บทที่ 2

กรอบแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดสำหรับการจัดการด้านความปลอดภัยของข้อมูล

เนื่องจากในปัจจุบันมาตรฐานหรือเฟรมเวิร์ค สำหรับการจัดการด้านความปลอดภัยของข้อมูลมีหลากหลาย ขึ้นอยู่กับการนำไปใช้ของแต่ละองค์กร ("Framework" หมายถึง ขั้นตอนหรือวิธีการที่องค์กรสามารถนำมาประยุกต์ใช้ตามหลักการมาตรฐานสากล) เช่น COSO Framework เป็นมาตรฐานสำหรับการควบคุมภายใน หรือ "Internal Control" หรือ “Corporate Governance” , CobiT Framework ก็จะหมายถึง "IT Governance" ที่มีการกำหนดขอบเขตแคบในเรื่องส่วนของระบบสารสนเทศ และถ้ากล่าวถึงมาตรฐานสากลอย่าง ISO27001/17799 หมายถึง ISMS หรือ Information Security Management System ซึ่งเป็นมาตรฐานที่นำมาประกอบการค้นคว้า เป็นมาตรฐานที่เกี่ยวข้องกับการรักษาความปลอดภัยทางด้านข้อมูลในภาพรวมของทั้งองค์กร เพื่อนำมาประยุกต์ใช้กับองค์กรในกรณีศึกษา

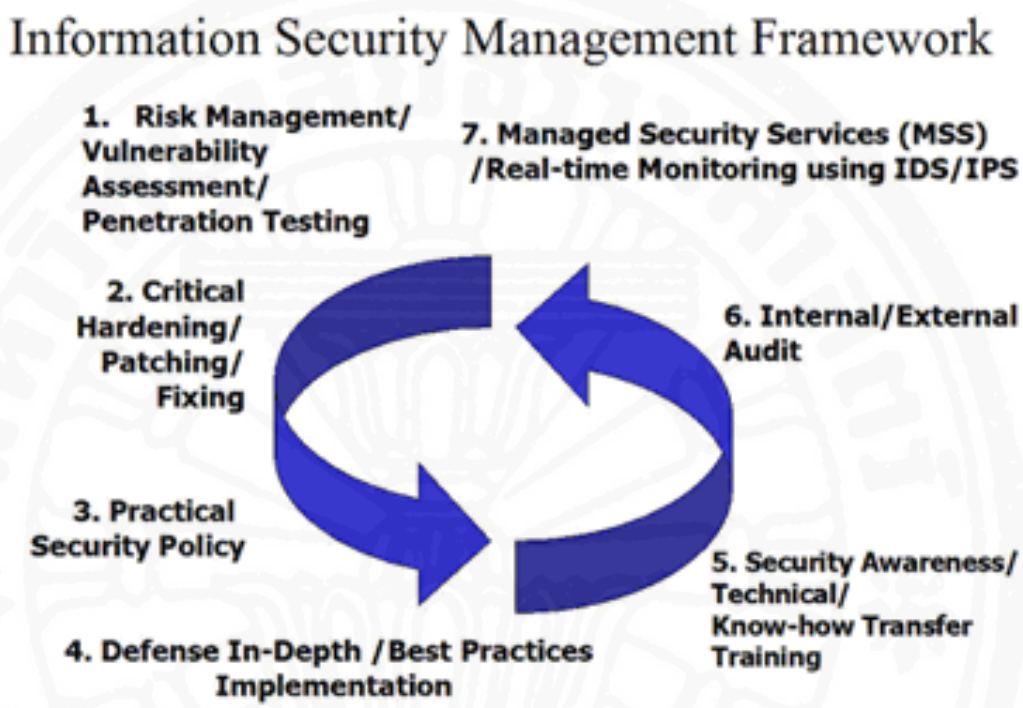
2.1.1 Information Security Management Framework (ISMF)

มาตรฐาน ISMF 7 (Information Security Management Framework) เป็นมาตรฐานสำหรับการตรวจสอบและการประเมินความปลอดภัยระบบสารสนเทศที่พัฒนาโดยนักวิชาการคนไทย โดยSMF เป็นการนำเอาหลักการด้าน Information Security Policy ของมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO17799 ตลอดจน มาตรฐาน Cobit ของ ISACA (www.isaca.org) และ CBK (Common Body of Knowledge) ของ ISC2 (www.isc2.org) มาประยุกต์ใช้เพื่อให้ได้ประโยชน์สูงสุด และสามารถนำมาปฏิบัติได้จริงในสภาวะแวดล้อมปัจจุบัน

จุดประสงค์เพื่อให้เป็นแนวทางในการบริหารจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพให้ทันกับสถานการณ์ปัจจุบัน เน้นในการแก้ปัญหาด้านเทคโนโลยีและสารสนเทศโดยมองถึงปัญหาทางธุรกิจมากขึ้นมีทั้งหมด 7 ขั้นตอนตาม รูปภาพที่ 2.1

ภาพที่ 2.1

7 ขั้นตอน ของมาตรฐาน ISMF 7 (Information Security Management Framework)



โดยทั้ง 7 ขั้นตอนอาศัยหลักของการพัฒนาอย่างต่อเนื่อง (Continuous Improvement) ในการบริหารคุณภาพ (Quality Management) ซึ่งประกอบเป็น 4 แนวความคิดหลัก ประกอบด้วย 1. วางแผน(Plan) 2. ปฏิบัติ(Do) 3. ตรวจสอบ(Check) และ 4. แก้ไข(Act) แต่อย่างไรก็ตามการปรับแนวความคิดด้านการพัฒนาอย่างต่อเนื่องนั้นยังไม่สามารถนำมาใช้ในทางการรักษาความปลอดภัยของข้อมูลได้โดยตรง เนื่องจากแนวคิดด้านการรักษาความปลอดภัยของข้อมูลนั้นไม่ใช่การลดช่องโหว่ลงให้เท่ากับศูนย์ (zero risk) ทั้งนี้เนื่องจากการกระทำกล่าวนั้นอาจทำได้หากแต่ต้องใช้ต้นทุนที่สูงมากจนไม่คุ้มค่า และอาจขัดขวางต่อการทำธุรกิจของบริษัทอีกด้วย ดังนั้นการจัดการด้านรักษาความปลอดภัยของข้อมูลนั้นจึงควรตั้งอยู่บนแนวคิดด้าน การบริหารความเสี่ยง(Risk Management) โดยคำนึงถึงความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Tolerance และ Risk Acceptance)เป็นหลัก เพื่อรับมือกับความเสี่ยงหรือความไม่ปลอดภัยของระบบที่ไม่ใช่แค่การทำเพียงแค่ซื้ออุปกรณ์เพิ่มและป้องกันระบบเท่านั้น

2.1.2 ISO27001/17799:2005

เป็นมาตรฐานเกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ได้รับการพัฒนามาจาก Information Security Management standard 'BS 7799 ออกโดย British Standard Institute (BSI): ซึ่งมาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization) ที่ถูกกำหนดเพื่อเป็นแนวทางการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยมีการกำหนดแนวทางสำหรับองค์กรในด้านการปฏิบัติงาน, การจัดการเพื่อให้เกิดประสิทธิภาพ การพัฒนามาตรฐานความปลอดภัย เพื่อการสร้างความมั่นใจในการเชื่อมโยงระหว่างองค์กร เนื่องจากข้อมูลของแต่องค์กรถือเป็นสินทรัพย์ที่มีความสำคัญ ดังนั้นการรักษาความปลอดภัยของข้อมูล, การวิเคราะห์และการบริหารความเสี่ยงที่อาจเกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพและหากกล่าวถึงความปลอดภัยข้อมูล จะต้องประกอบด้วย 3 องค์ประกอบ ดังต่อไปนี้

- Confidentiality คือ สิทธิ์ในการเข้าถึงข้อมูลต่างๆ ในระบบงาน โดยผู้ที่จะสามารถเข้าถึงข้อมูลในระบบนั้นได้ จะต้องได้รับการกำหนดสิทธิ์ในการเข้าใช้ หรือได้รับการอนุญาตก่อน
- Integrity คือ ข้อมูลต่าง ๆ ในระบบจะต้องมีความถูกต้อง มีการกำหนดมาตรการหรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันการบิดเบือนหรือผิดพลาดของข้อมูล
- Availability คือ ผู้มีสิทธิหรือได้รับอนุญาตในการเข้าถึงข้อมูลจะสามารถเข้าถึงข้อมูลเหล่านั้นได้ตามต้องการโดยผ่านช่องทางที่องค์กรกำหนด

2.1.2.1 มาตรฐาน ISO27001/17799

สำหรับการจัดการเพื่อรักษาความปลอดภัยของข้อมูล ประกอบไปด้วย

1. นโยบายความมั่นคงปลอดภัย (Security policy)

เป็นการกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยการสร้างนโยบายขององค์กรที่เหมาะสมและมีการเปลี่ยนแปลงให้ทันสมัยเสมอ

