วารสารวิชาชีพบัญชี
บทความวิจัย

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 ของบริษัทจดทะเบียนในมุมมองของผู้ตรวจสอบสารสนเทศ

ฐิติ วิรทัศนุสรณ์*
ดร.มนวิกา ผดุงสิทธิ์**

บทนำ

ในปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทอย่างมากในการปฏิบัติงานขององค์กร ทำให้องค์กรสามารถปฏิบัติงานหลักได้เพื่อตอบสนองความต้องการของลูกค้าได้ดีขึ้น ทำให้เกิดกำไรและการเจริญเติบโตที่ยั่งยืน นอกจากนี้ เทคโนโลยีสารสนเทศยังได้มีส่วนส่งเสริมให้งานสนับสนุนขององค์กรดำเนินไปอย่างมีประสิทธิภาพและประสิทธิผล ซึ่งท้ายที่สุดก็ส่งผลต่อความมีประสิทธิภาพและประสิทธิผลของกิจกรรมต่างๆ ในห่วงโซ่มูลค่า (Value Chain) การประสานงานกันระหว่างกิจกรรมต่างๆ ทำให้เกิดการแลกเปลี่ยนข้อมูลและความรู้ระหว่างกัน มีการเชื่อมโยงเครือข่ายต่างๆ ทั้งภายในองค์กรและระหว่างองค์กรมากขึ้น รวมถึงการเชื่อมโยงเครือข่ายข้ามภูมิภาค

กล่าวได้ว่าแทบทุกองค์กรได้นำระบบสารสนเทศเข้ามามีส่วนช่วยในการติดต่อประสานงานเพื่อเพิ่มคุณค่าธุรกิจด้วยการเชื่อมโยงแลกเปลี่ยนข้อมูลเชิงพาณิชย์ระหว่างกัน ปรับเปลี่ยนการทำธุรกรรมประจำวันจากรูปแบบกระดาษมาเป็นรูปแบบทางอิเล็กทรอนิกส์

ปีที่ 4 ฉบับที่ 10
มีนาคม 2551
หน้า 53-65

* ผู้ช่วยหัวหน้าส่วนวิเคราะห์และรายงานทางการเงิน ธนาคารกสิกรไทย จำกัด มหาชน
** ผู้ช่วยศาสตราจารย์ประจำภาควิชาการบัญชี คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

ทำให้การดำเนินธุรกิจเป็นไปด้วยความรวดเร็ว ต่อเนื่อง สามารถตอบสนองความต้องการของผู้บริโภคได้ทันเวลา ด้วยต้นทุนที่ต่ำลง ดังนั้น ระบบสารสนเทศจึงเป็นปัจจัยสำคัญที่จะทำให้ธุรกิจมีความได้เปรียบในการแข่งขัน และสามารถอยู่รอดได้ ระบบเครือข่ายอินเทอร์เน็ต (Internet) เป็นเทคโนโลยีหลักที่เป็นตัวแปรสำคัญต่อการเปลี่ยนแปลงวิธีการปฏิบัติและขั้นตอนในการดำเนินธุรกิจ เนื่องจากเป็นเครือข่ายสื่อสารข้อมูลที่เป็นมาตรฐานเดียวกันที่สามารถโยงใยได้ทั่วโลกโดยไม่มีข้อจำกัดทางด้านเวลา สถานที่หรือรูปแบบของข้อมูล อย่างไรก็ตาม การเปิดกว้างในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกัน ทำให้เพิ่มความเสี่ยงในการเปิดช่องให้บุคคลอื่นที่ประสงค์ร้ายมาบุกรุกทำลาย ขโมย หรือแก้ไขข้อมูล โอกาสที่ระบบงานจะขัดข้องหรือหยุดชะงัก ใช้งานไม่ได้ก็เพิ่มสูงขึ้นด้วยเช่นกัน ความปลอดภัยของข้อมูลจึงเป็นประเด็นที่หน่วยงานหรือองค์กรที่มีการประยุกต์ใช้เทคโนโลยีสารสนเทศในการจัดเก็บและประมวลผลข้อมูลสารสนเทศ จะต้องพิจารณาให้ความสำคัญ

ประโยชน์ของเทคโนโลยีสารสนเทศนั้นมีนานัปการ แต่หากองค์กรไม่มีการบริหารจัดการอย่างระมัดระวัง ความสูญเสียที่อาจเกิดขึ้นก็ส่งผลกระทบต่อองค์กรอย่างมากเช่นกัน เช่น North Bay Health Care Group ต้องสูญเสียเกือบ 9 แสนเหรียญจากการที่พนักงานจ่ายเงินของบริษัทได้ใช้คอมพิวเตอร์เข้าไปโปรแกรมระบบบัญชีโดยไม่ได้รับอนุญาต และได้ทำการสั่งจ่ายเช็คจำนวน 127 ฉบับให้กับตัวเองและผู้อื่น หรือกรณี Denial of Service Attack ซึ่งเกิดขึ้นกับระบบเครือข่าย Cudsys ซึ่งเป็นเมล์เซิฟเวอร์ที่อยู่ในความดูแลของ U.S. District Court ของ New York ที่ถูกโจมตีจากผู้ใช้และระบบคอมพิวเตอร์โดยการส่ง Email จำนวนมากเข้าไปยังเมล์เซิฟเวอร์ ทำให้ระบบเครือข่ายดังกล่าวต้องปิดระบบตัวเอง ไม่สามารถให้บริการได้ นอกจากนี้ การโจมตีโดยมัลแวร์หรือโปรแกรมประสงค์ร้าย (Malicious Application; Malware) ได้เพิ่มจำนวนขึ้นอย่างรวดเร็ว รวมทั้งความหลากหลายของมัลแวร์ ดังเช่นกรณีที่ Roger Duronio ซึ่งทำงานอยู่ที่บริษัท PaineWebber ได้ใช้มัลแวร์ประเภท Logic Bomb ที่ถูกตั้งเวลาให้ทำงานหลังจากที่เขาได้ลาออกจากบริษัทเป็นที่เรียบร้อยแล้ว มาสร้างความเสียหายให้กับเครือข่ายคอมพิวเตอร์ของบริษัทมากกว่า 1,500 เครือข่าย ทำให้เกิดมูลค่าความเสียหายเป็นจำนวนเงินกว่า 3 พันล้านเหรียญ นอกจากนี้ มัลแวร์ดังกล่าวยังได้ทำการซื้อ Put Option ในตลาดหุ้นให้กับบริษัท PaineWebber สร้างความเสียหายให้กับบริษัท และตลาดหุ้นในสหรัฐอเมริกา

