บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

สรุปผลการวิจัย

จากการศึกษาเพื่อจัดทำรายงานวิจัย เรื่อง การสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูลโดยการประยุกต์ใช้ ISO 17799 กรณีศึกษาของบริษัทให้บริการด้านการจัดซื้อออนไลน์ นั้นเป็นการศึกษา เพื่อนำเสนอความเสี่ยงในด้านต่างๆที่อาจเกิดขึ้น และหาแนวทางการประยุกต์มาตรฐานรักษาความปลอดภัยของข้อมูล ISO 17799 ที่เหมาะสม มาใช้ โดยเป็นการนำเสนอแก่ผู้บริหารองค์กร ให้เห็นถึงความเสี่ยงที่อาจเกิดขึ้นถ้าไม่มีการบริหารหรือการควบคุมความเสี่ยง และภัยคุกคามต่างๆก่อน

จากศึกษาและผลการสำรวจความเสี่ยงในเหตุการณ์ต่างๆนั้น สามารถเรียงตามความเสี่ยงและประเภทของความเสี่ยงทั้ง 3 ประเภท คือ สิทธิในการเข้าถึงข้อมูล(Confidentiality) ความถูกต้องและสมบูรณ์ของข้อมูล (Integrity) และการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน (Availability) ดังตารางที่ 5.1

ตารางที่ 5.1
ลำดับเหตุการณ์ความเสี่ยงทั้งหมดขององค์กร

ลำดับที่	เหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ	ระดับความเสี่ยง	ประเภทของความเสี่ยง
1	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด	56.04 สูง	Confidentiality
2	การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้	55.09 สูง	Availability
3	การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล	54.51 สูง	Confidentiality
4	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	50.85 สูง	Confidentiality

ตารางที่ 5.1 (ต่อ)

ลำดับเหตุการณ์ความเสี่ยงทั้งหมดขององค์กร

ลำดับที่	เหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ	ระดับความเสี่ยง	ประเภทของความเสี่ยง
5	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้	50.73 สูง	Availability
6	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	50.36 สูง	Availability
7	ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน (corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด	49.27 สูง	Integrity
8	มีการแก้ไขโปรแกรมประยุกต์(Application)อย่างไม่ถูกต้อง	46.18 ปานกลาง	Integrity
9	การเกิดความผิดพลาดในการรายงานข้อมูล	46.09 ปานกลาง	Integrity
10	การเข้าถึงข้อมูลจากผู้ที่ไม่สิทธิใช้งานจริง	45.34 ปานกลาง	Confidentiality
11	การเข้าใช้ข้อมูลสำรอง (Back up) โดยปราศจากการควบคุม	45.20 ปานกลาง	Confidentiality
12	การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (application) ระบบ(system) หรือ ซอฟแวร์ (Software)ที่มีการแก้ไขเปลี่ยนแปลง	45.18 ปานกลาง	Integrity
13	การดูแลรักษา(maintenance)ระบบ ทำให้ระบบไม่สามารถใช้งานได้	45.09 ปานกลาง	Availability
14	ข้อมูลที่เก็บสำรอง (Back up)ไม่เพียงพอ	44.91 ปานกลาง	Availability
15	การขาดการพัฒนา หรือปรับปรุง ระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานให้ทันสมัย	44.45 ปานกลาง	Integrity

ตารางที่ 5.1 (ต่อ)

ลำดับเหตุการณ์ความเสี่ยงทั้งหมดขององค์กร

ลำดับที่	เหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ	ระดับความเสี่ยง	ประเภทของความเสี่ยง
16	การรักษารหัสผ่าน (Password) ของส่วนบุคคลอย่างไม่เหมาะสม	43.45 ปานกลาง	Confidentiality
17	งบประมาณในการสำรอง (Back up) ข้อมูลไม่เพียงพอ	42.45 ปานกลาง	Availability
18	ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย	42.45 ปานกลาง	Availability
19	ข้อมูลภายในองค์กรขาดการพัฒนาหรืออัพเดท (Update)ให้ทันสมัย	42.00 ปานกลาง	Integrity
20	การขาดกระบวนการภายในเพื่อจัดการ,สร้าง,และควบคุมข้อมูลภายในองค์กร	41.64 ปานกลาง	Integrity
21	พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม	39.64 ปานกลาง	Availability
22	การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง	38.21 ปานกลาง	Confidentiality
23	การออกแบบระบบซับซ้อนเกินไป	37.45 ปานกลาง	Availability
24	การระบุชื่อข้อมูลที่สร้างขึ้นไม่ถูกต้อง	35.72 ปานกลาง	Confidentiality
25	กระบวนการควบคุมต่างๆมีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่ให้ความใส่ใจ	35.36 ปานกลาง	Integrity
26	การติดตั้งฮาร์ดแวร์หรือซอฟแวร์ไม่ถูกต้อง	32.64 ปานกลาง	Availability