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

เป็นการบริหารจัดการความปลอดภัยของข้อมูลทั้งภายในและภายนอกองค์กร เพื่อควบคุมการดำเนินงานให้เป็นไปตามขั้นตอนที่ถูกต้องและมีประสิทธิภาพ

3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

เป็นการควบคุมและการจำแนกสินทรัพย์ขององค์กร ช่วยในการกำหนดระดับการป้องกันความเสียหายที่อาจเกิดขึ้นโดยคำนึงถึงลักษณะและ ความสำคัญ รวมถึงความจำเป็นในการใช้งาน

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

เป็นการกำหนดมาตรการเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดของมนุษย์ ว่าด้วยเรื่องการสร้างความมั่นคงปลอดภัยทั้งก่อนการจ้างงาน ในระหว่างการจ้างงานและเมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

ความปลอดภัยเกี่ยวกับสถานที่และสภาพแวดล้อม เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกที่ไม่ได้รับอนุญาต รวมไปถึงป้องกันความเสียหายและการแทรกแซงข้อมูลต่างๆที่อาจเกิดขึ้น

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

การบริหารจัดการด้านการปฏิบัติงานและการติดต่อสื่อสาร เป็นการกำหนดแนวทางในการปฏิบัติงานและเพิ่มความปลอดภัยของอุปกรณ์ประมวลผลข้อมูล เพื่อลดความผิดพลาดของระบบรวมทั้งการจัดการกับเหตุการณ์ที่เกิดขึ้น กรณีเกิดปัญหา และมีการวิเคราะห์เพื่อหาสาเหตุของปัญหา วางแผนและกำหนดแนวทางแก้ไขเพื่อป้องกันไม่ให้เกิดเหตุการณ์นี้ขึ้นอีกในอนาคต

7. การควบคุมการเข้าถึง (Access control)

เพื่อป้องกันการเข้าถึงเครือข่าย, ระบบปฏิบัติการ รวมทั้งแอพพลิเคชันและสารสนเทศต่างๆ โดยไม่ได้รับอนุญาตโดยมีการอ้างอิงถึงข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน หน้าที่ความรับผิดชอบ นอกจากนั้นยังครอบคลุมถึงอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกของพนักงาน

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ รวมมีการบริหารจัดการช่องโหว่ทั้งในฮาร์ดแวร์และซอฟแวร์ และให้ความสำคัญต่อการสร้างมาตรการการเข้ารหัสข้อมูลต่างๆในองค์กร

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม รวมทั้งเพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ รวมทั้งเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญ การล้มเหลวหรือหายนะต่อระบบสารสนเทศไม่เกิดขึ้นหรือเกิดน้อยที่สุดรวมทั้งต้องสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสมและเร็วที่สุด

11. การปฏิบัติตามข้อกำหนด (Compliance)

ทั้งตามทางกฎหมายและตามนโยบาย มาตรฐานความมั่นคงปลอดภัยที่เป็นข้อกำหนดทางเทคนิคนอกจากนี้ต้องมีการตรวจสอบและควบคุมทั้งทางด้านซอฟต์แวร์และฮาร์ดแวร์ด้วย เพื่อให้เกิดการนำไปใช้อย่างถูกต้องและเหมาะสมเพื่อให้เกิดประสิทธิภาพสูงสุดแก่ระบบอีกทั้งควรมีการกำหนดขอบเขตในการตรวจสอบและควบคุม การตรวจสอบนั้น มีการจัดทำเอกสารในเรื่องระเบียบขั้นตอน ความต้องการ และความรับผิดชอบ

ทั้ง 11 ข้อดังกล่าวจะเห็นได้ว่าการบริหารจัดการและส่งเสริมด้านความปลอดภัยข้อมูล จะต้องอาศัยและมีการกำหนดนโยบายการดำเนินงานภายในองค์กรที่ชัดเจนโดยอาศัยความเข้าใจ การเห็นชอบและการสนับสนุนทั้งจากผู้บริหารขององค์กรและพนักงานทุกคนในองค์กร รวมทั้งควรมีการให้ข้อมูล มีการเผยแพร่เอกสารเกี่ยวกับนโยบายที่เกี่ยวข้องให้แก่พนักงานทุกคนได้รับทราบ เพื่อ เข้าใจวัตถุประสงค์ ขอบเขตการดำเนินงาน หลักการ และเป้าหมายของความปลอดภัยข้อมูล รวมไปถึงมาตรฐานที่ สอดคล้องกับการดำเนินธุรกิจขององค์กรสำหรับการถือปฏิบัติที่ตรงกัน และจากนั้นควรต้องมีการประเมินผลว่าบรรลุตามนโยบายที่กำหนดไว้หรือไม่ส่งผลกระทบต่อการดำเนินธุรกิจอย่างไร และผลจากการเปลี่ยนแปลงดังกล่าวส่งผลต่อเทคโนโลยีอะไรและอย่างไร เพื่อให้เกิดผลสัมฤทธิ์ในการปฏิบัติ

2.1.2.2 <u>ประโยชน์ของ ISO27001/17799:2005</u>

ที่มีต่อองค์กรในการนำไปประยุกต์ใช้เพื่อเป็นกรอบแนวทางในการจัดการด้านความปลอดภัยของข้อมูล ดังต่อไปนี้

- เพื่อสร้างกระบวนการต่างๆในองค์กรที่ชัดเจนตามมาตรฐานสากล เช่น กระบวนการในการวางแผน(Plan), กระบวนการในการปฏิบัติ(Do), กระบวนการในการตรวจสอบ (Check) และกระบวนการในการตอบสนอง(Act) ในการรักษาความปลอดภัยของข้อมูลสารสนเทศต่างๆในองค์กร
- เพื่อนำเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในอดีต มาเป็นประสบการณ์ และพัฒนาความรู้ทั้งตัวบุคคลและตัวองค์กร
- เพื่อการลดความเสี่ยงที่อาจเกิดขึ้นกับระบบ เพราะมีการประเมินความเสี่ยงและการบริหารจัดการที่เหมาะสม รวมถึงการติดตามผลที่เกิดและมีการแก้ไขแล้ว
- เพื่อสร้างภาพพจน์และเพื่อได้รับการยอมรับจาก คู่ค้า หรือ ลูกค้า ในระดับมาตรฐานโลก รวมถึงการสร้างความมั่นใจในการติดต่อระหว่างองค์กร
- เพื่อช่วยในการลดต้นทุนขององค์กรในระยะยาว

2.2 การบริหารความเสี่ยง (Risk Management)

ปัจจุบันการบริหารความเสี่ยง หรือ Risk Management นั้น นับว่าเป็นสิ่งจำเป็นสำหรับองค์กร โดยเฉพาะอย่างยิ่งองค์กรที่ให้บริการผ่านสื่ออย่างอินเตอร์เน็ต จึงทำให้ยากที่จะหลีกเลี่ยงได้ เนื่องจากยุคปัจจุบันปัญหาด้านความปลอดภัยกับข้อมูล หรือ Information Security ได้เกิดขึ้นอย่างมากมาย ทั้งได้ทวีความรุนแรงและได้สร้างความเสียหายมากขึ้นไปตามกระแสการใช้งานอินเตอร์เน็ต และระบบสารสนเทศต่างๆในองค์กรที่มีจำนวนเพิ่มขึ้น

รวมทั้งเรื่องของ กฎระเบียบข้อบังคับ และ กฎหมายต่างๆ ที่ออกมามีผลบังคับใช้หรือส่งผลให้องค์กรในยุคปัจจุบันต้องปฏิบัติและปรับตัวตาม ซึ่งปัจจุบันมาตรฐานสำหรับการบริหารความเสี่ยงก็มีออกมาให้เลือกใช้งานและประยุกต์ใช้งานอย่างมาก ในงานวิจัยฉบับนี้จึงขอยกมาตรฐานที่เกี่ยวข้องและสามารถนำไปประยุกต์ใช้สำหรับองค์กรที่ให้บริการด้านการซื้อผ่านออนไลน์เท่านั้น

2.2.1 มาตรฐาน NIST

มาตรฐาน NIST 800-30 "Risk Management Guide for Information Technology Systems" เป็นมาตรฐานของ NIST (National Institute of Standards and Technology) ว่าด้วยเรื่องวิธีการ หรือขั้นตอนในการบริหารความเสี่ยงอย่างถูกต้องตามหลักการมาตรฐานสากลที่ทั่วโลกยอมรับและนำมาประยุกต์ใช้กันทั่วไป (Risk Management Methodologies) ซึ่งมีวัตถุประสงค์ในด้านการจัดการความเสี่ยงให้บรรลุผลสำเร็จ โดยเน้นถึงเรื่อง

- การระบุถึงการคุกคามและการถูกโจมตี (Threat and Vulnerability Identification) สามารถกำหนดภัย และ ช่องโหว่ ของระบบที่อาจจะเกิดขึ้น
- ปัจจัยความน่าจะเป็นในการเกิดความเสี่ยง (Likelihood Determination) ดูจากโอกาสของความเสี่ยงที่อาจจะเกิดขึ้น
- การวิเคราะห์ผลกระทบ (Impact Analysis) จากความเสี่ยงที่อาจจะเกิดขึ้นทั้งทางตรงและทางอ้อม
- การควบคุม (Control Recommendations) และวิธีการแก้ไขปัญหาของความเสี่ยงในรูปแบบต่างๆ

