ดร.สิงห์ทอง บัวชุม
D.P.A., ปร.ด., รป.ด., รป.ม., รม., บย

สถาบัน THE BEST CENTER
2145/7 ซ.รามคำแหง 43/1 ถ.รามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
โทร.0-2318-6868, 0-2314-1492 โทรสาร 0-2718-6274
www.thebestcenter.com facebook.com/bestcentergroup
คุณภาพทางวิชาการต้องมาที่ 1

คู่มือเตรียมสอบ

นักการข่าวปฏิบัติการ

(ด้านความมั่นคงปลอดภัยไซเบอร์)

สำนักข่าวกรองแห่งชาติ

ปี69

แนวข้อสอบมากกว่า 400 ข้อ

ความรู้ความสามารถทั่วไปและความสามารถที่ใช้เฉพาะตำแหน่ง

หลักสูตรและวิธีการสอบแข่งขันเพื่อวัดความรู้ความสามารถที่ใช้เฉพาะตำแหน่ง
(คะแนนเต็ม 200 คะแนน)

ทดสอบความรู้ความสามารถดังต่อไปนี้ โดยวิธีการสอบข้อเขียน

1) วิชาความรู้ด้านความมั่นคงปลอดภัยไซเบอร์(คะแนนเต็ม 100 คะแนน)

ทดสอบความรู้ความสามารถ ความเข้าใจเกี่ยวกับลักษณะงานที่ปฏิบัติ รวมถึงความรู้ทางวิชาการที่ใช้ในการปฏิบัติงานในตำแหน่งนักการข่าวปฏิบัติการ (ด้านความมั่นคงปลอดภัยไซเบอร์) ความรู้ด้านเทคโนโลยีการออกแบบ และดูแลระบบด้านความมั่นคงปลอดภัย การวิเคราะห์และออกแบบโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัย

2) วิชาความรู้เกี่ยวกับสถานการณ์ปัจจุบัน (คะแนนเต็ม 60 คะแนน)

ทดสอบความรู้ความสามารถในการประมวลและวิเคราะห์ข่าวสาร รวมทั้งการประเมินแนวโน้มเกี่ยวกับสถานการณ์สำคัญด้านการเมือง เศรษฐกิจ สังคม ทั้งที่เกิดขึ้นภายในประเทศและต่างประเทศ ซึ่งอาจส่งผลกระทบต่อผลประโยชน์ ความมั่นคง หรือความสงบเรียบร้อยของประเทศไทย ความรู้เรื่องการรักษาความปลอดภัยแห่งชาติและทักษะความเข้าใจและการใช้เทคโนโลยีดิจิทัล

2) วิชาภาษาอังกฤษ (คะแนนเต็ม 40 คะแนน)

ทดสอบความรู้ความสามารถและทักษะในการใช้ภาษาอังกฤษ โดยการให้สรุปความ หรือตีความจากข้อความสั้น ๆ หรือบทความ และให้พิจารณาเลือกใช้ภาษาในรูปแบบต่าง ๆ จากคำหรือกลุ่มคำประโยคหรือข้อความสั้น ๆ หรือเรียงความ การใช้ไวยากรณ์

299.-

คู่มือสอบนักการข่าวปฏิบัติการ (ด้านความมั่นคงปลอดภัยไซเบอร์)
สำนักข่าวกรองแห่งชาติ

รวบรวมและเรียบเรียงโดย.....

ฝ่ายวิชาการ สถาบัน THE BEST CENTER

ราคา 299 บาท

จัดพิมพ์และจำหน่ายโดย

The Best Center InterGroup Co., Ltd.

บริษัท เดอะเบสท์ เซ็นเตอร์ อินเตอร์กรุ๊ป จำกัด

บริหารงานโดย ดร.สิงห์ทอง บัวชุมและอาจารย์จันทนี บัวชุม (ติวเตอร์กุ้ง ย่าน ม. ราม)

เลขที่ 2145/7 ซอยรามคำแหง 43/1 ถนนรามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240

โทรศัพท์.081-496-9907,0-2314-1492, 0-2318-6868 โทรสาร. 0-2718-6274 line id: @ thebestcenter

www.thebestcenter.com หรือ www.facebook.com/bestcentergroup

คู่มือสอบ
นักการข่าวปฏิบัติการ
(ด้านความมั่นคงปลอดภัยไซเบอร์)
สำนักข่าวกรองแห่งชาติ

ราคา 299 -.

คำนำ

สำหรับชุดคู่มือสอบสำหรับตำแหน่งนักการข่าวปฏิบัติการ (ด้านความมั่นคงปลอดภัยไซเบอร์) สำนักข่าวกรองแห่งชาติ เล่มนี้ ทางสถาบัน THE BEST CENTER และฝ่ายวิชาการของสถาบันได้เรียบเรียงขึ้น เพื่อให้ผู้สมัครสอบใช้สำหรับเตรียมสอบในการสอบแข่งขันฯในครั้งนี้

ทางสถาบัน THE BEST CENTER ได้เล็งเห็นความสำคัญจึงได้จัดทำหนังสือ เล่มนี้ขึ้นมา ภายในเล่มประกอบด้วยทุกส่วนที่กำหนดในการสอบ เจาะข้อสอบทุกส่วน พร้อมคำเฉลยอธิบาย มาจัดทำเป็นหนังสือชุดนี้ขึ้น เพื่อให้ผู้สอบได้เตรียมตัวอ่านล่วงหน้า มีความพร้อมในการทำข้อสอบ

ท้ายนี้ คณะผู้จัดทำขอขอบคุณทางสถาบัน THE BEST CENTER ที่ได้ให้การสนับสนุนและมีส่วนร่วมในการจัดทำต้นฉบับ ทำให้หนังสือเล่มนี้สามารถสำเร็จขึ้นมาเป็นเล่มได้ พร้อมกันนี้คณะผู้จัดทำขอน้อมรับข้อบกพร่องใดๆ อันเกิดขึ้นและยินดีรับฟังความคิดเห็นจากทุกๆท่าน เพื่อที่จะนำมาปรับปรุงแก้ไขให้ดียิ่งขึ้น

ขอให้โชคดีในการสอบทุกท่าน

ฝ่ายวิชาการ

สถาบัน The Best Center

www.thebestcenter.com

สารบัญ

ความรู้เกี่ยวกับสำนักข่าวกรองแห่งชาติ

ก่อนจะมาเป็น "สำนักข่าวกรองแห่งชาติ"

ประเทศต่าง ๆ รวมทั้งไทยจัดตั้งและพัฒนาองค์การข่าวกรองอย่างจริงจังต่อเนื่องภายหลังสงครามโลกครั้งที่ 2 ยุติลง โดยสถานการณ์การเมืองระหว่างประเทศในเอเชียที่เป็นปัจจัยสำคัญในการผลักดันให้เกิดหน่วยงานด้านการข่าวกรองระดับชาติของไทย คือ ภัยคุกคามคอมมิวนิสต์ สหรัฐฯ ที่เป็นแกนนำต่อสู้ ด้านประชาธิปไตย มองว่าไทยอยู่ในจุดยุทธศาสตร์ **Southeast Asia Mainland** ที่เหมาะสมสำหรับต่อต้านคอมมิวนิสต์ สถานการณ์ระหว่างประเทศขณะนั้นจึงกดดันให้รัฐบาลไทยภายใต้การนำของจอมพล ป.พิบูลสงคราม ต้องปรับเปลี่ยนนโยบาย เพื่อรองรับการที่สหรัฐฯ สนับสนุนให้ประเทศในเอเชียตะวันออกเฉียงใต้ต่อต้านลัทธิคอมมิวนิสต์ ไทยจึงได้จัดตั้งหน่วยงานข่าวกรองระดับชาติ อันเป็นที่มาของการตั้ง “กรมประมวลราชการแผ่นดิน” ขึ้นตามพระราชกฤษฎีกาจัดวางระเบียบกรมประมวลราชการแผ่นดิน ทบวงคณะรัฐมนตรีฝ่ายการเมือง ในสำนักคณะรัฐมนตรี พ.ศ.2497 พล.ต.อ.เผ่า ศรียานนท์ อธิบดีกรมตำรวจ ดำรงตำแหน่งอธิบดีกรมประมวลราชการแผ่นดินคนแรก โดยนำตำรวจสันติบาลและแกนนำเสรีไทยสายสหรัฐฯ มาดำรงตำแหน่งสำคัญ

วิสัยทัศน์

“เป็นหน่วยข่าวกรองสมัยใหม่ เพื่อความมั่นคงของชาติ และประชาชน”

พันธกิจ

1. เป็นหน่วยงานหลักในการปฏิบัติงานข่าวกรอง ต่อต้านข่าวกรองในประเทศและต่างประเทศ ข่าวกรองทางการสื่อสาร
2. พัฒนาและส่งเสริมมาตรฐานการรักษาความปลอดภัยหน่วยงานรัฐฝ่ายพลเรือน
3. เป็นศูนย์กลางบูรณาการงานข่าวกรองของชาติ
4. เสริมสร้างศักยภาพขององค์กรให้ทันสมัย และบุคลากรเป็นมืออาชีพ
5. การบริหารงานอย่างมีประสิทธิภาพและธรรมาภิบาล

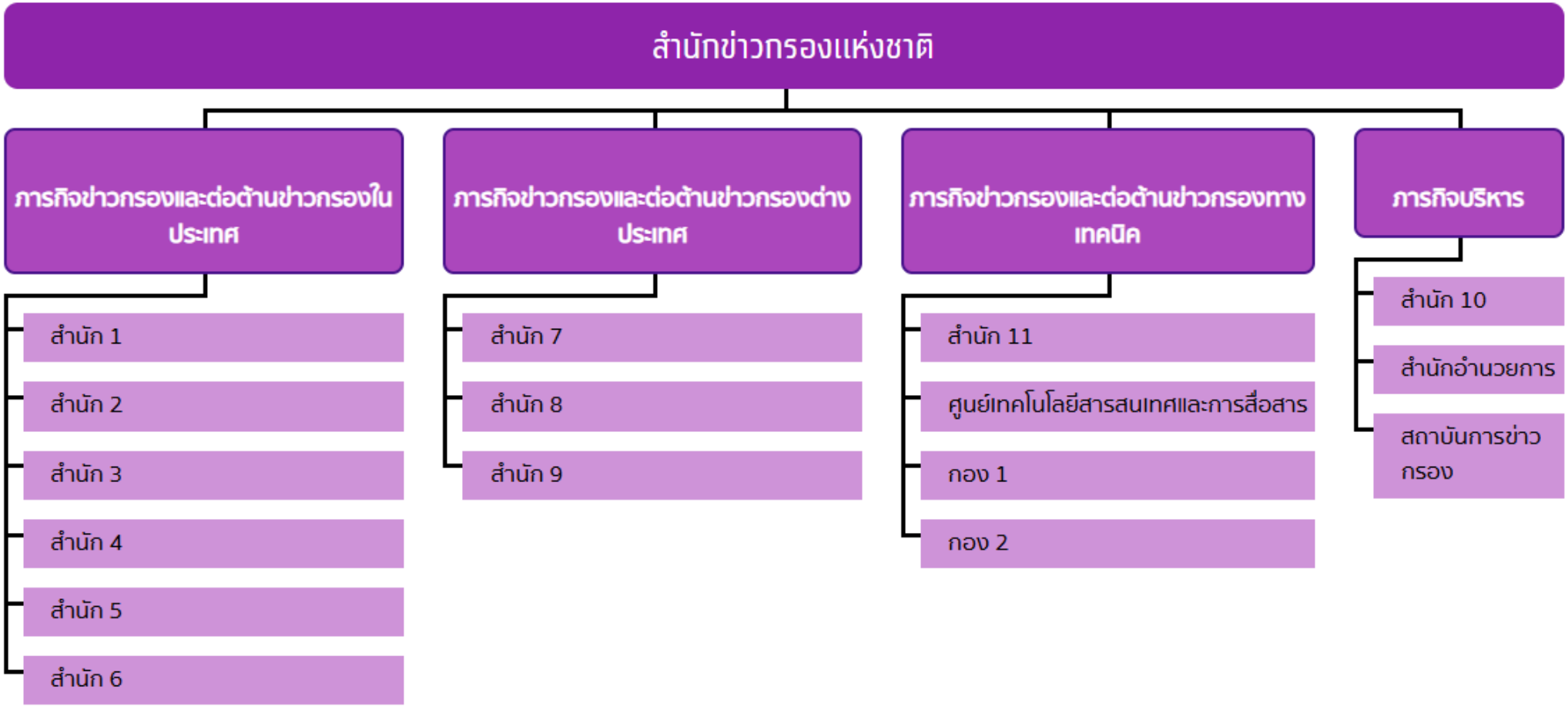
<u>อำนาจหน้าที่ของสำนักข่าวกรองแห่งชาติ</u>

กำหนดไว้ในกฎหมายและระเบียบหลายฉบับ ดังนี้

- มาตรา 5 ของพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552
- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

