เอกสารประกอบการสอบคัดเลือก

น.ประทวนเลื่อนฐานะเป็น น.สัญญาบัตร

โควตา น.ประทวนทำหน้าที่ในตำแหน่ง น.สัญญาบัตร

วิชาสงครามไซเบอร์และการรักษาความปลอดภัยระบบสารสนเทศ

วิชากฎหมาย ข้อบังคับ และระเบียบเกี่ยวกับคอมพิวเตอร์
และการรักษาความปลอดภัยระบบสารสนเทศของ ทอ.

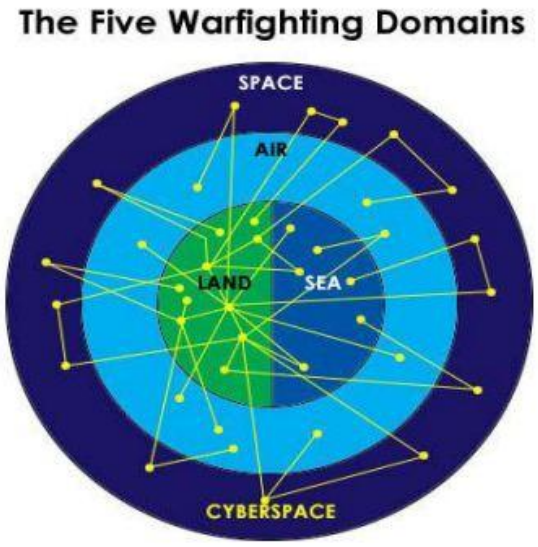
สงครามไซเบอร์

สารบัญ

บทที่ ๑
Introduction to Cyber Operations
ปฐมบทการปฏิบัติการสงครามไซเบอร์

สงครามไซเบอร์ คือ ความขัดแย้งที่มีพื้นที่ทำสงครามครอบคลุมในส่วนของคอมพิวเตอร์และอินเตอร์เน็ตโดยเป็นปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้ามและต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา ส่วนมากจะมีแรงจูงใจทางการเมือง ทางเศรษฐกิจหรือแม้กระทั่งความสัมพันธ์ระดับประเทศ หากจะกล่าวว่าเป็นวิธีการใดๆก็ตามที่ทำให้เราคาดว่าจะได้รับชัยชนะตามวัตถุประสงค์ส่วนบุคคล ส่วนองค์กร ผ่านการใช้อุปกรณ์เทคโนโลยีที่สามารถติดต่อสื่อสารได้ก็คงไม่ผิดไปนัก

ไซเบอร์สเปซ คือ พื้นที่ทำการรบ งงไหมครับ หากเปรียบเทียบให้เห็นภาพกับสงครามโลกครั้งที่ ๒ การสู้รบด้วยทหารราบ รถถัง พื้นที่ทำการรบคือบนพื้น (Ground Space) เรือรบ เรือดำน้ำ เรือบรรทุกเครื่องบินมีพื้นที่ทำการรบทางน้ำ (Sea Space) เครื่องบินลำเลียง เครื่องบินขับไล่ เครื่องบินทิ้งระเบิดมีพื้นที่ทางการรบทางอากาศ (Air Space) พื้นที่ทางการรบของไซเบอร์สเปซก็คือการติดต่อสื่อสารแลกเปลี่ยนข้อมูล ในรูปแบบใดๆผ่านอุปกรณ์ต่างๆของทั้งการปฏิบัติการทางบก ทางเรือ ทางอากาศ นั่นเอง



รูปที่ ๑.๑ ภาพประกอบพื้นที่ทำการรบในส่วนของไซเบอร์สเปซ

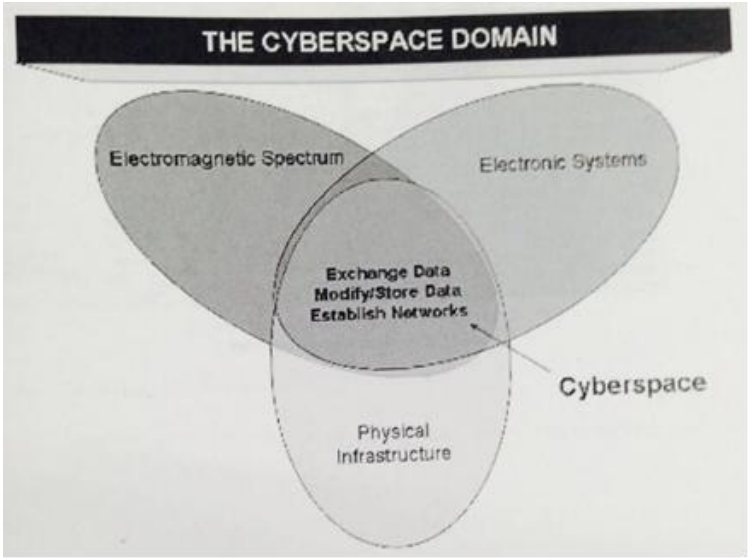
๑.๑ คุณลักษณะของไซเบอร์สเปซ

ลักษณะการทำงานในส่วนของไซเบอร์สเปซ ที่ใช้ในการแลกเปลี่ยนข้อมูลติดต่อสื่อสารผ่านกองกำลังทางบก ทางน้ำ ทางอากาศและอวกาศนั้น จะมีองค์ประกอบที่สำคัญๆอยู่สามอย่างด้วยกันคือ

๑. Electromagnetic Spectrum หรือ สเปกตรัมแม่เหล็กไฟฟ้า ประกอบไปด้วยคลื่นวิทยุ ทั้งระบบ A.M. ระบบ F.M. คลื่นโทรทัศน์ และไมโครเวฟ รังสีอินฟราเรด แสง รังสีอัลตร้าไวโอเลต รังสีเอกซ์ รังสีแกมมา

๒. Electronic Systems คือ การรวมกลุ่มของอุปกรณ์ วงจรอิเล็กทรอนิกส์ และส่วนประกอบต่างๆ ที่ถูกออกแบบมาสำหรับการทำงานของอุปกรณ์ที่มีฟังก์ชันการใช้งานที่ซับซ้อน ยกตัวอย่างเช่น ระบบสื่อสารโทรคมนาคม ระบบคอมพิวเตอร์ ระบบผลิตพลังงาน ระบบเรดาห์ ระบบเสียง เพลง อิเล็กทรอนิกส์ และอื่นๆ อีกมาก

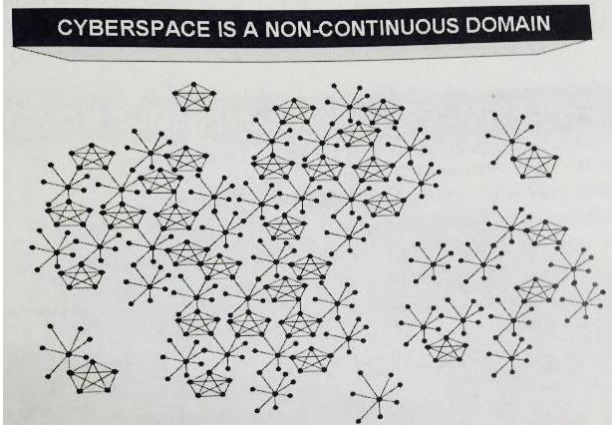
๓. Physical Infrastructure คือ โครงสร้างพื้นฐานทางกายภาพที่จับต้องได้ ไม่ว่าจะเป็นอุปกรณ์ที่เกี่ยวกับระบบธุรกิจ ระดับชาติ การขนส่ง การสื่อสาร ระบบการผลิตน้ำ กระแสไฟฟ้า ซึ่งโดยส่วนมากจะเป็นการลงทุนที่มีค่าใช้จ่ายค่อนข้างสูง



รูปที่ ๑.๒ องค์ประกอบที่ทำให้เกิดไซเบอร์สเปซ

ไซเบอร์สเปซเป็นโดเมนที่ไม่ได้ต่อเนื่องกัน

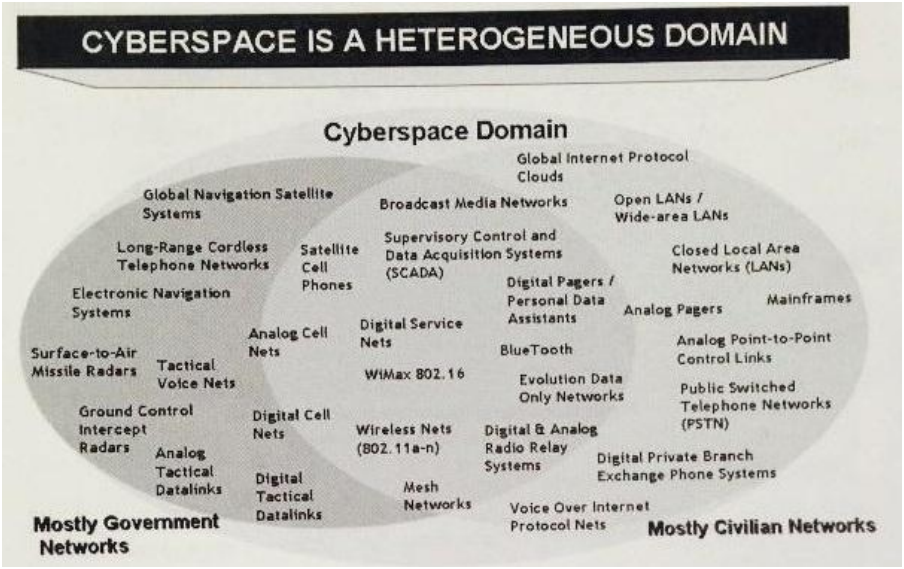
แม้ว่าไซเบอร์สเปซจะก่อให้เกิดการเชื่อมโยงกันอย่างมหาศาลมากขึ้นเรื่อยๆโดยเฉพาะการเชื่อมต่อระดับสากลหรือแทบจะทั้งโลก (Interconnected) แต่การเชื่อมต่อเน็ตเวิร์กในขอบเขตดังกล่าวนี้ได้ถูกแบ่งออกเป็นหลายๆส่วน ได้แก่ โปรโตคอล ไฟร์วอลล์ การเข้ารหัส และอุปกรณ์ที่ใช้งานผ่านเน็ตเวิร์กที่หลากหลาย ซึ่งทั้งหมดนี้ได้ถูกแยกออกจากกัน ตัวอย่างก็เช่น มีคอมพิวเตอร์อีกมากมายหลายเครื่องที่ไม่ได้เชื่อมต่อกับอินเตอร์เน็ต แต่ถูกแยกออกไปใช้เพื่อวัตถุประสงค์และมีการเชื่อมต่อเฉพาะทาง



รูปที่ ๑.๓ แสดงให้เห็นภาพว่าไซเบอร์สเปซเป็นโดเมนที่ไม่ได้เชื่อมต่อกันทั้งหมด

ไซเบอร์สเปซเป็นโดเมนที่มีลักษณะเฉพาะต่างกัน

เนื่องจากมีหน่วยงานที่สร้างไซเบอร์สเปซของตัวเองโดยมีจุดมุ่งหมายและความต้องการที่ต่างกัน แท้ที่จริงแล้วมันคือการรวบรวมกลุ่มของระบบหลายๆระบบ โดยอีกนัยหนึ่ง ไซเบอร์สเปซก็คือการกำเนิดขึ้นของเน็ตเวิร์กที่มีชนิดแตกต่างกัน มีฟังก์ชันการใช้งานที่แตกต่างกัน ระดับการเชื่อมต่อ ความซับซ้อนของเทคโนโลยีและช่องโหว่ที่แตกต่างกัน จะเห็นจากรูปที่ ๑.๔ ด้านล่างว่าไซเบอร์สเปซเหล่านั้นมีความสามารถในการแลกเปลี่ยนข้อมูลข่าวสารด้วยเทคโนโลยี อินเตอร์เฟซ และ โปรโตคอลที่ไม่เหมือนกันเลย ซึ่งจากกลุ่มไซเบอร์สเปซเหล่านี้ได้ก่อให้เกิดนวัตกรรมขั้นสูงให้กับแวดวงอุตสาหกรรมการติดต่อสื่อสาร คอมพิวเตอร์ และอิเล็กทรอนิกส์เป็นอย่างมาก



รูปที่ ๑.๔ ไซเบอร์สเปซที่มีความแตกต่างกันไปก่อให้เกิดนวัตกรรมใหม่ๆในแวดวงอุตสาหกรรม

ไซเบอร์สเปซมีการเปลี่ยนแปลงอย่างรวดเร็ว

ไซเบอร์สเปซส่วนมากจะถูกนำไปใช้และขับเคลื่อนในวงการพาณิชย์ ซึ่งโดเมนนี้มีวิวัฒนาการและสามารถขยายตัวด้วยความรวดเร็วดังที่เราเห็นเทคโนโลยีการติดต่อสื่อสารในปัจจุบัน สามารถพูดได้อีกนัยหนึ่งว่าส่วนของไซเบอร์สเปซมีส่วนในการผลักดันนวัตกรรมใหม่ๆออกมาอย่างต่อเนื่อง รวมถึงยังมีการแทนที่ปรับเปลี่ยน และอัพเดทโปรโตคอลอยู่ตลอดเวลา อาจจะเพราะเนื่องจากไซเบอร์สเปซเป็นปฏิบัติการที่มีความรวดเร็วมากเพราะอิเล็กตรอนนั้นเดินทางด้วยความเร็วแสงและก่อให้เกิดผลลัพธ์ทางการกระทำแทบจะทันทีทันใด ตัวอย่างเช่นประเทศสหรัฐอเมริกานั้นสามารถโจมตี และถูกโจมตีอย่างรวดเร็วจากโดเมนภายนอกผ่านการเชื่อมต่อเครือข่ายใหญ่ๆเช่นอินเตอร์เน็ต ซึ่งเรื่องนี้สามารถเกิดขึ้นได้ข้ามพรมแดนโดยผู้ที่โจมตีอาจจะอยู่คนละซีกโลกกันเลยทีเดียว

ไซเบอร์สเปซประกอบไปด้วยพื้นที่ทางการรบทั้งทางด้านตรรกะและกายภาพ

ในส่วนของไซเบอร์สเปซนั้นถูกเชื่อมโยงโดยโครงสร้างพื้นฐานทางกายภาพ ระบบอิเล็กทรอนิกส์ผ่านทางการใช้สเปกตรัมแม่เหล็กไฟฟ้า EMS (Electro-Magnetic Systems) ตามที่ได้กล่าวไปข้างต้น ซึ่งเมื่อมีการคิดค้นระบบและโครงสร้างพื้นฐานใหม่ๆ ก็จะทำให้เกิดการใช้ EMS ที่มากขึ้น ระบบอาจจะถูกออกแบบให้เปลี่ยนคลื่นความถี่ เช่นเมื่อมีการส่งผ่านข้อมูล ส่งผลให้รูปแบบการรบเปลี่ยนแปลงไปแต่นั่นก็ยังอยู่ในรูปแบบการใช้งาน EMS ภายใต้ขอบเขตของไซเบอร์สเปซอยู่ดี

