การวิเคราะห์และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ

Analysis and Design of Information Security Management Model

โดย

ร.ต.บัณฑิต ทานะมัย

รหัส 44067628

อาจารย์ที่ปรึกษา

ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2546

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ
นักศึกษา	ร.ต.บัณฑิต ทานะมัย
อาจารย์ที่ปรึกษา	ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขวงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2546

บทคัดย่อ

เพื่อให้มีความปลอดภัยกับระบบเทคโนโลยีสารสนเทศ ซึ่งได้แก่ทรัพย์สินที่เป็นข้อมูล อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และสาธารณูปโภคต่างๆที่เกี่ยวข้องกับระบบขององค์กรจากภัยคุกคามทั้งที่เกิดจากภายในเครือข่ายขององค์กรเอง เช่นเกิดจากความบกพร่องของบุคลากร หรืออุปกรณ์ เอง และมาจากภายนอกระบบขององค์กร เช่นอาจมีการบุกรุก หรือล้วงความลับในองค์กรจากผู้ไม่หวังดี ดังนั้นจึงต้องมีการจัดการความปลอดภัยสารสนเทศ เพื่อป้องกันภัยคุกคามดังกล่าวที่จะก่อให้เกิดความเสียหายต่อการดำเนินงานขององค์กร โดยทำการวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ ตามมาตรฐานความปลอดภัย ISO 17799 ซึ่งเป็นที่ยอมรับกันว่าเป็นมาตรฐานด้านการจัดการความปลอดภัยสารสนเทศในระดับสากล เพื่อนำไปประยุกต์ใช้ให้เหมาะสมกับองค์กรใดๆอย่างมีประสิทธิภาพ

Title	Analysis and Design of Information Security Management Model
Student	Plt.Off. Bundit Tanamai
Advisor	Asst.Prof.Chanboon Sathiwiriyawong , Ph. D.
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2003

ABSTRACT

For security to Information Technology of a organization such as information, hardware, software and facility resources from threats or vulnerabilities both of inbound and outbound the system. The threats or vulnerabilities may come from internal user error and system resources error or unauthorized external user access. Therefore, the objective of this Project is to develop Information Security Management System Model that to comply with ISO 17799 as to be an Internationally recognized Information Security Management Standard. The Information Security Management System Model can be applied to any organization to protect the risk or danger from threats and vulnerability by making good risk management to determine good Security System and Policy .

กิตติกรรมประกาศ

ในการศึกษาวิชาโครงการพิเศษฉบับนี้ กระผมได้รับการแนะแนว และให้การสนับสนุนจากผศ. ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ผู้ควบคุมโครงการโดยได้ให้ทั้งข้อมูล คำแนะนำ และความรู้เพิ่มเติม เพื่อจัดทำโครงการพิเศษฉบับนี้ด้วยดีมาโดยตลอดตั้งแต่เริ่มจนจบสมบูรณ์ จึงขอขอบพระคุณมา ณ ที่นี้

ร.ต.บัณฑิต ทานะมัย

สารบัญ

สารบัญ(ต่อ)

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความเป็นมาของระบบการรักษาความปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัย ในชีวิตและทรัพย์สินถือเป็นอุปสงค์พื้นฐานที่สำคัญยิ่งของการแสวงหาปัจจัย 4 ประการ (อาหาร เครื่องนุ่งห่ม ที่อยู่อาศัย และยารักษารักโรค) เพื่อให้มีวิถีชีวิตที่เป็นปกติสุขได้ ในทำนองเดียวกันองค์กรที่ดำเนินกิจการโดยอาศัยเครื่องมืออิเล็กทรอนิกส์เป็นหลัก ภายใต้โครงสร้างพื้นฐานทางระบบเทคโนโลยีสารสนเทศ ที่ประกอบด้วยคอมพิวเตอร์ทั้งในรูปของฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่ายข้อมูลเป็นเครื่องมือ หรือกลไกในการดำเนินงานก็จะต้องมุ่งแสวงหาระบบคอมพิวเตอร์และโปรแกรมประยุกต์ที่จำเป็นรวมถึงการติดตั้งเครือข่ายภายใน และการเชื่อมต่อกับโลกภายนอกด้วย เพื่อให้สามารถสนับสนุนกระบวนการดำเนินงานตามวัตถุประสงค์ในการรับส่ง เก็บรักษา สืบค้น และประมวลผลข้อมูลที่จำเป็นต่อกิจการขององค์กรได้อย่างมีเสถียรภาพนั่นคือ ต้องมีความมั่นคงปลอดภัยในการดำเนินงาน เพื่อให้สามารถบรรลุเป้าประสงค์นี้ ดังนั้นองค์กรจึงจำเป็นต้องมีการลงทุนพัฒนาระบบการรักษาความปลอดภัยของการดำเนินงานเชิงอิเล็กทรอนิกส์ ขึ้นมาอย่างถูกต้องตามมาตรฐานรักษาความปลอดภัย

องค์กรอิเล็กทรอนิกส์ ซึ่งเป็นองค์กรใดๆ ที่การดำเนินงานเกือบทั้งหมดต้องอาศัยอุปกรณ์คอมพิวเตอร์ช่วยในการทำงาน เพื่อการติดต่อสื่อสาร และจัดการกับฐานข้อมูลที่ใช้ในองค์กรรูปแบบต่างๆ โดยที่มีการเชื่อมต่อคอมพิวเตอร์ทุกเครื่องเข้าด้วยกันเป็นเครือข่ายอย่างครอบคลุมทั่วทั้งองค์กร เพื่อทำให้สามารถแลกเปลี่ยน หรือใช้ข้อมูลร่วมกันระหว่างคอมพิวเตอร์เหล่านี้ได้อย่างสะดวกรวดเร็ว รวมทั้งยังช่วยทำให้สามารถใช้ทรัพยากรต่างๆ ที่มีราคาแพงร่วมกันได้ เช่นเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ เครื่องพิมพ์เลเซอร์ เครื่องบันทึกซีดี เครื่องโทรสาร เป็นต้น

ดังนั้นการรักษาความปลอดภัยจึงเป็นการจัดการระบบหนึ่งซึ่งถูกเพิ่มเข้าไปในระบบเทคโนโลยีสารสนเทศ (Information Technology System) เพื่อป้องกันการบุกรุกจากแฮกเกอร์ และแครกเกอร์ ซึ่งเป็นความก้าวหน้าของเทคโนโลยีสารสนเทศที่ถูกนำไปใช้ในด้านลบ ได้แก่กลุ่มบุคคลที่เขียนโปรแกรมขึ้นมาเพื่อบุกรุกเข้าไปในระบบเครือข่ายที่ตนเองไม่ได้รับอนุญาตให้เข้าไปใช้บริการ โดยแฮกเกอร์นั้นอาจทำเพื่อความสนุก ลองความสามารถตนเองส่วนแครกเกอร์นั้นทำเพื่อเงิน เพื่อการทำลายล้าง ดังนั้นอาจพูดได้ว่าแฮกเกอร์นั้นเป็นนักเจาะระบบด้านดี ส่วนแครกเกอร์นั้นเป็นผู้ก่อการร้ายก็ว่าได้ แต่เรามักจะได้ยินคำว่าแฮกเกอร์ในด้านร้ายมากกว่า ซึ่งเป็นความเข้าใจที่ผิด แต่เพื่อความเคยชินในความเข้าใจ เราจะใช้คำว่า “แฮกเกอร์ “ ในทั้งสองความหมาย

การเข้ามาของนักเจาะระบบอาจทำให้ระบบเครือข่ายตลอดจนข้อมูลขององค์กรเสียหายได้ ระบบคอมพิวเตอร์ของหน่วยงานราชการ มหาวิทยาลัย และองค์กรเอกชนมักตกเป็นเป้าหมายของแฮกเกอร์ ดังนั้นการรักษาความปลอดภัยจึงมีความสำคัญอย่างยิ่งในระบบเทคโนโลยีสารสนเทศขององค์กร โดยเฉพาะองค์กรที่ต้องมีการรักษาความถูกต้องของข้อมูล ตลอดจนการเก็บรักษาข้อมูลที่มีความสำคัญด้วย จึงเห็นได้อย่างชัดเจนว่าทุกองค์กรให้ความสำคัญกับการรักษาความปลอดภัยนี้จนอาจกล่าวได้ว่าการรักษาความปลอดภัยได้กลายเป็นส่วนหนึ่งของระบบเทคโนโลยีสารสนเทศไปแล้ว

ความพยายามที่จะทำให้การรักษาความปลอดภัยมีประสิทธิภาพมายิ่งขึ้นกลายเป็นวัตถุประสงค์หลักของผู้วางนโยบายเพื่อพัฒนาระบบการรักษาความปลอดภัย ซึ่งไม่เพียงแต่ต้องทำหน้าที่พัฒนาระบบการรักษาความปลอดภัยให้สามารถป้องกันการบุกรุกของแฮกเกอร์ได้เท่านั้น แต่ต้องสามารถรองรับกับปัญหา และผลกระทบที่อาจเกิดขึ้นจากการถูกบุกรุกทั้งในปัจจุบัน และอนาคตได้ด้วย แต่โดยสภาพความเป็นจริงในระบบเทคโนโลยีสารสนเทศ ปัจจุบันถูกบุกรุกโดยแฮกเกอร์ไม่เว้นแต่ละวัน แม้องค์กรจะมีการทุ่มงบประมาณจำนวนมากเพื่อพัฒนาระบบการรักษาความปลอดภัยก็ตาม แต่ประสิทธิภาพของระบบการรักษาความปลอดภัยก็ยังมีเทคโนโลยีที่ตามหลังเทคโนโลยีของแฮกเกอร์อยู่ เทคโนโลยีของแฮกเกอร์เจริญรุดหน้าเร็วกว่าเทคโนโลยีของระบบการรักษาความปลอดภัยอยู่เสมอ

1.2 สิ่งที่นักพัฒนาระบบการรักษาความปลอดภัยต้องการ

ปัญหาของการพัฒนาระบบการรักษาความปลอดภัยให้มีประสิทธิภาพเพียงพอที่จะยับยั้งการถูกบุกรุกจากแฮกเกอร์ นอกจากจะมีปัญหาในเรื่องการใช้เทคโนโลยีที่มีอยู่ได้อย่างไม่เต็มประสิทธิภาพเนื่องจากขาดบุคลากรที่มีความรู้ความชำนาญในด้านนี้โดยตรงแล้วยังมีเรื่องของงบประมาณอันจำกัดและปัญหาทางเทคนิคอื่นๆ อีกมากมาย อาทิ เช่น รูปแบบการบุกรุกกลุ่มข้อมูลที่ตกเป็นเป้าหมายของแฮกเกอร์ ปัญหา และผลกระทบที่เกิดขึ้นกับระบบเครือข่ายหลังจากถูกบุกรุก

ซึ่งปัญหาเหล่านี้จำเป็นต้องอาศัยข้อมูลที่มีการเก็บรวบรวมบันทึกในขณะที่ระบบเครือข่ายขององค์กรถูกบุกรุกโดยแฮกเกอร์ เพราะข้อมูลเหล่านั้นเป็นข้อมูลที่จะทำให้ได้วิธีการแก้ปัญหาที่ดีที่สุดในการพัฒนาระบบการรักษาความปลอดภัย ข้อมูลที่เป็นที่ต้องการของนักพัฒนาระบบการรักษาความปลอดภัย คือ ข้อมูลที่มีการจัดเก็บแบบต่อเนื่อง (Continuous Information) เพื่อจะสามารถรู้ถึงการเปลี่ยนแปลง และการทำงานของระบบการรักษาความปลอดภัย ตลอดจนรูปแบบการบุกรุกของแฮกเกอร์ได้อย่างชัดเจน

นอกจากนั้นควรเป็นข้อมูลที่ได้จากการเก็บบันทึกในสถานการณ์ที่เกิดขึ้นจริงในระบบเครือข่ายที่มีระบบการรักษาความปลอดภัยด้วย เพราะการนำข้อมูลที่ได้มาจากการจำลองสถานการณ์ซึ่งเป็นข้อมูลที่ถูกสมมติขึ้นมาใช้กับการพัฒนาระบบการรักษาความปลอดภัย นอกจากจะไม่สามารถพัฒนาระบบการรักษาความปลอดภัยที่ดี พอที่จะป้องกันการบุกรุกจากแฮกเกอร์แล้วยังอาจเกิดความไม่น่าเชื่อถือในระบบการรักษาความปลอดภัยนั้นอีกด้วย วิธีการที่จะได้มาซึ่งข้อมูลดังกล่าวนั้นคือต้องมีการติดตาม และเก็บข้อมูลตลอดเวลา ปัจจัยซึ่งมีผลต่อการติดตาม และเก็บรวบรวมข้อมูลคือ ระยะเวลา และกำลังแรงงานแม้จะมีการทุ่มงบประมาณในการเก็บรวมรวมข้อมูลมากเพียงใดก็ตามแต่คงจะไม่มีใครปฏิเสธว่า หลายครั้งที่ข้อมูลซึ่งอาจจะเป็นข้อมูลที่มีความสำคัญไม่ได้ถูกเก็บบันทึกไว้ เนื่องจากการเฝ้าติดตามเก็บบันทึกข้อมูลโดยอาศัยกำลังแรงงานนั้นไม่อาจทำได้ตลอดเวลา ดังนั้นปัญหาของการเก็บรวบรวมข้อมูลเพื่อใช้ในการพัฒนาระบบการรักษาความปลอดภัย คือ ต้องเก็บข้อมูลจำนวนมากเท่าไร และควรมีความต่อเนื่องในการเก็บข้อมูลมากน้อยเพียงใด ในขณะที่ปัญหาของนักพัฒนาระบบรักษาความปลอดภัย คือ ข้อมูลที่ได้มานั้นอาจนำมาพัฒนาระบบรักษาความปลอดภัยที่ไม่สามารถรองรับในสถานการณ์จริงได้ เพราะระบบการรักษาความปลอดภัยที่ดี จะต้องสามารถรองรับกับทุกสถานการณ์ทั้งสถานการณ์ที่เกิดขึ้นในปัจจุบันและอนาคต ดังนั้นข้อมูลที่ได้มาอาจเป็นข้อมูลที่ดีที่สุดในการพัฒนาระบบการรักษาความปลอดภัยที่ใช้กับสถานการณ์ที่เกิดขึ้นในปัจจุบันเท่านั้น

ดังนั้นจึงมีความจำเป็นที่จะต้องทำการศึกษาวิเคราะห์และออกแบบระบบการรักษาความปลอดภัยสารสนเทศ เพื่อนำไปกำหนดเป็นนโยบาย และมาตรการต่างๆในการป้องกันทรัพยากรที่มีในระบบสารสนเทศให้มีความปลอดภัยจากผลกระทบจากทั้งภายใน และภายนอกองค์กร โครงการศึกษากรณีพิเศษนี้ได้เสนอการวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ ที่อ้างอิงมาตรฐาน ISO17799 ซึ่งสามารถนำไปประยุกต์ใช้ให้เหมาะสมกับแต่ละองค์กรได้

1.3 วัตถุประสงค์ของการศึกษา

1.3.1 เพื่อศึกษาการจัดการความปลอดภัยสารสนเทศ

1.3.2 เพื่อนำมาวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ

1.3.3 เพื่อให้สามารถนำรูปแบบการจัดการความปลอดภัยสารสนเทศไปประยุกต์ใช้กับระบบเทคโนโลยีสารสนเทศองค์ และสามารถกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กรได้

1.4 ขอบเขตการศึกษา

1.4.1 ศึกษาองค์ประกอบพื้นฐานของระบบเทคโนโลยีสารสนเทศที่ใช้ในองค์กรโดยสังเขป

1.4.2 ศึกษาความบกพร่อง (Vulnerability) และภัยคุกคาม (Threat) ที่มีต่อระบบเทคโนโลยีสารสนเทศโดยสังเขป

1.4.3 ศึกษาเทคโนโลยีที่ใช้ในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยสังเขป

1.4.4 ศึกษามาตรฐานความปลอดภัยสารสนเทศ ISO 17799 โดยสังเขป

1.4.5 วิเคราะห์ความเสี่ยงผลกระทบที่จะเกิดกับระบบเทคโนโลยีสารสนเทศ เพื่อออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศ ภัยคุกคามต่างๆที่มีต่อระบบเทคโนโลยีสารสนเทศ และเทคโนโลยีการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อเป็นแนวทางในการวิเคราะห์ออกแบบ และจัดทำแผนนโยบาย การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับองค์กรให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย ISO 17799 ตลอดจนสามารถนำไปประยุกต์ใช้ในการปฏิบัติงานจริงภายในองค์กรได้

บทที่ 2
องค์ประกอบพื้นฐานของระบบเทคโนโลยีสารสนเทศ

ปัจจุบันคำว่า ระบบคอมพิวเตอร์ มักใช้คำว่า เทคโนโลยีสารสนเทศ (Information Technology : IT) แทน และใช้คำย่อว่า "ไอที" แทนคำเต็มกันมากขึ้น รวมถึงมีแนวโน้มว่าจะเป็นคำที่ยอมรับในแวดวงวิชาการคอมพิวเตอร์ทั่วไป

เทคโนโลยีสารสนเทศ หมายถึง การใช้เทคโนโลยีคอมพิวเตอร์เพื่อการประมวลผล ร่วมกับการใช้เทคโนโลยีการสื่อสารโทรคมนาคมเพื่อการสื่อสารแลกเปลี่ยนข้อมูล นอกจากนี้ เทคโนโลยีสารสนเทศยังได้พัฒนาเพื่อใช้ประโยชน์ร่วมกับอุปกรณ์อื่นๆ อย่างกว้างขวาง เช่น เครื่องโทรศัพท์ เครื่องโทรสาร กล้องถ่ายรูป กล้องวิดีทัศน์ เครื่องเก็บเงิน ฯลฯ ทำให้การสื่อสารข้อมูลเป็นไปได้ทุกรูปแบบอย่างรวดเร็ว (เจนศักดิ์ ตั้งพันธุ์สุริยะ.2540)

2.1 องค์ประกอบของระบบเทคโนโลยีสารสนเทศ หรืออีกนัยหนึ่ง โครงสร้างพื้นฐานของระบบคอมพิวเตอร์ (พรชัย จิตต์พานิชย์.2001)

2.1.1 เครื่องอุปกรณ์ หรือฮาร์ดแวร์ (Hardware) ได้แก่ เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่ใช้ในการประมวลผล และสื่อสารข้อมูล

2.1.2 โปรแกรม หรือซอฟท์แวร์ (Software) ได้แก่ คำสั่ง และระบบงานต่างๆที่ทำให้ ฮาร์ดแวร์ทำงานตามต้องการ โดยผู้พัฒนาระบบงาน และนักเขียนโปรแกรมแบ่งเป็น 2 ประเภท

2.1.2.1 ซอฟต์แวร์ระบบ (System Software) เป็นชุดคำสั่งหรือโปรแกรมที่เขียนขึ้นโดยบริษัทผู้สร้างเครื่อง ซึ่งจะใช้ควบคุมการทำงานต่างๆ ของเครื่อง

2.1.2.2 ซอฟต์แวร์ประยุกต์ (Application Software) เป็นชุดคำสั่ง หรือโปรแกรมที่ผู้ใช้เครื่องพัฒนาโดยผู้พัฒนาระบบงาน และนักเขียนโปรแกรม ซึ่งอาจเป็นผู้พัฒนาภายนอก หรือผู้พัฒนาที่เป็นบุคลากรภายในขององค์กรหรืออาจจะใช้โปรแกรมสำเร็จรูป (Package) ที่มีผู้ผลิตขึ้นเพื่อจำหน่าย โดยสามารถนำมาใช้ตามความเหมาะสมกับงานของตน

2.1.3 บุคลากร (People) บุคลากรในองค์กรอาจแบ่งเป็น 2 จำพวก คือ บุคลากรที่ทำงานรับผิดชอบด้านระบบเทคโนโลยีสารสนเทศโดยตรง และบุคลากรที่เป็นผู้ใช้งาน บุคลากรทั้ง 2 จำพวก เป็นองค์ประกอบที่สำคัญต่อความสำเร็จ และกิจการจำเป็นต้องพัฒนาฝึกอบรมให้

2.1.4 บุคลากรมีความรู้ความเข้าใจในระบบเทคโนโลยีสารสนเทศที่จะนำมาใช้ เพราะแม้องค์กรจะมีระบบฮาร์ดแวร์ และซอฟต์แวร์ที่ดี แต่หากพนักงานไม่ได้รับการพัฒนาให้ใช้งานได้อย่างถูกต้องเหมาะสม ระบบงานนั้นไม่อาจใช้งานได้เต็มประสิทธิภาพ หรืออาจเกิดผลร้ายในกรณีที่พนักงานเข้าใจผิด ต่อต้าน หรือไม่ปฏิบัติตามระเบียบวิธีปฏิบัติงานที่กำหนดขึ้น ทำให้ข้อมูลเชื่อถือไม่ได้ เป็นต้น

2.1.5 วิธีปฏิบัติงาน (Procedure) ได้แก่ แผนงาน คู่มือ วิธีปฏิบัติงาน กิจกรรมการควบคุมต่างๆ ที่กำหนดขึ้น เพื่อให้การปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศเป็นระเบียบ และข้อมูลข่าวสารถูกต้อง ปลอดภัย

2.1.6 ข้อมูล (Data) ได้แก่ ข้อมูลดิบ และสารสนเทศที่ผ่านการประมวลแล้วทุกระดับ เป็นทรัพย์สินที่ต้องการ จึงต้องมีการรวบรวม ประมวล จัดเก็บ และเผยแพร่อย่างถูกต้อง ทรัพย์สินดังกล่าวมีความสำคัญและสัมพันธ์กับความสำเร็จในการนำระบบเทคโนโลยีสารสนเทศมาใช้ องค์กรต้องเตรียมความพร้อมในการวางแผน การกำหนดขอบเขต และวัตถุประสงค์ของการนำคอมพิวเตอร์มาใช้ให้ ชัดเจน

2.2 เทคโนโลยีสารสนเทศ (พรชัย จิตต์พานิชย์.2001)

เทคโนโลยีสารสนเทศ (Information Technology : IT) หมายถึง การเรียกค้น จัดเก็บ ประมวลผล การเผยแพร่ แจกจ่าย กระจาย สื่อสาร สารสนเทศในรูปแบบของอิเล็กทรอนิกส์ รวมถึง วิทยุ โทรทัศน์ โทรศัพท์ คอมพิวเตอร์ และอื่นๆ เป็นการดำเนินการที่เกี่ยวข้องกับการจัดทำสารสนเทศไว้ใช้งาน เทคโนโลยีสารสนเทศ มีองค์ประกอบสำคัญ 2 สิ่ง คือ

- คอมพิวเตอร์ (Computer)
- ระบบการสื่อสารข้อมูล (Data Communications)

2.2.1 ความหมายของคอมพิวเตอร์ (Computer)

คอมพิวเตอร์ หมายถึง เครื่องอิเล็กทรอนิกส์ ที่มีสมรรถนะในการประมวลผลข้อมูลได้อย่างอัตโนมัติโดยอาศัยคำสั่งหรือชุดคำสั่งที่เขียนขึ้นมาเป็นโปรแกรม กำหนดเงื่อนไขให้คอมพิวเตอร์ทำงานอย่างเป็นระบบด้วยความรวดเร็ว ถูกต้อง ในการจดจำข้อมูล คิดคำนวณทางคณิตศาสตร์ การเคลื่อนย้ายข้อมูลและการพิมพ์ผลลัพธ์ออกมา ไม่ว่าจะมีการ

กำหนดในเรื่องความจำ ข้อมูลหรือ คำสั่งต่างๆ สลับซับซ้อน เพียงใดก็ตาม เครื่องคอมพิวเตอร์สามารถทำงานให้ได้ผลลัพธ์ออกมาอย่างถูกต้อง ถ้าข้อมูลและคำสั่งที่ป้อนเข้าไปในเครื่องนั้น มีความถูกต้อง (Hyperdictionary.2003)

2.2.2 การสื่อสาร

การสื่อสารหมายถึงการส่งสัญญาณจากผู้ส่งสาร(Sender)ไปยังผู้รับสาร (Receiver) โดยอาศัยตัวกลาง (Transmission Media) ทำหน้าที่ในการส่ง ซึ่งแบ่งออกเป็น การสื่อสารแบบจุดต่อจุด และการสื่อสารแบบกระจาย ความหมายของการสื่อสารดังกล่าว เป็นการสื่อสารโดยทั่วไป ใช้สำหรับส่งข่าวสารระหว่างกัน ไม่ว่าจะอาศัยตัวกลางชนิดใดทำหน้าที่ในการส่งก็ตาม แต่ความหมายของการสื่อสารข้อมูลที่จะกล่าวถึงต่อไปนี้ หมายความเฉพาะการสื่อสารข้อมูลด้วยระบบคอมพิวเตอร์เท่านั้น

2.2.3 การสื่อสารข้อมูล (Data Communications)

การสื่อสารข้อมูล (Data Communications) หมายถึงการสื่อสารข้อมูลระหว่างคอมพิวเตอร์ที่ต่อเชื่อมถึงกัน โดยถือว่าเป็นความพยายามที่จะเพิ่มขีดความสามารถให้กับคอมพิวเตอร์ในการส่งผ่านข้อมูล ไม่ว่าจะเป็นข้อมูลในลักษณะตัวอักษร ภาพ หรือเสียง ในเวลาที่รวดเร็ว มีความถูกต้องน่าเชื่อถือ และสามารถที่จะเก็บบันทึก ตลอดจนนำมาใช้งานใหม่ได้โดยสะดวก โดยการส่งผ่านข้อมูลผ่านตัวกลางประเภทต่างๆเช่นสายโทรศัพท์ เส้นใยแก้วนำแสง (Fiber Optics) หรือดาวเทียม เพื่อเชื่อมโยงระบบคอมพิวเตอร์เข้าด้วยกันวิธีการสื่อสาร แบ่งออกเป็น 2 ประเภท คือ

2.2.3.1 การสื่อสารตามสาย คือการใช้สายในการรับส่งสัญญาณข้อมูลข่าวสาร เช่น สายสื่อสารชนิดต่างๆ ไม่ว่าจะเป็นสายไฟฟ้า สายโทรศัพท์ และที่กำลังเป็นที่นิยม คือ เส้นใยแก้วนำแสง ซึ่งเป็นเส้นใยแก้วที่มีขนาดเล็กเท่าเส้นผม นำหลายๆ เส้นมามัดรวมกันมีความสามารถส่งข้อมูลข่าวสารได้ทั้งตัวอักษร ภาพ และเสียงในเวลาเดียวกัน ในอัตราความเร็วเท่ากับความเร็วของแสง

2.2.3.2 การสื่อสารวิทยุ คือ การส่งสัญญาณคลื่นแม่เหล็กไฟฟ้าผ่านอากาศไปยังเครื่องรับสัญญาณคลื่นแม่เหล็กไฟฟ้ามีลักษณะพิเศษ คือ ถ้าสามารถมองเห็นได้ จะมีลักษณะคล้ายคลื่น(Wave) และ มีความถี่ต่างๆ กัน แต่ความจริงแล้วไม่สามารถมองเห็นได้ ในทางทฤษฎีและปฏิบัติ มีการแบ่งย่านความถี่เรียกว่า แบนด์ (Band) และความถี่มีหน่วยเป็น เฮิทซ์ (Hertz)

การสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์มีหลากหลายวิธีแล้วแต่ความเหมาะสมเป็นกรณีๆ ไป เช่น เครือข่ายบริเวณเฉพาะที่ (Local Area Network : LAN) หรือเครือข่ายบริเวณกว้าง (Wide Area Network : WAN) ที่อยู่ภายในอาคารเดียวกัน ก็จะใช้การสื่อสารตามสาย (Coaxial Cable) แต่ถ้าเป็นเครือข่ายบริเวณกว้าง ระหว่างอาคารใช้สายโทรศัพท์ ระหว่างจังหวัดใช้ไมโครเวฟ (Microwave) ระหว่างประเทศ ใช้ดาวเทียม (Satellite) ส่วนเครือข่ายอินเตอร์เน็ต ผู้ใช้บริการติดต่อกับผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider : ISP) โดยการใช้สายโทรศัพท์ ส่วนการติดต่อระหว่างผู้ให้บริการอินเตอร์เน็ตกับเครือข่ายอื่นๆ จะใช้ ไมโครเวฟและดาวเทียม

2.2.4 เครือข่ายคอมพิวเตอร์ (Computer Network)

เครือข่ายคอมพิวเตอร์(Computer Network)หมายถึงการสื่อสารข้อมูลระหว่างคอมพิวเตอร์ที่ต่อเชื่อมเข้าด้วยกันเป็นกลุ่ม หรือเป็นเครือข่าย มีคอมพิวเตอร์ขนาดใหญ่เป็นศูนย์กลางในการจัดเก็บ และประมวลผลข้อมูล คอมพิวเตอร์ศูนย์กลาง เรียกว่า "แม่ข่าย" (Host) เครือข่ายคอมพิวเตอร์แบ่งออกเป็น 2 ลักษณะ

2.2.4.1 เครือข่ายบริเวณเฉพาะที่ (Local Area Network : LAN) เป็นเครือข่ายพื้นฐาน ซึ่งเป็นที่นิยมกันอย่างแพร่หลาย

2.2.4.2 เครือข่ายบริเวณกว้าง (Wide Area Network : WAN) เป็นเครือข่ายระยะไกล สำหรับองค์กรขนาดกลางถึงขนาดใหญ่ หรือเป็นเครือข่ายที่เกิดจากการต่อเชื่อม ระหว่างเครือข่ายบริเวณเฉพาะที่หลายๆ เครือข่าย