ดังนั้น องค์กรจะต้องจัดให้มีการรักษาความปลอดภัยของข้อมูลซึ่งเป็นการรักษาข้อมูลไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลทางธุรกิจ อันจะช่วยบรรเทาภัยคุกคามในหลายรูปแบบที่จะมีผลต่อข้อมูล ด้วยการควบคุมที่เหมาะสม ซึ่งระดับความเหมาะสมของการควบคุมความปลอดภัยของข้อมูลนั้นเป็นการผสมผสานกันอย่างลงตัวของลักษณะทางกายภาพและการควบคุมทางด้านเทคนิคหรือการควบคุมด้านการปฏิบัติงาน การป้องกันรักษาความปลอดภัยของข้อมูลจะสนับสนุนให้องค์กรสามารถแบ่งปันข้อมูลทางธุรกิจร่วมกันโดยข้อมูลอยู่บนพื้นฐานของความมั่นคงปลอดภัย ทำให้องค์กรได้รับความเชื่อมั่นจากลูกค้า ผู้ผลิต และหน่วยงานธุรกิจอื่น อันส่งผลให้ธุรกิจมีการขยายตัว มีผลประกอบการที่ดี และสร้างกระแสเงินสดเข้าให้กับองค์กร

แนวทางปฏิบัติหนึ่งที่องค์กรสามารถนำมาใช้เพื่อรักษาความปลอดภัยของข้อมูลและลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามต่างๆ คือการประยุกต์ใช้มาตรฐานรักษาความปลอดภัย ISO/IEC 17799 ซึ่งเป็นมาตรฐานที่รวบรวมมาตรการพื้นฐาน (Baseline) ที่มีชื่อว่า BS 7799 (British Standard 7799) ที่เป็นมาตรฐานทางอุตสาหกรรมที่หลายองค์กรยึดถือร่วมกัน และถูกนำไปใช้อย่างแพร่หลาย แม้แต่องค์กรที่ไม่ได้อยู่ในภาคอุตสาหกรรมก็นิยมนำมาตรฐานดังกล่าวไปประยุกต์ใช้ในประเทศไทย บริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยหลายบริษัทได้ยึดถือมาตรฐานฉบับนี้เป็นเกณฑ์ในการตรวจสอบทางด้านเทคโนโลยีสารสนเทศ

เพื่อให้มั่นใจได้ว่าระบบสารสนเทศและข้อมูลที่ใช้งานอยู่มีความถูกต้อง และเชื่อถือได้

งานวิจัยนี้มีวัตถุประสงค์ที่จะศึกษาว่าบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยที่ได้นำระบบสารสนเทศมาสนับสนุนการปฏิบัติงานนั้น ได้มีการนำมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 มาปฏิบัติมากน้อยเพียงใด และหากนำมาปฏิบัติสามารถปฏิบัติตามข้อกำหนดที่มาตรฐานได้กำหนดไว้ครบทุกประเด็นหรือไม่ และการปฏิบัติตามมาตรฐานดังกล่าวมีผลให้ความถูกต้องเชื่อถือได้ของข้อมูลสารสนเทศเพิ่มขึ้นหรือไม่ มีข้อจำกัดในการนำมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 มาประยุกต์ใช้หรือไม่ รวมถึงการศึกษาข้อบกพร่อง หรือข้อผิดพลาดอันเกิดจากการไม่ปฏิบัติตามมาตรฐานดังกล่าว โดยงานวิจัยนี้จะศึกษาในมุมมองของผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยที่มีสถานะเป็นบริษัทจดทะเบียนในช่วงปี พ.ศ. 2549 ถึงปี พ.ศ. 2550 โดยไม่รวมบริษัทที่อยู่ในระหว่างการฟื้นฟูกิจการ บริษัทจดทะเบียนในตลาดหลักทรัพย์เอ็มเอไอ (MAI) และบริษัทจัดการกองทุนรวมต่างๆ ซึ่งผลการศึกษาที่ได้จะทำให้ทราบว่าในปัจจุบันบริษัทจดทะเบียนได้ให้ความสำคัญกับความปลอดภัยของข้อมูลมากน้อยเพียงใด การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ได้ส่งผลต่อความน่าเชื่อถือของข้อมูลหรือไม่ รวมถึงข้อจำกัดในการปฏิบัติตามมาตรฐานดังกล่าวซึ่งจะเป็นข้อมูลเบื้องต้นที่สำคัญที่หน่วยงานกำกับดูแลสามารถนำไปใช้ในการพิจารณาปรับปรุงมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 17799 ฉบับภาษาไทยให้สอดคล้องเหมาะสมกับการใช้งานระบบสารสนเทศภายในประเทศไทย

แนวคิดและงานวิจัยที่เกี่ยวข้อง

หลักการพื้นฐานของการรักษาความปลอดภัยของข้อมูลจะมุ่งเน้นไปที่การรักษาความปลอดภัยของข้อมูลในทุกรูปแบบที่เกี่ยวกับเทคโนโลยีที่ใช้ในการประมวลผล การเก็บรักษา การติดต่อสื่อสาร และทรัพยากรที่เกี่ยวข้องคอมพิวเตอร์ของแต่ละบุคคลหรือองค์กร การรักษาความปลอดภัยของข้อมูลมีองค์ประกอบทางด้านเทคนิคและด้าน ขึ้นอยู่กับพฤติกรรมของมนุษย์ และมีผลกระทบต่อบุคคลหลายกลุ่มซึ่งเป็นผู้ใช้งานข้อมูลเหล่านั้น องค์กรจึงจำเป็นต้องหาทางป้องกันการเข้าถึงข้อมูล เพื่อคงไว้ซึ่งข้อมูลที่มีความปลอดภัย (Helokunnin and Kamal, 2002) Calder (2006) แบ่งองค์ประกอบของการรักษาความปลอดภัยของข้อมูลออกเป็น 3 องค์ประกอบคือ (1) Confidentiality เป็นการป้องกันข้อมูลที่สำคัญขององค์กรไม่ให้ถูกเปิดเผยโดยไม่ได้รับอนุญาต หรือถูกขโมยโดยไม่สามารถติดตามได้ (Humphreys et al., 1998) การรักษาความลับของข้อมูลต่างๆ ภายในหน่วยงาน อาจกระทำได้หลากหลายวิธีด้วยกัน ไม่ว่าจะเป็นการกำหนดสิทธิ์การเข้าถึงข้อมูล การกำหนดรหัสผ่าน หรือการแบ่งแยกหน้าที่ให้เหมาะสมกับหน้าที่ความรับผิดชอบ (2) Integrity เป็นความถูกต้องครบถ้วนของข้อมูล ซึ่งองค์กรจำเป็นต้องมีการกำหนดมาตรการหรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลเพื่อป้องกันความผิดพลาดหรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต และ (3) Availability ความพร้อมใช้ของข้อมูล ซึ่งเป็นสิ่งที่สำคัญที่สุดเพราะถ้าปราศจากข้อมูลที่ทันเวลาแล้วนั้น องค์กรจะไม่สามารถดำเนินธุรกิจตามปกติได้ (Gerber and Von Solms, 2001)

มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 เป็นมาตรฐานที่เป็นสากล และถูกนำมาใช้อย่างแพร่หลายเพื่อให้ได้มาซึ่งข้อมูลที่มีลักษณะทั้ง 3 องค์ประกอบข้างต้น มาตรฐานดังกล่าวมีจุดเริ่มต้นจากการรวบรวมมาตรการพื้นฐาน (Baseline) ที่มีชื่อว่า BS 7799 (British Standard 7799) ซึ่ง British Standard Institute (BSI) ได้ผลักดันให้เป็นมาตรฐานสากล ISO/IEC 17799 (International Organization of Standard 17799) ในปี ค.ศ. 2000 โดยเนื้อหาแบ่งเป็น 2 ส่วนคือ

