หัวข้อการค้นคว้าอิสระ	การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษา องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย Development of Information Technology Security policy by Applying ISO/IEC 27001 relate to Computer Crime Act 2551 A case study of Thai Public Broadcasting Service (ThaiPBS)
ชื่อผู้เขียน	นางสาววิภาวรรณ คุ้มศิริ Miss Wipawan Kumsiri
แผนกวิชา/คณะ	สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ดร. กมล เกียรติเรืองกมลา
ปีการศึกษา	2551

บทสรุป

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อต้องการ ลดความเสี่ยงต่างๆ ที่เกิดขึ้นกับระบบสารสนเทศภายในองค์การฯ โดยการใช้มาตรฐาน ISO/IEC27001 เป็นแนวทางปฏิบัติ ซึ่งผู้วิจัยได้ทำการศึกษาจากการสุ่มตัวอย่างโดยการใช้สูตร *Taro Yamane* คำนวณจากกลุ่มประชากรทั้งหมด 750 คน ซึ่งเป็นพนักงานภายในองค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศ โดยมีเครื่องมือที่ใช้ในการวิจัยอยู่ 2 แบบ คือ

แบบที่ 1 : แบบสอบถาม สำรวจระดับความเสี่ยงที่เกิดขึ้นภายในองค์การฯ

แบบที่ 2 : แบบสัมภาษณ์ เชิงนโยบาย ใช้สำหรับสำรวจการดำเนินงานตามมาตรฐาน ISO/IEC27001

ผลการศึกษาพบว่าจากการสำรวจการดำเนินงาน ตามมาตรฐาน ISO/IEC 27001 ทั้ง 11 หมวด พบว่า องค์การฯ ได้ดำเนินการตามมาตรฐาน ISO/IEC27001 แล้วเสร็จ คิดเป็นร้อยละ 33.84 และกำลังดำเนินการคิดเป็นร้อยละ 10.53 และอีกร้อยละ 55.63 ที่องค์การฯ ยังไม่เริ่มดำเนินการ

และจากเหตุการณ์ความเสี่ยงที่เกิดขึ้นภายในองค์การฯ ทั้ง 25 เหตุการณ์ โดยทั้ง 25 เหตุการณ์จะถูกจัดแบ่งความเสี่ยง 3 ด้าน คือ ด้านที่ 1 : ด้าน Confidentiality - สิทธิในการเข้าถึงข้อมูลต่างๆ , ด้านที่ 2 : ด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล ,ด้านที่ 3 : ด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ

ผู้วิจัยได้นำค่าที่ได้จากการสำรวจมาคำนวณตามสูตรการประเมินความเสี่ยง

ระดับความเสี่ยง (R) = โอกาสเกิดภัยคุกคาม (L) x ความรุนแรงของผลกระทบ (I)

และเมื่อได้ระดับความเสี่ยงแล้ว ได้นำค่าไปเปรียบเทียบ ในตารางเมตริกซ์ 5 x 5 โดยมีการจัดระดับค่าความเสี่ยงดังนี้

> 48.00 ความเสี่ยงสูง

= 16.01 – 48.00 ความเสี่ยงปานกลาง

$\leq$ 16.00 ความเสี่ยงต่ำ

และจากค่าที่ได้ จะพบว่าในปัจจุบันองค์การฯ จะมีเหตุการณ์ความเสี่ยงสูงจำนวน 12 เหตุการณ์ ความเสี่ยงปานกลางจำนวน 8 เหตุการณ์ ความเสี่ยงต่ำจำนวน 5 เหตุการณ์ โดยมีรายละเอียดดังนี้

ลำดับ	เหตุการณ์ความเสี่ยง	ระดับความเสี่ยง	ประเภท
1	การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	สูง (78.45)	Confidentiality
2	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้	สูง (68.21)	Integrity
3	การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง	สูง (63.36)	Integrity
4	การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ	สูง (59.62)	Integrity

ลำดับ	เหตุการณ์ความเสี่ยง	ระดับความเสี่ยง	ประเภท
5	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน	สูง (58.61)	Confidentiality
6	การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้	สูง (54.54)	Availability
7	การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง	สูง (51.78)	Confidentiality
8	ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และ ซอฟต์แวร์ทำงานผิดพลาด	สูง (51.49)	Integrity
9	การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง	สูง (50.30)	Confidentiality
10	ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ	สูง (50.71)	Availability
11	การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูล	สูง (50.30)	Integrity
12	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	สูง (49.90)	Confidentiality
13	การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม	ปานกลาง (36.86)	Confidentiality
14	การติดตั้งฮาร์ดแวร์,ซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง	ปานกลาง (33.18)	Availability
15	มีการแก้ไขโปรแกรมประยุกต์ (Application) ไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ	ปานกลาง (30.09)	Integrity
16	การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง	ปานกลาง (29.86)	Confidentiality
17	ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย	ปานกลาง (28.60)	Integrity
18	การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป	ปานกลาง (23.14)	Availability
19	พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม	ปานกลาง (21.69)	Availability