2.3 รูปแบบการสื่อสารข้อมูลในเครือข่าย

เครือข่ายอินทราเน็ต (Intranet) เป็นเครือข่ายภายในองค์กร ที่เปลี่ยนโปรโตคอล ในการสื่อสารบนระบบเครือข่าย แบบแลนเดิมๆ ไปเป็นโปรโตคอล TCP/IP เช่นเดียวกับอินเตอร์เน็ต และสามารถใช้โปรแกรมต่างๆ ที่พัฒนาเพื่อ ใช้กับอินเตอร์เน็ตได้ ทำให้มีค่าใช้จ่ายถูกลงมาก ต่างกันตรงที่ อินทราเน็ต จะเป็นเครือข่ายปิด ใช้เฉพาะในองค์กรเท่านั้น

2.3.1 เครือข่ายเอ็กซ์ทราเน็ต (Extranet) เป็นระบบแบบเดียวกับอินทราเน็ต แต่ใช้เชื่อมโยงกันระหว่างองค์กรต่างๆ โดยทั่วๆไปจะเป็นองค์กร ที่ทำธุรกิจร่วมกัน ซึ่งต่างจากอินเตอร์เน็ต เพราะเอ็กซ์ตราเน็ตมีการใช้งาน จำกัดขอบเขตเฉพาะกลุ่ม เช่นกลุ่มธนาคาร จะมีเครือข่ายโอนเงิน เป็นกลุ่มของตนเอง แต่สามารถเปิดช่องให้สำหรับลูกค้าที่มีสิทธิ์เข้ามาใช้บริการของ Server ได้ส่วนมากใช้ในเรื่อง E-commerce

2.3.2 เครือข่ายอินเทอร์เนต(Internet) อินเตอร์เน็ต (Internet) หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่ต่อเชื่อมกันทั่วโลก โดยมีมาตรฐานการรับส่งข้อมูลแบบเดียวกัน

คอมพิวเตอร์แต่ละเครื่อง สามารถรับส่งข้อมูลได้ทั้งแบบตัวอักษร รูปภาพนิ่ง หรือภาพเคลื่อนไหว และเสียง การค้นหาข้อมูลจากที่ต่างๆ กระทำได้อย่างรวดเร็ว ดังนั้น อินเตอร์เน็ตจึงมีประโยชน์สำหรับยุคเทคโนโลยีสารสนเทศเช่นในปัจจุบันและเนื่องจากอินเตอร์เน็ตมีมาตรฐานการรับส่งข้อมูลที่ชัดเจนและเป็นรูปแบบหนึ่งเดียว ทำให้การโฆษณาเผยแพร่ข้อมูลต่างๆ สามารถเข้าถึงกลุ่มเป้าหมายในวงกว้างโดยเสียค่าใช้จ่ายไม่มาก จึงเป็นเรื่องที่มีคุณประโยชน์มาก เช่น ด้านการศึกษาค้นคว้า ด้านไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail : E-Mail) ด้านการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange : EDI) และด้านบันเทิง

2.4 ระบบสารสนเทศ (พรชัย จิตต์พานิชย์.2001)

2.4.1 ความหมายของสารสนเทศ

สารสนเทศ (Information) หมายถึง สิ่งที่ได้จากการนำเอาข้อมูลที่เก็บรวบรวมไว้มาประมวลผล กล่าวคือ สารสนเทศที่ดีจะต้องมีการจัดเก็บไว้เป็นอย่างดี การนำมาใช้ในและการประมวลผลสามารถ ควบคุมดูแลได้ง่าย การควบคุมดูแลอาจจะมีข้อกำหนดให้ผู้ใดบ้างเป็นผู้ใช้ได้ สารสนเทศที่เป็นความลับจะต้องมีระบบขั้นตอนที่ดี การแก้ไขหรือเกี่ยวข้องจะกระทำได้โดยใครบ้าง ซึ่งเป็นเรื่องที่ต้องมีการควบคุม เช่นกัน นอกจากนี้ การเก็บจะต้องไม่เกิดการสูญหายหรือถูกทำลาย คุณสมบัติของสารสนเทศที่ดีจะต้องไม่มีส่วนการเก็บที่ซ้ำซ้อนเพราะจะเป็นการสิ้นเปลืองเนื้อที่เก็บ มีลักษณะง่ายต่อการเก็บมีความเป็นรูปแบบเดียวกัน สารสนเทศแต่ละชุดมีความหมายในตัวเอง หรือมีความเป็นอิสระในตัวเอง (Hyperdictionary.2003)

2.4.2 ความหมายของข้อมูล

ข้อมูล (Data) หมายถึง ความจริงที่เกี่ยวกับสิ่งต่างๆ เช่น คน สถานที่ สิ่งของ ซึ่งได้รับการรวบรวมเอาไว้ เมื่อข้อมูลได้รับการเก็บรักษาไว้จะสามารถเรียกมาใช้ประโยชน์ได้ในภายหลังข้อมูลจึงเป็นสิ่งที่ต้องมีการเก็บรวบรวม และรักษาไว้ (Hyperdictionary.2003)

บทที่ 3
ลักษณะ และประเภทของภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

3.1 ชนิดของภัยคุกคาม (อุษณา ภัทรมนตรี.2544)

ภัยคุกคาม (Threats) ที่มีต่อระบบคอมพิวเตอร์นั้น สามารถทำอันตรายต่อส่วนต่างๆของระบบได้ ไม่ว่าจะเป็น ตัวฮาร์ดแวร์ ตัวซอฟต์แวร์ หรือตัวข้อมูล (Data) ที่ถูกเก็บไว้ในระบบ เราสามารถจำแนกชนิดของภัยคุกคามได้เป็นชนิดใหญ่ๆ ดังนี้

3.1.1 การขัดขวางการทำงานของระบบ (Interruption) นั่นคือ มีการโจมตีระบบ และทำให้ระบบสูญหาย และ/หรือเสียหายจนไม่สามารถทำหน้าที่ของมันเองได้อย่างมีประสิทธิภาพ ตัวอย่างของการกระทำเช่นนี้ ได้แก่

3.1.1.1 การทำลายส่วนใดส่วนหนึ่งของระบบฮาร์ดแวร์ (HardwareDevice Destruction)

3.1.1.2 การลบส่วนใดส่วนหนึ่งของโปรแกรม หรือการลบส่วนใดส่วนหนึ่งของไฟล์ข้อมูล ซึ่งจะทำให้การทำงานของโปรแกรมนั้นๆ ผิดปกติหรือไม่ทำงานเลย

3.1.2 การลักลอบเข้ามาในระบบ (Interception) คือการเข้ามาในระบบ และดำเนินกิจกรรมต่างๆ โดยไม่ได้รับอนุญาตการลักลอบนั้นอาจทำโดยตัวโปรแกรมหรือโดยบุคคลโดยตรง เช่น

3.1.2.1 การที่มีโปรแกรมลักลอบเข้าในระบบ และทำการคัดลอก(Copy)ไฟล์ข้อมูลที่เป็นความลับไป

3.1.2.2 การที่มีบุคคลทำการขโมยข้อมูลในระหว่างการติดต่อสื่อสารภายในระบบเครือข่าย โดยใช้วิธีการดักดูข้อมูลที่ถูกส่งไปตามสาย (Wire Tapping) ภายในระบบเครือข่ายคอมพิวเตอร์นั้นๆ

3.1.3 การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Modification) คือ การเปลี่ยนแปลงแก้ไขข้อมูลสำคัญที่เก็บภายในระบบฐานข้อมูล (Database) ของระบบหรือภายในส่วนอื่นๆ ของระบบ เป็นต้น โดยที่ข้อมูลนั้นอาจเอื้อประโยชน์แก่ผู้ทุจริตได้

3.1.4 การเพิ่มรายการหรือข้อมูล (Fabricate) คือ การที่บุคคลที่ไม่ได้รับอนุญาตทำการเพิ่มรายการ(Transaction)ที่ไม่ถูกต้องเข้ามาในระบบ หรือการเพิ่มข้อมูลในฐานข้อมูลที่มีอยู่ ซึ่งหากผู้ปลอมแปลงมีความสามารถและประสบการณ์สูง จะทำให้เจ้าของระบบไม่สามารถแยกรายการหรือความแตกต่างได้เลย

3.2 จุดอ่อนของระบบคอมพิวเตอร์ (อุษณา ภัทรมนตรี.2544)

ในส่วนต่างๆของระบบคอมพิวเตอร์นั้นจะมีจุดอ่อน (Vulnerabilities) ซึ่งง่ายต่อการถูกคุกคามและโจมตีอยู่แล้วเป็นลักษณะเฉพาะตัว หากเราต้องการที่จะอุดรอยรั่วเพื่อป้องกันการถูกโจมตีนี้ เราควรต้องรู้จุดอ่อนนั้นๆ ว่าอยู่ที่ใดบ้าง และในแต่ละจุดนั้น มีอะไรบ้างที่จะต้องทำการป้องกัน โดยทั่วไปจุดอ่อนต่างๆ ในระบบคอมพิวเตอร์มีดังนี้

3.3 ภัยคุกคามที่มีต่อระบบคอมพิวเตอร์ (อุษณา ภัทรมนตรี.2544)

3.3.1 ภัยคุกคามที่มีต่อระบบฮาร์ดแวร์ (Threats to Hardware)

ภัยที่คุกคามต่อระบบ Hardware นี้ สามารถจำแนกได้เป็น 3 กลุ่มใหญ่ๆ ดังนี้

3.3.1.1 ภัยที่มีต่อระบบการจ่ายไฟฟ้า ที่เรียกว่า Power Surge ซึ่งเป็นอันตรายต่อระบบการทำงานของเครื่องคอมพิวเตอร์

3.3.1.2 ภัยที่เกิดจากการทำลายทางกายภาพโดยตรงต่อระบบคอมพิวเตอร์นั้น เช่น น้ำท่วม หรือมีการกระแทกคอมพิวเตอร์อย่างแรง เป็นต้น

3.3.1.3 ภัยจากการลักขโมยโดยตรง

3.3.2 ภัยคุกคามที่มีต่อระบบซอฟต์แวร์ (Threats to Software)

ภัยที่มีต่อระบบซอฟต์แวร์ แบ่งได้เป็น 3 พวกใหญ่ๆ คือ

3.3.2.1 การลบซอฟต์แวร์ (Software Deletion) การลบทั้งหมด หรือการลบเพียงบางส่วนของซอฟต์แวร์ ซึ่งอาจสร้างความเสียหายให้กับระบบได้ การลบบางครั้งอาจเกิดจากความตั้งใจโดยตรง หรืออาจเกิดจากความบังเอิญโดยที่ไม่ได้ตั้งใจ

3.3.2.2 การขโมยซอฟต์แวร์ (Software Theft) คือ มีการคัดลอก และแจกจ่ายตัว ซอฟต์แวร์โดยไม่ได้รับอนุญาต เนื่องจากซอฟต์แวร์เป็นทรัพย์สินทางปัญญา ดังนั้นการ

กระทำเช่นนี้ จึงสร้างความเสียหายให้กับบริษัทผู้ผลิตซอฟต์แวร์เป็นอย่างมาก ดังที่ปรากฏให้เห็นอย่างแพร่หลายในบางประเทศ

3.3.2.3 การเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Software Modification) ซึ่งการทำเช่นนี้ อาจทำให้โปรแกรมที่ทำงานอยู่อย่างปกติเปลี่ยนเป็นทำงานผิดพลาดหรือมีการทำงานที่ผิดจุดมุ่งหมาย และเป็นอันตรายต่อระบบการรักษาความปลอดภัยของข้อมูลได้ เช่น การที่โปรแกรมนั้น ทำการเปิดเผยข้อมูลที่สำคัญต่อบุคคลที่ไม่ได้รับอนุญาต หรือการที่โปรแกรมทำให้ตัวระบบซอฟต์แวร์นั้นหยุดการทำงานในขณะที่กำลังปฏิบัติงานอยู่

3.3.3 ภัยที่มีต่อระบบข้อมูล (Threats to Data)

ภัยพวกนี้ ได้แก่ การที่ข้อมูลอาจถูกเปิดเผยโดยมิได้รับอนุญาต หรือ การที่ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขเพื่อผลประโยชน์บางอย่าง โดยมิได้มีการตรวจสอบแก้ไข หรือการที่ข้อมูลนั้นถูกทำให้ไม่สามารถนำมาใช้งานได้

3.3.4 ภัยที่มีต่อระบบเครือข่าย (Threats in Network)

นอกจากภัยคุกคามตามข้อ 1-3 ปัจจุบันมีการใช้งานระบบเครือข่าย (Network) ซึ่งเป็นระบบเปิด และมีผู้ใช้งานจำนวนมาก สามารถใช้งานร่วมกัน มีจุดอ่อนหลายจุดในการเกิดความเสี่ยงต่อระบบ ดังนี้

3.3.4.1 การใช้งานร่วมกัน (Sharing) ก่อให้เกิดปัญหาในการจัดการที่เกี่ยวกับการให้อนุญาตแก่ผู้ใช้ภายในระบบ เพราะหากไม่มีการจัดการระบบที่ดีแล้ว อาจมีการลักลอบเข้ามาใช้ระบบโดยไม่ได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายในเชิงธุรกิจ และการรักษาความลับของข้อมูลได้

3.3.4.2 ความสลับซับซ้อนของระบบ (Complexity) เนื่องจากว่า ระบบเครือข่ายนี้ เกิดจากการนำเอาระบบปฏิบัติการ (Operating System) จากคอมพิวเตอร์หลายตัว มาทำงานร่วมกัน หรือ อาจเกิดจากการนำเอาระบบปฏิบัติการหลายชนิดมาทำงานร่วมกัน ซึ่งก่อให้เกิดความยุ่งยากในกาจัดการป้องกันการรั่วไหลของข้อมูลจากระบบที่สลับซับซ้อนได้ อนึ่ง ระบบปฏิบัติการโดยทั่วไปนั้น ก็มิได้ถูกออกแบบมาเพื่อการรักษาความปลอดภัยของข้อมูลในระบบ ดังนั้น หากนำระบบปฏิบัติการหลายตัว และหลากหลายชนิดมาทำงานร่วมกัน จึงอาจก่อให้เกิดความไม่ปลอดภัยในการรักษาความปลอดภัยของข้อมูลได้มากยิ่งขึ้น

3.3.4.3 การกำหนดพารามิเตอร์ของระบบเครือข่ายที่ไม่แน่นอน(Unknown Parameter) เนื่องจากความง่ายในการเพิ่มเติม และขยายระบบเครือข่าย ดังนั้น จึงเป็นการยากที่จะกำหนดขอบเขตของผู้ใช้ในระบบเครือข่ายที่แน่นอนได้ ผลก็คือ การกำหนดขอบเขต และเป้าหมายที่แน่นอนในการรักษาความปลอดภัยของข้อมูลภายในระบบเครือข่ายนั้น สามารถทำได้ยากขึ้น

3.3.4.4 มีจุดอ่อนอยู่หลายจุดภายในระบบเครือข่าย (Many Points of Attacks) เนื่องจากระบบเครือข่ายนั้น มีระบบคอมพิวเตอร์อยู่หลากหลาย ทำให้ผู้ดูแลระบบเครือข่ายไม่สามารถที่จะควบคุมดูแลผู้ที่เข้ามาใช้ทรัพยากรในระบบได้ทั่วถึงเพราะการอนุญาตให้ผู้ใช้เข้ามาในเครือข่ายได้นั้น ต้องอาศัยระบบปฏิบัติงาน และการควบคุมระบบที่มีประสิทธิภาพของระบบต่างๆ ที่กระจายอยู่ทั่วทั้งเครือข่ายด้วย และการควบคุมทุกส่วนของระบบเครือข่ายนั้น ทำได้โดยยาก

3.3.4.5 ความไม่สามารถรู้ถึงผู้ที่เข้ามาใช้ระบบเครือข่าย (Anonymity) เนื่องจากระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันนี้ ได้มีการต่อเชื่อมกันเกือบทั่วทั้งโลกแล้ว ดังนั้น ผู้ใช้ที่เข้ามาใช้ระบบ อาจมาจากสถานที่ที่ห่างไกลกันนับพันๆกิโลเมตรออกไป โดยทำการเข้ามาในระบบโดยผ่านเครือข่ายอื่นๆ หลายเครือข่าย ที่มีการเชื่อมต่อกันทางอิเล็กทรอนิกส์ การอนุญาตให้เข้ามาในระบบผ่านทางเครือข่ายได้นั้นมักจะอาศัยการตรวจสอบจากระบบคอมพิวเตอร์ด้วยกันเอง ที่เรียกว่า Computer –To– Computer Authentication ซึ่งต้องมีการจัดการ และควบคุมที่ดี มิฉะนั้น อาจเกิดการลักลอบเข้ามาในระบบโดยไม่ได้รับอนุญาตได้โดยง่าย

3.3.5 ปัญหาหลักในการดูแลรักษาความปลอดภัย

3.3.5.1 ความประมาทของผู้ใช้หรือไม่มีความรู้ในการใช้งานเทคโนโลยี

3.3.5.2 อาชญากรรมทางคอมพิวเตอร์

3.3.5.3 ภัยพิบัติทางธรรมชาติ

3.3.5.4 ความผิดพลาดของ Hardware และ Software

3.4 อาชญากรรมคอมพิวเตอร์ (Forcht, Karen Anne.1997)

ความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศ โดยเฉพาะคอมพิวเตอร์ นำประโยชน์มหาศาลมาสู่สังคมมนุษย์ แต่ขณะเดียวกัน ก็มีบุคคลที่ใช้คอมพิวเตอร์ไปในทางที่ไม่ถูกไม่ควร ไม่ว่าผู้นั้นจะกระทำโดยเจตนา หรืออยากทดลองภูมิปัญญาทางวิทยาการของตนเอง โดยทำการล่วงละเมิดเข้าไปในระบบคอมพิวเตอร์ของ ผู้อื่นโดยไม่ได้รับอนุญาต หรือโดยปราศจากอำนาจ ในบางกรณีมีเจตนาทุจริตลักลอบเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นเพื่อประสงค์ต่อทรัพย์ ก่อให้เกิดความเสียหายอย่างมากมาย ทำให้เห็นถึงความแตกต่างกับความผิดอาญาที่ประสงค์ต่อทรัพย์สินในรูปแบบเก่าอย่างสิ้นเชิง เพราะปัจจุบันเพียงแต่นั่งอยู่หน้าจอคอมพิวเตอร์ก็สามารถจารกรรมทรัพย์สินหรือข้อมูลลับบางประเภท ที่หากผู้อื่นล่วงรู้อาจจะสร้างความเสียหายแก่เจ้าของข้อมูลได้ การกระทำดังกล่าว ถือว่าเป็นส่วนหนึ่งของความผิดอันเกี่ยวเนื่องกับคอมพิวเตอร์ (Computer Related Crime) ซึ่งมักจะเรียกกันโดยทั่วไปว่า อาชญากรรมคอมพิวเตอร์ (Computer Crime)

3.4.1 ความหมายของอาชญากรรมคอมพิวเตอร์

โดยทั่วไป หน่วยงานต่างๆ จะใช้คำที่มีความหมายว่า อาชญากรรมทางคอมพิวเตอร์อย่างหลากหลาย เช่นใช้คำว่า การใช้คอมพิวเตอร์ในการกระทำความผิด (Computer Abuse) การฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud) และ อาชญากรรมคอมพิวเตอร์ (Computer Crime)

3.4.2 ลักษณะของอาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์เกิดขึ้นเมื่อมีบุคคล หรือคณะบุคคลกระทำความผิด โดยใช้คอมพิวเตอร์เป็นเครื่องมือเพื่อกระทำความผิด และมีผู้ได้รับความเสียหาย หรืออาจได้รับความเสียหายจากการที่มีผู้บุกรุกหรือพยายามที่จะเข้าไปในระบบคอมพิวเตอร์ เพื่อวัตถุประสงค์ลักลอบเข้าไป การลักลอบเข้าถึงข้อมูลคอมพิวเตอร์เพื่อฉกฉวยประโยชน์ อันก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล

3.4.3 ประเภทของอาชญากรรมคอมพิวเตอร์

3.4.3.1 การลักขโมยบริการ (Theft of Service)

การใช้ประโยชน์บางอย่างจากคอมพิวเตอร์จะต้องมีค่าใช้จ่ายเกิดขึ้น นอกเหนือจากตัวเครื่องหรือแม้กระทั่งตัวเครื่องเองก็มีการให้เช่าการให้เช่าเครื่อง หรือการให้บริการโดยปกติแล้ว จะมีผู้เกี่ยวข้องอยู่สองฝ่าย คือฝ่ายให้บริการกับฝ่ายผู้ใช้บริการโดยทำเป็นข้อตกลง หรือสัญญาระหว่างกัน ผู้ให้บริการก็จะได้รับผล

ประโยชน์ในรูปของค่าบริการส่วนผู้ใช้บริการก็จะได้รับผลประโยชน์เป็นการใช้บริการนั้นๆ โดยจะต้องชำระค่าบริการให้ผู้ให้บริการ อาชญากรรมประเภทนี้ จะเกิดขึ้น เมื่อมีผู้มาลักลอบใช้บริการโดยไม่ชำระค่าบริการ ทำให้ผู้ให้บริการต้องเสียรายได้เป็นมูลค่ามหาศาล

3.4.4.2 การจารกรรมข้อมูล (Theft of Information)

ในกรณีที่ข้อมูลในคอมพิวเตอร์ที่ต้องการจัดเก็บไว้เป็นความลับ หรือกำหนดการใช้เฉพาะบุคคลหรือกลุ่มบุคคลแล้ว หากถูกบุคคลที่ปราศจากอำนาจหน้าที่ในการเรียกใช้ข้อมูลและทำการแก้ไขเปลี่ยนแปลงข้อมูลชุดดังกล่าว ย่อมก่อให้ผลของความเสียหายรุนแรงกว่ากรณีที่เป็นข้อมูลประเภทที่เปิดให้บุคคลอื่นสามารถเรียกใช้ได้

3.4.4.3 การยักยอก/แก้ไข ข้อมูล ชุดคำสั่ง หรือโปรแกรม

3.4.4.4 การเข้าถึงข้อมูลโดยปราศจากอำนาจหรือโดยฉ้อฉล ผู้กระทำจะแสวงหาประโยชน์จากการเข้าถึงข้อมูลหรือชุดคำสั่ง โดยไม่มีเจตนาหวังผลประโยชน์ในทางการค้า เช่น การแสดงความสามารถว่าตนเองสามารถเข้าสู่ระบบได้ อาจจะแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูล รวมทั้งการแพร่ไวรัสคอมพิวเตอร์

3.4.4.5 การเปิดเผยข้อมูลที่มีเจ้าของโดยปราศจากอำนาจหรือโดยฉ้อฉล กรณีนี้ ผู้กระทำจะหวังผลประโยชน์มากกว่า โดยมากจะเป็นข้อมูลทางธุรกิจ โดยเฉพาะความลับทางการค้าที่มีมูลค่ามหาศาล เช่น ฐานข้อมูลลูกค้า แผนการตลาด เป็นต้น

จากที่กล่าวถึงภัยคุกคาม การโจมตี ตลอดจนอาชญากรรมทางคอมพิวเตอร์ จะเห็นได้ว่า การกระทำที่ไม่ประสงค์ดีดังกล่าวก่อให้เกิดความเสียหายอย่างใหญ่หลวงต่อกิจการหรือองค์กรอย่างไรก็ดี ปัจจุบันการกระทำความผิดที่เกิดขึ้นบ่อยครั้งและส่งผลกระทบอย่างรุนแรง คือ กระทำต่อข้อมูลในระบบคอมพิวเตอร์ ทั้งนี้เพราะข้อมูลเป็นทรัพย์สินที่มีคุณค่ามหาศาลจนกระทั่งปัจจุบันนี้ อาจจะกล่าวได้ว่า "การรักษาความปลอดภัยของระบบคอมพิวเตอร์"นั้นแทบจะมีความหมายเดียวกับ "การรักษาความปลอดภัยของข้อมูล"ทีเดียว

3.5 การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ (Forcht, Karen Anne.1997)

3.5.1 การลักลอบเข้าถึง และใช้ข้อมูล

การกระทำความผิดในการลักลอบเข้าถึง และการใช้ข้อมูลนั้น เนื่องจากปัจจุบัน ฐานข้อมูลในคอมพิวเตอร์ของหน่วยงานต่างๆ นิยมใช้ระบบฐานข้อมูลสำเร็จรูป สามารถเข้าถึงได้โดยง่าย ทำให้การลักลอบเข้าถึงข้อมูลโดยปราศจากอำนาจ (Unauthorized Access) สามารถทำได้โดยสะดวก ไม่ว่าผู้กระทำจะเป็นบุคคลภายในหรือบุคคลภายนอกหน่วยงานก็ตาม โดยปกติแล้วเกือบทุกหน่วยงานจะมีการจำกัดอำนาจ และเวลาของการเข้าถึงสำหรับบุคคลในหน่วยงานไว้เพื่อวัตถุประสงค์การเข้าถึงข้อมูลเฉพาะอย่าง แต่ผู้กระทำจะกระทำนอกเหนืออำนาจ หรือเวลาโดยหาโอกาสที่เหมาะสม เพื่อกระทำการโดยปราศจากการอนุญาตให้เข้าถึงข้อมูล การเข้าถึงข้อมูลบางกรณี ผู้กระทำมีอำนาจแห่งการเข้าถึง แต่ได้ใช้การเข้าถึงนั้นเพื่อที่จะได้รับหรือทำการแก้ไขข้อมูลในคอมพิวเตอร์นั้นซึ่งผู้ที่เข้าถึงไม่มีสิทธิที่จะได้รับหรือแก้ไขเปลี่ยนแปลงข้อมูลนั้นจะเรียกการกระทำในลักษณะนี้ว่า "การกระทำเกินกว่าอำนาจแห่งการเข้าถึง" (Exceeds Authorized Access)

สำหรับวิธีการของการเข้าถึงข้อมูล ด้วยเทคโนโลยีในปัจจุบัน ไม่ต้องเข้าไปในสถานที่ตั้งของคอมพิวเตอร์หลักเพียงแต่มีคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งซอฟต์แวร์ในการติดต่อกับเครือข่ายและโมเด็มที่พ่วงกับคู่สายโทรศัพท์ ก็จะสามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ประสงค์จะเข้าถึงและใช้ข้อมูลนั้นได้ ความมุ่งหวังของผู้กระทำที่เป็นบุคคลภายในหน่วยงาน บางกรณี ไม่ถึงกับเป็นการจารกรรมข้อมูลเพื่อประโยชน์ทางธุรกิจ แต่กระทำเพราะความอยากรู้อยากเห็นข้อมูลส่วนตัวของตนเอง หรือของพนักงานคนอื่นที่หน่วยงานเก็บไว้เป็นความลับ เช่น เงินเดือนพนักงาน แต่ก็มีบางหน่วยงานจะต้องให้ความสนใจเป็นอย่างยิ่งเพราะผู้กระทำได้กระทำไปเนื่องจากต้องการทดสอบความสามารถของตนเองในการที่จะผ่านระบบการรักษาความปลอดภัย

ระบบการรักษาความปลอดภัยของคอมพิวเตอร์ที่ใช้กันโดยทั่วไป อุปกรณ์ต่างๆ จะจำกัดการเข้าถึง โดยผู้มีอำนาจใช้จะต้องมีการระบุผู้ใช้ (User Identification : USER ID) และรหัสผ่าน (Password) เพื่อใช้เป็นกุญแจเข้าไปในระบบ อย่างไรก็ตาม ในทางปฏิบัติอาจจะไม่แน่นหนาพอเท่าที่ควรจะเป็น เพราะทั้งการระบุผู้ใช้ และรหัสผ่านมักไม่ได้ถูกเก็บเป็นความลับส่วนตัว แต่จะเป็นที่ทราบกันในบรรดาเพื่อนร่วมงานเพื่อความสะดวกในการปฏิบัติงาน หรือบางกรณีสถานที่ที่จะต้องพิสูจน์รหัสผ่านอยู่ใน

ตำแหน่งที่ไม่เหมาะสมบุคคลอื่นสามารถเห็นรหัสผ่านของผู้พิสูจน์ได้ง่าย และหลายครั้งที่ผู้กระทำความผิดสามารถเข้าถึงข้อมูลจากการเดารหัสผ่าน โดยการสุ่มตัวเลขหรือตัวอักษรที่มีความสัมพันธ์กับเจ้าของรหัสผ่าน เช่น ชื่อเล่น วันเดือนปีเกิด เป็นต้น

3.5.2 การคัดลอกข้อมูล

การคัดลอกข้อมูลโดยปราศจากอำนาจ เป็นการกระทำหลังจากผ่านขั้นตอนของการเข้าถึงข้อมูลแล้ว การคัดลอกข้อมูลสามารถกระทำได้ 2 แบบ แบบที่หนึ่ง คือ การคัดลอกข้อมูลเหมือนต้นแบบทั้งหมดหรือทำสำเนา (Copy) อีกแบบหนึ่งคือ การคัดลอกข้อมูลเหมือนต้นฉบับทั้งหมดหรือบางส่วนหรือตัดทอน (Extract) การกระทำทั้งสองแบบ ผู้กระทำสามารถกระทำได้โดยง่าย เพียงแต่สามารถเข้าถึงข้อมูลดังที่กล่าวมาแล้ว เว้นแต่ในบางกรณีเท่านั้น ที่จำเป็นจะต้องอาศัยความรู้ทางเทคโนโลยีสารสนเทศเข้ามาช่วย แต่ไม่ว่าจะกระทำด้วยวิธีใดก็ตามจะไม่ทำให้ข้อมูลลดน้อยลงไป และผู้กระทำก็ไม่ประสงค์จะแทรกแซงเนื้อหาแต่ประการใด นอกเหนือจากการคัดลอกข้อมูล ยังมีการกระทำอีกลักษณะหนึ่ง คือ การลักลอบสกัดข้อมูลของบุคคลอื่นโดยปราศจากอำนาจ เช่น การแอบซ่อนอุปกรณ์ดักฟัง การใช้กล้องถ่ายภาพที่สามารถทำงานได้ในระยะไกล หรือการใช้อุปกรณ์อื่นๆ ที่เชื่อมโยงกับคอมพิวเตอร์ เพื่อที่จะทำการสกัดข้อมูล โดยจะเรียกการกระทำดังกล่าวว่า เป็นการสกัดโดยปราศจากอำนาจ (Unauthorized Interception)