(1) BS 7799 Part 1: ISO/IEC 17799: 2000 (Code of practice for Information Security Management) หรือ ISO/IEC 17799 ซึ่งประกอบไปด้วยการควบคุมทางด้านการจัดการความปลอดภัยของข้อมูลที่ควรปฏิบัติจำนวน 127 ข้อ ใน 10 หัวข้อหลัก เพื่อสร้างความปลอดภัยของข้อมูลภายในองค์กร

(2) BS 7799 Part 2: BS 7799-2: 2002 (Information Security Management System (ISMS) - Specification with Guidance for use) หรือ BS 7799 ซึ่งจะเกี่ยวข้องกับการจัดตั้งระบบการจัดการด้านความปลอดภัยของข้อมูลในองค์กร โดยเริ่มจากการริเริ่มที่จะมีกระบวนการรักษาความปลอดภัยของข้อมูล การประเมินความเสี่ยง การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยในหน่วยงาน รวมถึงการออกข้อกำหนดและมาตรการเพื่อให้บุคลากรในหน่วยงานปฏิบัติตาม

ส่วนที่ 1 เป็นเพียงแนวทางปฏิบัติ ถ้าองค์กรต้องการได้รับการรับรองมาตรฐานการรักษาความปลอดภัยของข้อมูลภายในองค์กร จะต้องดำเนินการตามมาตรฐานในส่วนที่ 2 ผลลัพธ์ของการพัฒนากระบวนการรักษาความปลอดภัยของข้อมูล จะทำให้หน่วยงานทราบถึงเหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศ ได้เห็นถึงช่องโหว่หรือจุดอ่อนในด้านการรักษาความปลอดภัย (Security Weakness) ของระบบสารสนเทศภายในหน่วยงาน หรือองค์กร

มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799:2000 ได้ถูกพัฒนาปรับปรุงเนื้อหาอย่างต่อเนื่อง เพื่อให้ครอบคลุมถึงสถานการณ์ที่เปลี่ยนแปลงไปของการใช้งานระบบสารสนเทศ โดยในปี ค.ศ. 2005 ได้ปรับเป็นมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799:2005 ซึ่งได้เพิ่มหลักการพื้นฐานของการรักษาความปลอดภัยของข้อมูลจาก 127 ข้อกำหนด ใน 10 หัวข้อหลักเป็น 133 ข้อกำหนด ใน 11 หัวข้อหลัก ซึ่งหลักการที่สำคัญ 11 หัวข้อประกอบด้วย[1]

หัวข้อที่ 1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy) เป็นการกำหนดทิศทาง และให้การสนับสนุนสำหรับการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

หัวข้อที่ 2 การจัดโครงสร้างของการรักษาความปลอดภัยภายในองค์กร (Organizational of Information Security) เป็นการบริหาร และจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

หัวข้อที่ 3 การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) เป็นการป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจจะเกิดขึ้นได้ โดยกำหนดระดับการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

หัวข้อที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) เป็นการทำให้พนักงาน ผู้องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคาม และปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้ ทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร และลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หัวข้อที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and Environment Security) เป็นการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงทรัพย์สินสารสนเทศขององค์กร ทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

หัวข้อที่ 6 การบริหารจัดการด้านการสื่อสาร และการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management) เป็นการปฏิบัติเพื่อให้เกิดความมั่นใจว่าการปฏิบัติงานและการประมวลผลข้อมูลเป็นไปอย่างถูกต้องปลอดภัย

1 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2549.

หัวข้อที่ 7 การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร (Access Control) เป็นการควบคุมการเข้าถึงระบบสารสนเทศ โดยให้ผู้ที่ได้รับอนุญาตเท่านั้นที่จะมีสิทธิ์ในการเข้าถึงระบบสารสนเทศ

หัวข้อที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance) เป็นการจัดหาและการพัฒนาระบบสารสนเทศ โดยพิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยที่เป็นองค์ประกอบพื้นฐานที่สำคัญ ตลอดจนการป้องกันความผิดพลาดในการประมวลผลสารสนเทศ การสูญหาย เปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต หรือใช้งานผิดวัตถุประสงค์

หัวข้อที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management) เป็นการจัดการกับเหตุการณ์หรือจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรในช่วงระยะเวลาที่เหมาะสม

หัวข้อที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management) เป็นการป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ อันเป็นผลมาจากความล้มเหลวที่มีต่อระบบสารสนเทศ และองค์กรสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

หัวข้อที่ 11 การปฏิบัติตามข้อกำหนด (Compliance) เป็นการหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ อันจะนำไปสู่การถูกฟ้องร้องดำเนินคดี ทั้งในคดีแพ่ง และอาญา

ในอดีต มาตรฐานการรักษาความปลอดภัยของข้อมูลอาจจะไม่เป็นที่จำเป็นมากนัก เนื่องจากระบบคอมพิวเตอร์ไม่ได้มีการเชื่อมโยงกันเป็นเครือข่ายกว้างแต่ด้วยความก้าวหน้าของเทคโนโลยีในปัจจุบัน ทำให้มีการเชื่อมโยงเครือข่ายสื่อสารข้อมูลมากขึ้น ช่องโหว่ที่สำคัญที่ทำให้ระบบสารสนเทศขององค์กรถูกโจมตีจากผู้ที่ไม่หวังดีก็เปิดกว้างขึ้น มาตรฐานการรักษาความปลอดภัยของข้อมูลจึงมีความสำคัญ งานวิจัยของ Ziegenfuss (1995) เปิดเผยว่า จากการสอบถามความเห็นของผู้สอบบัญชีในหน่วยงานกำกับของรัฐบาลที่เป็นสมาชิกของ National Association of Local Government Auditors (NALGA) และ Virginia Local Government Auditors' Association (VLGAA) รัฐเวอร์จิเนีย ประเทศสหรัฐอเมริกา พบว่า ร้อยละ 90 ของกลุ่มตัวอย่างเชื่อว่าการฉ้อโกงจะเป็นปัญหาที่สำคัญของหน่วยงานรัฐบาล โดยสาเหตุที่ทำให้การทุจริตเพิ่มขึ้นประกอบด้วยการขาดการบริหารจัดการที่ดี (ร้อยละ 80) แรงกดดันทางเศรษฐกิจ (ร้อยละ 71) ความอ่อนแอทางสังคม (ร้อยละ 71) การขาดความรับผิดชอบในการกระทำของตัวเอง (ร้อยละ 66) การขาดการฝึกอบรมเกี่ยวกับการป้องกันและแก้ไขการทุจริต (ร้อยละ 57) อาชญากรรมมีความซับซ้อนมากขึ้น (ร้อยละ 46) ความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ (ร้อยละ 41) และภาระงานที่เพิ่มขึ้น (ร้อยละ 39) นอกจากนี้ ยังพบว่าการป้องกันการทุจริตที่มีประสิทธิภาพมากที่สุดประกอบด้วยการตรวจทานการตรวจสอบภายใน การตรวจสอบโดยเฉพาะจากผู้บริหาร การแจ้งให้พนักงานทราบ การควบคุมภายในและการตรวจพบการทุจริตโดยบังเอิญ (ไม่ได้มีการวางแผนการตรวจสอบไว้ก่อน) อย่างไรก็ตาม หน่วยงานราชการที่ศึกษาส่วนใหญ่ไม่มีนโยบายหรือกระบวนการสำหรับการจัดการพนักงานที่ต้องสงสัยว่าจะทำการทุจริต