โดยงานวิจัยฉบับนี้ได้นำเสนอแนวทางการควบคุมเฉพาะความเสี่ยงสูงทั้ง 7 เหตุการณ์ เนื่องจากความเสี่ยงสูงจัดเป็นภัยคุกคามที่องค์กรต้องให้ความสนใจ ในการดูแล และจัดหาตัวควบคุม (Control) ที่เหมาะสมก่อน เพื่อลดความเสี่ยงของภัยคุกคามดังกล่าว

และจากการนำเสนอแนวทางการควบคุมความเสี่ยงทั้ง 7 เพื่อองค์กรตัวอย่างนำไปปรับใช้ให้เหมาะสมนั้น บางกรณีที่บางข้อเสนอ องค์กรได้เริ่มดำเนินการไปบ้างแล้ว แต่ผลจากการประเมินของพนักงานที่มีส่วนเกี่ยวข้องยังจัดให้ความเสี่ยงดังกล่าวเป็นความเสี่ยงสูงอยู่นั้น อาจมีสาเหตุจาก

- พนักงานผู้ตอบแบบสอบถาม มีการรับรู้ข้อมูลข่าวสารด้านความปลอดภัยที่แตกต่างกัน
- พนักงานผู้ตอบแบบสอบถามไม่เข้าใจความหมายของคำถามอย่างลึกซึ้ง
- องค์กรเลือกตัวควบคุม (Control) ความเสี่ยงที่ไม่เหมาะสม หรือขาดการดำเนินงานที่จริงจัง เป็นต้น

และจากการทดสอบสมมติฐาน เพื่อนำไปประยุกต์ใช้ในการสร้างมาตรฐานการรักษาความปลอดภัยตาม ISO 17799 ให้เหมาะสมในแต่ละกลุ่มตัวอย่าง จึงต้องมีการทดสอบสมมติฐานขึ้นมา โดยจากการทดสอบสมมติฐานแล้วพบว่าตัวแปรอิสระที่นำมาใช้ทดสอบสมมติฐาน คือ ช่วงอายุการทำงานของพนักงานที่ตอบแบบสอบถามและหน่วยงานที่เป็น IT กับหน่วยงานที่เป็น Non-IT เทียบกับตัวแปรตามคือ มาตรฐานความปลอดมั่นคงปลอดภัยตาม ISO17799 ทั้ง 11 ข้อ พบว่า ตัวแปรอิสระที่นำมามีความคิดเห็นที่แตกต่างในแต่ละข้อของมาตรฐาน ISO 17799 ดังต่อไปนี้ตามตารางที่ 5.2

ตารางที่ 5.2

ผลการทดสอบความแตกต่างด้านความคิด ในแต่ละหัวข้อตามมาตรฐาน ISO 17799

หมายเหตุ Yes = แสดงว่ามีความคิดเห็นแตกต่างกัน, No = แสดงว่ามีความคิดเห็นไม่แตกต่างกัน

มาตรฐานการรักษาความปลอดภัย	ผลการทดสอบสมมติฐาน (ตามตัวแปรอิสระ)	
	ช่วงอายุการทำงาน	หน่วยงานทาง IT และ Non-IT
การทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร	Yes	No
การทราบรายละเอียดของนโยบาย	Yes	No
การทราบแหล่งที่สามารถเข้าไปอ่านนโยบาย	Yes	No
การทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศ	Yes	No
การรักษาและไม่เปิดเผยความลับขององค์กร	Yes	No
มาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร	Yes	Yes
การทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ	Yes	Yes
การแบ่งประเภทของข้อมูล	No	No
ความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ขององค์กร	No	Yes
การได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ	No	No
การทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร	No	No
ความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญ	No	No
การระวังและป้องกันอุปกรณ์จากอุบัติเหตุ	Yes	No

ตารางที่ 5.2(ต่อ)

