ดร.สิงห์ทอง บัวชุม
D.P.A., ปร.ด., รป.ด., รป.ม., นม., นบ

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
คุณภาพทางวิชาการต้องมาที่ 1
www.thebestcenter.com; www.facebook.com/bestcentergroup

คู่มือเตรียมสอบ

สำนักข่าวกรองแห่งชาติ

นักการข่าว ปฏิบัติการ

ด้านความมั่นคงปลอดภัยไซเบอร์

ประกอบด้วย

- **วิชาความรู้ด้านความมั่นคงปลอดภัยไซเบอร์** (คะแนนเต็ม 100 คะแนน)
  ทดสอบความรู้ความสามารถเกี่ยวกับลักษณะงานที่ปฏิบัติในด้านต่าง ๆ รวมถึงความรู้ทางวิชาการที่ใช้ในการปฏิบัติงานตามตำแหน่งที่สมัคร ได้แก่ ด้านเทคโนโลยีการออกแบบ และดูแลระบบด้านความมั่นคง ปลอดภัย การวิเคราะห์และออกแบบโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัย
- **วิชาความรู้เกี่ยวกับสถานการณ์ปัจจุบัน** (คะแนนเต็ม 50 คะแนน)
  ทดสอบความรู้เกี่ยวกับสถานการณ์สำคัญด้านการเมือง เศรษฐกิจ สังคม ทั้งที่เกิดขึ้น ภายในประเทศและต่างประเทศ ซึ่งอาจส่งผลกระทบต่อผลประโยชน์ ความมั่นคงหรือความสงบเรียบร้อยของประเทศไทย รวมถึงความรู้เรื่องการรักษาความปลอดภัยแห่งชาติ
- **วิชาภาษายังกฤษ** (คะแนนเต็ม 50 คะแนน)
  ทดสอบความรู้ความสามารถในการใช้ภาษาอังกฤษ โดยการให้สรุปความ หรือตีความ ข้อความสั้น ๆ หรือบทความ และให้พิจารณาเลือกใช้ภาษาในรูปแบบต่าง ๆ จากคำหรือกลุ่มประโยคหรือข้อความสั้น ๆ หรือเรียงความ การใช้ไวยากรณ์

คำนำ

คู่มือเตรียมสอบ สำหรับตำแหน่ง นักการข่าวปฏิบัติการ ด้านความมั่นคงปลอดภัยไซเบอร์ สำนักข่าวกรองแห่งชาติ เล่มนี้ โดยทางสถาบัน THE BEST CENTER และคณะได้เรียบเรียงขึ้น เพื่อให้ผู้สมัครสอบใช้สำหรับเตรียมตัวสอบในการสอบแข่งขันฯ ในครั้งนี้

ดังนั้นทางสถาบัน THE BEST CENTER ได้เล็งเห็นความสำคัญจึงได้จัดทำหนังสือเล่มนี้ขึ้นมา ประกอบด้วยความรู้เกี่ยวกับการเนื้อหา พ.ร.บ. ระเบียบและเจาะแนวข้อสอบเพื่อให้ผู้ที่สอบได้เตรียมตัวอ่านล่วงหน้า มีความพร้อมในการทำข้อสอบ

ท้ายนี้ คณะผู้จัดทำขอขอบคุณทางสถาบัน THE BEST CENTER ที่ได้ให้การสนับสนุนและมีส่วนร่วมในการจัดทำต้นฉบับนี้ ทำให้หนังสือเล่มนี้สามารถสำเร็จขึ้นมาเป็นเล่มได้ พร้อมกันนี้คณะผู้จัดทำขอน้อมรับข้อบกพร่องใด ๆ อันเกิดขึ้นและยินดีรับฟังความคิดเห็นจากทุก ๆ ท่าน เพื่อที่จะนำมาปรับปรุงแก้ไขให้ดียิ่งขึ้น

ขอให้โชคดีในการสอบทุกท่าน

ฝ่ายวิชาการ

สถาบัน The Best Center

www.thebestcenter.com

สารบัญ

➢ประวัติความเป็นมา

ประเทศไทยมีการดำเนินงานด้านการข่าวกรองมาตั้งแต่โบราณและตลอดทุกยุคทุกสมัย ในประวัติศาสตร์ยามศึกสงคราม ทหารมีหน้าที่สอดแนม ลาดตระเวนใช้ไส้ศึก แต่การดำเนินงานในลักษณะหน่วยข่าวกรองสมัยใหม่และเป็นหน่วยข่าวกรองกลางของชาติเกิดขึ้นหลังสงครามโลกครั้งที่สอง

