แผนความปลอดภัยสำหรับระบบสารสนเทศ บริษัท เทเลโฟนไทย จำกัด

Information System Security Plan for Telephonethai Co.,Ltd.

โดย

นายวิฑูรย์ ปึงไพบูลย์

รหัส 44067240

อาจารย์ที่ปรึกษา

ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 2 ปีการศึกษา 2545
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	**แผนความปลอดภัยสำหรับระบบสารสนเทศ บริษัท เทเลโฟนไทย จำกัด**
นักศึกษา	นายวิฑูรย์ ปิงไพบูลย์
อาจารย์ที่ปรึกษา	ดร.จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

ปัจจุบันระบบความปลอดภัยสำหรับระบบสารสนเทศขององค์กรธุรกิจถือว่ามีความสำคัญอย่างยิ่ง แต่ระบบความปลอดภัยที่ดีไม่ได้หมายความว่าจะต้องใช้เทคโนโลยีการเข้ารหัสหรือใช้อุปกรณ์ที่ทันสมัยที่สุด หากแต่ระบบความความปลอดภัยที่ดีและมีประสิทธิภาพนั้น หมายถึงระบบนั้นจะต้องถูกออกแบบและสร้างขึ้นมาอย่างรัดกุมและมีแบบแผน ซึ่งขั้นตอนหนึ่งที่สำคัญในการออกแบบและสร้างระบบความปลอดภัย ก็คือ การจัดทำและกำหนดแผนทางด้านความปลอดภัยให้กับองค์กร

ในโครงการฉบับนี้ได้อธิบายถึงลักษณะของระบบสารสนเทศและระบบความปลอดภัยที่ใช้งานปัจจุบันสำหรับบริษัทเอกชนที่ทำธุรกิจทางด้านโทรคมนาคม ทำการประเมินความเสี่ยงของระบบและจัดทำเป็นแผนความปลอดภัยของระบบสารสนเทศสำหรับบริษัท โดยอ้างอิงจากมาตรฐานสากลในด้านความปลอดภัยของระบบสารสนเทศ ISO17799

Title	Information System Security Plan for Telephonethai Co.,Ltd.
Student	Mr.Withoon Puengphaiboon
Advisor	Dr.Chanboon Sathitwiriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2002

ABSTRACT

At present, security for the organization's information systems are very important. The good security doesn't mean using the up-to-date encryption technology or equipment, but mean that it systematically must be designed and implemented . The Important step is developing the security plan for the organization.

In this project have explained to the As-is information and security systems of the telecommunication company ,assess the risk of information system and set up the security plan for the company by referring to international standard for information security (ISO 17799) .

กิตติกรรมประกาศ

ผู้เขียนขอขอบพระคุณท่านอาจารย์ที่ปรึกษา ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ ที่ได้ให้ความช่วยเหลือ แนะนำและสนับสนุนการจัดทำโครงการศึกษากรณีพิเศษฉบับนี้เป็นอย่างดี ขอบพระคุณ คุณพ่อ คุณแม่ และ คุณนันทนท ดิษยทัศนางกูร ที่ช่วยเหลือและให้กำลังใจผู้เขียนเสมอมา จึงทำให้โครงการศึกษากรณีพิเศษฉบับนี้สำเร็จลุล่วงลงได้ด้วยดี

สารบัญ

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

บทที่ 1

บทนำ

1.1 หลักการและเหตุผลในการศึกษา

ในขณะที่องค์กรธุรกิจปัจจุบันเริ่มสร้างช่องทางใหม่ๆในการทำธุรกิจโดยนำระบบสารสนเทศรวมทั้งอินเตอร์เน็ตเข้ามาใช้เพื่อขับเคลื่อนไปตามกระแสโลกธุรกิจสมัยใหม่ เปิดสู่ตลาดโลก และสร้างระบบการประสานงานระหว่างคู่ค้าหรือลูกค้าได้อย่างประสิทธิภาพ ซึ่งได้ทำให้เกิดการพึ่งพาเครือข่ายอย่างชนิดที่เรียกว่าขาดไม่ได้เลย เพราะเหตุนี้เองจึงทำให้เกิดความคิดในการป้องกันต่อการถูกคุกคามโจมตีระบบความปลอดภัยผ่านทางเครือข่าย ซึ่งปัจจัยสำคัญที่สุดของการแก้ปัญหาเรื่องระบบความปลอดภัยของเครือข่ายควรเริ่มต้นด้วยการทำความเข้าใจและมีการทำงานโดยมีการประสานงานกันระหว่างหน่วยงานต่างๆที่ต้องใช้งานระบบสารสนเทศกับหน่วยงานที่ดูแลระบบสารสนเทศในองค์กร หากปราศจากการป้องกันอย่างเหมาะสมแล้ว ก็อาจจะมีส่วนหนึ่งส่วนใดของเครือข่ายกลายเป็นจุดที่ล่อแหลมต่อการถูกล่วงละเมิดเรื่องความปลอดภัยหรือก่อให้เกิดกิจกรรมที่ไม่ได้รับอนุญาตโดย Cracker คู่แข่งในตลาด หรือแม้กระทั่งพนักงานในองค์กรเอง

ถึงแม้ว่าจะมีความเสี่ยงต่อปัญหาเรื่องความปลอดภัยต่อการใช้งานเครือข่าย แต่อินเตอร์เน็ตก็ยังคงเป็นหนทางที่มีความสำคัญและสะดวก ในการดำเนินงานทางธุรกิจ เนื่องจากมีเทคโนโลยีด้านความปลอดภัยที่พัฒนาขึ้นมาเรื่อยๆเพื่อป้องกันปัญหานี้

ดังนั้นหากองค์กรใดต้องการปรับเปลี่ยนหรือสร้างระบบความปลอดภัยโดยที่ต้องให้แน่ใจว่าเครือข่ายและระบบมีความปลอดภัยจากการถูกจู่โจมเข้ามาสร้างความเสียหาย จึงควรจะหาวิธีลดปัจจัยเสี่ยงให้เหลือน้อยที่สุด ซึ่งก็คือ ควรมีการออกแบบระบบความปลอดภัยโดยที่ต้องมีการประเมินถึงการใช้งานระบบสารสนเทศและระบบความปลอดภัยที่ใช้อยู่ในปัจจุบันและกำหนดได้ว่าตรงไหนมีช่องว่าง แล้วจึงทำงานร่วมกันระหว่างหน่วยงานที่ใช้งานระบบต่างๆกับหน่วยงานที่ดูแลระบบสารสนเทศเพื่อประเมินความต้องการและพัฒนาแผนงานขึ้นมา โดยปัจจัยหลักของเรื่องนี้ที่ต้องทำความเข้าใจก็คือ ผู้ใช้งานระบบเป็นใครบ้างและเขาเหล่านั้นอยู่ไหน และนำข้อมูลที่ได้มาพิจารณาจัดทำแผนความปลอดภัยเพื่อกำหนดแนวทางให้กับผู้ใช้งานในการเข้าถึงระบบสารสนเทศของบริษัท โดยแผนนี้ควรได้รับการสนับสนุนและเห็นชอบจากผู้บริหาร และเนื่องจากความต้องการทางธุรกิจและเทคโนโลยีด้านความปลอดภัยมีการเปลี่ยนแปลงอยู่เสมอ ดังนั้นแผนความ

ปลอดภัยจึงควรจะมีการปรับปรุงแก้ไขให้มีความเหมาะสมและมีความทันสมัยเป็นระยะๆเช่นกัน (ธีรชัย เดชานันทศิลป์. 2545)

1.2 วัตถุประสงค์ในการศึกษา

1. เพื่อใช้เป็นแนวทางในการวิเคราะห์และออกแบบระบบความปลอดภัยที่เหมาะสมกับลักษณะและพฤติกรรมการใช้งานระบบสารสนเทศของบริษัท
2. เพื่อให้ผู้ใช้งานตระหนักถึงความสำคัญของความปลอดภัยของระบบสารสนเทศ
3. เพื่อให้ผู้ใช้งานยึดถือและอ้างอิงเป็นแนวทางปฏิบัติเมื่อมีการใช้งาน
4. เพื่อเป็นการสร้างมาตรฐานในการปฏิบัติงานของบริษัท

1.3 ขอบเขตและแนวทางการศึกษา

1. ขอบเขตที่ศึกษาครอบคลุมเฉพาะระบบคอมพิวเตอร์และเครือข่าย LAN สำหรับสำนักงานของบริษัทในส่วนกลาง
2. ศึกษาทฤษฎีที่เกี่ยวข้องกับกระบวนการสร้างและพัฒนาแผนความปลอดภัยและวิธีการประเมินความเสี่ยงของระบบสารสนเทศ
3. ศึกษาลักษณะการใช้งานระบบสารสนเทศและระบบความปลอดภัยที่ใช้ปัจจุบันของบริษัท
4. ศึกษาถึงมาตรฐานสากลด้านความปลอดภัยของสารสนเทศ ISO 17799
5. ทำการประเมินความเสี่ยงของระบบสารสนเทศโดยใช้ทฤษฎีที่ได้ศึกษา
6. กำหนดแผนความปลอดภัยในด้านต่างๆสำหรับระบบสารสนเทศในบริษัท โดยอ้างอิงจากผลการประเมินความเสี่ยงและมาตรฐานสากลด้านความปลอดภัยของสารสนเทศ ISO 17799

1.4 ผลที่คาดว่าจะได้รับ

1. เพิ่มความปลอดภัยให้กับระบบสารสนเทศของบริษัทผู้ใช้งานตระหนักถึงความสำคัญของความปลอดภัยของระบบสารสนเทศ
2. มีเอกสารที่ใช้ยึดถือและอ้างอิงเป็นแนวทางปฏิบัติเมื่อมีการใช้งาน
3. ทำให้เกิดมาตรฐานในการปฏิบัติงานของบริษัท
4. เพิ่มทักษะในการวิเคราะห์ความเสี่ยงของระบบสารสนเทศและการสร้างแผนความปลอดภัย

บทที่ 2

ทฤษฎีที่เกี่ยวข้อง

2.1 มาตรฐานด้านความปลอดภัยของสารสนเทศ ISO 17799 : แนวปฏิบัติสำหรับการบริหารความปลอดภัยสำหรับสารสนเทศ (ISO/IEC. 2000)

2.1.1 ขอบเขต

มาตรฐานนี้เป็นการให้คำแนะนำสำหรับการบริหารความปลอดภัยของข้อมูลและสารสนเทศสำหรับการจัดทำ การประยุกต์ใช้ และการบำรุงรักษาระบบความปลอดภัยของสารสนเทศในองค์กรและนำไปใช้ให้เกิดประสิทธิผลรวมทั้งทำให้เกิดความมั่นใจระหว่างองค์กร ข้อแนะนำในมาตรฐานนี้ต้องมีการเลือกนำไปใช้ให้สอดคล้องกับกฎหมายและระเบียบต่างๆ

2.1.2 นิยามและความหมาย

1. **ความปลอดภัยของสารสนเทศ (Information Security)** ครอบคลุมถึง
   - Confidentiality คือ การทำให้เกิดความมั่นใจว่าสารสนเทศสามารถเข้าถึงได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น
   - Integrity คือ การป้องกันเพื่อความถูกต้องและความสมบูรณ์ของสารสนเทศและขั้นตอนการประมวลผล
   - Availability คือ การทำให้เกิดความมั่นใจว่าบุคคลที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องได้ตลอดเวลาที่ต้องการ
2. **การประเมินความเสี่ยง (Risk Assessment)** คือ การประเมินภัยคุกคาม ผลกระทบ จุดอ่อนของสารสนเทศและสิ่งอำนวยความสะดวกสำหรับการประมวลผลข้อมูลที่อาจเกิดขึ้นได้
3. **การบริหารความเสี่ยง (Risk Management)** คือ กระบวนการในการแยกแยะ การควบคุม การทำให้เหลือน้อยที่สุดหรือการกำจัดความเสี่ยงที่อาจส่งผลต่อความปลอดภัยของระบบสารสนเทศ โดยที่มีค่าใช้จ่ายที่สามารถยอมรับได้

2.1.3 รายละเอียดของมาตรฐาน ISO 17799

1. **นโยบายความปลอดภัย (Security Policy)** มีวัตถุประสงค์เพื่อจัดหาแนวทางในการบริหารและการสนับสนุนความปลอดภัยของสารสนเทศ โดยที่ฝ่ายบริหารต้องมีนโยบายที่ชัดเจนและมี

การสนับสนุนและมีข้อตกลงเกี่ยวกับความปลอดภัยของสารสนเทศโดยจัดทำเป็นประเด็นและมีการดูแลรักษานโยบายความปลอดภัยของสารสนเทศทั่วทั้งองค์กร

- จัดทำเอกสารนโยบายความปลอดภัย โดยที่นโยบายมีการอนุมัติจากฝ่ายบริหารและมีการตีพิมพ์รวมทั้งแจ้งให้พนักงานทุกคนรับทราบ
- ทำการทบทวนและประเมินผล กล่าวคือ นโยบายต่างๆต้องมีผู้รับผิดชอบในการบำรุงรักษาและมีการทบทวนตามช่วงเวลา

2. นโยบายด้านองค์กร (Organizational Policy)

1) มีโครงสร้างพื้นฐานของความปลอดภัย เพื่อบริหารความปลอดภัยสารสนเทศในองค์กร โดยจัดให้มีการประชุมปรึกษาหารือกับหน่วยงานต่างๆเพื่อกำหนด ประยุกต์ใช้สารสนเทศ การจัดสรรหน้าที่ความรับผิดชอบ การมีที่ปรึกษาด้านความปลอดภัยสารสนเทศ การกำหนดความปลอดภัยแกบริษัทคู่ค้า ผู้รับเหมาและบริษัทที่ปรึกษาต่างๆ

- มีการจัดการประชุมทางด้านการบริหารการจัดการความปลอดภัยข้อมูลโดยทีมงานผู้บริหารมีส่วนร่วมที่กำหนดหาแนวทางและวิสัยทัศน์ด้านความปลอดภัย
- จัดความร่วมมือด้านความปลอดภัยข้อมูลโดยจัดให้มีหน่วยงานต่างๆเข้ามามีส่วนร่วมประชุมหรือกำหนดบทบาทเกี่ยวกับการควบคุมความปลอดภัยของสารสนเทศ
- มีการจัดสรรอำนาจหน้าที่ความรับผิดชอบด้านความปลอดภัยของสารสนเทศ
- มีขั้นตอนในการให้อำนาจเกี่ยวกับอุปกรณ์อำนวยความสะดวกต่างๆด้านสารสนเทศเช่น การนำอุปกรณ์ใหม่ๆ เข้ามาใช้ด้านสารสนเทศต้องได้รับอนุมัติ การอนุญาตจากบุคคลที่รับผิดชอบด้านความปลอดภัย
- มีผู้เชี่ยวชาญด้านความปลอดภัยให้คำแนะนำเกี่ยวกับความปลอดภัยของข้อมูลสารสนเทศ

2) การจัดการความปลอดภัย การเข้าถึงข้อมูลของบุคคลที่สามเพื่อรักษาความปลอดภัยต่อสิ่งอำนวยความสะดวก การประมวลผลข้อมูลรวมทั้งทรัพย์สินข้อมูล ประกอบไปด้วย ขั้นตอนคือ จำแนกแยกแยะความเสี่ยงที่เกิดจากการเข้าถึงของบุคคลที่สาม ได้แก่ การเข้าถึง

- จำแนกแยกแยะความเสี่ยงที่อาจเกิดขึ้นจากการเข้าถึงของบุคคลที่สามที่เกี่ยวข้อง ได้แก่ ชนิดของการเข้าถึงกายภาพและลอจิกคัล เหตุผลและความจำเป็นในการเข้าถึงบริษัทที่เข้ามาให้บริการ พนักงานรักษาความปลอดภัย แม่บ้าน พนักงานทำความสะอาด นักศึกษาฝึกงาน ผู้ให้คำปรึกษา
- กำหนดสัญญาความต้องการด้านความปลอดภัยกับบริษัทร่วมการค้าให้ปฏิบัติตามนโยบายความปลอดภัยต่างๆ ซึ่งสัญญาควรประกอบไปด้วย นโยบายความปลอดภัยข้อมูลทั่วๆ ไป

การค้าครองทรัพย์สินต่างๆ การอธิบายลักษณะของการให้บริการ การคุ้มครองทรัพย์สินทางปัญญา ข้อตกลงในการเข้าถึงข้อมูลหรือสิ่งอำนวยความสะดวกทางการประมวลผล

3) การทำเอ้าท์ซอสซิ่ง (Outsourcing) เพื่อรักษาความปลอดภัยข้อมูลในกรณีที่การประมวลผลข้อมูลอยู่ในความรับผิดชอบ โดยองค์กรใดองค์กรหนึ่งประกอบด้วย

- มีการกำหนดสนธิสัญญาเกี่ยวกับความต้องการด้านความปลอดภัยกับบุคคลภายนอกเช่น สิทธิในการตรวจสอบได้ ระดับการเข้าถึงทางกายภาพที่อนุญาตได้ เป็นต้น

3. การจัดการแยกชนิดของทรัพย์สินและการจัดการควบคุม (Asset classification and control) มีวัตถุประสงค์เพื่อคงไว้ซึ่งการปกป้องคุ้มครองทรัพย์สินขององค์กรอย่างเหมาะสม

1) มีการจัดทำบัญชีทรัพย์สิน เพื่อบำรุงรักษาป้องกันทรัพย์สินขององค์กรอย่างเหมาะสม ทรัพย์สินที่สำคัญต้องมีการจัดทำบัญชีและแต่งตั้งผู้รับผิดชอบ ประกอบด้วย

- จัดทำทรัพย์สินคงคลัง ประกอบไปด้วยทรัพย์สินทางข้อมูล ได้แก่ฐานข้อมูล แฟ้มข้อมูล เอกสาร แผนงานต่อเนื่อง ซอฟท์แวร์ ทรัพย์สินทางกายภาพ

2) จัดทำการแบ่งแยกชนิดของสารสนเทศ มีวัตถุประสงค์เพื่อ ทำให้เกิดความมั่นใจว่าทรัพย์สินข้อมูลได้รับการคุ้มครองในระดับที่เหมาะสม

- มีการจัดทำข้อแนะนำในการแบ่งแยกประเภทและการจัดเก็บ
- มีการจัดทำประทับตราและการส่งมอบจัดเก็บ โดยกำหนดขั้นตอนกระบวนการต่างๆ ประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร การทำลาย

4. มีการจัดการความปลอดภัยของบุคคล (Personnel Security) เพื่อลดความเสี่ยงจากการกระทำผิดพลาดของมนุษย์ การขโมย การฉ้อโกง การใช้งานในทางที่ผิด

1) ความปลอดภัยในงานและทรัพยากร เพื่อลดความเสี่ยงจากการผิดพลาดของมนุษย์ การขโมย การฉ้อโกง โดยกำหนดความปลอดภัยในหน้าที่การงาน มีนโยบายและการตรวจสอบพนักงานทั้งในขั้นตอนการรับสมัครรวมถึงพนักงานลูกจ้างชั่วคราว มีการทำข้อตกลงเกี่ยวกับความลับของข้อมูลกับบุคลากร ในสัญญาจ้างงาน กำหนดความปลอดภัยข้อมูลเป็นเงื่อนไขและนิยามหนึ่งของความรับผิดชอบของพนักงานในการจ้างงาน

2) การฝึกอบรมพนักงาน เพื่อเกิดความมั่นใจว่าพนักงานตระหนักและใส่ใจในภัยคุกคามที่เกิดกับความปลอดภัยข้อมูล รวมทั้งการสร้างความสนับสนุนในนโยบายความปลอดภัยรวมทั้งการใช้งานข้อมมูลได้อย่างถูกต้องเพื่อลดควววามเสี่ยงให้น้อยที่สุด โดยให้การศึกษาและการฝึกอบรมเกี่ยวกับความปลอดภัยของข้อมูลแก่พนักงานทุกระดับในการใช้งานการประมวลผลข้อมูลเช่น ขั้นตอนการล็อกออน การใช้ซอฟท์แวร์

3) มีการจัดการการตอบสนองต่อเหตุสุดวิสัยและการทำงานที่ผิดปกติ (Responding to security incidents and malfunctions) เพื่อลดความเสียหายของข้อมูลจากเหตุสุดวิสัยและการทำงานที่ผิดปกติรวมทั้งเพื่อการตรวจสอบและเรียนรู้จากเหตุสุดวิสัยที่เกิดขึ้น โดยจะต้องประกอบไปด้วย คือมีการรายงานเหตุสุดวิสัยไปยังบุคคลหรือฝ่ายจัดการได้ทราบทันทีทันใด มีการจัดทำรายงานจุดอ่อนของความปลอดภัย มีการจัดทำรายงานการทำงานที่ผิดปกติของซอฟท์แวร์ จัดทำนโยบายจากประสบการณ์ที่ได้รับจากเหตุสุดวิสัย จัดสร้างกฎระเบียบลงโทษพนักงาน

5. การจัดการความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

1) มีการจัดการที่ปลอดภัย (Secure area) เพื่อป้องกันการเข้าถึง การแทรกแซง การทำลายข้อมูลทุกชนิดขององค์กร โดยมีการจัดแยกพื้นที่ให้ชัดเจน มีขั้นตอนคือ

- กำหนดขอบเขตพื้นที่ทางกายภาพขึ้นมาให้ชัดเจน
- กำหนดทางเข้างทางกายภาพที่มีการควบคุมอย่างชัดเจนเพื่อให้บุคคลที่มีสิทธิเท่านั้นที่สามารถเข้าไปยังพื้นที่ได้
- กำหนดพื้นที่ของสำนักงาน ห้องทำงานและห้องอำนวยความสะดวกต่างๆซึ่งต้องมีการ ล็อคอย่างดีเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- มีการจัดการการทำงานในพื้นที่ที่ปลอดภัย โดยมีการจัดการควบคุมทำข้อเสนอแนะสำหรับพนักงานและลูกจ้าง
- มีการจัดการพื้นที่สำหรับการรับส่งพัสดุและพื้นที่ใช้บรรจุพัสดุ ซึ่งถ้าเป็นไปได้จะต้องมีการจัดการแยกจากพื้นที่ที่มีอุปกรณ์ในการประมวลผลข้อมูล มีการตรวจสอบพัสดุอุปกรณ์ก่อนนำไปใช้ มีการจัดทำทะเบียนควบคุม มีประตูกั้นทางภายในและภายนอก