งานวิจัยของ Thompson (1997) พบว่าองค์กรส่วนใหญ่ยังไม่มีความพร้อมในการจัดการเกี่ยวกับเรื่องการทุจริต ซึ่งสอดคล้องกับงานวิจัยของ Ziegenfuss (1995) Thompson (1997) ซึ่งเป็นเจ้าหน้าที่สืบสวนสอบสวนในหน่วยงาน Computer Crime Investigation Squad ได้สำรวจการรักษาความปลอดภัยของบริษัทจดทะเบียนในตลาดหลักทรัพย์ของประเทศออสเตรเลีย จำนวน 300 บริษัท เพื่อเป็นข้อมูลพื้นฐานในการทำความเข้าใจภัยคุกคามทางคอมพิวเตอร์ การแก้ปัญหาอาชญากรรมคอมพิวเตอร์และการออกกฎหมายให้

เหมาะสม จากการศึกษาพบว่า ร้อยละ 25 ขององค์กรที่ศึกษาไม่มีนโยบายการรักษาความปลอดภัย ร้อยละ 50 ไม่มีการอบรมให้ความรู้เรื่องการรักษาความปลอดภัยทางคอมพิวเตอร์ ร้อยละ 34 ไม่มีการอบรมให้ความรู้เกี่ยวกับจรรยาบรรณในการใช้คอมพิวเตอร์และเทคโนโลยี และร้อยละ 81 มีพนักงานที่มีระดับความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ไปในทางที่ผิดในระดับที่ต่ำหรือไม่มีเลย

ประเทศที่มีความพร้อมทางด้านเทคโนโลยีจะมีการเตรียมพร้อมในเรื่องของการรักษาความปลอดภัยของข้อมูลมากกว่าประเทศที่มีความก้าวหน้าทางเทคโนโลยีต่ำ Warren (2002) ได้ศึกษากลุ่มตัวอย่างจำนวน 4,254 บริษัทใน 29 ประเทศ พบว่า โดยเปรียบเทียบแล้ว กลุ่มตัวอย่างในประเทศออสเตรเลียมีการจัดทำนโยบายการรักษาความปลอดภัย (ร้อยละ 68) รองลงมาคือประเทศสหรัฐอเมริกา (ร้อยละ 60) กลุ่มตัวอย่างในประเทศสหรัฐอเมริกามีการใช้เครื่องมือหรือระบบการรักษาความปลอดภัยมากที่สุด (ร้อยละ 45) และมีการอบรมให้ความรู้ด้านการรักษาความปลอดภัยมากที่สุดเช่นกัน (ร้อยละ 32) โดยรวมแล้ว งานวิจัยดังกล่าวพบว่าการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลในประเทศต่างๆ ยังคงมีระดับไม่สูงนัก

นอกจากนี้ Warren (2002) ยังพบว่า อุปสรรคที่ขัดขวางการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศประกอบด้วยการขาดความรู้ของผู้ใช้งาน (ร้อยละ 57) การขาดงบประมาณ (ร้อยละ 49) การขาดความชำนาญ (ร้อยละ 44) และความซับซ้อนของเทคโนโลยี (ร้อยละ 31) จากการสำรวจองค์กรของประเทศอังกฤษพบว่า ส่วนใหญ่มีความกังวลในเรื่องการรักษาความปลอดภัยที่มีผลกระทบต่อข้อมูล การโจมตีของไวรัส และการลักขโมยคอมพิวเตอร์ เช่น คอมพิวเตอร์โน้ตบุ๊ค ส่วนภัยคุกคามที่หน่วยงานมีความวิตกกังวลน้อยที่สุดก็คือ การลักขโมยซอฟต์แวร์ การเจาะระบบ และการเจตนาใช้เทคโนโลยีสารสนเทศไปในทางที่ผิด

อย่างไรก็ตาม เมื่อเทคโนโลยีมีความเจริญก้าวหน้าขึ้น การใช้คอมพิวเตอร์ไปในทางที่ผิดได้พัฒนารูปแบบใหม่ๆ ขึ้น Annual Google Communications Intelligence Report (2008) ซึ่งเป็นรายงานที่ทำโดยกูเกิลรายงานว่า ภัยคุกคามคอมพิวเตอร์จะมีความซับซ้อนมากขึ้น ธุรกิจจะต้องเผชิญกับมัลแวร์หรือโปรแกรมประสงค์ร้ายประเภทต่างๆ ที่มากหลายมากขึ้น รวมทั้งจะต้องป้องกันข้อมูลที่เป็นความลับที่อาจจะรั่วไหลจากวิธีการ Social Engineering ซึ่งเป็นเทคนิคที่ผู้ไม่หวังดีใช้ในการหลอกล่อพนักงานขององค์กรให้เปิดเผยข้อมูลที่เป็นความลับ ส่วนภัยคุกคามอันดับหนึ่งสำหรับองค์กรส่วนใหญ่คือสแปม ซึ่งเกิดจากการใช้ระบบการสื่อสารทางอิเล็กทรอนิกส์ในทางที่ไม่ถูกต้อง และที่น่าเป็นห่วงคือองค์กรไม่สามารถคาดได้ว่าจะเกิดสแปมขึ้นในช่วงใด ทำให้ต้องมีการจัดเตรียมทรัพยากรเผื่อไว้ ซึ่งส่งผลต่อต้นทุนในการจัดสแปม

สำหรับประเทศไทย คณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งได้จัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำมาตรฐาน ISO/IEC 17799 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความปลอดภัยทางด้านอิเล็กทรอนิกส์ โดยมีการปรับเปลี่ยนให้มีความเหมาะสมกับสภาวะแวดล้อม และสถานการณ์ทางด้านเทคโนโลยีสารสนเทศในประเทศไทย ปัจจุบันมาตรฐาน ISO/IEC 17799 ฉบับภาษาไทยมี 2 ฉบับ โดยเนื้อหาของฉบับแรกจะสอดคล้องกับมาตรฐาน ISO/IEC 17799:2000 ส่วนเนื้อหาของฉบับที่สองได้ปรับปรุงเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 17799:2005 และได้ประกาศใช้เมื่อเดือนสิงหาคม พ.ศ.2549 โดยมีข้อกำหนดออกมาให้ปฏิบัติถึง 133 ข้อกำหนด ใน 11 หัวข้อ (ดวงกมล ทรัพย์พิทยากร, 2548)

ผลการสำรวจการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลในหน่วยงานภาครัฐบาลของคณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวง

เทคโนโลยีสารสนเทศและการสื่อสาร (2549) พบว่า หน่วยงานจำเป็นต้องมีมาตรการด้านความมั่นคงปลอดภัย เนื่องจากทุกหน่วยงานประสบกับความเสี่ยงจากการที่ระบบสารสนเทศถูกโจมตีจากผู้ไม่ประสงค์ดีและจากไวรัส การนำนโยบายความมั่นคงปลอดภัยไปปฏิบัติ การติดตามผล รวมทั้งการฝึกอบรม ยังไม่มีการจัดทำอย่างเป็นระบบหรือเป็นมาตรฐานสากล บุคลากรของหน่วยงานยังคงมีความเข้าใจในเรื่องเทคโนโลยีการรักษาความมั่นคงปลอดภัยในระดับต่ำ การทำธุรกรรมทางอิเล็กทรอนิกส์ยังคงขาดความเป็นมาตรฐาน หน่วยงานยังไม่มีการวางแผนฉุกเฉินและการฝึกอบรมเชิงปฏิบัติการเพื่อเตรียมความพร้อม รวมทั้งตัวบทกฎหมายยังไม่ครอบคลุมและไม่ชัดเจน

จะเห็นได้ว่าข้อกำหนดของมาตรฐานการรักษาความปลอดภัยของข้อมูลที่มีจำนวนมาก อาจทำให้กระบวนการทำงานและความซับซ้อนในการทำงานของทั้งผู้ใช้งานและผู้ดูแลระบบงานเพิ่มมากขึ้น ดังนั้น ผู้พัฒนาระบบการรักษาความปลอดภัยจึงควรคำนึงถึงความสมดุลระหว่างการรักษาความปลอดภัยและความคล่องตัวในการปฏิบัติงานด้วย (Gelbstein and Kamal, 2002) นอกจากความซับซ้อนของตัวมาตรฐานการรักษาความปลอดภัยข้อมูล ISO/IEC 17799 เองแล้ว Von Solms and Von Solms (2006) ได้แนะนำว่า องค์กรควรจะมีนโยบายการรักษาความปลอดภัยของข้อมูลอย่างชัดเจน การสื่อสารนโยบายออกไปเพื่อให้มีการนำนโยบายดังกล่าวมาปฏิบัติทั้งในระดับปฏิบัติการและระดับที่สูงกว่า รวมทั้งมีบุคลากรที่มีความรู้ความสามารถ มีแนวทางการปฏิบัติงานที่ดีและความตื่นตัวของบุคลากรที่เกี่ยวข้อง ซึ่งปัจจัยต่างๆ เหล่านี้จะสนับสนุนให้การนำมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 มาปฏิบัติในองค์กรประสบผลสำเร็จ

สมมติฐานของงานวิจัย

จากการศึกษาข้างต้น โดยเฉพาะอย่างยิ่ง การศึกษาการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลในหน่วยงานภาครัฐบาลของคณะอนุกรรมการความมั่นคงฯ ได้แสดงให้เห็นว่า แนวโน้มการทุจริตมีแนวโน้มสูงขึ้น สาเหตุส่วนหนึ่งมาจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ที่ก่อให้เกิดการทุจริตได้ง่ายขึ้น และในการทุจริตแต่ละครั้งก็มีความซับซ้อนมากกว่าในอดีตที่ผ่านมา แต่หน่วยงานในกำกับดูแลของภาครัฐบาลยังไม่มีแผนในการรักษาความปลอดภัยของข้อมูล ขาดความรู้ความเข้าใจในมาตรฐาน และไม่สามารถนำไปปรับใช้ภายในหน่วยงานได้อย่างมีประสิทธิภาพ งานวิจัยนี้จึงมีวัตถุประสงค์ที่จะสำรวจระดับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 ในส่วนของภาคเอกชน โดยเลือกกลุ่มเป้าหมายที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย เนื่องจากเป็นองค์กรที่มีความเกี่ยวข้องกับบุคคลและหน่วยงานอื่นเป็นจำนวนมากที่ใช้งบการเงินของบริษัท การไม่ปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลอาจส่งผลกระทบต่อความถูกต้องของข้อมูลภายในบริษัท ซึ่งท้ายที่สุดแล้วจะมีผลต่อความถูกต้องของงบการเงิน

เนื่องจากบริษัทจดทะเบียนในตลาดหลักทรัพย์ในประเทศไทยอยู่ภายใต้การกำกับดูแลของตลาดหลักทรัพย์แห่งประเทศไทยซึ่งได้กำหนดให้บริษัทจดทะเบียนทุกบริษัทต้องเปิดเผยการปฏิบัติตามหลักการกำกับดูแลกิจการที่ดี 15 ข้อ ตั้งแต่รอบระยะเวลาบัญชีสิ้นสุดวันที่ 31 ธันวาคม 2545 เป็นต้นไป ดังนั้น การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลจึงเป็นส่วนสนับสนุนให้บริษัทมีการกำกับดูแลกิจการที่ดี จึงคาดว่าบริษัทจดทะเบียนน่าจะมีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลอยู่ในระดับที่สูง ซึ่งจะแตกต่างจากผลสำรวจของหน่วยงานภาครัฐที่พบว่ามีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลในระดับที่ต่ำ โดยเขียนในรูปของสมมติฐานทางเลือก (Alternative Hypotheses) ได้ดังนี้

H_1 : บริษัทจดทะเบียนในตลาดหลักทรัพย์มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ในระดับที่สูง

สำหรับสมมติฐานในข้อที่ 2 อ้างอิงตามการศึกษาของ Von Solms (2001) ที่กล่าวว่า คุณภาพของข้อมูลขึ้นอยู่กับมาตรฐานที่ยึดปฏิบัติ ดังนั้น การพัฒนามาตรฐานให้มีคุณภาพมากขึ้นจะมีส่วนช่วยให้ข้อมูลมีความน่าเชื่อถือมากขึ้น สามารถเปรียบเทียบกันได้ระหว่างประเทศ ซึ่งเขียนในรูปของสมมติฐานทางเลือกได้ดังนี้

H_2 : การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 มีความสัมพันธ์ในทิศทางเดียวกันกับความน่าเชื่อถือของข้อมูล

ประชากรและการเก็บข้อมูล

ประชากรในงานวิจัยนี้คือ บริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ในช่วงปี พ.ศ. 2549-2550 จำนวน 472 บริษัท โดยเป็นการวิจัยเชิงสำรวจ เหตุผลที่เลือกสำรวจเฉพาะบริษัทจดทะเบียนนั้นเนื่องจากบริษัทจดทะเบียนได้รับการตรวจสอบทั้งในรูปแบบที่เป็นทางการและไม่เป็นทางการจากหน่วยงานกำกับดูแลและประชาชนทั่วไป รวมทั้งมีความพร้อมทางด้านทรัพยากร ซึ่งปัจจัยเหล่านี้น่าจะทำให้บริษัทจดทะเบียนนำมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 มาปฏิบัติมากกว่าหน่วยงานอื่น โดยผู้ที่ตอบแบบสอบถามคือผู้ตรวจสอบสารสนเทศของบริษัทจดทะเบียน

