บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องจากปัจจุบันโครงสร้างและวิธีการดำเนินงานของแต่ละองค์กร มีการทำธุรกรรมแบบ e-Business และมีการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกันในรูปแบบ EDI - Electronic Data Interchangeมากขึ้น ทำให้องค์กรต้องมีการปรับเปลี่ยนเพื่อรองรับการขยายตัวที่เป็นแบบเครือข่ายและการดำเนินธุรกิจแบบไร้พรมแดน (e-Organization)

ดังนั้นคอมพิวเตอร์และอินเทอร์เน็ตจึงกลายเป็นสิ่งสำคัญต่อการเปลี่ยนแปลงดังกล่าว ทั้งวิธีการและรูปแบบของการดำเนินกิจกรรมในการทำงาน โดยเฉพาะการดำเนินกิจกรรมต่าง ๆ ผ่านเว็บไซต์ ที่ก่อให้เกิดรูปแบบการทำการค้า(e-Commerce) และการให้บริการ (e-Service) โดยผ่านอินเทอร์เน็ต เนื่องจากอินเทอร์เน็ตมีการกระจายครอบคลุมและเข้าถึงเกือบทุกพื้นที่ทั่วโลก

การรักษาความมั่นคงปลอดภัยของข้อมูลสำหรับองค์กรจึงสำคัญมาก เพราะความเสี่ยงและปัญหาส่วนใหญ่ที่ตามมานั้นส่งผลกระทบต่อการพัฒนาและผลประโยชน์ขององค์กรอย่างมาก เช่น ปัญหาในเรื่องการบุกรุกจากผู้ที่ไม่ได้รับอนุญาต ,ปัญหาในเรื่องความลับความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ,ปัญหาเรื่องไวรัส หนอนอิเล็กทรอนิกส์ และอีกหลายปัญหาที่เกิดขึ้นในปัจจุบัน เพราะยิ่งมีการเปิดกว้างและมีการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตเข้ามาใช้งานมากเท่าใด องค์กรก็ยิ่งมีความเสี่ยงที่จะเปิดช่องให้แก่บุคคลอื่นหรือโปรแกรมต่างๆที่ประสงค์ร้าย ทั้งจากภายในและภายนอก บุกรุกเข้ามาเพื่อขโมย หรือแก้ไขข้อมูล ทำให้ระบบการทำงานขององค์กรต้องหยุดชะงักและอาจใช้งานไม่ได้

การรับมือกับความเสี่ยงเหล่านี้ขององค์กรด้วยการติดตั้งระบบรักษาความปลอดภัย เช่น Firewall, ระบบป้องกันผู้บุกรุก (Intrusion-detection) และระบบป้องกันไวรัส นั้นไม่เพียงพอ องค์กรจึงควรมีการนำเอามาตรฐาน การบริหารความปลอดภัยของข้อมูลอย่าง BS7799 – ISO/IEC 17799 เข้ามาประยุกต์ใช้กับกระบวนการทางธุรกิจขององค์กร เพื่อให้องค์กรเกิดความมั่นคงปลอดภัยและเป็นการสร้างมาตรฐานให้ตัวองค์กรเอง

เพราะปัจจุบันในประเทศไทยคณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2546 ได้นำมาตรฐาน ISO/IEC 17799หรือ BS7799 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย จำนวน 144 ข้อ เพื่อให้เป็นแนวทางเสริมสร้างการรักษาความปลอดภัยให้กับองค์กรหรือหน่วยงานที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์

โดยเฉพาะสำหรับองค์กรที่ให้บริการเรื่องการจัดซื้อออนไลน์(e-Procurement) หรือองค์กรที่เป็นตลาดกลางอิเล็กทรอนิกส์ ที่ต้องให้ความสำคัญอย่างมากใน เรื่องการป้องกันการเข้าถึงข้อมูลของลูกค้า, ความปลอดภัยด้านระบบที่ให้บริการและการสำรองข้อมูลฯลฯ เพราะเป็นองค์กรที่เสี่ยงต่อการบุกรุก เนื่องจากธุรกรรมต่างๆที่ให้บริการนั้นส่วนใหญ่ให้บริการผ่านช่องทางทางอินเตอร์เน็ต