สรุปรวมกันได้ดังต่อไปนี้

1. ปฏิบัติงานเกี่ยวกับกิจการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสารและการรักษาความปลอดภัยฝ่ายพลเรือน
2. ติดตามสถานการณ์ภายในประเทศและต่างประเทศ ที่มีผลกระทบต่อความมั่นคงแห่งชาติและรายงานตรงต่อนายกรัฐมนตรีและสภาความมั่นคงแห่งชาติและกระจายข่าวกรองที่มีผลกระทบต่อความมั่นคงแห่งชาติให้หน่วยงานของรัฐ หรือรัฐวิสาหกิจที่เกี่ยวข้องใช้ประโยชน์ตามความเหมาะสม
3. ศึกษา วิจัยและพัฒนา เกี่ยวกับกิจการการข่าวกรอง การต่อต้านข่าวกรองและการรักษาความปลอดภัยฝ่ายพลเรือนเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน
4. เป็นศูนย์กลางประสานกิจการข่าวกรอง การต่อต้านข่าวกรอง กับหน่วยงานอื่นทั้งในประเทศและต่างประเทศ และเป็นองค์การรักษาความปลอดภัยฝ่ายพลเรือน ทำหน้าที่เป็นประธานคณะที่ปรึกษาการข่าว และรับผิดชอบการบริหารจัดการศูนย์ประสานข่าวกรองแห่งชาติ
5. เสนอแนะนโยบายและมาตรการ ตลอดจนให้คำแนะนำ และคำปรึกษาด้านการข่าวกรองการต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนต่อนายกรัฐมนตรี สภาความมั่นคงแห่งชาติ หน่วยงานราชการและรัฐวิสาหกิจ


สำนักข่าวกรองแห่งชาติ
ภารกิจข่าวกรองและต่อต้านข่าวกรองในประเทศ
สำนัก 1
สำนัก 2
สำนัก 3
สำนัก 4
สำนัก 5
สำนัก 6
ภารกิจข่าวกรองและต่อต้านข่าวกรองต่างประเทศ
สำนัก 7
สำนัก 8
สำนัก 9
ภารกิจข่าวกรองและต่อต้านข่าวกรองทางเทคนิค
สำนัก 11
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กอง 1
กอง 2
ภารกิจบริหาร
สำนัก 10
สำนักอำนวยการ
สถาบันการข่าวกรอง


รู้จัก สขช. ใน 2 นาที
สวัสดีเราทำงาน สำนักข่าวกรองแห่งชาติ ชื่อย่อ สขช.
นายธนากร บัวรัษฎ์ เป็นผู้อำนวยการสำนักข่าวกรองแห่งชาติ คนปัจจุบัน
สขช.ก่อตั้งปี 2497 ตอนนั้นเรียก "กรมประมวลราชการแผ่นดิน" ปี 2502 เปลี่ยนชื่อเป็น "กรมประมวลข่าวกลาง
ต่อมาปี 2528 เปลี่ยนชื่อเป็น "สำนักข่าวกรองแห่งชาติ"
ปี 2562 สขช. ปรับปรุงกฎหมาย เพื่อเหตุผลในการปฏิบัติหน้าที่ของ สขช. จึงเกิด "พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562 อำนาจหน้าที่ สขช. เป็นไปตามที่เขียนไว้ใน พ.ร.บ.ฉบับนี้
เราทำงานภาคสนาม เฝ้าระวังสถานการณ์ ให้ประเทศชาติ และประชาชนปลอดภัย
เราติดตามข่าวสารต่างประเทศ วิเคราะห์ ประเมิน ให้ผู้กำหนดนโยบายใช้ประโยชน์
เรามีทีมไซเบอร์คอยป้องกัน การโจมตีทางไซเบอร์ของผู้ไม่หวังดี เข้ามาทำลายโครงสร้างพื้นฐาน มาเอาข้อมูลรั่วไหลไปปล่อย
เราเป็น "แกนกลาง" คนในแวดวงข่าวกรองในประเทศ และ "เป็นหลัก" ในการทำงาน ข่าวกรองต่างประเทศ
ทั้งหมด เพื่อชาติ เพื่อความปลอดภัย และ เพื่อความสุขของประชาชน

ความรู้ด้านเทคโนโลยีกับการออกแบบและการดูแลระบบด้านความมั่นคงปลอดภัย

➢การออกแบบเทคโนโลยี

เทคโนโลยี หมายถึง การประยุกต์เอาความรู้ทางด้านวิทยาศาสตร์ มาใช้ให้เกิดประโยชน์และเป็นหัวใจของการสร้างมูลค่าเพิ่มให้กับสินค้าและผลิตภัณฑ์

เช่น การนำทรายซึ่งเป็นสารประกอบของซิลิกอนที่มีราคาต่ำ มาสกัดเอาสารซิลิกอนให้บริสุทธิ์และเจือสารบางอย่างให้เกิดเป็นสิ่งที่เรียกว่าสารกึ่งตัวนำ นำมาผลิตเป็นทรานซิสเตอร์และไอซี ซึ่งไอซีนี้เป็นอุปกรณ์ที่รวมวงจรอิเล็กทรอนิกส์จำนวนมากไว้ด้วยกัน ใช้ทำชิพ ซึ่งเป็นส่วนสำคัญของคอมพิวเตอร์ ทำให้มีราคาสูงเทคโนโลยีจึงเป็นหนทางที่จะช่วยพัฒนาให้สินค้าและบริการต่าง ๆมีมูลค่าเพิ่มขึ้น

➢เทคโนโลยี คืออะไร

เทคโนโลยี (Technology) คือ การใช้ความรู้ เครื่องมือ ความคิด หลักการ เทคนิค ความรู้ ระเบียบวิธี กระบวนการตลอดจน ผลงานทางวิทยาศาสตร์ทั้งสิ่งประดิษฐ์และวิธีการ มาประยุกต์ใช้ในระบบงานเพื่อช่วยให้เกิดการเปลี่ยนแปลงในการทำงานให้ดียิ่ง ขึ้นและเพื่อเพิ่มประสิทธิภาพและประสิทธิผลของงานให้มีมากยิ่งขึ้น

Technology

การนำเทคโนโลยีมาใช้กับงานในสาขาใดสาขาหนึ่งนั้นเทคโนโลยี มีความสำคัญ 3 ประการ คือ

1.ประสิทธิภาพ (Efficiency) เทคโนโลยีจะช่วยให้การทำงานบรรลุผลตามเป้าหมายได้ เที่ยงตรงและรวดเร็ว

2.ประสิทธิผล (Productivity) เกิดผลผลิตเต็มที่ ได้ประสิทธิผลสูงสุด

3.ประหยัด (Economy) ประหยัดทั้งเวลาและแรงงาน ลงทุนน้อยแต่ได้ผลมาก

➢ความสำคัญของเทคโนโลยี

1.เป็นพื้นฐานปัจจัยจำเป็นในการดำเนินชีวิตของมนุษย์

2.เป็นปัจจัยหลักที่จะมีส่วนร่วมในการพัฒนา

3.เป็นเรื่องราวของมนุษย์ และธรรมชาติ

ในช่วงสองทศวรรษที่ผ่านมา วิทยาศาสตร์ และ เทคโนโลยี ได้มีบทบาทสำคัญเพิ่มขึ้นจนสามารถสร้างนวัตกรรม (Innovation) ซึ่งก็คือ การเรียนรู้ การผลิตและ การใช้ประโยชน์จากความคิดใหม่ ให้เกิดผลทั้งทางเศรษฐกิจ สังคม การเมือง สิ่งแวดล้อม และวัฒนธรรม เทคโนโลยีทำให้สังคมโลกที่เรียบง่าย กลายเป็นสังคมที่มีการดำรงชีวิตที่ สลับซับซ้อนมากขึ้น ก่อให้เกิดกระแสแห่งความไร้พรมแดน หรือกระแสโลกาภิวัฒน์ ที่เข้ามาสู่ทุกประเทศอย่าง รวดเร็ว จากความก้าวหน้าของเทคโนโลยีสารสนเทศ อันเป็นการผสมผสาน 4 ศาสตร์ เข้าด้วยกัน ได้แก่ อิเล็กทรอนิกส์ โทรคมนาคม และข่าวสาร (Electronics , Computer , Telecommunication and Information หรือเรียกย่อๆ ว่า ECTI) ทำให้สังคมโลกสามารถสื่อสารกันได้ทุกแห่งทั่วโลกอย่างรวดเร็ว สามารถรับรู้ข่าวสารความเคลื่อนไหวต่างๆ ได้พร้อมกัน สามารถบริหารจัดการและตัดสินใจได้ทุกขณะเวลา การลงทุนค้าขาย และธุรกรรมการเงินได้อย่างรวดเร็ว ดังนั้น เทคโนโลยี กำลังทำให้โลกใบนี้ “เล็กลง” ทุกขณะ

➢**การสร้างสิ่งของใช้ด้วยกระบวนการเทคโนโลยี**

กระบวนการเทคโนโลยี หมายถึง กระบวนการบริหารจัดการสร้างหรือผลิตชิ้นงานและซ่อมแซมปรับปรุงแก้ไขชิ้นงานให้มีสภาพการใช้งานได้เป็นอย่างดี ซึ่งเป็นการนำเอาวิทยาการทางศิลปะและวิทยาศาสตร์มาประยุกต์ใช้ให้เกิดประโยชน์กับการทำวานถูกต้องและปลอดภัย เพื่อพัฒนาคุณภาพชีวิตของมนุษย์ให้ดียิ่งขึ้น

➢**องค์ประกอบของกระบวนการเทคโนโลยี**

กระบวนการเทคโนโลยีเป็นขั้นตอนในการแก้ปัญหา ทำให้การเป็นไปอย่างมีระบบและมีลำดับขั้นตอน สามารถย้อนกลับไปแก้ไขปรับปรุงได้ง่าย ประกอบด้วยขั้นตอนต่างๆ ดังนี้

1.การกำหนดปัญหาหรือความต้องการ

2.การรวบรวมข้อมูล

3.การเลือกวิธีแก้ไขปัญหาหรือสนองความต้องการ

4.การออกแบบและปฏิบัติการแก้ไขปัญหา

5.การทดสอบ

6.การปรับปรุงแก้ไข

7.การประเมินผล

➢**การออกแบบเทคโนโลยี**

การออกแบบเทคโนโลยี เป็นการออกแบบ เขียนแบบ สร้างหรือผลิตชิ้นงานต่างๆ โดย ผ่านกระบวนการออกแบบที่แสดงให้เห็นถึงความเข้าใจในองค์ประกอบผลหรือผลิตภัณฑ์ที่มีความสมบูรณ์ในตนเอง มีความสวยงาม มีประโยชน์ในการใช้สอย ราคาประหยัด และไม่ทำลายสิ่งแวดล้อม สามารถนำมาใช้ยกระดับมาตรฐานคุณภาพชีวิตให้สูงขึ้นได้ทุกระดับ เช่นอาคาร ที่พักอาศัย โทรศัพท์ โทรทัศน์ พัดลม ตู้เย็น และสิ่งอำนวยความสะดวกอื่นๆ เพื่อให้ดำรงชีวิตประจำวันได้อย่างมีความสุข

➢**กระบวนการออกแบบ**

1.วัตถุประสงค์ การระบุความต้องการหรือวัตถุประสงค์เงื่อนไขที่กำหนด

2.การสำรวจ การสำรวจข้อมูลข่าวสารเพื่อนำมาใช้เป็นข้อมูล

3.กระบวนการสร้างความคิด การร่างภาพ การร่างแบบ ลำดับแนวคิดที่มีโอกาสเป็นในการออกแบบหรือหาคำตอบ อาจใช้หุ่นจำลองตรวจสอบแนวคิดที่ดีที่เหมาะสม

4.เลือกแนวความคิด การเลือกแนวความคิดที่ดี ที่เหมาะสมเพื่อนำไปใช้ในการออกแบบ เขียนแบบ และกำหนดรายการประกอบแบบต่อไป

5.วางแผนลงมือปฏิบัติงาน การตัดสินใจการออกแบบ เขียนแบบ เลือกเครื่องมือ เครื่องใช้ วัสดุอุปกรณ์ และกระบวนการทำงานที่เหมาะสม กำหนดเวลา สถานที่ทำงาน กระบวนการปฏิบัติงาน

6.การประเมินค่า การตรวจสอบประเมินค่าความสำเร็จของผลงาน คือ แบบการสร้างชิ้นงาน ผลิตภัณฑ์หรือสิ่งของ เครื่องใช้ว่ามีค่าอยู่ระดับใด ควรจะต้องพัฒนาไปอย่างไร เพื่อให้ได้ผลงานสมบูรณ์ยิ่งๆขึ้นไป

➢**ความหมายของการออกแบบ**

ความหมายของการออกแบบ การออกแบบ คืออะไร ซึ่งความหมายของคำว่า “ออกแบบ” นั้นถูกให้คำนิยาม หรือคำจำกัดความ ไว้หลายรูปแบบมากมาย ตามความเข้าใจ การตีความหมาย และการสื่อสารออกมาด้วยตัวอักษรของแต่ละคน ตัวอย่างความหมายของการออกแบบ เช่น

– การออกแบบ หมายถึง การรู้จักวางแผนจัดตั้งขั้นตอน และรู้จักเลือกใช้วัสดุวิธีการเพื่อทำตามที่ต้องการนั้น โดยให้สอดคล้องกับลักษณะรูปแบบ และคุณสมบัติของวัสดุแต่ละชนิด ตามความคิดสร้างสรรค์ และการสร้างสรรค์สิ่งใหม่ขึ้นมา เช่น การจะทำโต๊ะขึ้นมาซักหนึ่งตัว เราจะต้องวางแผนไว้เป็นขั้นตอน โดยต้องเริ่มต้นจากการเลือกวัสดุที่จะใช้ในการทำโต๊ะนั้น ว่าจะใช้วัสดุอะไรที่เหมาะสม ในการยึดต่อระหว่างจุดต่างๆนั้นควรใช้กาว ตะปู สกรู หรือใช้ข้อต่อแบบใด รู้ถึงวัตถุประสงค์ของการนำไปใช้งาน ความแข็งแรงและการรองรับน้ำหนักของโต๊ะสามารถรองรับได้มากน้อยเพียงใด สีสันควรใช้สีอะไรจึงจะสวยงาม เป็นต้น

