บทที่ 5

สรุปผลการวิจัย

การศึกษาวิจัยเรื่องนี้ เป็นการศึกษานโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษา โดยมีวัตถุประสงค์เพื่อเปรียบเทียบนโยบายดังกล่าวกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากล 2 แบบ ได้แก่ มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005 และเพื่อเสนอแนะนโยบายที่เหมาะสมและสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากลให้กับธนาคารที่ใช้เป็นกรณีศึกษา

การศึกษาวิจัยในครั้งนี้ใช้วิธีการรวบรวมข้อมูลแบบปฐมภูมิ ได้แก่ การวิจัยด้วยเทคนิคเดลฟายแบบปรับปรุง (Ethnographic Delphi Futures Research: EDFR) และการสัมภาษณ์เชิงลึก (In-Depth Interview) และวิธีการรวบรวมข้อมูลแบบทุติยภูมิ ได้แก่ การค้นคว้าจากเอกสาร บทความ งานวิจัยที่เกี่ยวข้อง และการค้นคว้าทางอินเทอร์เน็ต แล้วจึงจัดทำ Gap Analysis เพื่อวิเคราะห์เปรียบเทียบผลการศึกษาและจัดทำเป็นข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตที่เหมาะสมให้กับธนาคารที่ใช้เป็นกรณีศึกษาต่อไป

อภิปรายผลการวิจัย

ในระดับองค์กร การวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารให้มีความสอดคล้องกับมาตรฐาน ISO/IEC 17799:2005 นั้นถือว่าเป็นสิ่งที่ถูกต้องเหมาะสมแล้ว อีกทั้งธนาคารก็ได้มีการวางแผนงานในการสื่อสารเนื้อหาโดยรวมของนโยบายออกไปให้พนักงานรับทราบ โดยให้ความสำคัญกับการสร้างความเข้าใจที่ถูกต้องในเรื่องของความแตกต่างระหว่างคำว่านโยบายกับมาตรฐานและระเบียบวิธีในการปฏิบัติงาน เพื่อหลีกเลี่ยงไม่ให้พนักงานเกิดความสับสน และยังได้ให้ความสำคัญกับการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงานทุกคนในธนาคาร นอกจากนี้ ธนาคารยังได้มีการวางกลไกต่างๆ

เพื่อช่วยให้ธนาคารรับทราบปัญหาที่เกิดขึ้นจากการนำนโยบายไปปฏิบัติจริง เพื่อที่จะได้พิจารณาปรับปรุงแก้ไขนโยบายดังกล่าวให้มีความเหมาะสมกับการทำงานมากที่สุด ซึ่งจะเห็นได้ว่า การวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารนั้น ไม่ได้เป็นเพียงการนำหัวข้อในการควบคุมทั้งหมดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 มาปรับใช้ภายในธนาคารเท่านั้น แต่นโยบายดังกล่าวยังได้ผ่านการพิจารณาในหลายๆแง่มุม ไม่ว่าจะเป็นในเรื่องของวัฒนธรรมองค์กร ลักษณะการดำเนินงานของธนาคาร และที่สำคัญคือ ลักษณะการทำงานรวมถึงความรู้สึกนึกคิดของพนักงาน เพื่อให้แน่ใจว่านโยบายที่ออกมานั้นจะประสบผลสำเร็จตามที่ธนาคารคาดหวัง

ทางด้านภาพรวมของการบริหารจัดการภายในของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้น พบว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีการบริหารจัดการภายในที่ดี ไม่ว่าจะเป็นในเรื่องของความปลอดภัยของตัวระบบ ที่ได้มีการคำนึงถึงเรื่องของความปลอดภัยข้อมูลสารสนเทศตั้งแต่ในช่วงเริ่มต้นของการออกแบบระบบ ไปจนถึงช่วงที่การพัฒนาระบบเสร็จสมบูรณ์แล้ว และธนาคารยังได้กำหนดให้มีการทดสอบความปลอดภัยของระบบ (Security Testing) โดยการตรวจสอบหาช่องโหว่ของระบบโดยทีมงานของธนาคารและบริษัทภายนอกที่มีความเชี่ยวชาญในการตรวจสอบช่องโหว่ของเว็บแอพพลิเคชั่นอย่างสม่ำเสมอ นอกจากนี้ บุคลากรที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารยังเป็นผู้ที่มีความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศเป็นอย่างดี ซึ่งสามารถเห็นได้จากการจัดให้มีการแลกเปลี่ยนความรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศระหว่างทีมงานต่างๆอยู่เสมอ