ระบบอิเล็กทรอนิกส์นั้นมีความสามารถในการเชื่อมกันระหว่างเทคนิคและโปรโตคอลซึ่งใช้ในการตรวจสอบได้หากมี “เอกลักษณ์”บางอย่างที่กำลังมองหาการเชื่อมต่อเข้าไปในระบบ ซึ่งการป้องกันเอกลักษณ์ที่ไม่พึงประสงค์เหล่านี้สามารถป้องกันได้โดยการเขียนโค้ดหรือการคิดเชิงตรรกะในระบบอิเล็คทรอนิกส์ เมื่อมีการเชื่อมต่อกันระหว่างระบบสองระบบเกิดขึ้น ผู้โจมตีก็จะใช้ประโยชน์จากความผิดพลาดทางการป้องกันเพื่อเข้าไปในอีกระบบ การเขียนโค้ดนั้นเป็นการคิดเชิงตรรกะผ่านทางไซเบอร์สเปซ ในเมื่อผู้โจมตีใช้ประโยชน์จากการเขียนโค้ดในการป้องกันที่มีช่องโหว่ ในฐานะฝ่ายป้องกันต้องระวังสิ่งผิดปกติในระบบของตัวเอง หรืออาจเขียนและปรับเปลี่ยนโค้ดเพื่อให้สามารถป้องกันช่องโหว่ในจุดนั้นได้ ซึ่งก็จะส่งผลให้ผู้โจมตีค้นหาวิธีการและช่องโหว่ใหม่ๆเสมอเป็นวัฏจักรที่ไม่มีวันจบสิ้นแม้ว่าภารกิจของผู้โจมตีจะลุล่วงหรือผู้ที่ทำการป้องกันไม่ต้องกังวลกับการโจมตีอีกแล้ว ทั้งนี้ก็เพื่อที่ต่างฝ่ายต่างก็ต้องการที่จะอยู่ในตำแหน่งที่มีความได้เปรียบตลอดไปในระยะยาวนั่นเอง

๑.๒ คอนเซปท์ของไซเบอร์สเปซ

ไซเบอร์สเปซนั้นมีจุดมุ่งหมายที่จะครอบครองชัยภูมิหรือตำแหน่งที่เหนือกว่าอีกฝ่ายหนึ่งโดยทำการปฏิการทางด้านไซเบอร์สเปซที่เชื่อมต่อกันอยู่ภายในเวลาที่จำกัดโดยที่ไม่ได้รับการอนุญาตอย่างถูกต้องจากอีกฝ่ายหนึ่ง พื้นฐานการออกแบบด้านการปฏิบัติการและปรัชญาการวางแผนเพื่อที่จะนำมาปรับใช้กับโดเมนนี้ โดยการปฏิบัติการนี้จะสามารถครอบครองความได้เปรียบทางด้านไซเบอร์สเปซ ซึ่งจะมีศักยภาพมากที่สุดเมื่อนำมาปรับใช้กับศูนย์ปฏิบัติการทางอากาศและอวกาศ (Air and Space Operation Center) หรือ AOC โดยหน้าที่หลักๆก็คือการเตรียมตัวระวังป้องกันภัยทางไซเบอร์จากสถานการณ์รอบตัวที่อาจเกิดขึ้น

การตอบโต้กลับทางไซเบอร์ก็เป็นภารกิจอีกรูปแบบหนึ่งซึ่งเป็นการปฏิบัติการร่วมกันระหว่างการปฏิบัติการเชิงรุกและการปฏิบัติการเชิงรับ เพื่อรักษาความได้เปรียบทางด้านไซเบอร์ โดยภารกิจการตอบโต้กลับทางไซเบอร์จะจัดการมาตรการตอบโต้โดยอ้างอิงตามระดับของภัยคุกคามที่ได้ประสบ ซึ่งอาจจะเป็นการเข้าควบคุมสถานการณ์หรือรอจังหวะเพื่อโจมตีกลับ

๑.๓ Offensive Counter-Cyber (OCC) การตอบโต้ทางไซเบอร์เชิงรุก

การปฏิบัติการเชิงรุกโดยการระงับ ลดทอน แทรกแซง ทำลาย หรือ หลอกล่อ ขโมยความสามารถของศัตรูที่ใช้ในไซเบอร์สเปซ รวมถึงการใช้งานอุปกรณ์อิเล็คทรอนิกส์ เน็ตเวิร์คและระบบอื่นๆ ซึ่งใช้ Electromagnetic Spectrum ในสภาพแวดล้อมทางไซเบอร์สเปซ โดยการปฏิบัติการเชิงรุกนั้นจะขึ้นตามรูปแบบหลักๆอยู่ ๘ ขั้นตอน ซึ่งการปฏิบัติการเชิงรุกจะประกอบไปด้วยขั้นตอนเหล่านี้เพียง ๑ - ๒ ขั้นตอนก็เป็นได้ แต่อย่างไรก็ตามจะต้องเป็นไปตามลำดับ ซึ่งขั้นตอนการปฏิบัติการเชิงรุกจะประกอบไปด้วย

๑. การตรวจสอบช่องโหว่

๒. ตรวจสอบเส้นทางที่เข้าถึง

๓. ทดสอบช่องโหว่และเส้นทางเชื่อมต่อโดยการปิดระบบหรือ ออฟไลน์

๔. ค้นหาข้อมูลและช่องทางที่เป็นประโยชน์ หรือการลองแหย่ฝั่งตรงข้ามดู

๕. สำรวจระบบเน็ตเวิร์คและสังเกตการณ์ปฏิบัติการของฝั่งตรงข้าม

๖. ดึงข้อมูลออกมา

๗. จำลองตัวอย่างการโจมตีทางเน็ตเวิร์ค แอพพลิเคชั่น และรายบุคคล

๘. ทำการโจมตีระบบเน็ตเวิร์ค แอพพลิเคชั่น และรายบุคคลจริงๆ

โดยขั้นตอนแรกๆของการปฏิบัติการไซเบอร์เชิงรุกก็คือ ทำการสำรวจช่องโหว่ในแอพพลิเคชั่นเครื่องเป้าหมาย หรือโครงสร้างของเครือข่ายและทดสอบเชื่อมต่อผ่านช่องโหว่เหล่านั้น ช่องโหว่ที่อยู่ภายในองค์ประกอบโครงสร้างหลายๆแอพพลิเคชั่นนั้น สามารถตรวจสอบได้เพราะแอพพลิเคชั่นเหล่านั้นมีขายอยู่ในท้องตลาดออนไลน์ และสามารถหาซื้อขายได้ทั่วไป เส้นทางที่เชื่อมต่อนั้น บ่อยครั้งจะถูกเปิดเผยโดยเทคโนโลยีที่สูงขึ้น ซึ่งวิศวกรทางด้านไอที ก็ต้องคอยดูแลระบบเฉพาะทางเหล่านั้นและพยายามจัดการปัญหาที่เกิดขึ้นมาใหม่ๆอยู่อย่างต่อเนื่อง

๑.๔ Defensive Counter-Cyber (DCC) การตอบโต้ทางไซเบอร์เชิงรับ

มาตรการป้องกันทุกรูปแบบในการตรวจสอบ ทำลาย ลบล้าง หรือลดทอนกองกำลังของศัตรูซึ่งพยายามที่จะเจาะหรือการโจมตีผ่านโลกไซเบอร์ การป้องกันตอบโต้กลับไซเบอร์รวมถึง การปฏิบัติการไซเบอร์ป้องกันเชิงรุกและเชิงรวมทั้งหมด

มาตรการป้องกันออกแบบมาเพื่อทำลายกองกำลังฝ่ายตรงข้ามโจมตีหรือจะ ปฏิเสธหรือลดประสิทธิภาพของฝ่ายตรงข้าม โดยการป้องกันและตอบโต้กลับทางไซเบอร์จะรวมถึงมาตรการที่จะรักษาป้องกัน, การกู้คืนและ ความสามารถในการสร้างมิตรภาพกับโลกไซเบอร์ก่อนระหว่างและหลังจากการโจมตีฝ่ายตรงข้าม การป้องกันทางไซเบอร์จากฝ่ายตรงข้ามมีทั้งหมด ๔ ขั้นตอนดังนี้

๑. สำรวจระบบเน็ตเวิร์ค

๒. พยายามค้นหาผู้บุกรุกและการกระทำอื่นๆที่อาจเกี่ยวข้อง

๓. อุดช่องโหว่ ป้องกันการบุกรุกและกิจกรรมอื่นๆ

๔. ทำการโจมตีตอบโต้กลับ

บทที่ ๒

Information Access and Cyber Risk

การเข้าถึงข้อมูลในรูปแบบต่างๆ และการตระหนักถึงการระวังป้องกันความเสี่ยง

ทุกวันนี้ คงไม่มีองค์กรใดที่ไม่มี Website เป็นของตัวเอง บางองค์กรหรือหน่วยงานอาจจะเช่า Web Hosting อยู่ หรือ บางองค์กรอาจมี Web Site เป็นของตนเองอยู่ในระบบเครือข่ายขององค์กร โดยมีการต่อเชื่อมเครือข่ายขององค์กรด้วย Frame Relay, ADSL หรือ Leased Line เข้ากับระบบเครือข่ายของ ISP ซึ่งส่วนใหญ่ก็จะมีการจัดซื้อ Firewall มาใช้ป้องกันระบบเครือข่ายภายในขององค์กร กับ ระบบอินเทอร์เน็ตจาก ISP และ มีการเปิดให้คนภายนอกสามารถเข้ามาเยี่ยมชม Web Site ได้ โดยเปิด Port TCP ๘๐ (http) และ Port TCP ๔๔๓ (https) ในกรณีที่ใช้โปรโตคอล SSL ในการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น

ปัญหาก็คือ ในเมื่อทุกองค์กรต้องเปิดทางให้มีการเข้าชม Web Site ทั้งแบบ Plain text traffic (Port ๘๐) และแบบ Encrypted text traffic (port ๔๔๓) ทำให้แฮกเกอร์สามารถจู่โจม Web Site ของเราโดยไม่ต้องเจาะผ่าน Firewall เนื่องจากเป็น Port ที่ Firewall มีความจำเป็นต้องเปิดใช้อยู่แล้ว

ใน โลกของ E-Commerce มีอัตราการใช้งาน Web Server ที่เพิ่มขึ้นทุกวัน (ดูข้อมูลจากwww.netcraft.com) และ จากข้อมูลของ UNCTAD (http://www.unctad.org) พบว่า Web Server ทั่วโลก มีทั้งแบบที่เข้ารหัสด้วย SSL แล้ว และ แบบไม่เข้ารหัสด้วย SSL ก็ยังคงมีใช้กันอยู่

ในเมื่อแฮกเกอร์มองเห็นช่องที่เรามีความจำเป็น ต้องเปิดใช้งานผ่านทาง Web Server และ Web Application แฮกเกอร์ในปัจจุบันจึงใช้วิธีที่เรียกว่า “Web Application Hacking” ในการเจาะเข้าสู่ระบบขององค์กรต่างๆ ทั่วโลก ขณะนี้มีการจู่โจมระบบโดยกลุ่มแฮกเกอร์ที่ต้องการทำสถิติ ในการเจาะ Web Site ดูรายละเอียดได้ที่ http://www.zone-h.org ดังนั้น ผู้ที่มี Web Site อยู่ และ โดยเฉพาะผู้ที่ต้องการหันมาทำธุรกิจในลักษณะของ E-commerce ซึ่งต้องมี Web Site ที่ใช้ Web server ที่เชื่อถือได้ และมีการเขียน Web application โดยคำนึงถึงเรื่อง “Security” เป็นหลัก จึงมีความจำเป็นอย่างยิ่งที่ต้องเรียนรู้ช่องโหว่ (Vulnerability) ของ Web application ที่แฮกเกอร์ชอบใช้ในการเจาะระบบ Web application ของเราซึ่งรวบรวมได้ทั้งหมด ๑๐ วิธีด้วยกัน (Top ๑๐ Web Application Hacking)

ตลอดจนเรียนรู้วิธีการป้องกันที่ถูกต้อง เพื่อที่จะไม่ให้ตกเป็นเหยื่อของเหล่าแฮกเกอร์ที่จ้องคอยเจาะระบบเราอยู่ ผ่านทาง Web Site ที่ยังไงเราก็ต้องเปิดให้เข้าถึง และ ยังมี Virus Worm ตัวใหม่ๆ ที่เขียนขึ้นเพื่อจู่โจม Port ๘๐ (HTTP)และ Port ๔๔๓ (SSL) โดยเฉพาะอีกด้วย รายละเอียดของ Top ๑๐ Web Application Hacking มี ๑๐ วิธี ดังนี้

๒.๑ Unvalidated Input

หมายถึง การที่ข้อมูลจากฝั่ง client ที่ส่วนใหญ่แล้ว จะมาจาก Internet Explorer (IE) Browser ไม่ได้รับการตรวจสอบก่อนถูกส่งมาประมวลผลโดย Web Application ที่ทำงานอยู่บน Web Server ทำให้แฮกเกอร์สามารถดักแก้ไขข้อมูลในฝั่ง client

ก่อนที่จะถูกส่งมายังฝั่ง server โดยใช้โปรแกรมที่สามารถดักข้อมูลได้ เช่น โปรแกรม Achilles เป็นต้น ดังนั้น ถ้าเรารับข้อมูลจากฝั่ง client โดยไม่ระมัดระวัง หรือ คิดว่าเป็นข้อมูลที่เราเป็นคนกำหนดเอง เช่น เทคนิคการใช้ Hidden Field หรือ Form Field ตลอดจนใช้ข้อมูลจาก Cookies เราอาจจะโดนแฮกเกอร์แก้ไข

ข้อมูลฝั่ง client ด้วย โปรแกรมดังกล่าวแล้วส่งกลับมาฝั่ง server ในรูปแบบที่แฮกเกอร์ต้องการ และมีผลกระทบกับการทำงานของ Web Application ในฝั่ง web server

วิธีการป้องกัน

เราควรจะตรวจสอบข้อมูลที่รับมาจากทั้ง ๒ ฝั่ง คือ ข้อมูลที่รับมาจาก client ผ่านทาง Browser และข้อมูลที่รับมาประมวลผลที่ web server โดยตรวจสอบที่ web server อีกครั้งก่อนนำไปประมวลผลด้วย Web application เราควรมีการฝึกอบรม Web Programmer ของเราให้ระมัดระวังในการรับ input จากฝั่ง client ตลอดจนมีการ Review Source code ไม่ว่าจะเขียนด้วย ASP, PHP หรือ JSP Script ก่อนที่จะนำไปใช้งานในระบบจริง ถ้ามีงบประมาณด้านรักษาความปลอดภัย ก็แนะนำให้ใช้ application level firewall หรือ Host-Based IDS/IPS ที่สามารถมองเห็น Malicious content และป้องกันในระดับ application layer

๒.๒ Broken Access Control

หมายถึง มีการป้องกันระบบไม่ดีพอเกี่ยวกับการกำหนดสิทธิของผู้ใช้ (Permission) ที่สามารถจะ Log-in /Log-on เข้าระบบ Web application ได้ ซึ่งผลที่ตามมาก็คือ ผู้ที่ไม่มีสิทธิเข้าระบบ (Unauthorized User) สามารถเข้าถึงข้อมูลที่เราต้องการป้องกันไว้ไม่ให้ Unauthorized User เข้ามาดูได้ เช่น เข้ามาดูไฟล์ข้อมูลบัตรเครดิตลูกค้าที่เก็บอยู่ใน Web Server หรือ เข้าถึงไฟล์ข้อมูลในลักษณะ Directory Browsing โดยเห็นไฟล์ทั้งหมดที่อยู่ใน web Server ของเรา ปัญหานี้เกิดจากการกำหนด File Permission ไม่ดีพอ และอาจเกิดจากปัญหาที่เรียกว่า “Path Traversal” หมายถึง แฮกเกอร์จะลองสุ่มพิมพ์ path หรือ sub directory ลงไปในช่อง URL เช่น http://www.abc.com/../../customer.mdb เป็นต้น นอกจากนี้อาจเกิดจากปัญหาการ cache ข้อมูลในฝั่ง client ทำให้ข้อมูลที่ค้างอยู่ cache ถูกแฮกเกอร์เรียกกลับมาดูใหม่ได้ โดยไม่ต้อง Log-in เข้าระบบก่อน