ผลการทดสอบความแตกต่างด้านความคิด ในแต่ละหัวข้อตามมาตรฐาน ISO 17799

หมายเหตุ Yes = แสดงว่ามีความคิดเห็นแตกต่างกัน, No = แสดงว่ามีความคิดเห็นไม่แตกต่างกัน

มาตรฐานการรักษาความปลอดภัย	ผลการทดสอบสมมติฐาน (ตามตัวแปรอิสระ)	
	ช่วงอายุการทำงาน	หน่วยงานทาง IT และ Non-IT
ความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัย	Yes	No
การป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงาน	No	No
การปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงานตามระยะเวลา	No	Yes
ความเหมาะสมของการบริหารจัดการเครือข่าย,ดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์(Application)ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย	No	No
การจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ	Yes	No
การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆ ออกไปนอกองค์กร	Yes	No
การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร	No	No
การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร	Yes	No
การตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT	No	No
การทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร	Yes	No
การแจ้งหรือสรุป สิทธิการใช้งานระบบและโปรแกรมให้ทราบตามระยะที่เหมาะสม	No	Yes
การให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน	Yes	Yes
มาตรฐานระบบบริหารจัดการรหัสผ่าน	Yes	Yes

ตารางที่ 5.2(ต่อ)

ผลการทดสอบความแตกต่างด้านความคิด ในแต่ละหัวข้อตามมาตรฐาน ISO 17799

หมายเหตุ Yes = แสดงว่ามีความคิดเห็นแตกต่างกัน, No = แสดงว่ามีความคิดเห็นไม่แตกต่างกัน

มาตรฐานการรักษาความปลอดภัย	ผลการทดสอบสมมติฐาน (ตามตัวแปรอิสระ)	
	ช่วงอายุการทำงาน	หน่วยงานทาง IT และ Non-IT
การให้ความสำคัญกับการ Lock Off หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน	Yes	Yes
การให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมขององค์กร	Yes	No
การทราบกฎระเบียบและสิทธิของการลงโปรแกรมที่ไม่ใช่โปรแกรมพื้นฐาน	No	No
การตรวจสอบอุปกรณ์พ่วงต่อพกพา ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร	No	Yes
ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล	No	No
ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อน	No	No
ความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร	No	No
การแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ	No	Yes
การรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร	No	No
การเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี	No	No
การลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร	No	No
ความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร	Yes	No

ตารางที่ 5.2(ต่อ)

ผลการทดสอบความแตกต่างด้านความคิด ในแต่ละหัวข้อตามมาตรฐาน ISO 17799

หมายเหตุ Yes = แสดงว่ามีความคิดเห็นแตกต่างกัน, No = แสดงว่ามีความคิดเห็นไม่แตกต่างกัน

มาตรฐานการรักษาความปลอดภัย	ผลการทดสอบสมมติฐาน (ตามตัวแปรอิสระ)	
	ช่วงอายุการทำงาน	หน่วยงานทาง IT และ Non-IT
การกำกับ ดูแล และควบคุมการปฏิบัติงานตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร	Yes	No

ซึ่งผลจากการตารางนี้ผู้บริหารองค์กรสามารถนำไปใช้สำหรับการให้ความสนใจเป็นรายกลุ่มที่มีความคิดเห็นแตกต่างออกไป เช่น ความคิดเห็นด้านการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร ถ้ามองตามช่วงอายุการทำงาน พบว่ามีความคิดเห็นแตกต่างแต่ถ้ามองตามตัวแปรด้านหน่วยงานพบว่าไม่แตกต่างกัน

แสดงว่า ช่วงอายุงานของพนักงานมีการรับรู้การจัดทำนโยบายด้านเทคโนโลยีสารสนเทศขององค์กรที่ไม่เท่ากัน ซึ่งอาจเกิดจากประสบการณ์หรือระยะเวลาในการทำงานในองค์กร จึงทำให้การรับรู้ในแต่ละช่วงไม่เท่ากัน ดังนั้นองค์กรควรเพิ่มการประชาสัมพันธ์ด้านนโยบาย และให้ข้อมูลที่แตกต่างกันออกไปตามช่วงอายุการทำงานของพนักงาน อย่างเช่น พนักงานใหม่หรือพึ่งทำงานได้ไม่นานอาจต้องเพิ่มการดูแลเป็นพิเศษ ในการให้ข้อมูลข่าวสาร การฝึกอบรม หรือการประชาสัมพันธ์เพิ่มเติม เป็นต้น