ส่วนเรื่องของการจัดทำเอกสารที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้น พบว่า ทีมงานที่มีหน้าที่รับผิดชอบในส่วนต่างๆของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีการจัดทำเอกสารที่เกี่ยวข้องอยู่ในระดับที่เหมาะสมและมีการจัดเก็บไว้เป็นอย่างดี ไม่ว่าจะเป็นเอกสารการออกแบบระบบ รายงานการพบข้อผิดพลาดในระหว่างการทดสอบระบบ คู่มือและข้อกำหนดในการติดตั้งระบบ ไปจนถึงระเบียบวิธีในการทำงาน และการปฏิบัติตนเมื่อต้องให้ความช่วยเหลือลูกค้า หรือเมื่อมีเหตุการณ์ความผิดปกติเกิดขึ้นกับระบบเป็นต้น

ผลจากการทำ Gap Analysis โดยการเปรียบเทียบลักษณะของการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารกับหัวข้อของการควบคุมที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 ทั้ง 11 หัวข้อ 133 มาตรการ สรุปได้ว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีมาตรการในการป้องกันความปลอดภัยข้อมูลสารสนเทศครบทั้ง 133 มาตรการตามที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 นอกจากนี้ ธนาคารยังได้นำหลักการของ PDCA ที่ระบุไว้ในมาตรฐาน ISO/IEC 27001:2005 มาประยุกต์ใช้ในการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอีกด้วย

ข้อเสนอแนะจากการวิจัย

ผู้วิจัยเห็นว่า นอกจากการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงานของธนาคารแล้ว ปัจจัยส่วนหนึ่งที่จะช่วยให้พนักงานของธนาคารปฏิบัติตามนโยบายด้านความปลอดภัยข้อมูลสารสนเทศอย่างจริงจังก็คือ การให้รางวัลและการกำหนดบทลงโทษที่เหมาะสม เนื่องจากปัจจุบันธนาคารก็มีกฎระเบียบในการปฏิบัติงานมากมาย แต่ก็ปรากฏว่ามีพนักงานส่วนหนึ่งที่เพิกเฉย ไม่สนใจที่จะปฏิบัติตามกฎระเบียบดังกล่าว ส่วนหนึ่งอาจเนื่องมาจากการไม่เห็นความสำคัญของการปฏิบัติตามกฎระเบียบ ซึ่งขัดกับความเคยชินในการทำงานของตน ประกอบกับการไม่มีบทลงโทษที่ชัดเจน ทำให้พนักงานไม่ใส่ใจที่จะปฏิบัติตามกฎระเบียบนั้น เนื่องจากไม่ได้เกิดผลเสียหายขึ้นกับตน นอกจากนี้ การที่ธนาคารไม่กำหนดบทลงโทษที่ชัดเจนยังส่งผลให้เกิดพฤติกรรมการเลียนแบบกันไม่ปฏิบัติตามกฎระเบียบของธนาคารอีกด้วย ดังนั้น ธนาคารควรมีการกำหนดบทลงโทษผู้ที่ไม่ปฏิบัติตามนโยบายของธนาคารอย่างเหมาะสม โดยอาจพิจารณากำหนดบทลงโทษตามผลเสียหายที่มีต่อธนาคารอันเนื่องมาจากการที่พนักงานไม่ปฏิบัติตามนโยบายของธนาคาร และควรจะมีการประกาศบทลงโทษนั้นให้พนักงานทราบโดยทั่วกัน