– การออกแบบ หมายถึง การปรับปรุงแบบ ผลงานหรือสิ่งต่างๆ ที่มีอยู่แล้วให้เหมาะสม และดูมีความแปลกใหม่ขึ้น เช่น โต๊ะที่เราทำขึ้นมาใช้ เมื่อใช้ไปนานๆก็เกิดความเบื่อหน่ายในรูปทรง หรือสี เราก็จัดการปรับปรุงให้เป็น รูปแบบใหม่ให้สวยกว่าเดิม ทั้งความเหมาะสม ความสะดวกสบายในการใช้งานยังคงเหมือนเดิมหรือดีกว่าเดิม เป็นต้น

– การออกแบบ หมายถึง การรวบรวมหรือการจัดองค์ประกอบทั้งที่เป็น 2 มิติ และ 3 มิติ เข้าด้วยกันอย่างมีหลักเกณฑ์ การนำองค์ประกอบของการออกแบบมาจัดรวมกันนั้น ผู้ออกแบบจะต้องคำนึงถึงประโยชน์ในการใช้สอยและความสวยงาม อันเป็นคุณลักษณะสำคัญของการออกแบบ เป็นศิลปะของมนุษย์เนื่องจากเป็นการสร้างค่านิยมทางความงาม และสนองคุณประโยชน์ทางกายภาพให้แก่มนุษย์ด้วย

– การออกแบบ หมายถึง กระบวนการที่สนองความต้องการในสิ่งใหม่ๆของมนุษย์ ซึ่งส่วนใหญ่เพื่อการดำรงชีวิตให้อยู่รอด และสร้างความสะดวกสบายมากยิ่งขึ้น

การออกแบบ (Design) คือศาสตร์แห่งความคิด และต้องใช้ศิลป์ร่วมด้วย เป็นการสร้างสรรค์ และการแก้ไขปัญหาที่มีอยู่ เพื่อสนองต่อจุดมุ่งหมาย และนำกลับมาใช้งานได้อย่างน่าพอใจ ความน่าพอใจนั้น แบ่งออกเป็น 3 ข้อหลักๆ ได้ดังนี้

1. ความสวยงาม เป็นสิ่งแรกที่เราได้สัมผัสก่อน คนเราแต่ละคนต่างมีความรับรู้เรื่อง ความสวยงาม กับความพอใจ ในทั้ง 2 เรื่องนี้ไม่เท่ากัน จึงเป็นสิ่งที่ถกเถียงกันอย่างมาก และไม่มีเกณฑ์ ในการตัดสินใดๆ เป็นตัวที่กำหนดอย่างชัดเจน ดังนั้นงานที่เราได้มีการจัดองค์ประกอบที่เหมาะสมนั้น ก็จะมองว่าสวยงามได้เหมือนกัน

2. มีประโยชน์ใช้สอยที่ดี เป็นเรื่องที่สำคัญมากในงานออกแบบทุกประเภท เช่นถ้าเป็นการออกแบบสิ่งของ เช่น เก้าอี้,โซฟา นั้นจะต้องออกแบบมาให้นั่งสบาย ไม่ปวดเมื่อย ถ้าเป็นงานกราฟฟิค เช่น งานสื่อสิ่งพิมพ์นั้น ตัวหนังสือจะต้องอ่านง่าย เข้าใจง่าย ถึงจะได้ชื่อว่า เป็นงานออกแบบที่มีประโยชน์ใช้สอยที่ดีได้

3. มีแนวความคิดในการออกแบบที่ดี เป็นหนทางความคิด ที่ทำให้งานออกแบบสามารถตอบสนอง ต่อความรู้สึกพอใจ ชื่นชม มีคุณค่า บางคนอาจให้ความสำคัญมากหรือน้อย หรืออาจไม่ให้ความสำคัญเลยก็ได้ ดังนั้นบางครั้งในการออกแบบ โดยใช้แนวความคิดที่ดี อาจจะทำให้ผลงาน หรือสิ่งที่ออกแบบมีคุณค่ามากขึ้นก็ได้

ดังนั้นนักออกแบบ (Designer) คือ ผู้ที่พยายามค้นหา และสร้างสรรค์สิ่งใหม่ หาวิธีแก้ไข หรือหาคำตอบใหม่ๆสำหรับปัญหาต่างๆ

การดูแลระบบด้านความมั่นคงปลอดภัย

➢ความหมายและหลักการรักษาความมั่นคงปลอดภัย

เมื่อกล่าวถึงการรักษาความมั่นคงปลอดภัย สิ่งที่ผู้คนโดยทั่วไปคำนึงถึงเป็นสิ่งแรก คือ การค้นหาการบุกรุกของผู้ไม่ประสงค์ดีกับระบบคอมพิวเตอร์ซึ่งนิยมเรียกว่า “แฮกเกอร์” รวมถึงการกำจัดโปรแกรมที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของคอมพิวเตอร์ หรือมัลแวร์ประเภทต่างๆ โดยไม่ตระหนักรู้ถึงความหมายที่แท้จริงของ “ความมั่นคงปลอดภัย” ของระบบคอมพิวเตอร์ ซึ่งแท้จริงแล้วมีความหมายครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรในระบบคอมพิวเตอร์ในทุกๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการ ซอฟต์แวร์ต่างๆ ที่ถูกติดตั้ง และการเชื่อมต่อกันเป็นเครือข่าย และรวมถึงข้อมูลหรือสารสนเทศซึ่งถูกจัดเก็บและประมวลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อเป็นระบบ ความหมายของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์จึงมีขอบเขตมากกว่าการรักษาความมั่นคงปลอดภัยให้กับคอมพิวเตอร์หรืออุปกรณ์เพียงอย่างเดียว

1. ทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศ มีความหมายครอบคลุมถึงเครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อต่าง ๆ และครอบคลุมถึงองค์ประกอบอื่นๆ ดังต่อไปนี้

1.1 มนุษย์ (people) ได้แก่ ผู้ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ เช่น ผู้ใช้งาน ผู้ดูแลระบบ ทั้งนี้โดยปกติแล้วมนุษย์จะถูกประเมินเป็นภัยคุกคามหลักต่อทรัพยากรสารสนเทศเนื่องจากมีเป็นทรัพยากรที่เป็นมีจุดอ่อนมากที่สุดในการรักษาความมั่นคงปลอดภัย แม้ว่าทรัพยากรอื่นๆ จะถูกปกป้องและกำหนดมาตรการอย่างรัดกุมที่สุดแล้ว หากผู้คนที่เกี่ยวข้องกับทรัพยากรนั้นละเลยหรือขาดความตระหนักรู้ก็จะส่งผลให้ทรัพยากรนั้นถูกโจมตีสำเร็จ เช่น การให้บริการรับฝากไฟล์ผ่านอินเทอร์เน็ตซึ่งเลือกใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยที่เข้มแข็งมาก แต่ผู้ใช้งานบันทึกข้อมูลสำหรับใช้พิสูจน์ตัวจริงและกำหนดสิทธิ์โดยเขียนลงบนกระดาษแปะไว้ที่หน้าจอมอนิเตอร์ ย่อมเป็นการเพิ่มความเสี่ยงที่จะมีผู้ไม่ประสงค์ดีใช้ข้อมูลดังกล่าวเข้าถึงข้อมูลที่ถูกจัดเก็บในระบบนั้น โดยอาจเปลี่ยนแปลง แก้ไข หรือลบข้อมูลนั้นโดยไม่ได้รับอนุญาต เป็นต้น นอกจากนี้มนุษย์ยังเป็นองค์ประกอบสำคัญของการโจมตีความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ด้วยเหตุจูงใจที่หลากหลาย เช่น ความต้องการชื่อเสียง ความโลภ แนวทางทางการเมืองโดยเมื่อโจมตีสำเร็จอาจได้รับค่าจ้างหรือการยอมรับจากสังคมที่เขาต้องการ เป็นต้น

1.2 ฮาร์ดแวร์และอุปกรณ์ต่อเชื่อมต่าง ๆ (hardware and its peripheral) ในที่นี้มีความหมาย รวมถึงเครื่องคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟนซึ่งมีความสามารถในการรับข้อมูล ประมวลผล แสดงผลและเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ได้ ความไม่มั่นคงปลอดภัยของอุปกรณ์เหล่านี้อาจเกิดขึ้น เนื่องจากมีภัยคุกคามเกิดขึ้นกับอุปกรณ์โดยตรง เช่น การขโมย ซึ่งส่งผลให้เจ้าของไม่สามารถใช้งานได้หรือนำข้อมูลส่วนบุคคลในอุปกรณ์นั้นไปเปิดเผยทำให้ความลับของข้อมูลนั้นถูกทำลายลง หรืออาจเกิดจากไฟฟ้ากระชากและทำ ให้ข้อมูลที่จัดเก็บในอุปกรณ์นั้น ๆ เสียหาย นอกจากนี้ยังรวมถึงการที่ฮาร์ดแวร์นั้น ๆ ถูกทำลายหรือทำให้ใช้การไม่ได้โดยมีสาเหตุจากธรรมชาติ เช่น น้ำท่วม ฟ้าผ่าอุปกรณ์ เป็นต้น

1.3 ซอฟต์แวร์ (software) ที่ถูกพัฒนาขึ้นมักมีข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัย เนื่องจากคุณสมบัตินี้มักถูกละเลยในระหว่างขั้นตอนการวิเคราะห์และพัฒนาซอฟต์แวร์นั้นๆ ทำให้เมื่อมีการนำมาใช้งานมักจะมีช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์เราเตอร์สำหรับใช้งานอินเทอร์เน็ตสำหรับเชื่อมต่อผ่านระบบเอดีเอสแอลบางรุ่นมีข้อบกพร่องเกี่ยวกับความมั่นคงปลอดภัยและเมื่อผู้ไม่ประสงค์ดีโจมตีระบบสำเร็จจะสามารถปลอมแปลงกระบวนการสอบถามโดเมนเนมได้ เป็นต้น

ดังนั้นผู้ใช้งานหรือผู้ดูแลระบบ จะต้องดำเนินการ ปรับปรุงคุณสมบัติซอฟแวร์ตามหลังอยู่เสมอๆ ทั้งนี้การปรับปรุงคุณสมบัติดังกล่าว ผู้พัฒนาซอฟต์แวร์อาจสร้างช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยไม่ได้ตั้งใจก็เป็นได้

1.4 ข้อมูลและสารสนเทศ (data and information) เป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้สร้าง ประมวลผล และรับส่งข้อมูลสารสนเทศนั้นๆ ด้วยเหตุนี้ทรัพยากรนี้จึงเป็นเป้าหมายหลักของการโจมตีของผู้ไม่ประสงค์ดีโดยผลเสียหายที่เกิดขึ้นมักจะเกิดขึ้นในสามลักษณะสำคัญคือ การเปิดเผยความลับ การแก้ไขข้อมูลโดยไม่มีสิทธิ์ และการทำให้ข้อมูลนั้นๆ ไม่สามารถเข้าถึงได้ เช่น ถูกลบ เปลี่ยนแปลงสิทธิ์หรือถูกเข้ารหัสลับเพื่อเรียกค่าไถ่ เป็นต้น

1.5 ขั้นตอนระเบียบวิธีปฏิบัติ (procedure) ขั้นตอนการดำเนินการกับข้อมูลมักถูกละเลยจากผู้ที่เกี่ยวข้องทำให้มีช่องโหว่ที่อาจทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้ เช่น องค์กรต่างๆ มักมีการฝึกอบรมพนักงานให้ดำเนินการอย่างใดอย่างหนึ่งกับซอฟต์แวร์ที่ใช้ในองค์กรในรูปแบบของคู่มือการทำงานทำให้พนักงานที่มีหน้าที่คล้ายคลึงกันสามารถใช้งานซอฟต์แวร์ได้เหมือนๆ กัน โดยมักละเลยการสร้างความตระหนักรู้เกี่ยวกับการใช้งานซอฟต์แวร์อย่างมั่นคงปลอดภัยเป็นผลให้เกิดช่องโหว่ของการรักษาความมั่นคงปลอดภัยได้ เช่น พนักงานบัญชีคนหนึ่งอาจเข้าใช้งานระบบเงินเดือนค้างไว้โดยไม่ได้ล็อกหน้าจอขณะพักรับประทานอาหารกลางวัน ผู้ไม่ประสงค์ดีอาจเข้าใช้งานซอฟต์แวร์และปรับเปลี่ยนข้อมูลในระบบบัญชีได้ เป็นต้น

1.6 เครือข่าย (network) ระบบสารสนเทศในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่ายการรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และมักเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตแม้ว่าการเชื่อมต่อกันดังที่ได้กล่าวมาจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจากระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่าย ยิ่งมีขนาดมากเท่าไรย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตี และเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้น

เมื่อกล่าวโดยนัยแล้วจะเห็นว่า ทรัพยากรสารสนเทศมีองค์ประกอบสำคัญๆ ดังที่ได้กล่าวมา อย่างไรก็ดีทรัพยากรสารสนเทศอาจถูกนิยามได้ในความหมายที่ใกล้เคียงกันแต่ถูกนิยามขึ้นมาในระยะเริ่มต้น คือ ระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ มนุษย์ และข้อมูล ซึ่งจะขาดองค์ประกอบสำคัญคือ เครือข่ายและขั้นตอนวิธีปฏิบัติซึ่งเป็นองค์ประกอบที่สำคัญในปัจจุบัน เนื่องจากการประยุกต์ใช้งานเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบันมีการแลกเปลี่ยนทรัพยากรกันผ่านช่องทางการสื่อสารและระบบเครือข่าย ตลอดจนการประมวลผลข้อมูลในปัจจุบันมีความซับซ้อนมากขึ้นกว่าในอดีต ดังนั้นเมื่อกล่าวถึงระบบคอมพิวเตอร์ในปัจจุบันจึงนิยมใช้คำว่าทรัพยากรสารสนเทศซึ่งมีความหมายครอบคลุมถึงทรัพยากรเครือข่ายและขั้นตอนวิธีปฏิบัติที่เกี่ยวข้อง

2. การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัย หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้นๆ ในที่นี้จะยกตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลซึ่งอาจมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่างๆ ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ไม่ให้ถูกทำลายโดยมัลแวร์[1] และป้องกันการแพร่ระบาดของหนอนอินเทอร์เน็ต[2] ซึ่งอาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ นักศึกษาอาจพิจารณาตั้งพาสเวิร์ดเพื่อควบคุมการเข้าถึงเข้าถึงเครื่องคอมพิวเตอร์ จัดการเข้ารหัสลับฮาร์ดดิสก์ ติดตั้งซอฟต์แวร์ตรวจจับคอมพิวเตอร์ไวรัส และเปิดการใช้งานไฟร์วอลล์ส่วนบุคคล[3] เป็นต้น โดยทั่วไปการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศสามารถจำแนกตามเป้าหมายของการรักษาความมั่นคงปลอดภัยได้ดังต่อไปนี้

2.1 ความมั่นคงปลอดภัยเชิงกายภาพ (physical security) เพื่อป้องกันอุปกรณ์ สิ่งของ หรือบริเวณให้ปราศจากการเข้าถึงโดยไม่ได้รับอนุญาต และการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล สร้างห้องปฏิบัติการสำหรับระบบคอมพิวเตอร์และเครือข่าย การจัดให้มีระบบไฟสำรอง การจัดให้มีระบบดับเพลิง การจัดให้มีการพิสูจน์ตัวจริงก่อนเข้าถึงฮาร์ดแวร์หรือห้องที่ใช้จัดเก็บฮาร์ดแวร์ตลอดจนทรัพยากรเครือข่ายที่เกี่ยวข้อง เป็นต้น

2.2 ความมั่นคงปลอดภัยส่วนบุคคล (personnel security) เพื่อรักษาบุคลากร หรือกลุ่มของผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงและดำเนินงานได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรับผิดชอบ โดยกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้างานของตนเอง แต่สามารถแก้ไขและตรวจสอบผู้ทำการแก้ไขทรัพยากรนั้นๆ ได้ การบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าสู่ระบบในครั้งแรกและทุกๆ สามเดือน เป็นต้น

2.3 ความมั่นคงปลอดภัยของการดำเนินงาน (operation security) เพื่อปกป้องหรือป้องกันกระบวนการทำงาน ตลอดจนกิจกรรมอื่นๆ ที่เกี่ยวข้อง เช่น สหกรณ์ออมทรัพย์ควรการจัดให้มีกลไกการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลที่จัดเก็บ ประมวลผล เมื่อสมาชิกดำเนินธุรกรรมกับสหกรณ์การกำหนดห้ามเจ้าหน้าที่เขียนรหัสผ่านสำหรับเข้าใช้งานระบบลงบนกระดาษ หรือการตรวจสอบสิทธิ์ในการเข้าถึงทรัพยากรก่อนการเข้าถึง การทำให้มั่นใจได้ว่าเอกสารลับถูกจัดเก็บหรือทำลายตามที่กำหนดในนโยบายการรักษาความมั่นคงปลอดภัย เป็นต้น

---

[1] มัลแวร์ (malware) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบให้โจมตีต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ แบ่งเป็นหลายชนิดขึ้นอยู่กับลักษณะเฉพาะของซอฟต์แวร์นั้น ๆ เช่น คอมพิวเตอร์ไวรัส หนอนอินเทอร์เน็ต โทรจัน เป็นต้น

[2] หนอนอินเทอร์เน็ต (worms) หมายถึง มัลแวร์หรือซอฟต์แวร์ไม่พึงประสงค์ประเภทหนึ่งที่แพร่กระจายตัวเองผ่านเครือข่ายคอมพิวเตอร์ โดยใช้ประโยชน์จากช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของซอฟต์แวร์หรือบริการต่างๆ เช่น ช่องโหว่ของการแชร์ไฟล์ร่วมกันของระบบปฏิบัติการ เป็นต้น

[3] ไฟร์วอลล์ส่วนบุคคล (personal firewall) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทำหน้าที่ป้องกันคอมพิวเตอร์เครื่องนั้นจากการโจมตีทางเครือข่ายด้วยการวิเคราะห์ข้อมูลที่เข้าและออกจากคอมพิวเตอร์นั้นๆ

2.4 ความมั่นคงปลอดภัยของการสื่อสาร (communication security) เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่าง ๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขาซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้ เป็นต้น

2.5 ความมั่นคงปลอดภัยของเครือข่าย (network security) เพื่อป้องกันการเข้าถึงอุปกรณ์เครือข่ายต่าง ๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อย ๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่าง ๆ รวมถึงการจัดให้มีการเฝ้าตรวจความมั่นคงปลอดภัย และการจัดให้มีการพิสูจน์ตัวจริงของผู้ใช้งานก่อนจึงจะสามารถใช้งานเครือข่ายได้ จะเห็นได้ว่ามีความแตกต่างจากความมั่นคงปลอดภัยของการสื่อสาร โดยมีขอบเขตที่แคบกว่าและพิจารณาที่การเชื่อมต่อในบริเวณที่เกี่ยวข้อง เช่น ระบบเครือข่ายภายในบ้าน ระบบเครือข่ายภายในบริษัท เป็นต้น

2.6 ความมั่นคงปลอดภัยของข้อมูลข่าวสาร (information security) เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ขององค์ประกอบต่างๆ ที่ถูกผนวกรวมเข้าเป็นระบบสารสนเทศ นับตั้งแต่กระบวนการสร้าง ประมวลผล และการรับส่งสารสนเทศนั้นๆ

3. หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประกอบด้วย 2 หลักการ ได้แก่ หลักการพื้นฐาน และหลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.1 หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กรหรือบุคคลนั้น ๆ ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริมสร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้ และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม

3.1.1 การรักษาความลับ (confidentiality) หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญเช่น ข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ข้อมูลส่วนบุคคลอื่น ๆ เช่น หมายเลขประจำตัวประชาชน กำหนดการของบุคคลสำคัญ รายชื่อผู้โดยสารของเที่ยวบินต่าง ๆ เป็นต้น

3.1.2 การรักษาความครบถ้วนสมบูรณ์ (integrity) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความถูกต้องสมบูรณ์ และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้ เช่น หากมีการแก้ไขไฟล์ที่ถูกสร้างขึ้นแล้วมีการส่งผ่านไฟล์นั้นเข้าสู่เครือข่ายคอมพิวเตอร์ ผู้ที่เกี่ยวข้องจะต้องสามารถตรวจสอบได้ว่าไฟล์นั้นว่าถูกแก้ไขเปลี่ยนแปลงไประหว่างการส่งผ่านช่องทางการสื่อสารหรือไม่ เป็นต้น

3.1.3 การรักษาความพร้อมใช้ (availability) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้นๆ สามารถเข้าใช้งานได้ เช่น เมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์ อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น

ภาพ องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากภาพ จะเห็นว่าทรัพยากรสารสนเทศที่ต้องการให้มีความมั่นคงปลอดภัยนั้นอาจถูกจัดเก็บอยู่ในฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) หรือถูกส่งผ่านระบบการสื่อสาร (communication) ก็เป็นได้ และการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรสารสนเทศนั้นจะมีความเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางกายภาพ (physical security) ในทุกระดับโดยการจัดให้มีเทคโนโลยีและกระบวนการที่เหมาะสมสำหรับการเข้าถึงทางกายภาพต่อฮาร์ดแวร์ ซอฟต์แวร์ และระบบการสื่อสาร นอกจากนี้ยังมีความจำเป็นต้องสร้างการรักษาความมั่นคงปลอดภัยส่วนบุคคล (personal security) เนื่องจากมนุษย์เป็นจุดอ่อนที่สุดของระบบการรักษาความมั่นคงปลอดภัย และมักละเมิดกฎเกณฑ์ที่จำเป็น ทั้งนี้ อาจแก้ไขได้โดยการสร้างความตระหนักรู้ถึงเหตุผลและความสำคัญของการรักษาความมั่นคงปลอดภัย เป็นต้น ทั้งนี้มาตรการและเทคโนโลยีที่นำมาใช้จะต้องมีการกำหนดให้สอดคล้องกับการจัดการรักษาความมั่นคงปลอดภัยในระดับองค์กรโดยการกำหนดยุทธศาสตร์ นโยบายและกฎระเบียบที่เกี่ยวข้อง ตลอดจนมีการกำกับดูแลอย่างเหมาะสม

3.2 หลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศจึงเป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงาน และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของทรัพยากรสารสนเทศนั้น ๆ

3.2.1 ช่องโหว่ (vulnerability) คือ ความบกพร่องหรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศ โดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์ การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้น ๆ เช่น ช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของซอฟต์แวร์เว็บเบราว์เซอร์ การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญ ๆ ที่เกี่ยวข้องกับกระบวนการทำงานโดยไม่มีการตรวจสอบ หรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะดังต่อไปนี้

1) ช่องโหว่ที่เกี่ยวข้องกับฮาร์ดแวร์ หมายถึงข้อบกพร่องที่เกี่ยวข้องกับความมั่นคง ปลอดภัยของฮาร์ดแวร์ เช่น ช่องโหว่ของการเข้ารหัสของระบบขายปลีกครบวงจร (Point of Sale ; POS) ซึ่งส่งผลให้ผู้โจมตีสามารถขโมยข้อมูลบัตรเครดิตของผู้ใช้บริการ หรือช่องโหว่ของระบบสมองกลที่ใช้ควบคุมรถยนต์ที่เมื่อถูกโจมตีผ่านเครือข่ายแล้วจะทำให้ผู้โจมตีสามารถควบคุมการระบบควบคุมภายในรถยนต์คันนั้น ๆ ได้ เป็นต้น

2) ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่างๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้นๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์และซอฟต์แวร์ระบบอื่น ๆ ที่เกี่ยวข้อง เช่น ช่องโหว่ของระบบปฏิบัติการที่เกี่ยวข้องกับการแชร์ไฟล์ผ่านระบบเครือข่ายคอมพิวเตอร์ที่หากผู้ไม่ประสงค์ดีโจมตีต่อบริการแชร์ไฟล์สำเร็จอาจทำการลบโฟลเดอร์ หรือไฟล์ต่างๆ โดยไม่ได้รับอนุญาต เป็นต้น

3) ช่องโหว่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับการจัดการข้อมูลต่างๆ ทั้งที่เป็นข้อมูลที่ไม่ได้จัดเก็บในรูปแบบดิจิทัล และข้อมูลในรูปแบบดิจิทัล เช่น หากองค์กรหรือบุคคลจัดเก็บข้อมูลซึ่งใช้ในการพิสูจน์ตัวจริงอย่างไม่เหมาะสม เมื่อข้อมูลนั้นรั่วไหลออกไปอาจส่งผลให้เกิดการโจมตีต่อองค์กรนั้นๆ ได้ หรือเปิดโอกาสให้มีการโจมตีต่อทรัพยากรอื่นๆ เป็นต้น

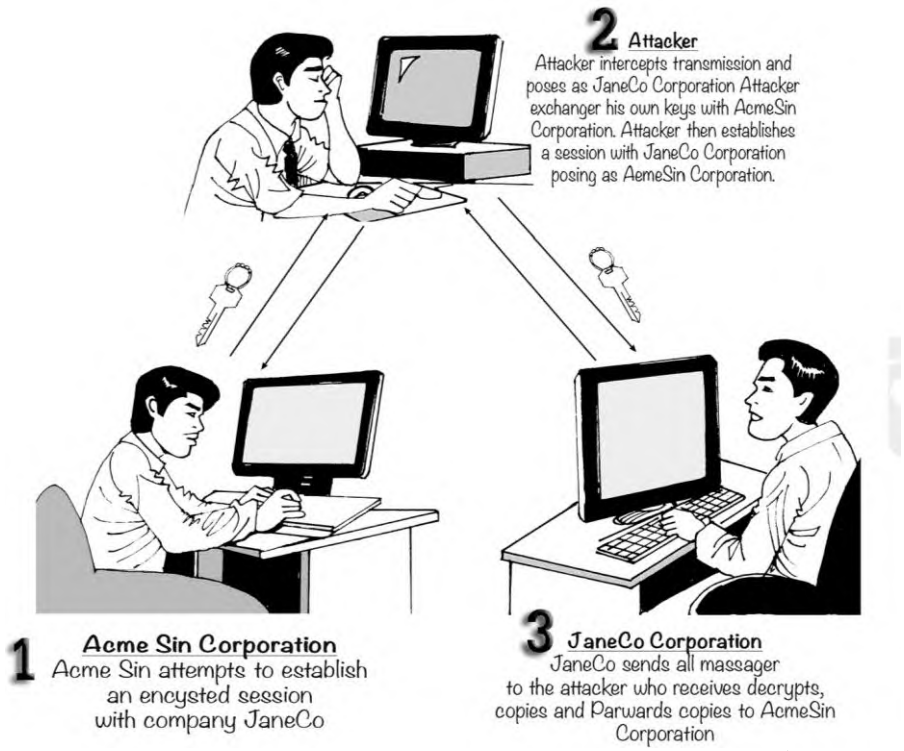
3.2.2 ภัยคุกคาม (threat) คือ บุคคลหรือผู้ใดก็ตามที่สามารถใช้ประโยชน์จากช่องโหว่ที่มีเข้าถึงและทำลายความมั่นคงปลอดภัยของทรัพยากรสารสนเทศได้ ภัยคุกคามต่อทรัพยากรสารสนเทศ จำแนกได้ 4 ลักษณะคือ

