจากหลักการโรงพยาบาลไม่มีการจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 5 หมายถึง สามารถนำไปปฏิบัติได้มากที่สุด ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• ควรมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ เช่น การควบคุมการเข้าออก กำหนดบริเวณสำหรับการเข้าถึงชั้นความลับของข้อมูลต่างๆ หรือบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยของการพัฒนาระบบ และมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานเพื่อหลีกเลี่ยงความไม่สมบูรณ์ในการพัฒนาระบบที่อาจจะมีผลกระทบต่อโครงสร้างของระบบ เช่น ระบบสำรองกระแสไฟฟ้า (UPS), เครื่องกำเนิดกระแสไฟฟ้าสารอง (Generator), ระบบควบคุมอากาศ และควบคุมความชื้น (กระทรวงสาธารณสุข. 2556) ควรมีการทดสอบระบบก่อนใช้งานจริง เช่น มีการคำนวณจำนวนชั่วโมงของการสำรองไฟ ให้ตอบโจทย์การทำงานให้มากที่สุดตามความเหมาะสม ไม่มากไม่น้อยจนเกินไป และมีการบำรุงดูแลรบบอย่างต่อเนื่อง

ข้อค้นพบ	แนวทางการปฏิบัติ
11) การทดสอบด้านความมั่นคงปลอดภัยของระบบ จากการสำรวจพบว่าภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล เทคโนโลยีล้าสมัย และข้อผิดพลาดทางเทคนิคของซอฟต์แวร์จากการทบทวนวรรณกรรม ส่วนมากสาเหตุเกิดจากไม่มีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา (ค่ามัธยฐานของการประเมินค่า (Rating Scale) จากผู้เชี่ยวชาญทั้ง 17 ท่าน เท่ากับ 4 หมายถึง สามารถนำไปปฏิบัติได้มาก ค่าฐานนิยม เท่ากับ 5 และค่าพิสัยระหว่างควอไทล์หรือค่า IR (Interquartile Range) เท่ากับ 1 ค่าสถิติกรณีเท่ากับ 1 แสดงว่าความคิดเห็นที่ได้จากกลุ่มผู้เชี่ยวชาญสอดคล้องกัน)	• การทดสอบด้านความมั่นคงปลอดภัยของระบบ แผนแนวทางปฏิบัติ มีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา และการทดสอบด้านความมั่นคงปลอดภัยต้องทำการทดสอบการใช้งานในช่วงของการพัฒนา หากไม่ผ่านการทดสอบต้องแก้ไขให้แล้วเสร็จก่อนการส่งมอบ (สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์. 2558) และมีการทดสอบระบบก่อนการใช้งานจริง เพื่อให้ได้ผลลัพธ์ตามความต้องการหากมีข้อผิดพลาดสามารถแก้ไขได้ตรงจุดโดยไม่กระทบกับผู้ใช้บริการ • ควรมีการอบรมให้ความรู้นักพัฒนาระบบและสร้างความตระหนักเน้นย้ำในการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบซึ่งถูกละเลยในบางครั้งให้มากขึ้น • ต้องคำนึงถึงการทดสอบในสภาพแวดล้อมที่สมจริง มีการทดสอบที่ครอบคลุม โดยต้องมั่นใจว่าข้อมูลหรือฟังก์ชันการทำงานของระบบต้องมีความปลอดภัย ไม่มีช่องโหว่ โดยสิ่งที่ต้องให้ความสนใจในการทดสอบด้านนี้ คือ confidentiality, integrity, authentication, availability, authorization and non-repudiation ประเด็นเหล่านี้ต้องได้รับการยอมรับ

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ในการศึกษาวิจัยครั้งต่อไปควรศึกษางานแต่ละหน่วยงานในโรงพยาบาลให้ครอบคลุมทุกโรงพยาบาล เช่นโรงพยาบาลรัฐในกรุงเทพมหานคร หรือ โรงพยาบาลเอกชนในจังหวัดอื่นๆ โดยอาจจะศึกษาจากตัวแปรอื่นๆ หรือ การนำแนวทางปฏิบัติที่กล่าวมาไปประยุกต์ในโรงพยาบาล หรือหน่วยงานต่างๆ ในการประสิทธิภาพในการควบคุมภัยคุกคามของระบบสารสนเทศก่อนและหลังนำแนวทางไปประยุกต์ใช้

กิตติกรรมประกาศ

งานวิจัยฉบับนี้สำเร็จลงได้ด้วยดี เนื่องจากได้รับความกรุณาอย่างสูงจาก ผศ. ดร.โกวิท รพีพิศาล อาจารย์ที่ปรึกษางานวิจัย ที่กรุณาให้คำแนะนำปรึกษาตลอดจนปรับปรุงแก้ไขข้อบกพร่องต่างๆ ด้วยความเอาใจใส่อย่างดียิ่ง ผศ. ดร.วศิณ ชูประยูร ผู้อำนวยการหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ และ ดร.วรทรรศน์ มาฆะศิรานนท์ อาจารย์วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับการเป็นกรรมการสอบการค้นคว้าอิสระ ขอขอบพระคุณ ดร.สุทธิศักดิ์ จันทวงษ์โส (อาจารย์วิทยาลัยเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยรังสิต), นพ.วิจารณ์ เทวธารานันท์ (แพทย์สาขาอายุรศาสตร์ โรงพยาบาล สมิติเวช ธนบุรี) และคุณประสิทธิ์ ผาตี (ผู้ช่วยผู้จัดการ แผนกคอมพิวเตอร์ โรงพยาบาล จักษุรัตนิน) ซึ่งเป็นผู้ทรงคุณวุฒิที่ให้ความอนุเคราะห์ตรวจสอบคุณภาพเครื่องมือวิจัย และผู้เชี่ยวชาญเฉพาะทางทั้ง 17 ท่านในการแสดงความคิดเห็นสำหรับแนวทางในการควบคุมความปลอดภัยของระบบสารสนเทศในโรงพยาบาล

บรรณานุกรม

กระทรวงสาธารณสุข. (2556). แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข.สืบค้นจาก http://old.ddc.moph.go.th/cdc/edoc/file_itc/ policies_it_2556.pdf

เฉลิม สุวรรณะ. (2554). การรักษาความมั่นคงปลอดภัยสารสนเทศกรณีศึกษา ศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี (สารนิพนธ์วิทยาศาสตรมหาบัณฑิต). กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร

ไพศาล ลักขณานุรักษ์. (2557). คู่มือการจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล สืบค้นจาก http://www.dgr.go.th/isdgr/file/it/risk_it.pdf

ศราวุฒิ จันทะคัด. (2554). การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา: บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด (สารนิพนธ์วิทยาศาสตรมหาบัณฑิต). กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร

เศรษฐพงค์ มะลิสุวรรณ. (2557). ภัยคุกคามความมั่นคงระบบสารสนเทศ.สืบค้นจาก http://www.pi.ac.th/ /includes/download.php?id=1808

Forbes. Hacking Hospitals And Holding Hostages: Cybersecurity In 2016. (2016). From https:// //www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages- cybersecurity-in-2016/#4a31e4b67d59

International Organization for Standardization. (2014). About ISO. from http://www.iso.org/iso/home/about.html

University of South Carolina Board of Trustees. (2014). Information Technology Security. from https://www.uts.sc.edu/itsecurity/threats.shtml