3.5.3 การแก้ไขเปลี่ยนแปลงข้อมูล

การแก้ไขเปลี่ยนแปลงข้อมูล เป็นการกระทำที่ต้องอาศัยการเข้าถึงข้อมูลโดยผู้กระทำมุ่งกระทำการบางอย่างเกี่ยวกับข้อมูลในคอมพิวเตอร์ เช่น การเพิ่มเติมเข้าไป การตัดทอนข้อมูล หรือการจำกัดข้อมูล ข้อมูลที่ถูกเปลี่ยนแปลงล้วนแล้วแต่เป็นข้อมูลที่มีความสำคัญ หรือเป็นข้อมูลหลัก เช่น การแก้ไขเปลี่ยนแปลงชื่อโดเมน (Domain Name) เป็นต้น

โดยปกติ การแก้ไขเปลี่ยนแปลงข้อมูล ผู้กระทำจะมีวัตถุประสงค์เพื่อการฉ้อโกง เรียกกันว่า การฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud) เช่น การฉ้อโกงโดยบัตรฝากถอนเงินสดอัตโนมัติ (Automatic Teller Machine : ATM) การฉ้อโกงทางบัตรเครดิต การฉ้อโกงโดยการยักยอกโอนถ่ายเงินทางอิเล็กทรอนิกส์ และจากการสำรวจของหลายๆ สถาบัน ปรากฏว่า การฉ้อโกงทางคอมพิวเตอร์เป็นการกระทำความผิดที่เกิดขึ้นมากที่สุดในจำนวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3.5.4 การลบ และการทำลายข้อมูล

การลบข้อมูล และการทำลายข้อมูลอันนำมาซึ่งความเสียหายนั้น บางกรณีอาจจะรวมถึงการแก้ไขเปลี่ยนแปลงข้อมูลเพื่อที่จะทำลายข้อมูลที่มีอยู่ การลบและการทำลายข้อมูลนี้ จะต้องอาศัยการเข้าถึงทางคอมพิวเตอร์ โดยความเสียหายที่เกิดขึ้น เจ้าของข้อมูลไม่สามารถที่จะรู้เห็นได้ด้วยทางกายภาพ จึงจำเป็นอย่างยิ่งที่ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลไว้ระดับหนึ่ง ซึ่งไม่สามารถที่จะครอบคลุมการป้องกันไว้ได้ทั้งหมด ก็เพราะสาเหตุ และวิธีการของผู้ไม่ประสงค์ดี ที่ต้องการจะลบหรือทำลายข้อมูลนั้นมีมากมายหลายสาเหตุ บางกรณีเกิดจากความโกรธแค้นของพนักงานในหน่วยงาน บางกรณีเกิดจากเหตุผลทางการเมืองหรือเหตุผลทางธุรกิจ และสาเหตุที่พบมากที่สุด ก็คือการฉ้อโกงต่างๆ ซึ่งต้องมีการลบหรือทำลายข้อมูลอันเป็นส่วนหนึ่งของการฉ้อโกง ส่วนวิธีการก็มีหลากหลายรูปแบบ เริ่มตั้งแต่การทำให้เครื่องคอมพิวเตอร์หยุดทำงานหรือระบบขัดข้อง (Crash System) การเข้าถึงโดยปราศจากอำนาจ เพื่อเข้าไปลบข้อมูลหรือทำลายข้อมูล เช่น ข้อมูลที่ตนเป็นลูกหนี้ การใส่โปรแกรมบางชนิดซึ่งมีความสามารถที่จะลบข้อมูลจำนวนมากในระยะเวลาอันสั้น โดยโปรแกรมบางชนิดสามารถตั้งเวลาหรือเงื่อนไขให้ทำลายข้อมูลภายหลังจากที่ ผู้กระทำได้ออกจากระบบคอมพิวเตอร์นั้นไปแล้ว

3.5.5 ไวรัสคอมพิวเตอร์กับการทำลายข้อมูล

ไวรัสคอมพิวเตอร์ (Virus Computer) คือ โปรแกรมที่มีความสามารถในการแก้ไขดัดแปลงโปรแกรมอื่น เพื่อที่จะทำให้โปรแกรมนั้น ๆ สามารถเป็นที่อยู่ของไวรัสคอมพิวเตอร์ได้ และสามารถทำให้ไวรัสคอมพิวเตอร์ทำงานได้ต่อไปเรื่อยๆ เมื่อมีการเรียกใช้โปรแกรมที่มีโปรแกรมไวรัสคอมพิวเตอร์นั้น

ไวรัสคอมพิวเตอร์ เป็นชุดคำสั่งหรือโปรแกรม ซึ่งสามารถแก้ไขดัดแปลงข้อมูลหรือทำลายข้อมูลได้ ทันที และไวรัสคอมพิวเตอร์ ยังสามารถอยู่ในเครื่องคอมพิวเตอร์ทำการทำลายข้อมูลตามเงื่อนไขหรือเงื่อนเวลาที่กำหนด อีกทั้งยังสามารถแพร่พันธุ์ อันมีลักษณะคล้ายคลึงกับไวรัสในตัวมนุษย์ โดยวัตถุประสงค์หลักของผู้กระทำก็เพื่อทำลายข้อมูลในคอมพิวเตอร์

ความเสียหายที่เกิดขึ้นนั้น อาจจะเกิดขึ้นกับข้อมูลเพียงบางส่วนหรือทั้งหมดก็ได้ ขึ้นอยู่กับว่า ไวรัสคอมพิวเตอร์ที่อยู่ในเครื่องเป็นไวรัสคอมพิวเตอร์ชนิดใด โดยทั่วไป จะแบ่งความเสียหายออกเป็น 3 ระดับ คือ ระดับแรก ข้อมูลไม่เสียหายเลย เพียงแต่เครื่องนั้นใช้งานไม่ได้ชั่วคราว อันเนื่องมาจากการเกิดไวรัสคอมพิวเตอร์ชนิดที่มีการเติมขยะลง

ไป คำว่า "ขยะ" หมายถึงข้อมูลที่ระบบคอมพิวเตอร์ไม่ต้องการ แต่ ผู้ก่อให้เกิดข้อมูลประเภทนี้ ใส่ไว้ในเครื่องเป็นจำนวนมาก อันทำให้เครื่องคอมพิวเตอร์นั้นไม่สามารถทำงานต่อไปได้ เพราะไม่มีหน่วยความจำหรือเนื้อที่พอที่จะทำงาน ระดับที่สอง คือการก่อให้เกิดความเสียหายต่อข้อมูลที่เป็นการบอกตำแหน่งที่อยู่ของแฟ้มข้อมูลต่างๆ โดยปกติคอมพิวเตอร์จะทำงานกับแฟ้มข้อมูลได้ จะต้องมี ตารางบอกตำแหน่งของแฟ้มข้อมูลนั้นๆ เพื่อคอมพิวเตอร์จะได้เข้าถึงข้อมูลในตำแหน่งที่เก็บข้อมูลได้อย่างถูกต้อง และรวดเร็ว แต่ไวรัสคอมพิวเตอร์ประเภทนี้ จะสร้างความสับสนให้กับตารางบอกตำแหน่ง แต่จะไม่ทำลายข้อมูลที่เก็บอยู่ในคอมพิวเตอร์นั้น ๆ ดังนั้น ถ้าสามารถแก้ไขตารางให้บอกตำแหน่งที่ถูกต้องได้ก็สามารถนำข้อมูลกลับมาใช้ได้ และระดับสุดท้าย อันก่อให้เกิดความเสียหายอย่างมากคือการทำลายข้อมูลในคอมพิวเตอร์ และจัดรูปแบบ (Format) เพื่อใช้ในการเก็บข้อมูลใหม่ ความเสียหายระดับนี้ โดยทั่วไปไม่สามารถที่จะนำข้อมูลกลับมาใช้ได้อีก เว้นแต่จะมีการทำการสำรอง (Backup) ข้อมูลไว้ในสื่อต่างๆ

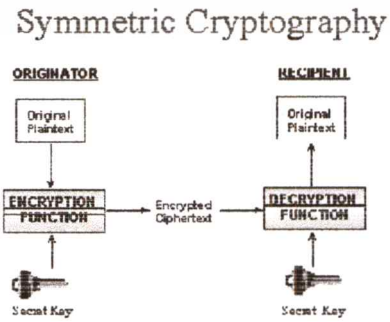
บทที่ 4

เทคโนโลยีการรักษาความปลอดภัยระบบสารสนเทศ

4.1 การเข้ารหัสลับ (Stalling, William.1999)

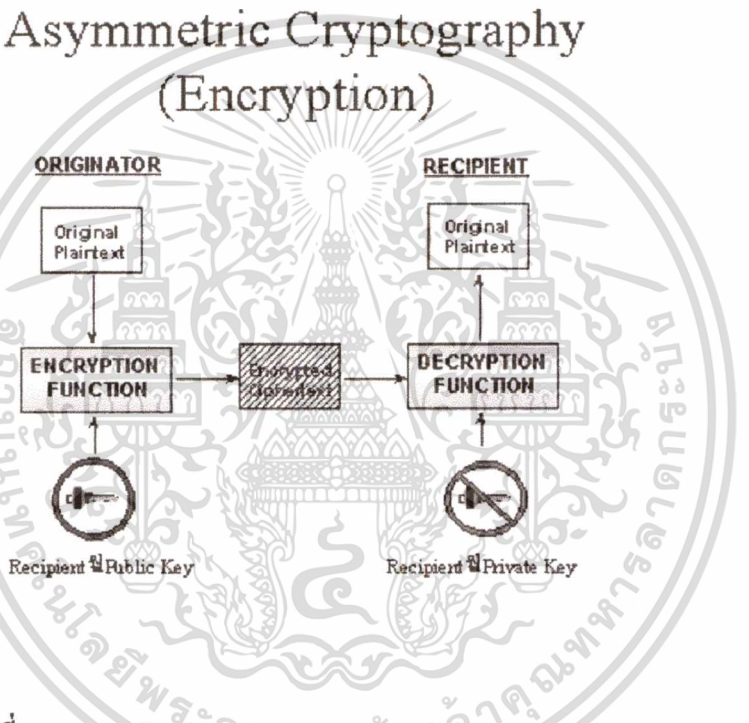
การเข้ารหัสลับ (Cryptography) คือ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ด้วยการเข้ารหัสลับ (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ ด้วยการถอดรหัสลับ (Decryption) นั่นคือ สามารถรักษาข้อมูลให้เป็นความลับ (Confidentiality) และกำหนดผู้ มีสิทธิ์ได้ (Authentication & Authorization) สำหรับการเข้ารหัสลับ และถอดรหัสลับนั้นจะอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน และต้องอาศัยกุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้ สำหรับตัวกุญแจนั้นจะมีความยาวเป็นบิต (bit) และ ยิ่งกุญแจมีความยาวมาก ยิ่งปลอดภัยมาก เนื่องจากจะต้องใช้เวลานานมากขึ้นในการ คาดเดากุญแจ โดยผู้ลุกคาม) ในการเข้า และถอดรหัสลับสามารถแบ่งออกเป็น 2 ประเภท คือ การรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography หรือ Secret Key Cryptography) และการรหัสลับแบบอสมมาตร (Asymmetric Key Cryptography หรือ Public Key Cryptography)

4.1.1 การรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography) หมายถึง การเข้า และถอดรหัสลับ โดยใช้กุญแจลับที่เหมือนกัน (Secret Key) กุญแจลับจะเป็นกุญแจเดียวกัน ซึ่งจะต้องเป็นที่รู้กันเพียงผู้รับและผู้ส่งเท่านั้น



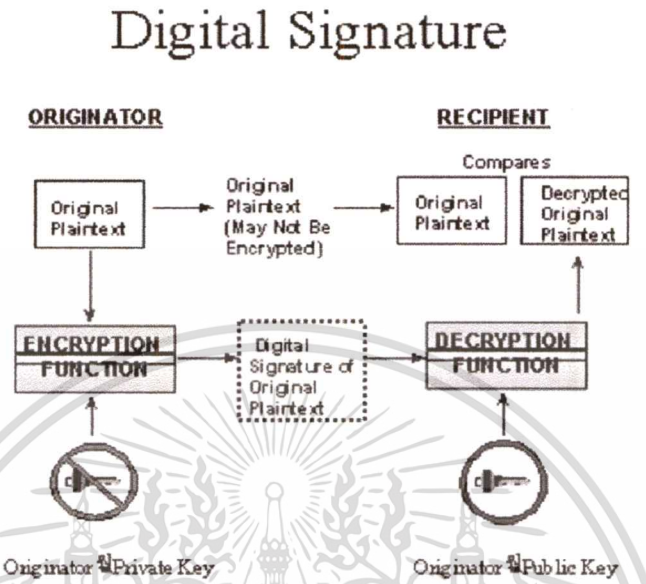
ภาพที่ 4.1 การรหัสลับแบบกุญแจสมมาตร(Symmetric Key Cryptography)

4.1.2 การรหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Cryptography) หมายถึง การเข้าและ ถอดรหัสลับด้วยกุญแจต่างกัน โดย การเข้ารหัสใช้กุญแจสาธารณะ (Public Key) และถอดรหัสใช้กุญแจส่วนตัว(Private Key) ในการส่งข้อความด้วยการเข้ารหัสลับแบบกุญแจอสมมาตร จะเน้นที่ผู้รับเป็นหลัก คือ จะใช้กุญแจสาธารณะของผู้รับซึ่งเป็นที่เปิดเผยในการเข้ารหัส และ จะใช้กุญแจส่วนตัวของผู้รับในการถอดรหัสลับ



ภาพที่ 4.2 การรหัสลับแบบกุญแจอสมมาตร(Asymmetric Key Cryptography)

4.1.3 ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) ในการส่งข้อมูลผ่านเครือข่ายนั้น นอกจากจะทำให้ข้อมูลที่ส่งนั้นเป็นความลับสำหรับผู้ไม่มีสิทธิ์ โดยการใช้เทคโนโลยีการรหัสแล้ว สำหรับการทำนิติกรรมสัญญาโดยทั่วไป ลายมือชื่อจะเป็นสิ่งที่ใช้ในการระบุตัวบุคคล (Authentication) และ ยังมีแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้นๆซึ่งเชื่อมโยงถึง การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) สำหรับในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้น จะใช้ ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ซึ่งมีรูปแบบต่างๆเช่น สิ่งที่ระบุตัวบุคคลทางชีวภาพ (ลายพิมพ์นิ้วมือ เสียง ม่านตา เป็นต้น) หรือ จะเป็นสิ่งที่มอบให้แก่บุคคลนั้นๆในรูปแบบของรหัสประจำตัว



ภาพที่ 4.3 ลายมือชื่ออิเล็กทรอนิกส์(Digital Signature)

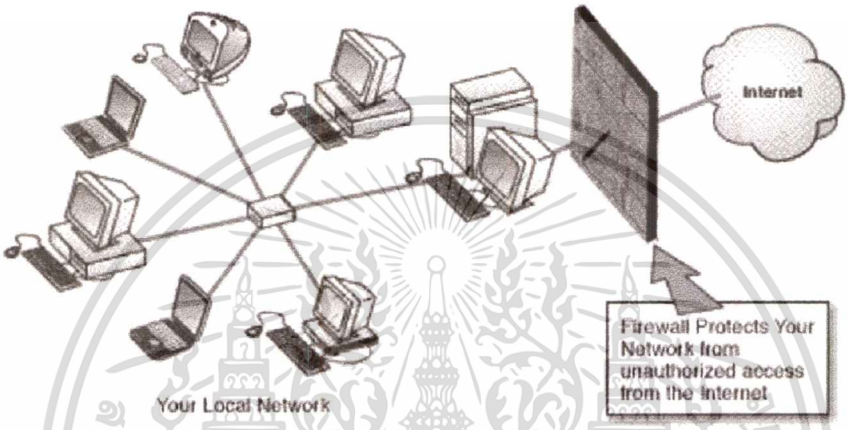
4.2 ไฟร์วอลล์ (เรืองไกร รังสิพล.2544)

ไฟร์วอลล์(Firewall) คือ ระบบหนึ่ง หรือกลุ่มของระบบที่บังคับใช้นโยบายการควบคุมการเข้าถึงของระหว่างเครือข่ายสองเครือข่ายเช่น ป้องกันการ login ที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย ปิดกั้นไม่ให้ traffic จากนอกเครือข่ายเข้ามาภายในเครือข่ายโดยที่วิธีการกระทำนั้นก็จะแตกต่างกันไปแล้วแต่ระบบ แต่ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่านไฟร์วอลล์ โดยหลักการแล้วเราสามารถมองไฟร์วอลล์ ได้ว่าประกอบด้วยกลไกสองส่วน โดยส่วนแรกมีหน้าที่ในการกั้น traffic และส่วนที่สองมีหน้าที่ในการปล่อย traffic ให้ผ่านไปได้แบ่งเป็น 4 ประเภท คือ

4.2.1 Packet Filtering เป็นการตรวจสอบ Packet ของข้อมูลที่วิ่งผ่านทีละ Packet ว่าตรงกับเงื่อนไขที่อนุญาตหรือไม่ ถ้าไม่ตรงเงื่อนไขที่ระบุไว้ก็จะไม่สามารถผ่านไปได้

4.2.2 Application Gateways เป็นการตรวจสอบข้อมูลในระดับ Application ที่ใช้งานว่า Application ใดบ้างที่อนุญาตให้ใช้ได้ ก็จะให้มีการติดต่อผ่านเข้าออกได้

4.2.3 Packet Inspection เป็นการตรวจสอบ Packet ของข้อมูลที่วิ่งผ่าน โดยเปรียบเทียบกับเงื่อนไขที่ระบบกำหนดไว้ และ Packet จะต้องตรงกับตารางสถานะการทำงานของการเชื่อมต่อด้วยจึงจะติดต่อผ่านเข้าออกได้



ภาพที่ 4.4 ไฟร์วอลล์ (Firewall)

4.3 ระบบตรวจจับผู้บุกรุก (เรืองไกร รังสิพล.2544)

ระบบตรวจจับผู้บุกรุก(Intrusion Detection System) คือ ระบบที่ทำการตรวจจับการบุกรุกของผู้ที่พยายามที่จะเจาะเข้าสู่ระบบ หรือการใช้ระบบในทางที่ผิด (Misuse) IP Secutity (IP Sec) แบ่งออกเป็น 3 ประเภท

4.3.1 Network Intrusion Detection System (NIDS) จะทำการเฝ้าดู packet ที่วิ่งผ่าน wire ในเครือข่าย และพยายามที่จะค้นหาว่า hacker/cracker พยายามที่จะเจาะเข้าระบบสู่ระบบ ซึ่งตัวอย่างที่เห็นได้ชัดคือระบบที่จะเฝ้าตรวจ TCP connection request หรือว่า SYN ที่พยายามจะเชื่อมต่อมายัง port ต่างๆ ของเครื่องเป้าหมาย ซึ่ง NIDS นั้นอาจจะถูกติดตั้งบนเครื่องเป้าหมายเอง และจะคอยตรวจทุก traffic ของตัวเอง หรืออาจจะถูกติดตั้งบนเครื่องที่แยกอยู่ต่างหากและจะคอยตรวจทุก packet ที่ผ่านมาในเครือข่าย

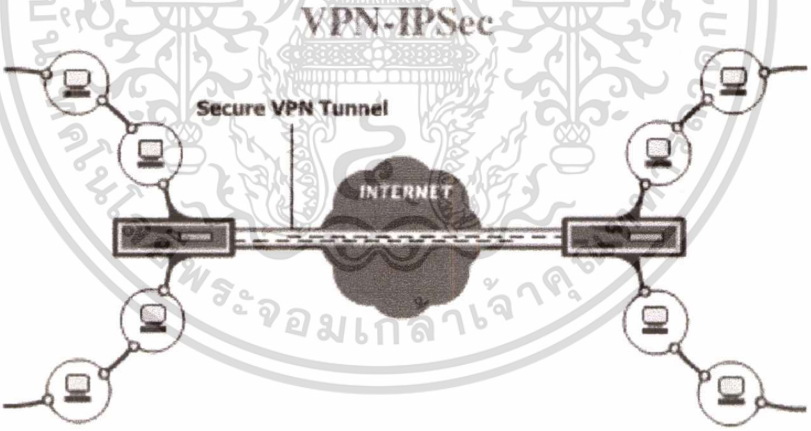
4.3.2 Syatem Integrity Verifiers (SIV) จะคอยตรวจสอบ system files ว่ามีการเปลี่ยนแปลงเกิดขึ้นหรือไม่ ซึ่งโปรแกรมที่ได้รับความนิยมมากที่สุดคือ "Tripwire" ซึ่งขณะเดียวกัน SYN อาจจะคอยตรวจสอบ components อื่นๆ อย่างเช่น windows registry หรือ cron

configuration หรืออาจจะตรวจจับเมื่อผู้ใช้ปกติพยายามที่จะใช้สิทธิ์ของ root หรือ admin ซึ่ง products ส่วนใหญ่ที่เป็น SYN มักจะเป็นแค่ tools มากกว่า systems ที่สมบูรณ์แบบ อย่างเช่นในกรณีของ Tripwire จะตรวจจับการเปลี่ยนแปลงของ system files ที่สำคัญ แต่จะไม่มีการแจ้งเตือนที่เป็นแบบ real time

4.3.3 Log File Monitors (LFM) จะทำการเฝ้าดู log files ต่างๆที่สร้างขึ้นมาโดย services ในเครือข่าย ซึ่ง LFM จะค้นหารูปแบบของ log files ที่จะบ่งบอกถึงการบุกรุก ตัวอย่างเช่น parser ของ HTTP server log files เช่น Swatch

4.4 IP Security (IP Sec)

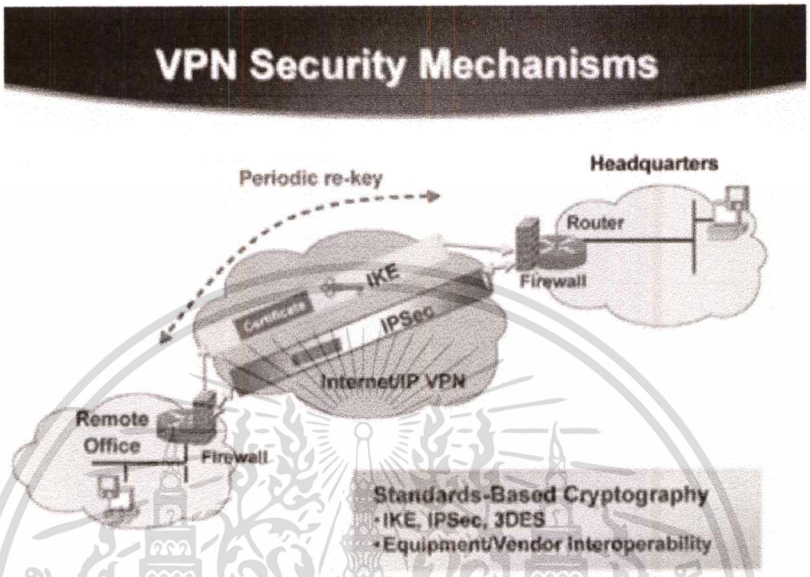
IP Security เป็นการรักษาความปลอดภัยระดับ IP มีหน้าที่ในการให้บริการ 3 ประเภท คือ การพิสูจน์ตน(Authentication), การรักษาความลับ(Confidential) และการบริหารกุญแจ (Key Management)



ภาพที่ 4.5 IP Security (IP Sec)

4.5 Virtual Private Network (VPN)

Virtual Private Network หมายถึง เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้ โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบน เครือข่ายไอพีก็ได้ แต่ยังสามารถ คงความเป็นเครือข่ายเฉพาะ ขององค์กรได้ ด้วยการ เข้ารหัสแพ็กเก็ตก่อนส่ง เพื่อให้ข้อมูล มีความปลอดภัยมากขึ้น



ภาพที่ 4.6 Virtual Private Network (VPN)

4.6 โปรแกรมป้องกันไวรัส (Antivirus Program)

โปรแกรมป้องกันไวรัส คือโปรแกรมที่ใช้ตรวจจับ ป้องกันการแพร่กระจาย และทำลายไวรัสได้ก่อนที่ไวรัสต่างๆจะเข้ามาทำลายระบบเทคโนโลยีสารสนเทศ ตัวอย่างเช่น Symantec Norton AntiVirus, McAfee VirusScan, Panda Antivirus Platinum หรือ PC-cillin เป็นต้

บทที่ 5

มาตรฐาน ISO 17799

ว่าด้วยเทคโนโลยีสารสนเทศ - แนวปฏิบัติการบริหารความปลอดภัยสารสนเทศ

5.1 ขอบเขต

มาตรฐานนี้เป็นการให้คำแนะนำสำหรับการบริหารความปลอดภัยข้อมูลสารสนเทศ สำหรับการจัดทำการประยุกต์ใช้และการบำรุงรักษาระบบความปลอดภัยสารสนเทศในองค์กร โดยมีวัตถุประสงค์เพื่อเป็นแนวทางขั้นต้นในการพัฒนามาตรฐานความปลอดภัยในองค์กรและนำไปใช้ให้เกิดประสิทธิผล รวมทั้งทำให้เกิดความมั่นใจระหว่างองค์กร ข้อแนะนำในมาตรฐานนี้ต้องมีการเลือกนำไปใช้ให้สอดคล้องกับกฎหมายและกฎระเบียบต่างๆ

5.2 นิยามและความหมาย (Carlson T.2001)

ความปลอดภัยสารสนเทศ (Information security) ครอบคลุมถึง

5.2.1 ความลับ (Confidentiality) คือการทำให้เกิดความมั่นใจว่าสารสนเทศเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาต

5.2.2 ความมีบูรณภาพ (Integrity) คือการป้องกันเพื่อความถูกต้องและความสมบูรณ์ของสารสนเทศและขั้นตอนการประมวลผล

5.2.3 ความพร้อมใช้งาน (Availability) หมายถึงการทำให้เกิดความมั่นใจว่าผู้ที่ได้รับอนุญาตมีสิทธิ์เข้าถึงเข้มูลและทรัพย์สินที่เกี่ยวข้องได้ตลอดเวลาที่ต้องการ

5.3 การประเมินความเสี่ยง (Risk Assessment) คือการประเมินภัยคุกคาม ผลกระทบ จุด อ่อนของสารสนเทศและสิ่งอำนวยความสะดวกสำหรับการประมวลผลข้อมูลที่อาจเกิดขึ้นได้

5.4 การบริหารความเสี่ยง (Risk management) คือกระบวนการในการแยกแยะ การควบคุม การทำให้เหลือน้อยที่สุด หรือ การกำจัดความเสี่ยงที่อาจส่งผลต่อความปลอดภัยระบบสารสนเทศและมีต้นทุนที่ยอมรับได้

5.5 นโยบายความปลอดภัย (Simpson.2003)

นโยบายความปลอดภัยสารสนเทศ (Security Policy) มีวัตถุประสงค์เพื่อจัดหาแนวทางในการบริหาร และการสนับสนุนความปลอดภัยสารสนเทศ โดยที่ฝ่ายบริหารต้องมีทิศทางนโยบายที่ชัดเจนและมีการสนับสนุนและมีพันธะสัญญาเกี่ยวกับความปลอดภัยสารสนเทศโดยจัดทำเป็นประเด็นและบำรุงรักษานโยบายความปลอดภัยสารสนเทศทั่วทั้งองค์กร

5.5.1 จัดทำเอกสารนโยบายความปลอดภัย โดยที่นโยบายมีการอนุมัติจากฝ่ายบริหารและมีการ ตีพิมพ์รวมทั้งแจ้งให้พนักงานทุกคนทราบ

5.5.2 จัดทำการทบทวนและการประเมินผล คือนโยบายต่างๆ ต้องมีผู้รับผิดชอบในการบำรุงรักษาและมีการทบทวนตามช่วงเวลา

5.6 องค์กรความปลอดภัย (Simpson.2003)

องค์กรความปลอดภัย(Organization Security)มีโครงสร้างพื้นฐานของความปลอดภัยสารสนเทศเพื่อบริหารความปลอดภัยสารสนเทศในองค์กร โดยจัดให้มีการประชุมปรึกษาหารือกับหน่วยงานต่างๆ เพื่อกำหนดประยุกต์ใช้สารสนเทศการจัดสรรหน้าที่ความรับผิดชอบการมีที่ปรึกษาด้านความปลอดภัยสารสนเทศ การกำหนดความปลอดภัยแก่บริษัทคู่ค้า ผู้รับเหมาและบริษัทที่ปรึกษาต่างๆ

5.6.1 มีการจัดการประชุมทางด้านการบริหารการจัดการความปลอดภัยข้อมูลโดยทีมงานผู้บริหารมีส่วนร่วมที่กำหนดหาแนวทางและวิสัยทัศน์ด้านความปลอดภัย

5.6.2 จัดความร่วมมือด้านความปลอดภัยข้อมูลโดยจัดให้มีแผนกงาน หรือฝ่ายต่างๆ เข้ามามีส่วนร่วมประชุมหรือกำหนดบทบาทเกี่ยวับการควบคุมความปลอดภัยสารสนเทศ

5.6.3 มีการจัดสรรอำนาจหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศ

5.6.4 มีขั้นตอนในการให้อำนาจเกี่ยวกับอุปกรณ์ อำนวยความสะดวกต่างๆด้านสารสนเทศ เช่น การนำอุปกรณ์ใหม่ๆ เข้ามาใช้ด้านสารสนเทศต้องได้รับการอนุมัติ อนุญาตจากบุคคลที่รับผิดชอบด้านความปลอดภัย

5.6.5 มีผู้เชี่ยวชาญด้านความปลอดภัยให้คำแนะนำเกี่ยวกับความปลอดภัยของข้อมูลสารสนเทศ

5.7 การจัดการความปลอดภัย (ISO 17799.2000)