วิธีการป้องกัน

พยายามอย่าใช้ User ID ที่ง่ายเกินไป และ Default User ID ที่ง่ายต่อการเดา โดยเฉพาะ User ID ที่เป็นค่า default ควรลบทิ้งให้หมด สำหรับปัญหา Directory Browsing หรือ Path Traversal นั้น ควรมีการ set file system permission ให้รัดกุม เพื่อป้องกัน ช่องโหว่ที่อาจถูกโจมตี และ ปิด file permission ใน sub directory ต่างๆ ที่ไม่ได้ใช้ และ ไม่มีความจำเป็นต้องให้คนภายนอกเข้า เพื่อป้องกันแฮกเกอร์สุ่มพิมพ์ path เข้ามาดึงข้อมูลได้ และควรมีการตรวจสอบ Web Server log file และ IDS/IPS log file เป็นระยะๆ ว่ามี Intrusion หรือ Error แปลกๆ หรือไม่

๒.๓ Broken Authentication and Session Management

หมายถึง ระบบ Authentication ที่เราใช้อยู่ในการเข้าถึง Web Application ของเรานั้นไม่แข็งแกร่งเพียงพอ เช่น การตั้ง Password ง่ายเกินไป, มีการเก็บ Password ไว้ในฝั่ง Client โดยเก็บเป็นไฟล์ Cookie ที่เข้ารหัสแบบไม่ซับซ้อนทำให้แฮกเกอร์เดาได้ง่าย หรือใช้ชื่อ User ที่ง่ายเกินไป เช่น User Admin เป็นต้น บางทีก็ใช้ Path ที่ง่ายต่อการเดาได้ เช่น www.abc.com/admin หมายถึง การเข้าถึงหน้า admin ของระบบ แฮกเกอร์สามารถใช้โปรแกรมประเภท Dictionary Attack หรือ Brute Force Attack ในการลองเดาสุ่ม

Password ของระบบ Web Application ของเรา ตลอดจนใช้โปรแกรมประเภท Password Sniffer ดักจับ Password ที่อยู่ในรูปแบบ Plain Text หรือ บางทีแฮกเกอร์ก็ใช้วิธีง่ายๆ ในการขโมย Password เรา โดยแกล้งปลอมตัวเป็นเรา แล้วแกล้งลืม Password (Forgot Password) ระบบก็จะถามคำถามกลับมา ซึ่งถ้าคำถามนั้นง่ายเกินไป แฮกเกอร์ก็จะเดาคำตอบได้ไม่ยากนัก ทำให้แฮกเกอร์ได้ Password เราไปในที่สุด

วิธีการป้องกัน

ที่สำคัญที่สุด คือการตั้งชื่อ User Name และ Password ควรจะมีความซับซ้อน ไม่สามารถเดาได้ง่าย มีความยาวไม่ต่ำกว่า ๘ ตัวอักษร และมีข้อกำหนดในการใช้ Password (Password Policy) ว่าควรมีการเปลี่ยน Password เป็นระยะๆ ตลอดจนให้มีการกำหนด Account Lockout เช่น ถ้า Logon ผิดเกิน ๓ ครั้ง ก็ให้ Lock Account นั้นไปเลยเป็นต้น การเก็บ Password ไว้ในฝั่ง Client นั้น ค่อนข้างที่จะอันตราย ถ้ามีความจำเป็นต้องเก็บในฝั่ง Client จริงๆ ก็ควรมีการเข้ารหัสที่ซับซ้อน (Hashed or Encrypted) ไม่สามารถถอดได้ง่ายๆ การ Login เข้าระบบควรผ่านทาง https protocol คือ มีการใช้ SSL เข้ามาร่วมด้วย เพื่อเข้ารหัส Username และ Password ให้ปลอดภัยจากพวกโปรแกรม Password Sniffing ถ้ามีงบประมาณควรใช้ Two-Factor Authentication เช่น ระบบ One Time Password ก็จะช่วยให้ปลอดภัยมากขึ้น การใช้ SSL ควรใช้ Digital Certificate ที่ได้รับการ Sign อย่างถูกต้องโดย CA (Certificate Authority) ถ้าเราใช้ CA แบบ Self Signed จะทำให้เกิดปัญหา Man in the Middle Attack (MIM) ทำให้แฮกเกอร์สามารถเจาะข้อมูลเราได้แม้ว่าเราจะใช้ SSL แล้วก็ตาม (ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับ SSL Hacking ดูที่ http://www.acisonline.net)

๒.๔ Cross Site Scripting (XSS) Flaws

หมายถึง แฮกเกอร์สามารถใช้ Web Application ของเรา เช่น ระบบ Web Board ในการฝัง Malicious Script แฝงไว้ใน Web Board แทนที่จะใส่ข้อมูลตามปกติ เมื่อมีคนเข้า Refresh หน้า Web Board ก็จะทำให้ Malicious Script ที่ฝังไว้นั้นทำงานโดยอัตโนมัติ ตามความต้องการของแฮกเกอร์ หรือ อีกวิธีหนึ่ง แฮกเกอร์จะส่ง e-mail ไปหลอกให้เป้าหมาย Click ไปที่ URL Link ที่แฮกเกอร์ได้เตรียมไว้ใน e-mail เมื่อเป้าหมาย Click ไปที่ Link นั้น ก็จะไปสั่ง Run Malicious Script ที่อยู่ในตำแหน่งที่แฮกเกอร์ทำดักรอไว้ วิธีการหลอกแบบนี้ในวงการเรียกว่า “PHISHING” ซึ่งโดนกันไปแล้วหลายองค์กร เช่น Citibank, eBay เป็นต้น (ข้อมูลเพิ่มเติมดูได้ที่ http://www.acisonline.net)

วิธีการป้องกัน

อย่างแรกเลยต้องมีการให้ข้อมูลกับผู้ใช้คอมพิวเตอร์ทั่วไป ที่ใช้ e-mail และ web browser กันเป็นประจำให้ระมัดระวัง URL Link แปลกๆ หรือ e-mail แปลกๆ ที่เข้ามาในระบบก่อนจะ Click ควรจะดูให้รอบคอบก่อน เรียกว่า เป็นการทำ “Security Awareness Training” ให้กับ User ซึ่งควรจะทำทุกปี ปีละ ๒-๓ ครั้ง เพื่อให้รู้ทันกลเม็ดของแฮกเกอร์ และไวรัสที่ชอบส่ง e-mail มาหลอกอยู่เป็นประจำ สำหรับในฝั่งของผู้ดูแลระบบ เช่น Web Master ก็ควรจะแก้ไข source codeใน Web Board ของตนให้ฉลาดพอที่จะแยกแยะออกว่ากำลังรับข้อมูลปกติ หรือรับข้อมูลที่เป็น Malicious Script ซึ่งจะสังเกตได้ไม่ยาก เพราะ Script มักจะมีเครื่องหมาย “< > ( ) # & ” ให้ Web Master ทำการ “กรอง” เครื่องหมายเหล่านี้ก่อนที่จะนำข้อมูลไปประมวลผลโดย Web application ต่อไป

๒.๕ Buffer Overflow

หมายถึง ในฝั่งของ Client และ Server ไม่ว่าจะเป็น IE Browser และ IIS Web Server หรือ Netscape Browser และ Apache Web Server ที่เราใช้กันอยู่เป็นประจำ ล้วนมีช่องโหว่ (Vulnerability) หรือ Bug ที่อยู่ในโปรแกรม เมื่อแฮกเกอร์สามารถค้นพบ Bug ดังกล่าว แฮกเกอร์ก็จะฉวยโอกาสเขียนโปรแกรมเจาะระบบที่เราเรียกว่า “Exploit” ในการเจาะผ่านช่องโหว่ที่ถูกค้นพบ ซึ่งช่วงหลังๆ แม้แต่ SSL Modules ทั้ง IIS และ Apache web server ก็ล้วนมีช่องโหว่ให้แฮกเกอร์เจาะผ่านทาง Buffer Overflow ทั้งสิ้น

<u>วิธีการป้องกัน</u>

จะเห็นว่าปัญหานี้มาจากผู้ผลิตไม่ใช่ปัญหาการเขียนโปรแกรม Web application ดังนั้นเราต้องคอยหมั่นติดตามข่าวสาร New Vulnerability และ คอยลง Patch ให้กับระบบของเราอย่างสม่ำเสมอ และลง ให้ทันท่วงทีก่อนที่จะมี exploit ใหม่ๆ ออกมาให้แฮกเกอร์ใช้การเจาะระบบของเรา สำหรับ Top ๑๐ Web Application Hacking อีก ๕ ข้อ ที่เหลือผมขอกล่าวในฉบับต่อไปนะครับ

๒.๖ Injection Flaws

หมายถึง แฮกเกอร์สามารถที่จะแทรก Malicious Code หรือ คำสั่งที่แฮกเกอร์ใช้ในการเจาะระบบส่งผ่าน Web Application ไปยังระบบภายนอกที่เราเชื่อมต่ออยู่ เช่น ระบบฐานข้อมูล SQL โดยวิธี SQL Injection หรือ เรียก External Program ผ่าน shell command ของระบบปฏิบัติการ เป็นต้น

ส่วนใหญ่แล้วแฮกเกอร์จะใช้วิธีนี้ในช่วง การทำ Authentication หรือการ Login เข้าระบบผ่านทาง Web Application เช่น Web Site บางแห่งชอบใช้ “/admin” ในการเข้าสู่หน้า Admin ของ ระบบ ซึ่งเป็นช่องโหว่ให้แฮกเกอร์สามารถเดาได้เลยว่า เราใช้ http://www.mycompany.com/admin ในการเข้าไปจัดการบริหาร Web Site ดังนั้นเราจึงควรเปลี่ยนเป็นคำอื่นที่ไม่ใช่ “/admin” ก็จะช่วยได้มาก

วิธีการทำ SQL injection ก็คือ แฮกเกอร์จะใส่ชื่อ username อะไรก็ได้แต่ password สำหรับการทำ SQL injection จะใส่เป็น Logic Statement ยกตัวอย่างเช่น ‘ or ’๑′ = ’๑ หรือ ” or “๑″= “๑

ถ้า Web Application ของเราไม่มีการเขียน Input Validation ดัก password แปลกๆ แบบนี้ แฮกเกอร์ก็สามารถที่จะ bypass ระบบ Authentication ของเราและ Login เข้าสู่ระบบเราโดยไม่ต้องรู้ username และ password ของเรามาก่อนเลย

วิธีการเจาะระบบด้วย SQL injection ยังมีอีกหลายแบบจากที่ยกตัวอย่างมา ซึ่งแฮกเกอร์รุ่นใหม่สามารถเรียนรู้ได้ทางอินเทอร์เน็ตและวิธีการทำก็ไม่ยาก อย่างที่ยกตัวอย่างมาแล้ว

<u>วิธีการป้องกัน</u>

นักพัฒนาระบบ (Web Application Developer) ควรจะระมัดระวัง input string ที่มาจากทางฝั่ง Client (Web Browser) และไม่ควรใช้วิธีติดต่อกับระบบภายนอกโดยไม่จำเป็น ควรมีการ “กรอง” ข้อมูลขาเข้าที่มาจาก Web Browser ผ่านมาทางผู้ใช้ Client อย่างละเอียด และ ทำการ “กรอง” ข้อมูลที่มีลักษณะที่เป็น SQL injection statement ออกไปเสียก่อนที่จะส่งให้กับระบบฐานข้อมูล SQL ต่อไป

การใช้ Stored Procedure หรือ Trigger ก็เป็นทางออกหนึ่งในการเขียนโปรแกรมสั่งงานไปยังระบบฐานข้อมูล SQL ซึ่งมีความปลอดภัยมากกว่าการใช้ “Dynamic SQL Statement ” กับฐานข้อมูล SQL ตรงๆ

๒.๗ Improper Error Handling

หมายถึง มีการจัดการกับ Error message ไม่ดีพอ เวลาที่มีผู้ใช้ Web Application หรืออาจจะเป็นแฮกเกอร์ลองพิมพ์ Bad HTTP Request เข้ามาแต่ Web Server หรือ Web Application ของเราไม่มีข้อมูลจึงแสดง Error message ออกมาทางหน้า Browser ซึ่งข้อมูลที่แสดงออกมาทำให้แฮกเกอร์สามารถใช้เป็นประโยชน์ ในการนำไปเดาเพื่อหาข้อมูลเพิ่มเติมจากระบบ Web Application ของเราได้ เนื่องจากเมื่อการทำงานของ Web application หลุดไปจากปกติ ระบบมักจะแสดงค่า Error Message ออกมาแสดงถึงชื่อ user ที่ใช้ในการเข้าถึงฐานข้อมูล, แสดง File System Path หรือ Sub Directory Name ที่ชี้ไปยังไฟล์ฐานข้อมูล ตลอดจนทำให้แฮกเกอร์รู้ว่าเราใช้ระบบอะไรเป็นฐานข้อมูลเช่น ใช้ MySQL เป็นต้น

<u>วิธีการแก้ปัญหา</u>

ควรมีการกำหนดนโยบายการจัดการกับ Error message ให้กับระบบ โดยทำหน้า Error message ที่เตรียมไว้รับเวลามี Bad HTTP Request แปลกๆ เข้ามายัง Web Application ของเราโดยหน้า Error message ที่ดีไม่ควรจะบอกให้ผู้ใช้รู้ถึงข้อมูลระบบบางอย่างที่ผู้ใช้ทั่วไปไม่ควร รู้และถ้าผู้ใช้คนนั้นเป็นแฮกเกอร์ซึ่งย่อมมีความรู้มากกว่าผู้ใช้ธรรมดา การเห็นข้อมูล Error message ก็อาจนำไปใช้เป็นประโยชน์สำหรับแฮกเกอร์ได้

๒.๘ Insecure Storage

หมายถึง การเก็บรหัสผ่าน (password), เบอร์บัตรเครดิตลูกค้า หรือ ข้อมูลลับของลูกค้า ไว้อย่างไม่มีความปลอดภัยเพียงพอ ส่วนใหญ่จะเก็บแบบมีการเข้ารหัส (Encryption) ไว้ในฐานข้อมูลหรือ เก็บลงในไฟล์ที่อยู่ใน Web server และคิดว่าเมื่อเข้ารหัสแล้วแฮกเกอร์คงไม่สามารถอ่านออก แต่ สิ่งที่เราคิดนับว่าเป็นการประเมินแฮกเกอร์ต่ำเกินไป เนื่องจากอาจเกิดข้อผิดพลาดในการเข้ารหัส เช่น การเข้ารหัสนั้นใช้ Algorithm ที่อ่อนเกินไป ทำให้แฮกเกอร์แกะได้ง่ายๆ หรือมีการเก็บกุญแจ (key) หรือ รหัสลับ (Secret password) ไว้เป็นไฟล์แบบง่ายๆ ที่แฮกเกอร์ สามารถเข้าถึงได้ หรือ สามารถถอดรหัสได้โดยใช้เวลาไม่มากนัก

<u>วิธีการแก้ไข</u>

ควรมีการเข้ารหัสไฟล์ โดยใช้ Encryption Algorithm ที่ค่อนข้างซับซ้อนพอสมควร หรือแทนที่จะเก็บรหัสผ่านที่เข้ารหัสไว้ ให้หันมาเก็บค่า Message Digest หรือ ค่า “HASH” ของรหัสผ่านทาง โดยใช้ Algorithm SHA-๑ เป็นต้น

การเก็บกุญแจ (key), ใบรับรอง ดิจิตัล (Digital Certificate) หรือ ลายมือชื่อดิจิตัล (Digital Signature) ควรเก็บไว้อย่างปลอดภัย เช่น เก็บไว้ใน Token หรือ Smart Card ก็จะปลอดภัยกว่าการเก็บไว้เป็นไฟล์ในฮาร์ดดิสค์ เป็นต้น (ถ้าเก็บเป็นไฟล์ก็ควรทำการเข้ารหัสไว้ทุกครั้ง)