1) การดักรับ (interception) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์โดยถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง เป็นต้น

2) การขัดจังหวะ (interruption) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีกระทำแล้วส่งผลให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึง หรือใช้งานทรัพยากรนั้นๆ ได้ เช่น การตัดสายสัญญาณเครือข่าย การลบไฟล์ข้อมูล การทำลายคอมพิวเตอร์ ดังภาพด้านล่าง หรือการนำเข้าข้อความที่ระบบประมวลผลแล้วทำให้ระบบปฏิเสธการให้บริการ เป็นต้น

ภาพที่ การทำลายคอมพิวเตอร์ส่งผลให้ผู้มีสิทธิ์ใช้งานไม่สามารถใช้งานได้

3) การดัดแปลงแก้ไข (modification) หมายถึง การเข้าถึงและแก้ไขทรัพยากรสารสนเทศโดยไม่มีสิทธิ์ เช่น การเปลี่ยนแปลงการปรับตั้งค่าต่างๆ ของระบบปฏิบัติการ การอนุญาตให้มีการเข้าถึงจากระยะไกลโดยไม่มีการพิสูจน์ตัวจริง ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัย การดักรับโดยการเปลี่ยนเส้นทางและการเปลี่ยนแปลงข้อมูลที่ถูกรับส่งผ่านเครือข่าย ดังแสดงในภาพด้านล่างนี้ เป็นต้น โดยการดัดแปลงแก้ไขดังกล่าวอาจกระทำได้ในกรณีอื่นๆ เช่น เพื่อนของนักศึกษาอาจแก้ไขไฟล์รายงานของนักศึกษาที่ถูกบันทึกไว้ในสื่อจัดเก็บข้อมูล เช่น แฟลชไดฟร์โดยที่นักศึกษาไม่ทราบ เมื่อนักศึกษาส่งรายงานไปยังอาจารย์จึงพบว่าข้อมูลนั้นไม่ใช่ข้อมูลที่ถูกต้อง เป็นต้น



ภาพ การโจมตีที่มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่มีสิทธิ์

4) การปลอมแปลง (fabrication) หมายถึง การสร้างข้อมูลหรือสิ่งแปลกปลอมเข้าสู่ระบบสารสนเทศ เช่น การเพิ่มข้อมูลลงในระบบจัดการฐานข้อมูล การตั้งเครือข่ายไร้สายที่มีชื่อสถานีเหมือนกับเครือข่ายเป้าหมาย เพื่อดักรับข้อมูลต่างๆ และการปลอมแปลงหมายเลขไอพีเพื่อหลบเลี่ยงกลไกพิสูจน์ตัวจริงเพื่อเข้าใช้งานเครือข่าย การปลอมแปลงตนเองเป็นบุคคลอื่นเพื่อหลอกถามข้อมูลดังที่แสดงในภาพด้านล่างนี้ เป็นต้น วัตถุประสงค์หลักของการปลอมแปลงจึงเกี่ยวข้องกับการล่อลวงให้เหยื่อเข้าใจผิดว่าข้อมูลหรือสารสนเทศนั้นเป็นข้อมูลหรือตัวตนจริงๆ ของผู้นั้น หากเหยื่อตายใจและให้ข้อมูลหรือเปิดเผยข้อมูลสำคัญจะทำให้เกิดการละเมิดความมั่นคงปลอดภัยต่อเหยื่อนั้นๆ เช่น การส่งจดหมายโดยอ้างว่าผู้ส่งเป็นหัวหน้างานและให้ส่งความลับขององค์กรไปยังอีเมล หรือให้จัดพิมพ์เอกสารแล้วส่งไปยังผู้โจมตี เป็นต้น

ภาพ การปลอมแปลง

3.2.3 การโจมตี (attack) คือ การกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่าง ๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียงอย่างเดียวก็เป็นได้ เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่ อันเป็นการทำลายความลับของทรัพยากรนั้นๆ ทั้งนี้ การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือ การโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการ และการโจมตีด้วยเทคนิคเชิงสังคมอื่น ๆ เช่น การแอบอ้างเป็นพนักงานคอลเซนเตอร์เพื่อล่อลวงเป้าหมายให้กระทำการอย่างใดอย่างหนึ่งโดยเปิดเผยข้อมูลพิสูจน์ตัวจริง หรือการหลอกลวงให้ทำรายการบัญชีผ่านเอทีเอ็ม เป็นต้น

3.2.4 ผู้ไม่ประสงค์ดี (attacker) คือ บุคคลหรือกระบวนการที่เกิดขึ้นจากมนุษย์เพื่อกระทำการโจมตีต่อทรัพยากรสารสนเทศเป้าหมาย จากนิยามดังกล่าวจะเห็นได้ว่ามีความหมายใกล้เคียงกับภัยคุกคามแต่จำกัดสาเหตุไว้ที่มนุษย์เท่านั้น ซึ่งผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อระบบที่แตกต่างกันออกไปเช่น ความประมาท ค่าตอบแทน และความสะใจ เป็นต้น ในปัจจุบันนิยมใช้คำว่า แฮกเกอร์ (hacker) สามารถจำแนกประเภทจากแรงจูงใจในการโจมตีต่อระบบได้หลายลักษณะ เช่น แฮกเกอร์สมัครเล่น แฮกเกอร์หมวกขาว แฮกเกอร์หมวกดำ เป็นต้น

1) แฮกเกอร์มือสมัครเล่น (script kiddy) หมายถึง บุคคลทั่วไปที่โจมตีต่อช่องโหว่ของระบบด้วยเครื่องมือหรือซอฟต์แวร์ที่ผู้ไม่ประสงค์ดีคนอื่นเผยแพร่ไว้โดยปราศจากความเข้าใจถึงกระบวนการทำงานของซอฟต์แวร์นั้นๆ รวมไปถึงบุคคลทั่ว ๆ ไปที่ล่วงรู้ช่องโหว่ของการรักษาความมั่นคงปลอดภัยที่เข้าถึงหรือแก้ไขทรัพยากรที่ไม่มีสิทธิ์โดยไม่ได้ตั้งใจ เช่น การลบไฟล์เอกสารที่ใช้งานร่วมกันผ่านเครือข่ายได้เนื่องจากผู้ดูแลระบบกำหนดสิทธิ์ไว้ผิด เป็นต้น

2) แฮกเกอร์หมวกขาว (white hat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาช่องโหว่ และการโจมตีต่อระบบคอมพิวเตอร์ในเชิงป้องกันและรักษาความมั่นคงปลอดภัยให้กับระบบแล้วรายงานช่องโหว่หรือการโจมตีดังกล่าวต่อเจ้าของหรือผู้มีหน้าที่รับผิดชอบเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการปรับปรุงความมั่นคงปลอดภัยและแก้ไขข้อบกพร่องนั้นๆ ก่อนที่ช่องโหว่หรือข้อบกพร่องดังกล่าวจะถูกตรวจพบหรือถูกประกาศให้ทราบในที่สาธารณะ เช่น เว็บบอร์ดหรืออินเทอร์เน็ต เป็นต้น

3) แฮกเกอร์หมวกดำ (black hat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาและโจมตีต่อระบบคอมพิวเตอร์ เพื่อการทำลายความมั่นคงปลอดภัยโดยมีผลประโยชน์ส่วนตัวเป็นแรงจูงใจ เช่น ค่าตอบแทนจากองค์กรอาชญากรรม การล้างแค้น หรือความคิดเห็นทางการเมือง เป็นต้น

3.2.5 เอกซ์พลอยต์ (exploit) คือ แม้ว่าเอกซ์พลอยต์จะมีความหมายตามพจนานุกรมว่า “การใช้ประโยชน์หรือการทำประโยชน์” แต่เอกซ์พลอยต์ในที่นี้จะหมายถึงการโจมตีต่อช่องโหว่ที่มีในระบบสารสนเทศ เพื่อทำลายความมั่นคงปลอดภัยหรือเข้าใช้ประโยชน์จากช่องโหว่ที่มีอยู่ เช่น ช่องโหว่ของระบบจัดการเนื้อหาผ่านเว็บที่ถูกค้นพบและรายงาน อาจมีผู้ไม่ประสงค์ดีพัฒนาโปรแกรมที่สามารถโจมตีต่อช่องโหว่ดังกล่าวสำเร็จ แล้วแจกจ่ายให้กับผู้ที่สนใจนำโปรแกรมนี้ไปโจมตีต่อช่องโหว่นั้น นอกจากนี้ยังหมายถึงเทคนิคเทคนิควิธีใช้ในการโจมตี ด้วยเทคนิควิศวกรรมเชิงสังคม เช่น การพยายามตีสนิทกับเหยื่อซึ่งทำหน้าที่ในระบบสารสนเทศเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการโจมตี หรือการล่อลวงเพื่อใช้ประโยชน์จากเหยื่อในการเข้าถึงทรัพยากรสารสนเทศ เป็นต้น

3.2.6 เป้าหมาย (target) คือ บุคคล องค์กร ทรัพยากรสารสนเทศที่มีช่องโหว่และได้รับผลกระทบโดยตรงจากการการโจมตีที่อาจเกิดขึ้น

3.2.7 วิธีการโจมตี (attack vector) คือ กระบวนการ วิธีการ เครื่องมือและเทคนิคที่ใช้โจมตีต่อช่องโหว่ที่มีในเป้าหมายของการโจมตี

ดังที่ได้กล่าวข้างต้นแล้วว่า วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยคือ การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรสารสนเทศ ซึ่งมีความหมายนับตั้งแต่เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ เพียงเครื่องเดียว ซอฟต์แวร์ต่างๆ ไปจนถึงระบบสารสนเทศที่เชื่อมต่อกันผ่านเครือข่าย ฉะนั้นหากต้องการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรจึงมีแนวทางคล้ายคลึงกับการบริหารงาน โดยนอกจากจะต้องกำหนดแนวทางการจัดการทรัพยากรในภาพรวมแล้ว จะต้องดำเนินการพิจารณาความเหมาะสม ความสะดวกในการใช้งาน การกำหนดสิทธิ์และการเข้าถึง การสร้างนโยบายการรักษาความมั่นคงปลอดภัย ตลอดจนคัดเลือกเทคโนโลยีที่เกี่ยวข้องโดยคำนึงถึงความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัย และความง่ายในการใช้งาน ให้สอดคล้องกับความต้องการขององค์กร นโยบาย และผู้ใช้งานเป็นสำคัญ

----------✍

ความมั่นคงของระบบสารสนเทศ

➢ความหมายความมั่นคงของระบบสารสนเทศ

ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องผู้นำประเทศ ทรัพย์สิน ทรัพยากร และประชาชนของประเทศ

➢ความมั่นคงปลอดภัยขององค์กร

- ความมั่นคงปลอดภัยทางกายภาย Physical Security
- ความมั่นคงปลอดภัยส่วนบุคคล Personal Security
- ความมั่นคงปลอดภัยในการปฏิบัติงาน Operations Security
- ความมั่นคงปลอดภัยในการติดต่อสื่อสาร Communication Security
- ความมั่นคงปลอดภัยของเครือข่าย Network Security
- ความมั่นคงปลอดภัยของสารสนเทศ Information Security
- ความมั่นคงปลอดภัยของสารสนเทศ (Information Security)

ความมั่นคงปลอดภัยของสารสนเทศ คือ การป้องกันสารสนเทศและองค์ประกอบอื่นที่เกี่ยวข้อง

การรักษาความปลอดภัยทางข้อมูล Information Security คือ ผลที่เกิดขึ้นจาการใช้ระบบของนโยบายและ/หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต

<u>แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ</u>

กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้นประกอบด้วย

1. ความลับ Confidentiality

- เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้
- องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้
- ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่ website เพื่อสิทธิ์สนการทำธุรกรรมต่าง ๆ โดยลืมไปว่าเว็บไซต์เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก

2.ความสมบูรณ์ Integrity

•ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน

•สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

3.ความพร้อมใช้ Availability

•ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้นหากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลงในที่สุด

4.ความถูกต้องแม่นยำ Accuracy

•ความถูกต้องแม่นยำ หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอเมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