การเข้าถึงข้อมูลของบุคคลที่สามเพื่อรักษาความปลอดภัยต่อสิ่งอำนวยความสะดวก การประมวลผลข้อมูลรวมทั้งทรัพย์สินข้อมูล ประกอบไปด้วย ขั้นตอนคือ จำแนกแยกแยะความเสี่ยงที่เกิดจากการเข้าถึงของบุคคลที่สาม ได้แก่ การเข้าถึง

5.7.1 จำแนกแยกแยะความเสี่ยงที่อาจเกิดขึ้นจากการเข้าถึงของบุคคลที่สามที่เกี่ยวข้องได้แก่ ชนิดของการเข้าถึงทางกายภาพ และลอจิคัล เหตุผลและความจำเป็นในการเข้าถึงบริษัทที่เข้ามาให้บริการ พนักงานรักษาความปลอดภัย แม่บ้าน พนักงานทำความสะอาด นักศึกษาฝึกงาน ผู้ให้คำปรึกษา

5.7.2 กำหนดสัญญาความต้องการด้านความปลอดภัยกับบริษัทร่วมค้า ให้ปฏิบัติตามนโยบายความปลอดภัยต่างๆ ซึ่งสัญญาควรประกอบไปด้วย นโยบายความปลอดภัยข้อมูลทั่วๆ ไป การค้าครองทรัพย์สินต่างๆ การอธิบายลักษณะของการให้บริการแต่ละอย่าง ระดับของการได้รับบริการ การคุ้มครองทรัพย์สินทางปัญญา ข้อตกลงในการเข้าถึงข้อมูลหรือสิ่งอำนวยความสะดวกทางการประมวลผล

5.7.3 มีการกำหนดสนธิสัญญาเกี่ยวกับความต้องการด้านความปลอดภัยกับบุคคลภายนอกเช่น สิทธิในการตรวจสอบได้ ระดับการเข้าถึงทางกายภาพที่อนุญาตได้ เป็นต้น

5.8 การจัดการแยกชนิดของทรัพย์สิน และการจัดการควบคุม (Simpson.2003)

การจัดการแยกชนิดของทรัพย์สิน และการจัดการควบคุม (Asset Classification & Control) มีวัตถุประสงค์เพื่อคงไว้ซึ่งการปกป้องคุ้มครองทรัพย์สินขององค์กรอย่างเหมาะสม มีการจัดทำบัญชีทรัพย์สิน เพื่อบำรุงรักษาป้องกันทรัพย์สินขององค์กรอย่างเหมาะสม ทรัพย์สินที่สำคัญต้องมีการจัดทำบัญชี และแต่งตั้งผู้รับผิดชอบ ประกอบด้วย

5.8.1 จัดทำทรัพย์สินคงคลัง ประกอบไปด้วยทรัพย์สินทางข้อมูล ได้แก่ฐานข้อมูล แฟ้มข้อมูล เอกสาร แผนงานต่อเนื่อง ซอฟต์แวร์ ทรัพย์สินทางกายภาพ
จัดทำการแบ่งแยกชนิดของสารสนเทศ มีวัตถุประสงค์เพื่อ ทำให้เกิดความมั่นใจว่าทรัพย์สินข้อมูลได้รับการคุ้มครองในระดับที่เหมาะสม

5.8.2 มีการจัดทำข้อแนะนำในการแบ่งแยกประเภทและการจัดเก็บ

5.8.3 มีการจัดทำประทับตราและการส่งมอบจัดเก็บ โดยกำหนดขั้นตอนกระบวนการต่างๆ ประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร การทำลาย

5.9 การจัดการความปลอดภัยของบุคคล (Simpson.2003)

การจัดการความปลอดภัยของบุคคล (Personnel Security) มีวัตถุประสงค์เพื่อลดความเสี่ยงจากการกระทำผิดพลาดของมนุษย์ เช่น การขโมย การฉ้อโกง การใช้งานในทางที่ผิด ดังนั้นจึงต้องมีการจัดการความปลอดภัยของบุคคลดังนี้

5.9.1 ความปลอดภัยในงาน และทรัพยากร เพื่อลดความเสี่ยงจากการผิดพลาดของมนุษย์ การขโมย การฉ้อโกง โดยกำหนดความปลอดภัยในหน้าที่งาน มีนโยบาย และการตรวจสอบพนักงานทั้งในขั้นตอนการรับสมัคร รวมถึงพนักงานลูกจ้างชั่วคราว มีการทำข้อตกลงเกี่ยวกับความลับของข้อมูลกับบุคลากรในสัญญาจ้างงาน กำหนดความปลอดภัยข้อมูลเป็นเงื่อนไขและนิยามหนึ่งของความรับผิดชอบของพนักงานในการจ้างงาน

5.9.2 การฝึกอบรมพนักงาน เพื่อเกิดความมั่นใจว่าพนักงานตระหนักและใส่ใจในภัยคุกคามที่เกิดกับความปลอดภัยข้อมูล รวมทั้งการสร้างความสนับสนุนในนโยบายความปลอดภัยข้อมูลขององค์กร พนักงานต้องได้รับการฝึกอบรมเกี่ยวกับขั้นตอนความปลอดภัยรวมทั้งการใช้งานข้อมูลได้อย่างถูกต้องเพื่อลดความเสี่ยงให้น้อยที่สุด โ ดยให้การศึกษา และการฝึกอบรมเกี่ยวกับความปลอดภัยของข้อมูลแก่พนักงานทุกระดับ ในการใช้งานการประมวลผลข้อมูลเช่นขั้นตอนการล๊อกออนการใช้ซอฟท์แวร์

5.9.3 มีการจัดการการตอบสนองต่อเหตุสุดวิสัย และการทำงานที่ผิดปกติ (Responding to security incidents and malfunctions) เพื่อลดความเสียหายของข้อมูลจากเหตุสุดวิสัยที่เกิดขึ้น โดยจะต้องประกอบไปด้วย คือมีการรายงานเหตุสุดวิสัยไปยังบุคคลหรือฝ่ายจัดการได้ทราบทันทีทันใด มีการจัดทำรายงานจุดอ่อนของความปลอดภัย มีการจัดทำรายงานการทำงานที่ผิดปกติของซอฟต์แวร์ จัดทำนโยบายจากประสบการณ์ที่ได้รับจากเหตุสุดวิสัย จัดสร้างกฎระเบียบลงโทษพนักงาน

5.10 การจัดการความปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Simpson.2003)

การจัดการความปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and environmental security) เป็นการกำหนดขอบเขตการจัดการความปลอดภัยทางกายภาพ และสิ่งแวดล้อม เพื่อป้องกันผู้ไม่มีสิทธิ์ที่จะเข้ามาใช้ระบบสารสนเทศ หรือเข้ามาก่อความเสียหายกับระบบสารสนเทศ ทำให้สูญเสียการดำเนินธุรกิจ จึงต้องมีการจัดการความปลอดภัยดังนี้

5.10.1 มีการจัดการที่ปลอดภัย (Secure area) เพื่อป้องกันการเข้าถึง การแทรกแซง การทำลายข้อมูลทุกชนิดขององค์กร โดยมีการจัดแยกพื้นที่ให้ชัดเจน มีขั้นตอน คือ

5.10.1.1 กำหนดขอบเขตพื้นที่ทางกายภาพขึ้นมาให้ชัดเจน

5.10.1.2 กำหนดทางเข้าทางกายภาพที่มีการควบคุมอย่างชัดเจนเพื่อให้บุคคลที่มีสิทธิ เท่านั้นที่สามารถเข้าไปยังพื้นที่ได้

5.10.1.3 กำหนดพื้นที่ของออฟฟิศ ห้องทำงานและห้องอำนวยความสะดวกต่างๆ ซึ่งต้องมีการล้อคอย่างดีเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.10.1.4 มีการจัดการการทำงานในพื้นที่ที่ปลอดภัย โดยมีการจัดการควบคุมทำข้อเสนอแนะสำหรับพนักงานและลูกจ้าง

5.10.1.5 มีการจัดการพื้นที่สำหรับการรับส่งพัสดุและพื้นที่ใช้บรรจุพัสดุ ซึ่งถ้าเป็นไปได้จะต้องมีการจัดการแยกจากพื้นที่ที่มีอุปกรณ์ในการประมวลผลข้อมูล มีการตรวจสอบพัสดุอุปกรณ์ก่อนนำไปใช้ มีการจัดทำการลงทะเบียน มีประตูกั้นทั้งภายในและภายนอก

5.10.1.6 มีการจัดการความปลอดภัยของอุปกรณ์ (Equipment Security) เพื่อป้องกันการสูญหาย การทำลายทรัพย์สิน และทำให้การดำเนินธุรกิจชะงักงัน โดยมีการจัดการประเด็นต่างๆ คือ

5.10.1.7 จัดการสถานที่ตั้งของอุปกรณ์และมีการป้องกันให้ปลอดภัย เพื่อหลีกเลี่ยงความเสี่ยงจากการถูกขโมย ไฟไหม้ การระเบิด ควัน น้ำท่วม ฝุ่น แรงสั่นสะเทือน สารเคมี คลื่นไฟฟ้า คลื่นแม่เหล็ก มีการกำหนดนโยบายการรับประทานอาหาร การสูบบุหรี่ในพื้นที่ที่มีอุปกรณ์ สำหรับการประมวลผลข้อมูล

5.10.1.8 มีการจัดการอุปกรณ์สำรองไฟฟ้า (Power supplies) อุปกรณ์ควรได้รับการป้องกันจากการขาดกระแสไฟฟ้า โดยการจัดหาไฟสำรองรวมทั้งอุปกรณ์สำรองปั่นไฟ

5.10.1.9 ความปลอดภัยของสายเคเบิ้ล คือสายไฟและสายสัญญาณที่ใช้เชื่อมโยงข้อมูลควรป้องกันจากการถูกจัดจังหวะหรือการทำลาย

5.10.1.10 การบำรุงรักษาอุปกรณ์ ควรมีการตรวจสอบเป็นประจำเพื่อความพร้อมใช้งานและความมีบูรณภาพ

5.10.1.11 การจัดการกับอุปกรณ์ส่วนตัวของพนักงานที่นำเข้ามาใช้ควรได้รับการอนุญาต

5.10.1.12 มีการจัดการความปลอดภัยอุปกรณ์ที่ทิ้งทำลายหรือการนำกลับมาใช้ใหม่ เช่น อุปกรณ์สื่อบันทึกข้อมูลต่างต้องมีการทำลายมากกว่าการลบหรือการเขียนทับการควบคุมทั่วๆไป เพื่อป้องกันการขโมยข้อมูลและอุปกรณ์ต่างๆ ที่ใช้ในการประมวลผลข้อมูล

5.10.1.13 การจัดการ โต๊ะทำงานให้สะอาดและมีหน้าจอคอมพิวเตอร์ที่ปลอดภัย

5.10.1.14 การเคลื่อนย้ายทรัพย์สิน อุปกรณ์ ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ การเคลื่อนย้ายต้องมีการทำเป็นบันทึกและได้รับอนุญาตอย่างถูกต้อง

5.11 การบริหารการติดต่อสื่อสาร และการปฏิบัติการ(Simpson.2003)

การบริหารการติดต่อสื่อสาร และการปฏิบัติการ (Communications and operations management) เป็นเอกสารรายละเอียดเกี่ยวกับการจัดการ วิธีการ ขั้นตอนปฏิบัติงานกับการประมวลผลข้อมูลทั้งหมดดังรายละเอียดต่อไปนี้

5.11.1 จัดสรรความรับผิดชอบและมีขั้นตอนปฏิบัติงาน เพื่อทำให้เกิดความถูกต้องและปลอดภัยต่อการดำเนินการกับอุปกรณ์ประมวลผลข้อมูล

5.11.2 มีเอกสารขั้นตอนการปฏิบัติงาน ที่มีคำแนะนำในด้านต่างๆ เช่น การจัดเก็บ การดำเนินการเกี่ยวกับข้อมูล

5.11.3 การเปลี่ยนแปลงขั้นตอนการปฏิบัติงานต้องมีเอกสารควบคุม โดยมีการจัดทำบันทึกแยกแยะสิ่งที่เปลี่ยนแปลง มีการประเมินผลถึงผลกระทบจากการเปลี่ยนแปลง มีขั้นตอนการอนุมัติเป็นทางการ จัดทำความรับผิดชอบในกรณียกเลิกหรือล้มเหลวที่อาจเกิดขึ้น

5.11.4 มีขั้นตอนปฏิบัติกรณีมีเหตุสุดวิสัยเกิดขึ้น ขั้นตอนการปฏิบัติงานและการจัดการเหตุสุดวิสัยต้องจัดทำขึ้นเพื่อให้เกิดประสิทธิภาพ และความรวดเร็วอันอาจเกิดจาก ความล้มเหลวของระบบ การสูญเสียบริการ การปฏิเสธการให้บริการ ผลลัพธ์ที่ผิดพลาดจากข้อมูลที่ไม่สมบูรณ์ มีคู่มือการปฏิบัติสำหรับแผนบรรเทาปัญหา (Contingency plan) มีการตรวจสอบและหาหลักฐาน เพื่อใช้ในการวิเคราะห์ปัญหามีการปฏิบัติการกู้คืนระบบ

5.11.5 มีการจัดแยกหน้าที่หรือกิจกรรม ซึ่งเป็นวิธีการในการลดความเสี่ยงในกรณีที่ระบบถูกนำไปใช้ในทางที่ผิด

5.11.6 จัดการแยกอุปกรณ์ที่ใช้ในการพัฒนาระบบและอุปกรณ์ที่ใช้ปฏิบัติงานจริง โดยมีการกำหนดกฎเกณฑ์อย่างชัดเจนและเป็นลายลักษณ์อักษรในการเคลื่อนย้ายซอฟท์แวร์จากระบบที่พัฒนาไปสู่ระบบปฏิบัติงานจริง

5.11.7 มีการจัดอุปกรณ์สิ่งอำนวยความสะดวกต่างๆ ซึ่งการจัดสิ่งอำนวยความสะดวกต่างๆ เช่นการใช้คู่สัญญาจากภายนอกต้องมีการพิจารณาความเสี่ยง และต้องมีการควบคุมกำหนดกฎเกณฑ์ข้อตกลงในสัญญา

5.12 การวางแผน และการยอมรับระบบ (Simpson.2003)

การวางแผน และการยอมรับระบบ (System planning and acceptances)

5.12.1 มีวัตถุประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบให้น้อยลง การวางแผนล่วงหน้าที่ชัดเจนและการเตรียมการเป็นสิ่งจำเป็นเพื่อตอบสนองต่อความพร้อมใช้งานในทรัพยากรรวมทั้งสามารถมีข้อกำหนดการปฏิบัติงานที่เกี่ยวกับระบบใหม่ มีการจัดทำเป็นเอกสารและมีการทดสอบก่อนที่จะยอมรับและนำมาใช้งานจริง

5.12.2 ความสามารถในการวางแผน โดยผู้จัดการต้องตรวจสอบความสามารถของระบบและใช้ข้อมูลเพื่อแยกแยะและเพื่อหลีกเลี่ยงปัญหาคอขวดที่อาจเกิดขึ้น

5.12.3 การยอมรับระบบ เงื่อนไขการยอมรับระบบสารสนเทศที่จัดทำขึ้นใหม่ การอัพเกรดรวมทั้งเวอร์ชั่นใหม่ ควรจะมีการจัดทำการทดสอบที่เหมาะสมก่อนที่จะเป็นที่ยอมรับซึ่งเงื่อนไขยอมรับควรประกอบไปด้วย ประสิทธิภาพและความสามารถ การกู้คืนข้อผิดพลาด มีแผนบรรเทาปัญหา การจัดเตรียมและการทดสอบมีขั้นตอนการปฏิบัติเป็นประจำ มีข้อตกลงเกี่ยวกับความปลอดภัย มีคู่มือการปฏิบัติงานที่มีประสิทธิภาพ มีการจัดการฝึกอบรม มีหลักเกณฑ์การยืนยันการติดตั้งระบบใหม่ไม่ส่งผลกระทบกับระบบเก่า

5.12.4 มีการจัดการป้องกันต่อซอฟต์แวร์ประสงค์ร้าย (Malicious software) เพื่อปกป้องความมีบูรณภาพของซอฟต์แวร์และข้อมูล ซอฟต์แวร์ประสงค์ร้ายได้แก่ ไวรัสคอมพิวเตอร์ หนอนเครือข่าย ม้าโทรจัน และ ลอจิกบอมบ์

5.12.5 มีการจัดการควบคุมเพื่อต่อต้านซอฟต์แวร์ประสงค์ร้าย ควรมีคู่มือปฏิบัติงานให้ผู้ใช้งานคอมพิวเตอร์ระมัดระวังต่อซอฟท์แวร์ประสงค์ร้าย การควบคุมต้องมีประเด็นด้านเหล่านี้คือ มีนโยบายเกี่ยวกับซอฟท์แวร์ลิขสิทธิ์และการห้ามใช้ซอฟท์แวร์ที่ไม่ได้รับอนุญาต มีนโยบายเกี่ยวกับการป้องกันความเสี่ยงเกี่ยวกับการได้รับแฟ้มข้อมูลจากเครือข่ายภายนอกหรือจากสื่อต่างๆ มีการติดตั้งและอัพเดตซอฟต์แวร์ต่อต้านไวรัสเป็นประจำ มีการตรวจสอบไฟล์ที่แนบมากับเมล์ มีการจัดสรรความรับผิดชอบในการกู้คืน มีการจัดทำสำรองข้อมูลและซอฟต์แวร์ มีขั้นตอนตรวจสอบข้อมูลสารสนเทศเกี่ยวกับซอฟท์แวร์ประสงค์ร้ายและการแจ้งเตือน

5.12.6 มีการจัดการลักษณะงานแบบแม่บ้าน (Housekeeping) วัตถุประสงค์เพื่อรักษาไว้ซึ่งความมีบูรณภาพและความพร้อมใช้งานของการประมวลผลข้อมูลและบริการติดต่อสื่อสารเครือข่าย ได้แก่ งานที่เกี่ยวกับ

5.12.7 การทำสำรองข้อมูล (Information back-up) การสำรองข้อมูลทางธุรกิจที่สำคัญและการสำรองซอฟท์แวร์ควรทำเป็นปกติประจำ และมีการเก็บไว้สถานที่ที่แยกจากกัน

5.12.8 การจัดการบันทึกงานปฏิบัติการ (Operator logs) พนักงานปฏิบัติการควรเก็บบันทึกกิจกรรมต่างๆ ที่ประกอบไปด้วย เวลาในการเริ่มต้น และเสร็จสิ้นของระบบ การทำงานผิดพลาดและการแก้ไข ผู้รับผิดชอบในการจัดทำบันทึก

5.12.9 การเก็บรายงานบันทึกความผิดพลาด (Fault logging) ความผิดพลาดที่เกิดขึ้นควรมีการจัดทำรายงานบันทึกและแก้ไขที่ถูกต้อง โดยมีการตรวจสอบความผิดพลาด รวมทั้งทบทวนเครื่องมือที่ใช้ในการแก้ไขข้อผิดพลาด

5.12.10 การจัดการเครือข่าย (Network management) วัตถุประสงค์เพื่อทำให้เกิดความมั่นใจถึงวิธีการป้องกันข้อมูลในเครือข่าย และการปกป้องโครงสร้างพื้นฐานต่างๆ

5.12.11 การควบคุมเครือข่าย ผู้จัดการเครือข่ายต้องประยุกต์ใช้เครื่องมือป้องกันข้อมูลในเครือข่ายรวมทั้งป้องกันการเชื่อมต่อจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยพิจารณาจากมีการจัดความรับผิดชอบและขั้นตอนการจัดการอุปกรณ์ระยะไกล มีการควบคุมเป็นพิเศษกับข้อมูลที่เคลื่อนย้ายในเครือข่ายสาธารณะเพื่อคงไว้ซึ่งความลับ ความมีบูรณภาพของข้อมูล มีการจัดการกิจกรรมและบริการต่างๆ ทางธุรกิจให้สอดคล้องกับโครงสร้างพื้นฐานของการประมวลผลข้อมูล

5.12.12 การจัดการจัดเก็บสื่อบันทึก และความปลอดภัยของสื่อบันทึก (Media handling and security) เพื่อป้องกันทรัพย์สินเสียหายและการชะงักงันทางกิจกรรมของธุรกิจ ต้องมีการควบคุมและป้องกันทางกายภาพและมีขั้นตอนการปฏิบัติงานที่เหมาะสมเพื่อปกป้องสื่อบันทึกคอมพิวเตอร์ ได้แก่ เทป ดิสก์ คาสเซ็ท ข้อมูลนำเข้าและนำออก เอกสารระบบ

5.12.13 การจัดการเกี่ยวกับการเคลื่อนย้ายสื่อบันทึกคอมพิวเตอร์ควรมีขั้นตอนจากฝ่ายบริหาร เช่น มีการทำลาย มีการอนุญาตเป็นทางการสำหรับการเคลื่อนย้าย มีการจัดเก็บในที่ที่ปลอดภัยและมีสภาพแวดล้อมที่ปลอดภัย

5.12.14 การกำจัดสื่อบันทึก (Disposal of media) สื่อบันทึกที่ไม่ต้องการต้องมีการกำจัดอย่างปลอดภัย ควรมีขั้นตอนการปฏิบัติเพื่อลดความเสี่ยงโดยพิจารณาจากประเด็นต่อไปนี้ สื่อบันทึกได้แก่ กระดาษเอกสาร เทปบันทึก กระดาษพิมพ์เขียว กระดาษรายงาน กระดาษผงหมึก เทปแม่เหล็ก แผ่นดิสก์ คาสเซ็ท ออฟติคัลดิสก์ โปรแกรมต่างๆ ข้อมูลทดสอบ เอกสารระบบ เป็นต้น มีการจัดทำบันทึกเป็นลายลักษณ์อักษร

5.12.15 จัดทำขั้นตอนในการจัดเก็บข้อมูลเพื่อป้องกันการเปิดเผยข้อมูลและการใช้ในทางที่ผิด ขั้นตอนการปฏิบัติควรแยกสำหรับเอกสาร ระบบคอมพิวเตอร์ เครือข่าย โมบายเมล์ เสียง มัลติมีเดีย อุปกรณ์ไปรษณีย์ แฟกซ์ มีขั้นตอนการปฏิบัติคือ มีการจัดทำและมีสัญลักษณ์สำหรับสื่อบันทึกทุกรายการ จำกัดบุคคลและการอนุญาตการเข้าถึง จัดทำบันทึกรายการสำหรับผู้รับข้อมูล

5.12.16 การจัดการความปลอดภัยกับเอกสารของระบบ เอกสารของระบบได้แก่ข้อมูลที่มีความสำคัญ เช่น คำบรรยายการทำงานของแอพพลิเคชั่น ขั้นตอนการทำงาน โครงสร้างข้อมูล

ซึ่งต้องมีการจัดเก็บอย่างปลอดภัยและอนุญาตเฉพาะผู้เป็นเจ้าของแอพพลิเคชั่น เมื่อมีการแลกเปลี่ยนในเครือข่ายสาธารณะต้องปกป้องคุ้มครองด้วย

5.12.17 การแลกเปลี่ยนข้อมูล และซอฟต์แวร์

เพื่อป้องกันการสูญหาย การดัดแปร การใช้ในทางที่ผิดของข้อมูลซึ่งเกิดการแลกเปลี่ยนระหว่างองค์กร

5.12.17.1 ทำการค้าร่วมกันต้องมีเอกสารข้อตกลงระหว่างกันในการทำการค้าผ่านอิเล็กทรอนิกส์รวมทั้งมีรายละเอียดการอนุญาตการเข้าถึงข้อมูล

5.12.17.2 มีการทำข้อตกลงว่าด้วยการแลกเปลี่ยนข้อมูลและซอฟต์แวร์ ข้อตกลงอย่างเป็นทางการควรจัดทำขึ้นสำหรับการแลกเปลี่ยนข้อมูลหรือซอฟท์แวร์ระหว่างองค์กร ซึ่งข้อตกลงรวมถึงการจัดส่ง ความรับผิดชอบของผู้ส่ง มีมาตรฐานฉลากติดระหว่างองค์กรในเรื่องของลิขสิทธ์และมีการจัดทำการเข้ารหัส

5.12.17.3 มีการจัดการความปลอดภัยสื่อบันทึกระหว่างจัดส่ง เนื่องจากการขนส่งข้อมูลอาจเกิดการเข้าถึงโดยไม่ได้รับอนุญาต มีการขัดจังหวะในขณะส่งทางกายภาพ การจัดส่งทางกายภาพต่างๆ ต้องใช้การจัดส่งที่เชื่อถือได้จากผู้ให้บริการจัดส่งพัสดุมีการบรรจุที่ดี

5.12.17.4 มีการจัดการความปลอดภัยอิเล็กทรอนิกส์เมล์

(1) การจัดการความเสี่ยง พิจารณาจากประเด็นต่างๆ เช่น ประเด็นจุดอ่อนของการเข้าถึง ประเด็นการดัดแปลงและการปฏิเสธการให้บริการ ประเด็นจุดอ่อนในเรื่องข้อบกพร่อง เช่น สถานที่ผู้รับ ประเด็นของผลกระทบต่อการติดต่อสื่อสารของขั้นตอนทางธุรกิจ ประเด็นด้านกฎหมาย ประเด็นด้านการตีความ ประเด็นด้านการควบคุมผู้ใช้การเข้าถึงจากระยะไกล

(2) มีการจัดทำนโยบายอิเล็กทรอนิกส์เมล์ ประกอบไปด้วย การโจมตีเมล์จากไวรัสการคุ้มครองแฟ้มข้อมูลแนบ ข้อแนะนำในกรณีห้ามใช้เมล์ การระบุความรับผิดชอบของลูกจ้างต่อการใช้เมล์ มีการเข้ารหัสข้อความ และการควบคุมด้านการพิสูจน์ตัวตน

5.12.18 การจัดการความปลอดภัยระบบสำนักงานอิเล็กทรอนิกส์ โดยมีการจัดทำนโยบายและข้อแนะนำสำหรับการลดความเสี่ยงต่อความปลอดภัยของระบบสำนักงานอิเล็กทรอนิกส์ ได้แก่ เอกสาร คอมพิวเตอร์ โมบาย เมล์ เสียง มัลติมีเดีย แฟกซ์ และอุปกรณ์สื่อสารอื่นๆ

5.12.19 ระบบการเผยแพร่ต่อสาธารณะ (Public available systems) ความเอาใจใส่ต่อการป้องกันบูรณภาพ ข้อมูลเผยแพร่ตีพิมพ์ในรูปอิเล็กทรอนิกส์ต้องมีการป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตซึ่งอาจนำมาซึ่งความเสื่อมเสียชื่อเสียงต่อสาธารณะขององค์กร เช่น ข้อมูลในเว็บเซิฟเวอร์ที่เข้าถึงได้ทางอินเตอร์เน็ตจะต้องมีข้อมูลที่สอดคล้องกับกฎหมาย กฎเกณฑ์ ข้อบังคับ จะต้องได้รับอนุญาตอย่างเป็นทางการก่อนเผยแพร่สู่สาธารณะ ซอฟต์แวร์ ข้อมูล สารสนเทศอื่นๆ ที่ต้องการความมีบูรณภาพอย่างสูงแต่ถูกนำไปเผยแพร่ในที่สาธารณะจะต้องได้รับการปกป้องโดยกลไกที่เหมาะสม เช่น ลายเซ็นดิจิทัล รวมทั้งข้อมูลแบบสอบถามตอบกลับจะต้องได้รับการคุ้มครองตามกฎหมาย

5.12.20 การแลกเปลี่ยนข้อมูลสารสนเทศในรูปแบบอื่นๆ ต้องมีขั้นตอนการปฏิบัติงานและเครื่องมือควบคุมต่างๆ ที่จัดทำขึ้นเพื่อป้องกันการแลกเปลี่ยนข้อมูลที่ส่งผ่านด้วยเสียงโทรสาร วีดีโอ รวมทั้งมีการกำหนดนโยบายสำหรับการปฏิบัติงานแก่ผู้ใช้งานซึ่งเกี่ยวข้องประเด็น เช่น การเตือนให้พนักงานระมัดระวังในการไม่เปิดเผยข้อมูลวิกฤต การถูกดักฟัง การแทร็บสายข้อมูล ส่งถึงผู้รับปลายทางที่ถูกต้อง การเตือนพนักงานไม่ให้เปิดเผยข้อมูลที่เป็นความลับต่อสาธารณะ การใช้โทรสารติดต่อปลายทางที่ถูกต้อง

5.13 การควบคุมการเข้าถึง (Simpson.2003)

การควบคุมการเข้าถึง (Access Control) เป็นการกำหนดความต้องการทางธุรกิจเพื่อการควบคุมการเข้าถึง โดยมีวัตถุประสงค์เพื่อควบคุมการเข้าถึงข้อมูล การควบคุมการเข้าถึงข้อมูล และขั้นตอนการทำงานของธุรกิจควรได้รับการควบคุม โดยเป็นไปตามความต้องการทางธุรกิจ และความปลอดภัยโดยต้องมีการกำหนดนโยบายสำหรับการอนุญาต และการเผยแพร่ข้อมูลให้รับรู้

5.13.1 นโยบายควบคุมการเข้าถึง

5.13.1.1 การจัดทำนโยบาย และความต้องการทางธุรกิจ คือความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึงควรกำหนด และจัดทำเป็นเอกสารให้ชัดเจน การควบคุมการเข้าถึงต้องมีกรรมสิทธิ์สำหรับพนักงานหรือกลุ่มพนักงานที่ชัดเจนในนโยบายโดยที่นโยบายควรเกี่ยวข้องกัน เช่น การกำหนดความต้องการของแต่ละบุคคลสำหรับแอพพลิเคชั่น จัดแยกชนิดของข้อมูลที่เกี่ยวกับแอพพลิเคชั่นธุรกิจ ความสอดคล้องระหว่างการควบคุมการเข้าถึงกับชนิดของข้อมูลที่จัดแยก กฎหมาย ข้อบังคับที่สอดคล้อง เป็นต้น