๒.๙ Denial of Service

หมายถึงระบบ Web Application หรือ Web Server ของเรา อาจหยุดทำงานได้เมื่อเจอกับ Bad HTTP Request แปลกๆ หรือ มีการเรียกเข้ามาอย่างต่อเนื่องจำนวนมาก ทำให้เกิดการจราจรหนาแน่นบน Web Server ของเรา โดยปกติ Web Server จะจัดการกับ Concurrent session ได้จำนวนหนึ่ง ถ้ามี HTTP Request เข้ามาเกินค่าที่ Web Server จะสามารถรับได้ ก็จะเกิด Error ขึ้น ทำให้ผู้ใช้ไม่สามารถเข้า Web Site เราได้ นอกจากนี้ อาจจะทำให้เครื่องเกิด CPU Overload หรือ Out of Memory ก็เป็นรูปแบบหนึ่งของ Denial of Service เช่นกัน กล่าวโดยรวมก็คือ ทำให้ระบบของเรามีปัญหาเรื่อง “Availability”

วิธีการแก้ไข

การป้องกัน DoS หรือ DDoS Attack นั้นไม่ง่าย และ ส่วนใหญ่ ไม่สามารถป้องกันได้ ๑๐๐% การติดตั้ง Hardware IPS (Intrusion Prevention System) เป็นอีกทางเลือกหนึ่ง แต่ก็มีค่าใช้จ่ายค่อนข้างสูง หากต้องการประหยัดงบประมาณก็ควรต้อง ทำการ “Hardening” ระบบให้เรียบร้อย เช่น Network OS ที่ใช้อยู่ก็ควรจะลง Patch อย่างสม่ำเสมอ, Web Server ก็เช่นเดียวกัน เพราะมีช่องโหว่ เกิดขึ้นเป็นประจำ ตลอดจนปรับแต่งค่า Parameter บางค่าของ Network OS เพื่อให้รองรับกับการโจมตีแบบ DoS /DDoS Attack

๒.๑๐ Insecure Configuration Management

หมายถึง เป็นปัญหาที่เกิดขึ้นจากผู้ดูแลระบบ หรือ ผู้ติดตั้ง Web Server มักจะติดตั้งในลักษณะ “Default Configuration” ซึ่งยังคงมีช่องโหว่มากมาย หรือบางครั้งก็ไม่ได้ทำการ Update Patch ระบบให้ครบถ้วนจนถึง Patch ล่าสุด ปัญหาที่เจอบ่อยๆ ก็คือมีการกำหนดสิทธิในการเข้าถึงไฟล์ต่างๆ ใน Web Server ไม่ดีพอทำให้มีไฟล์หลุดออกมาให้ผู้ใช้เข้าถึงได้ เช่น แสดงออกมาในลักษณะ “Directory Browsing” ตลอดจนค่า default ต่างๆ ไม่ว่าจะเป็น Default Username และ Default Password ก็มักจะถูกทิ้งไว้โดยไม่ได้เปลี่ยนอยู่เป็นประจำ

วิธีการแก้ปัญหา

ให้ทำการแก้ไขค่า “Default” ต่างๆ ทันทีที่ติดตั้งระบบเสร็จ และทำการ Patch ระบบให้ถึง Patch ล่าสุด และตาม Patch อย่างสม่ำเสมอ เรียกว่า ทำการ “Hardening” ระบบนั่นเอง Services ใดที่ไม่ได้ใช้ก็ไม่ต้องเปิดบริการ เราควรตรวจสอบสิทธิ File and Subdirectory Permission ในระบบว่าตั้งไว้ถูกต้อง และปลอดภัยหรือไม่ ตลอดจนเปิดระบบ Web Server log file เพื่อที่จะได้สามารถตรวจสอบ (Audit) HTTP Request ที่ส่งมายัง Web Server ได้ โดยดูจาก Web Server log file ที่เราได้เปิดไว้ และ เราควรหมั่นติดตามข่าวสารเรื่องช่องโหว่ (Vulnerability) ใหม่ๆ อย่างสม่ำเสมอ และ มีการตรวจวิเคราะห์ Web Server log file, Network log file, Firewal log file และ IDS/IPS log file เป็นระยะๆ

จะเห็นได้ว่า แฮกเกอร์ในปัจจุบันสามารถเจาะระบบเราโดยผ่านทะลุ Firewall ได้อย่างง่ายดาย เพราะเรามีความจำเป็นต้องเปิดให้บริการ Web Server ในทุกองค์กร ดังนั้นการตรวจสอบเรื่องของ Web Application Source Code และ Web Server Configuration จึงเป็นทางออกสำหรับการแก้ไขปัญหาทางด้านความปลอดภัยของระบบให้รอดพ้นจาก เหล่าไวรัสและแฮกเกอร์ซึ่งนับวันจะเพิ่มจำนวนและเพิ่มความสามารถขึ้นเป็นทวีคูณ

๒.๑๑ ภัยคุกคามอื่นๆ

นอกจากช่องโหว่ทางแอพพลิเคชั่นแล้ว ภัยคุกคามต่างๆที่มีอยู่ในโลกออนไลน์ที่ดูไม่มีวันจะจบสิ้น ได้แก่ Virus สามารถแพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป มันไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ต้องอาศัยไฟล์พาหะ สิ่งที่มันทำคือสร้างความเสียหายให้กับไฟล์ Malware ที่พบเห็นการแพร่ระบาดทั่วไปและเหมือนจะสร้างความเสียหายให้กับระบบเศรษฐกิจมากที่สุดก็คือ worm และ worm ก็ยังแบ่งออกเป็นชนิดแยกย่อยได้ดังต่อไปนี้

- Email Worm เช่น mass-mailing worm ที่ค้นหารายชื่ออีเมลล์ในเครื่องที่ตกเป็นเหยื่อแล้ว ก็ส่งตัวเองไปหาอีเมลล์เหล่านั้น
- File-sharing Networks Worm คัดลอกตัวเองไปไว้ในโฟลเดอร์ที่ขึ้นค้นหรือประกอบด้วยคำว่าด้วย sha และแชร์โฟลเดอร์ของโปรแกรม P๒P เช่น KaZaa
- Internet Worm, Network Worm โจมตีช่องโหว่ของโปรแกรมและระบบปฏิบัติการเช่นเวิร์ม Blaster, Sasser ที่เรารู้จักกันดี
- IRC Worm ส่งตัวเองจากเครื่องที่ตกเป็นเหยื่อไปหาคนที่อยู่ในห้องสนทนาเดียวกัน
- Instant Messaging Worm ส่งตัวเองจากเครื่องที่ตกเป็นเหยื่อไปหาคนที่อยู่ใน contact list ผ่านทางโปรแกรม IM เช่น MSN, ICQ

Trojan ไม่สามารถแพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ ต้องอาศัยการหลอกคนใช้ให้ดาวโหลดเอาไปใส่เครื่องเองหรือด้วยวิธีอื่นๆ สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล ซึ่งจะทำอะไรก็ได้ และโทรจันยังมีอีกหลายชนิด trojan ยังแบ่งออกได้เป็นหลายชนิดดังนี้

- Remote Access Trojan (RAT) หรือ Backdoor ที่เปิดช่องทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาควบคุม หรือทำอะไรก็ได้บนเครื่องที่ตกเป็นเหยื่อในแบบระยะไกล
- Data Sending/Password Sending Trojan โขมยรหัสผ่านแล้วส่งไปให้ผู้ไม่ประสงค์ดี
- Keylogger Trojan ดักจับทุกข้อความที่พิมพ์ผ่านแป้นพิมพ์
- Destructive Trojan ลบไฟล์บนเครื่องที่ตกเป็นเหยื่อ
- Denial of Service (DoS) Attack Trojan ใช้ทำ DDoS เพื่อโจมตีระบบอื่น
- Proxy Trojan เปลี่ยนเครื่องที่ตกเป็นเหยื่อให้กลายเป็น proxy server หรือ web server, mail server เพื่อสร้าง zombie network
- FTP Trojan เปลี่ยนเครื่องที่ตกเป็นเหยื่อให้กลายเป็น FTP server
- Security software Killer Trojan ฆ่า process หรือลบโปรแกรมป้องกันไวรัส/โทรจัน/ไฟล์วอลบนเครื่องที่ตกเป็นเหยื่อ
- Trojan Downloader ดาวน์โหลด adware, spyware, worm เอามาติดตั้งบนเครื่องเหยื่อ

Spyware ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ ต้องอาศัยการหลอกคนใช้ให้ดาวโหลดเอาไปใส่เครื่องเองห รืออาศัยช่องโหว่ของ web browser ในการติดตั้งตัวเองลงในเครื่องเหยื่อ สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้ ซึ่งแบ่งออกได้เป็นหลายชนิด (ซึ่งบางส่วนก็มีพฤติกรรมคล้ายๆ trojan ด้วย) เช่น

- Adware ดาวน์โหลดและแสดงแบนเนอร์โฆษณา
- Dialer อยู่ตามเว็บโป๊เพื่อใช้ต่อโทรศัพท์ทางไกลไปต่างประเทศ
- Spyware เก็บรวมรวมพฤติกรรมการใช้อินเตอร์เน็ตบนเครื่องเหยื่อ
- Hijacker เปลี่ยนแปลง start page, bookmark บนบราวเซอร์เช่นใน IE
- Trojan like เช่น trojan downlaoder ดาวน์โหลด spyware หรือแบนเนอร์โฆษณา
- BHO (Browser Helper Objects) ยัดเยียดฟังก์ชั่นที่ไม่พึงประสงค์บนบราวเซอร์เช่นใน IE
- Toolbar ยัดเยียด toolbar ที่ไม่พึงประสงค์บนบราวเซอร์เช่นใน IE

Hybrid malware/Blended Threats คือ malware ที่รวมความสามารถของ virus, worm, trojan, spyware เข้าไว้ด้วยกัน

Phishing เป็นเทคนิคการทำ social engineer โดยใช้อีเมลล์เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลการทำธุรกรรมทางการเงินบนอินเตอร์เน็ตเช่น บัตรเครดิตหรือพวก online bank account

Zombie Network เครื่องคอมพิวเตอร์จำนวนมากๆ จากทั่วโลกที่ตกเป็นเหยื่อของ worm, trojan และ malware อย่างอื่น (compromised machine) ซึ่งจะถูก attacker/hacker ใช้เป็นฐานปฏิบัติการในการส่ง spam mail, phishing, DoS หรือเอาไว้เก็บไฟล์หรือซอฟแวร์ที่ผิดกฎหมาย

๒.๑๒ ความหมายของชื่อตระกูลไวรัส

โดยส่วนประกอบของชื่อไวรัสนั้นแบ่งได้เป็นส่วนๆ ดังนี้ Family Names, Group_Name, Variant Tail, W๓๒, Mydoom, bb, @mm

๑. ส่วนแรกแสดงชื่อตระกูลของไวรัส (Family_Names) ส่วนมากแล้วจะตั้งตามที่ไวรัสตัวนั้น ก่อปัญหาขึ้นกับระบบปฏิบัติการอะไร หรือภาษาที่ใช้ในการเขียนของไวรัส ดังต่อไปนี้

Family_Names ความหมาย

WM ไวรัสที่เป็นมาโครของโปรแกรม Word
W๙๗M ไวรัสที่เป็นมาโครของโปรแกรม Word ๙๗
XM ไวรัสที่เป็นมาโครของโปรแกรม Excel
X๙๗M ไวรัสที่เป็นมาโครของโปรแกรม Excel ๙๗
W๙๕ ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ ๙๕
W๓๒/Win๓๒ ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ ๓๒ บิต
WNT ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ NT ๓๒ บิต
I-Worm/Worm หนอนอินเทอร์เน็ต
Trojan/Troj โทรจัน
VBS ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
AOL โทรจัน America Online
PWSTEAL โทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux ไวรัสที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์
Palm ไวรัสที่มีผลกระทบกับระบบปฏิบัติการ Palm OS
Backdoor เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

๒. ส่วนชื่อของไวรัส (Group_Name)
ตัวนี้จะถูกตั้งขึ้นจากชื่อของผู้ที่เขียนไวรัส หรือนามแฝง ที่ใช้แทรกในโค้ดของตัวโปรแกรมไวรัส

๓. ส่วนของ Variant

รายละเอียดส่วนนี้จะบอกว่าสายพันธุ์ของไวรัสชนิดนั้น ๆ มีการปรับปรุงสายพันธุ์จนมีความสามารถต่างจากสายพันธุ์เดิมที่มีอยู่ซึ่ง Vvariant มี ๒ ลักษณะคือ

๓.๑ Major_Variants จะตามหลังส่วนชื่อของไวรัส เพื่อบ่งบอกว่ามีความแตกต่างกันอย่างชัดเจน เช่น W

๓.๒ Mydoom.bb@MM (bb เป็น Major_Variant) แตกต่างจาก W๓๒.Mydoom.Q@MM อย่างชัดเจน

๓.๒ Minor_Variants ใช้บ่งบอกในกรณีที่แตกต่างกันนิดหน่อย ในบางครั้ง Minor_Variant เป็นตัวเลขที่บอกขนาดไฟล์ของไวรัส ตัวอย่างเช่น W๓๒.Funlove.๔๐๙๙ หนอนชนิดนี้มีขนาด ๔๐๙๙ KB.