ดังนั้นผู้วิจัยจึงจะทำการศึกษาถึงความเสี่ยงต่างๆที่จะเกิดขึ้นกับผู้ให้บริการในธุรกิจดังกล่าวจากกรณีศึกษาของบริษัท A จำกัด ซึ่งเป็นบริษัทผู้นำด้านการให้บริการด้านการจัดซื้อออนไลน์ในประเทศไทย และหาแนวทางการประยุกต์ใช้มาตรฐานการบริหารความปลอดภัยของข้อมูล BS7799 – ISO/IEC 17799 เพื่อลดความเสี่ยงที่อาจเกิดขึ้น เพื่อเตรียมความพร้อมและเตรียมป้องกันปัญหาจากผู้ไม่ประสงค์ดี รวมทั้งเพื่อสร้างความได้เปรียบในการแข่งขันให้แก่บริษัทได้อีกด้วยอีกทั้งเป็นการรองรับกฎหมายต่างๆที่กำลังจะถูกประกาศใช้ในอนาคต และสุดท้ายคือเพื่อเป็นแนวทางในการพัฒนาและปรับปรุงคุณภาพอย่างต่อเนื่องต่อไป โดยใช้ตัวชี้วัดมาตรฐานตาม ระบบ ISO17799:2000

1.2 วัตถุประสงค์งานวิจัย

1. เพื่อทำการศึกษาแนวทางขั้นตอนการดำเนินงาน สำหรับการประยุกต์ใช้มาตรฐานสากล ISO 17799 ในการรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์และระบบสารสนเทศในองค์กรที่ให้บริการด้านการจัดซื้อออนไลน์(e-Procurement)

2. เพื่อทำการศึกษาปัจจัยที่มีผลต่อความเสี่ยงด้านความปลอดภัยของข้อมูลที่อาจเกิดขึ้นกรณีที่องค์กรขาดการป้องกัน

3. เพื่อนำผลที่ได้สรุปแก่ผู้บริหารขององค์กร สำหรับนำไปจัดทำนโยบายเพิ่มเติมและปรับปรุงองค์กรเพื่อให้เหมาะสมกับการพัฒนาทางธุรกิจที่องค์กรเป็น

1.3 ขอบเขตการวิจัย

1. การวิจัยนี้มุ่งทำการศึกษาแนวทางการประยุกต์ใช้ข้อกำหนดของมาตรฐาน ISO 17799 กับองค์กรที่ให้บริการด้านการจัดซื้อออนไลน์(e-Procurement) เพื่อพัฒนาศักยภาพในการบริหารความปลอดภัยของข้อมูล

2. การวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นได้กับข้อมูลและระบบสารสนเทศ โดยตัวชี้วัด (KPI) ที่ใช้ในการวัดผล จะพิจารณาตามหลักของ ISO 17799 โดยจะทำการวัดผลในด้านการดำเนินงานขององค์กร

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อทราบรายละเอียดมาตรฐานการบริหารความปลอดภัยของข้อมูลตามมาตรฐานสากลอย่าง ISO 17799

2. เพื่อทราบแนวทางการปฏิบัติที่เหมาะสมเพื่อองค์กรได้นำหลัก ISO 17799 มาประยุกต์ใช้ในการรักษาและป้องกัน ความปลอดภัยให้แก่ข้อมูลและระบบสารสนเทศขององค์กร รวมทั้งเพื่อลดความเสี่ยงต่างๆที่อาจเกิดขึ้นได้ต่อข้อมูลและทรัพย์สิน เพื่อองค์กรสามารถดำเนินธุรกิจและธุรกรรมได้โดยไม่ติดขัด

3. เพื่อเตรียมความพร้อมในการรองรับการประกาศใช้มาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

4. เพื่อสร้าง "Good Image and Reputation" เสริมภาพลักษณ์แก่องค์กรให้ดียิ่งขึ้น เพราะการนำระบบบริหารดังกล่าวมาใช้จึงถือเป็นสัญญาณที่ว่าเป็นองค์กรที่มีคุณภาพ

5. เพื่อเป็นการเตรียมความพร้อมในการแข่งขันกับผู้ให้บริการต่างชาติรายอื่น และเพื่อเป็นมาตรฐานการให้บริการในอนาคตด้วย ในการให้บริการลูกค้าที่มีมาตรฐาน ISO