ช่วงเวลาดังกล่าว เป็นช่วงที่ต่างประเทศมีการพัฒนาองค์การข่าวกรองอย่างจริงจัง รัฐบาลในสมัยจอมพล ป. พิบูลสงคราม เห็นความจำเป็นที่จะต้องจัดตั้งหน่วยราชการที่เป็นศูนย์กลาง รวบรวมข้อมูลข่าวสารต่าง ๆ ที่ได้รับจากการปฏิบัติงานการข่าวตามปกติ หรือจากหน่วยข่าวกรองต่าง ๆ ที่มีอยู่ในขณะนั้น ได้แก่ หน่วยข่าวฝ่ายทหาร และหน่วยข่าวตำรวจ รวมทั้งข่าวที่ได้จากวิธีการทางลับ และข่าวจากแหล่งข่าวเปิดที่มีผลกระทบต่อผลประโยชน์และความมั่นคงของประเทศ ซึ่งจำเป็นต่อการตัดสินใจกำหนดนโยบายและท่าทีทางการเมืองภายในและต่างประเทศของรัฐบาล จึงได้จัดตั้ง "กรมประมวลราชการแผ่นดิน" อยู่ในสังกัดทบวงคณะรัฐมนตรีฝ่ายการเมือง เมื่อวันที่ 1 มกราคม 2497 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2496 (ประกาศในราชกิจจานุเบกษา เล่มที่ 70 ตอนที่ 81 หน้าที่ 13 เมื่อวันที่ 31 ธันวาคม 2496) โดยได้แต่งตั้งให้พลตำรวจเอก เผ่า ศรียานนท์ อธิบดีกรมตำรวจในขณะนั้น เป็นอธิบดีกรมประมวลราชการแผ่นดินอีกตำแหน่งหนึ่ง ต่อมาในสมัยจอมพล สฤษดิ์ ธนะรัชต์ กรมประมวลราชการแผ่นดิน ได้เปลี่ยนชื่อเป็น "กรมประมวลข่าวกลาง" เมื่อวันที่ 2 ธันวาคม 2502 ตามพระราชบัญญัติจัดระเบียบราชการสำนักนายกรัฐมนตรี (ฉบับที่ 6) พ.ศ. 2502 และต่อมาในสมัยพลเอก เปรม ติณสูลานนท์ กรมประมวลข่าวกลางได้เปลี่ยนชื่อเป็น "สำนักข่าวกรองแห่งชาติ (สขช.)" เมื่อวันที่ 30 สิงหาคม 2528 ตามพระราชบัญญัติข่าวกรองแห่งชาติและพระราชบัญญัติแก้ไขเพิ่มเติม ตามประกาศคณะปฏิวัติ ฉบับที่ 213 มีฐานะเป็นหน่วยข่าว แห่งชาติขึ้นตรงต่อนายกรัฐมนตรี

สขช. จึงเป็นหน่วยข่าวระดับชาติหน่วยเดียวของประเทศไทยที่ เป็นหน่วยราชการพลเรือน มีหัวหน้าส่วนราชการเป็นข้าราชการพลเรือนสามัญ ปัจจุบัน นายสุวพันธุ์ ตันยุวรรธนะ ดำรงตำแหน่งผู้อำนวยการสำนักข่าวกรองแห่งชาติ

➢วิสัยทัศน์

“เป็นหน่วยข่าวกรองที่ทันสมัย เพื่อความมั่นคงของชาติและประชาชน”

➢พันธกิจ

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

➢ค่านิยม

"มุ่งมั่น ทุ่มเท มีวินัย เสียสละ เพื่อชาติและประชาชน"

➢หน้าที่ความรับผิดชอบ

อำนาจหน้าที่ของสำนักข่าวกรองแห่งชาติ กำหนดไว้ใน มาตรา 4 ของพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2528, พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552 และ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 **สรุปรวมกันได้ดังต่อไปนี้**

1. ปฏิบัติงานเกี่ยวกับกิจการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสารและการรักษาความปลอดภัยฝ่ายพลเรือน