๔. ส่วนท้าย (Tail)

เป็นส่วนที่จะบอกว่าวิธีการแพร่กระจาย ประกอบด้วย

๔.๑ @M หรือ @m บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mailer" ที่จะส่งตัวเองผ่านทางอี-เมล์เมื่อผู้ใช้ส่งอี-เมล์เท่านั้น

๔.๒ @MM หรือ @mm บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mass-mailer" ที่จะส่งตัวเองผ่านทุกอี-เมล์แอดเดรสที่อยู่ในเมล์บอกซ์

ตัวอย่าง

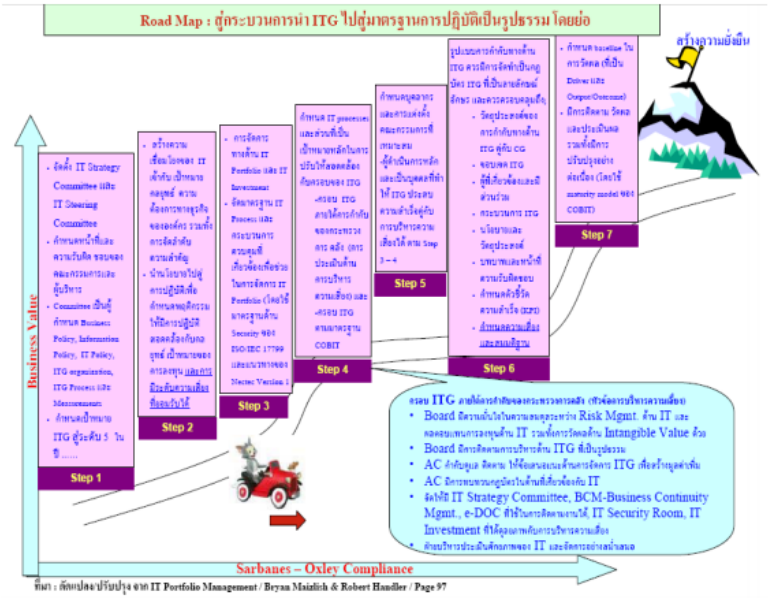
W๓๒/Mydoom.bb@mm หมายความว่า
ไวรัสชนิดนี้โจมตีในเพลตฟอร์มของวินโดว ๓๒ บิต
ชื่อของไวรัสคือ Mydoom
Variant สายพันธุ์ของตัวนี้คือ bb
และมีความสามารถที่จะส่งตัวเองผ่านทุกอี-เมล์แอดเดรสที่อยู่ในเมล์บอกซ์

บทที่ ๓

Governance of Cyber Security

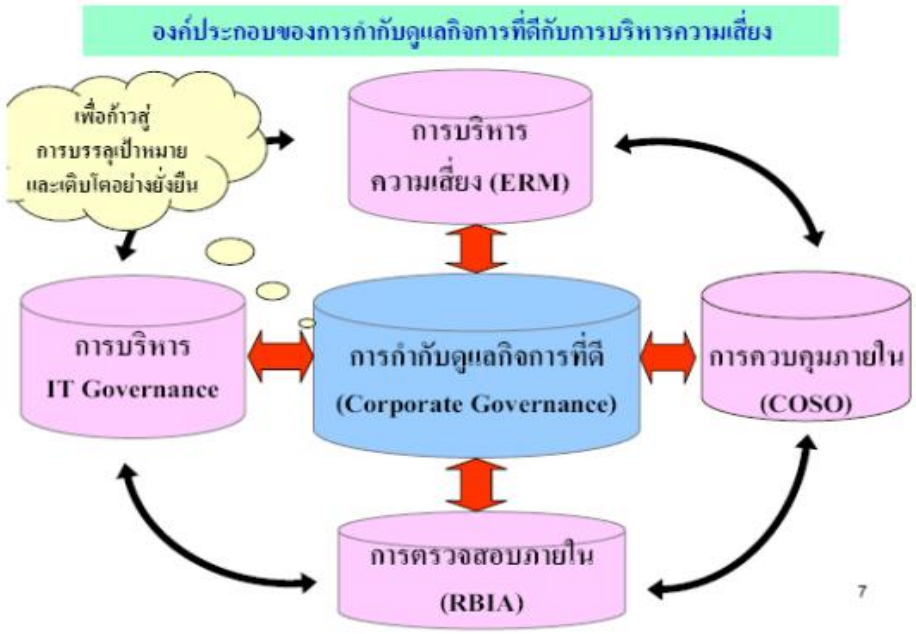
ธรรมาภิบาลของการรักษาความปลอดภัยทางด้านไซเบอร์

ไอซีทีธรรมาภิบาล (ICT Governance) IT Governance เป็นหน้าที่และความรับผิดชอบเกี่ยวกับการจัดการที่ดีทางด้านเทคโนโลยี สารสนเทศควบคู่กันไปกับความสามารถด้านอื่น ๆ ของคณะกรรมการและผู้บริหารระดับสูงที่ใช้ เป็นกรอบและองค์ประกอบของกระบวนการบริหารงานในการปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้างศักยภาพ คุณค่าเพิ่ม และการเติบโตอย่างยั่งยืนอย่างรู้คุณค่าให้กับองค์กรควบคู่กันไปกับหลักการกำกับดูแลองค์กรที่ดีที่แยกกันไม่ได้ ในกระบวนการบริหารความเสี่ยงตามองค์ประกอบ ของการจัดการตั้งแต่การวางแผน การจัดองค์กร การจัดการพนักงาน การดำเนินการและการควบคุม



๓.๑ ความหมายของ IT Governance

IT Governance / ITG หรือ ธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ คือ รูปแบบ โครงสร้างของความสัมพันธ์และกระบวนการการจัดการและการปฏิบัติในองค์กร ที่กำกับและ ควบคุมองค์กรให้บรรลุถึงเป้าประสงค์ โดยการสร้างมูลค่าเพิ่มให้เกิดขึ้น ในขณะเดียวกันก็สามารถ สร้างความสมดุลในการจัดการกับความเสี่ยงที่เกิดขึ้นเทียบกับสิ่งที่ได้รับจากเทคโนโลยีสารสนเทศ และจากกระบวนการที่เกี่ยวข้อง หรือ ITG คือการบริหารดุลยภาพทางด้านการลงทุนและ กระบวนการจัดการทางด้านเทคโนโลยีสารสนเทศกับการบริหารความเสี่ยง และประโยชน์ที่ได้รับ ในรูปแบบต่างๆ ที่เกี่ยวข้องกับ Intangible Assets / Value และ Tangible Assets / Value เพื่อสร้าง คุณค่าเพิ่มผ่าน Business process สู่ Business objectives ขององค์กร ได้อย่างมั่นใจ หรือเป็น การบริหารกระบวนการความสัมพันธ์ และดุลยภาพ ระหว่าง เป้าประสงค์ทางธุรกิจกับเป้าประสงค์ ทางด้านการจัดการสารสนเทศ เพื่อให้มีการบริหารความเสี่ยงอย่างเป็นกระบวนการตามหลักการของ COSO- ERM อย่างผสมผสาน และ อย่างบูรณาการ กับมาตรฐานต่างๆที่เกี่ยวข้อง



๓.๒ ความสำคัญของ IT Governance

IT Governance ทำให้เกิดการบริหารและการบูรณาการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ลดความเสี่ยง เพิ่มศักยภาพโดยทำงานข้ามสายงานได้ และประสานงานระหว่าง องค์กรได้อย่างรวดเร็ว ทันเวลา มีประสิทธิภาพสอดประสานกับ การดำเนินงานระดับต่างๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่างๆ เพื่อการผลักดัน ความสำเร็จ ของการจัดการทั่วทั้งองค์กรอย่างเป็นกระบวนการ เทคโนโลยีสารสนเทศสร้างความเสี่ยงใหม่ๆ การสูญเสียโอกาสที่มีผลต่อประสิทธิภาพ ประสิทธิผลในการดำเนินการ การปฏิบัติตามนโยบาย กฎหมาย ระเบียบ ประกาศ คำสั่ง ฯลฯ รวมทั้งผลกระทบต่อความน่าเชื่อถือและความถูกต้องของการตรวจสอบและการจัดทำรายงาน ซึ่ง เป็นหัวใจของการบริหารและการควบคุมภายในอย่างคาดไม่ถึง ในการบริหารงานระดับต่าง ๆ ของ องค์กรควบคู่กันไป ด้วยดังนั้น การผสมผสานความสามารถด้านต่าง ๆ ขององค์กรกับศักยภาพของ ระบบงานและการจัดการเทคโนโลยีสารสนเทศที่ดี จึงเป็นทั้งหน้าที่ความรับผิดชอบที่ไม่อาจ หลีกเลี่ยงได้ของคณะกรรมการและผู้บริหารระดับสูงขององค์กรในปัจจุบัน ความสำคัญของ IT Governance เคียงคู่กับความสำคัญของ Corporate Governance ในทุก มุมมองอย่างแยกกันไม่ได้ ซึ่งอาจสรุปได้ดังนี้

๓.๒.๑ ความจำเป็นที่ต้องมีการควบคุมการจัดการ และการใช้เทคโนโลยีสารสนเทศ เพื่อการบรรลุกลยุทธ์และเป้าหมายขององค์กรความก้าวหน้าในการพัฒนาเทคโนโลยีสารสนเทศมาก ทำให้ ข้อมูลสามารถส่งผ่านถึงผู้รับได้อย่างรวดเร็วโดยปราศจากข้อจำกัดด้านเวลา ระยะทางและความ รวดเร็ว องค์กรที่มีการปฏิบัติงานในระบบอัตโนมัติจำเป็นต้องมีกลไกในการควบคุมที่ดียิ่งขึ้น โดยเฉพาะการควบคุมทั้งระบบคอมพิวเตอร์ และระบบเครือข่าย ทั้งในด้านของ Hardware และ Software ซึ่งระบบการควบคุมจำเป็นต้องพัฒนาไปพร้อมกับการพัฒนาของเทคโนโลยีที่เกิดขึ้น อย่างรวดเร็วและเป็นไปแบบก้าวกระโดด จึงจำเป็นต้องมี

การจัดการความเสี่ยงที่มาพร้อมกับการเปลี่ยนแปลงนี้ให้ดียิ่งขึ้น ไม่ว่าจะเป็นการจัดการกับข้อมูลที่เปิดเผยและข้อมูลที่เป็นความลับ รวมทั้งการนำข้อมูลไปใช้กระทำการที่ผิดกฎหมาย ดังนั้น การบริหารความเสี่ยงที่เกี่ยวข้อง เทคโนโลยีสารสนเทศจึงกลายมาเป็นส่วนสำคัญในการกำกับดูแลกิจการที่ดีขององค์กร (Corporate Governance) ผู้บริหารจะต้องสามารถตัดสินใจได้ว่าควรจะลงทุน ณ ระดับใดในเรื่องการรักษา ความปลอดภัยและการควบคุม และจะรักษาจุดสมดุลอย่างไรระหว่างความเสี่ยงที่รับได้กับการ ลงทุนในด้านการควบคุม แต่ถ้าเป็นเรื่องของการปฏิบัติตาม Compliance ก็เป็นสิ่งที่องค์กรไม่อาจ หลีกเลี่ยงได้ ตามหลัก GRC (Governance-Risk management-Compliance) ที่เป็น first priority ของ องค์กรยุคใหม่ในปัจจุบัน

๓.๒.๒ ความจำเป็นของการควบคุมและกำกับทางด้านเทคโนโลยีสารสนเทศ ตามกฎหมายที่ยอมรับในระดับสากล คือไม่ทำผิด Compliance (Not Doing the Wrong Thing- Laws/Rules and Constraints) แต่ องค์กรควรมีนโยบายที่จะดำเนินการในสิ่งที่ถูกและได้มาตรฐานต้องเท่านั้น ยกตัวอย่างเช่น องค์กรต่าง ๆ ที่อยู่ใน ตลาดหลักทรัพย์ในสหรัฐฯ จำเป็นต้องให้ความสำคัญกับการควบคุมและการประมวลข้อมูลโดยมี การระบุในกฎหมาย Sarbanes-Oxley Act, ๒๐๐๒ ใน หัวข้อที่ ๔๐๔ ที่กล่าวถึง “ Management’s Report on Internal Controls over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports” ว่ารายงานของการควบคุมภายในจะต้องครอบคลุมเนื้อหาดังนี้

๓.๒.๒.๑ การระบุความรับผิดชอบของผู้บริหารที่มีต่อการจัดการให้มีการควบคุมภายในในการ จัดทำรายงานทางการเงินขององค์กร

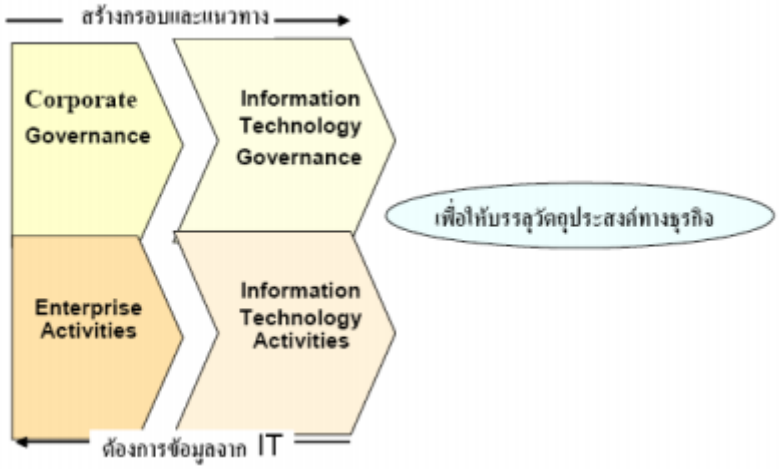
๓.๒.๒.๒ การตรวจสอบของผู้บริหารถึงความถูกต้องและความมีประสิทธิผลในการควบคุม ภายในของการจัดทำรายงานทางการเงินขององค์กร ณ วันสิ้นสุดรอบการเงิน

๓.๒.๒.๓ การระบุถึงกรอบการจัดการในการประเมินความถูกต้องและความมีประสิทธิผลใน การควบคุมภายในของการจัดทำรายงานทางการเงินขององค์กร

๓.๒.๒.๔. การตรวจรับรองโดยองค์กรตรวจสอบบัญชีและรายงานถึงการตรวจสอบของผู้บริหาร ถึงความถูกต้องและความมีประสิทธิผลในการควบคุมภายในของการจัดทำรายงานทางการเงินขององค์กร ซึ่งการใช้ข้อมูลโดยพึ่งพาเทคโนโลยีสารสนเทศเป็นสิ่งที่จำเป็น การมีการควบคุมที่ดีในการ จัดการข้อมูลรวมทั้งการควบคุมคุณภาพและการรักษาความปลอดภัยในการเข้าถึงข้อมูล จึงมีความสำคัญอย่างยิ่ง โดยปกติการเซ็นชื่อรับรองงบการเงินจะกระทำโดย CEO และ CFO แต่ปัจจุบัน เริ่มมีหลายองค์กรให้ CIOเซ็นชื่อร่วมด้วย โดยให้ความสำคัญกับ Technology Support เพื่อให้ได้มา ซึ่งรายงานทางการเงินที่เชื่อถือได้ก่อนที่ผู้สอบบัญชีจะรับรองงบการเงิน

๓.๓ ความสัมพันธ์ระหว่าง Corporate Governance กับ IT Governance IT Governance

เป็นส่วนสำคัญที่รวมอยู่ในความสำเร็จของ Corporate Governance โดยจะ เป็นจุดวัดของการปรับปรุงในด้านประสิทธิผล และประสิทธิภาพของกระบวนการปฏิบัติงานของ องค์กร โดยธรรมาภิบาลขององค์กรจะเป็นกรอบในการกำหนดแนวทางสำหรับธรรมาภิบาลทางด้าน เทคโนโลยีสารสนเทศ ส่วนกิจกรรม / กระบวนการต่างๆ ขององค์กร จะต้องใช้ข้อมูลจากกิจกรรม / กระบวนการของเทคโนโลยีสารสนเทศ ดังนี้



จะกำกับควบคุม เป็นผู้ขับเคลื่อน และกำหนดรูปแบบของ IT Governance ในขณะเดียวกันเทคโนโลยีสารสนเทศก็ได้สนับสนุนข้อมูลที่จำเป็นต่างๆ เพื่อใช้ใน การวางแผนด้านกลยุทธ์และในบางครั้งยังเป็นส่วนที่มีอิทธิพลในการสร้างโอกาสใหม่ๆ ให้กับ องค์กร จึงถือได้ว่าเทคโนโลยีสารสนเทศและการวางแผนด้านกลยุทธ์มีความสัมพันธ์แบบพึ่งพากัน โดยกิจกรรมในองค์กร จำเป็นต้องใช้ข้อมูลจาก IT Activities เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจ โดย IT Activities จะต้องสอดคล้องกับกิจกรรมในองค์กร และช่วยให้องค์กรสามารถใช้ประโยชน์ จากข้อมูลอย่างเต็มที่ในการสร้างประโยชน์สูงสุด และได้ผลตอบแทนจากการลงทุนจากโอกาสทาง ธุรกิจต่างๆ รวมทั้งสามารถเพิ่มความได้เปรียบในการแข่งขันมากขึ้น โดยปกติแล้วองค์กร จะมีการกำกับ บริหาร และ ควบคุมโดยใช้หลักการจัดการและการ ปฏิบัติที่เหมาะสมหรือที่ดีที่สุด หรือ Promotion of Best Practice ซึ่งเป็นข้อหนึ่งของหลัก การกำกับ ดูแลกิจการที่ดี/CG เพื่อให้มั่นใจว่าองค์กรจะสามารถบรรลุเป้าประสงค์ที่ต้องการ โดยต้องมีการควบคุมความเสี่ยงจากต้นเหตุที่ดีด้วยเช่นกัน ในขณะเดียวกันเทคโนโลยีสารสนเทศก็จำเป็นต้องมีการกำกับ บริหาร และควบคุมที่ดีโดยยึดหลักการของ Good Practices หรือ Best