2) มีการจัดการความปลอดภัยของอุปกรณ์ (Equipment Security) เพื่อป้องกันการสูญหาย การทำลายทรัพย์สินและทำให้การดำเนินธุรกิจหยุดชะงัก โดยมีการจัดการประเด็นต่างๆ คือ

- จัดการสถานที่ตั้งของอุปกรณ์และมีการป้องกันให้ปลอดภัย เพื่อหลีกเลี่ยงความเสี่ยงจากการถูกขโมย ไฟไหม้ การระเบิด ควัน น้ำท่วม ฝุ่น แรงสั่นสะเทือน สารเคมี คลื่นแม่เหล็กไฟฟ้า มีการกำหนดนโยบายการรับประทานอาหาร การสูบบุหรี่ในพื้นที่ที่มีอุปกรณ์สำหรับการประมวลผลข้อมูล
- มีการจัดการอุปกรณ์แหล่งจ่ายไฟฟ้าสำรอง (Power Supplies) อุปกรณ์ควรได้รับการป้องกันจากการขาดกระแสไฟฟ้า โดยการจัดหาแหล่งจ่ายไฟสำรองรวมทั้งอุปกรณ์ปั่นไฟสำรอง

- ความปลอดภัยของสายเคเบิ้ล คือสายไฟและสายสัญญาณที่ใช้เชื่อมโยงข้อมูลควรได้รับการป้องกันการจากถูกขัดจังหวะหรือการถูกทำลาย
- การบำรุงรักษาอุปกรณ์ ควรมีการตรวจสอบเป็นประจำเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน
- การจัดการกับอุปกรณ์ส่วนตัวของพนักงาน ควรได้รับการอนุญาตก่อนที่จะนำมาใช้
- การจัดการความปลอดภัยอุปกรณ์ที่ทิ้งทำลายหรือการนำกลับมาใช้ใหม่ เช่น อุปกรณ์สื่อบันทึกข้อมูลต่างต้องมีการทำลายมากกว่าการลบหรือการเขียนทับ

3) การควบคุมทั่วๆไป เพื่อป้องกันการขโมยข้อมูลและอุปกรณ์ต่างๆที่ใช้ในการประมวลผลข้อมูล
- การจัดการโต๊ะทำงานให้สะอาดและมีหน้าจอคอมพิวเตอร์ที่ปลอดภัย
- การเคลื่อนย้ายทรัพย์สิน อุปกรณ์ ข้อมูล ฮาร์ดแวร์ ซอฟท์แวร์ การเคลื่อนย้ายต้องมีการทำบันทึกและได้รับอนุญาตอย่างถูกต้อง

6. การบริหารการสื่อสารและการปฏิบัติการ (Communications and operations management)

1) จัดสรรความรับผิดชอบและมีขั้นตอนการปฏิบัติงาน เพื่อทำให้เกิดความถูกต้องและปลอดภัยต่อการดำเนินการกับอุปกรณ์ประมวลผลข้อมูล
- มีเอกสารขั้นตอนการปฏิบัติงาน ที่มีคำแนะนำในด้านต่างๆ เช่น การจัดเก็บ การดำเนินการเกี่ยวกับข้อมูล
- การเปลี่ยนแปลงขั้นตอนการปฏิบัติงานต้องมีเอกสารควบคุม โดยมีการจัดทำบันทึกแยกแยะสิ่งที่เปลี่ยนแปลง มีการประเมินผลถึงผลผลกระทบจากการเปลี่ยนแปลง มีขั้นตอนการอนุมัติเป็นทางการ กำหนดความรับผิดชอบในกรณีที่มีการยกเลิกหรือล้มเหลวเกิดขึ้น
- มีขั้นตอนปฏิบัติกรณีมีเหตุสุดวิสัยเกิดขึ้น ขั้นตอนการปฏิบัติงานและการจัดการเหตุสุดวิสัยต้องจัดทำขึ้นเพื่อให้เกิดประสิทธิภาพและความรวดเร็วอันอาจเกิดจาก ความล้มเหลวของระบบ การสูญเสียบริการ การปฏิเสธการให้บริการ ผลลัพธ์ที่ผิดพลาดจากข้อมูลที่ไม่สมบูรณ์ มีคู่มือการปฏิบัติสำหรับแผนบรรเทาปัญหา (Contigency Plan) มีการตรวจสอบและหาหลักฐานเพื่อใช้ในการวิเคราะห์ปัญหา มีการปฏิบัติการกู้คืนระบบ
- มีการจัดแยกหน้าที่หรือกิจกรรม ซึ่งเป็นวิธีการในการลดความเสี่ยงในกรณีที่ระบบถูกนำไปใช้ในทางที่ผิด
- จัดการแยกอุปกรณ์ที่ใช้ในการพัฒนาระบบและอุปกรณ์ที่ใช้ปฏิบัติงานจริง โดยมีการกำหนดกฎเกณฑ์อย่างชัดเจนและเป็นลายลักษณ์อักษรในการเคลื่อนย้ายซอฟท์แวร์จากระบบที่พัฒนาไปสู่ระบบปฏิบัติงานจริง

- มีการจัดอุปกรณ์สิ่งอำนวยความสะดวกต่างๆซึ่งการจัดสิ่งอำนวยความสะดวกต่างๆ เช่น การใช้คู่สัญญาจากภายนอกต้องมีการพิจารณาความเสี่ยงและต้องมีการควบคุมกำหนดกฎเกณฑ์ข้อตกลงในสัญญา

2) การวางแผนและการตรวจรับระบบ (System Planning and acceptances)

มีวัตถุประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบให้น้อยลง การวางแผนล่วงหน้าที่ชัดเจนและมีการเตรียมการเป็นสิ่งจำเป็นเพื่อตอบสนองต่อความพร้อมใช้งาน รวมทั้งสามารถมีข้อกำหนดการปฏิบัติงานที่เกี่ยวกับระบบใหม่ มีการจัดทำเป็นเอกสารและมีการทดสอบก่อนที่จะยอมรับและนำมาใช้งานจริง

- ความสามารถในการวางแผน โดยผู้จัดการต้องตรวจสอบความสามารถของระบบและใช้ข้อมูลเพื่อแยกแยะและเพื่อหลีกเลี่ยงปัญหาคอขวดที่อาจเกิดขึ้น
- การตรวจรับระบบ เงื่อนไขการตรวจรับระบบสารสนเทศที่จัดทำใหม่ การอัพเกรด รวมทั้งเวอร์ชันใหม่ ควรจะมีการจัดทำการทดสอบที่เหมาะสมก่อนที่จะเป็นที่ยอมรับ ซึ่งเงื่อนไขการตรวจรับควรประกอบด้วย ประสิทธิภาพและความสามารถ การกู้คืนข้อผิดพลาด มีแผนบรรเทาปัญหา การจัดเตรียมและการทดสอบมีขั้นตอนการปฏิบัติเป็นประจำ มีข้อตกลงเกี่ยวกับความปลอดภัย มีคู่มือการปฏิบัติงานที่มีประสิทธิภาพ มีการจัดการฝึกอบรม มีหลักเกณฑ์การยืนยันการติดตั้งระบบใหม่ที่ไม่ส่งผลกระทบกับระบบเดิม

3) การจัดการป้องกันต่อซอฟท์แวร์ประสงค์ร้าย (Malicious software) เพื่อปกป้องความมีบูรณภาพของซอฟท์แวร์และข้อมูล ซอฟท์แวร์ประสงค์ร้าย ได้แก่ ไวรัสคอมพิวเตอร์ หนอนเครือข่าย ม้าโทรจัน และลอจิกบอมบ์

- มีการจัดการควบคุมเพื่อต่อต้านซอฟท์แวร์ประสงค์ร้าย โดยควรมีคู่มือปฏิบัติงานให้ผู้ใช้งานคอมพิวเตอร์ระมัดระวังต่อซอฟท์แวร์ประสงค์ร้าย การควบคุมต้องมีประเด็นด้านเหล่านี้ คือ มีนโยบายเกี่ยวกับการใช้ซอฟท์แวร์ลิขสิทธิ์และการห้ามใช้ซอฟท์แวร์ที่ไม่ได้รับอนุญาต มีนโยบายเกี่ยวกับการป้องกันความเสี่ยงเกี่ยวกับการได้รับแฟ้มข้อมูลจากเครือข่ายภายนอกหรือจากสื่อต่างๆ มีการติดตั้งและปรับปรุงซอฟท์แวร์ต่อต้านไวรัสให้ทันสมัยอยู่เสมอ มีการตรวจสอบไฟล์ที่แนบมากับเมล์ มีการจัดสรรความรับผิดชอบในการกู้คืน มีการจัดทำสำรองข้อมูลและซอฟท์แวร์ มีขั้นตอนตรวจสอบข้อมูลสารสนเทศเกี่ยวกับซอฟท์แวร์ประสงค์ร้ายและมีการแจ้งเตือน

4) การจัดการลักษณะงานแบบ Housekeeping โดยมีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความมีบูรณภาพและความพร้อมใช้งานของการประมวลผลข้อมูลและบริการติดต่อสื่อสารในเครือข่าย ซึ่งได้แก่ งานที่เกี่ยวกับ

- การทำสำรองข้อมูล (Information back up) การสำรองข้อมูลทางธุรกิจที่สำคัญและการทำสำรองซอฟท์แวร์ควรทำเป็นปกติประจำและมีการเก็บไว้ในสถานที่ที่แยกจากกัน
- การจัดการบันทึกงานปฏิบัติการ (Operation log) พนักงานปฏิบัติการควรเก็บบันทึกกิจกรรมต่างๆที่ประกอบไปด้วย เวลาในการเริ่มสตาร์ทและเสร็จสิ้นของระบบ เหตุขัดข้องและการแก้ไข ผู้รับผิดชอบในการจัดทำบันทึก
- การเก็บรายงานบันทึกเหตุขัดข้อง (Fault logging) เหตุเสียที่เกิดขึ้นควรมีการจัดทำรายงานบันทึกและแก้ไขที่ถูกต้อง โดยมีการตรวจสอบความผิดพลาด รวมทั้งทบทวนเครื่องมือที่ใช้ในการแก้ไขเหตุขัดข้อง

5) การจัดการเครือข่าย (Network management)

โดยมีวัตถุประสงค์เพื่อทำให้เกิดความมั่นใจถึงวิธีการป้องกันข้อมูลในเครือข่ายและการปกป้องโครงสร้างพื้นฐานต่างๆ

- การควบคุมเครือข่าย ผู้จัดการเครือข่ายต้องประยุกต์ใช้เครื่องมือป้องกันข้อมูลในเครือข่าย รวมทั้งป้องกันการเชื่อมต่อจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยมีการจัดความรับผิดชอบและขั้นตอนการจัดการอุปกรณ์ระยะไกล มีการควบคุมเป็นพิเศษกับข้อมูลที่เคลื่อนย้ายในเครือข่ายสาธารณะเพื่อคงไว้ซึ่งความลับ ความมีบูรณภาพของข้อมูล มีการจัดการกิจกรรมและบริการต่างๆทางธุรกิจให้สอดคล้องกับโครงสร้างพื้นฐานของการประมวลผลข้อมูล

6) การจัดการสื่อบันทึกและความปลอดภัยของสื่อบันทึก (Media handling and security)

เพื่อป้องกันทรัพย์สินเสียหายและการชะงักงันทางกิจกรรมของธุรกิจ ต้องมีการควบคุมและป้องกันทางกายภาพและมีขั้นตอนการปฏิบัติงานที่เหมาะสมเพื่อปกป้องสื่อบันทึกคอมพิวเตอร์ได้แก่ เทป ดิสก์ คาสเซ็ท ข้อมูลนำเข้าและนำออก เอกสารระบบ

- การจัดการเกี่ยวกับการเคลื่อนย้ายสื่อบันทึกคอมพิวเตอร์ ควรมีขั้นตอนจากฝ่ายบริหาร เช่น มีการทำลาย มีการอนุญาตเป็นทางการสำหรับการเคลื่อนย้าย มีการจัดเก็บไปไว้ในที่ที่ปลอดภัยและมีสภาพแวดล้อมที่ปลอดภัย
- การกำจัดสื่อบันทึก สื่อบันทึกที่ไม่ต้องการต้องมีการกำจัดอย่างปลอดภัย ควรมีขั้นตอนการปฏิบัติเพื่อลดความเสี่ยง โดยพิจารณาจากประเด็นต่อไปนี้ สื่อบันทึกได้แก่ กระดาษเอกสาร เทปบันทึก กระดาษพิมพ์เขียว กระดาษรายงาน กระดาษผงหมึก เทปแม่เหล็ก แผ่นดิสก์ คาสเซ็ท ออฟติคัลดิสก์ โปรแกรมต่างๆ ข้อมูลทดสอบ เอกสารระบบ เป็นต้น และมีการจัดทำบันทึกเป็นลายลักษณ์อักษร
- จัดทำขั้นตอนในการจัดเก็บข้อมูล เพื่อป้องกันการเปิดเผยข้อมูลและการใช้ในทางที่ผิด ขั้นตอนการปฏิบัติควรแยกสำหรับเอกสารระบบคอมพิวเตอร์ เครือข่าย เมล์ เสียง มัลติมีเดีย

อุปกรณ์ไปรษณีย์ แฟกซ์ ซึ่งมีขั้นตอนปฏิบัติคือ มีการจัดทำและมีสัญลักษณ์สำหรับสื่อบันทึกทุกรายการ จำกัดบุคคลและการอนุญาตการเข้าถึง จัดทำบันทึกรายการสำหรับผู้รับข้อมูล

- การจัดการความปลอดภัยกับเอกสารของระบบ เอกสารของระบบได้แก่ ข้อมูลที่มีความสำคัญ เช่น คำบรรยายการทำงานของ Application ขั้นตอนการทำงาน โครงสร้างข้อมูล ซึ่งต้องมีการจัดเก็บอย่างปลอดภัยและอนุญาตเฉพาะผู้เป็นเจ้าของ Application เมื่อมีการแลกเปลี่ยนในเครือข่ายสาธารณะก็ต้องมีการป้องกันด้วย

7) การแลกเปลี่ยนข้อมูลและซอฟท์แวร์

เพื่อป้องกันการสูญหาย การดัดแปลง การใช้ในทางที่ผิดของข้อมูลซึ่งเกิดจากการแลกเปลี่ยนระหว่างองค์กร

- การทำการค้าร่วมกันต้องมีเอกสารข้อตกลงระหว่างกันในการทำการค้าผ่านอิเล็กทรอนิกส์ รวมทั้งมีรายละเอียดการอนุญาตการเข้าถึงข้อมูล
- มีการทำข้อตกลงว่าด้วยการแลกเปลี่ยนข้อมูลและซอฟท์แวร์ ข้อตกลงอย่างเป็นทางการควรจัดทำขึ้นสำหรับการแลกเปลี่ยนข้อมูลหรือซอฟท์แวร์ระหว่างองค์กร ซึ่งข้อตกลงดังกล่าวจะรวมถึงการจัดส่ง ความรับผิดชอบของผู้ส่ง มีมาตรฐานฉลากติดระหว่างองค์กร ในเรื่องของลิขสิทธิ์และมีการจัดทำการเข้ารหัส
- มีการจัดการความปลอดภัยสำหรับการค้าอิเล็กทรอนิกส์ ซึ่งเกี่ยวข้องกับการใช้ EDI Mail และการประมวลผลข้อมูลผ่านเครือข่ายสาธารณะเช่น อินเตอร์เน็ต ซึ่งการค้าอิเล็กทรอนิกส์มีจุดอ่อนสำหรับการถูกโจมตีในเครือข่าย การควบคุมจะต้องมีการพิสูจน์ตัวตน การอนุญาต สัญญาและข้อผูกมัด รายการราคาข้อมูล ลำดับที่ของการประมวลผลข้อมูล เงื่อนไขการชำระเงิน การจัดส่ง การยืนยันการรับสินค้า
- มีการจัดการความปลอดภัยสำหรับอิเล็กทรอนิกส์เมล์ กล่าวคือ
  - มีการจัดการความเสี่ยง โดยพิจารณาจากประเด็นต่างๆ เช่น ประเด็นจุดอ่อนของการเข้าถึง ประเด็นการดัดแปลงและการปฏิเสธการให้บริการ ประเด็นจุดอ่อนในเรื่องข้อบกพร่อง เช่น สถานที่ผู้รับ ประเด็นของผลกระทบต่อการติดต่อสื่อสารของขั้นตอนทางธุรกิจ ประเด็นด้านกฎหมาย ประเด็นด้านการตีความ ประเด็นด้านการควบคุมผู้ใช้การเข้าถึงจากระยะไกล
  - มีการจัดทำนโยบายอิเล็กทรอนิกส์เมล์ ประกอบไปด้วย การโจมตีเมล์จากไวรัส การคุ้มครองแฟ้มข้อมูลแนบ ข้อแนะนำในกรณีห้ามใช้เมล์ การระบุความรับผิดชอบของลูกจ้างต่อการใช้เมล์ มีการเข้ารหัสข้อความ และการควบคุมด้านการพิสูจน์ตัวตน

- การจัดการความปลอดภัยระบบสำนักงานอิเล็กทรอนิกส์ โดยมีการจัดทำนโยบายและข้อแนะนำสำหรับการลดความเสี่ยงต่อความปลอดภัยของระบบสำนักงานอิเล็กทรอนิกส์ ได้แก่ เอกสาร คอมพิวเตอร์ โมบาย เมล์ เสียง มัลติมีเดีย แฟกซ์และอุปกรณ์สื่อสารอื่นๆ
- ระบบการเผยแพร่ต่อสาธารณะ (Public Available Systems) ความเอาใจใส่ต่อการป้องกันบูรณภาพ ข้อมูลเผยแพร่ตีพิมพ์ในรูปอิเล็กทรอนิกส์ต้องมีการป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตซึ่งอาจนำมาซึ่งความเสื่อมเสียชื่อเสียงต่อสาธารณะขององค์กร เช่น ข้อมูลในเว็บเซิร์ฟเวอร์ที่เข้าถึงได้ทางอินเตอร์เน็ตจะต้องมีข้อมูลที่สอดคล้องกับกฎหมาย กฎเกณฑ์ ข้อบังคับ จะต้องได้รับอนุญาตอย่างเป็นทางการก่อนเผยแพร่สู่สาธารณะ ซอฟท์แวร์ ข้อมูล สารสนเทศอื่นๆ ที่ต้องการความมีบูรณภาพอย่างสูงแต่ถูกนำไปเผยแพร่ในที่สาธารณะจะต้องได้รับการปกป้องโดยกลไกที่เหมาะสม เช่น ลายเซ็นดิจิทัล รวมทั้งข้อมูลแบบสอบถามที่ตอบกลับจะต้องได้รับการคุ้มครองตามกฎหมาย
- การแลกเปลี่ยนข้อมูลสารสนเทศในรูปแบบอื่นๆ ต้องมีขั้นตอนการปฏิบัติงานและเครื่องมือควบคุมต่างๆ ที่จัดทำขึ้นเพื่อป้องกันการแลกเปลี่ยนข้อมูลที่ส่งผ่านด้วยเสียง โทรสาร วีดีโอ รวมทั้งมีการกำหนดนโยบายสำหรับการปฏิบัติงานแก่ผู้ใช้งานซึ่งเกี่ยวข้อง เช่น การเตือนให้พนักงานระมัดระวังในการไม่เปิดเผยข้อมูลวิกฤติ การถูกดักฟัง การแทร็ปสายข้อมูล การส่งถึงผู้รับปลายทางที่ถูกต้อง การเตือนพนักงานไม่ให้เปิดเผยข้อมูลที่เป็นความลับต่อสาธารณะ การใช้โทรสารติดต่อปลายทางที่ถูกต้อง

7. การควบคุมการเข้าถึง (Access Control)

1) การกำหนดความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง โดยมีวัตถุประสงค์เพื่อควบคุมการเข้าถึงข้อมูล

การควบคุมการเข้าถึงข้อมูลและขั้นตอนการทำงานของธุรกิจควรได้รับการควบคุมโดยเป็นไปตามความต้องการทางธุรกิจและความปลอดภัยโดยต้องมีการการกำหนดนโยบายสำหรับการอนุญาตและการเผยแพร่ข้อมูลให้รับรู้

- นโยบายควบคุมการเข้าถึง

การจัดทำนโยบายและความต้องการธุรกิจ คือ ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึงควรกำหนดและจัดทำเป็นเอกสารให้ชัดเจน การควบคุมการเข้าถึงต้องมีกำหนดและสิทธิสำหรับพนักงานหรือกลุ่มพนักงานที่ชัดเจนในนโยบาย โดยที่นโยบายควรเกี่ยวข้องกัน เช่น การกำหนดความต้องการของแต่ละบุคคลสำหรับแอพพลิเคชั่น จัดแยกชนิดของข้อมูลที่เกี่ยวกับแอพพลิเคชั่นทางธุรกิจ ความสอดคล้องระหว่างการควบคุมการเข้าถึงกับชนิดของข้อ

มูลที่จัดแยก ตลอดจนกฎหมายข้อบังคับที่สอดคล้อง เป็นต้น นอกจากนั้นควรมีการจัดทำกฎในการควบคุมโดยมีกฎเกณฑ์ในการบังคับใช้

2) การจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตในระบบสารสนเทศ ขั้นตอนการปฏิบัติที่เป็นทางการต้องจัดทำขึ้นเพื่อจัดสรรสิทธิในการเข้าถึงในระบบสารสนเทศและบริการสารสนเทศ โดยขั้นตอนจะต้องควบคุมตั้งแต่การลงทะเบียนของผู้ใช้ใหม่จนถึงการถอนทะเบียน

- การลงทะเบียนผู้ใช้ (Uer Registration) ต้องมีขั้นตอนปฏิบัติที่เป็นทางการเกี่ยวกับการลงทะเบียนและการถอนทะเบียนเพื่อประกาศการใช้สิทธิของผู้ใช้ต่างๆ เช่น มีการใช้ชื่อผู้ใช้ที่เป็นรหัสประจำตัวเฉพาะ ต้องมีการแบ่งระดับในการเข้าถึง ให้ผู้ใช้มีลายลักษณ์อักษรในการเข้าถึงข้อมูล จัดทำบันทึกและมีการตรวจสอบ
- การจัดการสิทธิส่วนบุคคล โดยต้องมีการควบคุมสำหรับการจัดสรรและการใช้สิทธิส่วนบุคคลในการเขียนทับลงระบบและแอพพลิเคชั่น ฐานข้อมูลสำหรับระบบที่มีผู้ใช้หลายหน่วยงาน
- การจัดการรหัสผ่านผู้ใช้ (User Password Management) ซึ่งมีแนวทางดังนี้
  - ให้พนักงานเก็บรหัสผ่านของตนเองและกลุ่มเป็นความลับโดยมีการระบุไว้ในสัญญาจ้างงาน
  - ให้พนักงานเก็บรหัสผ่านของตนเองเป็นความลับ รหัสผ่านชั่วคราวที่สร้างขึ้นสำหรับผู้ใช้ที่ลืมรหัสผ่านจะต้องบังคับให้เปลี่ยนแปลง
  - รหัสผ่านชั่วคราวที่สร้างให้ผู้ใช้ควรส่งผ่านด้วยวิธีการที่ปลอดภัยไม่ควรอยู่ในรูปข้อมูลกระจ่าง
  - รหัสผ่านไม่ควรเก็บในคอมพิวเตอร์ที่ไม่ได้ถูกป้องกัน ควรใช้เทคโนโลยีในการระบุและพิสูจน์ตัวตน
- มีการตรวจสอบการให้สิทธิผู้ใช้ ควรมีการตรวจสอบเป็นช่วงระยะเวลาทุกๆ 6 เดือนและทุก 3 เดือนสำหรับการขออนุญาตสำหรับสิทธิพิเศษ

3) ความรับผิดชอบผู้ใช้ (User Responsibilities) เพื่อป้องกันการเข้าถึงของผู้ใช้ที่ไม่ได้รับอนุญาต ความร่วมมือของผู้ใช้ที่ได้รับอนุญาตมีความจำเป็นต่อความปลอดภัยที่มีประสิทธิภาพ

- การใช้รหัสผ่าน ต้องมีการเก็บเป็นความลับ หลีกเลี่ยงการใช้กระดาษจดรหัสผ่าน เปลี่ยนรหัสผ่านเมื่อมีสิ่งชี้บอกว่าเกิดความไม่ปลอดภัย เลือกใช้รหัสผ่านที่มีคุณภาพอย่างต่ำ 6 ตัวอักษร จำได้ง่าย บุคคลอื่นเดาไม่ได้ หรือไม่เกี่ยวกับชื่อ เบอร์โทรศัพท์ วันเกิด เป็นต้น และไม่เป็นตัวเลขหรือตัวหนังสือล้วนๆ มีการเปลี่ยนรหัสผ่านเป็นระยะๆ และไม่ใช้รหัสผ่านที่

ใช้มาแล้ว เปลี่ยนรหัสผ่านชั่วคราวเมื่อ Log on ครั้งแรก และไม่ให้มีการแบ่งกันใช้รหัสผ่าน

- การจัดการอุปกรณ์อื่นๆของพนักงานผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ต่างๆต้องได้รับการป้องกัน เช่น เมื่อเสร็จงานให้ปิด Session มีการ Log off และติดกุญแจ เป็นต้น

4) การควบคุมการเข้าถึงเครือข่าย (Network Access Control) มีวัตถุประสงค์เพื่อป้องกันคุ้มครองบริการเครือข่าย คือการเข้าถึงบริการเครือข่ายทั้งจากภายในและภายนอกต้องมีการการควบคุมเพื่อที่ว่าผู้ใช้ ผู้มีสิทธิในเครือข่ายและบริการเครือข่ายจะไม่ทำให้เกิดความไม่ปลอดภัยกับเครือข่าย ทั้งนี้เพื่อก่อให้เกิดสิ่งต่อไปนี้

- มีการติดต่ออย่างเหมาะสมระหว่างเครือข่ายองค์กรและเครือข่ายขององค์กรอื่นๆ หรือเครือข่ายสาธารณะ
- เพื่อกลไกการพิสูจน์ตัวตนที่เหมาะสมสำหรับผู้ใช้และอุปกรณ์
- ควบคุมผู้ใช้ในการเข้าถึงบริการข้อมูล

- นโยบายการใช้บริการเครือข่าย โดยนโยบายจะต้องกล่าวถึงสิ่งต่อไปนี้
  - เครือข่ายและบริการใดที่ให้บริการการเข้าถึง
  - ขั้นตอนการปฏิบัติสำหรับการอนุญาตว่าบุคคลใดที่ได้รับอนุญาตให้เข้าถึงเครือข่ายและบริการเครือข่าย
  - มีการจัดการควบคุมและขั้นตอนในการปกป้องคุ้มครองการเข้าถึงการเชื่อมต่อเครือข่ายและบริการเครือข่าย
- มีการควบคุมเส้นทางการสื่อสารในเครือข่าย คือเส้นทางจากเครื่องผู้ใช้ไปยังเครื่องบริการต้องมีการควบคุม เครือข่ายต้องมีการออกแบบให้มีการแบ่งปันทรัพยากรและมีความยืดหยุ่นเรื่อง Routing มีการควบคุมเพื่อลดความเสี่ยง เพื่อป้องกันผู้ใช้เลือกเส้นทางภายนอกอื่นๆ
- มีการพิสูจน์ตัวตนสำหรับการการเชื่อมต่อภายนอก เช่น การเข้าถึงจากระยะไกลควรมีการเข้ารหัสในการพิสูจน์ตัวตน
- มีการพิสูจน์ตัวตนใน Node ต่างๆ
- มีการควบคุมพอร์ตต่างๆ ที่เข้าถึงจากระยะไกล สำหรับเครื่องคอมพิวเตอร์และระบบโทรคมนาคม
- มีการแบ่งแยกเครือข่ายสำหรับเครือข่ายในองค์กรและเครือข่ายภายนอกที่ใช้ติดต่อกัน
- มีการควบคุมการเชื่อมต่อเครือข่าย มีการกำหนดค่าเกตเวย์ ทราฟฟิก เครื่องเมล์เซิร์ฟเวอร์ การถ่ายโอนข้อมูลให้เป็นทางเดียวหรือสองทาง

- มีการควบคุมเส้นทางเครือข่าย คือมีการกำหนดตรวจสอบต้นทางและปลายทางให้ถูกต้อง
- มีการจัดการความปลอดภัยของบริการเครือข่ายอื่นๆให้มีความปลอดภัย

5) การจัดการควบคุมการเข้าถึงระบบปฏิบัติการ โดยเพื่อป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาต
   - ต้องมีการแยกแยะตัวบุคคลอย่างอัตโนมัติที่เทอร์มินัลโดยมีการพิสูจน์ตัวตนสำหรับการเข้าถึง
   - มีขั้นตอนวิธีการ Log on สู่เทอร์มินัล จำนวนครั้งที่อนุญาต มีข้อความแสดงถึงความสำเร็จหรือล้มเหลว เป็นต้น
   - มีการแยกแยะผู้ใช้และการพิสูจน์ตัวตนคือ ผู้ใช้ทุกคนต้องมีรหัสประจำตัวที่เป็นเลขประจำตัวผู้ใช้
   - มีการจัดการรหัสผ่านที่ป้องกันความปลอดภัย เช่น ผู้ใช้สามารถเปลี่ยนได้ มีทางเลือกสำหรับการเลือกใช้ สามารถบังคับผู้ใช้เปลี่ยนรหัสผ่านได้
   - มีการจัดการเรื่องการใช้โปรแกรมอรรถประโยชน์ที่สามารถทำลายระบบปฏิบัติการได้
   - มีการจัดการระบบเตือนภัยหรือความเสี่ยงให้ผู้ใช้ได้รับรู้อันตรายที่อาจเกิดขึ้น
   - มีการกำหนดช่วงเวลาปิดตัวของระบบเมื่อไม่มีการทำกิจกรรมใดๆ
   - มีความสามารถในการกำหนดเวลาในการเชื่อมต่อได้
6) การจัดการควบคุมการเข้าถึงแอพพลิเคชั่น (Application Access Control) เพื่อป้องกันการเข้าถึงข้อมูลในระบบสารสนเทศโดยไม่ได้รับอนุญาต อุปกรณ์ความปลอดภัยต้องนำมาใช้จำกัดการเข้าถึงระบบแอพพลิเคชั่น การเข้าถึงซอฟท์แวร์และข้อมูลทางดิจิทัลต้องมีการกำหนดสำหรับผู้มีสิทธิใช้งานเท่านั้น
7) การตรวจตราการเข้าถึงและการใช้ระบบ (Monitoring System Access and Use) เพื่อตรวจสอบกิจกรรมที่ไม่ได้รับอนุญาต ระบบควรจะมีการเฝ้าระวังตรวจตราการเข้าถึงและมีการจัดเก็บบันทึกเพื่อเป็นหลักฐานในกรณีเกิดเหตุสุดวิสัย โดยมีการบันทึกเหตุการณ์ มีการตรวจตราการใช้ระบบ มีขั้นตอนการปฏิบัติงานและขอบเขตความเสี่ยงเพื่อตรวจสอบผู้ใช้งาน มีการเข้าจังหวะสัญญาณนาฬิกาเพื่อเป็นหลักฐานในการตรวจตามวันและเวลาที่เกิดเหตุการณ์
8) การจัดการอุปกรณ์โมบายและการทำงานจากระยะไกล (Mobile Computing and Teleworking) เพื่อให้เกิดความมั่นใจในความปลอดภัยของข้อมูลเมื่อใช้อุปกรณ์โมบายและอุปกรณ์ทำงานจากระยะไกล โดยอุปกรณ์โมบายได้แก่ โน้ตบุ๊ค เครื่องปาล์ม แล็ปท็อป และโทรศัพท์มือถือ ต้องมั่นใจว่าข้อมูลทางธุรกิจไม่เสียหาย มีการสำรองข้อมูล การทำงานจากระยะไกลจะต้องมีการใช้

เทคโนโลยีสื่อสารต่างๆ เพื่อให้พนักงานทำงานจากนอกสถานที่ที่เป็นหลักแหล่งภายนอกองค์กรและต้องมีการจัดการป้องกันที่เหมาะสม

2.2 วัฏจักรของกระบวนการสร้างและพัฒนานโยบายทางด้านความปลอดภัย (The Security Policy Development Life Cycle : SPDLC) (ประชา ตระการศิลป์. 2543 : 125-127)

วัฏจักรของกระบวนการสร้างและพัฒนานโยบายทางด้านความปลอดภัยของระบบสารสนเทศสามารถแบ่งออกเป็น 6 ขั้นตอน คือ

2.2.1 การระบุประเด็นความไม่มั่นคงของระบบงาน (Identification of business-related security issues) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) สรุปรายการที่หน่วยงานของเราอาจจะเกิดความสูญเสีย
2) ประเมินมูลค่าความเสียหาย
3) หน่วยงานของเรามีจุดอ่อนตรงไหนบ้างในกระบวนการปฏิบัติการแต่ละกระบวนการ
4) ระดับความสูญเสียที่หน่วยงานของเราสามารถดำเนินการต่อไปได้โดยไม่มีอุปสรรคมากนักอยู่ที่ระดับใด
5) หน่วยงานของเรามีความสามารถในการลงทุนทางด้านระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ได้มากน้อยแค่ไหน

2.2.2 วิเคราะห์ความเสี่ยง ภัยคุกคาม ความอ่อนแอของระบบ (Analyze security risks, threats and vulnerabilities) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) ประเมินมูลค่าทรัพย์สินทางด้านข้อมูลข่าวสารของหน่วยงานเพื่อพิจารณาว่าคุ้มค่าต่อการลงทุนด้านระบบรักษาความปลอดภัยหรือไม่
2) วิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานในปัจจุบันว่ามีรูปแบบอย่างไร
3) ตามประวัติที่ผ่านมา เคยมีบุคคลที่ไม่ได้รับอนุญาตจากภายนอกพยายามเข้ามาในระบบเครือข่ายคอมพิวเตอร์ของเราหรือไม่
4) รวบรวมรายการของทรัพย์สิน การขู่ การคุกคามและความอ่อนแอไม่มั่นคง จุดอ่อนต่างๆในหน่วยงานของเรา
5) พิจารณา วิเคราะห์ความเสี่ยงเหล่านั้น และสร้างกระบวนการป้องกันที่สามารถตรวจสอบได้

2.2.3 การออกแบบสถาปัตยกรรมและกระบวนการของระบบ (Architecture and process design) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) แนวคิดในการออกแบบทางด้านสถาปัตยกรรมที่เกี่ยวข้องกับระบบความปลอดภัยและกระบวนการทำงานของระบบงานต่างๆที่เกี่ยวข้อง
2) การกำหนดให้ใช้เทคโนโลยีที่เหมาะสมกับหน้าที่ที่เกี่ยวข้องของระบบงาน
3) ขั้นตอนต่างๆของกระบวนการปฏิบัติงานจะต้องถูกตรวจสอบติดตามอย่างใกล้ชิดเป็นกระบวนการที่มีประสิทธิภาพสอดคล้องกับสถาปัตยกรรม ระบบการรักษาความปลอดภัยนี้

2.2.4 การประยุกต์ใช้เทคโนโลยีเพื่อความปลอดภัย (Security Technology and process implementation) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) การเลือกใช้อุปกรณ์เทคโนโลยีที่เหมาะสมตามแนวคิดของระบบงานที่ได้ออกแบบไว้
2) ใช้เทคโนโลยีต่างๆเพื่อความปลอดภัยของระบบงาน พร้อมทั้งบุคลากรที่ได้รับการฝึกอบรมขั้นตอนการควบคุม ตรวจสอบ(Manual Control) ที่ดี
3) กระตุ้นให้เกิดความตื่นตัวในเรื่องของระบบรักษาความปลอดภัยของระบบงานเครือข่าย พร้อมการฝึกอบรม
4) บรรจุหลักสูตรเกี่ยวกับระบบรักษาความปลอดภัยของระบบงานคอมพิวเตอร์ให้แก่เจ้าหน้าที่และผู้บริหารงานทุกระดับ

2.2.5 การตรวจสอบผลกระทบของเทคโนโลยีและกระบวนการความปลอดภัย (Audit of impact of security technology and process) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) ตรวจสอบ ทบทวน ผลลัพธ์ ว่าทางด้านนโยบายและทางด้านการใช้เทคโนโลยีนั้นได้บรรลุถึงเป้าหมายที่กำหนดไว้
2) กำหนดระเบียบปฏิบัติขั้นตอนและมาตรฐานในการที่จะบริหารจัดการข้อยกเว้นต่างๆที่อาจจะมี

2.2.6 การประเมินประสิทธิผลของสถาปัตยกรรมและกระบวนการปัจจุบัน (Evaluation of effectiveness of current architecture and processes) ซึ่งประกอบด้วยขั้นตอนย่อยๆในการปฏิบัติดังนี้

1) ตรวจสอบผลลัพธ์ในระบบรักษาความปลอดภัยทั้งในระดับนโยบายและทางด้านการใช้เทคโนโลยีในปัจจุบันว่าประสบความสำเร็จ ตามเป้าหมายที่วางไว้หรือไม่
2) ทบทวน ปรับปรุง เปลี่ยนแปลง พัฒนา ระบบรักษาความปลอดภัยทั้งทางด้านนโยบายและการใช้เทคโนโลยีอย่างต่อเนื่องสม่ำเสมอตามขั้นตอน SPDLC นี้

2.3 การประเมินความเสี่ยงของระบบสารสนเทศ

วิธีการประเมินความเสี่ยงของระบบสารสนเทศในรายงานฉบับนี้โดยส่วนใหญ่จะอ้างอิงตามวิธีการและเนื้อหาในเอกสาร Information Security Risk Assessment ของ United Stated General Accounting Office (GAO) ซึ่งประกอบด้วยส่วนสำคัญๆ ดังนี้

2.3.1 กระบวนการประเมินความเสี่ยง ในการประเมินความเสี่ยงโดยทั่วไปตามวิธีการของ GAOใน มีกระบวนการที่สำคัญๆดังนี้ (GAO. 1999)

1. ชี้ให้เห็นถึงประเภทของภัยคุกคามที่ทำให้เกิดอันตรายต่อระบบและทรัพย์สินที่สำคัญ โดยภัยคุมคามในที่นี้จะรวมไปถึง ผู้บุกรุก อาชญากรรม พนักงานที่ไม่พอใจบริษัท ผู้ก่อการร้าย หรือภัยธรรมชาติ
2. คาดการณ์ถึงภัยคุกคามที่อาจเกิดขึ้นได้จริง โดยการพิจารณาจากข้อมูลในอดีต
3. แยกและจัดลำดับของคุณค่า และความสำคัญของระบบและทรัพย์สินที่อาจได้รับผลกระทบจากภัยคุกคาม
4. ประมาณการถึงความสูญเสีย ความเสียหายที่อาจเกิดขึ้น รวมทั้งค่าใช้จ่ายในการแก้ไขที่เกิดขึ้นกับระบบและทรัพย์สินที่สำคัญที่สุดในกรณีที่ถูกคุกคาม
5. วางแผนการดำเนินการที่ช่วยลดความเสี่ยงซึ่งอาจรวมไปถึงการสร้างนโยบายใหม่ขององค์กรหรือขั้นตอนการทำงานใหม่ทั้งในด้านการควบคุมทางเทคนิคและกายภาพ
6. จัดทำเอกสารเกี่ยวกับผลการประเมินและพัฒนาแผนการดำเนินการเพื่อแก้ไข

2.3.2 การประเมินผลกระทบและจัดลำดับความสำคัญของระบบ (ฟ้าใหม่ สรรค์ใจ.2545 ; GAO. 1999)

จากกระบวนการใน 2.3.1 เราสามารถนำมาประยุกต์ใช้ในการประเมินและวิเคราะห์ผลกระทบระบบสารสนเทศได้ โดยเราจะแบ่งการประเมินเป็น 2 ลักษณะ คือ

1. **การประเมินเพื่อหาค่าผลกระทบโดยรวม** เป็นการพิจารณาผลรวมค่าผลกระทบจากปัจจัยต่างๆที่เราพิจารณาที่มีต่อระบบแต่ละระบบ ยกตัวอย่าง เช่น องค์กรสมมติองค์กรหนึ่งมีระบบสำคัญ 5 ระบบ คือ เว็บไซต์ทั่วไป เมล์เซิร์ฟเวอร์ ระบบบัญชี เครื่องคอมพิวเตอร์พนักงาน ระบบเครือข่ายขององค์กร ที่ผู้ดูแลระบบจะต้องประเมินคุณค่าและความปลอดภัยที่จะให้มีขึ้น โดยการกำหนดตัวเลขสำหรับแต่ละปัจจัยที่นำมาพิจารณา ดังตารางที่ 2.1ให้กับแต่ละระบบตามเงื่อนไข ซึ่งจะทำให้เราสามารถคำนวณค่าผลกระทบของความปลอดภัยที่มีต่อแต่ละระบบได้

ตารางที่ 2.1 การประเมินค่าผลกระทบโดยรวมของระบบ

ระบบที่มีความเสี่ยง	ความสำคัญต่อธุรกิจ	ปัจจัยที่นำมาพิจารณา				ผลกระทบที่มีโดยรวม
		ความสำคัญของระบบ	ความสำคัญที่มีต่อสาธารณะ	ผลกระทบต่อธุรกิจ	ความง่ายที่จะถูกโจมตี	
เว็บไซต์	ไม่สำคัญต่อการดำเนินธุรกิจมากเนื่องจากใช้เพื่อให้ข้อมูล	ปานกลาง(5)	มาก(10)	น้อย(2)	มาก(9)	26
เมล์เซิร์ฟเวอร์	ธุรกิจยังดำเนินไปได้แต่อาจจะลำบากขึ้น	มาก(9)	ปานกลาง(6)	มาก(8)	ปานกลาง(7)	30
ระบบบัญชี	มีความจำเป็นต่อการทำทรานแซกชั่นของธุรกิจ เป็นระบบที่ใช้เก็บข้อมูลทางด้านการเงินขององค์กรทั้งหมด	มาก(10)	มาก(10)	มาก(10)	ปานกลาง(6)	36
เครื่องคอมพิวเตอร์พนักงาน	ความเสียหายที่เกิดขึ้นกับส่วนนี้จะหยุดการทำงานภายในองค์กรทั้งหมด	มาก(10)	ปานกลาง(6)	มาก(10)	มาก(9)	35
ระบบเครือข่าย	เป็นระบบที่มีความสำคัญยิ่งยวดซึ่งใช้เชื่อมต่อระบบภายในองค์กรเข้าด้วยกัน	มาก(10)	ปานกลาง(7)	มาก(10)	มาก(8)	35

อย่างไรก็ดีการวิเคราะห์ผลกระทบนี้ไม่ได้เป็นเพียงการคำนวณตัวเลขดิบของข้อมูลพื้นฐานเพื่อให้ได้เป็นจำนวนเงินที่จะต้องเสียไปถ้าข้อมูลภายในองค์กรไม่สามารถใช้งานหรือถูกขโมยหรือเสียหายไป หากแต่จะต้องมีการพิจารณาตัวเลขตามประเด็นที่ได้แบ่งเป็นเงื่อนไขย่อย 4 เงื่อนไข ซึ่งแต่ละเงื่อนไขจะเป็นปัจจัยที่ต้องคำนึงถึงในการคำนวณหาผลกระทบโดยรวม โดยปัจจัยทั้ง 4 นี้ประกอบด้วย

