บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในยุคปัจจุบัน รูปแบบการทำงานขององค์กรเกือบทุกแห่งทั่วโลกเกิดความเปลี่ยนแปลงจากเดิมไปเป็นอย่างมาก ด้วยความก้าวหน้าของเทคโนโลยีส่งผลให้คอมพิวเตอร์ อุปกรณ์เทคโนโลยีสารสนเทศ และระบบต่างๆ เข้ามามีบทบาทสำคัญต่อกระบวนการทางธุรกิจอย่างหลีกเลี่ยงไม่ได้ ปรากฏการณ์เช่นนี้ส่งผลให้แนวโน้มในการดำเนินธุรกิจและความอยู่รอดขององค์กรจึงต้องพึ่งพาระบบเทคโนโลยีสารสนเทศมากขึ้น

ทั้งนี้ อุตสาหกรรมวิทยุ และโทรทัศน์เองก็นับว่ามีการพึ่งพาเทคโนโลยีมากยิ่งขึ้นเช่นเดียวกัน ตัวอย่างเช่น ต้องการอาศัยช่องทางในการติดต่อสื่อสาร เพิ่มช่องทางในการส่งภาพข่าวจากนักข่าวที่อยู่ตามสถานที่ต่างๆ เข้ามายังสถานีเพื่อนำไปใช้ในการออกอากาศได้ในระยะเวลาที่รวดเร็ว

ความเสี่ยงที่มีผลต่อความมั่นคงปลอดภัยของข้อมูล รวมไปถึงระบบสารสนเทศภายในองค์กร นอกจากจะมาสิ่งที่กล่าวไปแล้วข้างต้นนั้น อย่างมีสาเหตุมาจากภัยธรรมชาติ การจลาจล อุบัติเหตุ เหตุการณ์ร้ายแรงต่างๆ ที่ไม่คาดคิดสามารถเกิดขึ้นได้ตลอดเวลา ซึ่งบางเหตุการณ์ก็อยู่เหนือการควบคุมและป้องกันขององค์กร เพื่อให้องค์กรสามารถฝ่าวิกฤติที่เกิดขึ้นและสามารถกลับมาดำเนินธุรกิจได้อีกครั้ง องค์กรจึงต้องพิจารณาเตรียมการ และวางแผนเพื่อรับมือไว้ล่วงหน้า

กล่าวโดยสรุปจะเห็นได้ว่าภัยที่เกิดขึ้นกับตัวเรานั้น สาเหตุหลักมาจากการที่เราละเลยไม่ได้ใส่ใจให้ความสำคัญเรื่องความปลอดภัยข้อมูลหรือ "Information Security" อย่างเพียงพอ ทำให้เป็นต้นเหตุให้ปัญหาอีกหลายๆอย่างตามมา โดยเฉพาะถ้าเป็นความใส่ใจของผู้บริหารระดับสูงขององค์กรแล้ว ก็ยิ่งส่งผลกระทบต่อความปลอดภัยข้อมูลระบบสารสนเทศขององค์กรอย่างหลีกเลี่ยงไม่ได้ ดังนั้น การให้ความรู้ หรือ "Educate" ทุกคนตั้งแต่ ผู้บริหารระดับสูง, ผู้บริหารระดับกลาง, ผู้บริหารระบบ, ผู้ตรวจสอบภายใน รวมถึงผู้ใช้คอมพิวเตอร์ "ทุกคน" ในองค์กร ให้ "ตระหนัก" และ "เข้าใจ" ถึงภัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลภายในองค์กร

ดังนั้น ผู้จัดทำ จึงตระหนักถึงความสำคัญดังกล่าว จึงเพื่อจัดทำระบบในการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศขององค์การกระจายเสียงและแพร่ภาพสาธารณะ

คือ มาตรฐาน ISO 27001:2005 และมาตรฐาน ISO 17799:2005 หรือที่รู้จักกันในชื่อเดิมว่า BS 7799 มาตรฐานนี้เป็นมาตรฐานที่ได้รับการยอมรับและมีการนำไปประยุกต์ใช้งานในประเทศต่างๆ ทั่วโลก เนื้อหาของมาตรฐานมุ่งเน้นที่การรักษาความมั่นคงปลอดภัยให้กับข้อมูล ซึ่งถือเป็นทรัพย์สินที่สำคัญที่สุดขององค์กรจากความเสี่ยงหรือภัยคุกคามต่างๆ ที่อาจเกิดขึ้นต่อข้อมูลและอาจส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรได้ เช่น ภัยจากแฮกเกอร์ ภัยจากโปรแกรมมุ่งร้ายต่างๆ ภัยจากการขาดทักษะของพนักงาน