Practices เช่น เดียวกัน เพื่อให้ข้อมูลและเทคโนโลยี ที่ใช้ในองค์กรสามารถช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจได้ รวมทั้งการใช้ทรัพยากรต่างๆ อย่างมีเหตุมีผล และมีการบริหารความเสี่ยงที่เหมาะสม

จากประเด็นดังกล่าวจะเป็นพื้นฐานสำคัญในการกำหนดแนวทางของกิจกรรมทางด้าน เทคโนโลยีสารสนเทศซึ่งสามารถสรุปลักษณะของกิจกรรมหลักได้ดังนี้

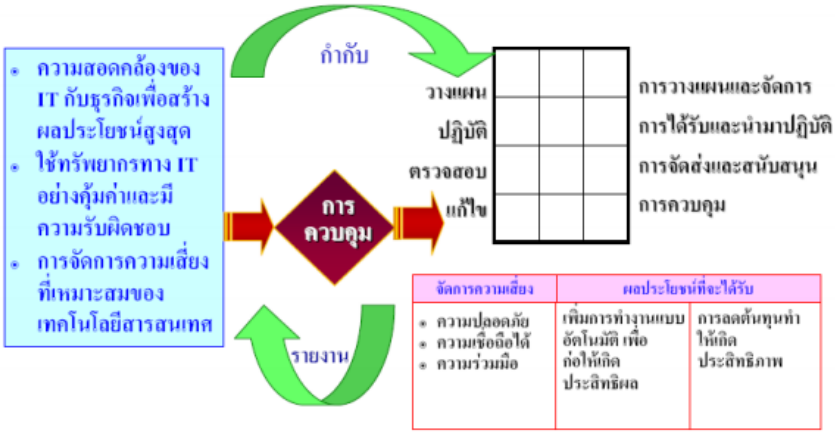
-การวางแผนและการจัดการองค์การ (Planning & Organization -PO)

-การจัดหาและการนำระบบออกใช้งานจริง (Acquisition & Implementation - AI)

-การส่งมอบและการบำรุงรักษา (Delivery & Support - DS)

-การติดตาม (Monitoring - M)

โดยมีวัตถุประสงค์ควบคู่ไปกับการบริหารความเสี่ยง (ในด้านความปลอดภัย ความเชื่อมั่น และความสอดคล้อง ของ IT Activities) และการได้มาซึ่งประโยชน์สูงสุด (ในด้านการเพิ่มประสิทธิภาพและประสิทธิผล) ผลลัพธ์ที่ได้ในรูปแบบของรายงาน จะบอกถึง IT Activities ว่า สามารถสอดคล้อง และสนับสนุนองค์กรให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กรหรือไม่ และทำได้ดีเพียงใดและอย่างไรดังนี้



การกำกับและจัดการกิจกรรมต่าง ๆ ทางด้านเทคโนโลยีสารสนเทศให้เกิดความสมดุลระหว่างการจัดการความเสี่ยงและผลประโยชน์ที่จะได้รับ

บทที่ ๔

Cyber Warfare

เข้าใจและตระหนักถึงสถานการณ์ของสงครามไซเบอร์รอบโลกในปัจจุบัน

๔.๑ สถานการณ์ทางด้านไซเบอร์ระดับโลก

ในช่วงหลายปีที่ผ่านมานั้นแต่ละประเทศได้มีการพัฒนาศักยภาพทางด้านไซเบอร์ไปอย่างรวดเร็ว การทำสงครามไซเบอร์นั้นมีการปรับเปลี่ยนรูปแบบไปจากเดิมที่เป็นการจารกรรมข้อมูล กลายไปเป็นการโจมตีเพื่อทำลายล้าง ซึ่งรูปแบบของการทำสงครามไซเบอร์เองนั้นมีวัตุประสงค์และจุดมุ่งหมายเหมือนกับการทำสงรามในรูปแบบปกติทุกอย่าง เพียงแต่เทคนิคและยุทธวิธีนั้นแตกต่างออกไป ซึ่งการทำสงครามไซเบอร์นั้นนับได้ว่าเป็นทางเลือกที่ดี เพราะถือว่ามีต้นทุนต่ำ แต่สามารถสร้างผลกระทบได้อย่างมากมาย ซึ่งปัญหาหลัก ๆ ที่แต่ละประเทศนั้นพบในมุมมองของการป้องกันประเทศคือ ทำอย่างไรที่จะสามารถระบุตัวผู้โจมตีได้อย่างชัดเจน เนื่องจากการโจมตีทางไซเบอร์นั้นแทบจะไม่เปิดเผยร่องรอยของการโจมตีให้สามารถระบุแหล่งที่มาได้เลย ส่วนใหญ่มักใช้การคาดเดาหรือการวิเคราะห์จากรูปแบบของเทคนิคที่ใช้ ข้อมูลบางอย่างที่ฝังอยู่ในมัลแวร์ ที่มีรูปแบบที่ซ้ำ ๆ กัน เช่น มัลแวร์ที่มาจากประเทศจีนมักจะมีตัวอักษรภาษาจีนแทรกอยู่ภายในโค้ด เป็นต้น อย่างไรก็ตามวิธีการนี้ก็อาจจะไม่แม่นยำเนื่องจากมีแฮกเกอร์บางกลุ่มที่ลวงให้เป้าหมายคิดว่าการโจมตีมาจากอีกกลุ่มหนึ่ง แฮกเกอร์ในบางประเทศยังรับงานรัฐบาลในการโจมตีประเทศอื่น โดยที่รัฐบาลประเทศนั้นได้ออกมาปฏิเสธ ซึ่งงานโจมตีนั้นมีหลากหลายรูปแบบ เช่น งาน DDoS หรือเจาะระบบเข้าไปในเครือข่ายที่แฮกเกอร์กลุ่มนั้นสามารถเจาะเข้าไปได้ก่อนหน้านั้นแล้ว นอกจากนี้ยังมีข้อมูลอีกว่ารัฐบาลบางประเทศสร้างโทรจันที่มีความซับซ้อนและปล่อยขายในตลาดมืดเอง เพื่อประโยชน์ในกาตรวจสอบว่ามีประเทศใดที่ซื้อเอาโทรจันนั้นไปใช้ในการดำเนินปฏิบัติการไซเบอร์ มีประเทศจำนวนมากที่มีความเคลื่อนไหวทางด้านไซเบอร์ในระดับโลก ไม่ว่าจะเป็นผู้โจมตีหรือถูกโจมตี เช่น สหรัฐอเมริกา รัสเซีย อิหร่าน อิสราเอล อินเดีย ซีเรีย เป็นต้น

ประเทศรัสเซียนั้นขึ้นชื่อว่าเป็นประเทศที่มีแฮกเกอร์อยู่ในระดับชั้นแนวหน้าของโลก มีฝีมือการโจมตีขั้นสูง และมีรูปแบบที่ซับซ้อนกว่าแฮกเกอร์จากประเทศจีนมาก การโจมตีของแฮกเกอร์รัสเซียนั้นมุ่งเน้นการโจมตีโดยใช้ช่องโหว่ Zero-day ในแอพพลิเคชันต่าง ๆ รวมทั้งใช้มัลแวร์ขั้นสูง รวมทั้งใช้เทคนิคบางประเภทซึ่งทำให้หลงเชื่อว่าการโจมตีนั้นมาจากเอเชียแทนที่จะเป็นรัสเซีย รัสเซียเป็นประเทศที่มักจะถูกโยงเข้าไปในปฏิบัติการทางไซเบอร์ที่โจมตีประเทศที่เคยเป็นส่วนหนึ่งของสหภาพโซเวียตมาก่อน เช่น การยิง DDoS ถล่มเอสโตเนียในปี ๒๐๐๗ หรือการโจมตีประเทศจอร์เจียในปี ๒๐๐๘ นอกจากนี้ยังมีกลุ่มแฮกเกอร์ที่ชื่อ APT๒๘ ที่มุ่งเป้าจารกรรมข้อมูลจากหน่วยงานภาครัฐของประเทศจอร์เจียเมื่อไม่นานมานี้อีกด้วย นอกจากนี้รัสเซียยังได้ส่งแฮกเกอร์แทรกซึมเข้าไปในองค์กรของสหรัฐอเมริกาอีกด้วย หนึ่งในการปฏิบัติการสำคัญของรัสเซียคือปฏิบัติการ Red October ซึ่งเป็นการสอดแนมคนจำนวน ๑ ล้านคนทั่วโลกซึ่งส่วนใหญ่เคยเป็นสหภาพโซเวียตมาก่อน โดยมุ่งเน้นไปที่สภานทูต ฐานทัพทหาร ธุรกิจพลังงาน รวมทั้งโครงสร้างพื้นฐาน และในปี ๒๐๑๔ อาวุธทางไซเบอร์ของรัสเซียซึ่งมีชื่อว่า Snake หรือ Ouroboros ถูกรายงานว่าได้สร้างความเสียหายกับระบบของ

รัฐบาลยูเครน ตามรายงานในเดือนตุลาคม ปี ๒๐๑๔ แฮกเกอร์ชาวรัสเซียได้ใช้ช่องโหว่ของ Microsoft Windows และซอฟต์แวร์ชนิดต่างๆ เพื่อใช้ในการสอดแนมคอมพิวเตอร์ขององค์กรนาโต้ สหภาพยุโรป ประเทศยูเครนและบริษัทที่เกี่ยวข้องกับพลังงาน การสื่อสาร โดยข้อมูลนี้ได้รับการอ้างอิงมาจากศูนย์ปฏิบัติการทางไซเบอร์ชื่อ ISight Partners

ในกลุ่มของประเทศในตะวันออกกลางนั้น ประเทศอิหร่านนับได้ว่าเป็นประเทศที่มุ่งเน้นทางด้านสงครามไซเบอร์เป็นอย่างมาก อันเป็นผลมาจากการที่อิหร่านถูกโจมตีทางไซเบอร์จากชาติตะวันตกมาก่อนในปี ๒๐๑๐ จากปรากฏการของ Stuxnet ที่ว่ากันว่าเป็น cyber missile ลูกแรกของโลกที่มุ่งเป้าทำลายโรงปฏิกรณ์นิวเคลียร์ของอิหร่านโดยได้รับการอ้างอิงจากนิตยสาร Business Insider อีกทั้งโปรแกรมระบบปฏิกรณ์ปรมาณูถูกรีเซ็ทให้ย้อนหลังไปถึงสองปี และ Stuxnet ยังได้แพร่กระจายไปสู่คอมพิวเตอร์สาธารณะอื่นๆอีกกว่า ๖๐,๐๐๐ เครื่องด้วยกัน แต่รัฐบาลของอิหร่านก็ได้แสดงให้เห็นว่าไม่ได้รับความเสียหายที่สำคัญมากนัก โดยผลพวงจากเหตุการณ์ดังกล่าวทำให้โปรแกรมเมอร์ชาวอิหร่านได้ร่วมมือกันหาวิธีการป้องกันจะอยู่ในสถานะที่ดีขึ้นมากในด้านของสงครามไซเบอร์ แต่สุดท้ายแล้วไม่มีรัฐบาลไหนออกมาแสดงความรับผิดชอบต่อความเสียหายที่เกิดขึ้น ในด้านปฏิบัติการของอิหร่านนั้น เริ่มเห็นชัดตั้งแต่ปี ๒๐๑๒ แล้วว่าได้มีกลุ่มแฮกเกอร์อิหร่านชื่อที่เรียกตัวเองว่า Cutting Sword of Justice ใช้ไวรัสในการโจมตีบริษัทน้ำมันของประเทศซาอุดิอาระเบียโดยลบข้อมูลไปกว่า ๗๕% ของข้อมูลทั้งหมดและแทนที่ด้วยรูปภาพธงชาติสหรัฐอเมริกาถูกเผา นอกจากนี้กลุ่มแฮกเกอร์ชื่อ Izz ad-Din al-Qassam ได้ดำเนินปฏิบัติการ Operation Ababil ซึ่งเป็นการโจมตีด้วย DDoS ต่อสถาบันการเงินหลายแห่งในสหรัฐอเมริการวมทั้งตลาดหลักทรัพย์ของนิวยอร์กอีกด้วย และล่าสุด กลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐบาลอิหร่านได้ดำเนินปฏิบัติการ Operation Cleaver ซึ่งมุ่งเน้นในการจารกรรมข้อมูล รวมไปถึงการทำลายเป้าหมายกว่า ๕๐ แห่งภายใน ๑๖ ประเทศทั่วโลก เช่น หน่วยงานทางด้านความมั่นคงของสหรัฐอเมริกา สนามบินและสายการบินของเกาหลีใต้ หน่วยงานทางด้านพลังงานในกลุ่มประเทศตะวันออกกลาง เช่น คูเวต การ์ตาร์ และซาอุดิอาระเบีย

นอกจากประเทศอิหร่านแล้วยังมีประเทศซีเรีย ซึ่งมีกลุ่มแฮกเกอร์ชื่อ Syrian Electronic Army ที่ได้เจาะเข้าไปในเครือข่ายขององค์กรชั้นนำของโลกไม่ว่าจะเป็นสำนักข่าวเอพี บีบีซี ไฟแนนเชียลไทมส์ และอีกมาก ด้วยเทคนิคต่างๆ เช่น DDoS, Phishing, Web-page defacement รวมทั้ง spamming โดยเฉพาะอย่างยิ่งการแฮก Twitter ของสำนักข่าวเอพีเพื่อโพสท์ข้อความว่าทำเนียบขาวถูกโจมตีด้วยระเบิดและประธานาธิบดีโอบามาได้รับบาดเจ็บนั้นได้สร้างความเสียหายต่อตลาดหุ้นเป็นมูลค่าสูงถึงสองแสนล้านดอลล่าห์เลยทีเดียว

อิสราเอล เป็นประเทศที่ขึ้นชื่อในเรื่องของเทคโนโลยีป้องกันประเทศ รวมทั้งเป็นประเทศชั้นนำทางด้านของเทคโนโลยีด้านไซเบอร์ด้วยเช่นกัน อย่างไรก็ตามก็มีรายงานว่าถูกโจมตีจากฝ่ายตรงข้ามทางด้านไซเบอร์หลายต่อหลายครั้ง ไม่ว่าจะเป็นการถูกโจมตีด้วย DDoS จากกว่า ๕๐๐,๐๐๐ เครื่องในปี ๒๐๐๘ การถูกมัลแวร์ชื่อ Mahdi โจมตีเป้าหมายจำนวน ๕๔ แห่งในประเทศในปี ๒๐๑๒ รวมทั้งมีข่าวว่าถูก Syrian Electronic Army โจมตีระบบจ่ายน้ำประปาที่เมืองไฮฟาในปี ๒๐๑๓

ประเทศสหรัฐอเมริกาเป็นประเทศที่เชื่อว่ามีการโจมตีทางไซเบอร์ที่มีความซับซ้อนที่สุด ไม่ว่าจะเป็น Stuxnet, ๗๔ Duqu, Flame และ Gauss.๗๕ ซึ่งมัลแวร์เหล่านี้มีความซับซ้อนเกินกว่าที่แฮกเกอร์ทั่วไปจะสามารถสร้างได้ และยังต้องการการลงทุนในการออกแบบและพัฒนาที่สูง