ในทางกลับกัน ธนาคารควรมีการให้รางวัลแก่ผู้ที่ปฏิบัติตามนโยบายของธนาคารอย่างเคร่งครัด เพื่อเป็นขวัญและกำลังใจให้กับพนักงานที่ปฏิบัติตามนโยบายของธนาคาร และเป็นตัวอย่างที่ดีให้เพื่อนพนักงานด้วยกัน โดยที่รางวัลนั้นควรจะเป็นรางวัลจากผู้บริหารระดับสูง เพื่อแสดงให้เห็นว่าผู้บริหารระดับสูงนั้นให้ความสำคัญกับนโยบายและพนักงานที่ปฏิบัติตามนโยบายดังกล่าว ทั้งนี้ รางวัลนั้นอาจจะไม่ได้อยู่ในรูปของสิ่งของหรือเงินรางวัล แต่อาจจะเป็นคำ

ชมเชยจากผู้บริหารระดับสูงก็ได้ และควรต้องมีการประกาศให้พนักงานทราบโดยทั่วกันเช่นเดียวกัน

ในส่วนของการสื่อสารนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารนั้น ผู้วิจัยมีความเห็นว่า ธนาคารสามารถใช้สื่อประเภทอื่นที่นอกเหนือไปจากโปสเตอร์และจดหมายอิเล็กทรอนิกส์ของธนาคารเพิ่มเติมได้ ไม่ว่าจะเป็นเสียงตามสาย วารสารสัมพันธ์ของธนาคาร หรืออินทราเน็ตของธนาคาร เป็นต้น ซึ่งธนาคารไม่จำเป็นต้องเสียค่าใช้จ่ายเพิ่มเติมเพื่อการสร้างสื่อเหล่านี้แต่อย่างใด และเนื่องจากธนาคารมีการวางแผนที่จะประกาศนโยบายให้พนักงานรับทราบไปพร้อมๆกับการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงาน ผู้วิจัยจึงมีความเห็นว่า การสร้างฐานข้อมูลความรู้ในเรื่องของนโยบายความปลอดภัยข้อมูลสารสนเทศของธนาคาร โดยอาศัยแนวความคิดของการบริหารจัดการองค์ความรู้ (Knowledge Management) ภายในองค์กร น่าจะเป็นวิธีการที่เหมาะสม โดยอาจเริ่มจากการสร้างเว็บไซต์ที่เป็นที่รวบรวมนโยบาย มาตรฐานและระเบียบวิธีในการปฏิบัติงาน รวมทั้งข้อมูลข่าวสารหรือบทความต่างๆที่เกี่ยวข้องกับความปลอดภัยข้อมูลสารสนเทศของธนาคาร เพื่อให้พนักงานทุกคนสามารถเข้าถึงและแลกเปลี่ยนความรู้ระหว่างกันได้ หลังจากนั้นจึงจัดให้มีการทำกิจกรรมต่างๆที่เกี่ยวข้องกับการป้องกันความปลอดภัยข้อมูลสารสนเทศของธนาคาร เพื่อส่งเสริมให้เกิดการมีส่วนร่วมในการปฏิบัติตามนโยบายของธนาคารและยกระดับความตระหนักรู้เรื่องของความปลอดภัยข้อมูลสารสนเทศของพนักงานไปพร้อมๆกัน

ในส่วนของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้น ผลสรุปจากการทำ Gap Analysis ดังกล่าวเป็นเพียงการสรุปว่าบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีหรือไม่มีมาตรการที่สอดคล้องกับหัวข้อของการควบคุมที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 ซึ่งการมีอยู่ของมาตรการดังกล่าวอาจไม่ได้หมายถึงการนำมาใช้อย่างมีประสิทธิภาพก็เป็นได้ ดังนั้น ผู้วิจัยจึงมีความเห็นว่า ธนาคารควรจะได้มีการจัดทำเอกสารที่แสดงถึงรายละเอียดของมาตรการต่างๆที่ธนาคารนำมาใช้เพื่อป้องกันความปลอดภัยข้อมูลสารสนเทศของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร โดยกำหนดหัวข้อตามหัวข้อของการควบคุมที่ระบุในมาตรฐาน ISO/IEC 17799:2005 เพื่อช่วยให้ผู้ที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารทราบว่า มาตรการที่ธนาคารนำมาใช้นั้นมีระดับของการควบคุมอยู่ในระดับใด ผู้ที่มีหน้าที่เกี่ยวข้องกับมาตรการนั้นๆได้รับทราบและมีการปฏิบัติตาม