2. ติดตามสถานการณ์ภายในประเทศและต่างประเทศ ที่มีผลกระทบต่อความมั่นคงแห่งชาติและรายงานตรงต่อนายกรัฐมนตรีและสภาความมั่นคงแห่งชาติ และกระจายข่าวกรองที่มีผลกระทบต่อความมั่นคงแห่งชาติให้หน่วยงานของรัฐ หรือรัฐวิสาหกิจที่เกี่ยวข้องใช้ประโยชน์ตามความเหมาะสม

3. ศึกษา วิจัยและพัฒนา เกี่ยวกับกิจการการข่าวกรอง การต่อต้านข่าวกรองและการรักษาความปลอดภัยฝ่ายพลเรือนเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน

4. เป็นศูนย์กลางประสานกิจการข่าวกรอง การต่อต้านข่าวกรอง กับหน่วยงานอื่นทั้งในประเทศและต่างประเทศ และเป็นองค์การรักษาความปลอดภัยฝ่ายพลเรือน ทำหน้าที่เป็นประธานคณะที่ปรึกษาการข่าว และรับผิดชอบการบริหารจัดการศูนย์ประสานข่าวกรองแห่งชาติ

5. เสนอแนะนโยบายและมาตรการ ตลอดจนให้คำแนะนำ และคำปรึกษาด้านการข่าวกรองการต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนต่อนายกรัฐมนตรี สภาความมั่นคงแห่งชาติ หน่วยงานราชการและรัฐวิสาหกิจ

➢ยุทธศาสตร์

1. พัฒนาประสิทธิภาพของระบบงานข่าวกรอง

2. ยกระดับงานข่าวกรองเพื่อการป้องกันและสนับสนุนการแก้ไขปัญหาภัยคุกคามต่อความมั่นคง