ในมุมทางด้านการป้องกันนั้น หลายประเทศได้เริ่มดำเนินการฝึกเตรียมความพร้อมทางด้านไซเบอร์ โดยล่าสุดในเดือนพฤศจิกายน ๒๐๑๔ ที่ผ่านมานั้น NATO ได้จัดการฝึกซ้อมทางด้านไซเบอร์ที่มีผู้เข้าร่วมมากถึง ๔๐๐ คนในประเทศเอสโตเนีย เป็นการฝึกไซเบอร์ที่ใหญ่ที่สุด นอกจากนี้สหรัฐอเมริกาได้จัดตั้งศูนย์ National Cyber Range ซึ่งเป็นศูนย์ฝึกซ้อมทางด้านไซเบอร์ที่สามารถจำลองเครือข่ายของทั้งประเทศเอาไว้ได้เพื่อฝึกซ้อมทั้งเชิงรุกและเชิงรับต่อสถานการณ์จริงที่อาจจะเกิดขึ้นในอนาคต

เมื่อช่วงต้นเดือนธันวาคม ๒๐๑๔ ที่ผ่านมาได้มีการเปิดเผยกลุ่มแฮกเกอร์ที่ชื่อว่า FIN๔ ซึ่งมุ่งเน้นการโจมตีองค์กรที่อยู่ในธุรกิจสถานพยาบาลและธุรกิจยาในประเทศที่ใช้ภาษาอังกฤษเป็นภาษาหลักในการสื่อสาร โดยรูปแบบของกลุ่มนี้แตกต่างจากกลุ่มแฮกเกอร์อื่นๆ ที่มักมุ่งเน้นในการใช้มัลแวร์ แต่แฮกเกอร์กลุ่มนี้ใช้เทคนิคขั้นสูงหลายๆ เทคนิคที่นอกเหนือจากมัลแวร์ รวมทั้งใช้ Social Engineering แบบมุ่งเป้าในการโจมตีเป้าหมาย

๔.๒ สถานการณ์ทางด้านไซเบอร์ของยุโรป

ปัจจุบันมีหลากหลายประเทศที่ดำเนินการพัฒนาทางด้านการป้องกันทางไซเบอร์ท่ามกลางสมาชิกสหภาพยุโรปด้วยกัน โดยส่วนใหญ่แล้วสมาชิกสหภาพยุโรปได้รับเอาแผนยุทธศาสตร์ทางด้านการป้องกันทางไซเบอร์ระดับชาติมาใช้ โดยยังได้อ้างถึงว่าการป้องกันทางไซเบอร์เป็นส่วนนึงของแผนการป้องกันเชิงกลยุทธ์ระดับชาติ สมาชิกสหภาพยุโรปกว่า ๑๕ ประเทศ ได้รวมวิสัยทัศน์ทางการทหารเข้ากับการป้องกันทางไซเบอร์ แต่มีจำนวนไม่มากนักที่พร้อมจะลงทุนกับอาวุธทางด้านไซเบอร์

ประเทศเดนมาร์ก ได้ทำข้อตกลงทางด้านการป้องกันระหว่างปี ๒๐๑๓-๒๐๑๗ โดยจัดตั้งศูนย์การป้องกันทางไซเบอร์ ภายใต้การควบคุมของ องค์กรการป้องกันแห่งชาติ พร้อมกับพัฒนาบุคลากรทางทหารให้มีความสามารถด้านการปฏิบัติการคอมพิวเตอร์และระบบเน็ตเวิร์ก เพื่อเตรียมพร้อมกับการปฏิบัติการทางทหารในส่วนของ Cyberspace ทั้งเชิงรุกและเชิงรับ

ประเทศเอสโตเนีย ในปี ๒๐๐๘ กลยุทธ์ทางด้านการรักษาความปลอดภัย ได้ถูกปรับปรุงใหม่ โดยองค์กรการป้องกันแห่งชาติและ กองกำลังป้องกันได้รับผิดชอบร่วมกันในส่วนของการป้องกันไซเบอร์ระดับชาติ โดยมีการระดมอาสาสมัครจากหน่วยงานต่างๆเพื่อพัฒนาขีดความสามารถทางด้านไซเบอร์

ประเทศฟินแลนด์ ได้ประกาศเมื่อปี ๒๐๑๑ ที่จะลงทุนในอาวุธการป้องกันทางไซเบอร์ จนกระทั่งปี ๒๐๑๓ แผนการป้องกันไซเบอร์ระดับชาติได้บ่งชี้ว่า กองกำลังป้องกันชาวฟินนิชได้พัฒนาขีดความสามารถที่ครอบคลุม ซึ่งประกอบด้วยองค์ความรู้ทางด้านไซเบอร์ สงครามไซเบอร์ และ ศักยภาพในการป้องกัน สำหรับหน่วยงานการป้องกันทางด้านไซเบอร์จะเริ่มปฏิบัติการในปี ๒๐๑๕

ประเทศฝรั่งเศส แผนระบบสารสนเทศและการรักษาความปลอดภัยปี ๒๐๑๑ ได้ประกอบไปด้วยจุดมุ่งหมายหลัก ๔ ประการ เพื่อที่จะทำให้ประเทศฝรั่งเศสมีขีดความสามารถระดับโลกในด้านการป้องกันทางไซเบอร์ และในปี ๒๐๑๓ ยังได้มีการบันทึกลงในหนังสือว่า การโจมตีทางไซเบอร์เป็นภัยคุกคามอันดับสามต่อการป้องกันระดับชาติ ประเทศฝรั่งเศสยังได้พัฒนาองค์ความรู้ขีดความสามารถทางด้านไซเบอร์ พอๆกับขีดความสามารถเชิงรุก สำหรับผู้ที่บริหารการป้องกันทางด้านไซเบอร์นั้นคือ หน่วยงานรักษาความปลอดภัยสารสนเทศและเครือข่ายแห่งประเทศฝรั่งเศส ซึ่งถูกก่อตั้งขึ้นเมื่อปี ๒๐๐๙ โดยรับผิดชอบในเรื่องของ การตรวจหาและตอบโต้การโจมตีทางไซเบอร์ สนับสนุนการวิจัยและพัฒนา เตรียมข้อมูลให้หน่วยงานอื่นๆของรัฐบาล และในเดือนมกราคมปี ๒๐๑๔ องค์กรการป้องกันแห่งชาติได้ทำรายได้จากการวิจัยและพัฒนาขีดความสามารถทางด้านการป้องกันทางไซเบอร์สูงถึง หนึ่งพันล้านฟรังก์

ประเทศเยอรมนี ได้จัดตั้งคณะกรรมการการป้องกันทางไซเบอร์แห่งชาติขึ้นเมื่อปี ๒๐๑๑ และหน่วยงานการตอบโต้ทางไซเบอร์แห่งชาติเพื่อทำงานตามนโยบายทางด้านไซเบอร์ ทั้งนี้กองทัพของเยอรมันซึ่งมีชื่อว่า Strategic Reconnaissance Unit เป็นหน่วยพิเศษที่มีความเชี่ยวชาญด้านไซเบอร์ซึ่งถูกฝึกฝนให้มีขีดความสามารถในเชิงรุกอีกด้วย

ประเทศอิตาลี ได้จัดตั้งกองกำลังสงครามอิเล็กทรอนิกส์เพื่อรับผิดชอบองค์ความรู้ การตรวจตรา การตรวจค้นและการลาดตระเวน และในปี ๒๐๑๓ หน่วยงานสำคัญของรัฐบาลได้เน้นให้เห็นถึงความจำเป็นที่จะพัฒนา โครงสร้างองค์ความรู้ทางด้านไซเบอร์ และขีดความสามารถทางการป้องกันด้านไซเบอร์ การบัญชาการและควบคุม เพื่อที่จะวางแผนให้กองทัพพร้อมปฏิบัติการทางด้าน Cyberspace

ประเทศเนเธอร์แลนด์ ได้ปรับใช้แผนการป้องกันยุทธศาสตร์ทางด้านไซเบอร์ขึ้นในปี ๒๐๑๒ โดยมีวัตถุประสงค์หลัก ๖ ประการ ได้แก่ การปรับตัวกับสถานการณ์เฉพาะหน้าได้อย่างครอบคลุม, พัฒนาขีดความสามารถการป้องกันทางไซเบอร์, พัฒนาขีดความสามารถทางไซเบอร์เชิงรุก, พัฒนาองค์ความรู้ทางด้าน Cyberspace ให้มีความแข็งแกร่งยิ่งขึ้น,พัฒนาและคิดค้นนวัตกรรมและรับเอาคนที่มีฝีมือเข้ามา และ สามารถทำงานร่วมกับองค์กรต่างๆในระดับสากล

ประเทศอังกฤษ แผนการป้องกันทางไซเบอร์ปี ๒๐๑๑ ได้กำหนดให้การโจมตีทางไซเบอร์เป็นภัยคุกคามระดับชาติ และในปี ๒๐๑๓ รัฐบาลอังกฤษยังได้ประกาศให้การปฏิบัติการร่วมระหว่างองค์กรอิสระ และหน่วยงานทางทหาร เพื่อพัฒนากองกำลังทางไซเบอร์สำหรับการตอบโต้กับสถานการณ์ต่างๆที่อาจเกิดขึ้นได้ โดยเฉพาะสิ่งที่เกี่ยวกับทางทหาร โดยการอ้างอิงจากงบประมาณทางทหารในปี ๒๐๑๔ รัฐบาลอังกฤษได้

ประกาศการลงทุนโปรแกรมการป้องกันทางไซเบอร์ระดับชาติเป็นงบประมาณสูงถึง ๖๕๐ ล้านยูโร และมีความเป็นไปได้ที่จะมีส่วนเพิ่มเติมอีกเป็นจำนวน ๑๕๐ล้าน ยูโร เพื่อที่จะวัดระดับการรักษาความปลอดภัยทางไซเบอร์เป็นระยะเวลาตลอด ๔ ปี และในปี ๒๐๑๔ อังกฤษได้ประกาศการลงทุนในงบวิจัยและพัฒนาด้านการตอบโต้อัตโนมัติในระบบการป้องกันทางไซเบอร์เป็นจำนวนเงิน ๒ ล้านยูโร

๔.๓ สถานการณ์ทางด้านไซเบอร์ของกลุ่มประเทศเอเชียแปซิฟิก

ในภูมิภาคนี้นั้นประเทศจีนนับได้ว่าเป็นประเทศที่มีกิจกรรมทางด้านไซเบอร์มากที่สุด โดยที่ว่ากันว่ารัฐบาลจีนได้สนับสนุนแฮกเกอร์จำนวนมากเพื่อปฏิบัติการตั้งแต่การจารกรรมข้อมูลที่เป็นความลับของประเทศมหาอำนาจ โดยเฉพาะอย่างยิ่งสหรัฐอเมริกา จนถึงประเทศต่าง ๆ ทั่วโลกมากมาย จากข้อมูลพบว่าในปี ๒๐๐๙ ได้มีนักวิจัยจากประเทศแคนาดาได้ออกมาเปิดเผยว่าจีนได้มีการดำเนินการจารกรรมไซเบอร์ต่อประเทศกว่า ๑๐๐ ประเทศ และในปี ๒๐๑๐ ได้มีรายงานว่าได้มีปริมาณข้อมูลมหาศาลซึ่งถูกย้ายทิศทางการส่งจากที่ต่างๆ ไปยังประเทศจีน เป็นเวลากว่า ๒๐ นาที ซึ่งข้อมูลเหล่านั้นมาจากเครือข่ายกว่า ๘,๐๐๐ เครือข่ายในสหรัฐ ๑,๑๐๐ เครือข่ายในประเทศออสเตรเลีย และ ๒๓๐ เครือข่ายจากประเทศฝั่งเศส ซึ่งจีนเองนั้นก็ได้ดำเนินการจารกรรมข้อมูล รวมทั้งโจมตีเครือข่ายเป้าหมายทั่วโลก รูปแบบการโจมตีของแฮกเกอร์จีนนั้นไม่ได้เป็นวิธีการที่มีความซับซ้อน แต่เป็นเทคนิคที่สามารถถูกนำไปใช้ซ้ำๆ ได้ในหลายๆ คน เช่น brute-force attack ตัวอย่างของแฮกเกอร์ของจีนที่รัฐบาลให้การสนับสนุนได้แก่ APT๑ ที่มีข่าวว่ามีฐานปฏิบัติการอยู่ในเซี่ยงไฮ้ และ The Comment Crew ซึ่งอยู่เบื้องหลังปฏิบัติการทางด้านไซเบอร์ที่สำคัญๆ มากมาย

ในขณะเดียวกันประเทศจีนเองก็ยังได้มีการเผยว่ามีประเทศต่างๆ ได้เจาะเข้ามาภายในเครือข่ายของจีนเช่นกัน ไม่ว่าจะเป็นจาก ไต้หวัน สหรัฐอเมริกา

นอกจากประเทศจีนแล้ว ประเทศเกาหลีเหนือเป็นอีกประเทศหนึ่งที่ได้มีการคาดการณ์ว่ามีการสนับสนุนแฮกเกอร์จำนวนมาก แม้ว่าประเทศจะดูล้าหลังเมื่อเทียบกับประเทศคู่ขัดแย้งอย่างเกาหลีใต้ แต่เกาหลีเหนือเองก็ได้ชื่อว่าเป็นประเทศที่ได้สะสมอาวุธไซเบอร์ไว้อย่างมากมาย ซึ่งได้เป็นข่าวในหน้าหนังสือพิมพ์ตั้งแต่ปี ๒๐๐๙ เป็นต้นมา ปฏิบัติการของประเทศเกาหลีเหนือนั้นหลักๆ เน้นจู่โจมไปที่เครือข่ายของเกาหลีใต้เป็นหลัก ไม่ว่าจะเป็นการจารกรรมข้อมูล การทำ DDoS หรือการส่งมัลแวร์เข้าไปเมื่อลบข้อมูลในฮาร์ดไดร์ฟ รวมทั้ง Spear phishing ว่ากันว่าเกาหลีเหนือมีทหารไซเบอร์อยู่ว่า ๓,๐๐๐ นาย แม้ว่าบางแหล่งข่าวจะแจ้งว่ามีประมาณ ๑,๘๐๐ นายก็ตาม ซึ่งส่วนใหญ่ได้รับการฝึกฝนจากประเทศจีนและรัสเซีย ล่าสุดเกาหลีเหนือยังถูกโยงเข้าไปมีส่วนพัวพันกับการแฮกบริษัท Sony Pictures ซึ่งมีการสร้างและฉายภาพยนตร์ซึ่งมีเนื้อหาเกี่ยวกับผู้นำของเกาหลีเหนือ ซึ่งภายหลังทางเกาหลีเหนือได้ออกมาปฏิเสธ แม้ว่าเกาหลีเหนือจะมีกองทัพไซเบอร์ที่เข้มแข็ง แต่ก็ได้มีข่าวว่าในปี ๒๐๑๓ นั้นเว็บไซต์ทั้งประเทศของเกาหลีเหนือล่มจากการกระทำจากปฏิบัติการร่วมระหว่างประเทศเกาหลีใต้และสหรัฐอเมริกา

ประเทศอินเดียและปากีสถานเป็นประเทศที่มีรายงานว่าได้ทำสงครามไซเบอร์ระหว่างกัน จากเหตุความขัดแย้งที่บริเวณพรมแดนของทั้งสองประเทศ ไม่ว่าจะเป็นการที่แฮกเกอร์ปากีสถานฝังมัลแวร์ลงไปในเว็บไซต์ดาวน์โหลดเพลงของอินเดียเพื่อเจาะเข้าไปในเครือข่ายต่าง ๆ ของอินเดีย รวมทั้งเหตุการณ์ที่กลุ่มที่เรียกตัวเองว่า Pakistani Cyber Army ได้ทำการเปลี่ยนหน้าเว็บไซต์และปิดเว็บของสำนักงานสอบสวนกลางของอินเดีย ในปี ๒๐๑๐ และเหตุการณ์เจาะเว็บไซต์กว่า ๑๐๐ เว็บในปี ๒๐๑๒ ในทางกลับกันได้มีปฏิบัติการชื่อ Operation Hangover ของแฮกเกอร์อินเดียซึ่งเจาะเข้าไปในเครือข่ายของอุตสาหกรรมหลักของประเทศปากีสถาน รวมทั้งภาคการทหาร