5.เป็นของแท้ Authenticity

สารสนเทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

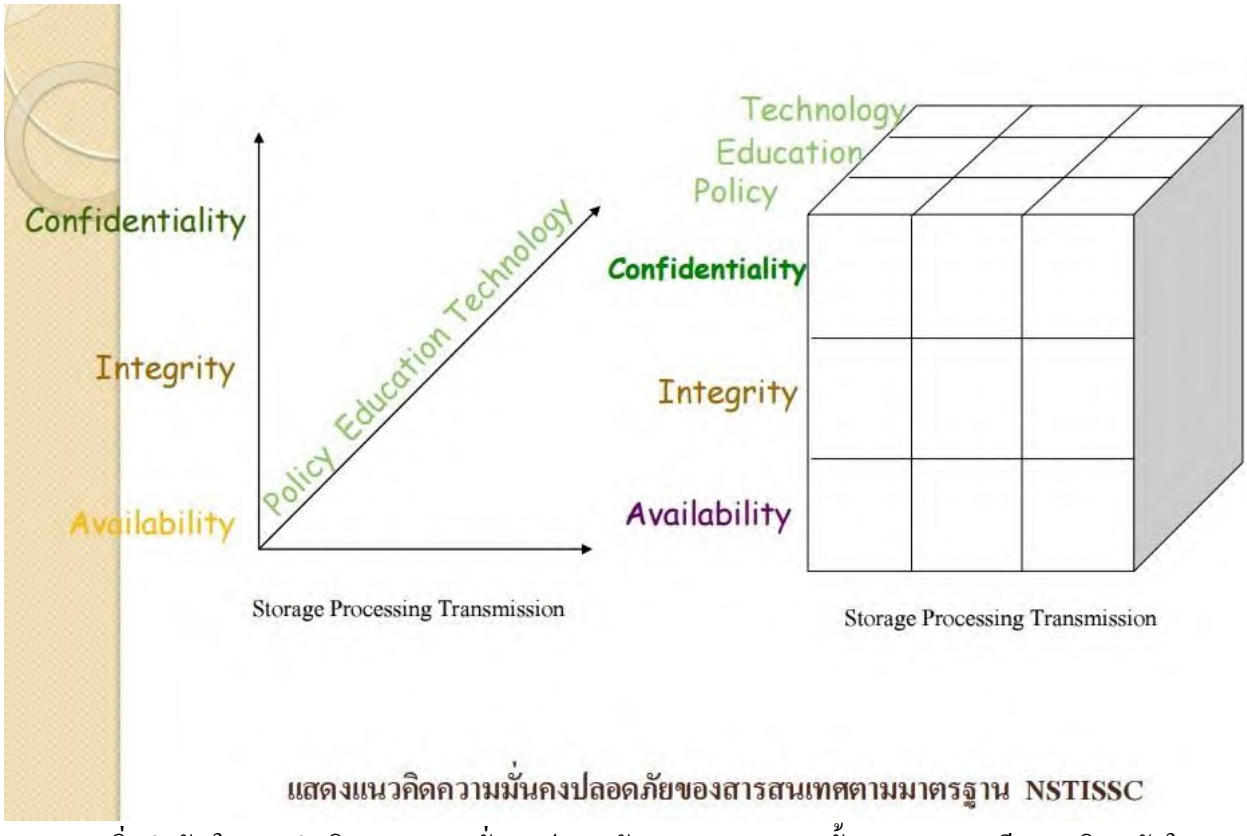
6.ความเป็นส่วนตัว Privacy

•ความเป็นส่วนตัว คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเจ้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้นมิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

➢แนวคิดของความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐานNSTISSC

NSTISSC (Nation Security Telecommunications and Information Systems Security

คือ คณะกรรมการด้านความมั่นคงโทรคมนาคมและระบบสารสนเทศแห่งชาติของต่างประเทศที่ได้รับการยอมรับแห่งหนึ่งได้กำหนดแนวคิดความมั่นคงปลอดภัยขึ้นมา ต่อมาได้กลายเป็นมาตรฐานการประเมินความมั่นคงของระบบสารสนเทศสิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศนั้น นอกจากจะมีความคิดหลักในด้านต่างๆ แล้วยังรวมถึงการกำหนดนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่จะนำมาใช้เป็นกลไกควบคุมและป้องกัน ที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยของสารสนเทศด้วย



แสดงแนวคิดความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC

-สิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ นั้น นอกจากจะมีความคิดหลักในด้านต่างๆ แล้ว ยังรวมถึงการ กำหนดนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่ จะนำมาใช้เป็นกลไกควบคุมและป้องกัน ที่ต้องเกี่ยวข้องกับการ จัดการความมั่นคงปลอดภัยของสารสนเทศด้วย

➢**องค์ประกอบของระบบสารสนเทศ กับ ความมั่นคงปลอดภัย**

1. Software ย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลาต้นทุน และกำลังคนที่จำกัดซึ่งมักจะทำภายหลังจากการพัฒนาซอฟต์แวร์เสร็จแล้ว

2. Hardware จะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ ที่ปลอดภัยให้กับอุปกรณ์ หรือฮาร์ดแวร์

3. Data ข้อมูล/สารสนเทศเป็นทรัพยากรที่มีค่าขององค์กรการ ป้องกันที่แน่นหนาก็ มี ความจำ เป็นสำหรับข้อมูลที่เป็นความลับซึ่งต้องอาศัยนโยบายความปลอดภัย และกลไกป้องกัน ที่ดี ควบคู่กัน

4. People บุคลากร คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมาก ที่สุด โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็ เป็น จุดอ่อนต่อการโจมตีได้จึงได้มีการศึกษากันอย่างจริงจัง เรียกว่า Social Engineering ซึ่งเป็นการป้องการการหลอกลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

5. Procedure ขั้นตอนการทำงานเป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถ ค้นหาจุดอ่อนเพื่อกระทำการอันก่อให้เกิดความเสียหายต่อ องค์กรและลูกค้าขององค์กรได้

6. Network เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่าง คอมพิวเตอร์ และระหว่างเครือข่ายคอมพิวเตอร์ทำให้ เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์โดยเฉพาะการเชื่อมต่อ ระบบสารสนเทศเข้า กับ เครือข่ายอินเตอร์เน็ต

อุปสรรคของงานความมันคงปลอดภัยของสารสนเทศ

-ความมั่นคงปลอดภัย คือ ความไม่สะดวก เนื่องจากต้องเสียเวลาในการ ป้อน password และกระบวนการอื่นๆในการพิสูจน์ ตัวผู้ใช้

-มีความซับซ้อนบางอย่างในคอมพิวเตอร์ ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry , Port, Service ที่เหล่านี้จะทราบในแวดวงของ Programmer หรือผู้ดูแลระบบ

-ผู้ใช้คอมไม่ระแวดระวัง

-การพัฒนาซอฟต์แวร์ไม่คำนึงถึงความปลอดภัยภายหลัง

-แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปัน ไม่ใช่ การป้องกัน

-มีการเข้าถึงข้อมูลได้จากทุกสถานที่

-ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟแวร์และฮาร์ดแวร์เพียง อย่างเดียว

-มิจฉาชีพมีความเชี่ยวชาญ (ในการเจาะข้อมูลของผู้อื่นมากเป็นพิเศษ)

-ฝ่ายบริหารมักจะไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัย

แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ

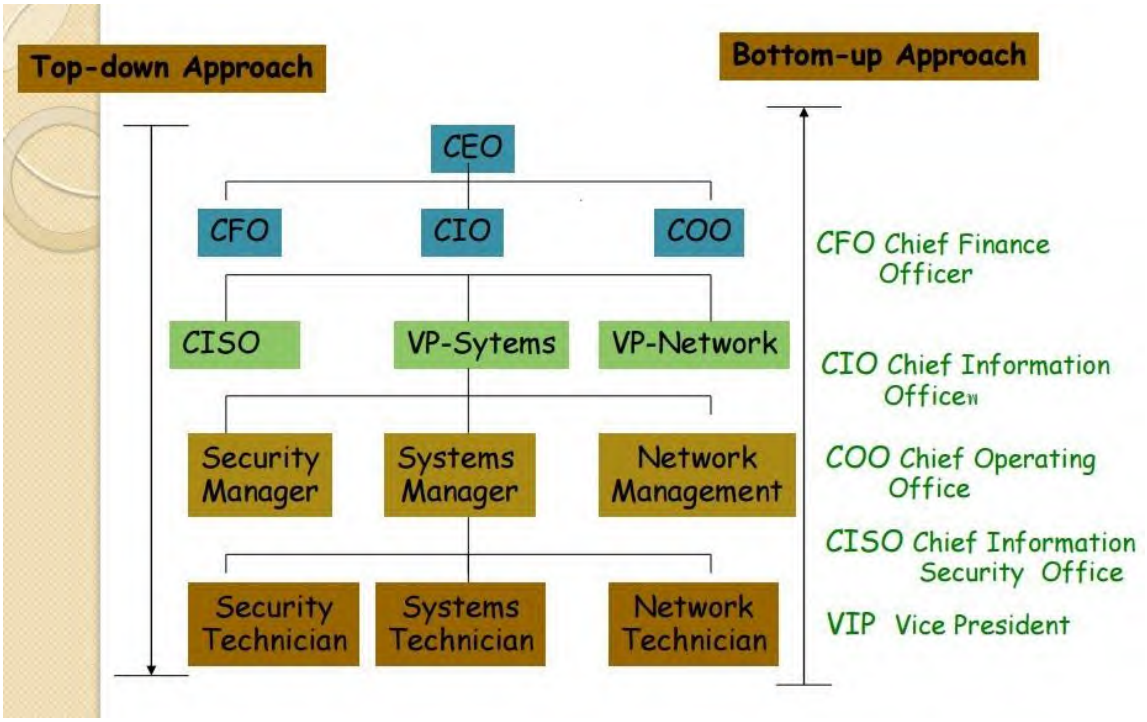
-Bottom - Up Approach เป็นแนวทางที่ผู้ดูแลระบบหรือเจ้าหน้าที่ ที่รับผิดชอบ ด้านความมั่นคงปลอดภัย โดยตรง เป็นผู้ริเริ่มหรือกำหนดมาตรการรักษาความปลอดภัยขึ้นมาระหว่างการพัฒนาระบบ

-ข้อดี คือ เจ้าหน้าที่จะสามารถดูแลงานด้วยตนเองในทุก ๆ วัน และใช้ความรู้ ความสามารถ ความเชี่ยวชาญที่มีการปรับปรุงกลไกควบคุมความปลอดภัยให้มี ประสิทธิภาพอย่างเต็มที่

-ข้อเสีย แนวทางนี้โดยทั่วไปมักจะทำให้การดำเนินงานความมั่นคงปลอดภัยของ สารสนเทศไม่ประสบผลสำเร็จเนื่องจากขาดปัจจัยความสำเร็จ เช่น ขาดการสนับสนุนจากผู้เกี่ยวข้อง หรือขาดอำนาจหน้าที่ในการสั่งการ

-Top - down Approach การดำเนินงานความมั่นคงปลอดภัยจะเริ่มต้น โดยผู้บริหารหรือผู้มีอำนาจหน้าที่โดยตรง ซึ่งสามารถ บังคับใช้นโยบาย บุคลากรที่รับผิดชอบ

-ข้อดี ขั้นตอนกระบวนการมั่นคงได้อย่างเต็มที่เนื่องจากได้รับการสนับสนุนจากผู้ที่เกี่ยวข้องเป็นอย่างดี มีการวางแผน กำหนด เป้าหมายและกระบวนการทำงานอย่างชัดเจนและเป็นทางการ

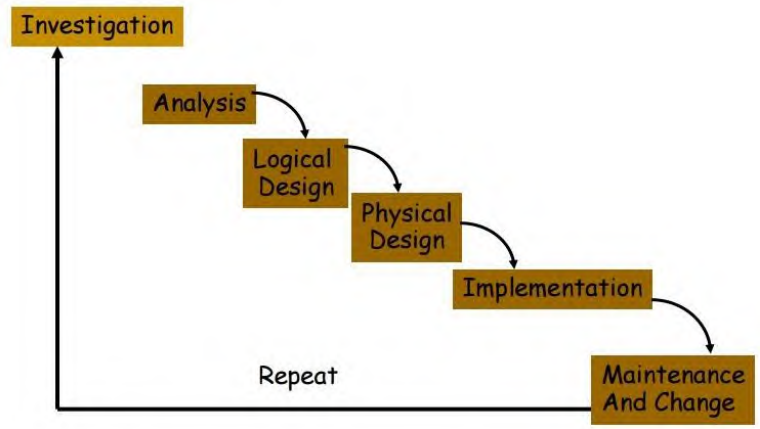


วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

-วงจรการพัฒนาระบบ System Development life Cycle: SDLC โดยแต่ละPhase ของ SDLC สามารถนำมาปรับใช้กับการดำเนินโครงการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศได้เรียกว่า Security Systems Development Life Cycle : SecSDLC

-บางองค์กร สามารถใช้วิธีการจัดการความเสี่ยง Risk Management เป็นกระบวนการหลักในการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศได้

SDLC เมื่อถูกนำไปปรับใช้ในองค์กร จะถูกแบ่งเป็น phase ในจำนวนที่แตกต่างกัน



เมื่อนำมาปรับใช้กับการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

-การสำรวจ Investigation เริ่มจากได้รับคำสั่งจากผู้บริการระดับสูงให้ดำเนินการพัฒนาระบบความมั่นคงปลอดภัย โดยมีการกำหนดเป้าหมาย กระบวนการ ผลลัพธ์ที่ต้องการ บุคลากร งบประมาณ และระยะเวลายังมีการกำหนด นโยบายความมั่น คงปลอดภัยในระดับองค์กรมาพร้อมกันด้วย

-ทีมงานที่รับผิดชอบจะนำรายละเอียดทำการสำรวจ เพื่อนำมาวิเคราะห์ปัญหากำหนดขอบเขต เป้าหมาย และวัตถุประสงค์ของโครงการ

-การวิเคราะห์ Analysis เป็นเฟสที่ทีมงานจะได้นำเอกสารมาทำการศึกษาเพิ่มเติมศึกษาถึงภัยคุกคาม และวิธีป้องกันรวมถึง กฎหมายสิทธิส่วนบุคคล การจัดการความเสี่ยง (ระบุความเสี่ยง)

-ประเมินหาความเสี่ยงที่มีผลกระทบในระดับร้ายแรง พร้อมกับเตรียมป้องกันไม่ให้เกิดความเสี่ยงต่างๆ ได้อีก

-การออกแบบระดับตรรกะ Logical Design เป็นเฟสที่ต้องจัดทำโครงร่างของระบบความมั่นคงปลอดภัยของสารสนเทศ ตรวจสอบและจัดทำนโยบายหลักที่จะนำไปใช้

-การออกแบบระดับกายภาพ Physical Design เป็นเฟสการกำหนดเทคโนโลยีสารสนเทศที่จะนำมาสนับสนุนโครงร่างระบบความมั่นคงปลอดภัยที่ได้ออกแบบไว้ในเฟสที่ผ่านมามีการประเมิน เทคโนโลยีพร้อมกับสร้างทางเลือกของเทคโนโลยีที่จะนำมาใช้