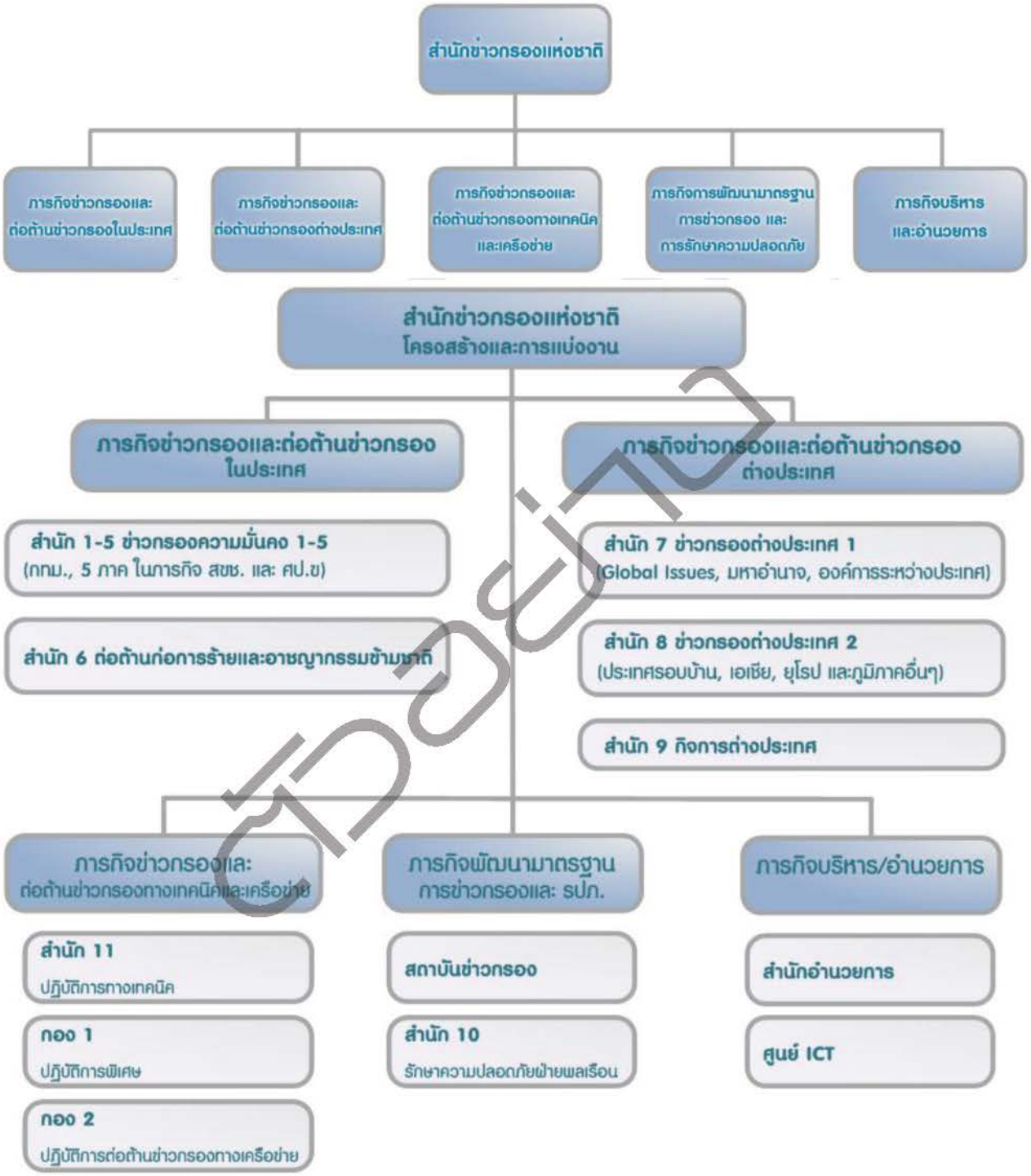
3. เสริมสร้างเอกภาพในประชาคมข่าวกรอง

4. เสริมสร้างความร่วมมือทางด้านข่าวกรองและการรักษาความปลอดภัยในภาคเอกชน องค์กรและภาคประชาชน

5. พัฒนามาตรฐานการรักษาความปลอดภัยในหน่วยงานของรัฐฝ่ายพลเรือนและเครือข่าย

6. ยกระดับสมรรถนะขององค์กรและศักยภาพของบุคลากร โดยยึดหลักธรรมาภิบาล

➢โครงสร้าง



🕮ความรู้ด้านเทคโนโลยีกับการออกแบบ และการดูแลระบบด้านความมั่นคงปลอดภัย

➢การออกแบบเทคโนโลยี

เทคโนโลยี หมายถึง การประยุกต์เอาความรู้ทางด้านวิทยาศาสตร์ มาใช้ให้เกิดประโยชน์ และเป็นหัวใจของการสร้างมูลค่าเพิ่มให้กับสินค้าและผลิตภัณฑ์

เช่น การนำทรายซึ่งเป็นสารประกอบของซิลิกอนที่มีราคาต่ำ มาสกัดเอาสารซิลิกอนให้บริสุทธิ์ และเจือสารบางอย่างให้เกิดเป็นสิ่งที่เรียกว่าสารกึ่งตัวนำ นำมาผลิตเป็นทรานซิสเตอร์และไอซี ซึ่งไอซีนี้เป็นอุปกรณ์ที่รวมวงจรอิเล็กทรอนิกส์จำนวนมากไว้ด้วยกัน ใช้ทำชิพ ซึ่งเป็นส่วนสำคัญของคอมพิวเตอร์ ทำให้มีราคาสูง เทคโนโลยีจึงเป็นหนทางที่จะช่วยพัฒนาให้สินค้าและบริการต่าง 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

ในช่วงสองทศวรรษทีผ่านมา วิทยาศาสตร์ และ เทคโนโลยี ได้มีบทบาทสำคัญเพิ่มขึ้นจนสามารถสร้างนวัตกรรม (Innovation) ซึงก็คือ การเรียนรู้ การผลิตและ การใช้ประโยชน์จากความคิดใหม่ ให้เกิดผลทั้งทางเศรษฐกิจ สังคม การเมือง สิ่งแวดล้อม และวัฒนธรรม เทคโนโลยีทำให้สังคมโลกทีเรียบง่าย กลายเป็นสังคมที่มีการดำรงชีวิตที สลับซับซ้อนมากขึ้น ก่อให้เกิดกระแสแห่งความไร้พรมแดน หรือกระแสโลกาภิวัฒน์ทีเข้ามาสู่ทุกประเทศอย่าง รวดเร็ว จากความก้าวหน้าของเทคโนโลยีสารสนเทศ อันเป็นการผสมผสาน 4 ศาสตร์ เข้าด้วยกันได้แก่ อิเล็อทรอนิกส์ โทรคมนาคม และข่าวสาร (Electronics , Computer , Telecommunication and Information หรือเรียกย่อๆ ว่า ECTI) ทำให้สังคมโลกสามารถสื่อสารกันได้ทุกแห่งทั่วโลกอย่างรวดเร็ว สามารถรับรู้ข่าวสาร ความเคลื่อนไหวต่างๆ ได้พร้อมกัน สามารถบริหาร