เพื่อเป็นการรักษาความปลอดภัยแก่ข้อมูลสารสนเทศที่เก็บรักษา ,กระบวนการหรือระบบการส่งข้อมูล ,สร้างรูปแบบการบริหารความเสี่ยง สำหรับการประกอบการตัดสินใจในการใช้งบประมาณขององค์กร และการจัดการการให้สิทธิการใช้งานที่ถูกต้อง

2.2.1.1 มาตรฐาน NIST 800-30

ว่าด้วยเรื่องดังต่อไปนี้

1. การจัดการความเสี่ยง (Risk Management Overview)

1.1 ความสำคัญของการจัดการความเสี่ยง (Importance of Risk Management)

1.2 การประยุกต์ใช้ให้เข้ากับองค์กร (Integration of Risk Management Into SDLC - system development life cycle)

2. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง เป็นการศึกษา วิเคราะห์ และประเมินทรัพย์สินสารสนเทศขององค์กร ว่ามีความเสี่ยงต่อการเกิดความเสียหายมากน้อยเพียงใด โดยพิจารณาจากระดับความสำคัญ ภัยคุกคามที่อาจเกิดขึ้น รวมทั้งจุดอ่อนของทรัพย์สินเหล่านั้น โดยผลลัพธ์จากการประเมินจะทำให้องค์กรทราบระดับความเสี่ยงต่อทรัพย์สินแต่ละอย่าง เพื่อนำมาวิเคราะห์สำหรับบริหารจัดการกับความเสี่ยงโดยกำหนดมาตรการอันเหมาะสมในการแก้ไขจุดอ่อน และการป้องกันภัยคุกคามต่างๆ โดยการประเมินความเสี่ยงมีทั้งหมด 9 ขั้นตอน ประกอบไปด้วย

2.1 System Characterization คือ การศึกษาถึงลักษณะเฉพาะต่างๆทั้ง Hardware, Software และทรัพยากรต่างๆในองค์กรเพื่ออธิบายลักษณะระบบและกำหนดขอบเขตในการประเมินความเสี่ยง จำแนกขอบเขตการของการให้สิทธิในการทำงาน และเตรียมข้อมูลที่มีผลต่อความเสี่ยง

การระบุความเสี่ยงในระบบข้อมูลสารสนเทศ ต้องอาศัยความเข้าใจในสภาพแวดล้อมของกระบวนการภายในระบบ ผู้ที่มีหน้าที่ในการประเมินความเสี่ยงต้องรวบรวมข้อมูลที่สัมพันธ์กับระบบทั้งหมดก่อน

นอกจากนี้ ยังต้องมีข้อมูลเพิ่มเติมที่เกี่ยวข้องกับสภาพแวดล้อมในการทำงานของข้อมูลและระบบอีก เช่น นโยบายความปลอดภัยของระบบขององค์กร โครงสร้างการรักษาความปลอดภัยของระบบ สถาปัตยกรรมเครือข่ายปัจจุบัน การควบคุมการทำงานของระบบขององค์กร เป็นต้น

2.2 Threat Identification คือ การบ่งชี้หรือระบุการคุกคามที่จะเกิดขึ้นได้ การศึกษาถึงช่องโหว่ของภัยคุกคามต่าง โดยทั่วไปสามารถกำหนดแหล่งกำเนิดของภัยคุกคามออกเป็น 3 ประเภทคือ

- ภัยคุกคามโดยธรรมชาติ (Natural Threats) เช่น น้ำท่วม แผ่นดินไหว เป็นต้น
- ภัยคุกคามโดยมนุษย์ (Human Threats) ทั้งการกระทำที่เกิดจากความไม่ตั้งใจและโดยเจตนาตั้งใจเพื่อการกระทำผิด
- ภัยคุกคามจากสภาพแวดล้อม (Environment Threats) เช่น ระบบไฟฟ้าขัดข้อง, มลภาวะ เป็นต้น

2.3 Vulnerability Identification คือ การบ่งชี้หรือระบุผลกระทบจากการถูกโจมตี การคาดการณ์ถึงความสูญเสียที่อาจเกิดขึ้น และการวิเคราะห์ภัยคุกคามที่มีต่อระบบข้อมูลสารสนเทศ โดยต้องมีการวิเคราะห์ความอ่อนแอหรือความไม่มั่นคงของสภาพแวดล้อมของ

ระบบ เป้าหมายคือการพัฒนาและปรับปรุงจุดที่เป็นความไม่มั่นคงของระบบที่ทำให้ระบบมีโอกาสได้รับภัยคุกคาม

2.4 Control Analysis คือ การวิเคราะห์การควบคุมที่องค์กรใช้งานอยู่เพื่อวิเคราะห์และประเมินตัว"Control" ที่ถูกนำมาใช้ในการลดผลกระทบของความเสี่ยงหรือกำจัดโอกาสที่จะเกิดภัยคุกคาม โดยเลือก"Control" ให้เข้ากับ "Threat" ทีจำเป็นและคุ้มค่ากับระบบโดยรวม รวมถึงการจัดแผนสำหรับการควบคุมที่เหมาะสม

2.5 Likelihood Determination คือ การศึกษาเพื่อกำหนดความน่าจะเป็นต่างๆที่อาจเป็นไปได้ และปัจจัยความน่าจะเป็นในการเกิดความเสี่ยงพร้อมจัดลำดับความน่าจะเป็น

โดยโอกาสที่ระบบเกิดความไม่มั่นคงหรือความเสี่ยงสามารถอธิบายได้ด้วยระดับของความเป็นไปได้ เช่น

ระดับสูง	หมายถึง	วิธีการควบคุมที่มีอยู่ไม่มีประสิทธิภาพและแหล่งกำเนิดภัยคุกคามมีความสามารถสูงในการกระตุ้นหรือก่อให้เกิดความเสี่ยงต่อระบบ
ระดับปานกลาง	หมายถึง	ระบบมีการควบคุมที่มีประสิทธิภาพแต่บางครั้งแหล่งกำเนิดภัยคุกคามมีความสามารถ พอที่จะก่อให้เกิดความเสี่ยงต่อระบบได้
ระดับต่ำ	หมายถึง	วิธีการควบคุมความปลอดภัยของระบบมีประสิทธิภาพสูง สามารถรักษาความมั่นคงของระบบได้ แหล่งกำเนิดภัยคุกคามไม่สามารถสร้างความเสี่ยงให้แก่ระบบได้

2.6 Impact Analysis คือ การประเมินและวิเคราะห์ผลกระทบที่อาจเกิดขึ้นพร้อมจัดลำดับความสำคัญ โดยศึกษาทั้ง “Data” , “Asset” และ “Mission”

โดยการประเมินผลกระทบจะประเมินผลที่สามารถจับต้องได้สามารถวัดปริมาณได้ในรูปของรายได้ที่สูญเสียไป หรือต้น ทุนในการซ่อมแซมระบบที่เพิ่มขึ้น ส่วนผลกระทบที่ไม่สามารถวัดปริมาณได้ก็สามารถอธิบายด้วยการวัดเป็นระดับผลกระทบของความรุนแรงที่มีต่อระบบ เช่น

ระดับสูง	หมายถึง	เกิดการสูญเสียทรัพย์สินและทรัพยากรหลักขององค์กรจำนวนมาก หรือเป็นอันตรายร้ายแรงต่อ

พันธกิจหรือชื่อเสียงขององค์กร หรือส่งผลให้เกิดการสูญเสียชีวิตหรือบาดเจ็บสาหัส

ระดับปานกลาง หมายถึง เกิดการสูญเสียต่อทรัพย์สินและทรัพยากรขององค์กร หรือส่งผลต่อพันธกิจหรือชื่อเสียงขององค์กร หรือส่งผลให้เกิดการบาดเจ็บ

ระดับต่ำ หมายถึง เกิดการสูญเสียทรัพย์สินและทรัพยากรขององค์กรเล็กน้อย หรือส่งผลต่อพันธกิจหรือชื่อเสียงขององค์กรบ้างเล็กน้อย

2.7 Risk Determination คือ การกำหนดความเสี่ยง โดยศึกษาความเสียหายของผลกระทบที่จะเกิด แผนที่เหมาะสมหรือจำเป็น เพื่อจัดทำระดับของความเสี่ยงและความเสี่ยงที่เกี่ยวข้อง รวมทั้งกำหนดเกณฑ์ความเสี่ยงที่สามารถยอมรับได้

<u>เมตริกซ์ระดับความเสี่ยง (Risk-Level Matrix)</u>

เป็นสูตรวัดความเสี่ยงได้จากผลคูณของโอกาสในการเกิดเหตุการณ์ที่มีความเสี่ยง (Likelihood) กับระดับผลกระทบ (Impact) ที่จะเกิดเหตุการณ์นั้น