การกำหนดขนาดตัวอย่างใช้สูตรของ Yamane (1967) โดยกำหนดค่าความคลาดเคลื่อนที่ 5% และค่าความเชื่อมั่นที่ 95% ซึ่งได้ขนาดตัวอย่างขั้นต่ำที่ต้องการเท่ากับ 217 ตัวอย่าง ผู้วิจัยได้ส่งแบบสอบถาม 1 ชุดต่อ 1 บริษัทซึ่งการเลือกตัวอย่างได้มีการกระจายตัวอย่างให้ครอบคลุมบริษัทจดทะเบียนในตลาดหลักทรัพย์ ในทุกกลุ่มอุตสาหกรรม โดยแบบสอบถามแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1: เป็นการสอบถามข้อมูลทั่วไปของผู้ตอบแบบสอบถาม เช่น เพศ อายุ ระดับการศึกษา สาขาที่สำเร็จการศึกษา ประสบการณ์การทำงาน และกลุ่มธุรกิจของบริษัท

ส่วนที่ 2: เป็นการสอบถามเกี่ยวกับรายละเอียดของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 ว่าบริษัทจดทะเบียนมีการปฏิบัติตามมาตรฐานดังกล่าวในหัวข้อใดบ้าง (โดยแบ่งเป็น 3 ตัวเลือก คือ ทำ ไม่ทำ และไม่เกี่ยวข้อง) ระดับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 โดยรวม (1 = น้อยที่สุด จนถึง 5 = มากที่สุด) ความเพียงพอในการปฏิบัติตามมาตรฐาน รวมทั้งอุปสรรคที่ทำให้บริษัทไม่สามารถปฏิบัติตามมาตรฐานได้

ส่วนที่ 3: เป็นการสอบถามความเห็นของผู้ตรวจสอบสารสนเทศเกี่ยวกับระดับความน่าเชื่อถือของข้อมูลภายในบริษัท รวมทั้งปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูล ซึ่งระดับของความเห็นของผู้ตรวจสอบสารสนเทศจะแบ่งเป็น 5 ระดับ (1 = น้อยที่สุด จนถึง 5 = มากที่สุด)

ผลการวิเคราะห์ข้อมูล

ผู้วิจัยได้ส่งแบบสอบถามไปยังบริษัทจดทะเบียนและได้รับอนุญาตในตลาดหลักทรัพย์แห่งประเทศไทยจำนวน 300 บริษัท โดยส่งตรงถึงผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของบริษัทฯ เนื่องจากเป็นผู้ที่มีความรู้เกี่ยวกับเรื่องความน่าเชื่อถือของข้อมูลและการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลโดยตรงตามวัตถุประสงค์ของงานวิจัยนี้ และได้รับแบบสอบถามตอบกลับจำนวน 59 ฉบับ คิดเป็นร้อยละ 19.67 และเมื่อใช้สูตรของ Yamane เพื่อหาความคลาดเคลื่อนพบว่าได้ค่าความคลาดเคลื่อนเท่ากับร้อยละ 12.18 ดังนั้น ผลสรุปที่ได้จากกลุ่มตัวอย่างอาจจะไม่ได้เป็นตัวแทนของประชากรทั้งหมด

จากข้อมูลสรุปเกี่ยวกับผู้ตอบแบบสอบถามพบว่าผู้ตอบแบบสอบถามร้อยละ 49 มีประสบการณ์ทางด้านการตรวจสอบสารสนเทศไม่เกิน 5 ปี ส่วนอีกร้อยละ 51 มีประสบการณ์อยู่ในช่วง 6-10 ปี ผู้ตอบแบบสอบถามร้อยละ 78 สำเร็จการศึกษาในระดับปริญญาตรี และระดับ

ปริญญาโทร้อยละ 22 โดยสาขาที่สำเร็จร้อยละ 88 เป็นสาขาคอมพิวเตอร์โดยตรง ร้อยละ 7 เป็นด้านระบบสารสนเทศทางการบัญชี และด้านอื่นๆ ร้อยละ 5 นอกจากนี้ยังพบว่า ผู้ตอบแบบสอบถามร้อยละ 42 ทำงานอยู่ในกลุ่มอุตสาหกรรมธุรกิจการเงิน โดยเป็นกลุ่มตัวอย่างที่ตอบแบบสอบถามกลับมามากที่สุด ซึ่งอาจเป็นไปได้ว่ากลุ่มธุรกิจการเงินมีการใช้เทคโนโลยีสารสนเทศค่อนข้างมากในการดำเนินธุรกิจ จึงให้ความสำคัญกับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลเพื่อป้องกันภัยคุกคามที่อาจจะเกิดขึ้นจากบุคคลที่ไม่ประสงค์ดีทั้งภายใน และภายนอกองค์กร อันจะมีผลทำให้การดำเนินธุรกิจหยุดชะงัก และเกิดความเสียหายจากภัยคุกคามดังกล่าว แบบสอบถามร้อยละ 17 มาจากกลุ่มอุตสาหกรรมบริการ ร้อยละ 15 และร้อยละ 12 มาจากกลุ่มอุตสาหกรรมเทคโนโลยีและกลุ่มอุตสาหกรรมทรัพยากรตามลำดับ

ตารางที่ 1 แสดงภาพรวมของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ใน 11 หัวข้อหลัก ซึ่งผู้ตอบแบบสอบถามทั้งหมดเห็นว่ามาตรฐานการรักษาความปลอดภัยนั้งกล่าวมีความเกี่ยวข้องกับองค์กรของตน เพียงแต่องค์กรจะนำมาปฏิบัติครบทุกหัวข้อหรือไม่เท่านั้น จากผลของแบบสอบถามพบว่า หัวข้อของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลมากที่สุด 4 อันดับประกอบด้วย การรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้องกับบุคลากร การรักษาความปลอดภัยของข้อมูลทางกายภาพ การบริหารจัดการการสื่อสาร และการควบคุมการเข้าถึงระบบสารสนเทศขององค์กร คิดเป็นร้อยละ 100 ร้อยละ 98.3 เป็นด้านการบริหารจัดการทรัพย์สินขององค์กร ด้านการปฏิบัติตามข้อกำหนดร้อยละ 94.9 และด้านการจัดทำนโยบายการรักษาความปลอดภัยของข้อมูล ร้อยละ 91.5

ตารางที่ 1 สัดส่วนการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัย	มี (%)	ไม่มี (%)
1. นโยบายการรักษาความปลอดภัยของข้อมูล	91.5	8.5
2. โครงสร้างทางด้านการรักษาความปลอดภัยของข้อมูลสำหรับองค์กร	88.1	11.9
3. การบริหารจัดการทรัพย์สินขององค์กร	98.3	1.7
4. การรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้องกับบุคลากร	100	-
5. การรักษาความปลอดภัยของข้อมูลทางกายภาพ	100	-
6. การบริหารจัดการการสื่อสาร	100	-
7. การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร	100	-
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	71.2	28.8
9. การบริหารจัดการช่องโหว่นฮาร์ดแวร์และซอฟแวร์	59.3	40.7
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร	66.1	33.9
11. การปฏิบัติตามข้อกำหนด	94.9	5.1

จากผลการทดสอบค่าเฉลี่ยของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลเพื่อทดสอบสมมติฐานที่ 1 ว่าบริษัทจดทะเบียนในตลาดหลักทรัพย์มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ในระดับที่สูงหรือไม่ พบว่าค่าเฉลี่ยของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลเท่ากับ 3.83 จากนั้น ผู้วิจัยได้กำหนดเกณฑ์เปรียบเทียบสำหรับใช้ในการทดสอบระดับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลดังนี้