ถึงแม้ว่า องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย จะเป็นองค์กรที่ไม่แสวงหาผลกำไร หรือต้องแข่งขันกับคู่แข่งในเชิงธุรกิจ แต่เพื่อสอดคล้องกับวัตถุประสงค์ของการก่อตั้ง ตาม

พระราชบัญญัติองค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย พ.ศ. 2551 มาตรา 8 โดยมีใจความว่า

(๑) จัดให้มีสถานีวิทยุกระจายเสียงและสถานีวิทยุโทรทัศน์ หรือเผยแพร่รายการในระบบอื่นหรือเทคโนโลยีทันสมัยอื่น โดยมีเครือข่ายให้บริการครอบคลุมพื้นที่ทั่วประเทศหรือให้มีสถานีวิทยุกระจายเสียงและสถานีวิทยุโทรทัศน์เพิ่มเติมเป็นเครือข่าย ไม่เก็บค่าสมาชิกและไม่หารายได้จากการโฆษณา เว้นแต่เป็นการสนับสนุนจากผู้สนับสนุนองค์การ

(๒) ให้บริการผลิตสื่อโสตทัศน์ หรือบริการระบบเครือข่ายสารสนเทศอื่น หรือบริการอื่นใดที่เกี่ยวข้องหรือเป็นประโยชน์ต่อการเผยแพร่รายการ

และเพื่อให้รองรับกับการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งได้มีการประกาศใช้ไปแล้วเมื่อวันที่ 18 มิถุนายน 2550 และมีผลบังคับใช้ ไปเมื่อวันที่ 18 กรกฎาคม 2550 และทางองค์การฯ เองก็อยู่ในขอบข่ายที่ต้องมีการปฏิบัติตาม ภาคผนวก แนบท้ายกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

ประเภท ข . ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)
ประเภท ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)

ดังนั้น องค์การฯ จึงมีความจำเป็นที่จะต้องมีการนำมาตรฐาน ISO/IEC27001 เข้าเป็นตัวช่วยในการสร้างนโยบายทางด้านความปลอดภัยของข้อมูล และเพื่อรองรับการตรวจสอบระบบทั้งจากภายใน (Internal Audit) และภายนอก (External Audit) ประกอบกับองค์การจะต้องเป็นองค์การที่ต้องมีการตรวจสอบการทำงาน และมาตรฐาน ISO/IEC 27001 เอง ก็ถือว่าเป็นมาตรฐานที่ได้รับการยอมรับกันทั่วโลก ในด้านของการกำหนดนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

วัตถุประสงค์ในการวิจัย

1. เพื่อสร้างแนวทางปฏิบัติทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศภายในองค์กร
2. เพื่อพัฒนาองค์กรในมุ่งสู่ความเป็นมาตรฐาน ISO/IEC 27001
3. เพื่อกำหนดแนวทางในการดำเนินงาน รวมถึงขั้นตอนในการตรวจสอบระบบสารสนเทศขององค์กร เพื่อให้รองรับกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2551
4. เพื่อให้ระบบรักษาความปลอดภัยของข้อมูลสารสนเทศภายในองค์กรมีความมั่นคงมากยิ่งขึ้น

ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถทราบถึงรายละเอียดมาตรฐานการบริหารความปลอดภัยของข้อมูลตามมาตรฐานสากล ISO/IEC 27001
2. สามารถทราบถึงแนวทางการปฏิบัติที่เหมาะสมเพื่อให้องค์กรนำหลัก ISO/IEC 27001 มาประยุกต์ใช้ในการแนวทางในการกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูล เพื่อลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นต่อข้อมูลภายในองค์กร

ขอบเขตของงานวิจัย

1. ขอบเขตด้านเนื้อหา การวิจัยครั้งนี้มุ่งทำการศึกษาแนวทางในการกำหนดนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ภายในองค์กรโดยการปฏิบัติตาม IT Best Practice ตามกรอบแนวความคิดของมาตรฐาน ISO27001

2. ขอบเขตด้านประชากร โดยประชากรที่ใช้ในการวิจัยครั้งนี้ จะถูกแบ่งเป็น 2 ส่วน คือ

ส่วนที่ 1 : กลุ่มคณะผู้บริหาร หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ หัวหน้าฝ่ายบริหารงานทั่วไป และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ ขององค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย

หน้าที่ของประชากรในแต่ละกลุ่มในส่วนที่ 1

1. <u>กลุ่มคณะผู้บริหาร</u> มีหน้าที่ในการตัดสินใจเกี่ยวกับการออกนโยบายในด้านต่างๆ และมีบทบาทในการผลักดันให้นโยบายมีผลบังคับใช้