ระดับความเสี่ยง (R) = โอกาสเกิดภัยคุกคาม (L) x ความรุนแรงของผลกระทบ (I)

เมตริกซ์ระดับความเสี่ยงสามารถมีได้หลายขนาดแล้วแต่ความต้องการของแต่ละองค์กรเช่น เมตริกซ์ 3 x 3 เมตริกซ์ 4 x 4 หรือเมตริกซ์ 5 x 5เป็นต้น ตัวอย่างในที่นี้ใช้เมตริกซ์ 3 x 3 จากโอกาสในการเกิดเหตุการณ์ที่มีความเสี่ยง 3 ระดับ (สูง ปานกลาง ต่ำ) และระดับผลกระทบหากเกิดเหตุการณ์ที่มีความเสี่ยง 3 ระดับ (สูง ปานกลาง ต่ำ) แสดงได้ดังตารางที่ 2.1

ประเภทความเป็นไปได้ของระดับโอกาสในการเกิดเหตุการณ์ มีดังนี้

ประเภท 1 โอกาสเกิดแน่นอนหรือแนวโน้มสูง ค่าความเป็นไปได้ของระดับโอกาสเกิดภัยคุกคามมีค่าเป็น 1

ประเภท 2 มีโอกาสเกิดขึ้นหรือโอกาสเกิดปานกลางค่าความเป็นไปได้ของระดับโอกาสเกิดภัยคุกคามมีค่าเป็น 0.5

ประเภท 3 ไม่มีแนวโน้มแต่มีโอกาสหรือโอกาสเกิดต่ำหรือแทบไม่มีโอกาสเกิดเลย ค่าความเป็นไปได้ของระดับโอกาสเกิดภัยคุกคามมีค่าเป็น 0.1

ประเภทของระดับความรุนแรงของผลกระทบหากเกิดเหตุการณ์ที่มีความเสี่ยงนั้น มีดังนี้

ประเภท 1 ระบบไม่สามารถทำงานได้, สูญเสียข้อมูลสำคัญ, ระบบถูกรบกวนหรือสภาพแวดล้อมหลักถูกทำลายอย่างรุนแรง กระทบต่อธุรกิจ มูลค่าความเสียหายสู' ค่าของระดับความรุนแรงของผลกระทบจากภัยคุกคามมีค่าเป็น 100

ประเภท 2 ระบบได้รับความเสียหายเล็กน้อย, ระบบผิดปกติเล็กน้อย หรือระบบที่ไม่ใช่ระบบหลักหรือสภาพแวดล้อมที่ไม่ใช่สภาพแวดล้อมหลักถูกทำลาย มูลค่าความเสียปานกลางค่าของระดับความรุนแรงของผลกระทบจากภัยคุกคามมีค่าเป็น 50

ประเภท 3 ระบบผิดปกติบางครั้งบางคราว, หรือโอกาสที่ระบบที่ไม่ใช่ระบบหลักหรือสภาพแวดล้อมที่ไม่ใช่สภาพแวดล้อมหลักถูกทำลายมีน้อยและไม่มีผลกระทบต่อการดำเนินงาน มูลค่าความเสียหายต่ำค่าของระดับความรุนแรงของผลกระทบจากภัยคุกคามมีค่าเป็น 10

ตารางที่ 2.1

เมตริกซ์ระดับความเสี่ยง 3 x 3

ระดับความรุนแรงของผลกระทบ	ระดับโอกาสในการเกิดเหตุการณ์		
	ประเภท 1 แนวโน้มสูงหรือสูงมาก = 1	ประเภท 2 ปานกลาง = 0.5	ประเภท 3 แนวโน้มต่ำหรือไม่เกิด = 0.1
ประเภท 1 = 100	สูง 100 x 1 =100	สูง 100 x 0.5 = 50	ปานกลาง 100 x 0.1 = 10
ประเภท 2 = 50	สูง 50 x1 = 50	ปานกลาง 50 x 0.5 = 25	ต่ำ 50 x 0.1 = 5
ประเภท 3 = 10	ปานกลาง 10 x 1 = 10	ต่ำ 10 x 0.5 = 5	ต่ำ 10 x 0.1 = 1

ระดับความเสี่ยง

- ระดับ 50.00 – 100.00 = ความเสี่ยงสูงมาก คือ ต้องการได้รับการแก้ไขทันทีและแก้ไขแผนปฏิบัติงานโดยด่วนหรือแผนการควบคุมต้องมีการปรับเปลี่ยน
- ระดับ 10.00 – 49.99 = ความเสี่ยงปานกลาง คือ ควรมีการแก้ไขแต่ไม่เร่งด่วน ผู้บริหารสามารถรอได้ และแผนการควบคุมควรได้รับการปรับปรุงแล้วนำมาใช้
- ระดับ 1.00 – 19.99 = ความเสี่ยง คือ สามารถยอมรับได้ โดยระบบควรได้รับการตรวจสอบเพื่อให้แน่ใจว่าแผนการควบคุมที่มีอยู่จะสามารถแก้ไขปัญหาและรับมือกับความเสี่ยงได้

2.8 Control Recommendations คือ การเสนอแนะตัว Control เป็นการเลือกใช้ Control ให้เหมาะสมกับมูลค่าของทรัพย์สิน (Asset) ที่องค์กรมีและความจำเป็นต้องป้องกัน

2.9 Results Documentation คือ การจัดทำเอกสารอ้างอิงถึงผลลัพธ์ที่ได้ และจัดทำรายงานการประเมินความเสี่ยงเพื่อการตัดสินใจของผู้บริหารขององค์กร

ดังภาพที่ 2.1 แผนภูมิแสดงหลักการการประเมินความเสี่ยงที่แสดงถึง Input และ Output ในแต่ขั้นตอนทั้ง 9 ขั้นตอนสำหรับการนำไปประยุกต์ใช้ขององค์กร

ภาพที่ 2.2

หลักการการประเมินความเสี่ยง[i1]

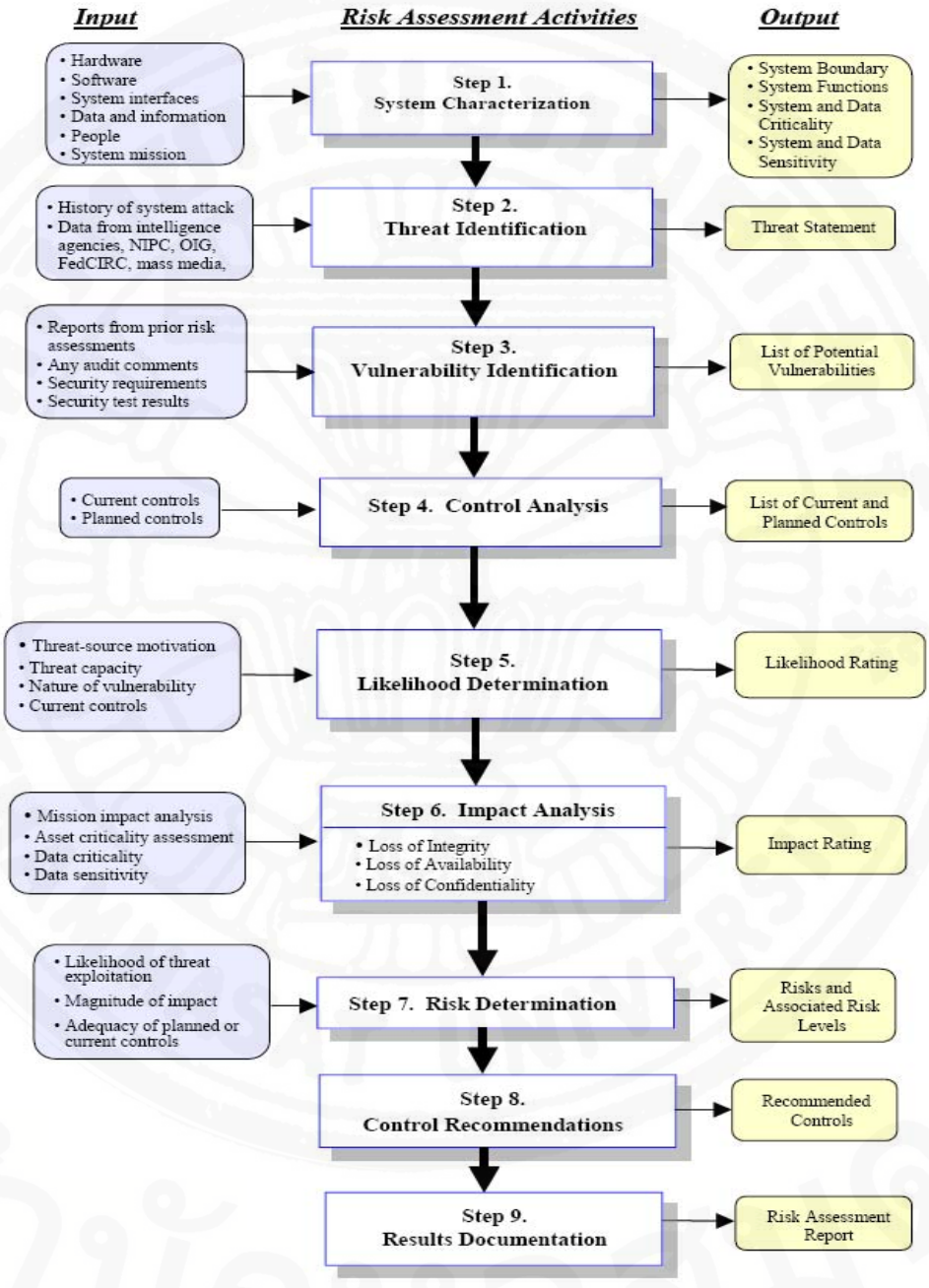


Figure 3-1. Risk Assessment Methodology Flowchart

---

[1]Gary Stoneburner Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems, 2002, p9.