- ค่าความสำคัญของข้อมูลหรือส่วนประกอบของโครงสร้างภายในองค์กร ตัวอย่างเช่น แผนการผลิตและจำหน่ายของผลิตภัณฑ์ ระบบบัญชี ฐานข้อมูลของลูกค้าและอื่นๆ ข้อมูลหรือส่วน

ประกอบเหล่านี้จะมีค่าความสำคัญที่ค่อนข้างสูง ในขณะที่เบอร์โทรศัพท์อาจจะมีค่าความสำคัญที่ต่ำกว่า ซึ่งก็เป็นไปตามความสำคัญนั่นเอง

- ความเป็นไปได้ที่จะไม่สามารถให้บริการต่อสาธารณะได้(หรือความสำคัญที่มีต่อสาธารณะ) ตัวอย่างเช่น ถ้าเว็บไซต์ขององค์กรล่มอาจจะทำให้ลูกค้าหรือบริษัทคู่ค้าเข้าใช้หรือหาข้อมูลที่ต้องการไม่ได้ ซึ่งอาจจะส่งผลต่อความน่าเชื่อถือในผลิตภัณฑ์และบริการขององค์กรได้
- ผลกระทบที่มีต่อการดำเนินธุรกิจเป็นการพิจารณาว่าการโจมตีต่อข้อมูลหรือส่วนประกอบภายในองค์กรจะส่งผลกับการดำเนินธุรกิจมากน้อยเพียงใด ถ้าผลกระทำทำให้ธุรกิจทำงานได้ไม่สะดวกค่านี้ก็จะน้อย แต่ถ้าทำให้กระบวนการธุรกิจหยุดดำเนินการตัวเลขนี้ก็จะมีค่ามาก
- ความง่ายต่อการโจมตี เป็นตัวเลขที่บ่งบอกว่าข้อมูลหรือส่วนประกอบนั้น มีโอกาสที่จะถูกโจมตีมากน้อยเพียงใด ซึ่งแน่นอนว่าในกรณีนี้ส่วนประกอบที่อยู่ใกล้สาธารณะอย่างอินเตอร์เน็ตก็มีโอกาสที่จะถูกโจมตีง่ายกว่า ส่วนประกอบเหล่านี้นอกจากถูกโจมตีที่ตัวเองแล้วยังอาจจะเป็นการสร้างช่องโหว่ให้ภัยคุกคามลุกลามเข้ามายังส่วนอื่นขององค์กรได้อีกด้วย

ซึ่งจากปัจจัยทั้ง 4 สามารถกำหนดเป็นระดับของผลกระทบในแต่ละปัจจัยโดยแบ่งเป็น 3 ระดับคือ น้อย ปานกลาง และมาก สำหรับแต่ละปัจจัยต้องพิจารณาภายใต้กลไกและข้อมูลระบบรักษาความปลอดภัยขององค์กร และเพื่อให้กระบวนการวิเคราะห์สามารถทำได้ง่ายขึ้น จึงได้กำหนดค่าตัวเลขที่บ่งบอกถึงระดับของปัจจัยต่างๆโดยตัวเลขจะมีค่าระหว่าง 1-10 โดยระดับน้อยจะหมายถึงตัวเลขอยู่ในช่วง 1-3 ระดับปานกลางจะอยู่ในช่วง 4-7 และระดับมากจะอยู่ในช่วง 8-10 ผลรวมของตัวเลขในทุกๆปัจจัย จะอยู่ในคอลัมน์สุดท้ายในตารางที่ 2.1 ตัวเลขในคอลัมน์สุดท้ายจะบ่งบอกถึงค่าผลกระทบของระบบรักษาความปลอดภัย โดยค่าที่มากกว่าจะหมายถึงผลกระทบที่เกิดขึ้นกับองค์กรจะมากกว่า ในขณะที่ตัวเลขน้อยจะบ่งบอกถึงผลกระทบที่น้อยกว่าเช่นกัน สำหรับการวิเคราะห์จริง แต่ละองค์กรสามารถกำหนดตัวเลขและน้ำหนักของตัวคูณในปัจจัยต่างๆขึ้นมาเองได้แล้วแต่ความเหมาะสม

จากตัวอย่างองค์กรสมมติของเราพบว่าถึงแม้ว่าตัวเลขในส่วนของความง่ายในการถูกโจมตีระบบจะต่ำ ซึ่งหมายความว่าการเข้าไปโจมตีระบบบัญชีขององค์กรจะเป็นสิ่งที่ทำได้ยาก แต่เมื่อพิจารณาถึงตัวเลขรวมทุกๆปัจจัยแล้ว จะเห็นว่าระบบบัญชีมีผลกระทบจากการถูกโจมตีมากที่สุด ซึ่งหมายความว่าองค์กรควรให้ความสำคัญในการดูแลป้องกันระบบบัญชีมากที่สุด ทั้งนี้เนื่องจากตัวเลขในพารามิเตอร์ตัวอื่นที่สูงนั่นเอง ไม่ว่าจะเป็นค่าความสำคัญหรือผลกระทบที่มีต่อธุรกิจ

2. **การกำหนดระดับความเสี่ยง** เป็นการกำหนดระดับของความเสี่ยงที่เกิดขึ้นกับระบบต่างๆ โดยการแบ่งระดับของโอกาสที่ภัยคุกคามจะเกิดขึ้นและระดับความรุนแรงหรือผลกระทบที่เกิดขึ้น

ในกรณีที่ระบบไม่สามารถใช้งานได้ และนำมาจัดทำเป็น Risk Assessment Matrix ซึ่งจะได้ค่าระดับความเสี่ยงออกมาสำหรับทุกๆระบบ โดยมีรายละเอียดการจัดทำดังต่อไปนี้

- ขั้นที่ 1 แบ่งระดับความรุนแรงหรือผลกระทบที่เกิดขึ้นเป็นระดับต่างๆ 4 ระดับ คือ

  ระดับที่ 1 : รุนแรงมาก หมายถึง มีความสูญเสียข้อมูลที่สำคัญอย่างยิ่ง ความเสียหายต่อระบบบุคคล หรือสภาพแวดล้อมอย่างรุนแรง

  ระดับที่ 2 : ค่อนข้างรุนแรง หมายถึง มีความสูญเสียข้อมูล ความเสียหายต่องานที่ทำหรือระบบหรือบุคคลหรือสภาพแวดล้อมค่อนข้างมาก

  ระดับที่ 3 : น้อย หมายถึง มีความเสียหายต่องานที่ทำหรือระบบหรือสภาพแวดล้อมเล็กน้อย

  ระดับที่ 4 : น้อยมาก หมายถึง มีความเสียหายต่องานที่ทำหรือระบบหรือสภาพแวดล้อมน้อยมาก

- ขั้นที่ 2 แบ่งระดับของโอกาสที่จะเกิดภัยคุกคามเป็นระดับต่างๆ 5 ระดับ คือ

  ระดับ A : มีโอกาสเกิดขึ้นได้บ่อยและซ้ำๆ

  ระดับ B : มีโอกาสเกิดขึ้นได้

  ระดับ C : มีโอกาสเกิดขึ้นได้เป็นครั้งคราว

  ระดับ D : มีโอกาสเกิดขึ้นได้น้อย

  ระดับ E : ไม่มีโอกาสเกิดขึ้นได้

- ขั้นที่ 3 นำข้อมูลที่ได้ในขั้นที่ 1 และ 2 มาจัดทำเป็น Risk Assessment Matrix เพื่อแบ่งระดับความเสี่ยงออกเป็นระดับต่างๆ ดังตารางที่ 2.2

ตารางที่ 2.2 Risk Assessment Matrix

ระดับความรุนแรง	โอกาสที่เกิดขึ้น				
	A	B	C	D	E
1	Risk 1	Risk 1	Risk 1	Risk 2	Risk 3
2	Risk 1	Risk 1	Risk 2	Risk 2	Risk 3
3	Risk 1	Risk 2	Risk 2	Risk 3	Risk 3
4	Risk 3	Risk 3	Risk 4	Risk 4	Risk 4

จากตารางที่ได้สามารถอธิบายระดับความเสี่ยงระดับต่างๆได้ดังนี้

Risk 1 หมายถึง ไม่สามารถยอมรับให้เกิดขึ้นได้และควรมีการแก้ไขโดยเร่งด่วน

Risk 2 หมายถึง ไม่สามารถยอมรับให้เกิดขึ้นได้และควรมีการแก้ไขโดยผ่านการพิจารณาจากผู้บริหารได้

Risk 3 หมายถึง สามารถยอมรับได้โดยมีการทบทวนจากผู้บริหาร

Risk 4 หมายถึง สามารถยอมรับได้โดยไม่ต้องมีการทบทวนจากผู้บริหาร

จากทั้ง 3 ขั้นตอนจะทำให้เราทราบถึงระดับความเสี่ยงที่เกิดขึ้นกับทุกๆ ระบบ และจากผลการประเมินผลกระทบทั้ง 2 ลักษณะข้างต้น เราจะนำผลที่จากทั้ง 2 วิธีมาพิจารณาร่วมกันในการจัดลำดับความสำคัญของระบบต่างๆ ซึ่งผลที่ได้จะทำให้เราทราบว่าระบบใดที่เราควรให้ความสำคัญในการป้องกันจากภัยคุกคามมากที่สุด

2.3.3 เครื่องมือที่ใช้ในการประเมินความเสี่ยง (GAO. 1999 ; ISO/IEC. 2000)

สำหรับเครื่องมือที่ใช้ช่วยในการประเมินสามารถทำได้หลายวิธี เช่น การสังเกตการณ์ การสัมภาษณ์ การทำแบบสอบถาม การใช้ซอฟต์แวร์เพื่อช่วยในการวิเคราะห์และจัดทำเอกสาร รวมถึงการไปดูสภาพการทำงานหรือสถานที่ทำงานจริง (Site Visit) ซึ่งวิธีเหล่านี้จะทำให้เราสามารถทราบได้ว่า ระบบคอมพิวเตอร์ที่ทำการประเมินยังมีจุดบกพร่องหรือจุดอ่อนตรงไหน ที่อาจเกิดอันตรายต่อระบบและควรได้รับการปรับปรุงแก้ไข

สำหรับรายงานฉบับนี้จะยกตัวอย่างวิธีการสอบถามและสังเกตการณ์จากการทำงานในศูนย์คอมพิวเตอร์ ซึ่งจะเริ่มจากการจัดทำแบบสอบถาม โดยตัวอย่างแบบสอบถามที่จัดทำขึ้นเป็นไปดังตารางที่ 2.3 โดยรายละเอียดที่ประเมินได้มาจากการพิจารณาจากระบบต่างๆที่มีใช้งานอยู่ในบริษัทและจากข้อกำหนดตามมาตรฐาน ISO 17799

ตารางที่ 2.3 แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ

แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ		**ประจำปี**	
รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
1.มีมาตรการป้องกันและแผนฉุกเฉินเพื่อไม่ให้เกิดผลเสียหายต่อศูนย์คอมพิวเตอร์โดยตรง			
• มีการกำหนดแผนแม่บทการรักษาความปลอดภัยด้านระบบสารสนเทศ			

ตารางที่ 2.3 แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
• มีแผนกู้ภัยเหตุการณ์ฉุกเฉิน โดยมีเอกสารแผนและการกำหนดความรับผิดชอบอย่างชัดเจน โดยระบุวิธีการที่ต้องทำตามลำดับขั้นตอน และระบุระบบที่วิกฤติที่ต้องได้รับการกู้ภัยก่อนระบบอื่น			
• แผนการกู้ภัยมีการระบุระบบและอุปกรณ์สำรอง			
• มีการจัดเก็บสำเนาไว้ในที่ห่างไกลหรือคนละอาคาร			
• มีการประกันทรัพย์สินในศูนย์คอมพิวเตอร์			
2.การจัดโครงสร้างการแบ่งแยกหน้าที่			
• มีการแบ่งแยกหน้าที่ในศูนย์คอมพิวเตอร์ระหว่างผู้ปฏิบัติการด้านคอมพิวเตอร์ ผู้เขียนโปรแกรม เป็นต้น			
• มีการแบ่งแยกหน้าที่ระหว่างศูนย์คอมพิวเตอร์กับผู้ใช้ สำหรับหน้าที่บางประการไม่ควรให้หน่วยงานคอมพิวเตอร์กระทำ แต่เป็นหน้าที่ของหน่วยงานหรือหน่วยงานผู้ใช้เพื่อให้สามารถสอบทานกันได้ หน้าที่ดังกล่าว การอนุมัติรหัสผ่านและระดับสิทธิการเข้าใช้ระบบงาน การอนุมัติการแก้ไขระบบงานโดยผู้บริหารระดับสูง เป็นต้น			
• มีการแต่งตั้งผู้ทำหน้าที่ Security Administrator			
3. มีการกำหนดวิธีปฏิบัติงานในศูนย์คอมพิวเตอร์			
• ตารางกำหนดเวลาการปฏิบัติงานของพนักงานในศูนย์			
• ตารางเวลาการบำรุงรักษาอุปกรณ์และระบบ			
• รายละเอียดวิธีปฏิบัติงานในแต่ละระบบ			

ตารางที่ 2.3 แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
• การจัดเก็บโปรแกรม/ข้อมูลและการทำลายแฟ้มข้อมูล			
• การ Backup ข้อมูลและโปรแกรมโดยมีการ Backup และ Update ทุกครั้งที่มีการเปลี่ยนแปลง			
• การจัดทำทะเบียนทรัพย์สินเครื่องคอมฯและอุปกรณ์			
4. การควบคุมด้าน Network			
• มีการจัดทำแผนผังแสดงเครือข่ายสื่อสาร			
• มีการตรวจสอบการติดตั้งอุปกรณ์จริง ว่าตรงกับแผนผังหรือไม่			
• อุปกรณ์ Network ติดตั้งในสถานที่ปลอดภัย			
• มีการกำหนดสิทธิในการเข้าใช้งานตามหน้าที่รับผิดชอบ			
• ผู้ใช้ Login เข้าระบบต้องใช้ User ID และ Password			
• เมื่อมีการเปลี่ยนแปลงสถานะของผู้ใช้ ผู้ดูแลระบบต้องยกเลิกสิทธิสำหรับผู้ใช้คนนั้นทันที			
• ผู้ดูแลได้สอบทาน Log File สำหรับการเข้าระบบอย่างเสมอ			
• ผู้ดูแลตรวจหาจุดอ่อนในระบบสม่ำเสมอเพื่อหาทางป้องกัน			
5. ความปลอดภัยโดยทั่วไปและมีการป้องกันไฟไหม้			
• ที่ตั้ง			
- ที่ตั้งของศูนย์คอมพิวเตอร์ อยู่ในพื้นที่หรือระดับชั้นที่น้ำท่วมได้หรือไม่ หรืออยู่ชั้นสูงๆของอาคาร ซึ่งยากที่เจ้าหน้าที่ดับเพลิงจะเข้าถึงหรือไม่ - ศูนย์ฯตั้งอยู่ในที่ปลอดภัย ไม่เปิดเผย แต่ไม่ลับตาจนไม่ทราบการเคลื่อนไหว เข้า-ออก			

ตารางที่ 2.3 แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
• การเข้าถึง			
- การเข้าถึงศูนย์คอมพิวเตอร์ จำกัดเฉพาะพนักงานด้านปฏิบัติการและควรเข้าเขตบางเขตเฉพาะตามตารางเวลาทำงานเท่านั้น - มีพนักงานอื่นเข้าไปในห้องคอมพิวเตอร์บ่อยหรือไม่ - มีการจัดเวร - มีระบบสัญญาณเตือนภัยและความปลอดภัยอื่นๆถ้าไม่มีคนประจำศูนย์ - มีการใช้ระบบควบคุมประตูเข้า-ออก หรือใช้ระบบควบคุมด้วยการ์ด และอนุญาตเฉพาะบุคคลที่มีหน้าที่รับผิดชอบ			
• การผ่านเข้าออกมีการบันทึกลงนามและเวลา			
• การเก็บรักษาแผ่น Diskette และเทปข้อมูล			
- แผ่น Diskette และเทป เก็บในที่ที่ปลอดภัย โดยเฉพาะจากสนามแม่เหล็ก			
- มีการสุ่มตรวจนับเป็นระยะๆ			
• การกำจัดวัสดุเชื้อไฟ มีข้อกำหนดว่า เฉพาะเครื่องใช้ที่จำเป็นเท่านั้นที่นำมาใช้ในห้องคอมพิวเตอร์ โดยต้องจำกัดจำนวนสิ่งของที่ติดไฟได้ง่าย และมีการห้ามนำอุปกรณ์ที่เป็นสื่อไฟ วัตถุระเบิดเข้าห้องคอมพิวเตอร์			
• มีระบบไฟฟ้าฉุกเฉินและระบบสำรองพลังงาน			
6.มีการควบคุมการป้องกันการเข้าถึงแฟ้มข้อมูลและโปรแกรมจากผู้ไม่ประสงค์ดี หรือการแก้ไขที่ไม่มีอำนาจ			
• การเข้าถึงข้อมูลและโปรแกรม			

ตารางที่ 2.3 แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
- มีขั้นตอนการอนุญาตให้เข้าถึงข้อมูลได้และการอนุญาตและระดับสิทธเป็นไปตามหลักความจำเป็นในการใช้งาน - มีการจัดการกับ Password เช่น ต้องมีการเปลี่ยนอย่างสม่ำเสมอ - มีการควบคุมการเข้าถึงระบบและการฝ่าฝืน - มีการพิจารณาเข้ารหัส (Encrypt) ข้อมูลที่มีความสำคัญ			
• หากสามารถเข้าถึงระบบได้หลายวิธี มีการสอบทานการควบคุมการเข้าถึงทุกวิธีการนั้น			

ในการสรุปผลเราจะพิจารณาได้จากคำตอบ กล่าวคือ หากคำตอบในแต่ละข้อส่วนใหญ่ คือ ไม่ใช่ แสดงให้เห็นว่าระบบโดยรวมยังมีความเสี่ยงในเรื่องการรักษาความปลอดภัย ซึ่งควรจะพิจารณาที่จะนำไประบุไว้ในแผนความปลอดภัย

บทที่ 3

รายละเอียดบริษัทและระบบสารสนเทศที่ใช้ปัจจุบัน

3.1 ประวัติโดยย่อ

บริษัท เทเลโฟนไทย จำกัด เป็นบริษัทของคนไทยได้ถือกำเนิดขึ้นเมื่อวันที่ 29 มิถุนายน 2535 ด้วยทุนจดทะเบียนเริ่มแรก 100 ล้านบาท บริษัทฯ ได้ร่วมลงนามในสัญญาร่วมกับองค์การโทรศัพท์แห่งประเทศไทย (ทศท.) เมื่อวันที่ 2 กรกฎาคม 2535 ในสัญญาร่วมการงานและร่วมลงทุนในโครงการขยายโทรศัพท์ภูมิภาค จำนวน 1 ล้านเลขหมาย โดยบริษัทฯ จะเป็นผู้ดำเนินการและบำรุงรักษาอุปกรณ์ในระบบ ซึ่งเริ่มดำเนินการเมื่อวันที่ 25 ตุลาคม 2536 โดยมีอายุสัมปทาน 25 ปี จนถึงวันที่ 25 ตุลาคม 2561 และในวันที่ 21 กันยายน 2538 ได้รับอนุมัติจากทศท. ให้ติดตั้งโทรศัพท์เพิ่มขึ้นอีก 5 แสนเลขหมายในเขตภูมิภาครวมเป็น 1.5 ล้านเลขหมาย

โครงข่ายโทรศัพท์พื้นฐานในเขตโทรศัพท์ภูมิภาคทั่วประเทศจำนวน 1.5 ล้านเลขหมายของเทเลโฟนไทย(ยกเว้น กรุงเทพฯ ,นนทบุรี, สมุทรปราการ และปทุมธานี) ใช้ระบบสายเคเบิลใยแก้วนำแสง (Fiber Optics Cable) เกือบทั้งโครงข่าย มีเพียงส่วนชุมสายย่อยที่ต่อไปยังตัวโทรศัพท์เท่านั้นที่ใช้ระบบสายเคเบิลทองแดง (Copper Cable) และระบบโครงข่าย 1.5 ล้านเลขหมายยังเป็นระบบดิจิตอลครบวงจร ซึ่งอุปกรณ์ของระบบ คือ อุปกรณ์ชุมสาย (Switching) ทั้งในชุมสายหลัก (MSU:Main Switching Unit) และชุมสายย่อย (RSU:Remote Switching Unit) และเครือข่ายสื่อสัญญาณ (Transmission Network) ได้รับการพัฒนาขึ้นมา ในระบบดิจิตอล โครงข่าย 1.5 ล้านเลขหมายของเทเลโฟนไทยจึงสามารถใช้งานได้อย่าง มีประสิทธิภาพและรองรับบริการเสริมเพื่อความสะดวกสบายของผู้ใช้บริการได้อย่างไม่มีขีดจำกัด

3.2 ลักษณะการดำเนินธุรกิจ

บริษัท เทเลโฟนไทย จำกัด เป็นบริษัทเอกชนที่ทำธุรกิจประเภทโทรคมนาคมซึ่งให้บริการ 2 ประเภทดังนี้

1.บริการโทรศัพท์พื้นฐาน ซึ่งได้รับสัมปทานจากองค์การโทรศัพท์แห่งประเทศไทยในการให้บริการโทรศัพท์พื้นฐานในเขตภูมิภาคผ่านระบบเครือข่ายโทรศัพท์ของตนเองที่มีอยู่ทั่วประเทศ โดยปัจจุบันมีลูกค้าทั้งที่เป็นประเภทที่พักอาศัยและประเภทธุรกิจที่ใช้บริการอยู่ในเขตภูมิภาครวมทั้งสิ้น 72 จังหวัดนอกจากนี้ยังให้บริการเสริมสำหรับโทรศัพท์พื้นฐาน เช่นบริการแสดงหมายเลขที่