2. <u>หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์</u> มีหน้าที่ในการออกกฎระเบียบที่เกี่ยวกับการจ้างงาน หรือการระบุเกี่ยวกับบทลงโทษ ไว้ในสัญญาจ้างงาน

3. <u>หัวหน้าฝ่ายบริหารงานทั่วไป</u> มีหน้าที่ในการดูแลความเรียบร้อยทางด้านกายภาพ ทางด้านการรักษาความปลอดภัยในการเข้า – ออกสำนักงาน และช่วยตรวจสอบในการนำของเข้า – ออกจากองค์การฯ

4. <u>หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ</u> มีหน้าที่ในการดูแลระบบสารสนเทศภายในองค์การฯ ให้เป็นไปอย่างมั่นคงปลอดภัย และให้การดำเนินงานในส่วนต่างๆ เป็นไปตามมาตรฐานสากล

ส่วนที่ 2 : พนักงานทั้งหมดขององค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทยโดยใช้ข้อมูลจำนวนพนักงาน ณ สิ้นเดือนสิงหาคม 2551 จากฝ่ายบริหารทรัพยากรบุคคล จำนวนทั้งสิ้น 750 คน ซึ่งจะแบ่งกลุ่มของประชากรออกเป็น 2 กลุ่ม คือ

กลุ่มที่ 1 กลุ่มพนักงานฝ่ายปฏิบัติการเครือข่ายและสารสนเทศขององค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย ที่เกี่ยวข้องต่อการนำ IT Best Practice มาประยุกต์ใช้กับงานให้บริการด้านเทคโนโลยีสารสนเทศขององค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย

กลุ่มที่ 2 กลุ่มพนักงานทั่วไป ที่เป็นผู้ใช้งานระบบเครือข่ายขององค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย

นิยามศัพท์

“องค์การฯ” หมายความว่า องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย

Methodologies หมายความว่า ขั้นตอน หรือ วิธีการในการบริหารความเสี่ยงอย่างถูกต้องตามหลักการมาตรฐานสากลที่ทั่วโลกยอมรับและนำมาประยุกต์ใช้กันโดยทั่วไป

Framework หมายความว่า กรอบแนวความคิด ขั้นตอน หรือ วิธีการที่ช่วยให้องค์กรได้ "Compliance" ตามหลักการมาตรฐานสากล ยกตัวอย่าง เช่น ถ้าพูดถึงการควบคุมภายใน หรือ "Internal Control" ก็จะหมายถึง COSO Framework หรือ Corporate Governance แต่ถ้าพูดถึง "IT Governance" ก็จะหมายถึง CobiT Framework ที่กำหนดขอบเขตแคบลงมาเจาะลึกในส่วนของระบบสารสนเทศ และ ถ้ากล่าวถึง Information Security Management System หรือ ISMS จะหมายถึง มาตรฐานสากล ISO/IEC 27001 (ชื่อเดิม ISO/ IEC 17799) นั่นเอง

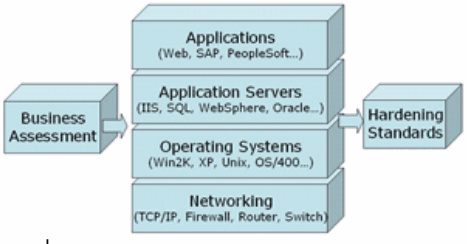
Hardening หมายความว่า กระบวนการในการรักษาความปลอดภัยให้กับระบบแบบลงลึกในรายละเอียด แบ่งออกเป็น 3 ส่วนสำคัญ คือ Hardening People, Process และ Technology มีรายละเอียดดังนี้

1.1. " Harden คน ให้มีความเข้าใจและตระหนักในเรื่องการรักษาความปลอดภัยข้อมูล "

1.2 " Harden กระบวนการจัดการด้านการรักษาความปลอดภัยข้อมูลที่ถูกต้องตามมาตรฐานสากล "

1.3 การ " Harden เชิงเทคนิค " ได้แก่ การปิดช่องโหว่ในระดับ Network Operating System เช่น Hardening Window 2000 Server หรือ Windows Server 2003 หรือ Hardening UNIX/Linux รวมทั้งการ Hardening Network Device เช่น Cisco Router/ Switching และ Hardening Security Device เช่น Firewall หรือ IPS/IDS เป็นต้น ตลอดจนการ Hardening Database เช่น Hardening Oracle หรือ Microsoft SQL Server และ การ Hardening Application เช่น Hardening Web Server IIS หรือ Apache เป็นต้น

ภาพที่ 1.1 ภาพการ Harden เชิงเทคนิค



ที่มา : http://www.acisonline.com