มาตรการเหล่านั้นหรือไม่ เพื่อประโยชน์ในการทบทวนและปรับปรุงมาตรการต่างๆให้มีความเหมาะสมกับการบริหารจัดการความปลอดภัยข้อมูลสารสนเทศของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมากที่สุด

หลังจากที่ได้มีการจัดทำเอกสารดังกล่าวขึ้นมาแล้วนั้น หากธนาคารเห็นว่าบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีมาตรการในการป้องกันความปลอดภัยข้อมูลสารสนเทศที่มีประสิทธิภาพและสอดคล้องกับหัวข้อของการควบคุมที่ระบุในมาตรฐาน ISO/IEC 17799:2005 ทุกประการแล้วนั้น ผู้วิจัยเห็นว่า ธนาคารควรพิจารณานำบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารเข้ารับการตรวจรับรองระบบเพื่อให้ได้ใบรับรองตามมาตรฐาน ISO/IEC 27001:2005 ทั้งนี้ เพื่อช่วยสร้างความมั่นใจให้กับลูกค้าที่ใช้และกำลังจะตัดสินใจใช้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร และเป็นตัวอย่างให้กับระบบงานอื่นๆของธนาคารในการยกระดับของการป้องกันความปลอดภัยข้อมูลสารสนเทศของตนให้มีประสิทธิภาพมากขึ้น อันจะส่งผลให้เกิดความตื่นตัวในเรื่องของการป้องกันความปลอดภัยข้อมูลสารสนเทศทั่วทั้งธนาคาร

และเนื่องจากในปัจจุบัน ภัยคุกคามและอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตได้เพิ่มจำนวนขึ้นเป็นอย่างมาก และมีวิธีในการทำงานที่ซับซ้อนมากขึ้น ประกอบกับลักษณะของการโจมตีระบบโดยผู้ไม่ประสงค์ดีนั้นจะเปลี่ยนไปเป็นการมุ่งโจมตีจุดอ่อนจากการไม่ระมัดระวังตัวของผู้ใช้งานระบบ มากกว่าจะมุ่งไปที่การโจมตีระบบซึ่งมีการพัฒนาให้มีความปลอดภัยในระดับที่สูงขึ้น ดังนั้น ผู้วิจัยจึงความเห็นว่า นอกเหนือจากการสร้างความตระหนักรู้เรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงานของธนาคารแล้ว ธนาคารควรจะมีการสร้างความตระหนักรู้เรื่องของความปลอดภัยข้อมูลสารสนเทศให้แก่ลูกค้าของธนาคารด้วยเช่นกัน ไม่ว่าจะเป็นในเรื่องของการใช้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารให้มีความปลอดภัย หรือวิธีในการป้องกันเครื่องคอมพิวเตอร์ของลูกค้าไม่ให้ถูกโจมตีจากไวรัสหรือโทรจันต่างๆ เพื่อประโยชน์ในการป้องกันความเสียหายที่อาจเกิดขึ้นกับลูกค้าของธนาคารจากการใช้บริการทางการเงินผ่านอินเทอร์เน็ตที่ไม่เหมาะสมโดยไม่รู้ตัว

ข้อเสนอแนะในการวิจัยครั้งต่อไป

ผู้วิจัยมีความเห็นว่า แนวทางในการศึกษาวิจัยครั้งต่อไปนั้นอาจจะมีลักษณะดังต่อไปนี้

1. เป็นการศึกษาถึงความพร้อมในการนำบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษาเข้ารับการตรวจรับรองระบบเพื่อขอใบรับรองตามมาตรฐาน ISO/IEC 27001:2005

2. เป็นการศึกษาถึงปัจจัยด้านการบริหารโครงการที่มีผลต่อการนำบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษาเข้ารับการตรวจรับรองระบบเพื่อขอใบรับรองตามมาตรฐาน ISO/IEC 27001:2005

3. เป็นการศึกษาถึงความเป็นไปได้ในการนำแนวความคิดของการบริหารจัดการองค์ความรู้ (Knowledge Management) เข้ามาใช้กับการสื่อสารนโยบายความปลอดภัยข้อมูลสารสนเทศขององค์กร