5.13.1.2 มีการจัดทำกฎในการควบคุมการเข้าถึงโดยมีกฎเกณฑ์ในการบังคับใช้

5.13.1.3 มีการจัดการการเข้าถึงของผู้ใช้งาน (User registration) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตในระบบสารสนเทศ ขั้นตอนการปฏิบัติที่เป็นทางการต้องจัดทำ

ขึ้นเพื่อจัดสรรสิทธิ์ในการเข้าถึงในระบบสารสนเทศและบริการสารสนเทศ โดยขั้นตอนจะต้องควบคุมตั้งแต่การลงทะเบียนของผู้ใช้ใหม่จนถึงการถอนการลงทะเบียน

5.13.1.4 การลงทะเบียนผู้ใช้ (User registration) ต้องมีขั้นตอนปฏิบัติที่เป็นทางการเกี่ยวกับการลงทะเบียน และการถอนการลงทะเบียนเพื่อประกาศการใช้สิทธิ์ของผู้ใช้ต่างๆ เช่น มีการใช้ชื่อผู้ใช้ที่เป็นรหัสประจำตัวเฉพาะ (Unique ID) ต้องมีการแบ่งระดับในการเข้าถึง ให้ผู้ใช้มีลายลักษณ์อักษรในการเข้าถึงข้อมูล จัดทำบันทึก และมีการตรวจสอบ

5.13.1.5 มีการจัดการสิทธิ์ส่วนบุคคล โดยต้องมีการควบคุมสำหรับการจัดสรร และการใช้สิทธิ์ส่วนบุคคลในการเขียนทับกับระบบ และแอพพลิเคชั่น ฐานข้อมูล สำหรับระบบที่มีผู้ใช้หลายฝ่าย

5.13.1.6 การจัดการรหัสผ่านผู้ใช้(User password management)การจัดการรหัสผ่านมีแนวคิดคือ

-ให้พนักงานเก็บรหัสผ่านของตนเองและของกลุ่มเป็นความลับโดยมีการระบุไว้ในสัญญาจ้างงาน

-ให้พนักงานเก็บรหัสผ่านของตนเองเป็นความลับ รหัสผ่านชั่วคราวที่สร้างขึ้นสำหรับผู้ใช้ที่ลืมรหัสผ่านจะต้องบังคับให้เปลี่ยนแปลง

-รหัสผ่านชั่วคราวที่สร้างให้ผู้ใช้ควรส่งผ่านด้วยวิธีการที่ปลอดภัยไม่ควรอยู่ในรูปข้อมูลกระจ่าง

-รหัสผ่านไม่ควรเก็บในคอมพิวเตอร์ที่ไม่ได้ถูกป้องกัน ควรใช้เทคโนโลยีในการระบุตัวตนและการพิสูจน์ตัวตน

5.13.1.7 มีการตรวจสอบการให้สิทธิ์ผู้ใช้ ควรมีการตรวจสอบเป็นช่วงระยะเวลา ทุก 6 เดือน และทุก 3 เดือนสำหรับการขออนุญาตสำหรับสิทธิพิเศษ

5.13.1.8 ความรับผิดชอบผู้ใช้ (User responsibilities) เพื่อป้องกันการเข้าถึงของผู้ใช้ที่ไม่ได้รับอนุญาตความร่วมมือของผู้ใช้ที่ได้รับอนุญาตมีความจำเป็นต่อความปลอดภัยที่มีประสิทธิภาพ

5.13.1.9 การใช้รหัสผ่าน (Password use) ต้องเก็บรหัสผ่านเป็นความลับ หลีกเลี่ยงการใช้กระดาษจดรหัสผ่าน เปลี่ยนรหัสผ่านเมื่อมีสิ่งชี้บอกว่าเกิดความไม่ปลอดภัย เลือกใช้รหัสผ่านที่มีคุณภาพอย่างต่ำ 6 ตัวอักษร จำได้ง่าย บุคคลอื่นเดาไม่ได้ หรือไม่เกี่ยวข้องกับชื่อเบอร์โทรศัพท์ วันเกิดเป็นต้น ไม่เป็นตัวเลขหรือตัว

หนังสือล้วน มีการเปลี่ยนรหัสผ่านเป็นช่วงและไม่ใช้รหัสผ่านที่ใช้มาแล้ว เปลี่ยนรหัสผ่านชั่วคราวเมื่อล็อกออกครั้งแรก ไม่ให้มีการแบ่งกันใช้รหัสผ่าน

5.13.1.10 การจัดการอุปกรณ์อื่นๆ ของพนักงานผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ต่างๆ ต้องได้รับการป้องกันเช่นเสร็จงานให้ปิดเซสชั่น มีการล็อกออฟ ติดกุญแจเป็นต้น

5.13.2 การควบคุมการเข้าถึงเครือข่าย (Network access control) มีวัตถุประสงค์เพื่อป้องกันคุ้มครองบริการเครือข่าย คือการเข้าถึงบริการเครือข่ายทั้งจากภายใน และภายนอกต้องมีการควบคุมเพื่อที่ว่าผู้ใช้ ผู้มีสิทธิ์ในเครือข่าย และบริการเครือข่ายทำให้เกิดความไม่ปลอดภัยกับเครือข่ายทั้งนี้เพื่อก่อให้เกิดสิ่งต่อไปนี้

5.13.2.1 มีการติดต่ออย่างเหมาะสมระหว่างเครือข่ายองค์กร และเครือข่ายขององค์กรอื่นๆ หรือ เครือข่ายสาธารณะ

5.13.2.2 เพื่อกลไกการพิสูจน์ตัวตนที่เหมาะสมสำหรับผู้ใช้และอุปกรณ์

5.13.2.3 ควบคุมผู้ใช้ในการเข้าถึงบริการข้อมูล

5.13.3 นโยบายการใช้บริการเครือข่าย โดยนโยบายจะต้องกล่าวถึงสิ่งต่อไปนี้ เครือข่ายและบริการใดที่ให้บริการการเข้าถึง

5.13.3.1 ขั้นตอนการปฏิบัติสำหรับการอนุญาตว่าบุคคลใดที่ได้รับอนุญาตให้เข้าถึงเครือข่ายและบริการเครือข่าย

5.13.3.2 มีการจัดการควบคุมและขั้นตอนในการปกป้องคุ้มครองการเข้าถึงการเชื่อมต่อเครือข่ายและบริการเครือข่าย

5.13.4 มีการควบคุมเส้นทางการสื่อสารในเครือข่าย คือเส้นทางจากเครื่องผู้ใช้ไปยังเครื่องบริการต้องมีการควบคุม เครือข่ายต้องมีการออกแบบให้มีการแบ่งปันทรัพยากรและมีความยืดหยุ่นเรื่องเร้าท์ติ้ง มีการควบคุมเพื่อลดความเสี่ยง เพื่อป้องกันผู้ใช้เลือกเส้นทางภายนอกอื่นๆ

5.13.5 มีการพิสูจน์ตัวตนสำหรับการเชื่อมต่อภายนอก เช่นการเข้าถึงจากระยะไกลควรมีการเข้ารหัสในการพิสูจน์ตัวตน

5.13.6 มีการพิสูจน์ตัวตนในโหมดต่างๆ

5.13.7 มีการควบคุมพอร์ตต่างๆ ที่เข้าถึงระยะไกล สำหรับเครื่องคอมพิวเตอร์และระบบโทรคมนาคม

5.13.8 มีการแบ่งแยกเครือข่ายสำหรับเครือข่ายในองค์กรและเครือข่ายภายนอกที่ใช้ติดต่อกัน

5.13.9 มีการควบคุมการเชื่อมต่อเครือข่าย มีการกำหนดค่าเกตเวย์ ทราฟฟิก เครื่องเมล์เซิฟเวอร์ การโอนถ่ายข้อมูลให้เป็นทางเดียวหรือสองทาง

5.13.10 มีการควบคุมเส้นทางเครือข่าย (Network routing control) ควรมีการกำหนดตรวจสอบต้นทางและปลายทางให้ถูกต้อง

5.13.11 มีการจัดการความปลอดภัยของบริการเครือข่ายอื่นๆ ให้มีความปลอดภัย

5.13.12 การจัดการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) โดยเพื่อป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาต

5.13.13 ต้องมีการแยกแยะตัวบุคคลอย่างอัตโนมัติที่เทอร์มินัล โดยมีการพิสูจน์ตัวตนสำหรับการเข้าถึง

5.13.14 มีขั้นตอนวิธีการล็อกออนสู่เทอร์มินัล จำนวนครั้งที่อนุญาต มีข้อความแสดงถึงความสำเร็จหรือล้มเหลว เป็นต้น

5.13.15 มีการแยกแยะผู้ใช้และการพิสูจน์ตัวตนคือผู้ใช้ทุกคนต้องมีรหัสประจำตัวที่เป็นเลขประจำตัวผู้ใช้

5.13.16 มีการจัดการรหัสผ่านที่ป้องกันความปลอดภัย เช่น ผู้ใช้สามารถเปลี่ยนได้ มีทางเลือกสำหรับการเลือกใช้ สามารถบังคับผู้ใช้เปลี่ยนรหัสผ่านได้

5.13.17 มีการจัดการเรื่องการใช้โปรแกรมอรรถประโยชน์ที่สามารถทำลายระบบปฏิบัติการได้

5.13.18 มีการจัดการระบบเตือนภัยหรือความเสี่ยงให้ผู้ใช้ได้รับรู้อันตรายที่อาจเกิดขึ้น

5.13.19 มีการกำหนดช่วงเวลาปิดตัวของระบบเมื่อไม่มีการทำกิจกรรมใดๆ

5.13.20 มีความสามารถในการกำหนดเวลาในการเชื่อมต่อได้

5.13.21 มีการจัดการการควบคุมการเข้าถึงแอพพลิเคชั่น (Application access control) เพื่อป้องกันการถึงข้อมูลในระบบสารสนเทศโดยไม่ได้รับอนุญาต อุปกรณ์ความปลอดภัยต้องนำมาใช้จำกัดการเข้าถึงระบบแอพพลิเคชั่น การเข้าถึงซอฟท์แวร์และข้อมูลทางดิจิทัลต้องมีการกำหนดเพื่อผู้ใช้งานที่มีสิทธิ์เท่านั้น

5.13.22 การตรวจตราการเข้าถึง และการใช้ระบบ (Monitoring System access and use) เพื่อตรวจสอบกิจกรรมที่ไม่ได้รับอนุญาต ระบบควรจะมีการเฝ้าระวังตรวจตราการเข้าถึงและมีการจัดเก็บบันทึกเพื่อเป็นหลักฐานในกรณีเกิดเหตุสุดวิสัย โดยมีการบันทึกเหตุการณ์มีการตรวจตราการใช้ระบบมีขั้นตอนการปฏิบัติงานและขอบแขตความเสี่ยงเพื่อตรวจสอบผู้ใช้งาน มีการเข้าจังหวะสัญญานนาฬิการเพื่อเป็นหลักฐานในการตรวจตามวันและเวลาที่เกิดเหตุการณ์

5.13.23 การจัดการอุปกรณ์โมบายและการทำงานจากบ้าน (Mobile computing and teleworking) เพื่อเกิดความมั่นใจในความปลอดภัยของข้อมูลเพื่อใช้โมบายและอุปกรณ์ทำงานจากบ้านระยะไกล โดยอุปกรณ์โมบายได้แก่โน้ตบุ๊ค ปาล์ม แลปท็อปและมือถือต้องมั่นใจว่า

ข้อมูลทางธุรกิจไม่เสียหายมีการสำรองข้อมูล การทำงานจากบ้านระยะไกลจะต้องมีการใช้เทคโนโลยีสื่อสารต่างๆ เพื่อให้พนักงานทำงานจากนอกสถานที่ที่เป็นหลักแหล่งภายนอกองค์กร และต้องมีการจัดการป้องกันที่เหมาะสม

5.14 การพัฒนาระบบและการบำรุงรักษา (Simpson.2003)

การพัฒนาระบบ และการบำรุงรักษา (System Development and Maintenance) เป็นการเริ่มต้นการวิเคราะห์ความต้องการความปลอดภัย และหาวิธีการในการควบคุมในทุกๆ ขั้นตอน เช่น การป้อนข้อมูล การประมวลผลข้อมูล การจัดเก็บข้อมูล และการสืบค้นข้อมูล จึงมีความจำเป็นต้องกำหนดนโยบายในการควบคุมการพัฒนาระบบ และการบำรุงรักษา ดังรายละเอียดต่อไปนี้

5.14.1 มีการกำหนดความต้องการด้านความปลอดภัยในระบบที่สร้างขึ้น

5.14.2 มีการกำหนดความปลอดภัยในระบบแอพพลิเคชั่น วัตถุประสงค์เพื่อป้องกันข้อมูลของผู้ใช้งานสูญหาย มีการดัดแปลงและนำไปใช้ในทางที่ผิดในระบบแอพพลิเคชั่น

5.14.3 มีการตรวจสอบการนำเข้าข้อมูล (Input data validation) การนำข้อมูลเข้าระบบแอพพลิเคชั่นต้องมีการตรวจสอบให้เกิดความมั่นใจว่าถูกต้องและเหมาะสม การตรวจสอบต้องเกิดขึ้นในขั้นตอนการนำข้อมูลเข้าในการประมวลผลและมีการตรวจสอบข้อผิดพลาดอื่นๆ เช่น ค่าตัวเลขที่เกินจากช่วงที่กำหนด

5.14.4 มีการควบคุมการประมลผลภายใน (Internal processing) ได้แก่มีการจัดขอบเขตของความเสี่ยงที่อาจเกิดขึ้นในโปรแกรม มีการตรวจสอบและการควบคุมต่อผลกระทบที่อาจเกิดกับข้อมูล มีการพิสูจน์ตัวตนข้อความ (Message authentication) ต้องมีการจัดทำขึ้นในแอพพลิเคชั่นที่ต้องการความปลอดภัยในเรื่องของความมีบูรณภาพของเนื้อหาของข้อความ

5.14.5 มีการควบคุมโดยการเข้ารหัส (Cryptographic controls) เพื่อก่อให้เกิดความลับ การพิสูจน์ตัวตนและความมีบูรณภาพของข้อมูล ระบบการเข้ารหัสและเทคนิคการเข้ารหัสควรนำมาใช้เพื่อปกป้องข้อมูลที่พิจารณาแล้วว่ามีความเสี่ยงและเนื่องจากเครื่องมือปกป้องอื่นๆ ไม่สามารถทำได้

5.14.5.1 นโยบายในการกำหนดใช้การเข้ารหัส ขึ้นอยู่กับการประเมินผลความเสี่ยงที่เกิดขึ้นว่ามีความเหมาะสมนำมาใช้ในองค์กรมากน้อยเพียงใด การกำหนดนโยบายพิจารณาโดยความสำคัญของข้อมูลทางธุรกิจ แนวคิดของการจัดการกุญแจเข้ารหัส บทบาทและบุคคลรับผิดชอบ ระดับในการคุ้มครองการเข้ารหัส มาตรฐานที่จะนำมาใช้ในองค์กร

5.14.5.2 การเข้ารหัส (Encryption) เป็นเทคนิคที่ใช้ปกป้องความลับของข้อมูลและข้อมูลวิกฤต

5.14.5.3 ลายเซ็นดิจิทัล (Digital signatures) เป็นการป้องกันโดยใช้วิธีพิสูจน์ตัวตนและความมีบูรณภาพของเอกสารอิเล็กทรอนิกส์ เช่น ใช้ในการค้าอิเล็กทรอนิกส์ โดยมีข้อพึงระวังในการรักษากุญแจส่วนตัว

5.14.5.4 บริการการห้ามปฏิเสธความรับผิดชอบ (Non – repudiation services) บริการการห้ามปฏิเสธความรับผิดควรพิจารณานำมาใช้เพื่อแก้ปัญหาการโต้แย้งเกี่ยวกับเหตุการณ์ที่อาจเกิดขึ้นหรืออาจไม่เกิดขึ้นเกี่ยวกับการกระทำต่างๆ

5.14.5.5 การจัดการกุญแจ (Key management) ต้องคำนึงถึงการคุ้มครองกุญแจเข้ารหัส การจัดการกับกุญแจเข้ารหัสเป็นสิ่งสำคัญและการสูญหายหรือเปิดเผยมีผลต่อความลับ การพิสูจน์ตัวตนและความมีบูรณภาพของข้อมูล ต้องมีมาตรฐาน ขั้นตอนการปฏิบัติและวิธีการใช้กุญแจ การสร้างกุญแจ ใบรับรองกุญแจสาธารณะ การแจกจ่ายกุญแจไปยังผู้รับกุญแจ การแลกเปลี่ยนและการอัพเดตกุญแจ การทำลายกุญแจ การกู้คืนกุญแจต้องมีการพิจารณาเป็นอย่างดี

5.14.6 การจัดการความปลอดภัยระบบแฟ้มข้อมูล (Security of system files) เพื่อให้เกิดความมั่นใจว่าโครงการด้านไอทีและกิจกรรมเกี่ยวข้องต่างๆ มีความปลอดภัยและการเข้าถึงแฟ้มข้อมูลได้รับการควบคุมที่ถูกต้อง

5.14.6.1 การควบคุมซอฟต์แวร์ที่ใช้งานอยู่ (Operational software) การควบคุมต้องมีการจัดทำอย่างเหมาะสมเพื่อมีการประยุกต์ใช้ซอฟท์แวร์ในระบบปฏิบัติงานที่ใช้อยู่ เพื่อลดความเสี่ยงในการขัดจังหวะของระบบที่ทำงานอยู่

5.14.6.2 การปกป้องข้อมูลที่ใช้ทดสอบระบบ ข้อมูลทดสอบต้องได้รับการควบคุม ต้องมีการแยกฐานข้อมูลที่ใช้งานอยู่กับข้อมูลที่ใช้ทดสอบ

5.14.6.3 การควบคุมการเข้าถึงไลบรารี่ของโปรแกรม (Program source library) เพื่อที่จะลดโอกาสในการขัดจังหวะของโปรแกรมคอมพิวเตอร์

5.14.7 การจัดการความปลอดภัยในขั้นตอนการพัฒนาและการสนับสนุนระบบ (Development and support process) เพื่อคงไว้ซึ่งความปลอดภัยในระบบแอพพลิเคชั่นและข้อมูลสารสนเทศ โดยมีขั้นตอนการปฏิบัติเกี่ยวกับการควบคุมการเปลี่ยนแปลงระบบซึ่งต้องมีขั้นตอนที่บังคับใช้อย่างเป็นทางการ การทบทวนเชิงเทคนิคสำหรับการเปลี่ยนแปลงกับระบบที่ใช้งานอยู่ จะต้องมีการทวนสอบและการทดลองก่อนนำไปใช้กับระบบงานจริง สำหรับการลงแพ็ท การติดตั้งโค้ดใหม่ มีการจำกัดการเปลี่ยนแปลงสำหับซอฟต์แวร์

แพคเกจ ซึ่งเป็นซอฟท์แวร์ที่พัฒนามาจากผู้ค้าซึ่งการเปลี่ยนแปลงต้องพิจารณาในเรื่องของความเสี่ยงของการควบคุมและความมีบูรณภาพของการประมวลผล และมีการระมัดระวังเรื่องการทำงานที่ผิดปกติของโค้ดต่างๆ หรือ โค้ดโทรจัน นอกจากนี้การจ้างเอ้าซอสเพื่อพัฒนาโปรแกรมต้องมีข้อตกลงเกี่ยวกับสิทธิทางปัญญาในร้างรองคุณภาพและความถูกต้อง การจัดการความล้มเหลวที่อาจเกิดขึ้น ข้อตกลงทางสัญญาเกี่ยวกับคุณภาพของโค้ด มีการทดสอบก่อนติดตั้งเพื่อตรวจดูโค้ดโทรจันเป็นต้น

5.15 การจัดการธุรกิจให้ธุรกิจดำเนินงานต่อเนื่อง (Simpson.2003)

การจัดการธุรกิจให้ธุรกิจดำเนินงานต่อเนื่อง (Business continuity management) คือ คุณลักษณะของการจัดการธุรกิจให้ดำเนินงานต่อเนื่อง มีวัตถุประสงค์เพื่อตอบสนองต่อการชะงักงันของธุรกิจและป้องกันกระบวนการวิกฤตทางเศรษฐกิจอันเกิดจากผลกระทบของความล้มเหลวของความปลอดภัย และการสูญเสียการใช้บริการต่างๆ และมีการจัดทำแผนบรรเทาปัญหา (Contingency plan) เพื่อทำให้ขั้นตอนการทำงานทางธุรกิจสามารถกู้คืนกลับมาทำงานได้ตามปกติ

5.15.1 มีขั้นตอนการจัดการดำเนินงานให้ต่อเนื่อง ควรมีขั้นตอนการจัดการ ในการพัฒนาและการคงไว้ซึ่งการดำเนินงานต่อเนื่องทั่วทั้งองค์กร โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้น โดยทำการแยกแยะและจัดลำดับสำคัญของหน่วยงานที่วิกฤต เข้าใจผลกระทบที่เกิดจากการทำให้ธุรกิจชะงักงัน พิจารณาซื้อประกันภัยที่เหมาะสม จัดทำกลยุทธ์และเอกสารการทำงานต่อเนื่อง ทดสอบและปรับปรุงแผนงานเป็นประจำและแผนงานต้องสอดคล้องกับขั้นตอนการทำงานและโครงสร้างองค์กร

5.15.2 การดำเนินงานต่อเนื่องของธุรกิจและการวิเคราะห์ผลกระทบ คือการดำเนินงานต่อเนื่องของธุรกิจควรจะมีการจำแนกแยกแยะเหตุการณ์ต่างๆ ที่อาจทำให้ขั้นตอนการทำงานของธุรกิจชะงักงัน เช่นอุปกรณ์ไม่ทำงาน ไฟไหม้ และ ต้องจัดการทำการประเมินความเสี่ยงเพื่อหาผลกระทบที่ทำให้เกิดการชะงักงันได้ โดยจะต้องให้ผู้เป็นเจ้าของขั้นตอนการทำงานนั้นๆ เข้ามามีส่วนร่วมทำงาน เพื่อให้ได้ผลประเมินความเสี่ยงแล้วต้องมีการจัดทำแผนกลยุทธ์โดยฝ่ายบริหารประกาศใช้ในองค์กร

5.15.3 การเขียนแผนงานต่อเนื่องและการประยุกต์ใช้ แผนงานควรจะพัฒนาขึ้นมาเพื่อคงไว้หรือกู้คืนการทำงานของธุรกิจให้กลับคงเดิมในช่วงระยะวลาที่ต้องการได้ โดยขั้นตอนการทำแผนพิจารณาประเด็นต่างๆ คือ ทำการจำแนกแยกแยะและทำข้อตกลงในส่วนของความรับผิดชอบและขั้นตอนปฏิบัติงานฉุกเฉิน และมีการจัดการประยุกต์ใช้ขั้นตอน

การทำงานฉุกเฉิน มีเอกสารเกี่ยวกับข้อตกลงด้านการทำงานและขั้นตอนการปฏิบัติงาน ให้ความรู้แก่พนักงาน จัดทำการทดสอบและปรับปรุงแผนอยู่เสมอ

5.15.4 โครงแบบของแผนงานต่อเนื่อง (Business continuity planning framework) โครงแบบของแผนงานต่อเนื่องต้องพิจารณาในประเด็นในเรื่องต่างๆ คือ แผนงานการอพยพ ขั้นตอนปฏิบัติกรณีฉุกเฉิน ขั้นตอนในการกลับคืน ขั้นตอนปฏิบัติการกลับสภาพเดิมการจัดตารางการบำรุงรักษา มีกิจกรรมให้ความรู้และการระมัดระวัง มีการจัดสรรความรับผิดชอบให้แก่บุคคล

5.15.5 การทดสอบ การบำรุงรักษาและการประเมินใหม่ สำหรับแผนการดำเนินงานให้ต่อเนื่อง

5.15.5.1 การทดสอบแผน การทดสอบอาจล้มเหลวได้เนื่องจากกำหนดสมมุติฐานของเหตุการณ์ผิดพลาด หรือเกิดจากการมองข้ามเหตุการณ์ไป การเปลี่ยนอุปกรณ์หรือบุคลากร จึงต้องมีการทดสอบเป็นประจำเพื่อเกิดความมั่นใจในประสิทธิผล การทดสอบควรทำเป็นหลายๆ เหตุการณ์ การทำเป็นทางเลือกต่าง การทดสอบการกู้คืน การทำสอบการจัดหาอุปกรณ์ของซัพพลายเออร์

5.15.5.2 การบำรุงรักษาและการประเมินแผนงานใหม่ คือ แผนงานต้องทบทวนอย่างต่อเนื่องและปรับปรุงอย่างต่อเนื่อง เช่น บุคคลรับผิดชอบ ที่อยู่ที่ติดต่อได้ กลยุทธ์ทางธุรกิจ ผู้จัดหาอุปกรณ์ ความเสี่ยงที่อาจเกิดขึ้น

5.16 ข้อบังคับอื่นๆ (Simpson.2003)

ข้อบังคับอื่นๆ (Compliance) มีวัตถุประสงค์เพื่อหลีกเลี่ยงอาชญากรรม กฎหมายแพ่งและพาณิชย์ กฎเกณฑ์ และข้อสัญญาต่างๆ มีลักษณะ คือ

5.16.1 มีการกำหนดนิยามพระราชบัญญัติต่างๆ และมีการจัดทำเป็นเอกสารสำหรับระบบสารสนเทศในแต่ละระบบและกำหนดบุคคลที่รับผิดชอบดูแล ข้อคำนึงด้านลิขสิทธิ์ทางปัญญา ได้แก่ copyright software copyright การป้องกันเอกสารบันทึกต่างๆที่สมควรต้องป้องกัน การปกป้องข้อมูลและข้อมูลส่วนบุคคล การป้องกันการใช้อุปกรณ์ต่างทางสารสนเทศในทางที่ผิด มีกฎเกณฑ์การควบคุมการเข้ารหัส มีการจัดการการรวบรวมหลักฐานในกรณีมีการละเมิดหรือทำผิดต่างๆ

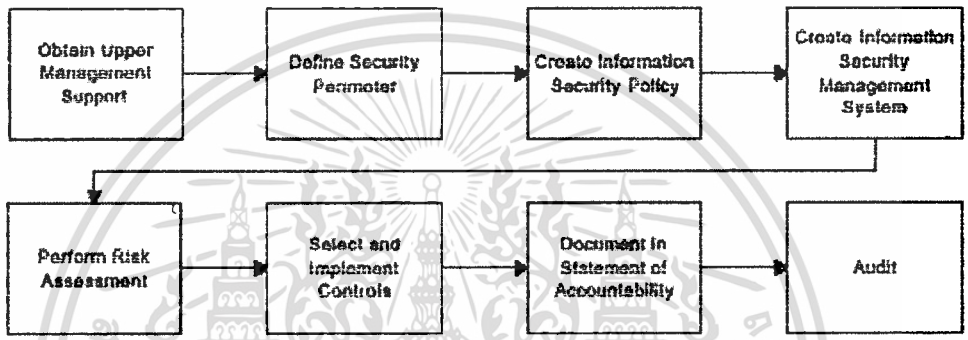
5.16.2 มีการทบทวนนโยบายความปลอดภัยและสิ่งประยุกต์ทางเทคนิคอื่นๆ เพื่อทำให้เกิดความเหมาะสมของนโยบายความปลอดภัยขององค์กรและตรงตามมาตรฐาน

5.16.3 มีการทวนสอบระบบ (System audit consideration) เพื่อก่อให้เกิดประสิทธิภาพสูงสุดและป้องกันการแทรกแซงให้น้อยที่สุด โดยมีกระบวนการทวนสอบหรือเจาะระบบ

บทที่ 6

การวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศ

การวิเคราะห์ และออกแบบรูปแบบการจัดการความปลอดภัยสารสนเทศตามมาตรฐาน ISO 17799 มีกระบวนการดังแสดงในภาพที่ 6.1(Carlson T.2001)



ภาพที่ 6.1 กระบวนการ ISO 17799

6.1 ขั้นตอนการได้รับการสนับสนุนจากผู้บริหารระดับสูง (Obtain Upper Management Support)

ผู้บริหารระดับสูงต้องให้ความสำคัญกับการรักษาความปลอดภัยข้อมูลสารสนเทศ จะต้องให้การสนับสนุนในทุกๆด้าน เพื่อกระบวนการจะได้บรรลุวัตถุประสงค์ด้วยดี

6.2 ขั้นตอนกำหนดปริมณฑลความปลอดภัย หรือขอบเขตซึ่งการควบคุมความปลอดภัยมีบังคับใช้ในการปกป้องทรัพย์สิน (Define Security Perimeter) จะต้องทำการตอบคำถามต่อไปนี้อย่างชัดเจน

-ส่วนใดของธุรกิจต้องการความถูกต้องสมบูรณ์ ความพร้อมใช้งานของข้อมูล ที่มีความจำเป็นต้องใช้ในการตัดสินใจในการดำเนินธุรกิจ

-สิ่งใดที่พิจารณาแล้วเห็นว่าต้องทำการประเมินความเสี่ยงความปลอดภัยสารสนเทศ

-ข้อมูลสารสนเทศใดที่ต้องการการปกป้อง

-เป็นความต้องการความปลอดภัยสารสนเทศขององค์กรใด

ปัจจัยหลักในการกำหนดปริมณฑลความปลอดภัย หรือขอบเขตซึ่งการจัดการความปลอดภัยสารสนเทศ

-จัดทำแผนงานกลยุทธ์การรักษาความปลอดภัยสารสนเทศ

-จัดตั้งองค์กรความปลอดภัยสารสนเทศ

-จัดตั้งวิธีการจัดการความเสี่ยง

-พัฒนาการประเมินความเสี่ยง

-กำหนดโครงสร้างการปฏิบัติการความเสี่ยง

-กำหนดรายการทรัพย์สินสารสนเทศ

6.3 ขั้นตอนกำหนดนโยบายการรักษาความปลอดภัยสารสนเทศ (Create Information Security Policy)