ลำดับ	เหตุการณ์ความเสี่ยง	ระดับความเสี่ยง	ประเภท
20	การเกิดความผิดพลาดในการรายงานผลข้อมูล	ปานกลาง (21.15)	Integrity
21	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	ต่ำ (15.72)	Availability
22	งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ	ต่ำ (14.86)	Availability
23	ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย	ต่ำ (14.14)	Availability
24	การเข้าใช้ข้อมูลสำคัญโดยปราศจากการควบคุม	ต่ำ (12.34)	Confidentiality
25	กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ	ต่ำ (7.20)	Integrity

ดังนั้น ทางผู้วิจัย จึงได้ทำการวางมาตรการเพื่อลดความเสี่ยงที่เกิดขึ้น โดยได้วางแผนไว้เป็น 3 ระยะคือ ระยะที่ 1 มาตรการในการลดความเสี่ยงสูง , ระยะที่ 2 มาตรการในการลดความเสี่ยงปานกลาง , ระยะที่ 3 มาตรการในการลดความเสี่ยงต่ำ

โดยในมาตรการผู้วิจัยจะใช้ มาตรฐาน ISO/IEC27001 เพื่อเป็นแนวทางทางในการลดความเสี่ยงเพื่อให้ได้ประสิทธิภาพมากยิ่งขึ้น และในการวางมาตรการในแต่ละระยะผู้วิจัย จะทำการวางมาตรารออกเป็น 2 ส่วน คือ ส่วนที่ 1 สำหรับพนักงานทั่วไป และส่วนที่ 2 สำหรับเจ้าหน้าที่เทคโนโลยีสารสนเทศ

มาตรการในการลดความเสี่ยงในระยะที่ 1 จะมีการออกนโยบาย รายละเอียดดังนี้

ส่วนที่ 1 นโยบายทางด้านความมั่นคงปลอดภัยของสารสนเทศ สำหรับพนักงานทั่วไป

1. องค์การ ไม่สนับสนุน หรือยินยอมให้พนักงานขององค์การ กระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง
   1.1) ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์การ หรือบุคคลอื่นๆ
   1.2) ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
   1.3) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง
2. องค์การ จะจัดให้มีชื่อผู้ใช้ (USER ID) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับ อินเทอร์เน็ต เป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่าน ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม ซึ่กฎการใช้รหัสผ่านมีดังนี้

2.1) ความยาวของตัวอักษรต้องไม่น้อยกว่า 6 ตัวอักษร

2.2) ผู้ใช้งานต้องมีการเปลี่ยน รหัสผ่าน (Password) ในการเข้าใช้ระบบทุก 1 เดือน และหากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอเลิกใช้ โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน

3. องค์การ ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน

4. ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช้ขององค์การ ในการเชื่อมต่อเข้ากับเครือข่ายขององค์การ

5. ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายขององค์การ ได้แก่ การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับโดยจดหมายอิเล็กทรอนิกส์ยกเว้นได้รับการเข้ารหัสโดยได้รับการยืนยันจากหน่วยงาน คอมพิวเตอร์

6. ไม่อนุญาตให้พนักงานใช้ e-mail อื่นใดที่องค์การ ไม่ได้กำหนดให้ใช้

7. ในกรณีการขอใช้อีเมล์ของรายการต่างๆ ขององค์การ ถ้าผู้ดูแลรายการมีความประสงค์ต้องการใช้อีเมล์รายการโต้ตอบกับผู้ชม ผู้ดูแลรายการนั้นจะต้องเซ็นหนังสือยินยอมเป็นผู้รับผิดชอบของอีเมล์ของรายการนั้น และถ้าในกรณีที่ผู้ดูแลรายการเป็นบุคคลภายนอกจะต้องมีพนักงานขององค์การ เซ็นกำกับในหนังสือยินยอมเป็นผู้รับผิดชอบของอีเมล์ของรายการนั้นด้วย

8. การเข้าใช้งาน application ต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบโดยให้ผู้บังคับบัญชาโดยตรงเป็นผู้ขอสิทธิในการใช้

9. ห้ามพนักงานนำ โปรแกรม หรือ Application ใดๆมาติดตั้งบนเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ องค์การ โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์และผู้บังคับบัญชาโดยตรง

10. ห้ามพนักงานใช้ โปรแกรม หรือ Application ที่ไม่ถูกลิขสิทธิ์

11. หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือผิดต่อกฎระเบียบขององค์การฯ ให้แจ้งต่อผู้บังคับบัญชาโดยตรงหรือเจ้าหน้าที่หน่วยงานคอมพิวเตอร์

12. ถ้าพนักงานท่านได้ไม่ปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ พนักงานท่านนั้นต้องได้รับบทลงโทษ ตามผู้บังคับบัญชาเห็นสมควร

ส่วนที่ 2 นโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ สำหรับฝ่ายสารสนเทศ

เพื่อใช้เป็นแนวทางในการเข้าใช้ระบบสารสนเทศ เพื่อช่วยลดความเสี่ยง และเพิ่มความมั่นคงปลอดภัยให้กับระบบสารสนเทศภายในองค์การ มีรายละเอียดดังต่อไปนี้

1. ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจัดอบรมให้ความรู้ทางด้านเทคโนโลยีสารสนเทศ รวมถึงปฏิบัติในการเข้าใช้ระบบสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย เดือนละ 1 ครั้ง
2. ฝ่ายเทคโนโลยีสารสนเทศต้องมีการประชาสัมพันธ์ ให้กับผู้ใช้งานทราบถึงนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้ผู้ใช้งานเข้าใช้ และตระหนักถึงความสำคัญในการปฏิบัติ เพื่อความมั่นคงปลอดภัยของข้อมูล
3. ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการอัพเดท ระบบป้องกันไวรัสให้ทันสมัยอยู่เสมอ
4. ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการแจ้ง หรือสรุป สิทธิการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์การ ให้แก่ผู้ใช้งานทราบทุก 6 เดือน
5. ฝ่ายเทคโนโลยีสารสนเทศ ควรมีการถอดสิทธิการเข้าใช้งานแก่ผู้ใช้งานทันที ที่ผู้ใช้งานท่านนั้นพ้นสภาพการเป็นพนักงานขององค์การ
6. ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดอบรมความรู้เกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้กับพนักงานทุกท่าน รวมถึงพนักงานที่เข้ามาใหม่ด้วย และมีการประสัมพันธ์ให้พนักงานทุกท่านตระหนักถึงความสำคัญของการปฏิบัติตามกฎหมาย
7. ในการบำรุงรักษาระบบ ควรกระทำ เมื่อที่ไม่มีการเรียกใช้งานจากผู้ใช้ หรือถ้าไม่สามารถกระทำได้ ควรจะแจ้งเป็นลายลักษณ์อักษรให้ผู้ใช้งานทราบล่วงหน้า 3 วันทำการ
8. ผู้ดูแลระบบฐานข้อมูล ต้องทำการสำรองข้อมูลของแต่ละระบบทุกวัน
9. ผู้ดูแลระบบฐานข้อมูล ต้องทำการทดสอบข้อมูลที่สำรองไว้ทุกๆ 1 เดือน เพื่อตรวจสอบว่าข้อมูลที่ได้สำรองครบถ้วน และสามารถนำกลับมาใช้ใหม่ได้
10. ในการดำเนินการแก้ไขระบบ จะต้องมีการบันทึกวันและเวลาที่ดำเนินการแก้ไข สาเหตุ วิธีการแก้ไข และรายชื่อผู้ดำเนินการแก้ไขไว้เป็นลายลักษณ์อักษรทุกครั้ง

มาตรการในการลดความเสี่ยงในระยะที่ 2 จะมีการออกนโยบายเพิ่มเติมซึ่งในระยะนี้จะเพิ่มเติมเฉพาะในส่วนที่ 2 สำหรับเจ้าหน้าที่สารสนเทศเท่านั้น โดยมีรายละเอียดดังนี้

11. จะต้องมีการจัดทำคู่มือในการติดตั้งฮาร์ดแวร์ หรือ ซอฟต์แวร์ ที่เป็นลายลักษณ์อักษร และต้องมีการปรับปรุงคู่มือให้ทันสมัยอยู่เสมอและในการดำเนินงานต้องดำเนินโดยผู้เชี่ยวชาญเท่านั้น
12. เจ้าหน้าที่สารสนเทศ จะต้องมีการบันทึกผลการตรวจสอบข้อมูลตั้งแต่ ก่อน ระหว่าง และหลังการประมวลผล
13. หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ ต้องมีการกำหนดคุณสมบัติของเจ้าหน้าที่สารสนเทศและดำเนินการทดสอบคุณสมบัติในการคัดเลือกพนักงาน ให้ตรงกับลักษณะงานที่ต้องการ
14. เจ้าหน้าที่สารสนเทศต้องได้รับการอบรม เกี่ยวกับความรู้ทางด้านความชำนาญตามสายงาน ปีละ 2 ครั้ง

มาตรการในการลดความเสี่ยงในระยะที่ 3 จะมีการออกนโยบายเพิ่มเติม โดยมีรายละเอียดดังนี้

เพิ่มเติมในส่วนที่ 1 : สำหรับพนักงานทั่วไป มีรายละเอียดดังนี้ คือ

13. ผู้ที่ต้องการเข้าใช้ระบบเครือข่ายภายในองค์การฯ จะต้องกรอกแบบฟอร์มที่ทางฝ่ายเทคโนโลยีสารสนเทศจัดทำขึ้น และต้องได้รับการอนุมัติการผู้บังคับบัญชาเท่านั้น

เพิ่มเติมในส่วนที่ 2 : สำหรับเจ้าหน้าที่สารสนเทศ มีรายละเอียดดังนี้ คือ

15. ต้องมีการรายงานผลการปฏิบัติงาน สรุปปัญหา และผลกระทบของปัญหาที่เกิดขึ้นให้กับผู้บังคับบัญชา ทราบทุก 1 เดือน
16. เจ้าหน้าที่สารสนเทศต้องมีการตรวจการใช้งานอุปกรณ์ทางด้านระบบเครือข่ายทุก 1 เดือน
17. ต้องมีการวางแผนและตรวจสอบการใช้ทรัพยากรของระบบ ทุก 1 เดือน