3. การบรรเทาหรือลดความเสี่ยง (Risk Mitigation)

3.1 ทางเลือกในการบรรเทาความเสี่ยง (Risk Mitigation Options)

- การตั้งสมมติฐานความเสี่ยง (Risk Assumption) การสันนิษฐานการเสี่ยงเพื่อยอมรับการเสี่ยงที่เป็นไปได้และดำเนินด้านระบบ Itต่อไป หรือประยุกต์การควบคุมเพื่อที่จะลดการเสี่ยงให้อยู่ในระดับที่ยอมรับได้

- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เพื่อหลีกเลี่ยงความเสี่ยงโดยการกำจัดการเสี่ยงที่เป็นสาเหตุให้และ/หรือเกิดผลที่ตามมา เช่น ปิดเครื่องควบคุมระบบเมื่อพบว่าเกิดความเสี่ยงขึ้น

- การตั้งขีดความเสี่ยง (Risk Limitation) เพื่อจำกัดความเสี่ยงที่อาจเกิดขึ้น และสามารถยอมรับได้

- การวางแผนรองรับความเสี่ยง (Risk Planning) เป็นการจัดการความเสี่ยงโดยการพัฒนาแผนสำหรับการแบ่งเบาการเสี่ยงสำหรับ การจัดลำดับการให้สิทธิ,การปฏิบัติและ ควบคุมรักษา

- การวิจัยและการรับรอง (Research and Acknowledgment) เพื่อบรรเทาความเสี่ยงของความเสียหายโดยทดสอบในจุดที่อาจ ถูกโจมตีได้ง่าย หรือรอยรั่วต่างๆและที่วิจัยตัว Controls เพื่อตรวจแก้ ในจุดนั้น

- การถ่ายโอนความเสี่ยง (Risk Transference) เพื่อถ่ายโอนความเสี่ยงโดยการใช้ทางเลือกอื่นๆที่จะสามารถชดเชยความเสียหายที่เกิดขึ้น เช่น การทำประกันภัย

3.2 การวางกลยุทธ์เพื่อบรรเทาความเสี่ยง (Risk Mitigation Strategy) เพื่อออกแบบและจัดเตรียมสำหรับการบรรเทาความเสี่ยงจากการคุกคามที่เกี่ยวกับมนุษย์ทั้งทางตรงและทางอ้อม พร้อมวางกลยุทธ์สำหรับการป้องกัน และลดขอบเขตของความเสี่ยง

3.3 Approach for Control Implementation วิธีการสำหรับควบคุมเครื่องมือ เพื่อให้ไม่เกิดผลกระทบหรือเกิดน้อยสุดกับการทำงานอื่นๆ ในการที่จะบรรเทาความเสี่ยง

3.4 ประเภทการควบคุม (Control Categories) โดยแบ่งเป็น 3 ประเภท คือ

- หน่วยควบคุมความปลอดภัยทางเทคนิค
- หน่วยควบคุมความปลอดภัยทางการจัดการ
- หน่วยควบคุมความปลอดภัยที่สามารถปฏิบัติได้

3.5 การวิเคราะห์ ค่าใช้จ่ายและประโยชน์ที่ได้ (Cost-Benefit Analysis) เป็นการจัดสรรทรัพยากรและประเมินค่าที่เหมาะสมสำหรับการลงทุน รวมทั้งเพื่อให้เหมาะกับสภาพของแต่ละองค์กร

3.6 การพิจารณาความเสี่ยงที่นอกเหนือ (Residual Risk) โดยการวิเคราะห์ขอบเขตในการบรรเทาความเสี่ยงให้ลดลงที่เป็นไปได้

4. การประเมิน (Evaluation And Assessment)

จุดมุ่งหมายคือ ความมีเหตุมีผล (Accountability) ทุกกิจกรรมในการดำเนินงานต้องสามารถติดตามได้และ ความแน่นอน (Assurance) ต้องมั่นใจว่าจุดมุ่งหมายหลักอื่นๆทั้งหมดมีอยู่จริง โดยเมื่อทำการประเมินการใช้งานเครื่องมือ ระบบ และกระบวนการต่างๆกัน จะต้องใช้หลักทั้งหมดของความปลอดภัยเข้ามาประกอบด้วยเสมอ และเนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา จึงเกิดความใหม่ๆขึ้นมาได้เสมอ ดังนั้นองค์กรจึงต้องไม่หยุดในการประเมินด้านต่างๆอยู่เสมอ

2.3 การจัดซื้อออนไลน์ (e-Procurement)

2.3.1 คำจำกัดความ

e-Procurement เป็นวิธีการจัดซื้อจัดหาผ่านระบบออนไลน์

e-Auction การประมูลออนไลน์เป็นการเสนอราคาแข่งขันกันผ่านอินเตอร์เน็ต มุ่งเน้นความคล่องตัวและความโปร่งใสในการดำเนินการและการแข่งขัน บ้างเรียกว่า Online Bidding ,e-Bidding , การประมูลออนไลน์หรือ การประมูลทางอิเล็กทรอนิกส์ ซึ่งเป็นรูปแบบหนึ่งในการจัดซื้อจัดหา

e-Marketplace Service Provider ผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ (e-Marketplace) ที่ทำหน้าที่เป็นผู้จัดการประมูล และเป็นสื่อกลางระหว่างผู้ซื้อกับผู้ขาย รวมทั้งจัดหาผู้ขายสินค้าเพิ่มเติมผ่านทางระบบอิเล็กทรอนิกส์ โดยมีศูนย์กลางการติดต่ออยู่ที่เว็บไซต์ของตลาดกลาง

2.3.2 e-Procurement

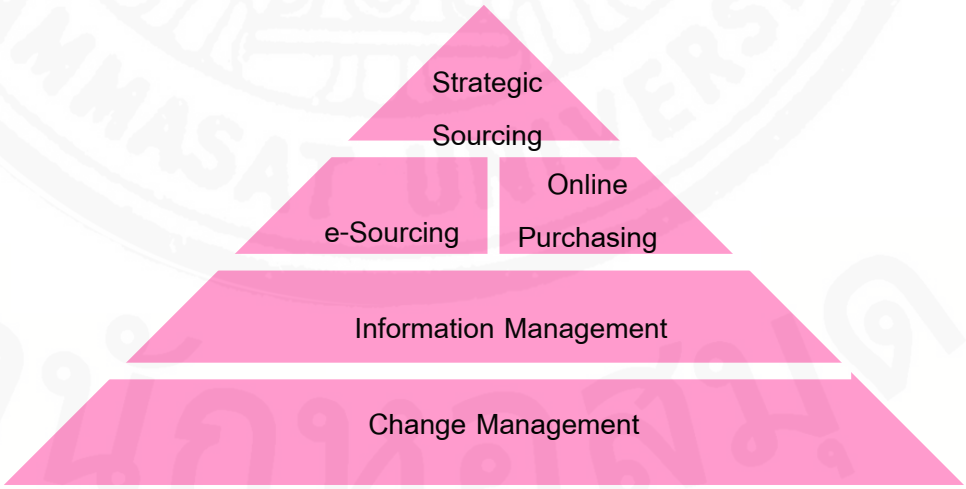
ระบบการจัดซื้อจัดหาออนไลน์เป็นการพัฒนาเทคโนโลยีการจัดซื้อจัดหารูปแบบหนึ่ง เป็นการผสมของข้อดีระหว่างการจัดซื้อแบบรวมอำนาจและการจัดซื้อแบบกระจายอำนาจ โดยเป็นการปรับเปลี่ยนรูปแบบการดำเนินการในการจัดซื้อจากเดิมที่เป็นการจัดซื้อตามความต้องการของผู้ใช้งาน (User) มาเป็นการจัดซื้อจัดหาอย่างเป็นระบบระเบียบ มีการวางแผนความต้องการล่วงหน้า โดยศึกษาและกำหนดกลยุทธ์ที่เหมาะสมกับสภาวะตลาดคู่กับการใช้งานเทคโนโลยีสารสนเทศในการจัดซื้อ

2.3.2.1 <u>องค์ประกอบหลัก</u> ของภาพรวมในการจัดซื้อจัดหาออนไลน์ คือ

- การจัดซื้อจัดหาเชิงกลยุทธ์ (Strategic Sourcing)
- การจัดหาออนไลน์ (e-Sourcing)
- การสั่งซื้อออนไลน์ (Online Purchasing)
- การบริหารการจัดการข้อมูล (Information Management)
- การบริหารการเปลี่ยนแปลง (Change Management)

ภาพที่ 2.3

แบบจำลององค์ประกอบของการจัดซื้อจัดหาออนไลน์



ที่มา: บริษัท พันธวณิช จำกัด. พลิกโฉมการจัดซื้อจัดหาแนวใหม่ด้วย e-Procurement., 2005.