การสร้างนโยบาย และหลักปฏิบัติเพื่อปกป้องสารสนเทศในองค์กร ให้มีความปลอดภัย การที่จะร่างนโยบายรักษาความปลอดภัยสำหรับบังคับใช้ทั่วทั้งองค์กร จะต้องมีความรู้ความเข้าใจในตัวองค์กรอย่างถี่ถ้วนเสียก่อน อันดับแรกคือ เราจะต้องศึกษาเป้าหมาย และทิศทางขององค์กรเสียก่อน โดยนโยบายที่จะร่างขึ้นนั้น จะต้องสอดคล้องกับเป้าหมาย และทิศทาง รวมไปถึงกฎระเบียบ ข้อบังคับ และกฎหมายที่ทางองค์กรใช้อยู่ สิ่งแรกที่ต้องดำเนินการต่อไปทันทีคือ การแต่งตั้งผู้ที่จะมาดูแลด้านนโยบายในฐานะเจ้าหน้าที่รักษาความปลอดภัยสารสนเทศ (Information Security Officer) ซึ่งอาจเป็นการจ้างผู้เชี่ยวชาญ มาทำงานโดยตรง หรือใช้พนักงานที่มีอยู่แล้วในองค์กร รับผิดชอบหน้าที่นี้โดยเฉพาะ การแต่งตั้งบุคคลที่เหมาะสมเพื่อควบคุมกระบวนการตั้งแต่ต้นจนจบมีความสำคัญอย่างมากต่อความสำเร็จ และความเชื่อมั่นของพนักงานทั่วไปที่มีต่อแผนงาน

6.4 ขั้นตอนการสร้างการจัดการการรักษาความปลอดภัยสารสนเทศ

การสร้างการจัดการการรักษาความปลอดภัยสารสนเทศ (Create Information Security Management System) เป็นการกำหนดนโยบาย มาตรฐาน วิธีการ แผน คณะกรรมการ และทีมงาน ที่มีการระบุหน้าที่อย่างชัดเจนให้เป็นไปตามมาตรฐาน ISO 17799 เพื่อนำเอานโยบายไปบังคับใช้ในการรักษาความปลอดภัย และการจัดการความปลอดภัยสารสนเทศ

6.5 ขั้นตอนการประเมินความเสี่ยงด้านความปลอดภัย

การประเมินความเสี่ยงด้านความปลอดภัย (Perform Security Risk Assessment) สำหรับระบบสารสนเทศ เป็นการวิเคราะห์ถึงโอกาสที่ระบบสารสนเทศอาจจะประสบกับภัยคุกคามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศในรูปแบบต่างๆ เช่น การทำลาย การเปิดเผย เปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ โดยเมื่อวิเคราะห์กำหนดถึงความบกพร่อง

(Vulnerabilities) และภัยคุกคาม (Threat) แล้วจากนั้นจึงวิเคราะห์ประเมินผลกระทบที่อาจต่อความปลอดภัย (Impact) และโอกาสเกิดภัยคุกคาม (Probability) ตามเกณฑ์ที่กำหนดไว้ เพื่อประเมินความเสี่ยง (Risk) อันจะนำไปสู่การกำหนดความต้องการด้านความปลอดภัย และกำหนดแนวทางมาตรการป้องกันระบบสารสนเทศให้มีความปลอดภัยต่อไป

การมุ่งประเด็นของแหล่งกำเนิดความเสี่ยงจะต้องตอบคำถามเหล่านี้

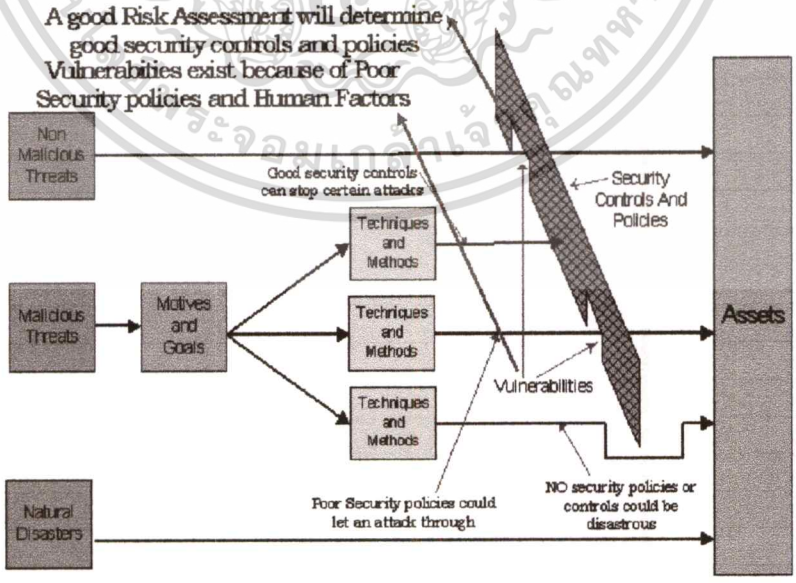
-อะไรทำให้เกิดความเสี่ยง

-ความเสี่ยงเกิดขึ้นได้อย่างไร

-ทำไมจึงเกิดความเสี่ยงนั้นๆขึ้น

-ใคร หรืออะไรที่ก่อให้เกิดความเสี่ยงขึ้นมา

การประเมินความเสี่ยงเป็นความสัมพันธ์ระหว่างภัยคุกคาม :จุดอ่อนช่องโหว่ : ทรัพย์สิน โดยการนำความสัมพันธ์ดังกล่าวมาร่วมพิจารณาในการประเมินความเสี่ยงอย่างมีประสิทธิภาพ จะทำให้การกำหนดวิธีการควบคุมความเสี่ยง รวมถึง นโยบายการรักษาความปลอดภัยเป็นไปอย่างถูกต้องตรงตามความต้องการมากที่สุด จุดอ่อนช่องโหว่อาจจะยังคงมีอยู่ ถ้าวิธีการควบคุมความเสี่ยง และนโยบายในการรักษาความปลอดภัยยังไม่ดีพอ ดังแสดงในภาพที่ 6.2



ภาพที่ 6.2 แสดงความสัมพันธ์ภัยคุกคาม :จุดอ่อนช่องโหว่ : ทรัพย์สิน

6.5.1 การวิเคราะห์ความเสี่ยงของระบบนั้นประกอบไปด้วยขั้นตอนใหญ่ ๆทั้งหมด 6 ขั้นตอน ได้แก่

6.5.1.1 ขั้นตอน Inventory, Definition, and Requirements การเข้ามาเก็บข้อมูล และเรียนรู้ทำความเข้าใจถึง "Business Process" ขององค์กรตลอดจนทำ Inventory ของ Hardware และ Software ที่ใช้งาน เพื่อเตรียมข้อมูลให้พร้อมในขั้นตอนต่อไป

6.5.1.2 ขั้นตอน Vulnerability & Threat Assessment การวิเคราะห์ช่องโหว่ และภัยต่าง ๆที่อาจเกิดขึ้นกับระบบทั้งระดับ Network Hosts ตลอดจน Application โดยเฉพาะอย่างยิ่ง "Web Application" ทุกวันนี้ การ Hack ส่วนใหญ่เกิดขึ้นกับ Web Sever ที่ไม่ได้ Harden หรือไม่ได้รับการดูแลลง Patch หรือ Hotfix อย่างสม่ำเสมอ ขั้นตอนนี้ต้องใช้ Tools ที่มีความสามารถในการเจาะระบบ และบุคลากรที่มีความชำนาญในการใช้ Tools ด้วยการที่บางองค์กรใช้ "Vulnerability Scanner" เช่น Internet Scanner จาก iss.net หรือ Nessus จาก nessus.org ตลอดจน Retina จาก eeye.com มาทำการวิเคราะห์เจาะหาช่องโหว่ก็ยังอาจไม่เพียงพอ หรือไม่สามารถเจาะเข้าสู่ระบบให้เห็นภาพชัดเจนได้ เพราะบุคลากรที่ใช้งาน Tools เหล่านี้ที่ไม่ได้เป็น Hacker หรือยังไม่มีสัญชาติญาณของ Hacker ตลอดจนยังไม่มี Skill ในระดับ Hacker ที่สามารถเจาะเข้าสู่ระบบได้ เราจึงอาจต้องทำการเจาะระบบโดยอาศัยความสามารถของ Professional Security Consultant หรือบริษัทที่รับงานด้านนี้ที่มีประสบการณ์เพียงพอที่จะเจาะเข้าสู่ระบบของเราได้ ในหลักการเราเรียกว่า การทำ "Penetration Test" หรืออีกนัยหนึ่งก็คือ " Ethical Hacking Our System" นั่นเอง การทำ "Vulnerability Assessment" ที่ดีนั้นเราควรจะได้รายงานผลดังนี้

— Network Mapping

ถ้า Attacker หรือ Hacker ที่ Hack เข้ามาจากภายนอก (จาก Internet) สามารถมองเห็นแผนผังของเครือข่ายของเราได้หรือไม่ โดยอาจจะดึงข้อ มูลจาก DNS Server ของเราที่ไม่ได้ป้องกัน Zone Transfer เป็นต้น

— Hosts and Services Discovery

การทำ Penetration Test สามารถได้ข้อมูลของ Host ที่อยู่ในระบบของเราหรือไม่ โดยควรจะแสดงให้เห็น IP Address ชนิดของ NOS ว่าเป็น Wind หรือ UNIX/Linux ตลอดจน Service ที่เปิดให้บริการอยู่ไม่ว่าจะเป็น HTTP Port 80 SMTP Port 25 หรือ SSH Port 22 เป็นต้น ข้อมูลของ Host นั้นควรจะเจาะได้เริ่มจาก Router ของเราที่ต่ออยู่กับ ISP แล้วมาที่ Firewall ตลอดจน Host ทั้งหมดที่อยู่

ใน DMZ (Demilitarized Zone) ถ้าสามารถเจาะเข้าถึง Host ที่อยู่ภายใน Internal Network (หลัง Firewall) ก็ยิ่งดี ในแง่ของการเจาะระบบแบบ Ethical Hacking แต่ไม่ดีแน่ ๆ ถ้าช่องโหว่ของระบบเราเปิดให้เข้าถึง Host ที่อยู่หลัง Firewall

- Vulnerability Analysis

เมื่อทราบถึง Host และ Service ที่เปิดอยู่แล้วควรรายงานช่องโหว่ของระบบที่มีอยู่ในแต่ละ Host ตลอดจนวิเคราะห์ว่า ถ้าช่องโหว่ถูกเจาะในระดับแรก แล้วจะมีการเจาะเพิ่มอีกในระดับต่อไปอย่างไร

- Vulnerability Measurement & Data Collection

ควรแสดงถึงขั้นตอนในการเจาะระบบให้ดูโดยละเอียด เพื่อความเข้าใจที่ดียิ่งขึ้น จะได้รู้ว่าควรป้องกันอย่างไรถึงจะได้ผล

- Security Design Review & Recommendation Identify Safeguard

หลังจากที่เราทราบแล้วว่าระบบเรามีช่องโหว่ก็ควรมีคำแนะนำในการออกแบบระบบให้มีความปลอดภัยมากกว่าที่เป็นอยู่โดยใช้หลักการ "Defense-in-Depth" กล่าวคือ ต้องพิจารณาเรื่องการ Hardening Host ต่าง ๆ การ Re-design Perimeter Network ใหม่ เช่น การ Re-config Firewall หรือ IDS ตลอดจน Screening Router, การ Implement IDS เพิ่มเติม, การ Encryption โดยใช้ SSL หรือ Server Shell, การกำหนด Security Polices & Procedures เช่น การใช้งาน Remote Access, การแก้ปัญหาในระดับ Application ตลอดจนการ Evaluate Source Code จากนั้นควรมีการพูดถึงการ Maintenance และ Monitoring อย่างต่อเนื่อง ตลอดจนแผนรองรับเหตุการณ์ที่อาจเกิดขึ้น (Incident Response)

จะเห็นได้ว่าขั้นตอนที่ 2 นั้นมีรายละเอียดปลีกย่อยค่อนข้างมาก และต้องการทีมงานที่มีประสบการณ์ และทักษะในด้าน Security ค่อนข้างสูง ดังนั้นการเลือกบริษัทที่จะมาทำแบบ Security Assessment นั้น จึงต้องพิจารณาอย่างรอบคอบ

6.5.1.3 ขั้นตอน "Evaluation of Control" หมายถึง การประเมินมูลค่าของ "Control" ที่ถูกนำมาใช้ในการลดผลกระทบของความเสี่ยง (Mitigate Risk) ในขั้นตอนนี้เราควรประเมินมูลค่าเป็นตัวเงินสำหรับ "Control" ต่างๆที่เราต้องการนำมาใช้เช่น มูลค่าของ Firewall หรือ Intrusion Detection ตลอดจนโปรแกรม Anti-virus หรือการจ้างบริษัท System Integrator (SI) มาจัดการติดตั้ง Service Packs หรือ Patches ต่างๆ รวมไปถึงการ "Hardening" ให้กับ NOS ที่เราใช้เป็น Server ไม่ว่าจะเป็น Web Server, Mail Server หรือ Database Server เป็นต้น

ในขั้นตอนนี้เราควรประเมินค่าใช้จ่ายหรือ Cost of Control ที่เราจะต้องจ่ายออกไปในการติดตั้ง "Control" ต่างๆ แต่เราจะไม่ตัดสินใจว่าจะใช้ "Control" ตัวใดในขั้นนี้ เราควรที่จะจัดเป็นลักษณะ "Brainstorm" คือช่วยกันคิดในหลายๆแง่มุมถึงประโยชน์ที่ได้รับจากการติดตั้ง "Control" ทั้งทางด้านเทคนิค และด้านการบริหารจัดการ เป็นที่ทราบกันดีว่าไม่สามารถลดความเสี่ยงของระบบให้เป็นศูนย์ได้ เพราะอย่างไรก็ยังคงต้องมีความเสี่ยงเหลืออยู่หลังจากที่เราติดตั้ง "Control" ต่างๆ ไปแล้ว ซึ่งทางเทคนิคเราเรียกว่า "Residual Risk" นั่นคือความเสี่ยงที่เรายอมรับได้นั่นเอง

6.5.1.4 ขั้นตอน "Analysis, Decision and Documentation" หมายถึงการวิเคราะห์ข้อมูลจากขั้นตอนที่หนึ่งถึงสามเพื่อนำมาตัดสินในในการเลือกใช้ Control ให้เหมาะสมกับมูลค่าของทรัพย์สิน (Asset) ที่เรามีความจำเป็นต้องป้องกัน หลักการก็คือ เราต้องไม่ให้ค่าใช้จ่ายในการติดตั้ง "Control" นั้นมากกว่ามูลค่าของทรัพย์สินที่เราต้องการป้องกัน การคิดค่าใช้จ่ายในการติดตั้ง "Control" เช่นการติดตั้ง Firewall หรือ IDS นั้น เราจะคิดเฉพาะมูลค่าของ Hardware, Software และค่าติดตั้งไม่ได้ เพราะยังมีต้นทุนแฝงที่เรายังมองไม่เห็นอีกหลายๆอย่าง เช่น ค่าใช้จ่ายด้านการบริหารจัดการ ค่าบำรุงรักษา (Maintenance) หรือต้นทุนที่เกิดขึ้นหลังจากที่ติดตั้งไปแล้วเกิดปัญหาขึ้นกับระบบเดิมโดยรวมทำให้พนักงานทำงานไม่ได้ หรือการทำงานช้าลงเพราะมีปัญหาด้านประสิทธิภาพในการทำงานของระบบใหม่ที่เราเพิ่งติดตั้ง "Control" เข้าไป ดังนั้น เราควรคิดให้รอบคอบเสียก่อน ที่จะดำเนินการติดตั้ง "Control" ต่างๆ ดังที่กล่าวมาแล้ว เราควรใช้ข้อมูลจากขั้นตอนที่หนึ่ง และขั้นตอนที่สอง มาประกอบการตัดสินใจว่าจะเลือกติดตั้ง "Control" ตัวใดให้เหมาะสม โดยเลือกจากรายการที่เราได้ประเมินค่าใช้จ่ายได้แล้ว ในขั้นตอนที่สามนั่นเสังเกตได้ว่า เราไม่จำเป็นจะต้องติดตั้ง "Control" ให้กับ "Threat" ทุกอย่างที่เราตรวจพบจากขั้นตอนการทำ "Vulnerability Assessment" การที่เราทำ "Risk Analysis" จะช่วยให้เราตัดสินใจได้ดียิ่งขึ้น และมีความชัดเจนในการเลือก "Control" ที่คุ้มค่ากับระบบโดยรวม หากเราไม่ทำ "Risk Analysis" เราก็อาจจะติดตั้ง "Control" ให้กับ "Threat" บางอย่างที่ไม่จำเป็นก็ได้ การตัดสินใจควรจะมาจากบุคคลหลายๆคนที่มีความเกี่ยวข้อง ตั้งแต่ผู้บริหารจนถึงผู้ที่ทำงานอยู่กับระบบเป็นประจำ การที่ทุกคนมาร่วมกันคิด จะทำให้การตัดสินใจนั้นมีความใกล้เคียงกับความเป็นจริงขององค์กรมากขึ้น โดยเฉพาะตัวเจ้าของระบบเองย่อมรู้ดีกว่าคนอื่น จากนั้นเราก็ควรจัดทำ

เอกสารเก็บรวบรวมผลจากการทำ "Assessment" และผลสรุปการตัดสินใจเลือกติดตั้ง "Control" ที่เหมาะสมเพื่อนำไปใช้ในขั้นตอนต่อไป

6.5.1.5 ขั้นตอน "Communication" หมายถึง การที่เราจะทำอย่างไรให้บุคคลอื่น หรือแผนกอื่นๆ ในองค์กรมีความเข้าใจว่าเรากำลังต้องการที่จะลดความเสี่ยงให้กับระบบขององค์กร ซึ่งแน่นอน ย่อมมีผลกระทบไม่มากก็น้อยต่อผู้ใช้งานระบบอยู่เป็นประจำ เราควรจะแสดงให้เห็นถึงผลจากการที่เราลองเจาะระบบในขั้นตอนที่สอง และชี้ให้เห็นถึงช่องโหว่ที่เราตรวจพบ ตลอดจนผลที่ได้รับในทางลบหากไม่มีการติดตั้ง "Control" ต่างๆ ให้เหมาะสม ขั้นตอนนี้คล้ายๆ กับการประชาสัมพันธ์ให้ทุกคนตั้งแต่ผู้บริหารระดับสูงจนถึงผู้ใช้ทั่วไป หากผู้บริหาร และผู้ใช้ระบบมีความเห็นตรงกับเราก็เท่ากับว่าเราประสบความสำเร็จในการติดตั้ง "Control" หรือ "Security Infrastructure" ให้กับระบบในระดับหนึ่งเลยที่เดียว

6.5.1.6 ขั้นตอน "Monitoring" ขั้นตอนนี้ถือเป็นขั้นตอนสุดท้ายกล่าวคือต้องมีการดูแลอยู่ตลอดหลังจากการที่เราได้ติดตั้ง "Control" ต่างๆไปแล้ว เพราะเมื่อองค์กรมีการเปลี่ยนแปลงการบริหารความเสี่ยง (Risk Management) ก็ต้องมีการปรับให้เข้ากับสถานการณ์ใหม่ๆที่เกิดขึ้น บางครั้งบางระบบถึงขนาดต้องทำใหม่ทั้งหมดจากขั้นตอนที่หนึ่งเลยก็มี เราควรปรับแต่งขั้นตอนในการบริหารความเสี่ยงให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไปของระบบด้วย

6.5.2 กำหนดประเภทรายการทรัพย์สิน ทรัพย์สินต่างๆ ในระบบสารสนเทศของ สามารถจำแนกออกเป็นประเภทหลักๆ ได้ 4 ประเภท คือ ทรัพย์สินประเภทข้อมูล (Information Assets) ทรัพย์สินประเภทซอฟต์แวร์ (Software Assets) ทรัพย์สินประเภทกายภาพ (Hardware Assets) บริการ (Facility) และทรัพยากรบุคคล โดยใช้โปรแกรม Asset Classification ในการแยกรายละเอียดรายการทรัพย์สินแต่ละประเภทมีดังนี้

6.5.3 คุณสมบัติของโปรแกรม Asset Classification

6.5.3.1 สามารถแยกรายละเอียดรายการทรัพย์สิน

6.5.3.2 สามารเพิ่ม/ลดรายการทรัพย์สินได้ตามความเหมาะสมของแต่ละองค์กร และแสดงรายงานรายละเอียดรายการทรัพย์สิน

6.5.3.3 สามารถระบุประเภทการบริการความปลอดภัย(Security Service)

-ความลับ (Confidential)

-ความถูกต้อง (Integrity)

-ความพร้อมใช้งาน(Availability)

-ความน่าเชื่อถือ (Reliability)

-ความรับผิดชอบ (Accountability)

-การพิสูจน์ตัวตน(Authenticity)

6.5.3.4 สามารถระบุ Risk Factor ที่จะนำไปคำนวณหาค่าความเสี่ยงของทรัพย์สิน

-ภัยคุกคาม (Threat)

-ความบกพร่อง(Vulnerability)

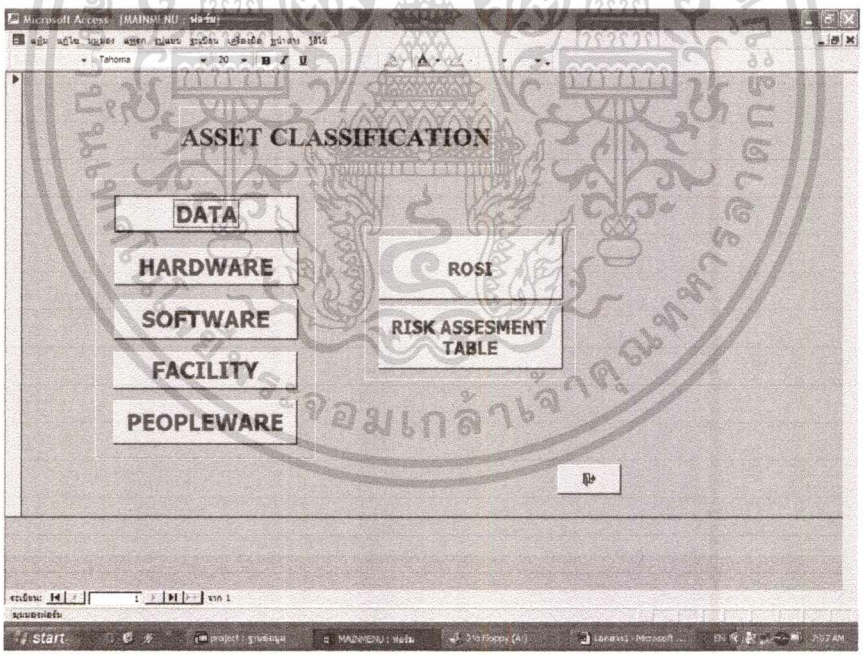
- โอกาสที่จะเกิดภัยคุกคาม (Probability)

-ผลกระทบ (Impact)

-มูลค่าทรัพย์สิน(Asset Value)

6.5.3.5 สามารถคำนวณ และแสดงผลตารางประเมินความเสี่ยง

6.5.4 วิธีการใช้โปรแกรม Asset Classification



ภาพที่ 6.3 หน้าจอแสดงเมนูหลักของโปรแกรม Asset Classification

6.5.4.1 เมนู DATA : เลือก/เพิ่ม/ลด DATA : เลือก/เพิ่ม/ลด ทรัพย์สินประเภทข้อมูล (Information Assets)

6.5.4.2 เมนู HARDWARE : เลือก/เพิ่ม/ลด ทรัพย์สินประเภทอุปกรณ์ฮาร์ดแวร์ (Hardware Assets)

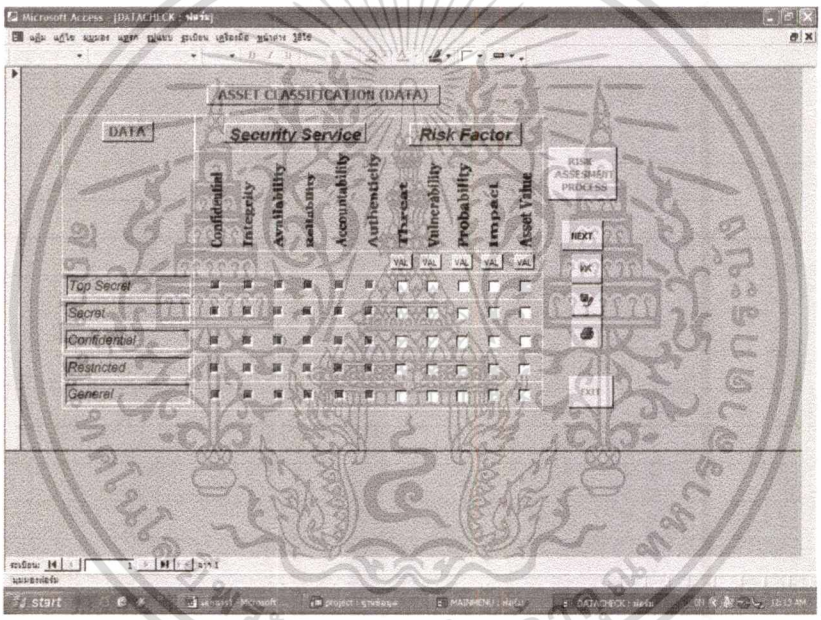
6.5.4.3 เมนู SOFTWARE : เลือก/เพิ่ม/ลด ทรัพย์สินประเภทซอฟต์แวร์ (Software Assets)

6.5.4.4 เมนูFACILITY : เลือก/เพิ่ม/ลด ทรัพย์สินประเภทสาธารณูปโภค (Facility Assets)

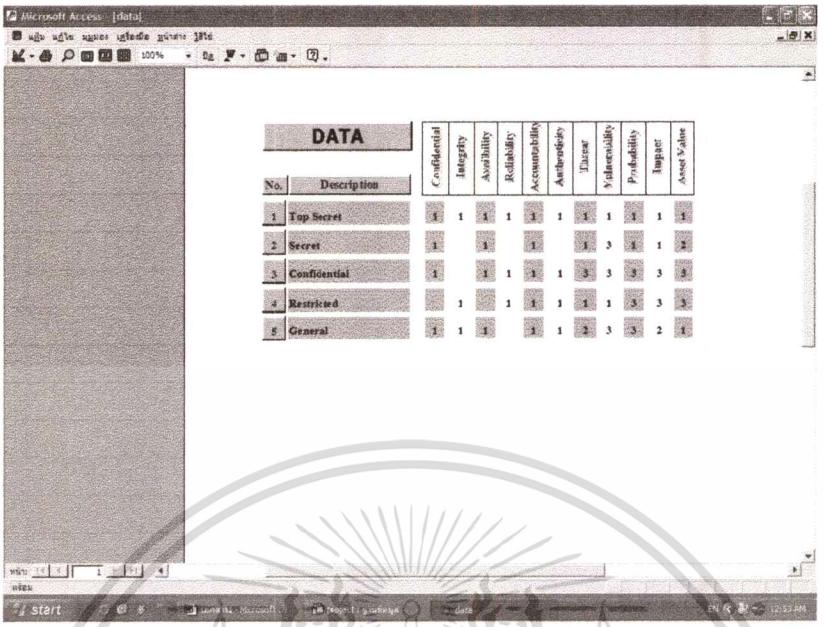
6.5.4.5 เมนู PEOPLEWARE : เลือก/เพิ่ม/ลด ทรัพย์สินประเภททรัพยากรบุคคล(People ware)

6.5.4.6 เมนู ROSI : สูตรการคำนวณ ROSI

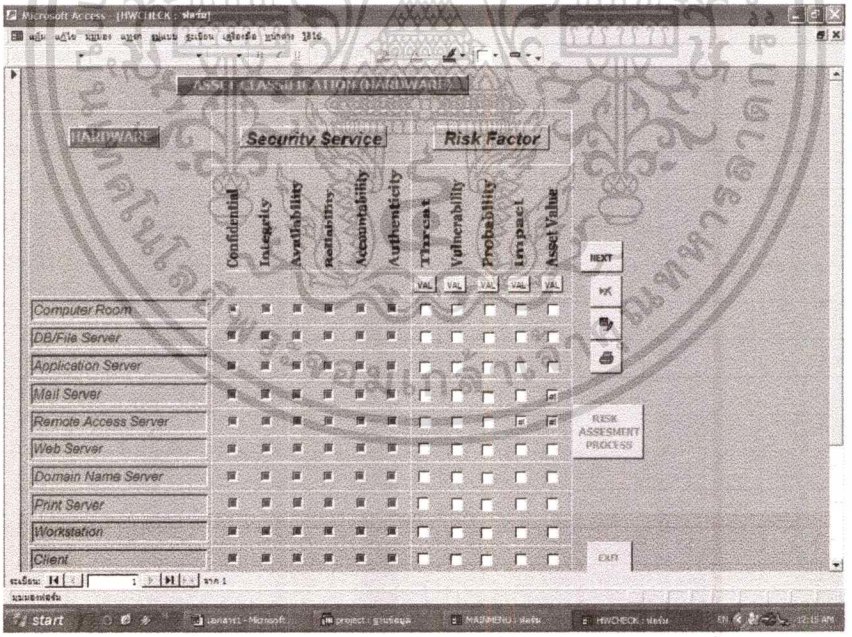
6.5.4.7 เมนู RISK ASSESMENT TABLE : เกณฑ์การประเมินความเสี่ยง