เรียกเข้า บริการระบบจัดลำดับหมายเลขรับโทรศัพท์ บริการตู้สาขาอัตโนมัติระบบต่อเข้าตรง เพื่อความสะดวกในการใช้บริการของผู้เช่ารวมทั้งเป็นการเพิ่มรายได้ให้กับบริษัทด้วย

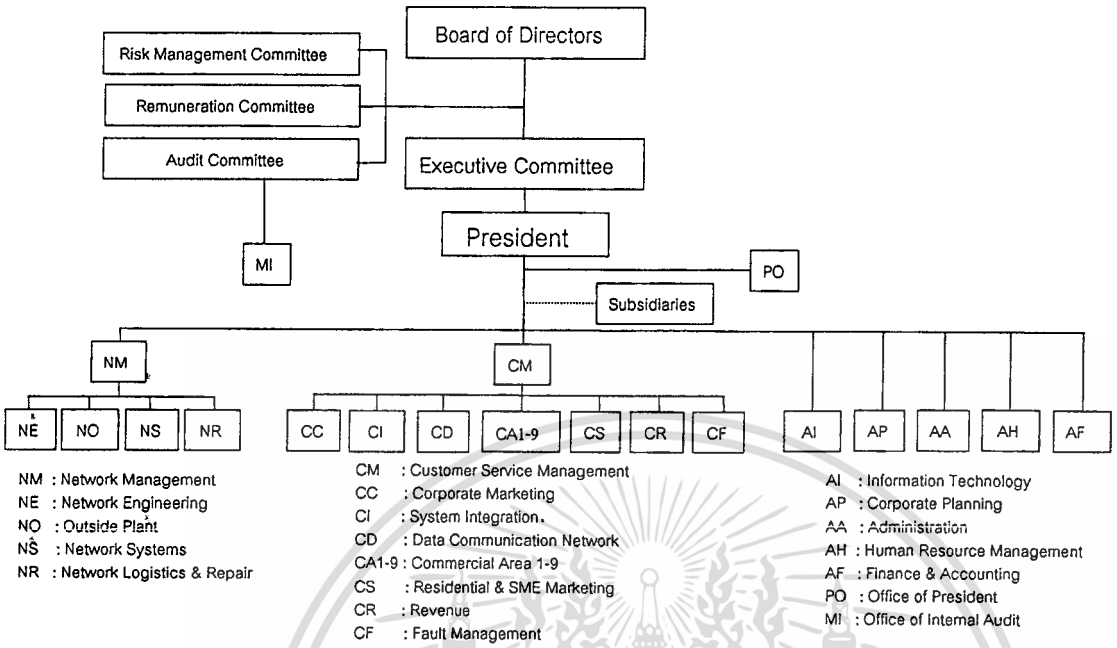
2. บริการวงจรเช่า (Leased Circuit) ซึ่งเป็นธุรกิจเสริมของบริษัท โดยมีการให้บริการผ่านเครือข่าย X.25 Network หรือ Multiservice Network ซึ่งเป็นเครือข่ายเพื่อใช้รองรับบริการรูปแบบใหม่ๆเช่น ADSL Frame Relay ATM และ Voice Over IP ซึ่งจะช่วยเพิ่มประสิทธิภาพการให้บริการวงจรสื่อสารข้อมูลของบริษัทได้เป็นอย่างดี และในปัจจุบันได้นำ Framc Rclay และ ADSL มาให้บริการกับระบบสื่อสารข้อมูลภายในบริษัทฯและลูกค้าภายนอกบางรายแล้วซึ่งส่วนใหญ่จะเป็นองค์กรขนาดใหญ่ เช่น ธนาคาร บริษัท ISP ต่างๆ หรือ บริษัทเอกชนที่มีสาขาอยู่ในต่างจังหวัด นอกจากนั้น ในธุรกิจวงจรเช่า บริษัทฯยังได้ให้บริการวงจรเช่าระบบสื่อสัญญาณตั้งแต่ 2 Mbps ขึ้นไปโดยลูกค้าส่วนใหญ่จะเป็นบริษัทโทรคมนาคมหรือ Operator รายอื่นๆ

ในการดำเนินธุรกิจ บริษัทได้แบ่งพื้นที่ความรับผิดชอบเป็น 9 เขตธุรกิจและจัดตั้งศูนย์บริหารงานในทุกๆเขต และมีสำนักงานใหญ่ (Headquarter) ตั้งอยู่ที่กรุงเทพฯ ซึ่งจะเป็นที่ตั้งของสำนักกรรมการผู้จัดการใหญ่และฝ่ายต่างๆของบริษัทโดยแต่ละฝ่ายจะมีผู้บริหารและพนักงานบางส่วนสนับสนุนการปฏิบัติงานของพนักงานในพื้นที่ ซึ่งในการทำงานก็จะมีการติดต่อสื่อสารกันระหว่างหน่วยงานในส่วนกลางกับหน่วยงานในเขตธุรกิจต่างๆอยู่เสมอ

3.3 โครงสร้างองค์กร

ประกอบด้วยหน่วยงานหลักๆ ดังนี้

1. สายงานบริหารโครงข่าย
2. สายงานบริการลูกค้า
3. ฝ่ายเทคโนโลยีสารสนเทศ
4. ฝ่ายวางแผนวิสาหกิจ
5. ฝ่ายธุรการ
6. ฝ่ายบริหารทรัพยากรบุคคล
7. ฝ่ายการเงินและบัญชี
8. สำนักงานกรรมการผู้จัดการใหญ่
9. สำนักงานตรวจสอบภายใน



รูปที่ 3.1 โครงสร้างองค์กรของบริษัท

สำหรับฝ่ายเทคโนโลยีสารสนเทศ มีผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นผู้บังคับบัญชาสูงสุดประกอบไปด้วยหน่วยงาน 3 ส่วนดังนี้

1. ส่วนบริการสารสนเทศ มีผู้จัดการส่วนบริการสารสนเทศเป็นผู้บังคับบัญชา และมีหน้าที่และความรับผิดชอบหลักดังนี้

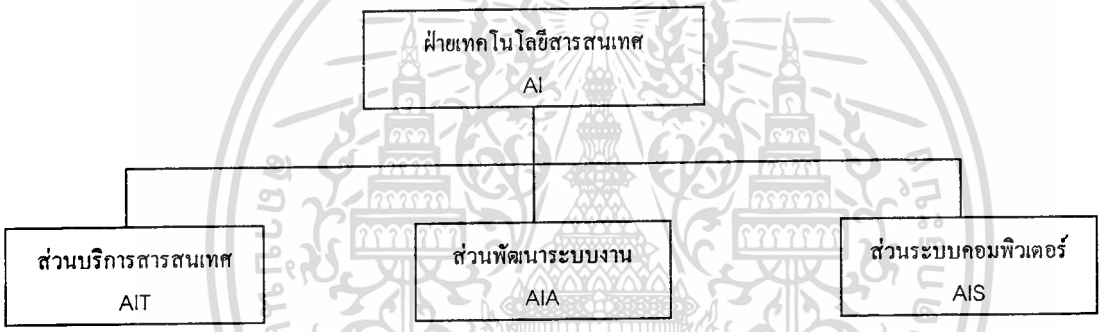
- จัดอบรมความรู้ทางด้านคอมพิวเตอร์ให้กับผู้ใช้
- ให้คำปรึกษาแนะนำกับผู้ใช้ที่มีปัญหาการใช้งานระบบ
- ติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ให้กับผู้ใช้
- ควบคุมดูแลอุปกรณ์สำรอง

2. ส่วนพัฒนาระบบงาน มีผู้จัดการส่วนพัฒนาระบบงานเป็นผู้บังคับบัญชา และมีหน้าที่และความรับผิดชอบดังนี้

- วิเคราะห์และพัฒนาฮาร์ดแวร์ ซอฟท์แวร์ระบบ เครื่องมือที่ใช้ในการพัฒนาระบบและทดสอบ
- จัดทำมาตรฐานของฮาร์ดแวร์ ซอฟท์แวร์ระบบ ซอฟท์แวร์ประยุกต์ เครือข่าย การทดสอบซอฟท์แวร์ การปฏิบัติงาน สำหรับฝ่ายเทคโนโลยีสารสนเทศ
- วางแผนการดำเนินงานโครงการต่างๆที่เกี่ยวข้องกับฝ่ายเทคโนโลยีสารสนเทศ

3. ส่วนระบบคอมพิวเตอร์ มีผู้จัดการส่วนระบบคอมพิวเตอร์เป็นผู้บังคับบัญชา และมีหน้าที่และความรับผิดชอบดังนี้

- พัฒนาซอฟท์แวร์ประยุกต์ที่ใช้ในบริษัท
- ดูแลรักษาระบบคอมพิวเตอร์ต่างๆ และระบบความปลอดภัยที่ใช้ในบริษัทให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
- ตรวจรับและทดสอบระบบใหม่ๆ
- สำรองข้อมูล ตรวจสอบสมรรถนะของระบบสารสนเทศ
- จัดซื้อจัดหาอุปกรณ์คอมพิวเตอร์
- ดูแลจัดสรรทรัพยากรและงบประมาณทางด้านระบบคอมพิวเตอร์



รูปที่ 3.2 โครงสร้างฝ่ายเทคโนโลยีสารสนเทศ

สำหรับบุคลากรระดับปฏิบัติงานในฝ่ายเทคโนโลยีสารสนเทศในปัจจุบันนี้จะประกอบด้วยตำแหน่งและหน้าที่ความรับผิดชอบต่างๆ ดังนี้

- เจ้าหน้าที่ Helpdesk มีหน้าที่ในการให้คำแนะนำและแก้ไขปัญหาเบื้องต้นในกับผู้ใช้
- เจ้าหน้าที่บริการสารสนเทศ มีหน้าที่ในการให้บริการติดตั้งและบำรุงรักษาด้านคอมพิวเตอร์และสารสนเทศให้กับผู้ใช้
- System Engineer มีหน้าที่ควบคุมดูแลและวิเคราะห์การใช้งานระบบปฏิบัติการและฮาร์ดแวร์ต่างๆ เพื่อหาแนวทางพัฒนาให้มีประสิทธิภาพมากขึ้น
- Software Engineer มีหน้าที่ควบคุมดูแลและวิเคราะห์ผลการพัฒนาซอฟท์แวร์ต่างๆ ของบริษัท
- System Programmer มีหน้าที่ติดตามการใช้ฮาร์ดแวร์และซอฟท์แวร์ระบบตลอดจนพัฒนาซอฟท์แวร์ระบบ

- System Analysis มีหน้าที่วิเคราะห์และออกแบบระบบคอมพิวเตอร์ ระบบงานและจัดทำเอกสารที่เกี่ยวข้อง
- Network Engineer มีหน้าที่วิเคราะห์และปฏิบัติการเกี่ยวกับอุปกรณ์และโปรแกรมทางด้านระบบเครือข่าย
- Database Administrator มีหน้าที่ควบคุมดูแลการใช้งาน บำรุงรักษาและกำหนดมาตรฐานระบบฐานข้อมูล
- Programmer มีหน้าที่เขียนโปรแกรมและพัฒนาซอฟท์แวร์ประยุกต์ตาม System Specification
- เจ้าหน้าที่ระบบคอมพิวเตอร์ มีหน้าที่ดูแลรักษาและแก้ไขระบบคอมพิวเตอร์ต่างๆให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

3.4 ระบบสารสนเทศที่ใช้ปัจจุบัน

ในส่วนของระบบสารสนเทศ บริษัทได้มีการใช้งานระบบสารสนเทศในด้านต่างๆเพื่ออำนวยความสะดวกและเพิ่มประสิทธิภาพในการทำงานของบริษัท ซึ่งเครื่องคอมพิวเตอร์ที่มีอยู่ในบริษัทส่วนใหญ่จะใช้งานผ่านเครือข่าย LAN ของบริษัทฯ โดยเครื่อง Client ที่ใช้งานอยู่ภายในจะติดต่อกับเครื่อง Server ต่างๆของบริษัท จำนวน 7 เครื่องดังต่อไปนี้

1) File & Print Server : เพื่อใช้ในการ Share ทรัพยากรร่วมกันของเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่าย LAN

2) Mail Server : เพื่อใช้ในการรับ-ส่ง E-mail สำหรับระบบ Intranet และ Internet

3) News Server : เพื่อใช้ในการใช้งานระบบ Intranet News ภายในบริษัท

4) Database Server : เพื่อใช้ในการจัดเก็บข้อมูลสำหรับระบบฐานข้อมูลต่างๆในบริษัท

5) Web Server : เพื่อใช้ในการค้นหาข้อมูลและบันทึกข้อมูลผ่าน Web ภายในบริษัท

6) Proxy Server : เพื่อใช้เป็น Buffer ตัวหนึ่งที่ช่วยจดจำและเก็บ Website ต่างๆที่เครื่อง Client ในบริษัทฯ เคยมีการ Access เข้าไปแล้ว ซึ่งถ้าในภายหลังมี Client เครื่องอื่นๆ ต้องการ Access ไปที่ Website เดียวกัน Proxy Server ก็จะนำรายละเอียดของ Website ไปแสดงผลให้กับเครื่อง Client นั้นๆได้ทันทีซึ่งจะทำให้เข้าถึงข้อมูลได้รวดเร็วขึ้น

7) Remote Access Server : เพื่อใช้ในการติดต่อเข้ากับเครือข่ายของบริษัทจากภายนอก

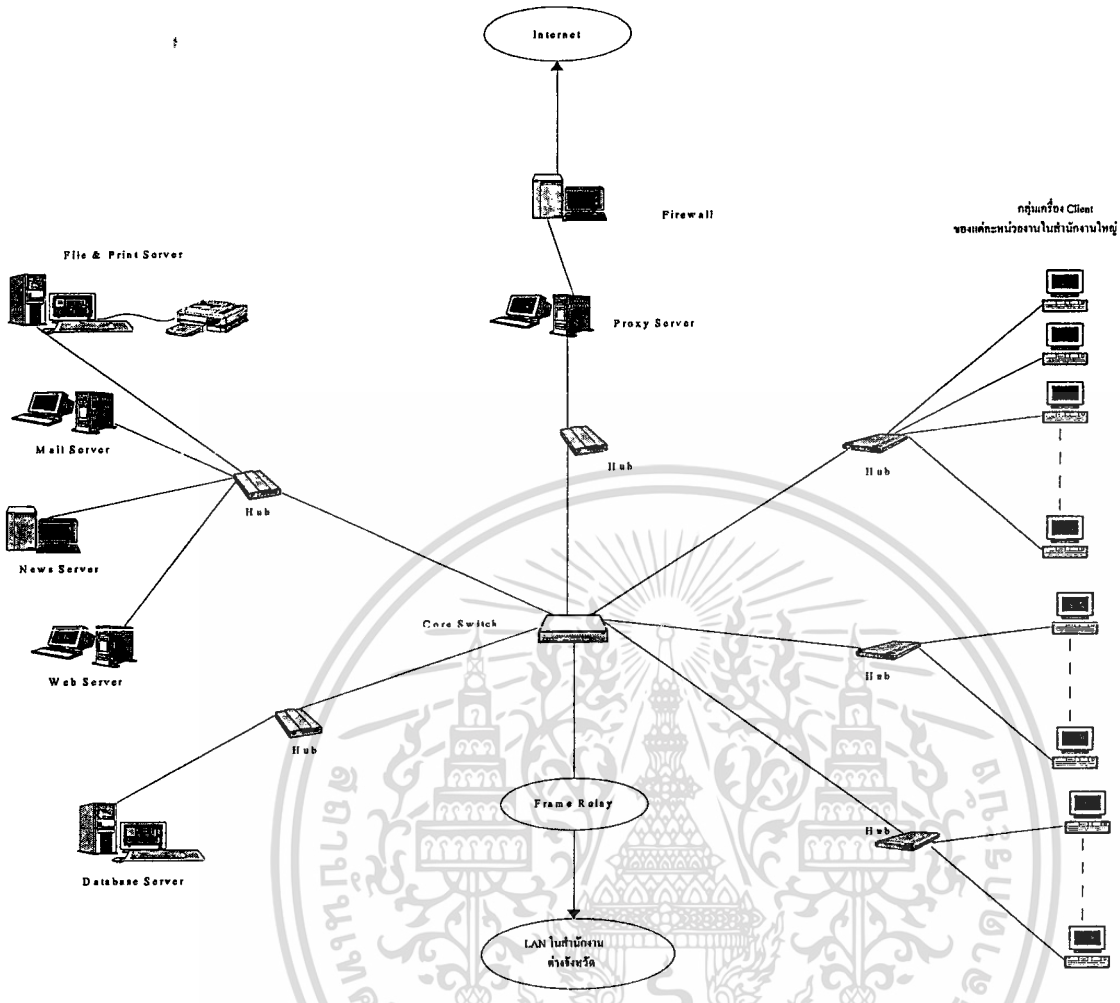
สำหรับรายละเอียดของเครือข่าย LAN ของบริษัทดังรูปที่ 3.3 มีคุณลักษณะดังนี้

1) Network Topology เป็นแบบ Star

2) เป็นเครือข่ายแบบ Fast Ethernet (10/100 Mbps) โดยผ่าน TCP/IP Protocol
3) Media ที่ใช้เชื่อมต่อระหว่าง Client และ Server ในโครงข่าย คือ สาย UTP (Unshielded Twisted Pair)
4) Network Architectures เป็นแบบ Client-Server ชนิด N-Tiered เนื่องจากมี Application Server หลายตัวดังที่กล่าวข้างต้น
5) ลักษณะ Circuit Configuration เป็นแบบ Multipoint
6) ในการติดต่อเข้ากับ Internet จะผ่าน เครื่อง Firewall ทำหน้าที่ป้องกันการโจรกรรมข้อมูลจากภายนอกและเพิ่มความปลอดภัยให้กับระบบ
7) มี Core Switch เป็นอุปกรณ์ Switching ในระดับ Network Layer ซึ่งทำหน้าที่ในการเชื่อมต่อสัญญาณระหว่างเครื่อง Client หรือระหว่างเครื่อง Client กับ Application Server ต่างๆ ซึ่งก็เสมือนกับอุปกรณ์ชุมสายในเครือข่ายโทรศัพท์ รวมทั้งยังมีหน้าที่ในการเลือกเส้นทาง (Routing) ในการเชื่อมต่อสัญญาณให้ด้วย
8) การติดต่อกับเครื่องคอมพิวเตอร์ในสำนักงานต่างจังหวัดสามารถติดต่อผ่านทาง Frame Relay ซึ่งเป็นโปรโตคอลที่ใช้งานบนเครือข่าย Multiservice ของบริษัทฯ ซึ่งเริ่มติดตั้งและใช้งานตั้งแต่ต้นปี 2544 ที่ผ่านมา

ในส่วนของการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานภายในบริษัท เพื่อสนับสนุนการปฏิบัติงานของพนักงาน มีหัวข้อหลักๆดังต่อไปนี้

1) การใช้งานด้าน Office Automation
2) การใช้งานทรัพยากรผ่านเครือข่าย LAN เช่น เก็บข้อมูลใน File Server หรือพิมพ์เอกสารผ่าน Network Printer
3) การใช้งาน Intranet ,E-mail ,FTP เพื่อติดต่อกับสำนักงานต่างจังหวัด
4) การใช้งาน Internet ผ่าน Proxy Server
5) การใช้งานและพัฒนา Application ต่างๆ เพื่อใช้ในการเก็บข้อมูลของบริษัท
6) การจัดทำ Remote Terminal เพื่อใช้ตรวจสอบระบบโครงข่ายโทรคมนาคม
7) การใช้งาน Document-Based Groupware ผ่านระบบเครือข่าย Intranet
8) การทำ Remote Access จากภายนอกเข้าสู่เครือข่ายของบริษัท
9) การใช้งาน Newsgroup เพื่อเผยแพร่ข่าวสารและแสดงความคิดเห็นของพนักงานภายในบริษัท



รูปที่ 3.3 เครือข่าย LAN ของบริษัท

3.5 ระบบความปลอดภัยที่ใช้ปัจจุบัน

โดยทั่วไปการติดตั้งระบบความปลอดภัย มีจุดประสงค์ทั้งสิ้น 3 อย่าง คือ

- เพื่อรักษาความลับข้อมูล(Confidentiality) หมายถึง การปกป้องข้อมูลไม่ให้ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตอย่างถูกต้อง และถ้ามีการขโมยข้อมูลไปแล้วก็ไม่สามารถอ่านหรือทำความเข้าใจข้อมูลนั้นได้ เนื่องจากวิธีการปกป้องข้อมูลอย่างเพียงพอ
- เพื่อป้องกันการปลอมแปลงข้อมูล(Integrity) หมายถึงการรักษาความถูกต้องของข้อมูลและป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การที่ระบบความปลอดภัยจะสามารถทำเช่นนี้ได้ จะต้องมีการควบคุมว่าผู้ใดจะสามารถทำอะไรได้บ้างกับข้อมูลนั้นๆ เช่น การอ่านหรือเขียนข้อมูลได้เพียงอย่างเดียว หรือได้ทั้งอ่านและเขียนข้อมูล เป็นต้น

- เพื่อทำให้ระบบสามารถที่จะทำงานได้ตามปกติและเต็มประสิทธิภาพ(Availability) หมายถึง ระบบต้องสามารถทำงานได้อย่างดีตามจุดมุ่งหมายในการใช้ และต้องมีขีดความสามารถปฏิบัติงานได้ในปริมาณตามที่ต้องการได้ รวมทั้งจะต้องปฏิบัติงานได้ภายในเวลาที่กำหนดด้วย