2.3.2.2 <u>วัตถุประสงค์ของการจัดซื้อจัดหาออนไลน์</u>

- เพื่อลดต้นทุนการดำเนินการ
- เพื่อลดขั้นตอนในการจัดหาและสั่งซื้อสินค้าที่มีการขอซื้อซ้ำๆ
- เพื่อลดการจัดซื้อนอกระบบ
- เพิ่มอำนาจการต่อรองกับผู้ขาย
- เพิ่มประสิทธิภาพให้กับงานจัดซื้อจัดหา

การจัดซื้อจัดหาเชิงกลยุทธ์ การจัดหาออนไลน์และการสั่งซื้อออนไลน์มีความสัมพันธ์กัน ซึ่งทั้ง 3 ส่วนเป็นการดำเนินงานที่อาศัยช่องทางทางอินเตอร์เน็ต โดยที่

<u>การจัดซื้อจัดหาเชิงกลยุทธ์</u> เป็นการเพิ่มอำนาจการต่อรองกับผู้ขาย เนื่องจากมีการวางแผนความต้องการและมีการกำหนดมาตรฐานของสินค้าที่ต้องการชัดเจน รวมถึงการศึกษาสภาวะตลาดและโซ่อุปทานของสินค้านั้นๆ เพื่อกำหนดกลยุทธ์การจัดหาให้ได้สินค้าที่ถูกต้องตามความต้องการขององค์กรในราคาที่เหมาะสมและก่อเกิดประโยชน์ร่วมกันในสายโซ่อุปทาน

<u>การจัดหาออนไลน์</u> มี 3 รูปแบบหลักๆ ได้แก่

- การประกวดราคาออนไลน์ (e-Tendering)
- การเสนอราคาออนไลน์ (e-RFQ)
- การประมูลออนไลน์ (e-Auction)

<u>การสั่งซื้อออนไลน์</u> เป็นเครื่องมือที่ปัจจุบันกำลังได้รับความนิยมสำหรับองค์กรขนาดใหญ่ เนื่องจากกระบวนการทำงานของระบบสั่งซื้อออนไลน์ จะช่วยทำให้ขั้นตอนของการสั่งซื้อสินค้าในองค์กรมีความกระชับมากขึ้น ช่วยลดต้นทุนการดำเนินการ ลดเอกสารที่ต้องจัดเก็บและสามารถเรียกดูรายงานการสั่งซื้อได้ทันที

2.3.3 <u>คุณสมบัติและหน้าที่หลักของผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ (e-Marketplace Service Provider)</u>

1. สามารถจัดหา Infrastructure และระบบสำรองฉุกเฉินต่างๆ สำหรับการทำ e-Auction ให้ถูกต้องตามมาตรฐานที่ศูนย์การจัดจ้างและพัสดุภาครัฐกำหนด

2. จัดอบรมผู้ขายเกี่ยวกับขั้นตอนของการทำ e-Auction และการใช้โปรแกรมที่เกี่ยวข้อง

3. ให้บริการรับรอง Catalogue สินค้าของผู้ขายทุกรายที่ผ่านการลงทะเบียนจากศูนย์ฯ เรียบร้อยแล้ว โดยตลาดสามารถคิดค่าบริการและค่านายหน้าได้ไม่เกินอัตราที่ศูนย์ฯ กำหนด (อาจยกเลิกถ้ามีการแข่งขันใน e-Marketplace)

4. การให้คำแนะนำเกี่ยวกับสินค้า ตลอดจนวิธีประมูลหรือวิธีกาจัดซื้อจัดหา ที่เหมาะสมแก่ผู้ซื้อ

5. จัดทำรายงานการดำเนินงานให้แก่กรมบัญชีกลาง และผู้ซื้อทุกครั้งหลังจากมีการทำ การประมูล (e-Auction) คุณสมบัติที่สำคัญของวัสดุครุภัณฑ์ที่จะนำมาพิจารณาในการทำ e-Auction คือ เป็นวัสดุหรือครุภัณฑ์ที่มีลักษณะเดียวกัน เช่น คอมพิวเตอร์ กระดาษ วัสดุสำนักงาน การเช่ารถยนต์ การเช่าเครื่องถ่ายเอกสาร เป็นต้น

2.4 กฎหมายที่เกี่ยวข้อง

2.4.1 พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

เป็นพระราชบัญญัติที่มีการประกาศกฎหมายว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ (ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน) โดยพระราชบัญญัตินี้มีบทบัญญัติที่ให้ใช้บังคับแก่ธุรกรรมทั้ง ในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ (ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร) โดยมีการระบุในมาตรา ๒๕ ว่าธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

2.4.2 ประกาศกระทรวงพาณิชย์เรื่อง ให้ผู้ประกอบการพาณิชย์กิจ ต้องจดทะเบียน

การประกาศเรื่องการจดทะเบียนผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์นั้น ได้กำหนดให้งานด้านพาณิชย์อิเล็กทรอนิกส์อยู่ภายใต้ความรับผิดชอบของ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

2.4.2.1 วัตถุประสงค์ของการจดทะเบียน

- เพื่อให้สามารถรู้ถึงการมีตัวตนที่แท้จริงของผู้ประกอบการว่า เป็นใคร อยู่ที่ไหน ทำธุรกรรมอะไร และเพื่อนำมากำหนดแนวทางในการส่งเสริมในด้านต่างๆให้สอดคล้องกับสภาวะทางเศรษฐกิจในปัจจุบัน เพื่อให้องค์กรที่จดทะเบียนสามารถนำพาณิชย์อิเล็กทรอนิกส์ไปใช้ในการประกอบธุรกิจได้อย่างเป็นรูปธรรม และประสบผลสำเร็จมากขึ้น

- เพื่อสร้างบริการทางตลาดกลางพาณิชย์อิเล็กทรอนิกส์ (e-Marketplace) สำหรับช่วยส่งเสริมการตลาด

2.4.2.2 ผู้ที่มีหน้าที่จดทะเบียนพาณิชย์อิเล็กทรอนิกส์

คือ บุคคลธรรมดาหรือนิติบุคคลที่มีสถานประกอบการตั้งอยู่ในประเทศไทย ซึ่งประกอบพาณิชย์กิจในเชิงพาณิชย์อันเป็นอาชีพปกติ ดังนี้

- ซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเตอร์เน็ต ได้แก่ บุคคลที่มีเว็บไซต์เพื่อทำการซื้อขายสินค้าหรือบริการ
- บริการอินเตอร์เน็ต (ISP : Internet Service Provider)
- ให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย (Web Hosting)
- บริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ ผ่านระบบเครือข่ายอินเทอร์เน็ต (e-Marketplace)

2.4.2.3 ประโยชน์ของการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์

- ช่วยให้องค์กรมีความน่าเชื่อถือ ช่วยให้ผู้บริโภคเกิดความมั่นใจในการตัดสินใจทำธุรกรรมหรือใช้บริการมากขึ้น รวมทั้งการการได้รับข่าวสาร การอบรมสัมมนาและสิทธิพิเศษต่าง ๆ จากกรมพัฒนาธุรกิจการค้า

- เว็บไซต์ขององค์กรที่ทำการขึ้นทะเบียนแล้ว สามารถยื่นขอใช้เครื่องหมายรับรองความน่าเชื่อถือ (Trust Mark) จากกรมพัฒนาธุรกิจการค้าและ หากองค์กรดังกล่าว มีคุณสมบัติครบถ้วนตามที่กรมพัฒนาธุรกิจการค้ากำหนด ผู้ประกอบการจะได้เครื่องหมายรับรองความน่าเชื่อถือ และสามารถนำเครื่องหมายนี้ไปติดไว้ที่หน้าเว็บไซต์ขององค์กร เพื่อเพิ่มความน่าเชื่อถือให้แก่เว็บไซต์อีกระดับหนึ่ง

- ทางกรมพัฒนาธุรกิจการค้าจะมีการนำรายชื่อเว็บไซต์ขององค์กรที่ทำการขึ้นทะเบียนแล้ว มาจัดทำเป็นฐานข้อมูลแยกตามประเภทธุรกิจ และนำไปเผยแพร่แก่ผู้ประกอบการรวมถึงประชาชนทั่วไปที่สนใจผ่านสื่อต่าง ๆ เพื่อเป็นการช่วยประชาสัมพันธ์ให้แก่องค์กรอีกทางหนึ่ง