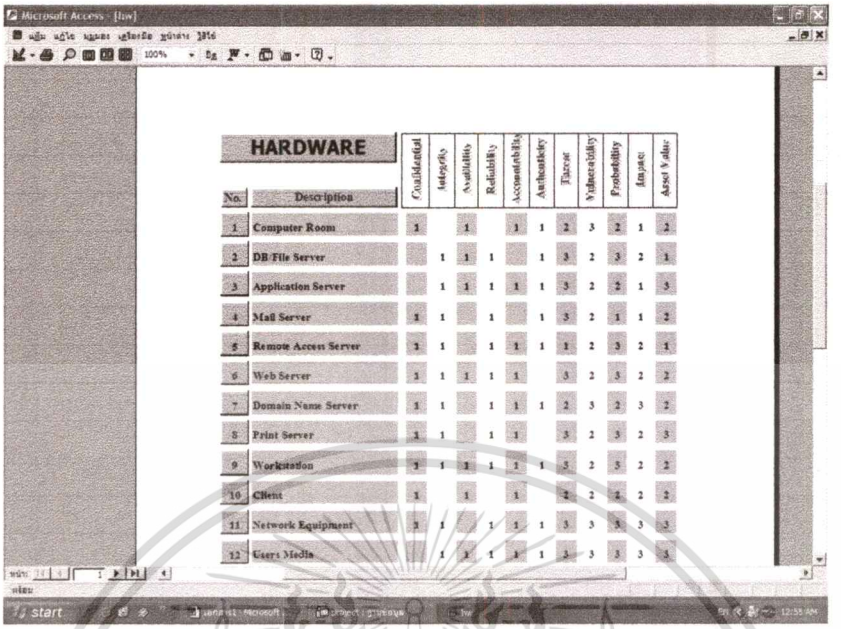
ภาพที่ 6.4 หน้าจอแสดงการจัดสรรทรัพย์สินประเภทข้อมูล (Information Assets)



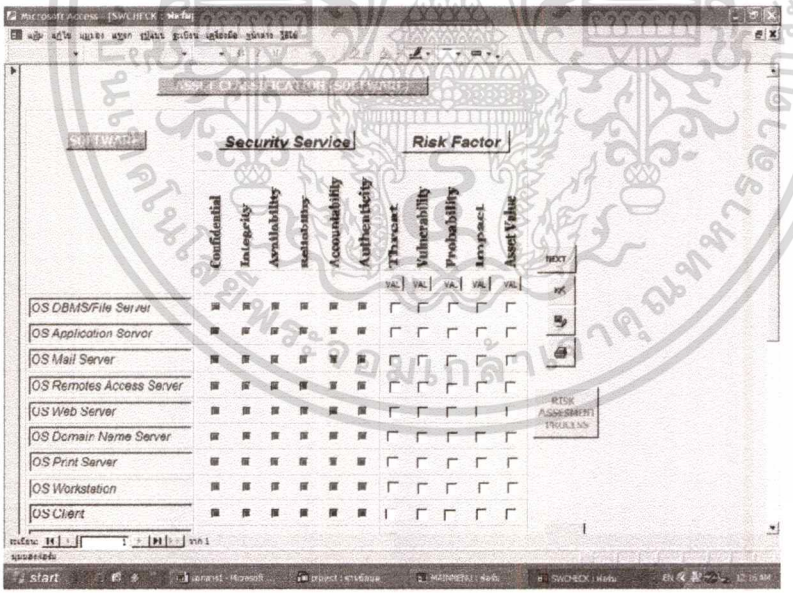
ภาพที่ 6.5 หน้าจอแสดงรายงานรายการทรัพย์สินประเภทข้อมูล (Information Assets)



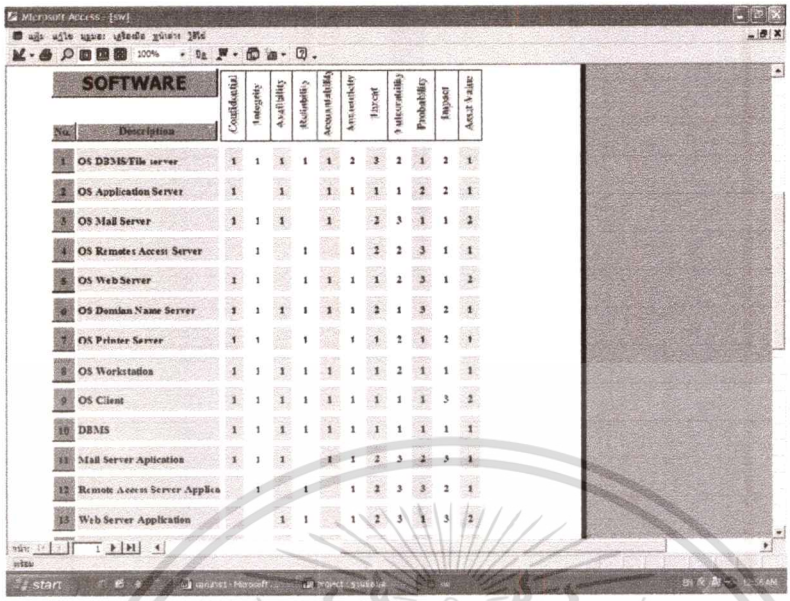
ภาพที่ 6.6 หน้าจอแสดงการจัดสรรทรัพย์สินประเภทซอฟต์แวร์ (Software Assets)



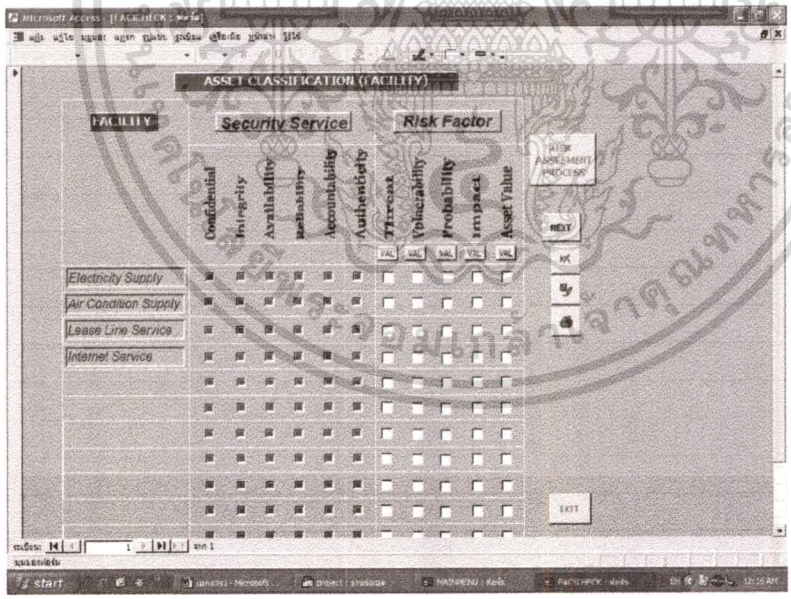
ภาพที่ 6.7 หน้าจอแสดงรายงานรายการทรัพย์สินประเภทซอฟต์แวร์ (Software Assets)



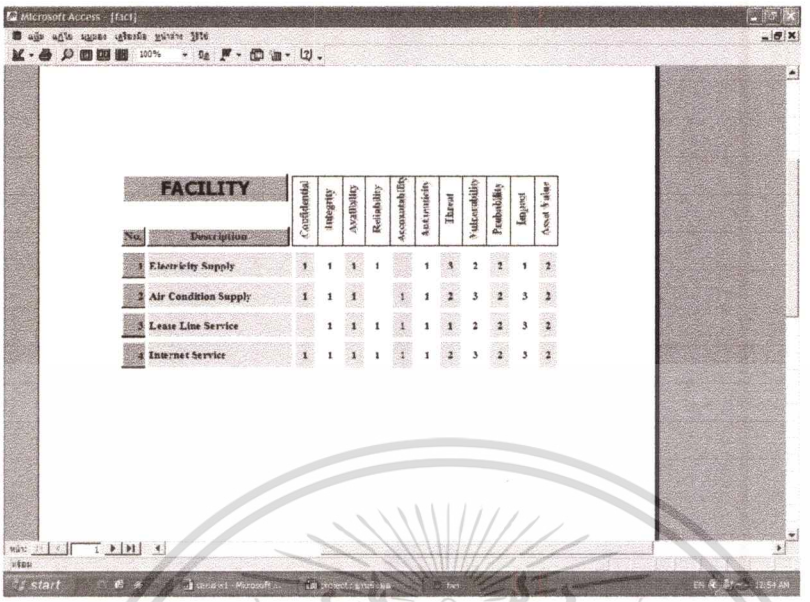
ภาพที่ 6.8 หน้าจอแสดงการจัดสรรทรัพย์สินประเภทอุปกรณ์ฮาร์ดแวร์ (Hardware Assets)



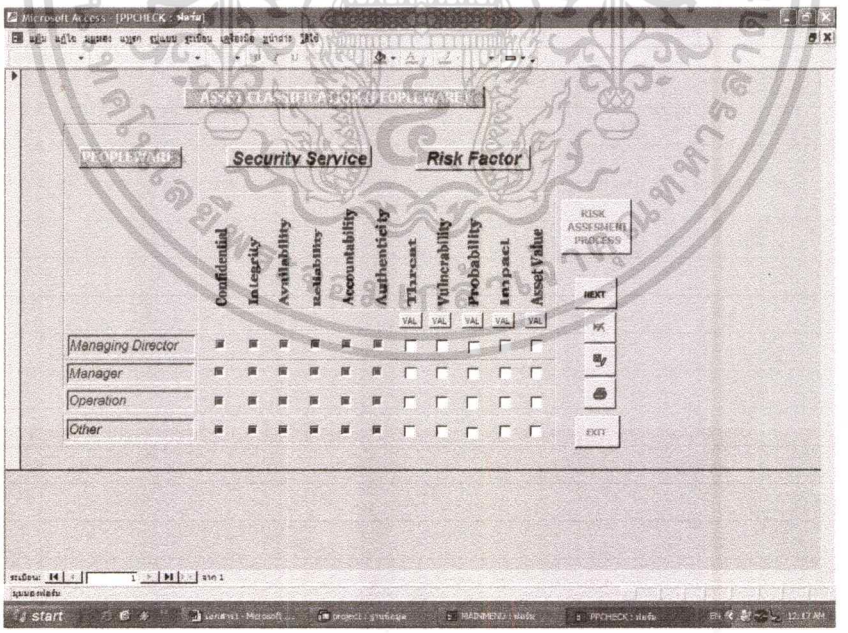
ภาพที่ 6.9 หน้าจอแสดงรายงานรายการทรัพย์สินประเภทอุปกรณ์ฮาร์ดแวร์ (Hardware Assets)



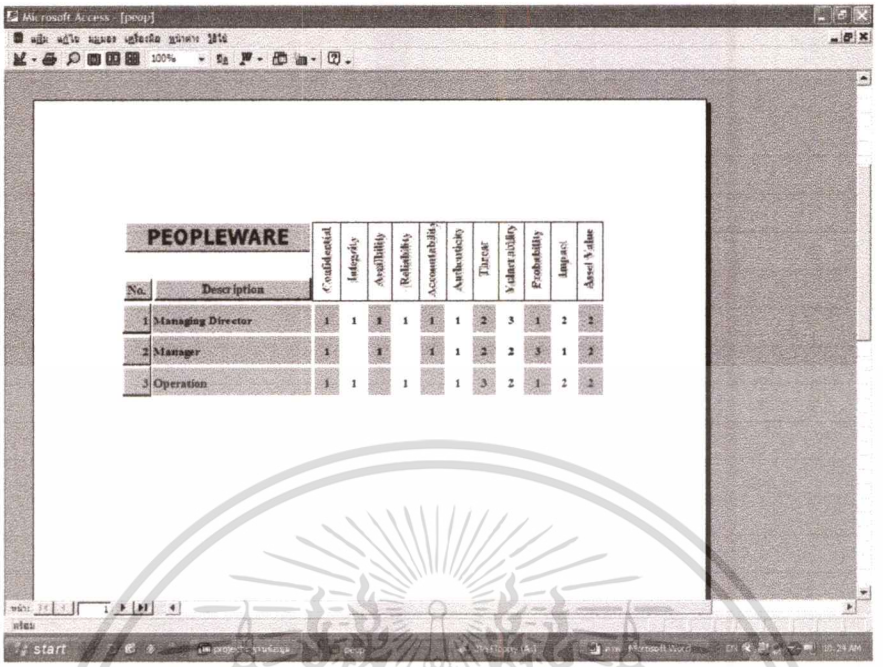
ภาพที่ 6.10 หน้าจอแสดงการจัดสรรทรัพย์สินประเภทสาธารณูปโภค (Facility Assets)



ภาพที่ 6.11 หน้าจอแสดงรายงานรายการทรัพย์สินประเภทสาธารณูปโภค (Facility Assets)



ภาพที่ 6.12 หน้าจอแสดงการจัดสรรทรัพยากรบุคคล(People ware)



PEOPLEWARE

No.	Description	Confidential	Integrity	Availability	Reliability	Accountability	Authenticity	Threat	Vulnerability	Probability	Impact	Asset Value
1	Managing Director	1	1	1	1	1	1	2	3	1	2	2
2	Manager	1		1		1	1	2	2	3	1	2
3	Operation	1	1		1		1	3	2	1	2	2

ภาพที่ 6.13 หน้าจอแสดงรายงานรายการทรัพยากรบุคคล(Peopleware)

6.5.5 การวิเคราะห์ความบกพร่อง (Vulnerabilities) เป็นการวิเคราะห์ถึงจุดอ่อน หรือจุดบกพร่องในระบบสารสนเทศ ที่อาจถูกภัยคุกคามต่างๆ ก่อความเสียหายต่อระบบสารสนเทศ ซึ่งความบกพร่องต่างๆ ในระบบสารสนเทศนั้น ได้แก่ การควบคุมการเข้าถึงที่ไม่ดี (Poor Access Control) การชำรุดทรุดโทรมขาดการซ่อมแซม (Disrepair) การทำงานผิดพลาดของฮาร์ดแวร์ (Miss Process of Hardware) การทำงานผิดพลาดของซอฟต์แวร์ (Miss Process of Software) ความผิดพลาดในการติดต่อสื่อสาร (Miss Process of Communication) และการไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention) ซึ่งสามารถวิเคราะห์ความบกพร่องของทรัพย์สินแต่ละประเภทได้ดังแสดงในตารางที่ 6.1

ตารางที่ 6.1 ตัวอย่างระดับความบกพร่อง (Vulnerabilities)

Vulnerabilities	Degree of Vulnerabilities	Rating
High	Vulnerabilities which allows threat to control/destroy an asset	2
Medium	Vulnerabilities which allows threat to compromise/access an asset	1
Low	Vulnerabilities which provides threat information which could be used to compromise an asset	0

- ความบกพร่องระดับสูง (High) หมายถึง ความบกพร่องที่ยอมให้ภัยคุกคามเข้ามาควบคุมและทำลายทรัพย์สินได้ กำหนดระดับความบกพร่อง เท่ากับ 2
- ความบกพร่องระดับกลาง (Medium) หมายถึง ความบกพร่องที่ยอมให้ภัยคุกคามเข้ามาเป็นอันตรายต่อทรัพย์สิน กำหนดระดับความบกพร่อง เท่ากับ 1
- ความบกพร่องระดับต่ำ (Low) หมายถึง ความบกพร่องที่เปิดช่องให้ข้อมูลภัยคุกคามเข้ามาเป็นอันตรายต่อทรัพย์สิน กำหนดระดับความบกพร่อง เท่ากับ 0

6.5.6 วิเคราะห์ภัยคุกคาม ภายหลังจากที่วิเคราะห์ถึงสภาพบกพร่องในระบบสารสนเทศของทรัพย์สินแต่ละประเภทตามประเภทความบกพร่องแล้วนั้น ก็จะเป็นการวิเคราะห์ถึงภัยคุกคาม (Threat) ต่างๆ ที่อาจเกิดขึ้นจากความบกพร่องที่ได้วิเคราะห์ไว้ข้างต้น พร้อมทั้งกำหนดแนวทางการบริหารความเสี่ยง (Risk Management) เพื่อควบคุมลดหรือบรรเทาความเสี่ยงจากภัยคุกคามต่างๆ ซึ่งสามารถวิเคราะห์ได้ดังแสดงในตารางที่ 6.2

ตารางที่ 6.2 ตัวอย่างระดับภัยคุกคาม (Threat)

Threat of event	Degree of threat	Rating
High	Threat has capability and motivation to destroy/compromise asset function	5
Medium	Threat has capability and motivation to degrade asset function	3
Low	Threat has minimal capability and motivation to effect asset	1

- ภัยคุกคามระดับสูง (High) หมายถึง ภัยคุกคามที่มีความสามารถ และแรงกระตุ้นในการทำลายความพร้อมใช้งานของทรัพย์สิน กำหนดระดับภัยคุกคามเท่ากับ 5

- ภัยคุกคามระดับกลาง (Medium) หมายถึง ภัยคุกคามที่มีความสามารถ และแรงกระตุ้นในการลดทอนความพร้อมใช้งานของทรัพย์สิน กำหนดระดับภัยคุกคามเท่ากับ 3
- ภัยคุกคามระดับต่ำ (Low) หมายถึง ภัยคุกคามที่มีความสามารถ และแรงกระตุ้นซึ่งมีผลกระทบต่ำสุดต่อทรัพย์สิน กำหนดระดับภัยคุกคามเท่ากับ 1

ตารางที่ 6.3 ตัวอย่างระดับของโอกาสที่จะเกิดภัยคุกคาม (Probability)

Probability	Frequency	Rating
Very Low	Unlikely to occur	0
Low	≤ Once per year	1
Medium	≤ Once per 6 months	2
High	≤ Once per months	3
Very High	≤ Once per week	4
Extreme	≤ Once per day	5

- ระดับของโอกาสที่จะเกิดภัยคุกคามต่ำมาก (Very Low) หมายถึง ภัยคุกคามที่ไม่เกิดขึ้นกำหนดระดับของโอกาสที่จะเกิดภัยคุกคาม เท่ากับ 0
- ระดับของโอกาสที่จะเกิดความเสี่ยงต่ำ (Low) หมายถึง ภัยคุกคามที่เกิดขึ้น 1 ครั้ง/ปี กำหนดระดับของโอกาสที่จะเกิดภัยคุกคาม เท่ากับ 1
- ระดับของโอกาสที่จะเกิดความเสี่ยงกลาง (Medium) หมายถึง ภัยคุกคามที่เกิดขึ้น 1 ครั้ง/6 เดือน กำหนดระดับของโอกาสที่จะเกิดภัยคุกคาม เท่ากับ 2
- ระดับของโอกาสที่จะเกิดความเสี่ยงสูง (High) หมายถึง ภัยคุกคามที่เกิดขึ้น 1 ครั้ง/ เดือน กำหนดระดับของโอกาสที่จะเกิดภัยคุกคาม เท่ากับ 3
- ระดับของโอกาสที่จะเกิดภัยคุกคามสูงมาก (Very High) หมายถึง ภัยคุกคามที่เกิดขึ้น 1 ครั้ง/สัปดาห์กำหนดระดับของโอกาสที่จะเกิดภัยคุกคามเท่ากับ 4
- ระดับของโอกาสที่จะเกิดภัยคุกคามสูงยิ่ง (Extreme) หมายถึง ภัยคุกคามที่เกิดขึ้น 1 ครั้ง/วัน กำหนดระดับของโอกาสที่จะเกิดภัยคุกคามเท่ากับ 5

ตารางที่ 6.4 ตัวอย่างระดับความรุนแรงของผลกระทบ (Impact)

Impact	Frequency	Rating
Insignificant	Minimal to no impact	0
Minor	No extra effort required to repair	1
Significant	Tangible impact, extra effort required to repair	2
Damaging	Significant expenditure of resources required /Damage to reputation and confidence	3
Serious	Extended outage and/or loss of connectivity/Compromise of large amount of data or services	4
Grave	Performance shutdown/Complete compromise	5

- ผลกระทบที่ไม่สำคัญ (Insignificant) หมายถึง แทบจะไม่มีผลกระทบเลย กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 0
- ผลกระทบน้อย (Minor) หมายถึง มีผลกระทบน้อย กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 1
- ผลกระทบที่สำคัญ (Significant) หมายถึง ผลกระทบโดยตรง ต้องการการตรวจซ่อมเป็นพิเศษ กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 2
- ผลกระทบที่ทำให้เกิดความเสียหาย (Damaging) หมายถึง การทำให้เสียค่าใช้จ่ายในการจัดหาทรัพย์สินมาทดแทนใหม่ และทำลายชื่อเสียง ความเชื่อมั่น กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 3
- ผลกระทบที่รุนแรง (Serious) หมายถึง ผลกระทบที่ก่อความเสียหายมากขึ้นต่อทรัพย์สิน กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 4
- ผลกระทบที่รุนแรงมาก (Grave) หมายถึง ผลกระทบที่ก่อความเสียหายขั้นที่ทำลายทรัพย์สินจนใช้งานไม่ได้อย่างถาวร กำหนดระดับความรุนแรงของผลกระทบเท่ากับ 5

6.5.7 เกณฑ์การประเมินความเสี่ยง ในการประเมินวิเคราะห์ความเสี่ยงจำเป็นจะต้องมีกำหนดเกณฑ์ในการประเมินวิเคราะห์เพื่อให้ทราบถึงแนวทาง หรือเหตุผลในการวิเคราะห์ ซึ่งความเสี่ยงต่อความปลอดภัยระบบสารสนเทศ คือ โอกาสที่ระบบสารสนเทศอาจจประสบกับภัยคุกคามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ในรูปแบบการทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูล และ การปฏิเสธการให้บริการของระบบ ดังนั้น ความเสี่ยงต่อ

ระบบสารสนเทศ (Risk) จึงเกิดจากผลกระทบ หรือความเสียหายต่อความปลอดภัยของระบบ (Impact) กับโอกาสในการเกิดภัยคุกคาม (Probability) ซึ่งพอจะกำหนดเป็นเกณฑ์การประเมินความเสี่ยงได้ดังนี้ และแสดงผลความเสี่ยงในภาพที่ 6.14

สูตรการคำนวณความเสี่ยง

ความเสี่ยง(Risk) = ผลกระทบ (Impact) X โอกาสในการเกิดภัยคุกคาม (Probability)

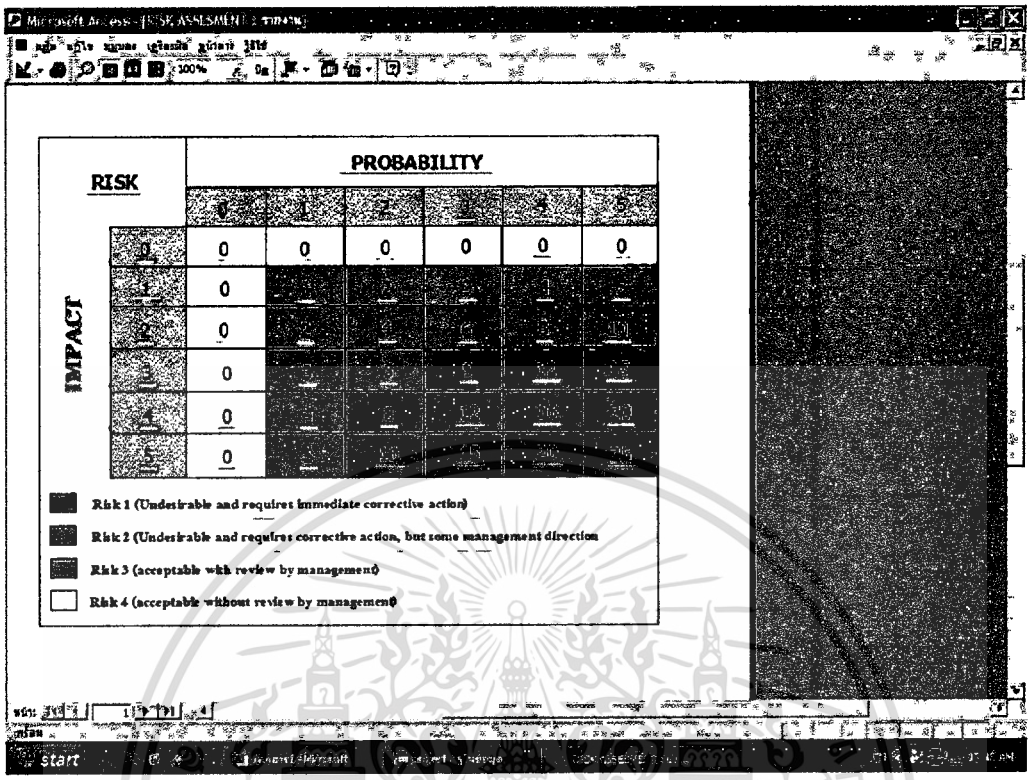
การจัดระดับความเสี่ยง จะพิจารณาจากผลคูณ ของระดับผลกระทบจากภัยคุกคาม(Impact)กับระดับของโอกาสในการเกิดภัยคุกคาม(Probability)

ความเสี่ยงระดับที่ 1 กำหนดระดับความเสี่ยงอยู่ระหว่าง 10 – 25 หมายถึง ความเสี่ยงที่ไม่ต้องการให้เกิดขึ้น และต้องการการแก้ไขความเสี่ยงโดยทันทีทันใด

ความเสี่ยงระดับที่ 2 กำหนดระดับความเสี่ยงอยู่ระหว่าง 4 – 10 หมายถึง ความเสี่ยงที่ไม่ต้องการให้เกิดขึ้น และต้องการการแก้ไขความเสี่ยง

ความเสี่ยงระดับที่ 3 กำหนดระดับความเสี่ยงอยู่ระหว่าง 1 – 3 หมายถึง ความเสี่ยงที่ยอมรับได้แต่ต้องทำการทบทวนการจัดการความเสี่ยง

ความเสี่ยงระดับที่ 4 กำหนดระดับความเสี่ยงเท่ากับ 0 หมายถึง ความเสี่ยงที่ยอมรับได้ โดยไม่ต้องการการทบทวนการจัดการความเสี่ยง



ภาพที่ 6.14 แสดงหน้าจอเกณฑ์การประเมินความเสี่ยง

6.5.8 ตัวอย่างแนวทางประเมินค่าใช้จ่ายในการสร้างระบบรักษาความปลอดภัย (eLeader .2002)

ปัจจุบันเป็นโลกของข้อมูลข่าวสาร มิอาจยอมให้เกิดการสูญเสียขึ้นกับข้อมูลที่สำคัญได้เช่นเดียวกับฝ่ายในโรงงานที่ไม่อาจยอมให้ถูกไฟไหม้ได้เช่นกัน ดังนั้น CIOs(Chief Information Officers) และ CSOs (Chief Security Officers) จึงต้องคำนึงถึงการลงทุนด้านความปลอดภัยของข้อมูล ก่อนที่จะเกิดความเสียหายต่อธุรกิจ แต่ทว่ายังมีปริศนาให้ต้องขบคิดอยู่ว่า เกิดอะไรขึ้นกับ Fire Sprinklers เมื่อ 20 ปีก่อน อะไรที่ทำให้ธุรกิจไม่เติบโตเท่าที่ควร คำตอบคือ CEOs (Chief Executive Officers) และ CFOs (Chief Finance Officers) ต่างต้องการพิสูจน์ที่ชี้ให้เห็นถึงผลตอบแทนการลงทุน แต่ปัญหาอยู่ที่ตัวเลขผลตอบแทนการลงทุนด้านความปลอดภัย (Return On Security Investment : ROSI) เป็นค่าที่ยังไม่สามารถบอกได้ เพราะเหตุการณ์ยังไม่เกิดขึ้นมันเป็นเพียงการป้องกันความเสียหายที่จะเกิดเท่านั้นเพื่อหาค่า ROSI นักวิจัยจำนวนหลายกลุ่มได้ลงมือศึกษาวิจัยเกี่ยวกับเรื่องนี้ แม้ว่างานวิจัยจะประกอบไปด้วยข้อมูลผลการวิจัยต่างๆมากมายแต่ผู้เชี่ยวชาญทั้งหลายต่างเห็นว่ายังคงเป็นเพียงการเริ่มต้นที่จะทำให้ ROSI กำหนดค่าออกมาเป็นตัวเลขได้ แต่ด้านผู้บริหารไอทีทั้งหลายก็ต้องการตัวเลข ROSI นี้เพื่อนำไปแสดงต่อผู้บริหาร เพื่อของบประมาณสำหรับการรักษาความปลอดภัย

Phil Go ซีไอโอที่ออกแบบโครงสร้างระบบความปลอดภัยของบริษัท Barton Malow ในรัฐ Southfield มิชิแกนกล่าวว่า งานวิจัยหลายชิ้นเป็นประโยชน์ต่อการทำงานของเขามาก โดยที่เขาไม่ต้องเสียเวลาคำนวณหาค่าตัวเลขต่างๆให้วุ่นวาย หากผลการวิจัยสามารถพิสูจน์ได้ว่าตัวเลข ROSI นั้น ไม่ได้มาจากการอุปโลกขึ้น และนั่นก็กลายเป็นจุดเริ่มต้นของการเสนอขายระบบความปลอดภัยของเวนเดอร์ ด้วยการแสดงผลตอบแทนการลงทุนด้วย ROSI และเราก็ใช้ค่า ROSI นี้ เสนอระบบความปลอดภัยนี้ต่อนายข้างของเราด้วยเช่นเดียวกัน

ด้าน TOM Oliver ผู้ออกแบบระบบความปลอดภัยให้กับ NASA ใช้เงินจำนวน 400,000 บาท เพื่อสรุปผลการตรวจสอบความปลอดภัยภายในระยะเวลา 7 สัปดาห์ Oliver ได้รับรายงานจากผู้ตรวจสอบซึ่งล้วนกล่าวว่าระบบความปลอดภัยที่ Oliver ได้ออกแบบมีความปลอดภัยสูง เหล่าผู้ตรวจสอบต่างไม่สามารถเข้าถึงข้อมูลสำคัญได้ แต่สิ่งที่ Oliver อยากทราบคือ เขาจะเปรียบเทียบค่าความปลอดภัยของระบบกับหน่วยงานอื่นของรัฐได้อย่างไร และถ้าเขาเพิ่มเงินอีก 20 ล้านให้กับระบบรักษาความปลอดภัย จะทำให้ระบบมีความปลอดภัยเพิ่มขึ้นหรือไม่ ผลการตรวจสอบไม่ได้แสดงให้เห็นถึงผลตอบแทนของการลงทุน Oliver จ่ายเงินจำนวน 4.4 ล้านบาท แต่คำตอบที่เขาได้รับกลับมีเพียง "You're good" ซึ่งเขาไม่ต้องการนั่นแสดงให้เห็นว่า การขายระบบรักษาความปลอดภัยเป็นเรื่องที่มากกว่าความกลัว และความไม่แน่ใจ แต่ต้องแสดงให้เห็นถึงผลตอบแทนที่จะได้รับจากการลงทุนด้วยโดยเฉพาะอย่างยิ่งในช่วงที่เศรษฐกิจซบเซา