จัดการและตัดสินใจได้ทุกขณะเวลา การลงทุนค้าขาย และธุรกรรมการเงินได้อย่างรวดเร็ว ดังนั้น เทคโนโลยีกำลังทำให้โลกใบนี้ “เล็กลง” ทุกขณะ

➢การสร้างสิ่งของใช้ด้วยกระบวนการเทคโนโลยี

กระบวนการเทคโนโลยี หมายถึง กระบวนการบริหารจัดการสร้างหรือผลิตชิ้นงานและซ่อมแซมปรับปรุงแก้ไขชิ้นงานให้มีสภาพการใช้งานได้เป็นอย่างดี ซึ่งเป็นการนำเอาวิทยาการทางศิลปะและวิทยาศาสตร์มาประยุกต์ใช้ให้เกิดประโยชน์กับการทำงานถูกต้องและปลอดภัย 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 สร้างหรือผลิตชิ้นงานต่างๆโดย 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 เขียนแบบและกำหนดรายการประกอบแบบต่อไป

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

6.การประเมินค่า การตรวจสอบประเมินค่าความสำเร็จของผลงาน คือ แบบการสร้างชิ้นงาน ผลิตภัณฑ์ หรือสิ่งของ 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 ในการยึดต่อระหว่างจุดต่างๆ นั้นควรใช้ กาว ตะปู สกรู หรือใช้ข้อต่อแบบใด รู้ถึงวัตถุประสงค์ของการนำไปใช้งาน ความแข็งแรงและการรองรับน้ำหนักของโต๊ะสามารถรองรับได้มากน้อยเพียงใด สีสันควรใช้สีอะไรจึงจะสวยงาม เป็นต้น

– การออกแบบ หมายถึง การปรับปรุงแบบ ผลงานหรือสิ่งต่างๆ ที่มีอยู่แล้วให้เหมาะสม และดูมีความแปลกใหม่ขึ้น เช่น โต๊ะที่เราทำขึ้นมาใช้ เมื่อใช้ไปนานๆก็เกิดความเบื่อหน่ายในรูปทรง หรือสี เราก็จัดการปรับปรุงให้เป็น รูปแบบใหม่ให้สวยกว่าเดิม ทั้งความเหมาะสม ความสะดวกสบายในการใช้งานยังคงเหมือนเดิม หรือดีกว่าเดิม 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 สิ่งที่ผู้คนโดยทั่วไปคำนึงถึงเป็นสิ่งแรกคือ การค้นหาการบุกรุกของผู้ไม่ประสงค์ดีกับระบบคอมพิวเตอร์ซึ่งนิยมเรียกว่า “แฮกเกอร์” รวมถึงการกำจัดโปรแกรมที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของคอมพิวเตอร์ หรือมัลแวร์ประเภทต่างๆ โดยไม่ตระหนักรู้ถึงความหมายที่แท้จริงของ “ความมั่นคงปลอดภัย” ของระบบคอมพิวเตอร์ ซึ่งแท้จริงแล้วมีความหมายครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรในระบบคอมพิวเตอร์ในทุกๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการ ซอฟต์แวร์ต่างๆ ที่ถูกติดตั้ง และการเชื่อมต่อกันเป็นเครือข่าย และรวมถึงข้อมูลหรือสารสนเทศซึ่งถูกจัดเก็บและประมวลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อเป็นระบบ ความหมายของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์จึงมีขอบเขตมากกว่าการรักษาความมั่นคงปลอดภัยให้กับคอมพิวเตอร์หรืออุปกรณ์เพียงอย่างเดียว

1. ทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศ มีความหมายครอบคลุมถึงเครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อต่างๆ 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 แนวทางทางการเมือง