1 = มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในระดับต่ำที่สุด
2 = มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในระดับต่ำ
3 = มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในระดับปานกลาง
4 = มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในระดับสูง
5 = มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยอยู่ในระดับสูงที่สุด

และเมื่อนำค่าเฉลี่ยมาเปรียบเทียบกับเกณฑ์ที่กำหนดไว้โดยใช้วิธี One Sample T-Test พบว่า กลุ่มตัวอย่างมีระดับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ในระดับปานกลาง ดังนั้นจึงปฏิเสธสมมติฐานที่ 1 ที่ว่าว่าบริษัทจดทะเบียนในตลาดหลักทรัพย์มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ในระดับที่สูง

นอกจากนี้ จากการสอบถามความคิดเห็นของผู้ตรวจสอบสารสนเทศเกี่ยวกับข้อจำกัดของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เห็นว่าการขาดความร่วมมือของหน่วยงานภายในองค์กรเป็นอุปสรรคที่สำคัญที่สุด รองลงมาคือความซับซ้อนของตัวมาตรฐาน และบุคลากรขาดความรู้เกี่ยวกับมาตรฐาน ซึ่งสอดคล้องกับบทความของดวงกมล ทรัพย์พิทยากร (2548) ที่มีข้อคิดเห็นว่า ข้อกำหนดจำนวนมากของมาตรฐานการรักษาความปลอดภัยของข้อมูล อาจทำให้กระบวนการทำงานและความซับซ้อนในการทำงานของทั้งผู้ใช้งานและผู้ดูแลระบบงานเพิ่มมากขึ้น อย่างไรก็ตาม แม้ว่าผู้ตอบแบบสอบถามจะเห็นว่าปัญหาเรื่องการขาดงบประมาณเป็นเรื่องที่สำคัญ แต่ปัญหาดังกล่าวก็ไม่ได้เป็นอุปสรรคที่สำคัญมากไปกว่าปัญหาอื่นๆ แสดงให้เห็นว่าบริษัทจดทะเบียนน่าจะมีความพร้อมทางด้านทรัพยากรที่จะสนับสนุนการนำมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 มาประยุกต์ใช้งาน นอกจากนี้ ผลการศึกษาข้างต้นยังสอดคล้องกับงานวิจัยของ Warren (2002) ที่พบว่าการที่บุคลากรขาดความรู้เป็นอุปสรรคที่ทำให้องค์กรไม่มีการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ค่าเฉลี่ยระดับความสำคัญของข้อจำกัด (1 = สำคัญน้อยที่สุด จนถึง 5 = สำคัญมากที่สุด) แสดงในตารางที่ 2

ตารางที่ 2 อุปสรรคในการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล

ปัจจัยที่มีผลต่อการปฏิบัติตามมาตรฐานฯ	ค่าเฉลี่ย
การขาดความร่วมมือของหน่วยงานภายในองค์กร	4.74
ความซับซ้อนของมาตรฐาน	4.56
การขาดความรู้ความสามารถของบุคลากร	4.53
การไม่ให้ความสำคัญของผู้บริหาร	4.36
การขาดงบประมาณ	4.29

ในการทดสอบสมมติฐานที่ 2 ผู้วิจัยได้ทดสอบความสัมพันธ์โดยการใช้การทดสอบ Correlation ระหว่างระดับการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 โดยรวมซึ่งมีค่าเฉลี่ยเท่ากับ 3.82 กับระดับความน่าเชื่อถือของข้อมูลภายในองค์กรในมุมมองของผู้ตรวจสอบสารสนเทศซึ่งมีค่าเฉลี่ยเท่ากับ 4.04 พบว่า ทั้งสองตัวแปรไม่มีความสัมพันธ์กันอย่าง

มีนัยสำคัญ ซึ่งอาจเป็นไปได้ว่ามาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 นั้น ประกอบด้วยข้อปฏิบัติที่แตกต่างกันหลายข้อ บางข้อปฏิบัติไม่ได้มีความสัมพันธ์โดยตรงกับข้อมูล เป็นแต่เพียงข้อปฏิบัติพื้นฐาน ซึ่งเป็นแนวทางกว้างๆ ในทางปฏิบัติเท่านั้น การปฏิบัติตามข้อกำหนดพื้นฐานจึงอาจไม่มีผลทำให้ความน่าเชื่อถือของข้อมูลเพิ่มขึ้นอย่างเป็นสาระสำคัญ

สำหรับคำถามที่ว่าในมุมมองของผู้ตรวจสอบสารสนเทศ ปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูลประกอบด้วยปัจจัยอะไรบ้างและมีความสำคัญมากน้อยเพียงใดนั้น ค่าเฉลี่ยของระดับความสำคัญ (1 = สำคัญน้อยที่สุด จนถึง 5 = สำคัญมากที่สุด) ของปัจจัยดังกล่าวแสดงในตารางที่ 3

ตารางที่ 3 ปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูล

ปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูล	ค่าเฉลี่ย
โปรแกรมเมอร์สามารถแก้ไขข้อมูลด้วยตนเอง	4.52
การแบ่งแยกหน้าที่ไม่เหมาะสม	4.41
โปรแกรมเมอร์สามารถแก้ไขโปรแกรมต้นแบบได้	4.29
การขาดการกำหนดสิทธิ์การเข้าถึงข้อมูล	4.13
การใช้รหัสผ่านร่วมกัน	3.51
การขาดการสำรองข้อมูล	3.02

จากตารางที่ 3 จะเห็นได้ว่า ปัจจัยสำคัญที่ทำให้ความน่าเชื่อถือของข้อมูลลดลงอย่างมากคือ การที่โปรแกรมเมอร์สามารถแก้ไขข้อมูลได้ด้วยตนเอง รองลงมาคือ การแบ่งแยกหน้าที่ความรับผิดชอบที่ไม่เหมาะสม การที่โปรแกรมเมอร์สามารถแก้ไขโปรแกรมต้นแบบได้ และการที่องค์กรไม่มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูล ซึ่งปัจจัยดังกล่าวข้างต้นเป็นปัจจัยที่ส่งผลต่อข้อมูลโดยตรง ดังนั้น ในการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเพื่อให้ได้มาซึ่งความน่าเชื่อถือของข้อมูลในระดับที่สูงนั้น องค์กรจึงควรให้ลำดับความสำคัญสำหรับข้อปฏิบัติที่ส่งผลต่อข้อมูลโดยตรงเพื่อให้เกิดประสิทธิภาพในการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลมากที่สุด