การที่เราไม่สามารถแสดง ROSI ออกมาเป็นจำนวนตัวเลขได้ ไม่ได้หมายความว่าไม่มีค่า ROSI อยู่ ตัวเลขเป็นเพียงเครื่องมือที่ใช้ในการขายความปลอดภัยเท่านั้น ตัวอย่างที่เห็นได้ คือ CSI (Computer Security Institute) และ FBI ได้ตรวจสอบการก่ออาชญากรรมทางคอมพิวเตอร์ และแสดงผลการสำรวจความเสียหายที่เกิดขึ้นในช่วงปี 1997 – 2001 มีมูลค่าทั้งสิ้น 40,165,419,800 บาท ซึ่งถ้าเราต้องการคำนวณหาค่า ROSI เราต้องใช้เวลานานมากในการกำหนดค่าต่างๆ ดังนั้น เราจึงไม่สามารถคำนวณค่า ROSI ได้ ทั้งที่จริงๆแล้วมีค่านี้อยู่

ในปี 2000 และ 2001 ทีมจากมหาวิทยาลัย Idaho ได้ใช้กรณีของ George Parmalee เป็นต้นแบบในการศึกษาเพื่อหาค่า ROSI โดยที่ทีมวิจัยได้ติดตั้งระบบการตรวจจับการบุกรุกในเน็ตเวิร์ก (Intrusion detection box) ขึ้นเพื่อคอยตรวจสอบการใช้งานอันน่าสงสัยของยูสเซอร์ ผ่านทางไฟร์วอลล์ จากทราฟฟิกขาเข้าของยูสเซอร์บางคน จะมีการแจ้งเตือนให้ติดตามการใช้งาน จากนั้นทีมวิจัยจึงเริ่มทดสอบแฮกระบบด้วยชื่อรหัส Hummer

detection ให้ผลตอบแทนการลงทุนที่มากกว่าการป้องกันด้วยวิธีอื่นๆ แต่คำถามที่ตามมาก็คือ ค่าใช้จ่ายในการตรวจจับการบุกรุกนี้เป็นเท่าไร ค่าใช้จ่ายรายวันในการรักษาความปลอดภัยเป็นเท่าใด และค่าใช้จ่ายภายหลังการเกิดปัญหาเป็นเท่าใด

Hau Qiang Wei ผู้นำทีมวิจัย Idaho ได้คัดเลือกผลการวิจัยทั้งหมด จากนั้นนำมาเปรียบเทียบกับทฤษฎีที่ได้ศึกษาไว้แล้วกำหนดค่าต่างๆ โดยรวบรวมมูลค่าทรัพย์สินทุกอย่างทั้งที่จับต้องได้ และจับต้องไม่ได้ มูลค่าความเสียหายที่เกิดจากการแฮกแบบต่างๆ ตามที่กำหนดไว้ โดย Department of Defense และค่าประมาณความเสียหายที่จะเกิดขึ้นต่อปี (Annual Loss Expectancy - ALE) ซึ่งมีค่าเท่ากับความเสียหายที่เกิดขึ้น คูณกับจำนวนครั้ง เช่น ความเสียหายมูลค่า 8 ล้านบาท เกิดขึ้นทุกๆ 2 ปี ดังนั้น ALE จะมีค่าเท่ากับ 4 ล้านบาท แล้วทีมวิจัย Idaho จะพยายามโจมตี intrusion detection box เพื่อตรวจสอบว่า มูลค่าความเสียหายที่เกิดขึ้น ตรงตามมูลค่าความเสียหายที่ควรจะเป็นตามทฤษฎีหรือไม่หลังจากนั้นการกำหนดต้นทุน และผลกำไรก็จะกลายเป็นเรื่องง่ายเพียงนำค่าต้นทุนที่ใช้ไปลบกับมูลค่าความเสียหายที่เกิดขึ้นหาก
ผลลัพธ์เป็นบวกแสดงว่าค่า ROSI เป็นบวก

จากการวิจัยของทีม Idaho ในครั้งนี้ได้ผลการวิจัยดังนี้

-มูลค่าของระบบ Intrusion detection (T) = 1,600,000 บาท

-ผลตอบแทนการลงทุนที่คาดว่าจะได้รับเป็นจำนวนเงิน (E) = 1,800,000 บาท

-มูลค่าความเสียหายที่ประมาณการว่าจะเกิดขึ้นภายใน 1 ปี (ALE) = 4,000,000 บาท

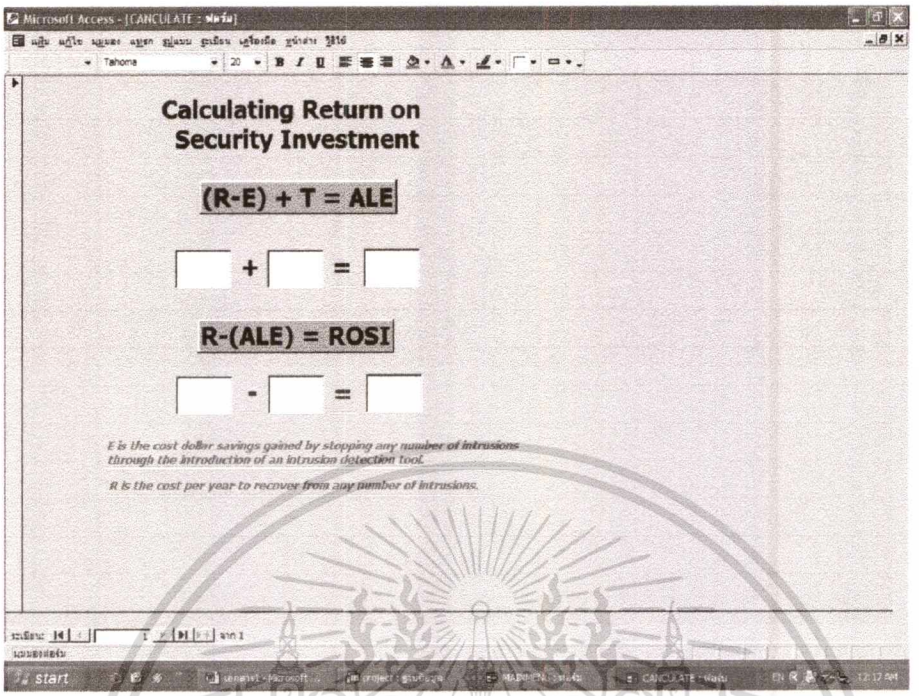
ดังนั้น เมื่อแทนค่าตัวเลขและคำนวณ ROSI ตามสูตรแล้วจะให้ผลดังนี้

$$(R - 1,800,000) + 1,600,000 = 4,000,000$$

$$R = 4,200,000$$

แทนค่า R ในสมการ R – (ALE) = ROSI จะได้

ROSI = 4,200,000 – 4,000,000 = 200,000



ภาพที่ 6.15 แสดงหน้าจอการคำนวณ ROSI

โมเดลของทีมวิจัย Idaho สามารถประมวลผลข้อมูลที่ CIOs ต้องการได้ และไม่เพียงแต่แสดงให้เห็นถึงการลงทุนที่คุ้มค่าเท่านั้น แต่สามารถคำนวณเป็นเงินจำนวนที่ใช้ในการลงทุนออกมาได้ด้วย ขั้นต่อไปทีม Idaho ได้เพิ่ม ROSI เข้ากับ Hummer เพื่อคำนวณมูลค่าจากความเสียหายที่เกิดขึ้นในแต่ละจุด แล้วรายงานผลในกรณีฉุกเฉิน หากค่าใช้จ่ายที่ต้องเสียไปในการกู้ระบบจากความเสียหายที่เกิดขึ้น สูงกว่างบประมาณที่ตั้งไว้ แสดงว่าการลงทุนระบบความปลอดภัย จะให้ผลตอบแทนที่คุ้มค่ากลับคืนมา

6.6 ขั้นตอนการเลือกวิธีการควบคุมความเสี่ยง

การเลือกวิธีการควบคุมความเสี่ยง (Select and Implement Controls) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้นั้นจะต้องมีการพิจารณาถึง cost/benefit justification หรือความคุ้มกับการลงทุน

- ทำการคัดเลือกวิธีการควบคุมโดยคำนึงถึงความกับการลงทุนให้มากที่สุด
- หลีกเลี่ยงการนำวิธีการควบคุมที่ซ้ำซ้อน
- ต้องแน่ใจว่าวิธีการควบคุมที่มีอยู่เดิมทำงานได้อย่างมีประสิทธิภาพ
- นำวิธีการควบคุมมาใช้อย่างเหมาะสม ไม่ว่าจะยกเลิกวิธีการเดิมหรือเพิ่มวิธีการ โดยที่มีค่าใช้จ่ายอย่างสมเหตุผล

วิธีการควบคุมความเสี่ยง

- เพื่อหลีกเลี่ยงหรือป้องกันเหตุการณ์ที่มากระทบ (Deter Control)
- เพื่อปกป้องทรัพย์สินข้อมูลจากเหตุการณ์ที่มากระทบ (Protect Control)
- เพื่อสืบค้นและระบุข้อผิดพลาดหลังจากเกิดเหตุการณ์ขึ้น (Detect Control)
- เพื่อมีปฏิกิริยาตอบโต้หรือเผชิญกับเหตุการณ์ที่เกิดขึ้น (Respond Control)
- เพื่อทำการกู้คืนความถูกต้องสมบูรณ์ ความพร้อมใช้งาน และความลับของข้อมูล (Recover Control)

ประเภทของการควบคุมความเสี่ยง

- การควบคุมทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Controls)
  - จัดการพื้นที่ความปลอดภัยอย่างชัดเจน
  - จัดการความปลอดภัยกับอุปกรณ์ฮาร์ดแวร์
  - มีนโยบายที่ชัดเจน
  - จัดการความปลอดภัยจากผู้ที่ไม่มีสิทธิในการใช้อุปกรณ์ฮาร์ดแวร์
  - กำหนดสิทธิในการเคลื่อนย้ายทรัพย์สิน
- การควบคุมการปฏิบัติงาน (Operational Controls)
  - เอกสารวิธีการปฏิบัติงาน
  - การจัดการระบบเครือข่าย
  - การจัดการการเปลี่ยนแปลงรูปแบบ
  - การจัดการกับเหตุการณ์ต่างๆ
  - การแยกการพัฒนาและการปฏิบัติต่อสิ่งแวดล้อม
  - การวางแผนความสามารถในการปฏิบัติงาน
  - การยอมรับระบบ
  - การป้องกันจากผู้ประสงค์ร้าย
  - การสำรองข้อมูล
  - การบันทึกเหตุการณ์และข้อผิดพลาดต่างๆ
  - การเปลี่ยนแปลงซอฟต์แวร์และข้อมูลต่างๆ
  - ความปลอดภัยระบบการค้าอิเล็กทรอนิกส์
  - ความปลอดภัยระบบจดหมายอิเล็กทรอนิกส์
  - ความปลอดภัยระบบสำนักงานอิเล็กทรอนิกส์
  - ความปลอดภัยสำนักพิมพ์อิเล็กทรอนิกส์

- การปลอดภัยการควบคุมสื่อต่างๆ

- การควบคุมทางเทคนิค (Technical Controls)
  - รหัสผู้ใช้ และการตรวจสอบรูปพรรณลักษณะของผู้ใช้
  - นโยบายการควบคุมการเข้าถึง
  - การจัดการการเข้าถึงของผู้ใช้งาน
  - การทบทวนสิทธิในการเข้าถึง
  - การควบคุมการเข้าถึงระบบเครือข่าย
  - การควบคุมการเข้าถึงระบบปฏิบัติการ
  - การควบคุมการใช้งานโปรแกรมต่างๆ
  - การควบคุมระบบติดตามการเข้าถึงและการใช้งาน

6.7 ขั้นตอนการเขียนข้อกำหนดวิธีการควบคุมความเสี่ยง (Create Statement of Applicability)

ความสำคัญเบื้องต้นที่องค์กรต้องจัดการดำเนินงานก่อนสิ่งอื่นๆ คือการกำหนดนโยบายด้านความปลอดภัยเบื้องต้น องค์กรควรที่จะตัดสินใจว่าใครควรจะเป็นผู้รับผิดชอบในส่วนนี้โดยตรง และจัดการดูแลทางด้านนี้รวมถึงกฎต่างๆ ที่จะต้องกำหนดขึ้นมาด้วยนโยบายที่สำคัญ คือ บุคคลใดสามารถที่จะเข้าถึงข้อมูลได้ในระดับไหน ระดับความสำคัญของยูสเซอร์ ที่จะเข้าไปในฐานข้อมูลหรือเข้ามาแอ็กเซสบนเน็ตเวิร์ก ควรที่จะกำหนดนโยบายเบื้องต้นเหล่านี้ด้วย ส่วนบุคคลที่จะเข้ามาดูแลจัดการทางด้านนี้ควรเป็นบุคคลที่มีความซื่อสัตย์ และสามารถไว้ใจได้เพราะบุคคลคนนี้จะสามารถเข้าไปได้ในทุกส่วนของเน็ตเวิร์กและดูแลระบบงานเน็ตเวร์กทั้งหมด นโยบายในเรื่องของรหัสผ่าน หลักการในการกำหนดรหัสผ่าน คือ ควรที่จะเปลี่ยนรหัสผ่านอยู่เสมอ ไม่ควรที่จะมีความหมายพิเศษ และไม่ควรที่จะบอกรหัสผ่านให้แก่ใครก่อนที่จะลาออกไปจากบริษัท เมื่อนโยบายถูกำหนดขึ้นมาแล้วจะต้องมีการกำหนดวิธีการและกำหนดเทคโนโลยีที่จะนำมาใช้รวมถึงทุกสิ่งทุกอย่างที่เกี่ยวข้องรวมทั้งจะช่วยให้การทำงานทางด้านความปลอดภัยสะดวกและมีประสิทธิภาพมากขึ้น แต่ถ้านโยบายที่ได้กำหนดขึ้นมานี้ไม่ได้ถูกนำไปใช้ก็จะไม่เกิดประโยชน์อะไรแก่องค์กร

6.8 ขั้นตอนการตรวจสอบ

การตรวจสอบ (Audit) เป็นการให้ถูกตรวจสอบการจัดการความปลอดภัยสารสนเทศ จาก 3 ส่วน คือ

- ตรวจสอบภายในองค์กร

- ตรวจสอบโดยลูกค้า
- ตรวจสอบโดยองค์กรอิสระ

ตารางที่ 6.5 สรุปกระบวนการ ISO 17799

	ขั้นตอน	ข้อมูลนำเข้า	กระบวนการ	เอกสารที่ได้
แผน	1	- วัตถุประสงค์ทางธุรกิจ - กระบวนการทางธุรกิจ - ความต้องการการป้องกันระบบสารสนเทศ	- จัดลำดับความสำคัญการรักษาความปลอดภัยของสารสนเทศที่ใช้ในธุรกิจ	- การวิเคราะห์ความเสี่ยงของธุรกิจ - รายการของกระบวนการระบบเทคโนโลยีสารสนเทศเพื่อการวิเคราะห์
	2	- รายการวิเคราะห์ของกระบวนการระบบเทคโนโลยีสารสนเทศ - แบบแผนผังทางตรรกและทางกายภาพ	- แบบแผนผังการจัดการความปลอดภัยสารสนเทศ	- เอกสารการจัดการความปลอดภัยสารสนเทศ
	3	- การวิเคราะห์ความเสี่ยงของธุรกิจ	- กำหนดนโยบายความปลอดภัยสารสนเทศ	- นโยบายความปลอดภัยสารสนเทศ
	4	-นโยบายความปลอดภัยสารสนเทศ	-จัดตั้งองค์กรความปลอดภัยสารสนเทศ	-ผังองค์กรความปลอดภัยสารสนเทศ -บทบาท และความรับผิดชอบระบุในผังองค์กรฯ
	5	- รายการทรัพย์สินระบบสารสนเทศ - การตีค่าทรัพย์สินความเป็นเจ้าของทรัพย์สิน -ความอ่อนไหวต่อสิ่งกระทบ	- แยกแยะและจัดลำดับความสำคัญของทรัพย์สิน	- รายการทรัพย์สินสารสนเทศ - ประเภทของกฎเกณฑ์ต่างๆ - ประเภทของทรัพย์สิน

ตารางที่ 6.5 สรุปกระบวนการ ISO 17799 (ต่อ)

	ขั้นตอน	ข้อมูลนำเข้า	กระบวนการ	เอกสารที่ได้
แผน	6	-การวิเคราะห์ภัยคุกคามและความบกพร่อง	-แยกแยะและประเมินผลความเสี่ยงของทรัพย์สิน	-รายงานผลประเมินความเสี่ยง - กำหนดอัตราของความบกพร่อง - การประเมินค่าความเสี่ยงทรัพย์สิน
	7	- กลยุทธ์การจัดการความเสี่ยง	-วางแผนการจัดการความเสี่ยง	- การจัดการความเสี่ยง -รายละเอียดนโยบายความปลอดภัย - วิธีการ - มาตรฐาน - เทคโนโลยีที่เลือกใช้ - การวิเคราะห์ความคุ้มทุน - รายงานผลการประเมินผล ณ ปัจจุบัน
กระทำตามแผน	8	- รายละเอียดนโยบายความปลอดภัยสารสนเทศ - วิธีการ - ผลิตภัณฑ์ - ส่วนแก้ไขเพิ่มเติม	- กลยุทธ์การบรรเทาความเสี่ยง	- แผนโครงการการบรรเทาความเสี่ยง - การรายงานผลการทดสอบ - การทบทวนการลดทอนความเสี่ยง - รายงานผลการวิเคราะห์ให้ทันเหตุการณ์สมอ

ตารางที่ 6.5 สรุปกระบวนการ ISO 17799 (ต่อ)

	ขั้นตอน	ข้อมูลนำเข้า	กระบวนการ	เอกสารที่ได้
กระทำตามแผน	9	- รายงานสภาวะการวิเคราะห์ความเสี่ยง ณ ปัจจุบัน - นำวิธีการควบคุมมาใช้ให้สอดคล้องกับมาตรฐาน ISO 17799	- เขียนข้อกำหนดหรือนโยบายต่างๆให้สอดคล้องกับมาตรฐาน ISO 17799	- ข้อกำหนด หรือนโยบายที่สอดคล้องกับมาตรฐาน ISO 17799
	10	-นโยบายความปลอดภัยสารสนเทศ และวิธีการปฏิบัติ -วิธีการปฏิบัติที่กำหนดขึ้นมาใหม่	-ฝึกอบรมเจ้าหน้าที่และสร้างความตระหนักเกี่ยวกับความปลอดภัย	-ให้การฝึกอบรมกับผู้บริหารระดับสูง ผู้ใช้งาน และเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ - บันทึกการฝึกอบรม
ตรวจสอบ	11	- รายงานการวิเคราะห์เหตุการณ์ต่างๆ - รายงานข้อบกพร่องของซอฟต์แวร์ - การบันทึกการปฏิบัติงาน - การบันทึกข้อผิดพลาด - รายงานจากผู้ตรวจสอบภายนอก	- ติดตามและทบทวนการจัดการความปลอดภัยสารสนเทศ	-รายงานผลการทบทวนการจัดการความปลอดภัยสารสนเทศ - บันทึกผลการประชุมของคณะกรรมการความปลอดภัย - แผนการปรับปรุงการจัดการความปลอดภัยสารสนเทศ
นำไปปฏิบัติ	12	-รายงานการทบทวนนโยบายความปลอดภัยสารสนเทศ และแผนปฏิบัติงาน	- รักษาระดับและทบทวนการจัดการความปลอดภัยสารสนเทศเพื่อการปรับปรุงอย่างต่อเนื่อง	-ปรับปรุงการจัดการความปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อลดผลกระทบจากเหตุการณ์การคุกคามและความบกพร่องต่างๆ

บทที่ 7
บทสรุป

การสร้างระบบรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศอย่างได้ผลนั้นต้องอาศัยแนวทางหลายอย่างทั้งด้านการบริหาร การจัดการ และเทคนิคที่ผสมผสานระหว่างการใช้ฮาร์ดแวร์ และซอฟต์แวร์ โดยแผนการรักษาความปลอดภัยที่ดีนั้น ต้องประกอบด้วยขบวนการ และขั้นตอนที่พัฒนาจากผู้บริหารที่มีความระมัดระวัง และรู้ตื้นลึกหนาบางขององค์กรตั้งแต่ภายในจนถึงภายนอกระบบเป็นอย่างดีรวมทั้งต้องมีการประเมินประสิทธิภาพของแผนการทำงานแต่ละส่วน โดยพิจารณาจากความเสี่ยง และข้อดีของแต่ละระบบ

จากข้อมูลทั้งหมดที่กล่าวมาแล้ว ทำให้ดูราวกับว่าการรักษาความปลอดภัยของข้อมูลเป็นหน้าที่อันหนักหนาของเหล่าผู้จัดการสารสนเทศขององค์การ เนื่องจากต้องรับผิดชอบในพื้นที่กว้างขวาง และเกี่ยวข้องกับการทำงานในระบบทุกส่วน และทุกขั้นตอนอย่างไม่มีข้อยกเว้น แต่โดยแท้จริงแล้วการรักษาความปลอดภัยข้อมูลที่ได้ผลที่สุดจะเกิดขึ้นได้ต่อเมื่อได้รับความร่วมมือร่วมใจ และต้องถือเป็นหน้าที่ของสมาชิกทุกคนในองค์กรไม่ใช่ของคนใดคนหนึ่งโดยเฉพาะนั่นเอง

7.1 การรักษาความปลอดภัยข้อมูลอย่างเป็นระบบ

ก็คือ การทำ "Information Security Risk Assessment" หมายถึง การวิเคราะห์ความเสี่ยงของระบบนั่นเอง ซึ่งเราต้องตอบคำถามต่างๆดังต่อไปนี้

7.1.1 ระบบของเรามีส่วนไหนบ้างที่มีโอกาสล่มหรือโดน Hacker เข้ามาถล่ม หรือแอบขโมยข้อมูล และภัยที่จะเกิดขึ้นกับระบบของเราจะมาจากทางไหนได้บ้างเช่น ภัยจาก Hacker ทั้งภายใน และภายนอกภัยจากไวรัส ภัยจาก Hardware มีปัญหาเป็นต้น (Threat Events)

7.1.2 ถ้ามีเหตุเกิดขึ้นกับระบบเช่น ระบบล่ม หรือโดน Hacker เข้ามา Hack จะทำความเสียหายในครั้งนั้นมากน้อยเพียงใด (Single Exposure Value)

7.1.3 โอกาสที่จะเกิดเหตุ ความถี่ หรือจำนวนครั้งที่เกิด (Frequency)

7.1.4 เราควรจะทำอย่างไรเพื่อที่จะไม่ให้เกิดปัญหากับระบบ หรือลดความรุนแรงของปัญหาที่เกิดขึ้น หรือ เราอาจจะทำการ "Transfer" ความเสี่ยงไปให้บุคคลที่ 3 (3rd party) (Safeguards and Controls)

7.1.5 ถ้าสรุปได้ว่าต้องมีการติดตั้ง Firewall หรือ IDS ในการป้องกันระบบ ค่าใช้จ่ายทั้งหมดรวมถึงค่า Implement และ Maintenance นั้นเป็นจำนวนเท่าไร่ (Safeguards and Controls Costs)

7.1.6 สุดท้ายต้องคำนวณ Cost/Benefit ระหว่างมูลค่าของความเสียหายที่เกิดขึ้นกับค่าใช้จ่ายที่เราต้องลงทุนในการป้องกันระบบว่าคุ้มกันหรือไม่ ตลอดจนคำนวณค่า ROI (Return On Investment)

จากคำตอบที่ได้จากคำถามต่าง ๆ ทำให้เราพอมองเห็นแล้วว่าเราควรที่จะลงทุนในการป้องกัน Asset ของเราหรือไม่คำว่า "Asset" นั้น หมายถึง "สิ่งที่เรามีความจำเป็นต้องป้องกัน" เช่น ข้อมูล (Information) ฐานข้อมูล (Database) บุคลากร (Personal) Hardware และ Software ตลอดจน Network Infrastructure เป็นต้น

บรรณานุกรม

เจนศักดิ์ ตั้งพันธุ์สุริยะ.2540. **แรกเริ่มเรียนรู้เรื่องรักษาความปลอดภัยให้ระบบคอมพิวเตอร์.** กรุงเทพฯ :ซีเอ็ดยูเคชั่น.

ทศพล กนกนุวัตร์. 2542. **How to Protect from Hackers.** กรุงเทพฯ:ซีเอ็ดยูเคชั่น.

อุษณา ภัทรมนตรี.**การตรวจสอบ และการควบคุมด้านคอมพิวเตอร์.** ศูนย์หนังสือมหาวิทยาลัยเกษตรศาสตร์.

Baker, Richard H. 1995.**Network Security.** Singapore : McGraw – Hill.

Kabay,Michel E..1996. **The NCSA Guide to Enterprise Security.** Pennsylvania : McGraw – Hill Companies.

Bintliff, Russell L. 1994.**Crimeproofing Your Business.** The United State of America : McGraw – Hill.

Pfleeger, Charles P .1997.**Security in Computing.** 2nd ed. The United State of America : Prentice-Hall.

Forcht, Karen Anne.1994.**Computer Security Management.** Danvers, Mass : Boyd & Fraser.

Stallings, William.**Cryptography and Network Security.** 2nd ed. Upper Saddle River : Prentice-Hall.

Barclay Simpson.2003.**ISO IEC 17799.**[Online].Available: http://www.barclaysimpson.com/iso17799.shtml

Carlson T.2001.**Information Security Management:Understanding ISO 17799.** Lucent Technologies Worldwide Services.

ภาคผนวก

ThaiCERT: Thai Computer Emergency Response Team

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ตัวอย่างระเบียบ

ว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย

ด้วย(หน่วยงาน / บริษัท / ห้าง / ร้าน)..... ได้จัดให้มีเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง เห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

"องค์กร" หมายความว่า ชื่อ (หน่วยงาน / บริษัท / ห้าง / ร้าน).....

"เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ขององค์กร.....

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร / บริษัท / ห้าง / ร้าน

"พนักงาน" หมายความว่า พนักงานและลูกจ้างขององค์กร / บริษัท / ห้าง / ร้าน รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ผู้ดูแลเครือข่ายคอมพิวเตอร์" หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ให้มี "คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์" ที่ผู้บังคับบัญชาแต่งตั้งจากพนักงานขององค์กร โดย คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์มีอำนาจหน้าที่ดังต่อไปนี้

- กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้
- ให้คำปรึกษาแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์เกี่ยวกับการปฏิบัติตามระเบียบนี้
- ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม
- ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้
- ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3 ข้อปฏิบัติของพนักงานในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ 1 พนักงานมีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้

การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสมต่อไป

ข้อ 2 พนักงานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ 3 พนักงานพึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย อาทิ เช่น ไม่ใช้การส่ง mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ 4 พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ 5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล พนักงานจะต้อง

- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานครอบครองใช้งานอยู่ ทั้งในระดับ BIOS และระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ 6 พนักงานจะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือขององค์กร หรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น

เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังพนักงานหรือบุคคลอื่น เป็นต้น
- เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของพนักงานอื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ
- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่อยู่เว็บ (web site) ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

ข้อ 7 เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม พนักงานจะต้อง

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน
- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กร ได้
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (server) ที่ต้องใช้งานตลอด 24 ชั่วโมง
- ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กร ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กร จัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด
- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

- ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งองค์กร จัดให้สำหรับใช้ในการ ติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร
- ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการดังกล่าวด้วย
- ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต
- คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นขององค์กร เช่น ข้อมูล และสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่องค์กร รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากองค์กร ภายในกำหนด 7 วันนับแต่วันพ้นสภาพการเป็นพนักงาน

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

ข้อ 1 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของพนักงานเพื่อให้เป็นไปตามระเบียบนี้

หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าพนักงานผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที

ข้อ 2 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อ

พิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ 3 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

ข้อ 4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ 5 เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่องค์กร ในทันทีที่พ้นหน้าที่ และให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ 6 ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กร จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป

ประวัติผู้เขียน

ชื่อ : **เรืออากาศตรีบัณฑิต ทานะมัย**

เกิดเมื่อ : **8 พฤษภาคม 2504**

สถานที่เกิด : **อ. หนองแค จ. สระบุรี**

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนวัดขอนชะโงก จ.สระบุรี

ระดับมัธยมศึกษาตอนต้น โรงเรียนสระบุรีวิทยาคม จ.สระบุรี

ระดับวิชาชีพ โรงเรียนจ่าอากาศ กองทัพอากาศ กรุงเทพฯ รุ่นที่ 20

ระดับมัธยมศึกษาตอนปลาย โรงเรียนธัญบุรี จ.ปทุมธานี

ระดับอุดมศึกษา ปริญญาบัตรศิลปศาสตร์บัณฑิต (รัฐศาสตร์) มหาวิทยาลัยรามคำแหง

ประวัติการทำงาน

กรมสื่อสารทหารอากาศ กองทัพอากาศ พ.ศ.2522 – 2536

บริษัทสามารถคอมเทค จำกัด พ.ศ.2536 – 2543

บริษัทโซโคเมค ยูนิทรีโอ จำกัด พ.ศ.2543- ปัจจุบัน