และในส่วนของบริษัทได้มีการติดตั้งและนำระบบความปลอดภัยเข้ามาใช้งาน ซึ่งสามารถแบ่งแยกส่วนของระบบความปลอดภัยตามชนิดของการป้องกันเป็น 3 ส่วน คือ การป้องกันทางด้านกายภาพ การป้องกันภัยโดยใช้อุปกรณ์ทางด้าน Hardware ซึ่งในที่นี้หมายถึง Firewall และ การป้องกันโดยใช้ Software ซึ่งในที่นี้หมายถึง โปรแกรมป้องกันไวรัส และการควบคุมการเข้าถึงและใช้งานระบบต่างๆโดยการกำหนด User ID และ Password สำหรับพนักงานในบริษัทโดยทั้ง 3 ส่วน มีรายละเอียดดังนี้

1) การป้องกันทางด้านกายภาพ

- มีพนักงานรักษาความปลอดภัยประจำตลอดเวลาบริเวณทางเข้า-ออกของสำนักงาน
- ประตูทางเข้า-ออกของสำนักงานในแต่ละชั้นมีการติดตั้งอุปกรณ์ควบคุมการเข้า-ออก ซึ่งพนักงานจะต้องติดบัตรพนักงานไว้ตลอดเวลาที่อยู่ในสำนักงานเพื่อใช้ในการเข้า-ออกสำนักงาน
- มีการจัดทำทะเบียนควบคุมการผ่านเข้า-ออกสำหรับคนที่ไม่มีสิทธิหรือในกรณีที่มีการเข้า-ออกในวันหยุดของบริษัท โดยบันทึก ชื่อ ที่อยู่ เหตุผลที่มาติดต่อ และเวลาเข้า-ออกในทะเบียนทุกครั้ง
- มีการติดตั้งเครื่องตรวจจับความร้อนและควันไฟภายในสำนักงานอยู่เป็นช่วงๆ

2) การป้องกันภัยโดยใช้อุปกรณ์ทางด้าน Hardware

- โดยการนำอุปกรณ์ Firewall มาใช้เพื่อช่วยในการป้องกันเครือข่ายภายในบริษัทจากการถูกบุกรุกผ่านทางเครือข่าย Internet
- ติดตั้ง Proxy Server เพื่อเพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอกโดยที่มีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)

3) การป้องกันโดยใช้ Software

- โดยการนำโปรแกรมป้องกันไวรัส Norton Antivirus Coporate Edition มาติดตั้งที่เครื่อง Client และ Server ที่ใช้งานผ่านเครือข่าย LAN ของบริษัท
- มีการกำหนดสิทธิของผู้ใช้และควบคุมการใช้งานในระบบต่างๆ เช่น ควบคุมและกำหนด User Login เข้า LAN สำหรับพนักงานแต่ละคนโดยผ่านเครื่อง Client ,กำหนด

User Account ให้กับพนักงานในการใช้งาน E-mail, ให้สิทธิเฉพาะพนักงานบางคนในการเชื่อมต่อกับ Internet , ควบคุมและกำหนด User Login เพื่อใช้งานระบบฐานข้อมูลในบริษัท

3.6 ลักษณะและประเภทของภัยคุกคามที่มีต่อระบบคอมพิวเตอร์ (Computer Threats) ของบริษัท

ภัยคุกคามที่มีต่อระบบคอมพิวเตอร์นั้น สามารถทำอันตรายต่อส่วนต่างๆของระบบได้ ไม่ว่าจะเป็น ตัวฮาร์ดแวร์ ซอฟท์แวร์ หรือข้อมูล ที่ถูกเก็บไว้ในระบบ เราสามารถจำแนกชนิดของภัยคุกคามได้เป็นชนิดใหญ่ๆ ดังนี้

1. การขัดขวางการทำงานของระบบ (Interruption) คือ มีการโจมตีระบบและทำให้ระบบสูญหายและ/หรือเสียหายจนไม่สามารถทำหน้าที่ของมันเองได้อย่างมีประสิทธิภาพ ตัวอย่างของการกระทำเช่นนี้ ได้แก่

- การทำลายส่วนใดส่วนหนึ่งของระบบคอมพิวเตอร์
- การลบส่วนใดส่วนหนึ่งของโปรแกรม หรือการลบส่วนใดส่วนหนึ่งของไฟล์ข้อมูล ซึ่งจะทำให้การทำงานของโปรแกรมนั้นๆ ผิดปกติหรือไม่ทำงานเลย

2. การลักลอบเข้ามาในระบบ (Interception) คือ มีการเข้ามาในระบบและดำเนินกิจกรรมต่างๆ โดยไม่ได้รับอนุญาต การลักลอบนั้นอาจทำโดยตัวโปรแกรมหรือโดยบุคคลใดโดยตรง เช่น

- การที่มีโปรแกรมลักลอบเข้ามาในระบบและทำการคัดลอกไฟล์ข้อมูลที่เป็นความลับไป
- การที่มีบุคคลทำการขโมยข้อมูล ในระหว่างการติดต่อสื่อสารภายในระบบเครือข่ายโดยใช้วิธีการดักดูข้อมูลที่ถูกส่งไปตามสายภายในระบบเครือข่ายคอมพิวเตอร์นั้นๆ

3. การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Modification) คือ การเปลี่ยนแปลงแก้ไขข้อมูลสำคัญที่เก็บภายในระบบฐานข้อมูลของระบบหรือภายในส่วนอื่นๆ ของระบบ เป็นต้น โดยที่ข้อมูลนั้นอาจเอื้อประโยชน์แก่ผู้ทุจริตได้

4. การเพิ่มรายการหรือข้อมูล (Fabrication) คือ การที่บุคคลที่ไม่ได้รับอนุญาตทำการเพิ่มรายการที่ไม่ถูกต้องเข้ามาในระบบ หรือการเพิ่มข้อมูลในฐานข้อมูลที่มีอยู่ ซึ่งหากผู้ปลอมแปลงมีความสามารถและประสบการณ์สูง จะทำให้เจ้าของระบบไม่สามารถแยกรายการหรือความแตกต่างได้เลย

จากการพิจารณาถึงลักษณะ รูปแบบการใช้งานของระบบสารสนเทศของบริษัทและประวัติการเกิดเหตุขัดข้องกับระบบสารสนเทศเท่าที่เคยมีมาในอดีต สามารถแบ่งลักษณะของภัยคุกคามที่มีโอกาสเกิดขึ้นกับระบบของบริษัทได้ดังต่อไปนี้

1. ภัยที่มีต่อฮาร์ดแวร์ สามารถจำแนกได้ดังนี้

- ภัยที่เกิดจากการชำรุดเสียหายของฮาร์ดแวร์ เช่น เกิดการกระแทก ฮาร์ดดิสก์ชำรุด
- ภัยที่เกิดระบบไฟฟ้า เช่น Power Surge
- ภัยจากการลักขโมย

2. ภัยที่มีต่อระบบซอฟท์แวร์

- การลบซอฟท์แวร์ ซึ่งอาจเกิดจากความตั้งใจหรือบังเอิญก็ได้
- การเปลี่ยนแปลงแก้ไขซอฟท์แวร์ ซึ่งทำให้โปรแกรมที่ทำงานอยู่ปกติเปลี่ยนเป็นทำงานผิดพลาดหรือผิดจุดมุ่งหมาย ทำให้ไม่สามารถใช้งานระบบหรือโปรแกรมได้
- การติดไวรัสคอมพิวเตอร์ทำให้ไม่สามารถใช้งานซอฟท์แวร์ระบบได้

3. ภัยที่มีต่อระบบข้อมูล

- การถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- การที่ข้อมูลถูกเปลี่ยนแปลงแก้ไข เช่น ข้อมูลที่ใช้ร่วมกันของผู้ใช้ที่จัดเก็บอยู่ใน Server
- การที่ข้อมูลถูกทำให้ไม่สามารถใช้งานได้

4. ภัยที่มีต่อระบบเครือข่าย เนื่องจากมีการใช้งานร่วมกันของผู้ใช้ระบบจำนวนมาก จึงมีภัยคุกคามที่อาจเกิดขึ้นได้ดังนี้

- การใช้งานร่วมกัน ซึ่งก่อให้เกิดปัญหาในการจัดการที่เกี่ยวกับการให้อนุญาตแก่ผู้ใช้ภายในระบบ ซึ่งอาจมีการแอบเข้ามาใช้ระบบโดยไม่ได้รับอนุญาต
- อุปกรณ์เครือข่ายเกิดการชำรุดเสียหายทำให้ไม่สามารถส่งผ่านข้อมูลได้ตามปกติ
- ไม่สามารถใช้งานเครือข่ายได้อย่างมีประสิทธิภาพอันเนื่องจากการติดไวรัสคอมพิวเตอร์

บทที่ 4

การสร้างแผนความปลอดภัยระบบสารสนเทศสำหรับบริษัท

4.1 การประเมินความเสี่ยงระบบสารสนเทศของบริษัท

ในการประเมินความเสี่ยงระบบสารสนเทศของบริษัท จะใช้กระบวนการและหลักเกณฑ์การประเมินค่าผลกระทบตามที่อธิบายในหัวข้อ 2.3 มาประกอบกันในการประเมินความเสี่ยงดังนี้

4.1.1 การประเมินผลกระทบโดยรวม ซึ่งเราจะได้ผลการประเมินและลำดับความสำคัญของระบบสารสนเทศของบริษัทเป็นไปดังตารางที่ 4.1

ตารางที่ 4.1 การประเมินค่าผลกระทบโดยรวมสำหรับระบบสารสนเทศของบริษัท

ระบบที่มีความเสี่ยง	ความสำคัญต่อธุรกิจ	ปัจจัยที่นำมาพิจารณา				ผลกระทบที่มีโดยรวม
		ความสำคัญของระบบ	ความสำคัญที่มีต่อสาธารณะ	ผลกระทบต่อธุรกิจ	ความง่ายที่จะถูกโจมตี	
เว็บไซต์และเว็บเซิร์ฟเวอร์	ไม่สำคัญต่อการดำเนินธุรกิจมาก เนื่องจากใช้เพื่อให้ข้อมูล	ปานกลาง(6)	มาก(10)	ปานกลาง(4)	มาก(9)	29
เมล์เซิร์ฟเวอร์	ธุรกิจยังดำเนินไปได้ แต่อาจจะลำบากขึ้น	มาก(9)	ปานกลาง(6)	มาก(8)	ปานกลาง(7)	30
ไฟล์เซิร์ฟเวอร์	ไม่สามารถใช้งานหรือข้อมูลจากทรัพยากรในเครือข่ายได้	มาก(10)	ปานกลาง(6)	มาก(10)	ปานกลาง(7)	33
ระบบฐานข้อมูลต่างๆ	มีความจำเป็นต่อการทำทรานแซกชั่นของธุรกิจ เป็นระบบที่ใช้เก็บข้อมูลทางด้านธุรกิจขององค์กรทั้งหมด	มาก(10)	มาก(9)	มาก(10)	ปานกลาง(6)	35

ตารางที่ 4.1 การประเมินค่าผลกระทบโดยรวมสำหรับระบบสารสนเทศของบริษัท(ต่อ)

ระบบที่มีความเสี่ยง	ความสำคัญต่อธุรกิจ	ปัจจัยที่นำมาพิจารณา				ผลกระทบที่มีโดยรวม
		ความสำคัญของระบบ	ความสำคัญที่มีต่อสาธารณะ	ผลกระทบต่อธุรกิจ	ความง่ายที่จะถูกโจมตี	
เครื่องคอมพิวเตอร์พนักงาน	ความเสียหายที่เกิดขึ้นกับเส่วนนี้จะหยุดการทำงานภายในองค์กรทั้งหมด	มาก(9)	ปานกลาง(6)	มาก(9)	มาก(8)	32
ระบบเครือข่าย	เป็นระบบที่มีความสำคัญยิ่งยวดซึ่งใช้เชื่อมต่อระบบภายในองค์กรเข้าด้วยกัน	มาก(10)	มาก(8)	มาก(10)	มาก(8)	36

4.1.2 การกำหนดระดับความเสี่ยง ตามที่กล่าวถึงในหัวข้อ 2.3.2 เราสามารถพิจารณาโอกาสที่จะเกิดภัยคุกคามและระดับความรุนแรงสำหรับแต่ละระบบ เพื่อทำการแบ่งระดับความเสี่ยงของแต่ละระบบได้ดังนี้

ตารางที่ 4.2 ระดับความเสี่ยงของระบบสารสนเทศต่างๆในบริษัท

ระบบ	โอกาสที่จะเกิดภัยคุกคาม	ระดับความรุนแรง	ระดับความเสี่ยง
เว็บไซต์และเว็บเซิร์ฟเวอร์	B	4	Risk 3
เมล์เซิร์ฟเวอร์	C	3	Risk 2
ไฟล์เซิร์ฟเวอร์	C	2	Risk 2
ระบบฐานข้อมูลต่างๆ	D	1	Risk 2
เครื่องคอมพิวเตอร์พนักงาน	B	3	Risk 2
ระบบเครือข่าย	B	1	Risk 1

จากผลการประเมินทั้ง 2 ลักษณะในตารางที่ 4.1 และ 4.2 สามารถจัดลำดับความสำคัญของระบบได้ดังตารางที่ 4.3

ตารางที่ 4.3 สรุปผลการจัดลำดับความสำคัญของระบบ

ระบบ	ผลกระทบที่มีโดยรวม	ระดับความเสี่ยง	ลำดับความสำคัญ
เว็บไซต์และเว็บเซิร์ฟเวอร์	29	Risk 3	6
เมล์เซิร์ฟเวอร์	30	Risk 2	5
ไฟล์เซิร์ฟเวอร์	33	Risk 2	3
ระบบฐานข้อมูลต่างๆ	35	Risk 2	2
เครื่องคอมพิวเตอร์พนักงาน	32	Risk 2	4
ระบบเครือข่าย	36	Risk 1	1

จากตารางจะสรุปได้ว่าระบบเครือข่ายจะเป็นระบบที่ควรให้ความสำคัญที่สุด รองลงมาก็จะเป็นระบบฐานข้อมูลต่างๆ ไฟล์เซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ของพนักงาน(Client) เมล์เซิร์ฟเวอร์ ส่วนเว็บเซิร์ฟเวอร์จะเป็นระบบที่มีค่าผลกระทบน้อยที่สุด

4.1.3 การประเมินความเสี่ยง โดยใช้แบบฟอร์มการประเมินตามตารางที่ 2.3 ทำการสอบถามข้อมูลต่างๆจากพนักงานของฝ่ายเทคโนโลยีสารสนเทศที่ดูแลด้านความปลอดภัยหรือพนักงานที่ทำหน้าที่เป็นเหมือน Security Administrator ซึ่งได้ผลการประเมินดังตารางที่ 4.4

ตารางที่ 4.4 ผลการประเมินความเสี่ยงของระบบสารสนเทศของบริษัท

แบบฟอร์มการประเมินความเสี่ยงของระบบสารสนเทศ		**ประจำปี 2545**	
รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
1.มีมาตรการป้องกันและแผนฉุกเฉินเพื่อไม่ให้เกิดผลเสียหายต่อศูนย์คอมพิวเตอร์โดยตรง			
• มีการกำหนดแผนแม่บทการรักษาความปลอดภัยด้านระบบสารสนเทศ		√	

ตารางที่ 4.4 ผลการประเมินความเสี่ยงของระบบสารสนเทศของบริษัท (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
• มีแผนกู้ภัยเหตุการณ์ฉุกเฉิน โดยมีเอกสารแผนและการกำหนดความรับผิดชอบอย่างชัดเจน โดยระบุวิธีการที่ต้องทำตามลำดับขั้นตอน และระบุระบบที่วิกฤติที่ต้องได้รับการกู้ภัยก่อนระบบอื่น		√	
• แผนการกู้ภัยมีการระบุระบบและอุปกรณ์สำรอง		√	
• มีการจัดเก็บสำเนาไว้ในที่ห่างไกลหรือคนละอาคาร		√	
• มีการประกันทรัพย์สินในศูนย์คอมพิวเตอร์	√		
2.การจัดโครงสร้างการแบ่งแยกหน้าที่			
• มีการแบ่งแยกหน้าที่ในศูนย์คอมพิวเตอร์ระหว่างผู้ปฏิบัติการด้านคอมพิวเตอร์ ผู้เขียนโปรแกรม เป็นต้น	√		
• มีการแบ่งแยกหน้าที่ระหว่างศูนย์คอมพิวเตอร์กับผู้ใช้ สำหรับหน้าที่บางประการไม่ควรให้หน่วยงานคอมพิวเตอร์กระทำ แต่เป็นหน้าที่ของหน่วยงานหรือหน่วยงานผู้ใช้เพื่อให้สามารถสอบทานกันได้ หน้าที่ดังกล่าว การอนุมัติรหัสผ่านและระดับสิทธิการเข้าใช้ระบบงาน การอนุมัติการแก้ไขระบบงานโดยผู้บริหารระดับสูง เป็นต้น	√		
• มีการแต่งตั้งผู้ทำหน้าที่ Security Administrator		√	
3. มีการกำหนดวิธีปฏิบัติงานในศูนย์คอมพิวเตอร์			
• ตารางกำหนดเวลาการปฏิบัติงานของพนักงานในศูนย์	√		
• ตารางเวลาการบำรุงรักษาอุปกรณ์และระบบ	√		
• รายละเอียดวิธีปฏิบัติงานในแต่ละระบบ	√		
• การจัดเก็บโปรแกรม/ข้อมูลและการทำลายแฟ้มข้อมูล		√	

ตารางที่ 4.4 ผลการประเมินความเสี่ยงของระบบสารสนเทศของบริษัท (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
• การ Backup ข้อมูลและโปรแกรมโดยมีการ Backup และ Update ทุกครั้งที่มีการเปลี่ยนแปลง		√	
• การจัดทำทะเบียนทรัพย์สินเครื่องคอมฯและอุปกรณ์	√		
4. การควบคุมด้าน Network			
• มีการจัดทำแผนผังแสดงเครือข่ายสื่อสาร	√		
• มีการตรวจสอบการติดตั้งอุปกรณ์จริง ว่าตรงกับแผนผังหรือไม่		√	
• อุปกรณ์ Network ติดตั้งในสถานที่ปลอดภัย	√		
• มีการกำหนดสิทธิในการเข้าใช้งานตามหน้าที่รับผิดชอบ		√	
• ผู้ใช้ Login เข้าระบบต้องใช้ User ID และ Password	√		
• เมื่อมีการเปลี่ยนแปลงสถานะของผู้ใช้ ผู้ดูแลระบบต้องยกเลิกสิทธิสำหรับผู้ใช้คนนั้นทันที	√		
• ผู้ดูแลได้สอบทาน Log File สำหรับการเข้าระบบอย่างเสมอ	√		
• ผู้ดูแลตรวจหาจุดอ่อนในระบบสม่ำเสมอเพื่อหาทางป้องกัน		√	
5. ความปลอดภัยโดยทั่วไปและมีการป้องกันไฟไหม้			
• ที่ตั้ง			

ตารางที่ 4.4 ผลการประเมินความเสี่ยงของระบบสารสนเทศของบริษัท (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
- ที่ตั้งของศูนย์คอมพิวเตอร์ อยู่ในพื้นที่หรือระดับชั้นที่น้ำท่วมได้หรือไม่ หรืออยู่ชั้นสูงๆของอาคาร ซึ่งยากที่เจ้าหน้าที่ดับเพลิงจะเข้าถึงหรือไม่	√		
- ศูนย์ฯตั้งอยู่ในที่ปลอดภัย ไม่เปิดเผย แต่ไม่ลับตาจนไม่ทราบการเคลื่อนไหว เข้า-ออก	√		
● การเข้าถึง			
- การเข้าถึงศูนย์คอมพิวเตอร์ จำกัดเฉพาะพนักงานด้านปฏิบัติการและควรเข้าเขตบางเขตเฉพาะตามตารางเวลาทำงานเท่านั้น	√		
- มีการควบคุมพนักงานอื่นในการเข้าห้องคอมพิวเตอร์	√		
- มีการจัดเวร	√		
- มีระบบสัญญาณเตือนภัยและความปลอดภัยอื่นๆถ้าไม่มีคนประจำศูนย์	√		
- มีการใช้ระบบควบคุมประตูเข้า-ออก หรือใช้ระบบควบคุมด้วยการ์ด และอนุญาตเฉพาะบุคคลที่มีหน้าที่รับผิดชอบ	√		
● การผ่านเข้าออกมีการบันทึกลงนามและเวลา	√		
● การเก็บรักษาแผ่น Diskette และเทปข้อมูล			
- แผ่น Diskette และเทป เก็บในที่ที่ปลอดภัย โดยเฉพาะเก็บห่างจากสนามแม่เหล็ก	√		
- มีการสุ่มตรวจนับเป็นระยะๆ		√	
● การกำจัดวัสดุเชื้อไฟ มีข้อกำหนดว่า เฉพาะเครื่องใช้ที่จำเป็นเท่านั้นที่นำมาใช้ในห้องคอมพิวเตอร์ โดยต้องจำกัดจำนวนสิ่งของที่ติดไฟได้ง่าย และมีการห้ามนำอุปกรณ์ที่เป็นสื่อไฟ วัตถุระเบิดเข้าห้องคอมพิวเตอร์	√		
● มีระบบไฟฟ้าฉุกเฉินและระบบสำรองพลังงาน	√		

ตารางที่ 4.4 ผลการประเมินความเสี่ยงของระบบสารสนเทศของบริษัท (ต่อ)

รายละเอียดที่ประเมิน	มี	ไม่มี	คำอธิบาย
6.มีการควบคุมการป้องกันการเข้าถึงแฟ้มข้อมูลและโปรแกรมจากผู้ไม่ประสงค์ดี หรือการแก้ไขที่ไม่มีอำนาจ			
● การเข้าถึงข้อมูลและโปรแกรม			
- มีขั้นตอนการอนุญาตให้เข้าถึงข้อมูลได้และการอนุญาตและระดับสิทธเป็นไปตามหลักความจำเป็นในการใช้งาน	√		
- มีการจัดการกับ Password เช่น ต้องมีการเปลี่ยนอย่างสม่ำเสมอ		√	
- มีการควบคุมการเข้าถึงระบบและการฝ่าฝืน	√		
- มีการพิจารณาเข้ารหัส (Encrypt) ข้อมูลที่มีความสำคัญ		√	
● หากสามารถเข้าถึงระบบได้หลายวิธี มีการสอบทานการควบคุมการเข้าถึงทุกวิธีการนั้น		√	