โดยเมื่อโจมตีสำเร็จอาจได้รับค่าจ้างหรือการยอมรับจากสังคมที่เขาต้องการ เป็นต้น

1.2 ฮาร์ดแวร์และอุปกรณ์ต่อเชื่อมต่าง ๆ (hardware and its peripheral) ในที่นี้มีความหมายรวมถึงเครื่องคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟนซึ่งมีความสามารถในการรับข้อมูล ประมวลผล แสดงผล และเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ได้ ความไม่มั่นคงปลอดภัยของอุปกรณ์เหล่านี้อาจเกิดขึ้นเนื่องจากมีภัยคุกคามเกิดขึ้นกับอุปกรณ์โดยตรง เช่น การขโมย ซึ่งส่งผลให้เจ้าของไม่สามารถใช้งานได้หรือนำข้อมูลส่วนบุคคลในอุปกรณ์นั้นไปเปิดเผยทำให้ความลับของข้อมูลนั้นถูกทำลายลง หรืออาจเกิดจากไฟฟ้ากระชากและทำ ให้ข้อมูลที่จัดเก็บในอุปกรณ์นั้นๆ เสียหาย นอกจากนี้ยังรวมถึงการที่ฮาร์ดแวร์นั้นๆ ถูกทำลายหรือทำให้ใช้การไม่ได้โดยมีสาเหตุจากธรรมชาติ เช่น น้ำท่วม ฟ้าผ่าอุปกรณ์ เป็นต้น

1.3 ซอฟต์แวร์ (software) ที่ถูกพัฒนาขึ้นมักมีข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัย เนื่องจากคุณสมบัตินี้มักถูกละเลยในระหว่างขั้นตอนการวิเคราะห์และพัฒนาซอฟต์แวร์นั้นๆ ทำให้เมื่อมีการนำมาใช้งานมักจะมีช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์เราเตอร์ส□ำหรับใช้งานอินเทอร์เน็ตสำหรับเชื่อมต่อผ่านระบบเอดีเอสแอลบางรุ่นมีข้อบกพร่องเกี่ยวกับความมั่นคงปลอดภัย และเมื่อผู้ไม่ประสงค์ดีโจมตีระบบสำเร็จจะสามารถปลอมแปลงกระบวนการสอบถามโดเมนเนมได้ เป็นต้น

ดังนั้นผู้ใช้งานหรือผู้ดูแลระบบ จะต้องดำเนินการ ปรับปรุงคุณสมบัติซอฟแวร์ตามหลังอยู่เสมอๆ ทั้งนี้การปรับปรุงคุณสมบัติดังกล่าว ผู้พัฒนาซอฟต์แวร์อาจสร้างช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยไม่ได้ตั้งใจก็เป็นได้

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

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

1.6 เครือข่าย (network) ระบบสารสนเทศในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่ายการรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และมักเชื่อมต่อกับเครือ ข่ายอินเทอร์เน็ต แม้ว่าการเชื่อมต่อกันดังที่ได้กล่าวมาจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจาก

ระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่ายยิ่งมีขนาดมากเท่าไรย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตี และเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้น

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

2. การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัย หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้นๆ ในที่นี้จะยกตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลซึ่งอาจมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่างๆ 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

---

[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

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

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

2.4 ความมั่นคงปลอดภัยของการสื่อสาร (communication security) เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่างๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่างๆ ที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขาซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้ เป็นต้น

2.5 ความมั่นคงปลอดภัยของเครือข่าย (network security) เพื่อป้องกันการเข้าถึงอุปกรณ์เครือข่ายต่างๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่างๆ 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 และหลักการอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.1 หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กรหรือบุคคลนั้นๆ ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริม

สร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้ และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม

3.1.1 การรักษาความลับ (confidentiality) หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญเช่น ข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ข้อมูลส่วนบุคคลอื่นๆ เช่น หมายเลขประจำตัวประชาชน กำหนดการของบุคคลสำคัญ รายชื่อผู้โดยสารของเที่ยวบินต่างๆ 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 และอาจหมายรวมถึงเจ้าหน้าที่ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น

ภาพ องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากภาพ จะเห็นว่าทรัพยากรสารสนเทศที่ต้องการให้มีความมั่นคงปลอดภัยนั้นอาจถูกจัดเก็บอยู่ในฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) หรือถูกส่งผ่านระบบการสื่อสาร (communication) ก็เป็นได้ และการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรสารสนเทศนั้นจะมีความเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางกายภาพ (physical security) ในทุกระดับโดยการจัดให้มีเทคโนโลยีและกระบวนการที่เหมาะสมสำหรับการเข้าถึงทางกายภาพต่อฮาร์ดแวร์ ซอฟต์แวร์ และระบบ