ข้อเสนอแนะงานวิจัย

สำหรับงานวิจัยฉบับนี้เป็นการวิเคราะห์ความเสี่ยงในการรักษาความปลอดภัยข้อมูลสารสนเทศขององค์กรตัวอย่าง เพื่อนำมาตรฐานการรักษาความปลอดภัยของข้อมูลมาประยุกต์ใช้งานให้เหมาะสมกับสภาพขององค์กรที่เป็นอยู่ในปัจจุบัน เพื่อเป็นการเพิ่มศักยภาพการให้บริการให้มีประสิทธิภาพมากขึ้นในการให้บริการแก่ลูกค้าทั้งภายนอกองค์กรและภายในองค์กรได้ รวมทั้งการวิเคราะห์ถึงเหตุการณ์ของภัยคุกคามที่จะก่อให้เกิดความเสี่ยงและส่งผลกระทบต่อการดำเนินงานและการให้บริการขององค์กร พร้อมนำเสนอแนวทางการควบคุมความเสี่ยงอิงตาม

มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูล ISO 17799 ที่เหมาะสมกับแต่ละความเสี่ยง เพื่อที่องค์กรและผู้ที่เกี่ยวข้องนำกลับมาพิจารณาถึงความเหมาะสมในการนำไปประยุกต์ใช้งานจริง ซึ่งแนวทางที่ผู้วิจัยนำเสนออาจเป็นข้อกำหนด หรือข้อปฏิบัติที่องค์กรนั้นมีอยู่แล้วแต่ขาดการนำเสนอหรือประชาสัมพันธ์กับพนักงานให้มีความรู้ที่ใกล้เคียงกัน

อย่างไรก็ตามงานวิจัยครั้งนี้เป็นการศึกษาจากความคิดเห็นของพนักงานในองค์กรด้านการให้บริการจัดซื้อออนไลน์ ดังนั้นองค์กรที่มีการให้บริการรูปแบบต่างๆผ่านทางออนไลน์จึงสามารถนำผลงานวิจัยที่ได้ไปปรับปรุง และประยุกต์ระบบภายในขององค์กรได้ เนื่องจากในองค์กรแต่ละองค์กรต่างก็มีการสภาพแวดล้อมในการทำงานที่แตกต่างกัน การนำเสนอเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงแก่ข้อมูลขององค์กรอาจต้องมีการปรับให้มาจากสภาพแวดล้อมจริงของแต่ละองค์กรด้วย ซึ่งจะช่วยให้การวิเคราะห์เพื่อหาความเสี่ยงมีความเหมาะสมและแม่นยำมากขึ้น จึงทำให้องค์กรสามารถวิเคราะห์หาความเสี่ยงในการรักษาความปลอดภัยข้อมูลและหาแนวทางป้องกันได้อย่างถูกต้องยิ่งขึ้น

โดยสิ่งที่ต้องคำนึงถึงเมื่อมีการประเมินความเสี่ยงก่อนการประยุกต์ใช้มาตรฐานการจัดการต่างๆนั้น ในการจัดทำแบบสอบถามสำหรับการประเมินหรือการสำรวจความคิดเห็น ต้องเข้าใจว่าพนักงานในองค์กรมรความรู้ ความเข้าใจในแต่ละเรื่องแตกต่างกัน ดังนั้นต้องมีการทำความเข้าใจพร้อมทั้งอธิบายความหมายของคำถามให้ชัดเจนก่อน เพื่อให้ได้ผลจากการตอบแบบสอบถามเป็นผลที่สามารถนำไปใช้วิเคราะห์ได้จริง และเพื่อเวลานำมาตรฐานกลับมาประยุกต์ใช้ ได้จัดความเข้มข้นในการใส่ใจกับแต่ละกลุ่มตัวอย่างที่เหมาะสม ซึ่งเป็นเตรียมความพร้อมและแก้ไขที่ตรงจุดและลดระยะดำเนินการ

และแนวทางการรักษาความปลอดภัยของข้อมูลนอกจากมาตรฐาน ISO 1779 แล้วนั้น ยังมีมาตรฐานอื่นๆที่ปัจจุบันได้รับความสนใจ อย่างเช่น COBIT Framework, COSO Framework เป็นต้น ซึ่งองค์กรต่างๆสามารถนำไปประยุกต์และปรับใช้ให้เหมาะสมแก่องค์กรของตนและธุรกิจที่ให้บริการได้อีก นอกเหนือจากมาตรฐาน ISO 17799 ที่กล่าวมา