จากตารางสามารถวิเคราะห์ผลการประเมินได้ดังนี้

1. เอกสารที่เกี่ยวข้องกับมาตรการป้องกันและแผนฉุกเฉินเพื่อไม่ให้เกิดผลเสียหายต่อศูนย์คอมพิวเตอร์โดยตรง ยังไม่มีการจัดทำดังนั้นในส่วนนี้ควรมีการปรับปรุงและควรระบุในแผนความปลอดภัยว่าต้องให้มีการจัดทำ
2. โครงสร้างองค์กรและการจัดสรรหน้าที่ของฝ่ายระบบสารสนเทศมีความชัดเจนและเหมาะสมเพียงพอแต่ควรมีการกำหนดหน่วยงานหรือกลุ่มบุคคลเพื่อดูแลด้านความปลอดภัยของระบบสารสนเทศดังต่อไปนี้

2.1 Information Security Officer ควรกำหนดให้มีหน้าที่ความรับผิดชอบดังนี้

- ดูแล ทบทวนและปรับปรุง นโยบายและขั้นตอนปฏิบัติทางด้านความปลอดภัยให้สามารถปกป้องทรัพย์สินขององค์กรได้อย่างมีประสิทธิภาพ
- เป็นตัวแทนของบริษัทในการดูแลเรื่องความปลอดภัยของสารสนเทศ
- ให้คำแนะนำในการจัดสรรหน้าที่ความรับผิดชอบที่เหมาะสมเกี่ยวกับงานด้าน IT
- สนับสนุนคนในบริษัทให้มีความตระหนักในด้านความปลอดภัยของสารสนเทศ

- เป็นทีมงานที่มีส่วนร่วมในการตัดสินใจเมื่อบริษัทมีการออกแบบ วางแผน จัดซื้อ หรือ ปรับปรุงเทคโนโลยีสารสนเทศ
- รับผิดชอบในด้านการพัฒนา จัดทำและปรับปรุงแก้ไขนโยบายทางด้านความปลอดภัยของสารสนเทศในบริษัท
- เป็นตัวกลางในการติดต่อในเรื่องที่เกี่ยวข้องกับความปลอดภัยของสารสนเทศ
- รายงานผู้บริหารของบริษัทเกี่ยวกับช่องโหว่ กิจกรรมทางด้านความปลอดภัยและความเสี่ยงที่เกิดขึ้นในบริษัท

2.2 Security Administrator เป็นตำแหน่งที่ขึ้นตรงกับ Information Security Officer และควรกำหนดให้มีหน้าที่ความรับผิดชอบดังนี้

- บริหารงานเพื่อสนับสนุนการติดตั้งระบบรักษาความปลอดภัย
- กำหนดวัตถุประสงค์สำหรบการพัฒนาระบบรักษาความปลอดภัย
- ปรึกษากับผู้เกี่ยวข้องในการจัดทำโปรแกรมในระดับต่างๆ เพื่อให้การประสานงานด้านความปลอดภัยของการจัดการข้อมูลเป็นไปด้วยดี
- สัมภาษณ์และประเมินผลการดำเนินการเกี่ยวกับเทคนิควิธีการ ความเข้าใจเกี่ยวกับวัตถุประสงค์ขององค์กร
- ตรวจจับการใช้งานและใช้ข้อมูลโดยไม่ได้รับอนุญาตและรายงานการตรวจสอบ
- จัดทำรายงานและสืบสวนการละเมิดฝ่าฝืนการรักษาความปลอดภัยและเหตุการณ์คุกคามต่างๆ
- ประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง เช่น ตำรวจ บริษัทประกันภัย
- จัดทำเอกสารเกี่ยวกับระบบการรักษาความปลอดภัยของบริษัท

2.3 ทีมงานปฏิบัติการฉุกเฉิน (Emergency Team) เป็นทีมงานพิเศษที่กำหนดขึ้นมาเพื่อปฏิบัติงานเฉพาะในกรณีที่เกิดเหตุฉุกเฉินกับระบบ โดยบุคลากรในทีมงานควรจะประกอบด้วยเจ้าหน้าที่จากส่วนต่างๆในฝ่ายเทคโนโลยีสารสนเทศ และควรกำหนดให้มีหน้าที่ความรับผิดชอบดังนี้

- ดำเนินการแก้ไขเหตุฉุกเฉินตามที่ได้รับแจ้งจากเจ้าหน้าที่ Helpdesk
- ประสานงานกับหน่วยงานอื่นๆที่เกี่ยวข้อง เช่น Vendor ในการดำเนินการแก้ไขเหตุฉุกเฉิน

3. การกำหนดวิธีปฏิบัติงานในศูนย์คอมพิวเตอร์ส่วนใหญ่มีการจัดทำไว้แล้ว ยกเว้นเรื่องการจัดเก็บโปรแกรม/ข้อมูล การทำลายแฟ้มข้อมูลและการ Backup ข้อมูลและโปรแกรม ซึ่งควรกำหนดให้มีการจัดทำให้ครบถ้วน

4. การควบคุมด้าน Network ควรมีการแก้ไขในเรื่องการตรวจสอบการติดตั้งอุปกรณ์จริงกับในแผนผัง การกำหนดสิทธิในการเข้าใช้งานตามหน้าที่รับผิดชอบและการตรวจหาจุดอ่อนในระบบสม่ำเสมอเพื่อหาทางป้องกัน
5. ความปลอดภัยโดยทั่วไปและมีการป้องกันไฟไหม้โดยพิจารณาเรื่องที่ตั้งและการเข้าถึงศูนย์คอมพิวเตอร์มีความเหมาะสมเพียงพอแล้ว
6. การควบคุมการป้องกันการเข้าถึงแฟ้มข้อมูลและโปรแกรมควรมีการแก้ไขในเรื่องการจัดการกับ Password เช่น ต้องมีการเปลี่ยนอย่างสม่ำเสมอ การพิจารณาเข้ารหัส (Encrypt) ข้อมูลที่มีความสำคัญและการสอบทานการควบคุมการเข้าถึงในกรณีที่สามารถเข้าถึงได้หลายวิธี

จากผลการประเมินค่าผลกระทบของระบบต่างๆและการประเมินความเสี่ยงข้างต้นจะเห็นว่าสามารถนำมาใช้เป็นแนวทางในการจัดทำแผนความปลอดภัยของบริษัทให้สอดคล้องและเหมาะสมกับผลการประเมินที่ได้ นอกจากนั้นก็ควรนำรายละเอียดในมาตรฐานสากล ISO 17799 ที่กล่าวถึงในบทที่ 4 ไปร่วมพิจารณาในการจัดทำแผนความปลอดภัยด้วย

4.2 แผนความปลอดภัย (ธนา หงษ์สุวรรณ. 2545)

โดยทั่วไป แผนความปลอดภัย จะหมายถึง สิ่งที่เขียนขึ้นเพื่อเป็นแนวปฏิบัติของคนในองค์กรเพื่อให้องค์กรนั้นมีความปลอดภัยจากความล้มเหลวของระบบคอมพิวเตอร์และเครือข่ายไม่ว่าความล้มเหลวนั้นจะมีสาเหตุจากภายในองค์กรเอง หรือภายนอกองค์กรก็ตาม แผนความปลอดภัยอาจเป็นเพียงกระดาษแผ่นเดียว อาจเป็นหนังสือเล่มหนึ่ง หรืออาจหลายเล่มก็ได้ขึ้นกับองค์กรนั้นจะจัดทำขึ้นมาอย่างไร

และเนื่องจากแผนความปลอดภัยเป็นแนวทางสำหรับทั้งองค์กรจึงมีผลถึงทุกคนในหน่วยงาน ดังนั้นในกฎข้อแรกของการบังคับใช้แผนความปลอดภัย คือต้องได้รับความเห็นชอบและต้องสื่อสารออกไปในนามของทีมผู้นำหรือผู้บริหารองค์กร ต้องได้รับการสนับสนุนอย่างเต็มที่ และจะต้องถือว่าเป็นส่วนหนึ่งของงาน

ผู้บริหารทุกคนจะต้องสื่อสารกับพนักงานให้เห็นว่าแผนความปลอดภัยมีความสำคัญอย่างไร เหตุใดจึงต้องกระทำ จะต้องสื่อสารให้ทุกคนรู้ว่าสิ่งใดควรทำและสิ่งใดไม่ควรทำ นอกจากนั้นควรจะมีบทบัญญัติด้วยว่าหากมีการละเมิดแผนความปลอดภัยแล้ว จะได้รับผลหรือบทลงโทษอย่างไร ซึ่งอาจมีตั้งแต่การตักเตือน พักงาน ไปจนถึงยกเลิกการว่าจ้าง เช่นเดียวกับแผนด้านอื่นๆขององค์กร เพื่อแสดงให้เห็นว่าองค์กรนี้ให้ความสำคัญกับแผนความปลอดภัยเท่าเทียมกับแผนหรือนโยบายด้านอื่น

ส่วนในตัวแผนเอง ควรจะระบุข้อห้าม ข้อปฏิบัติ รวมทั้งเหตุผลของการปฏิบัติในลักษณะดั่งกล่าวด้วย แผนที่ดีควรมีความชัดเจน ทำความเข้าใจได้ง่าย และสื่อสารถึงสิ่งที่องค์กรต้องการได้ เช่น แผนความปลอดภัยเกี่ยวกับ E-mail อาจบอกว่า " E-mail ถือเป็นทรัพย์สินของบริษัท และบริษัทมีสิทธิที่จะตรวจสอบ E-mail ดังนั้นพนักงานไม่ควรคาดหวังความเป็นส่วนตัวในระบบ E-mail ของบริษัท" แผนควรใช้เพื่อกำหนดทิศทางและให้ข้อมูล แต่ไม่จำเป็นต้องบอกถึงวิธีการควบคุมและบังคับใช้ เช่น อาจบอกว่า " การสื่อสารขององค์กรต้องไม่ถูกดักจับ" เพียงแค่นั้น เพราะในรายละเอียดจะไปถูกกล่าวถึงในมาตรฐาน (Standard) และแนวปฏิบัติ (Guidelines) แทน

แผนความปลอดภัยเป็นเรื่องที่ไม่ยากต่อการทำความเข้าใจและไม่ใช่เรื่องยากที่จะเขียนขึ้นมา แต่ยากสำหรับการปฏิบัติจริง เพราะเรื่องนี้เกี่ยวข้องผู้คนจำนวนมาก เช่นเดียวกับการออกกฎหรือระเบียบสักอย่างในองค์กรก็เป็นเรื่องที่ต้องระวังอยู่แล้ว เพราะจะมีผู้ไม่ตอบรับการเปลี่ยนแปลงนั้นมีอยู่ทั่วไป โดยเฉพาะหากการเปลี่ยนแปลงนั้นเข้ามาจำกัดอิสรภาพในการทำงาน ดังนั้นผู้บริหารต้องให้การสนับสนุนและเอาจริงเอาจัง จนทำให้คนในองค์กรรู้สึกว่าเป็นเรื่องสำคัญ และที่สำคัญยิ่งกว่า คือต้องอธิบายให้เข้าใจว่าแผนมิได้เกิดจากความมุ่งแก่อำนาจของผู้บังคับใช้ แต่เป็นไปเพื่อความปลอดภัยขององค์กร และเมื่อพนักงานทุกระดับเกิดความเข้าใจและให้ความร่วมมือ ก็จะส่งผลให้องค์กรประสบความสำเร็จ

4.3 แผนความปลอดภัยในด้านต่างๆ สำหรับบริษัท (ธนา หงษ์สุวรรณ. 2545)

สำหรับแนวทางในการสร้างแผนความปลอดภัยของบริษัท มีลำดับขั้นตอนการสร้างดังต่อไปนี้

1) กำหนดขอบเขตของแผน : เป็นการระบุว่าแผนจะใช้กว้างแค่ไหน แค่แผนกเดียว ฝ่ายเดียว หรือทั้งบริษัท หรือกำหนดเฉพาะฝ่ายคอมพิวเตอร์อย่างเดียวก็ได้ ซึ่งในรายงานฉบับนี้ ขอบเขตที่เหมาะสมสำหรับบริษัทจะครอบคลุมการใช้งานทุกหน่วยงานที่ตั้งอยู่ในส่วนกลางของบริษัท
2) สร้างการสนับสนุนจากผู้บริหาร : เพื่อขอความเห็นชอบจากผู้บริหารและออกเป็นข้อบังคับในการปฏิบัติ
3) วิเคราะห์ผลกระทบกับธุรกิจ : เพื่อเป็นการพิจารณาว่าแผนที่ออกมาจะช่วยปกป้องอะไรบ้าง ปกป้องจากอะไร หรือกล่าวง่ายๆก็คือ การตั้งคำถามว่าทำไปเพื่ออะไร
4) รวบรวมข้อมูลจากหน่วยงานต่างๆ : เพื่อให้เกิดการยอมรับในแผนและการเข้ามามีส่วนร่วมจากหน่วยงานอื่น
5) ทำการร่างแผน : เป็นการนำข้อมูลที่ได้มาร่างแผนให้สอดคล้องกับการใช้ระบบสารสนเทศในองค์กร ซึ่งในแผนแต่ละด้านที่จัดทำขึ้นควรมีรูปแบบของเอกสารที่เป็นมาตรฐานซึ่งควรจะ

ประกอบด้วย วัตถุประสงค์ ขอบเขตของการใช้แผน เนื้อหาของแผน หน้าที่ความรับผิดชอบของผู้ใช้ การบังคับใช้ และ ประวัติการแก้ไขเอกสาร

6) ตรวจสอบแก้ไขแผน : ให้ผู้เกี่ยวข้องร่วมกันตรวจสอบและให้ความเห็นเพิ่มเติม

7) ประกาศแผน : ขอความเห็นชอบจากผู้บริหาร แล้วประกาศให้พนักงานรับทราบตลอดจนชี้แจงและอธิบาย

8) ปรับปรุงเป็นระยะ : ทบทวนเนื้อหาของแผนให้เหมาะสมกับสถานการณ์เป็นระยะๆ

เมื่อพิจารณาจากการประเมินความเสี่ยงของระบบสารสนเทศในบริษัทและมาตรฐานความปลอดภัยของสารสนเทศ ISO 17799 จะเห็นว่าในส่วนของของแผนความปลอดภัยของบริษัทสามารถแบ่งออกได้เป็นหัวข้อหลักๆ ดังต่อไปนี้

1) **แผนด้านการใช้แผน** : แผนนี้จะเกี่ยวกับการใช้แผนเอง โดยจะเป็นแนวทางทั่วไป โดยควรมีการระบุอย่างชัดเจนว่าในการออกแผนมีขั้นตอนอย่างไร ใครที่เป็นคณะทำงานด้านแผนความปลอดภัยบ้าง กำหนดแนวทางในการเผยแพร่แผน ผู้บริหารตำแหน่งใดที่รับผิดชอบด้านแผน ซึ่งควรจะบอกถึงแนวทางในการตรวจสอบ สอบสวนและขั้นตอนการทำงานด้วย

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้ที่ต้องจัดทำร่างแผนความปลอดภัยในด้านต่างๆ และนำเสนอให้กับคณะทำงานด้านแผนความปลอดภัยและ Information Security Officer เพื่อทบทวนและอนุมัติ
- คณะทำงานด้านแผนความปลอดภัยประกอบด้วย ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายบริหารทรัพยากรบุคคล ผู้จัดการส่วนกฎหมาย และ มีประธานคณะทำงานเป็นกรรมการผู้จัดการใหญ่
- แผนจะถูกเผยแพร่ผ่านทางระบบอินทราเน็ตก่อนที่จะมีผลบังคับใช้ประมาณ 1 เดือน ซึ่งหลังจากวันที่มีผลบังคับใช้จะถือว่าพนักงานในทุกหน่วยงานจะต้องรับรู้ถึงแผนต่างๆเป็นอย่างดีแล้ว

2) **แผนด้านการเข้าถึงและการแปลงข้อมูล** : แผนนี้ควรจะต้องมีการจัดชั้นข้อมูลและแบ่งประเภทข้อมูลอย่างชัดเจนว่าข้อมูลใดเป็นความลับ ใครบ้างมีสิทธิหรือมีมุมมองในการเข้าถึงข้อมูลประเภทใด ระดับไหน ควรเขียนออกมาเป็นตาราง โดยด้านหนึ่งเป็นผู้ใช้หรือกลุ่มผู้ใช้ อีกด้านหนึ่งเป็นข้อมูล ควรมีการตรวจสอบด้วยว่าเป็นไปตามที่กำหนดหรือไม่ สำหรับข้อมูลสำคัญควรหาระบบตรวจสอบที่ระบุได้ว่าใครเข้ามาใช้ข้อมูลและใช้ในช่วงเวลาใด ขั้นตอนหรือวิธีการดำเนินการก่อนและหลังการแปลงข้อมูล

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- มีการกำหนดสิทธิการเข้าถึงแฟ้มข้อมูลและโปรแกรม พนักงานในแผนกต่างๆ จะสามารถเข้าใช้แฟ้มข้อมูล และโปรแกรมที่เกี่ยวข้องกับการทำงานของพนักงานเองเท่านั้น โดยสิทธิการใช้โปรแกรมและแฟ้มข้อมูลจะขึ้นอยู่กับตำแหน่ง และหน้าที่ที่เกี่ยวข้องกับแฟ้มข้อมูล พนักงานที่มีสิทธิใช้โปรแกรมและแฟ้มข้อมูล จะต้องมีส่วนรับผิดชอบในกรณีที่โปรแกรมหรือแฟ้มข้อมูลนั้นมีปัญหา ก่อให้เกิดความเสียหายในระบบงาน และพนักงานไม่ควรมอบหมายสิทธิการเข้าใช้ให้บุคคลอื่น ทั้งที่อยู่ในหน่วยงานและนอกหน่วยงาน
- ต้องไม่เข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล
- ห้ามทำการพิมพ์หรือ Copy Data ที่เป็นความลับ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลเท่านั้น
- ต้องเข้ารหัสข้อมูล (Data Encryption) ที่มีความสำคัญต่อการทำธุรกิจ เมื่อต้องการส่งข้อมูลผ่านระบบอินเทอร์เน็ต
- System Administrator ต้องไม่มีสิทธิเข้าถึงฐานข้อมูล และ Database Administrator ต้องจัดทำบัญชีรายชื่อผู้มีสิทธิ Read, Write, Copy ฐานข้อมูล และดำเนินการตรวจสอบความทันสมัยอย่างสม่ำเสมอ
- มีการสอบทานข้อมูลก่อนและหลังการแปลงข้อมูล โดยผู้ที่เกี่ยวข้องและรับผิดชอบต้องแจ้งให้ฝ่ายที่ใช้ข้อมูลทราบทั้งข้อมูลที่ก่อนเปลี่ยนแปลง และข้อมูลที่เกิดขึ้นหลังเปลี่ยนแปลง โดยมีรายละเอียดการเปลี่ยนแปลงแจ้งให้ผู้ใช้ทราบด้วย ตลอดจนมีการสำรองข้อมูลที่จะแปลงก่อนทำการแปลง เพื่อเป็นการลดความผิดพลาดเนื่องจากความผิดปกติ จากกระบวนการทำงานที่อาจเกิดขึ้น
- ต้องมีการจัดทำรายงานการแปลงข้อมูลที่สำคัญทุกครั้งที่มีการเปลี่ยนแปลงข้อมูล

3) แผนด้านรหัสผ่าน : แผนนี้จะกล่าวถึงการตั้งรหัสผ่าน ว่าต้องยาวเท่าไร และไม่ควรตั้งอย่างไร เช่น ชื่อที่เกี่ยวข้อง คำในพจนานุกรม รหัสผ่านแบบไหนที่ควรตั้ง อายุของรหัสผ่านนานเท่าใด รหัสผ่านของแต่ละคนซ้ำกันได้หรือไม่ หากไม่ใช้งานนานเท่าไร รหัสผ่านจะใช้ไม่ได้ หรือในกรณีที่มีการเปลี่ยนแปลงสถานะของผู้ใช้ จะต้องแจ้งผู้ดูแลให้ระงับ User ID และ Password ของผู้นั้นทันที และควรจะมีแผนสำหรับผู้ใช้แต่ละกลุ่มเข้มงวดไม่เท่ากัน ตามสิทธิการเข้าถึง ถ้ามีสิทธิมากก็ควรจะเข้มงวดมากกว่า นอกจากนั้นอาจกำหนดให้รหัสผ่านที่ใช้ในองค์กรกับภายนอกองค์กรต้องไม่เหมือนกัน เพราะหากรหัสผ่านถูกดักจับจากนอกองค์กร ก็จะไม่กระทบในองค์กร เป็นต้น