-การพัฒนา Implementation ดำเนินงานพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศที่ได้ออกแบบไว้ให้เกิดขึ้นจริง และทำการทดสอบจนกว่าจะไม่พบข้อผิดพลาด

-การบำรุงรักษาและเปลี่ยนแปลง Maintenance and Change การติดตามทดสอบแก้ไขและซ่อมบำรุงอยู่ตลอดเวลาควรมีการอัพเดทภัยคุกคาม รายละเอียดให้ทันสมัยอยู่อย่างสม่ำเสมอ

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
1 Investigation	•กำหนดเป้าหมายและขอบเขตโครงการ •ประมาณต้นทุน •ประเมินทรัพยากร •ศึกษาความเป็นไปได้	ผู้บริหารกำหนดกระบวนการดำเนินโครงการ เป้าหมาย และเอกสารแสดงนโยบายความมั่นคงที่มีอยู่

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
2 **Analysis**	•ศึกษาระบบเดิมตามเอกสารที่ได้รับในเฟสแรก	•วิเคราะห์นโยบายความมั่นคงปลอดภัยเดิม
	•กำหนดความต้องการของระบบ •ศึกษาการประสานงานระบบเก่ากับระบบใหม่ •จัดทำเอกสาร และปรับปรุงศึกษาความเป็นไปได้	•วิเคราะห์ภัยคุกคาม •พิจารณาประเด็นกฎหมาย •วิเคราะห์ความเสี่ยง

เฟส	กิจกรรมใน SDLC ธรรมดา	กิจกรรมใน SecSDLC
3 **Logical Design**	•ประเมินความจำเป็นทางธุรกิจ •เลือกข้อมูลสนับสนุนและโครงสร้างของระบบ •สร้างทางเลือกของระบบใหม่ •จัดทำเอกสารและปรับปรุงแก้ไข	•จัดทำโครงร่างระบบความมั่นคงปลอดภัย •วางแผนรับมือเหตุการณ์ไม่คาดคิด •วางแผนฟื้นฟูความเสียหาย

เฟส	กิจกรรมใน SDLC ธรรมดา	กิจกรรมใน SecSDLC
4 **Physical Design**	•เลือกเทคโนโลยีที่จะนำมาสนับสนุนระบบ •เลือกทางเลือกของระบบ •ตัดสินใจว่าจะซื้อหรือจะพัฒนาระบบเอง •จัดทำเอกสาร และปรับปรุงแก้ไข รายงานการศึกษาความเป็นไปได้	•เลือกเทคโนโลยีที่จะนำสนับสนุนโครงการ •กำหนดนิยาม •กำหนดเงื่อนไขในการคัดเลือกเทคโนโลยีความมั่นคงปลอดภัย •ทบทวนและพิจารณาอนุมัติโครงการ

เฟส	กิจกรรมใน SDLC ธรรมดา	กิจกรรมใน SecSDLC
5 Implementation	•พัฒนาหรือระบบใหม่ •สั่งซื้อ component ของระบบใหม่ •จัดทำเอกสารของระบบ •ฝึกอบรมผู้ใช้ •นำเสนอระบบต่อผู้ใช้ •ทดสอบระบบ	•ซื้อหรือพัฒนาระบบ •นำเสนอต่อผู้บริหารระดับสูง

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
6 Maintenance and Change	•สนับสนุนการใช้งานระบบ •ทดสอบระบบอยู่เป็นระยะ •อัดเกรดและซ่อมบำรุงระบบตามความจำเป็น	ติดตาม ทำสอบ แก้ไข อัพเดท และซ่อมบำรุงระบบทันทีที่พบว่ามีภัยคุกคาม

บทบาทของบุคลากรสารสนเทศในด้านความมั่นคงปลอดภัย

1.ผู้บริการระดับสูงSenior Manager

1.1. ผู้บริหารสารสนเทศระดับสงchief Information Officer : CIO มีหน้าที่ให้คำแนะนำและแสดงความคิดเห็นแก่ผู้บริหารระดับสูง

1.2. ผู้บริหารความมั่นคงปลอดภัยของสารสนเทศระดับสูง Chief Information Security Officer : CISO ทำหน้าที่ในการประเมิน จัดการ และพัฒนาระบบความมั่นคง ปลอดภัยของสารสนเทศในองค์กรโดยเฉพาะ

2.ทีมงานดำเนินโครงการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Project Team)

-ทีมงานดำเนินโครงการควรเป็นผู้ที่มีความรู้ ความสามารถในด้าน เทคโนโลยีอย่างลึกซึ้ง และควรจะมีความรู้ในด้านอื่นๆที่เกี่ยวข้องควบคู่ไปด้วย

<u>ทีมงานดำเนินโครงการประกอบไปด้วย</u>

-ผู้สนับสนุน Champion

-หัวหน้าทีม Team Leader

-นักพัฒนานโยบายความมั่นคงปลอดภัย Security Policy Development

-ผู้ชำนาญการประเมินความเสี่ยง Risk Assessment Specialist

-ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของสารสนเทศ Security Professional

-ผู้ดูแลระบบ System Administrator

-ผู้ใช้ระบบ End User

3.การเป็นเจ้าของข้อมูล Data Ownership ประกอบด้วย

3.1 เจ้าของข้อมูล Data Owners ผู้มีสิทธิในการใช้ข้อมูลและมีหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลด้วย

3.2 ผู้ดูแลข้อมูล Data Custodians เป็นผู้ที่ต้องทำงานร่วมกับ Data Owners โดยตรงทำหน้าที่จัดเก็บและบำรุงรักษาข้อมูล

3.3 ผู้ใช้ข้อมูล Data Users เป็นผู้ที่ทำงานกับข้อมูลโดยตรง

สรุป

-ความมั่นคงปลอดภัยของสารสนเทศ Information Security : IS คือการป้องกันสารสนเทศและองค์ประกอบ อื่น ๆ ที่เกี่ยวข้อง

<u>แนวคิด C.I.A Triangle ประกอบไปด้วย</u>

-ความลับ Confidentiality

-ความสมบูรณ์ Integrity

-ความพร้อมใช้ Availability

และยังกำหนดเพิ่มอีก คือ

-ความถูกต้องแม่นยำ Accuracy

-ความเป็นของแท้ Authenticity

-ความเป็นส่วนตัว Privacy

แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ มี 2 ลักษณะ คือ

1.Bottom-Up Approach คือ ผู้ดูแลระบบหรือทีมงานเป็นผู้ริเริ่มโครงการ

2.Top-down Approach คือผู้บริหารระดับสูงเป็นผู้ริเริ่มและกำหนดโครงการ

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ มี 6 เฟส คือ

-การสำรวจ Investigation

-การวิเคราะห์ Analysis

-การออกแบบระดับตรรกะ Logical Design

-การออกแบบและพัฒนากายภาพ Physical Design

-การพัฒนา Implementation

-การบำรุงรักษาและเปลี่ยนแปลง Maintenance and Change

บุคคลที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของสารสนเทศ

-ผู้บริหารสารสนเทศระดับสูง

-ผู้บริหารความมั่นคงปลอดภัยของสารสนเทศระดับสูง

-ผู้บริหาร โครงการ หรือหัวหน้าที่มี

-เจ้าหน้าที่เทคนิคด้านความมั่นคงปลอดภัยของสารสนเทศ เป็นต้น

----------✍

ความรู้เกี่ยวกับการวิเคราะห์และออกแบบระบบ

1. **ความหมายการวิเคราะห์ระบบ**

ระบบคืออะไร

ระบบคือกลุ่มขององค์การต่างๆ ที่ทำงานร่วมกันเพื่อจุดประสงค์อันเดียวกัน ระบบอาจจะประกอบด้วย บุคคลากร เครื่องมือ เครื่องใช้ พัสดุ วิธีการ ซึ่งทั้งหมดนี้จะต้องมีระบบจัดการอันหนึ่งเพื่อให้บรรลุจุดประสงค์อันเดียวกัน

➢ **การวิเคราะห์ระบบและการออกแบบ (** System Analysis and Design)

การวิเคราะห์และออกแบบระบบคือ วิธีการที่ใช้ในการสร้างระบบสารสนเทศขึ้นมาใหม่ในธุรกิจใดธุรกิจหนึ่ง หรือระบบย่อยของธุรกิจ นอกจากการสร้างระบบสารสนเทศใหม่แล้ว การวิเคราะห์ระบบช่วยในการแก้ไขระบบสารสนเทศเดิมที่มีอยู่แล้วให้ดีขึ้นด้วยก็ได้ การวิเคราะห์ระบบคือ การหาความต้องการ (Requirements) ของระบบสารสนเทศว่าคืออะไร หรือต้องการเพิ่มเติมอะไรเข้ามาในระบบและการออกแบบก็คือ การนำเอาความต้องการของระบบมาเป็นแบบแผนหรือเรียกว่าพิมพ์เขียว ในการสร้างระบบสารสนเทศนั้นให้ใช้ในงานได้จริง ผู้ที่ทำหน้านี้ก็คือ นักวิเคราะห์และออกแบบระบบ (System Analysis : SA)

เมื่อเราศึกษาระบบใดระบบหนึ่ง เราควรจะต้องเข้าใจการทำงานของระบบนั้นให้ดีโดย การถามตัวเองตลอดเวลาด้วยคำถามเหล่านี้

1. ระบบทำอะไร (What)2. ทำโดยใคร (Who)3. ทำเมื่อไร (When)4. ทำอย่างไร (How)

นักวิเคราะห์ระบบคือใคร ?คอมพิวเตอร์เป็นเพียงเครื่องมือที่ใช้สำหรับเก็บรวบรวมและประมวลผลให้กับผู้ใช้โดยให้ประโยชน์ต่อผู้ใช้คือ ความรวดเร็วและความถูกต้องของข้อมูล ซึ่งเป็นหัวใจสำคัญต่อการบริหารของธุรกิจในปัจจุบันที่มีการแข่งขันสูง

ผู้ใช้ (Users) จึงเป็นผู้กำหนดปัญหาและแนวทางของระบบงานที่นำมา แก้ไขซึ่งปัญหาแต่ผู้ใช้เองไม่ทราบวิธีจะนำเอาคอมพิวเตอร์มาใช้แก้ปัญหา หรือช่วยเหลือในการบริหาร ในทางตรงกันข้ามโปรแกรมเมอร์ (programmers)และช่างเทคนิค (technicians)เป็นผู้ที่สามารถจะใช้เทคโนโลยีของคอมพิวเตอร์และป้อนคำสั่งให้คอมพิวเตอร์ทำงานได้ต้องการ แต่โปรแกรมเมอร์หรือช่างเทคนิคมักจะไม่เข้าใจถึงระบบธุรกิจมากนัก ดังนั้นช่องว่างระหว่างนักธุรกิจหรือระบบงานในหน่วยงานต่างๆ กับโปรแกรมเมอร์หรือกับช่างเทคนิคจึงอาจเกิดขึ้นได้ นักวิเคราะห์ระบบจึงทำหน้าที่เป็นผู้สมานช่องว่างนี้ นักวิเคราะห์ระบบเป็นผู้ที่เกี่ยวข้องโดยตรงที่จะนำเอาความเข้าใจและเทคโนโลยีของคอมพิวเตอร์มาใช้ ในการพัฒนาระบบงานข้อมูลเพื่อช่วยแก้ปัญหาให้กับงานในหน่วยงานต่างๆ

2. **บทบาทของนักวิเคราะห์ระบบ**

นักวิเคราะห์ระบบจะเป็นผู้ที่ศึกษาถึงปัญหาและความต้องการของนักธุรกิจ โดยนำเอาปัจจัย 3 ประการ คือ คน (people) วิธีการ (method) และคอมพิวเตอร์เทคโนโลยี (computer technology) ใช้ในการปรับปรุงหรือแก้ปัญหาให้กับนักธุรกิจเมื่อได้มีการนำเอาพัฒนาการทางเทคโนโลยีของคอมพิวเตอร์มาใช้ นักวิเคราะห์ระบบจะต้องรับผิดชอบถึงการกำหนดลักษณะของข้อมูล (data) ที่จะจัดเก็บเข้าสู่ระบบงานคอมพิวเตอร์ การหมุนเวียน การเปลี่ยนแปลงของข้อมูลและระยะเวลาเพื่อให้เกิดประโยชน์สูงสุดต่อผู้ใช้หรือธุรกิจ (business users)

นักวิเคราะห์ระบบไม่ได้เพียงวิเคราะห์หรือดีไซน์ระบบงานเท่านั้น หากแต่ยังขายบริการทางด้านระบบงานข้อมูล โดยนำเอาประโยชน์จากเทคโนโลยีล่าสุดมาใช้ควบคู่กันไปด้วยจากบทบาทของนักวิเคราะห์ระบบที่กล่าวมาแล้วข้างต้น ทำให้นักวิเคราะห์ระบบจะต้องมีความรู้ทั้งทางภาคธุรกิจหรือการดำเนินงาน ในหน่วยงานต่างๆ และคอมพิวเตอร์ควบคู่กัน นักวิเคราะห์ระบบโดยส่วนใหญ่สามารถที่จะดีไซน์ระบบงานและเขียนโปรแกรมขึ้นได้ด้วยตัวเอง ส่วนนี้เองกลับทำให้บุคคลภายนอกเกิดความสับสนระหว่างโปรแกรมเมอร์กับนักวิเคราะห์ระบบ