การสื่อสาร นอกจากนี้ยังมีความจำเป็นต้องสร้างการรักษาความมั่นคงปลอดภัยส่วนบุคคล (personal security) เนื่องจากมนุษย์เป็นจุดอ่อนที่สุดของระบบการรักษาความมั่นคงปลอดภัย และมักละเมิดกฎเกณฑ์ที่จำเป็น ทั้งนี้ อาจแก้ไขได้โดยการสร้างความตระหนักรู้ถึงเหตุผลและความสำคัญของการรักษาความมั่นคงปลอดภัย เป็นต้น ทั้งนี้มาตรการและเทคโนโลยีที่นำมาใช้จะต้องมีการกำหนดให้สอดคล้องกับการจัดการรักษาความมั่นคงปลอดภัยในระดับองค์กร โดยการกำหนดยุทธศาสตร์ นโยบายและกฎระเบียบที่เกี่ยวข้อง ตลอดจนมีการกำกับดูแลอย่างเหมาะสม

3.2 หลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศจึงเป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงาน และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของทรัพยากรสารสนเทศนั้นๆ

3.2.1 ช่องโหว่ (vulnerability) คือ ความบกพร่องหรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศ โดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์ การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้นๆ เช่น ช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของซอฟต์แวร์เว็บเบราว์เซอร์ การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญๆ ที่เกี่ยวข้องกับกระบวนการทำงาน โดยไม่มีการตรวจสอบ หรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะ ดังต่อไปนี้

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

2) ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่างๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้นๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์และซอฟต์แวร์ระบบอื่นๆ 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

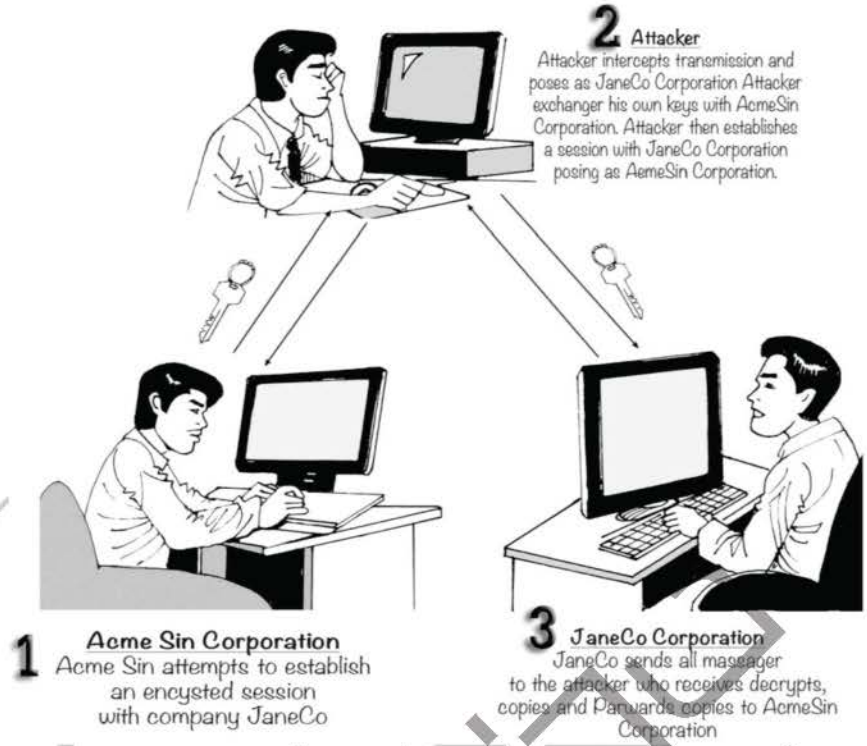
จำแนกได้ 4 ลักษณะคือ

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 แฟลชไดร์ฟโดยที่นักศึกษาไม่ทราบ 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 การกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่างๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียง

อย่างเดียวก็เป็นได้ เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่ อันเป็นการทำลายความลับของทรัพยากรนั้นๆ ทั้งนี้ การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือ การโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการ และการโจมตีด้วยเทคนิคเชิงสังคมอื่นๆ 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 รวมไปถึงบุคคลทั่วๆ 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 นอกจากนี้ยัง

หมายถึงเทคนิคเทคนิควิธีใช้ในการโจมตี 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

----------✍