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- รหัสผ่าน (Password) ให้ถือเป็นความลับเฉพาะตัว ห้ามมิให้เผยแพร่แก่บุคคลอื่นใด ถ้าเกิดความเสียหายในระบบที่เกิดจากการที่พนักงานให้รหัสผ่านแก่บุคคลอื่น พนักงานเจ้าของรหัสผ่านต้องรับผิดชอบ ความเสียหายที่เกิดขึ้นนั้น
- ไม่ควรใช้ชื่อเฉพาะตัวหรือชื่อคำใดคำหนึ่งมาใช้ แม้จะเป็นส่วนหนึ่งของชื่อก็ตาม
- ไม่ควรใช้ข้อมูลส่วนบุคคลมาเป็นรหัสผ่าน เช่น เลขประจำตัว บัตร ATM เบอร์โทรศัพท์ วัน เดือนปีเกิด
- ไม่ควรใช้ชื่อ login name หรือแม้แต่การสลับตัวอักษรกันไปมาจากชื่อนั้น
- ไม่ควรใช้คำที่มีในพจนานุกรมเป็นรหัสผ่าน
- รหัสผ่านควรมีความยาวไม่น้อยกว่า 7 ตัวอักษร
- ไม่ควรใช้ตัวอักษรหรือตัวเลขที่ซ้ำกันหลายๆ ตัว เช่น aaa9999
- รหัสผ่านที่ดีควรมี ตัวอักษร ตัวเลข และอักขระพิเศษปนอยู่ เช่น ra2n9es*
- ใช้รหัสผ่านที่คุณสามารถจำได้ง่ายและพิมพ์ได้อย่างรวดเร็ว เพื่อหลีกเลี่ยงจากการแอบจำของผู้ที่อยู่ใกล้เคียง
- ไม่ควรมีการเขียนรหัสผ่านไว้ไม่ว่าที่ใดก็ตาม หรือนำรหัสผ่านไปใช้ร่วมกับผู้อื่น
- ควรเปลี่ยนรหัสผ่านเป็นระยะๆ อย่างน้อยประมาณ 3 เดือนต่อ 1 ครั้ง
- ต้องใช้รหัสผ่านที่เป็นของตนเองในการแสดงตนเข้าใช้งาน หรือปฏิบัติงานในระบบข้อมูลตามสิทธิที่ได้รับเท่านั้น
- พนักงานที่ได้รับรหัสผ่านในครั้งแรกต้องเปลี่ยนรหัสผ่านใหม่ทันทีให้เป็นความลับเฉพาะตัว และต้องทำการเปลี่ยนรหัสผ่านใหม่ทันทีหากรหัสผ่านถูกเปิดเผย

4) **แผนการใช้งานอินเตอร์เน็ตและอินทราเน็ต** : แผนนี้จะครอบคลุมถึงการอนุญาตและไม่อนุญาตให้ใช้งานอะไรบ้าง(เช่น อาจให้ใช้ ICQ หรือ MSN แต่ไม่ให้ใช้เว็บบางแห่ง) ด้วยการระบุลงไปตามประเภทการใช้งาน เช่น E-mail, FTP,เว็บและการดาวน์โหลดไฟล์

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- พนักงานต้องไม่ใช้อินเตอร์เน็ตและอินทราเน็ตในเครือข่ายเพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม
- พนักงานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัทได้
- บริษัทสงวนสิทธิในการตรวจสอบการใช้งานอินเตอร์เน็ต โดยไม่จำเป็นต้องได้รับการยินยอมจากผู้ใช้

- หน่วยงานใดที่มีความจำเป็นต้องติดตั้งอินเทอร์เน็ตซอร์ฟเวอร์ (Internet Server) เพื่อใช้งานต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อนดำเนินการ

5) **แผนความปลอดภัยของเครือข่าย (Network Security)** : แผนนี้จะเกี่ยวข้องกับองค์ประกอบต่างๆในเครือข่าย เช่น อาจกำหนดว่าการเข้าถึง Server จะต้องกระทำผ่านไฟร์วอลล์เท่านั้น ติดตั้งอยู่ในเครือข่ายทุกส่วน หรือต้องมีการสุ่มจับการใช้งาน ต้องมีการสุ่มจับการใช้งาน ต้องมีการทดสอบกฎของ Firewall โดยใครบ้าง ต้องมีการตรวจสอบ(Audit) ที่ใด แค่ไหน และอย่างไร

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- ตั้งกฎของไฟร์วอลล์ให้สอดคล้องและเหมาะสมกับการใช้งานอินเตอร์เน็ตของบริษัทและมีการทบทวนกฎของไฟร์วอลล์อยู่เสมอ
- มีการทดสอบกฎของไฟร์วอลล์อยู่อย่างสม่ำเสมอโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ

6) **แผนด้านการใช้งานระยะไกล (Remote Access)** : แผนนี้ควรบอกถึงขั้นตอนการอนุญาตให้ใช้ ใครบ้างที่มีสิทธิใช้งาน ถ้าใช้งานต้องใช้งานโดยวิธีไหน เช่น อาจให้ผู้บริหารตั้งแต่ระดับกลางขึ้นไปหรือหน่วยงานในต่างจังหวัดใช้งานโดยการเชื่อมต่อผ่านโมเด็ม และเรื่องอื่นๆที่เกี่ยวข้อง

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- มีการควบคุมวิธีการเข้าถึงข้อมูล (Data Access) ของผู้ใช้ระบบ Online และกรณีแก้ไขข้อมูลสำหรับระบบงานที่สำคัญให้กำหนด Terminal บางเครื่องที่สามารถใช้แก้ไขข้อมูลได้เท่านั้น และการขอใช้ Terminal นั้นจะต้องมีการควบคุมดูแลอย่างใกล้ชิด โดยผู้เข้าใช้จะต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อน
- การเชื่อมต่อเข้าสู่เครือข่ายคอมพิวเตอร์ของบริษัทผ่าน Remote Access Server จะสามารถกระทำได้เฉพาะพนักงานตามรายชื่อที่ได้รับอนุญาตเท่านั้น

7) **แผนทางด้านเครื่อง Client** : แผนนี้ใช้สำหรับให้ผู้ใช้ถือเป็นแนวทางปฏิบัติ โดยส่วนใหญ่ก็จะเป็นการปฏิบัติตัวของผู้ใช้ในกรณีต่างๆ เช่น เมื่อไม่อยู่ที่โต๊ะทำงานควรจะ Log Out ออกจากระบบ หรืออาจใช้วิธีล็อคจอภาพ การป้องกันไวรัสควรทำอย่างไร ซึ่งอาจรวมถึงการอบรมผู้ใช้ด้วย นอกจากนั้นควรกล่าวถึงการนำเอาโปรแกรมอื่นมาใช่หรือมาติดตั้งว่าโปรแกรมใดอนุญาตหรือไม่อนุญาต เป็นต้น

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- พนักงานต้องทำการ Logout ออกจากระบบคอมพิวเตอร์ทันทีเมื่อเลิกใช้งาน หรือหากไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที ให้ใช้ Screen Saver ควบคุมหน้าจอคอมพิวเตอร์ด้วยรหัสผ่าน
- พนักงานทุกคนควรได้รับการอบรมให้มีความรู้และความเข้าใจที่ถูกต้องในการใช้งานระบบเครือข่ายของบริษัท
- เครื่องคอมพิวเตอร์พนักงานทุกเครื่องต้องมีการติดตั้งโปรแกรมป้องกันไวรัสตามมาตรฐานของบริษัทและมีการ Update ข้อมูลไวรัสอย่างสม่ำเสมอ
- พนักงานต้องใช้ Software ตามมาตรฐานที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดเท่านั้น กรณีที่นำ Software นอกเหนือจากมาตรฐานมาใช้ พนักงานต้องรับผิดชอบในผลเสียที่เกิดขึ้น
- หน่วยงานใดที่มีความจำเป็นต้องใช้ Software นอกเหนือจากฝ่ายเทคโนโลยีสารสนเทศกำหนด ให้ดำเนินการขอความเห็นจากผู้รับผิดชอบในฝ่ายเทคโนโลยีสารสนเทศ ก่อนนำมาใช้

8) **แผนทางด้าน Server** : แผนนี้จะกล่าวถึงแนวทางของการดูแล Server เช่น สเปกของ Server ที่ใช้งานจะต้องมีความมั่นคงเพียงใด เช่น อาจกำหนดว่า Server สำหรับเก็บข้อมูลต้องเป็นแบบ Raid-5 ต้องการการสำรองข้อมูลแบบไหน อย่างไร ต้องการการ Update หรือ Patch อะไรบ้าง บ่อยแค่ไหน

ในส่วนของเนื้อหาของแผนที่ได้กำหนดขึ้นมีรายละเอียดดังต่อไปนี้

- Harddisk ของ Server จะต้องมีระบบสำรองข้อมูลโดยต้องเป็น Harddisk ชนิด Raid 5
- ต้องกำหนดให้มีการทำ Network Segmentation เพื่อให้เกิด Server Security Zone เช่น การแบ่ง Segment ที่เป็น External Public Services Internal Non Critical Services และ Internal Critical Services ออกจากกัน และจัดให้มีการตรวจจับบุกรุกเข้าสู่ระบบที่เป็น Critical Application อย่างสม่ำเสมอ
- ต้องมีบันทึกการ Hardening หรือ Configuration Setup ของอุปกรณ์ Server ทุกครั้งที่ติดตั้ง Critical Application หรือเปลี่ยนแปลง
- มีการ Update Service Patch อย่างสม่ำเสมอและต้องมีบันทึกการติดตั้ง Service Patch ทุกครั้ง
- System Administrator ต้องไม่ใช้ Default Username / Default Password และไม่ตั้ง Username และ Password ที่ง่ายต่อการคาดเดา
- ต้องไม่เปิดเผย OS Version, Service Patch Version ให้กับบุคคลที่ไม่เกี่ยวข้อง

9) **แผนปฏิบัติการฉุกเฉิน** : แผนนี้จะกล่าวถึงแนวทางปฏิบัติในกรณีเกิดเหตุฉุกเฉินกับฝ่ายเทคโนโลยีสารสนเทศซึ่งมีหลักเกณฑ์และแนวทางจัดทำดังนี้

1. การจัดทำแผนฉุกเฉินเป็นหน้าที่ของคณะกรรมการแผนฉุกเฉิน

2. ควรจัดทำสำเนาของแผนและเอกสารประกอบแผนไว้ต่างสถานที่ 1 ชุด เพื่อให้มั่นใจว่า หากเกิดความเสียหายต่อศูนย์คอมพิวเตอร์เช่นไฟไหม้ น้ำท่วม ก็ยังคงมีแผนกู้ระบบที่สามารถนำมาใช้ได้ทันที
3. แผนฉุกเฉิน ประกอบไปด้วย

- แผนปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน กำหนดแนวทางการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน หรือภัยพิบัติที่มิอาจหลีกเลี่ยงได้ เพื่อป้องกัน และบรรเทาความเสียหายให้เกิดขึ้นน้อยที่สุด
- แผนปฏิบัติงานเพื่อกู้ระบบให้กลับคืนสู่สภาพปกติ (Recovery Plan) กำหนดแนวทางการแก้ไขระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารที่ประสบภัย ให้กลับคืนสู่สภาพปกติโดยเร็วที่สุด
- แผนปฏิบัติงานระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสาร กำหนดแนวทางการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารสำรองทดแทนเมื่อประสบภัย เพื่อให้สามารถดำเนินธุรกิจตลอดจนให้บริการแก่ลูกค้าได้อย่างต่อเนื่อง

จากแนวทางข้างต้น จึงได้กำหนดเป็นขั้นตอนการปฏิบัติการแผนฉุกเฉิน ในกรณีเกิดเหตุการณ์ฉุกเฉินหรือเหตุสุดวิสัยขึ้นกับระบบคอมพิวเตอร์ ให้ผู้เกี่ยวข้องปฏิบัติดังนี้

1. เมื่อรับทราบว่ามีเหตุฉุกเฉินเกิดขึ้น เจ้าหน้าที่ Help Desk จะประสานงานกับองค์กรหรือเจ้าหน้าที่ที่เกี่ยวข้อง เช่น เจ้าหน้าที่ประจำ Emergency Team และ Vendor ให้มาร่วมดำเนินการแก้ไข และแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศให้รับทราบ
2. ในกรณีที่ต้องใช้แผนฉุกเฉิน ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้มีอำนาจสั่งการ
3. ดำเนินการปฏิบัติตามวิธีพร้อมรับสถานการณ์ฉุกเฉินสำหรับเหตุการณ์ฉุกเฉินหรือเหตุสุดวิสัยต่างๆ ซึ่งในวิธีดังกล่าวจะระบุถึงเกณฑ์การตัดสินของการเริ่มต้นใช้แผน กระบวนการในการปฏิบัติงานตามแผน รายละเอียดของ Workflow และรายชื่อผู้รับผิดชอบพร้อมเบอร์โทรศัพท์
4. ดำเนินการแก้ไขตาม Workflow สำหรับอาการเสียหรือเหตุสุดวิสัยในแต่ละกรณี โดยในแต่ละขั้นตอนของ Workflow จะระบุถึงผู้รับผิดชอบและเบอร์โทรศัพท์
5. เมื่อระบบกลับคืนสู่สภาวะปกติ เจ้าหน้าที่ Help Desk จะต้องรายงานผลต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

ในส่วนของกิจกรรมของแผนปฏิบัติงานฉุกเฉิน ต้องครอบคลุมถึงสิ่งต่างๆดังต่อไปนี้

1. วิธีการและขั้นตอนของแต่ละกิจกรรม
2. อำนาจหน้าที่ และผู้รับผิดชอบของแต่ละขั้นตอน
3. ความสำคัญของทรัพยากรและวิธีการรักษาทรัพยากรที่จะต้องรักษาไว้ตามลำดับ คือ

- บุคลากร
- แฟ้มข้อมูลและโปรแกรม

- เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารข้อมูล

4. การเก็บสำรองภายนอกสถานที่ (Off Site Backup) ซึ่งประกอบด้วย

- Data File และ Database
- เอกสารระบบงาน (Document)
- Production Software และ Configuration File

5. รายชื่อบุคลากร เพื่อใช้ติดตามบุคคลที่เกี่ยวข้อง
6. การทดสอบแผนปฏิบัติการฉุกเฉินและปรับปรุงแผนให้สามารถใช้งานได้ตลอดเวลา

นอกจากแผนความปลอดภัยในแต่ละด้านแล้ว ยังมีเอกสารที่เกี่ยวข้องอีก 2 ประเภท คือ มาตรฐานและแนวปฏิบัติ ซึ่งเป็นเอกสารลำดับรองลงมาต่อจากแผน โดยที่

มาตรฐาน (Standard) จะทำหน้าที่ต่อจากแผนความปลอดภัย โดยทำหน้าที่กำหนดถึงระดับของเทคโนโลยีที่องค์กรนั้นใช้ในการบังคับนโยบาย เช่น"ทุกการสื่อสารในองค์กร จะต้องได้รับการรหัสด้วยเทคโนโลยี 3DES" หรือบอกระดับของขั้นตอนหรือกระบวนการว่าแค่ไหนถึงจะถือว่าเพียงพอ เช่น"หากผู้ใช้ป้อนรหัสผ่านผิดมากกว่า 3 ครั้ง บัญชีของผู้ใช้นั้นจะต้องถูกยกเลิกเป็นเวลา 3 ชม." มาตรฐานจะบอกถึงตำแหน่งหรือจุดที่จะต้องได้รับการตรวจสอบ จำนวนครั้ง และรายละเอียดของการตรวจสอบ เช่น "ต้องมีการรายงานผู้ที่หมุนโมเด็มเข้ามาใช้งานบริษัทหลัง 17.00 น.ทุกวัน" เป็นต้น ซึ่งจะเห็นได้ว่ามาตรฐานจะบอกถึงแต่วิธีการและระดับของวิธีการเท่านั้น ไม่ได้บอกถึงว่าบังคับอะไร และเหตุผลของการบังคับคืออะไร

สำหรับแนวปฏิบัติ (Guidelines) มีจุดมุ่งหมายเพื่อให้องค์กร แผนกหรือแต่ละบุคคล เข้าใจถึงวิธีปฏิบัติ อาจเปรียบได้กับคู่มือแนะนำการทำงานต่างๆที่จะไม่ขัดแย้งกับแผน เช่น วิธีการใช้ E-mail ให้ปลอดภัย หรือการใช้งานเครือข่ายแบบมีการเข้ารหัส ซึ่งเราสามารถนำแนวปฏิบัตินี้ไปใช้เปิดอบรมบุคลากรเพื่อเป็นการเผยแพร่แผนความปลอดภัยได้อีกด้วย

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

การควบคุมและรักษาความปลอดภัยของระบบคอมพิวเตอร์นั้นจะต้องอยู่บนพื้นฐานของความไม่ประมาท และต้องทำเป็นประจำอย่างสม่ำเสมอ เนื่องมาจากการควบคุมความปลอดภัยไม่อาจจะสามารถป้องกันผู้บุกรุกได้ 100 เปอร์เซ็นต์ แต่เพียงเพื่อชะลอให้ผู้บุกรุกเข้าถึงระบบได้ช้าลงเท่านั้น ฉะนั้นผู้ที่เกี่ยวข้องและผู้ที่ดูแลจะต้องรู้และคำนึงถึงอยู่เสมอเกี่ยวกับจุดอ่อนและข้อบกพร่องของระบบทั้งหมดเป็นอย่างดี โดยมีการเตรียมพร้อมทั้งในด้านของแผนรองรับ ขั้นตอนการปฏิบัติที่ชัดเจน มีการตรวจสอบที่ดี และมีแผนความปลอดภัยที่ชัดเจนและรัดกุม อย่างไรก็ตาม การป้องกันภัยที่ดีที่สุด คือความไม่ประมาทและการระมัดระวังอยู่เสมอ

ในรายงานฉบับนี้ได้ยกตัวอย่างจากบริษัทธุรกิจเอกชนซึ่งมีระบบสารสนเทศและระบบความปลอดภัยใช้งานในปัจจุบัน แต่ไม่ได้มีการจัดทำแผนความปลอดภัยเอาไว้ในองค์กรให้กับพนักงานได้รับรู้และตระหนักถึงความสำคัญ และได้กล่าวถึงวิธีการประเมินความเสี่ยงของระบบสารสนเทศ ผลการประเมินและได้นำเสนอถึงแผนความปลอดภัยของระบบสารสนเทศโดยได้อธิบายถึงความหมาย ความสำคัญ มาตรฐานสากลด้านความปลอดภัยของสารสนเทศ ISO17799 และแนวทางการสร้างแผน พร้อมได้นำเสนอถึงแผนหลักในด้านต่างๆที่ควรมีการจัดทำขึ้น เช่น ด้านการใช้นโยบาย การเข้าถึงข้อมูลด้านรหัสผ่าน การใช้งานอินเตอร์เน็ตและอินทราเน็ต ความปลอดภัยของเครือข่าย ด้านการใช้งานระยะไกล ด้านเครื่อง Client ด้าน Server และแผนปฏิบัติการฉุกเฉิน พร้อมทั้งได้กล่าวถึงเอกสารที่เกี่ยวข้องอีก 2 ประเภทคือ มาตรฐาน (Standard) และแนวปฏิบัติ (Guidelines)

5.2 ข้อเสนอแนะ

ในการประเมินความเสี่ยงและวิเคราะห์ผลกระทบที่เกิดกับระบบสารสนเทศในแต่ละองค์กรอาจจะมีขั้นตอนโดยรวมที่คล้ายกัน แต่ในรายละเอียดที่จะทำการประเมินแล้วแต่ละองค์กรจะไม่เหมือนกัน เนื่องจากแต่ละองค์กรมีลักษณะการดำเนินและเป้าหมายทางธุรกิจที่แตกต่างกัน ซึ่งส่งผลให้การให้ความสำคัญกับระบบต่างๆ ผลกระทบในด้านต่างๆ ตลอดจนปัจจัยต่างๆที่ส่งผลกระทบต่อระบบไม่เท่ากัน ดังนั้นในการประเมินความเสี่ยง ทีมงานที่ได้รับมอบหมายในการ

ประเมินควรจะพิจารณาถึงลักษณะของธุรกิจ ลักษณะและพฤติกรรมการใช้ระบบสารสนเทศในองค์กรของตนเอง และนำมากำหนดรายละเอียด วิธีการและรูปแบบการประเมินให้เหมาะสม เพื่อให้ได้ผลการประเมินที่สอดคล้องและเหมาะสมกับองค์กรมากที่สุด

บรรณานุกรม

ธนา หงษ์สุวรรณ. 2545. "นโยบายความปลอดภัย เรื่องยากที่ทำได้ในองค์กรของคุณ". **PC Magazine Security Turn-Pro Guide**: 28-32.

ธีรชัย เดชานันทศิลป์. 2545. **เรื่องน่ารู้ของการรักษาความปลอดภัยในเครือข่าย**. [Online]. Available: http://pantip.inet.co.th/tech/newscols/column/column2002/01-03-02/ns/ns.html.

ประชา ตระการศิลป์. 2543. **การพัฒนาระบบงานไคลเอนต์/เซิร์ฟเวอร์**. พิมพ์ครั้งที่ 2. กรุงเทพฯ: ศิลป์สยามบรรจุภัณฑ์และการพิมพ์.

ฟ้าใหม่ สรรค์ใจ. 2545. "ความปลอดภัยของข้อมูล สิ่งที่คุณจำเป็นต้องจัดการ". **PC Magazine**. 8(3): 187-191.

The International Organization for Standardization and The International Electrotechnical Commission. 2000. **ISO/IEC 17799 Information Security-Code of Practice for Information Security Management**. Geneva: ISO/IEC.

United States General Accounting Office. 1999. **Information Security Risk Assessment Practice of Leading Organization**. Washington , DC: GAO.

ประวัติผู้เขียน

ชื่อ-สกุล นายวิฑูรย์ ปึงไพบูลย์

วัน เดือน ปี เกิด 1 กรกฎาคม พ.ศ. 2517

สถานที่เกิด กรุงเทพฯ

ประวัติการศึกษา ประถมศึกษา โรงเรียนซานตาครูสศึกษา
มัธยมศึกษา โรงเรียนทวีธาภิเศก
ปริญญาตรี วิศวกรรมศาสตรบัณฑิต(วิศวกรรมไฟฟ้า)
มหาวิทยาลัยธรรมศาสตร์

ประวัติการทำงาน ปี 2539- 2545 บริษัท ไทยเทเลโฟนแอนด์เทเลคอมมิวนิเคชั่น จำกัด (มหาชน)
ปี 2545- ปัจจุบัน บริษัท ทีเอ ออเร้นจ์ จำกัด