3. **ความแตกต่างระหว่างโปรแกรมเมอร์และนักวิเคราะห์ระบบ**

โปรแกรมเมอร์ (programmer) หมายถึงบุคคลที่รับผิดชอบในด้านการเขียนโปรแกรม สิ่งที่เขาจะเชื่อมโยงนั้น ได้แก่ อุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติ (Operating System :OS) หรือแม้กระทั่งภาษาที่ใช้ในการเขียน เช่น COBOL, BASIC และ C++ งานของโปรแกรมเมอร์จะเป็นไปในลักษณะที่มีขอบเขต ที่แน่นอนคือโปรแกรมที่เขาเขียนขึ้นนั้นถูกต้องตามจุดประสงค์หรือไม่ กิจกรรมงานของโปรแกรมจะเกี่ยวข้องกับคนจำนวนน้อย เช่น กับโปรแกรมเมอร์ด้วยกันเอง หรือกับนักวิเคราะห์ระบบที่เป็นผู้วางแนวทางของระบบให้แก่เขา

นักวิเคราะห์ระบบ หรือที่เรียกกันย่อๆ ว่า SA (SYSTEM ANALYSIS) นั้น นอกจากจะต้องรับผิดชอบต่อการโปรแกรมคอมพิวเตอร์แล้ว ยังจะต้องรับผิดชอบงานในส่วนที่เกี่ยวกับการจัดหาอุปกรณ์ต่างๆ เกี่ยวกับคอมพิวเตอร์ ผู้ที่จะใช้ระบบแฟ้มหรือฐานข้อมูลต่างๆ รวมทั้งข้อมูลดิบที่จะป้อนเข้าระบบงานของนักวิเคราะห์ระบบไม่ได้อยู่ในลักษณะที่แน่นอนแบบโปรแกรมเมอร์ ไม่มีคำตอบที่แน่นอนจากระบบที่เขาวางไม่ว่าผิดหรือถูก งานของเขาเกิดจากการประนีประนอมและผสมผสานของปัจจัยต่างๆ ที่เกี่ยวข้องกับระบบงาน คือ ผู้ใช้ วิธีการ เทคโนโลยี และอุปกรณ์จนได้ผลลัพธ์ที่เหมาะสมออกมาเป็นระบบงาน (APPLICATION SYSTEM) งานของนักวิเคราะห์ระบบจึงมักจะต้องเกี่ยวข้องกับคนหลายระดับ ตั้งแต่ลูกค้าหรือผู้ใช้ นักธุรกิจ โปรแกรมเมอร์ ผู้ตรวจสอบบัญชีหรือแม้กระทั่งเซลล์แมนที่ขายระบบงานข้อมูลแม้ว่างานของนักวิเคราะห์ระบบจะดูเป็นงานที่ยากและซับซ้อน แต่งานในลักษณะนี้ก็เป็นงานที่ท้าทายให้กับบุคคลที่มีความคิดสร้างสรรค์และกว้างไกลเข้ามาอยู่เสมอ ความรู้สึกภาคภูมิใจที่ได้วางระบบงานออกมาเป็นรูปร่างและสามารถ ใช้ปฏิบัติได้จริง จะฝังอยู่ในสำนึกของเขาตลอดเวลา ความรู้สึกอันนี้คงจะถ่ายทอดออกมาเป็นตัวหนังสือไม่ได้ แต่จะทราบกันเองในหมู่ของนักวิเคราะห์ระบบด้วยกัน

4. **การเตรียมตัวเป็นนักวิเคราะห์บทบาทของนักวิเคราะห์ระบบ**

หลังจากที่เราได้วิเคราะห์ว่า นักวิเคราะห์ระบบจะทำหน้าที่เป็นแกนกลางระหว่างนักธุรกิจ (BUSINESS PEOPLE) หรือผู้ใช้ระบบ (USERS) กับโปรแกรมเมอร์(PROGRAMMERS) อย่างไรก็ตามธุรกิจหรือหน่วยงานต่างๆ จึงมักจะมีความคิดที่ว่านักวิเคราะห์ระบบจะต้องมีพื้นฐานการเขียนโปรแกรมเป็นอันดับแรก แนวความคิดนี้ แท้จริงแล้วเป็นเพียงส่วนหนึ่งเท่านั้นในคุณสมบัติอันควรมีของนักวิเคราะห์ระบบนักวิเคราะห์ระบบจะต้องมีความสามารถที่จะพัฒนาระบบเพื่อแก้ปัญหาให้กับผู้ใช้หรือธุรกิจอย่างมีเทคนิคและแบบแผน โปรแกรมเมอร์ที่เก่งมิได้หมายความว่าเขาจะเป็นนักวิเคราะห์ระบบที่ดีได้ในทางตรงกันข้าม โปรแกรมเมอร์ที่ไม่เก่งมิได้หมายความว่าเขาจะเป็นนักวิเคราะห์ระบบที่ดีไม่ได้

➢ **วงจรการพัฒนาระบบ (**System Development Life Cycle)

วงจรการพัฒนาระบบ (System Development Life Cycle :SDLC)
ระบบสารสนเทศทั้งหลายมีวงจรชีวิตที่เหมือนกันตั้งแต่เกิดจนตายวงจรนี้จะเป็นขั้นตอน ที่เป็นลำดับตั้งแต่ต้นจนเสร็จเรียบร้อย เป็นระบบที่ใช้งานได้ ซึ่งนักวิเคราะห์ระบบต้องทำความเข้าใจให้ดีว่าในแต่ละขั้นตอนจะต้องทำอะไร และทำอย่างไร ขั้นตอนการพัฒนาระบบมีอยู่ด้วยกัน 7 ขั้น ด้วยกัน คือ

1. เข้าใจปัญหา (Problem Recognition)
2. ศึกษาความเป็นไปได้ (Feasibility Study)
3. วิเคราะห์ (Analysis)
4. ออกแบบ (Design)
5. สร้างหรือพัฒนาระบบ (Construction)
6. การปรับเปลี่ยน (Conversion)
7. บำรุงรักษา (Maintenance)

ขั้นที่ 1 : **เข้าใจปัญหา (**Problem Recognition)

ระบบสารสนเทศจะเกิดขึ้นได้ก็ต่อเมื่อผู้บริหารหรือผู้ใช้ตระหนักว่า ต้องการระบบสารสนเทศหรือระบบจัดการเดิม ได้แก่ระบบเอกสารในตู้เอกสาร ไม่มีประสิทธิภาพเพียงพอที่ตอบสนองความต้องการในปัจจุบัน ปัจจุบันผู้บริหารตื่นตัวกันมากที่จะให้มีการพัฒนาระบบสารสนเทศมาใช้ในหน่วยงานของตน ในงานธุรกิจอุตสาหกรรม หรือใช้ในการผลิต ตัวอย่างเช่น บริษัทของเรา จำกัด ติดต่อซื้อสินค้าจากผู้ขายหลายบริษัท ซึ่งบริษัทของเราจะมีระบบ MIS ที่เก็บข้อมูลเกี่ยวกับหนี้สินที่บริษัทขอเราติดค้างผู้ขายอยู่ แต่ระบบเก็บข้อมูลผู้ขายได้เพียง 1,000 รายเท่านั้น แต่ปัจจุบันผู้ขายมีระบบเก็บข้อมูลถึง 900 ราย และอนาคตอันใกล้นี้จะเกิน 1,000 ราย ดังนั้นฝ่ายบริหารจึงเรียกนักวิเคราะห์ระบบเข้ามาศึกษา แก้ไขระบบงานปัญหาที่สำคัญของระบบสารสนเทศในปัจจุบัน คือ ระบบเขียนมานานแล้ว ส่วนใหญ่เขียนมาเพื่อติดตามเรื่องการเงิน ไม่ได้มีจุดประสงค์เพื่อให้ข้อมูลข่าวสารในการตัดสินใจ แต่ปัจจุบันฝ่าย บริหารต้องการดูสถิติการขายเพื่อใช้ในการคาดคะเนในอนาคต หรือความต้องการอื่นๆ เช่น สินค้าที่มียอดขายสูง หรือสินค้าที่ลูกค้าต้องการสูง หรือการแยกประเภทสินค้าต่างๆที่ทำได้ไม่ง่ายนักการที่จะแก้ไขระบบเดิมที่มีอยู่แล้วไม่ใช่เรื่องที่ง่ายนัก หรือแม้แต่การสร้างระบบใหม่ ดังนั้นควรจะมีการศึกษาเสียก่อนว่าความต้องการของเราเพียงพอที่เป็นไปได้หรือไม่ ได้แก่ "การศึกษาความเป็นไปได้" (Feasibility Study)

สรุป ขั้นตอนที่ 1: **เข้าใจปัญหา**

หน้าที่ : ตระหนักว่ามีปัญหาในระบบ

ผลลัพธ์ : อนุมัติการศึกษาความเป็นไปได้

เครื่องมือ : ไม่มี

บุคลากรและหน้าที่ความรับผิดชอบ : ผู้ใช้หรือผู้บริหารชี้แจงปัญหาต่อนักวิเคราะห์ระบบ

ขั้นตอนที่ 2 : **ศึกษาความเป็นไปได้ (**Feasibility Study)

จุดประสงค์ของการศึกษาความเป็นไปได้ก็คือ การกำหนดว่าปัญหาคืออะไรและตัดสินใจว่าการพัฒนาสร้างระบบสารสนเทศ หรือการแก้ไขระบบสารสนเทศเดิมมีความเป็นไปได้หรือไม่โดยเสียค่าใช้จ่ายและเวลาน้อยที่สุดและได้ผลเป็นที่น่าพอใจปัญหาต่อไปคือ นักวิเคราะห์ระบบจะต้องกำหนดให้ได้ว่าการแก้ไขปัญหาดังกล่าวมีความเป็นไปได้ทางเทคนิคและบุคลากร ปัญหาทางเทคนิคก็จะเกี่ยวข้องกับเรื่องคอมพิวเตอร์ และเครื่องมือเก่าๆถ้ามีรวมทั้งเครื่องคอมพิวเตอร์ซอฟต์แวร์ด้วย ตัวอย่างคือ คอมพิวเตอร์ที่ใช้อยู่ในบริษัทเพียงพอหรือไม่ คอมพิวเตอร์อาจจะมีเนื้อที่ของฮาร์ดดิสก์ไม่เพียงพอ รวมทั้งซอฟต์แวร์ ว่าอาจจะต้องซื้อใหม่ หรือพัฒนาขึ้นใหม่ เป็นต้น ความเป็นไปได้ทางด้านบุคลากร คือ บริษัทมีบุคคลที่เหมาะสมที่จะพัฒนาและติดตั้งระบบเพียงพอหรือไม่ ถ้าไม่มีจะหาได้หรือไม่ จากที่ใด เป็นต้น นอกจากนั้นควรจะให้ความสนใจว่าผู้ใช้ระบบมีความคิดเห็นอย่างไรกับการเปลี่ยนแปลง รวมทั้งความเห็นของผู้บริหารด้วย

สุดท้ายนักวิเคราะห์ระบบต้องวิเคราะห์ได้ว่า ความเป็นไปได้เรื่องค่าใช้จ่าย รวมทั้งเวลาที่ ใช้ในการพัฒนาระบบ และที่สำคัญคือ ผลประโยชน์ที่จะได้รับ เรื่องเวลาเป็นสิ่งสำคัญ เช่น การเปลี่ยนแปลงระบบเพื่อรองรับผู้ขายให้ได้มากกว่า 1,000 บริษัทนั้น ควรใช้เวลาไม่เกิน 1 ปี ตั้งแต่เริ่มต้นจนใช้งานได้ ค่าใช้จ่ายเริ่มตั้งแต่พัฒนาจนถึงใช้งานได้จริงได้แก่ เงินเดือน เครื่องมือ อุปกรณ์ ต่างๆ เป็นต้น พูดถึงเรื่องผลประโยชน์ที่ได้รับอาจมองเห็นได้ไม่ง่ายนัก แต่นักวิเคราะห์ระบบควรมองและตีออกมาในรูปเงินให้ได้ เช่น เมื่อนำระบบใหม่เข้ามาใช้อาจจะทำให้ค่าใช้จ่ายบุคลากรลดลง หรือกำไรเพิ่มมากขึ้น เช่น ทำให้ยอดขายเพิ่มมากขึ้น เนื่องจากผู้บริหารมีข้อมูลพร้อมที่จะช่วยในการตัดสินใจที่ดีขึ้น การคาดคะเนทั้งหลายเป็นไปอย่างหยาบๆ เราไม่สามารถหาตัวเลขที่แน่นอนตายตัวได้ เนื่องจากทั้งหมดยังไม่ได้เกิดขึ้นจริง หลังจากเตรียมตัวเลขเรียบร้อยแล้ว นักวิเคราะห์ระบบก็นำตัวเลข ค่าใช้จ่ายและผลประโยชน์ (Cost-Benefit) มาเปรียบเทียบกัน

สรุปขั้นตอนที่ 2 : การศึกษาความเป็นไปได้ (Feasibility Study)

หน้าที่ : กำหนดปัญหา และศึกษาว่าเป็นไปได้หรือไม่ที่จะเปลี่ยนแปลงระบบ

ผลลัพธ์ : รายงานความเป็นไปได้

เครื่องมือ : เก็บรวบรวมข้อมูลของระบบและคาดคะเนความต้องการของระบบ

บุคลากรและหน้าที่ความรับผิดชอบ : ผู้ใช้จะมีบทบาทสำคัญในการศึกษา

1. นักวิเคราะห์ระบบจะเก็บรวบรวมข้อมูลทั้งหมดที่จำเป็นทั้งหมดเกี่ยวกับปัญหา
2. นักวิเคราะห์ระบบคาดคะเนความต้องการของระบบและแนวทางการแก้ปัญหา
3. นักวิเคราะห์ระบบ กำหนดความต้องการที่แน่ชัดซึ่งจะใช้สำหรับขั้นตอนการวิเคราะห์ต่อไป
4. ผู้บริหารตัดสินใจว่าจะดำเนินโครงการต่อไปหรือไม่