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้มีวัตถุประสงค์ เพื่อศึกษาถึงการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ของบริษัทจดทะเบียนและรับอนุญาตในตลาดหลักทรัพย์แห่งประเทศไทย ความสัมพันธ์ของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 กับความถูกต้องน่าเชื่อถือของข้อมูลสารสนเทศ รวมถึงข้อจำกัดของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล และปัจจัยที่มีผลต่อความน่าเชื่อถือของข้อมูล โดยรวบรวมข้อมูลจากผู้ตรวจสอบสารสนเทศของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ผลการวิจัยสรุปได้ว่า บริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศ โดยภาพรวมแล้วมีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO/IEC 17799 ในระดับปานกลาง ซึ่งผลการวิจัยนี้จะแตกต่างจากผลการวิจัยของโครงการจัดทำแผนแม่บทการรักษาความปลอดภัยของข้อมูลแห่งชาติ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในปี พ.ศ. 2549 ซึ่งพบว่าหน่วยงานของภาครัฐบาลมีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ในระดับที่ต่ำ ซึ่งอาจเป็นไปได้ว่าบริษัทจดทะเบียนซึ่งเป็นองค์กรภาคเอกชนมีความพร้อมในด้านทรัพยากรมากกว่าหน่วยงานรัฐบาล อย่างไรก็ตาม ก็ยังคงมีอุปสรรคที่ทำให้องค์กรไม่สามารถปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลได้ ซึ่งข้อจำกัดดังกล่าวได้แก่ การขาดความร่วมมือของหน่วยงานภายในองค์กร มาตรฐานการรักษาความปลอดภัยของข้อมูลมีความซับซ้อน และบุคลากรยังไม่มีความรู้ความสามารถอย่างเพียงพอ ปัจจัยดังกล่าวส่งผลให้ยังไม่มีการนำมาตรฐานการรักษาความปลอดภัยของข้อมูลมาปฏิบัติกันอย่างจริงจัง ดังนั้น นอกจากหน่วยงาน

ที่ปฏิบัติควรจะทางแก้ไขปัญหาดังกล่าวเพื่อให้ข้อมูลของบริษัทมีความน่าเชื่อถือได้มากขึ้นกว่าที่เป็นอยู่ อันจะเป็นประโยชน์ในการวางแผนพัฒนาธุรกิจ และการแข่งขันแล้ว หน่วยงานที่มีหน้าที่รับผิดชอบในการกำหนดมาตรฐานควรจะพิจารณาด้วยว่าข้อกำหนดต่างๆ นั้นมีความซับซ้อนเกินไปหรือไม่ และควรมีการประชาสัมพันธ์เพื่อให้ความรู้กับองค์กรต่างๆ อย่างกว้างขวาง

นอกจากนี้ ผลการวิจัยยังพบอีกว่าการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ไม่ได้มีความสัมพันธ์กับความน่าเชื่อถือของข้อมูลอย่างมีนัยสำคัญ ดังนั้น การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 ทั้งหมดนั้นจึงไม่ได้เป็นหลักประกันเพียงอย่างเดียวที่จะทำให้ข้อมูลขององค์กรมีความน่าเชื่อถือ ยังคงมีปัจจัยอื่นที่ส่งผลต่อความน่าเชื่อถือของข้อมูล ดังนั้น นอกจากการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 แล้ว บุคลากรในองค์กรควรมีความระมัดระวังในการใช้ข้อมูล หรือมีความตื่นตัวในการป้องกันความเสี่ยงที่อาจจะเกิดขึ้นด้วย

อย่างไรก็ตาม งานวิจัยนี้ยังคงมีข้อจำกัดเนื่องจากแบบสอบถามที่ตอบกลับมีจำนวนค่อนข้างน้อย ข้อมูลที่ได้จึงอาจจะไม่ได้เป็นตัวแทนที่ดีของประชากรบริษัทจดทะเบียนทั้งหมด ดังนั้น ผลการวิจัยจึงทำให้เห็นภาพของการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 เพียงคร่าวๆ เท่านั้น ผู้ที่สนใจสามารถนำงานวิจัยนี้ไปพัฒนาต่อเพื่อให้ได้กลุ่มตัวอย่างที่มากขึ้น รวมถึงขยายการศึกษาไปถึงบริษัทเอกชนจำกัดหรือมีการแยกเฉพาะเจาะจงตามกลุ่มอุตสาหกรรม เนื่องจากแต่ละอุตสาหกรรมอาจจะให้ความสำคัญของเทคโนโลยีสารสนเทศไม่เท่ากัน เพื่อให้ได้ข้อมูลที่เป็นประโยชน์สำหรับการสนับสนุนให้มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูลมากขึ้น

บรรณานุกรม

ภาษาไทย

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2549), มาตรฐาน... การรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2)

ดวงกมล ทรัพย์พิทยากร. (2548), "ISO 17799 อดีต ปัจจุบัน และอนาคต", www.thaicert.nectec.or.th (As of July, 2005)

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2549), โครงการจัดทำแผนแม่บท ICT Security แห่งชาติ, บทที่ 3 สถานภาพด้านความมั่นคงปลอดภัย ICT, กรุงเทพมหานคร หน้า 12-15.

ISO 17799 (BS 7799) ความมั่นคงปลอดภัยจากภาครัฐสู่ภาครัฐ http://www.gits.net.th/ knowledge/ newsletter/ittalk/index.asp?MenuID=26&SubMenuID=8&Book=9> (As of February, 2007)

ภาษาอังกฤษ

Bisson, J. (2005), "The BS 7799/ISO17799 Standard for a Better Approach to Information Security", **White Paper: Information Security Analyst,** Callio Technologies.

Calder, A. (2006), "Information Security Based on ISO 27001/ISO 17799: A Management Guide", Chief Editor: Jan van Bon, Van Haren Publishing.

Gelbstein, K. and Kamal, A. (2002), "Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security", **United Nations ICT Task Force and the United Nations Institute for Training and Research,** New York: 47-59.

Gerber, M, and Von Solms, R. (2001), "From Risk Analysis to Security Requirements", **Computers & Security,** Vol. 20 (7): 577-584.

http://en.wikipedia.org/wiki/Computer_fraud_case_studies (As of January, 2007)

Humphreys, E.J., Moses, R.H., and Plate, E.A. (1998), "Guide to BS7799 Risk Assessment and Management", British Standards Institution.

International Organization for Standardization. (2005), "International Standard ISO/IEC 27001", First Edition.

Ritchie R.L. and Brindley C.S. (2001), "The Information-Risk Conundrum", **Marketing Intelligence and Planning,** Vol.19 (1): 29-37.

Sanderson, E and Forcht, K.A. (1996), "Information Security in Business Environments", **Information Management Computer Security,** Vol. 4 (1): 32-37.

Thompson, D. (1998), "1997 Computer Crime and Security Survey", **Information Management & Computer Security,** Vol. 6 (2): 78-101.

Von Solms, S.H. (2001), "Corporate Governance and Information Security", **Computers & Security,** Vol. 20 (3): 215-218.

Von Solms, S.H. and Von Solms, R. (2006), "Information Security Governance: A Model Based on the Direct-Control Cycle", **Computers & Security,** Vol. 26 (6): 408-412.

Warren, M.J. (2002), "Security Practice: Survey Evidence from Three Countries", **Logistics Information Management,** Vol. 15 (5/6): 347-351.

Yamane, T. (1967), Statistics: An Introductory Analysis 2nd edition. New York: Harper & Row.

Ziegenfuss, D.E. (1995), "State and Local Government Fraud Survey for 1995", **Managerial Auditing Journal,** Vol. 11 (9): 50-55.