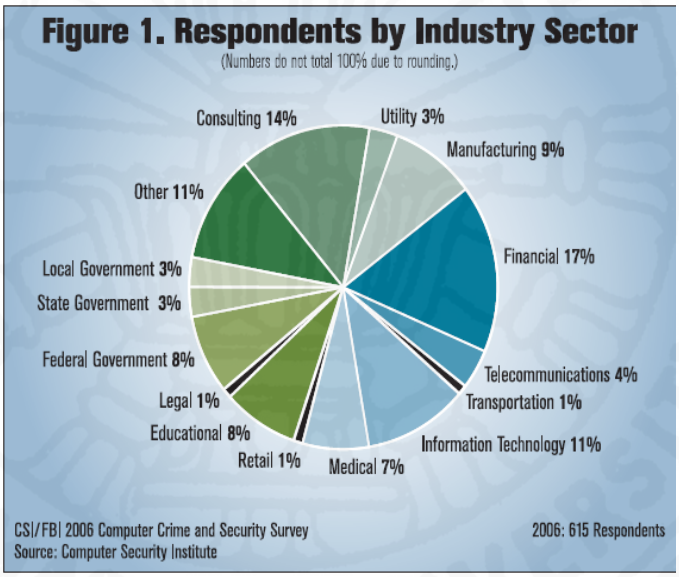
2.5 ผลการสำรวจทางสถิติ

ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และการรักษาความปลอดภัยโดยผลการสำรวจดังกล่าวเป็นผลสำรวจในระหว่างปี 2006 ที่ทาง Computer Security Institute จัดทำขึ้นเพื่อแสดงถึงสถานะปัจจุบันที่เกิดขึ้นของอาชญากรรมทางคอมพิวเตอร์และการรักษาความปลอดภัย

2.5.1 ผลสำรวจกลุ่มอุตสาหกรรมที่ให้ความสนใจต่ออาชญากรรมทางคอมพิวเตอร์และการรักษาความปลอดภัย

ภาพที่ 2.4

กลุ่มอุตสาหกรรมที่ให้ความสนใจต่อภัยคุกคามทางคอมพิวเตอร์[2]



จากภาพ 2.4 จะเห็นได้ว่ากลุ่มอุตสาหกรรมทางด้านการเงิน และงานที่ปรึกษาจะให้ความสนใจในด้านการรักษาความปลอดภัยรวมถึงภัยคุกคามต่างๆที่เกิดกับคอมพิวเตอร์เนื่องจากมีการจัดเก็บข้อมูลสำคัญของลูกค้าเป็นจำนวนมาก

---

[2]Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson , 2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY, San Francisco: Computer Security Institute, 2005, p3.

ตารางที่ 2.2

ข้อมูลของการถูกบุกรุกระบบ[3]

Table 1: How Many Incidents?

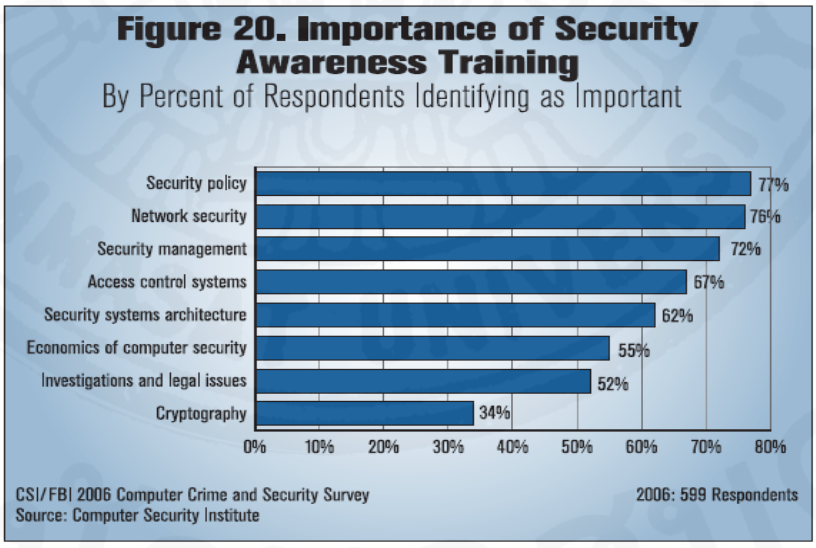
How many incidents, by % of respondents	1-5	6-10	>10	Don't know
2006	48	15	9	28
2005	43	19	9	28
2004	47	20	12	22
2003	38	20	16	26
2002	42	20	15	23
2001	33	24	11	31
2000	33	23	13	31
1999	34	22	14	29

CSI/FBI 2006 Computer Crime and Security Survey — 2006: 341 Respondents
Source: Computer Security Institute

จากตารางแสดงให้เห็นว่าจำนวนการถูกบุกรุกระบบตั้งแต่อดีตจนถึงปัจจุบัน ไม่ได้ลดจำนวนลง แม้ว่าจะมีมาตรฐานและวิธีการเพื่อป้องกันที่หลากหลายออกมาแล้วก็ตาม

ภาพที่ 2.5

สิ่งสำคัญสำหรับการฝึกอบรมเพื่อการรักษาความปลอดภัย[4]



ซึ่งผลการสำรวจ องค์กรส่วนใหญ่ให้ความสำคัญในด้าน Security Policy และ Network Security

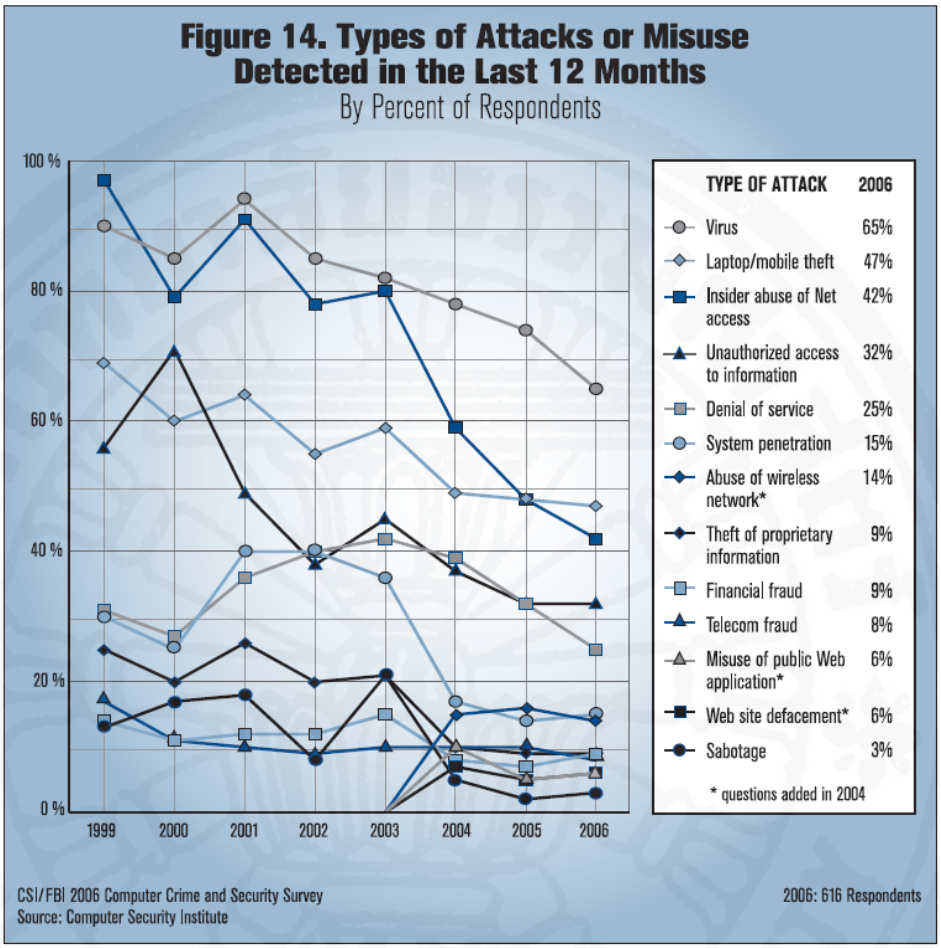
ภาพที่ 2.6

---

[3]**Ibid.**, p.11.

[4]**Ibid.**, p.20.

%ของแต่ละประเภทของการโจมตี[5]

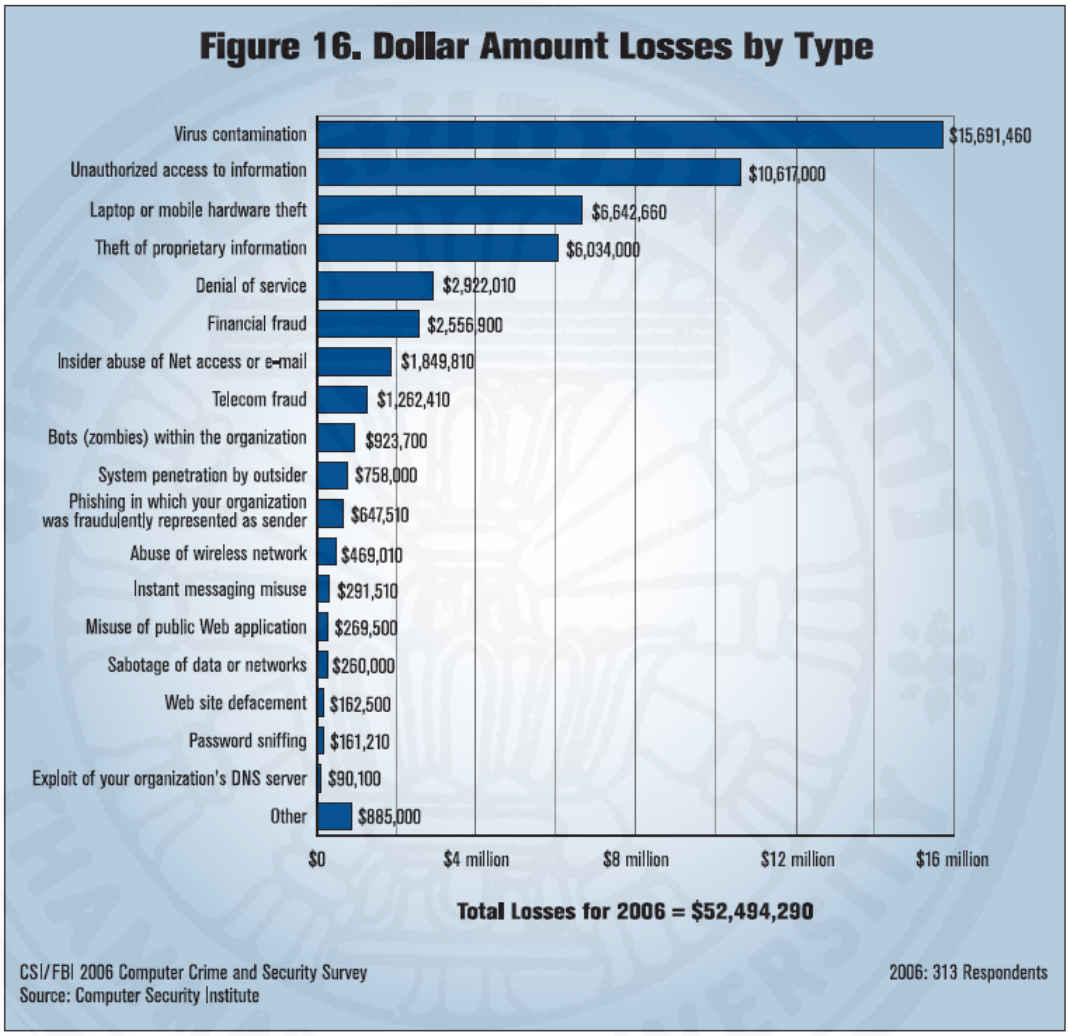


จากภาพแสดงว่าปัจจุบันการโจมตีในรูปแบบไวรัสได้ลดลงจากปีก่อนๆ แต่ปัญหากับการใช้เครือข่ายไร้สาย(Wireless network) และความเสียหายที่เกิดกับเว็บไซต์ เริ่มเพิ่มจำนวนมากขึ้นทุกปี

[5]Ibid., p.13.

ภาพที่ 2.7

เงินลงทุนในการแก้ไขปัญหาแต่ละประเภท[6]



โดยการลงทุนส่วนใหญ่ เน้นเรื่องการควบคุมไวรัส แสดงว่าแนวโน้มในแต่ละองค์กรให้ความสำคัญกับการป้องกันการบุกรุกจากโปรแกรมที่ไม่ประสงค์ดี

[6]Ibid., p.15.

ภาพที่ 2.8

การตอบสนองต่อปัญหาที่เกิดขึ้นในช่วง 2 ปีที่ผ่านมา[7]

Table 2. Respondents Identify the Most Critical Issues for the Next Two Years

Most critical computer security issues in next two years	# of respondents
Data protection (e.g.., data classification, identification and encryption) and application software (e.g. Web application, VoIP) vulnerability security	73
Policy and regulatory compliance (Sarbanes–Oxley, HIPAA)	63
Identity theft and leakage of private information (e.g. proprietary information, intellectual property and business secrets)	58
Viruses and worms	52
Management involvement, risk management, or supportive resources (human resources, capital budgeting and expenditures)	47
Access control (e.g. passwords)	43
User education, training and awareness	43
Wireless infrastructure security	41
Internal network security (e.g. insider threat)	38
Spyware	34
Social engineering (e.g. phishing, pharming)	33
Mobile (handheld) computing devices	27
Malware or malicious code	20
Patch management	17
Zero-day attacks	16
Intrusion detection systems	16
Instant messaging	15
E-mail attacks (e.g. spam)	15
Employee misuse	12
Physical security	10
Web attacks	9
Two-factor authentication	9
Bots and botnets	7
Disaster recovery (e.g. data back-up)	7
Denial of service	7
Endpoint security	6
Managed cybersecurity provider	5
PKI implementation	4
Rootkits	3
Sniffing	3
Standardization, configuration management	3

CSI/FBI 2006 Computer Crime and Security Survey — 2006: 426 Respondents
Source: Computer Security Institute

[7] **Ibid.**, p.24.

2.6 งานวิจัยที่เกี่ยวข้อง

จากการศึกษาถึงภัยคุกคาม และปัจจัยที่ก่อให้เกิดความเสี่ยงที่เป็นพฤติกรรมและลักษณะการทำงานของบุคคลในองค์กร ในการรักษาความปลอดภัยข้อมูลสารสนเทศขององค์กรขนาดกลางและขนาดใหญ่ โดยการแยกประเภทของความเสี่ยงตามความปลอดภัยของข้อมูล ได้แก่ ความเชื่อถือ (Confidentiality) ความถูกต้องและสมบูรณ์ (Integrity) และ ความสามารถในการนำมาใช้ประโยชน์ได้เมื่อต้องการ (Availability) ความเสี่ยงที่เป็นไปได้ว่าจะเกิดขึ้นกับความปลอดภัยของข้อมูล

จากงานวิจัยพบว่าภัยคุกคามที่ก่อให้เกิดความเสี่ยงต่อการรักษาความปลอดภัยข้อมูล ที่มีความเสี่ยงในระดับสูง ซึ่งองค์กรขนาดกลางและใหญ่ควรให้ความสนใจและหาแนวทางการแก้ไขมีอยู่ 8 ภัยคุกคามเรียงลำดับตามความเสี่ยงจากสูงไปต่ำดังนี้

1. การใช้ชื่อ (user ID) ร่วมกันเพื่อเข้าใช้ข้อมูล
2. การรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด
3. การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้
4. การปกป้องรหัสผ่าน (password) อย่างไม่เหมาะสม
5. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม
6. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม
7. ระบบรักษาความปลอดภัยข้อมูลและขั้นตอนการให้สิทธิการใช้งานไม่มีการเปลี่ยนแปลงให้ทันสมัย
8. การออกแบบระบบซับซ้อนเกินไป

ซึ่งภัยคุกคามดังกล่าวส่วนหนึ่งจะมาจาก การที่ภายในองค์กรมีการเชื่อมต่ออินเตอร์เน็ต ทำให้ผู้บุกรุกที่จะเข้ามาสร้างปัญหาให้กับองค์กร สามารถเข้าทางเครือข่ายอินเตอร์เน็ต หากระบบการรักษาความปลอดภัยขององค์กรไม่มีประสิทธิภาพมากพอ อย่างไรก็ตาม ความเสี่ยงสามารถเกิดขึ้นได้จากภายในองค์กรเองเช่นกัน เมื่อผู้บุกรุกเป็นพนักงานในองค์กร

แนวทางการป้องกันและแก้ปัญหาจากภัยคุกคามที่เกิดขึ้น ควรจะสอดคล้องกับการจัดการบริหารระบบความปลอดภัยที่มีประสิทธิภาพ ซึ่งโดยสรุปแล้วสามารถแบ่ง การควบคุมความเสี่ยงในการรักษาความปลอดภัยข้อมูลขององค์กรเป็น 3 ส่วนหลักๆได้แก่

1. การควบคุมที่เกี่ยวข้องกับบุคคลากรในองค์กร เช่น การจัดฝึกอบรมพนักงาน

2. การควบคุมที่เกี่ยวข้องกับกระบวนการทำงานและนโยบายขององค์กร เช่น การควบคุมการเข้าใช้ข้อมูล (Access Control), การสำรองและกู้ข้อมูล (Backup and Recovery) เพื่อเป็นการป้องกันการสูญหายของข้อมูลที่ใช้งานอยู่

3. การควบคุมที่เกี่ยวข้องกับการใช้เทคโนโลยีภายในองค์กร เช่น การจัดทำกระบวนการและนโยบายที่เหมาะสมในการควบคุมการใช้งานเทคโนโลยีต่างๆ[8]

[8] ทรงชล มหารมณ์, “การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสำหรับองค์กรขนาดใหญ่และขนาดกลาง ในเขตกรุงเทพมหานคร”, งานวิจัยค้นคว้าอิสระ วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์, 2548.