๔.๔ สถานการณ์สงครามไซเบอร์ในกลุ่มประเทศอาเซียน

ประเทศในกลุ่มอาเซียนส่วนใหญ่เป็นประเทศกำลังพัฒนาซึ่งมีความตระหนักทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ต่ำ เทคนิคที่แฮกเกอร์ใช้ส่วนใหญ่มักจะเป็น APT ที่มาในรูปแบบของ Spear phishing ซึ่งในอีเมลนั้นมักจะมีไฟล์แนบซึ่งแสดงให้เชื่อว่ามีข้อมูลสำคัญอยู่ภายในนั้น ซึ่ง APT นั้นมุ่งเน้นไปที่หน่วยงานภาครัฐเป็นหลักในประเทศกลุ่มอาเซียน ซึ่งกลุ่มอุตสาหกรรมที่ตกเป็นเป้าจากการโจมตีคือ โทรคมนาคม การขนส่ง พลังงาน ธนาคาร เป็นต้น ในส่วนของการทำสงครามไซเบอร์อันเป็นผลมาจากความขัดแย้งระหว่างประเทศในกลุ่มนี้นั้นยังไม่ปรากฏเด่นชัด นอกเหนือไปจาก APT และ Spear phishing แล้วนั้น เครือข่ายต่างๆที่อยู่ในกลุ่มประเทศเหล่านี้ส่วนใหญ่มีระดับการรักษาความมั่นคงปลอดภัยในระดับที่ต่ำ และง่ายแก่การเจาะเข้าไป รวมทั้งใช้เป็นทั้งฐานในการปฏิบัติการไซเบอร์ในพื้นที่อื่น เช่น เป็นฐานในการตั้ง CnC server เป็นต้น ซึ่งพอจะสรุปขีดความสามารถของแต่ละประเทศในกลุ่มอาเซียนได้ดังนี้

ประเทศกัมพูชา มีความเกี่ยวข้องกับนโยบายทางด้านไซเบอร์และการรักษาความปลอดภัยในระดับที่ต่ำมาก โดยการใช้งานส่วนใหญ่จะเกี่ยวข้องกับซอฟต์แวร์ประเภทโอเพ่นซอร์ส แต่ก็ยังไม่เป็นที่แน่ชัด ในภาพรวมเป็นที่เข้าใจได้ว่ากัมพูชามีขีดความสามารถในการป้องกันการโจมตีทางด้านไซเบอร์ในระดับที่ต่ำ

ประเทศอินโดนีเซีย รัฐบาลอินโดนีเซียได้ประกาศแผนที่จะจัดตั้งศูนย์ปฏิบัติการด้านไซเบอร์เพื่อที่จะใช้ในการปฏิบัติการร่วมกับการรักษาความปลอดภัยทางไซเบอร์นานาชาติโดยรวมถึงการปฏิบัติการเฉพาะทางด้านการรักษาความปลอดภัยทางไซเบอร์โดยกองทัพของกองทัพอินโดนีเซีย ทางหน่วยงานกลางยังพยายามที่จะรวบรวมหน่วยงานราชการต่างๆและองค์กรระดับชาติต่างๆ ให้เข้าร่วมเพื่อที่จะเพิ่มขีดความสามารถด้านยุทธศาสตร์ข้ามหน่วยงาน รวมถึงมีการเสนอการจัดตั้งกองกำลังไซเบอร์เรียบร้อยแล้ว แต่ทั้งนี้ก็ยังไม่เป็นที่แน่ชัดว่ามีความก้าวหน้าในระดับใดในขั้นต้น แต่การประกาศของรัฐบาลครั้งนี้ได้สื่อให้เห็นว่ากองทัพอินโดนีเซียได้ตระหนักถึงภัยคุกคามทางด้านไซเบอร์เป็นอย่างดี

ประเทศมาเลเซีย มีรายงานมาว่ากองทัพมาเลเซียได้เริ่มที่จะพัฒนาขีดความสามารถเพื่อที่จะป้องกันทรัพย์สินต่างๆ โดยรวมถึงภัยคุกคามด้านไซเบอร์ ซึ่งองค์กรการป้องกันของมาเลเซียได้ประกาศที่จะสนับสนุนการพัฒนาแผนแม่บทการรักษาความปลอดภัยทางไซเบอร์ของเอเชียตะวันออกเฉียงใต้ มาเลเซียได้สะท้อนแง่มุมที่ตระหนักถึงความเสี่ยงทางด้านภัยคุกคามทางไซเบอร์โดยกองทัพของมาเลเซียเอง แต่ถูกลดทอนความสำคัญลงไปเนื่องจากนโยบายแนวทางการพัฒนาทางด้านไซเบอร์ที่ไม่ชัดเจน

ประเทศพม่า องค์กรการป้องกันและบริการทางคอมพิวเตอร์ซึ่งอยู่ภายใต้การบังคับบัญชาของกองทัพพม่า ได้รวมสงครามเน็ตเวิร์คเซ็นทริค ขีดความสามารถทางไซเบอร์ของประเทศทางแถบตะวันออกของทวีปเอเชียและสงครามอิเล็กทรอนิกส์ เข้าด้วยกัน โดยมีการสังเกตว่าขีดความสามารถทางด้านสงครามไซเบอร์ของพม่านั้นมีการเติบโตอย่างมีนัยยะสำคัญมากขึ้นทุกๆปี โดยมีความช่วยเหลือของประเทศในกลุ่มภูมิภาค รัสเซียและจีนได้รับบทบาทที่จะฝึกและพัฒนาเจ้าหน้าที่บุคลากรให้ ส่วนทางด้านสิงคโปร์รวมถึงจีนก็ให้การสนับสนุนทางด้านอุปกรณ์และเครื่องมือต่างๆ

ประเทศฟิลิปปินส์ กองทัพของฟิลิปปินส์ได้สร้างศูนย์ปฏิบัติการรักษาความปลอดภัย โดยเน้นจุดมุ่งหมายสำคัญไปที่บทบาทการป้องกัน การคุ้มกันระบบของกองทัพ อย่างไรก็ตาม ยังไม่ปรากฏถึงแนวทางการดำเนินงานที่แน่ชัด

ประเทศสิงคโปร์ กองทัพของสิงคโปร์ได้จัดตั้งศูนย์การรักษาความปลอดภัยทางไซเบอร์ ซึ่งเน้นไปที่การป้องกันระบบเน็ตเวิร์คของกองทัพ สิ่งเหล่านี้ชี้ให้เห็นว่ามีการตระหนักถึงความสำคัญของความเสี่ยงทางไซเบอร์และกำลังหาทางดำเนินการ แต่ก็ไม่มีการเผยแพร่ข้อมูลสู่สาธารณะ

ประเทศเวียดนาม ยังไม่ปรากฏเป็นที่แน่ชัดว่ามีการดำเนินงานด้านสงครามไซเบอร์ แต่มีมาตรการการรักษาความปลอดภัยจากรัฐบาล ซึ่งใช้เป็นบทลงโทษกับผู้กระทำผิด ปัจจุบันตกเป็นเป้าหมายของแฮกเกอร์หลายๆประเทศโดยเฉพาะประเทศจีน

ส่วนประเทศบรูไนและลาว มีการดำเนินการและการตระหนักถึงภัยคุกคามทางด้านไซเบอร์ที่ค่อนข้างน้อยในปัจจุบัน

บทที่ ๕

Cyber Security and Cyber Laws

การตระหนักถึงสิทธิ กฎหมายของการระวังป้องกันทางไซเบอร์

๕.๑ กฎหมายทางด้านเทคโนโลยีสารสนเทศ

ทำไมต้องมีการออกกฎหมายเทคโนโลยีสารสนเทศ สังคมสารสนเทศเป็นสังคมใหม่การอยู่ร่วมกันในสังคมสารสนเทศ จำเป็นต้องมีกฎเกณฑ์เพื่อการ อยู่ร่วมกันโดยสันติและสงบสุข เอื้อประโยชน์ซึ่งกันและกัน ทุกวันนี้เครือข่ายอินเทอร์เน็ตได้เข้ามามีบทบาท ในชีวิตประจำวัน มีการใช้คอมพิวเตอร์ และระบบสื่อสารกันมาก ขณะเดียวกันก็มีผู้ใช้เทคโนโลยี สารสนเทศในทางที่ไม่ถูก ไม่ควร ดังนั้น จึงจำเป็นต้องมีกฎหมายเทคโนโลยีสารสนเทศ และเมื่อมีกฎหมายแล้ว ผู้ใช้เทคโนโลยีสารสนเทศจะปฏิเสธ ความผิดว่าไม่รู้กฎหมายไม่ได้

กฎหมายเทคโนโลยีสารสนเทศ กฎหมายเทคโนโลยีสารสนเทศของประเทศไทยเริ่มวันที่ ๑๕ ธันวาคม ๒๕๔๑ โดยคณะ กรรมการ เทคโนโลยีสารสนเทศแห่งชาติ (กทสช) ได้ทำการศึกษาและยกร่างกฎหมายเทคโนโลยีสารสนเทศ จำนวน ๖ ฉบับ ได้แก่

๑. กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law) เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับ นิติสัมพันธ์ต่างๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่ จัดทำขึ้น ให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

๒. กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law) เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใดๆ ทางเทคโนโลยีให้เสมอด้วยการลง ลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้ บริการอื่น ที่เกี่ยวข้องกับ ลายมือชื่ออิเล็กทรอนิกส์

๓. กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึง และเท่าเทียมกัน(National Information Infrastructure Law) เพื่อก่อให้เกิดการส่งเสริม สนับสนุน และพัฒนาโครงสร้างพื้นฐานสารสนเทศ อันได้แก่โครงข่าย โทรคมนาคม เทคโนโลยีสารสนเทศ สารสนเทศทรัพยากรมนุษย์ และโครงสร้างพื้นฐานสารสนเทศสำคัญ อื่นๆ อันเป็นปัจจัยพื้นฐาน สำคัญในการพัฒนาสังคม และชุมชนโดยอาศัยกลไกของรัฐ ซึ่งรองรับ เจตนารมณ์สำคัญประการหนึ่งของแนวนโยบายพื้นฐานแห่งรัฐตามรัฐธรรมนูญ มาตรา ๗๘ ในการกระจาย สารสนเทศให้ทั่วถึง และเท่าเทียมกัน และนับเป็นกลไกสำคัญในการช่วยลดความเหลื่อมล้ำของสังคม อย่างค่อยเป็นค่อยไป เพื่อสนับสนุนให้ท้องถิ่นมีศักยภาพในการปกครองตนเองพัฒนาเศรษฐกิจภายในชุมชน และนำไปสู่สังคมแห่งปัญญา และการเรียนรู้

๔. กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law) เพื่อก่อให้เกิดการรับรองสิทธิ และให้ความคุ้มครองข้อมูลส่วนบุคคลซึ่งอาจถูกประมวลผลเปิดเผย หรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

๕. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law) เพื่อกำหนดมาตรการทางอาญา ในการลงโทษผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ทั้งนี้เพื่อเป็นหลักประกันสิทธิเสรีภาพ และการคุ้มครองการอยู่ร่วมกันของ สังคม

๖. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Law) เพื่อกำหนดกลไกสำคัญทางกฎหมายในการรองรับระบบการโอนเงินทางอิเล็กทรอนิกส์ ทั้งที่เป็น การโอนเงินระหว่างสถาบันการเงิน และ ระบบการชำระเงินรูปแบบใหม่ในรูปของเงินอิเล็กทรอนิกส์ ก่อให้เกิดความเชื่อมั่นต่อระบบการทำธุรกรรมทางการเงิน และการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น

๕.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ.๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ผ่านการเห็นชอบจาก สภานิติบัญญัติ การลงพระปรมาภิไธย และการประกาศลงในราชกิจจานุเบกษาแล้ว เมื่อ ๑๘ มิถุนายน พ.ศ. ๒๕๕๐ และจะมีผลใช้บังคับตั้งแต่ ๑๙ กรกฎาคม พ.ศ. ๒๕๕๐ เป็นต้นไป ดังนั้นผู้ใช้คอมพิวเตอร์ อินเทอร์เน็ตโดยทั่วไป ผู้ให้บริการ ซึ่งรวมไปถึงหน่วยงานต่างๆ ที่เปิดบริการอินเทอร์เน็ตให้แก่ผู้อื่นหรือ กลุ่มพนักงานนักศึกษาในองค์กร ควรทราบถึงรายละเอียดของพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยประเทศไทยได้มีการบังคับใช้เป็นที่เรียบร้อยแล้ว

๕.๒.๑ ความเป็นมาของพระราชบัญญัติ ๒๕๕๐

๕.๒.๑.๑ สภาพปัญหาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ในปัจจุบัน

๕.๒.๑.๑(๑) ความสำคัญของคอมพิวเตอร์ในชีวิตประจำวัน

๕.๒.๑.๑(๒) ผลของการกระทำผิดกระทบหรือความเสียหายในวงกว้างและรวดเร็ว

๕.๒.๑.๑.(๓) ยังไม่มีกฎหมายกำหนดความผิดมาก่อน

๕.๒.๑.๑(๓.๑) การที่กฎหมายอาญามุ่งคุ้มครอง วัตถุที่มีรูปร่างเท่านั้น แต่ในยุคไอที ข้อมูลข่าวสาร เป็นวัตถุที่ไม่มีรูปร่าง ตัวอย่างของการก่ออาชญากรรมทางคอมพิวเตอร์ได้แก่ การ โจรกรรมเงินในบัญชีลูกค้าของธนาคาร การโจรกรรมความลับของบริษัทต่างๆ ที่เก็บ ไว้ในคอมพิวเตอร์ การปล่อยไวรัสเข้าไปในคอมพิวเตอร์

๕.๒.๑.๑(๓.๒) พยานหลักฐานที่เกี่ยวกับคอมพิวเตอร์นั้นสามารถเปลี่ยนแปลงได้ตลอดเวลาและถูก กระทำได้ง่ายแต่ยากต่อการสืบหา

๕.๒.๑.๑.(๓.๓) ปัญหาเรื่องขอบเขตพื้นที่ซึ่งเป็นเรื่องที่มี ความสำคัญ เพราะผู้กระทำความผิดอาจ กระทำจากที่อื่นๆ ที่ไม่ใช่ประเทศไทย ซึ่งอยู่นอกเขตอำนาจของศาลไทย

๕.๒.๑.๒ เจตนารมณ์ในการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เนื่องจากปัญหาภัยคุกคามที่เกิดจาก ไวรัสคอมพิวเตอร์ แฮกเกอร์ การเผยแพร่รูปภาพ ข้อความ ที่มีลักษณะลามก อนาจาร หรือข้อมูลอันเป็นเท็จที่ก่อให้เกิดความเสียหายต่อบุคคล ต่อความมั่นคงทางการ เมือง สังคม และเศรษฐกิจของประเทศ จึงเป็นเหตุให้เกิดการร่างพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ขึ้นโดยมีเจตนารมณ์ดังนี้

๕.๒.๑.๒(๑) เพื่อเป็นการใช้กรอบแห่งกฎหมายในการกำหนดฐานความผิดและบทลงโทษในการเรียกร้อง ค่าเสียหายแก่ผู้กระทำความผิดเพื่อคุ้มครองสิทธิให้แก่ประชาชน

๕.๒.๑.๒.(๒) เพื่อกำหนดบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานเจ้าหน้าที่ทั้งด้านนโยบาย มาตรฐาน แนวปฏิบัติ และกำหนดหน้าที่ของผู้ให้บริการไม่ว่าจะแก่ตนเองหรือบุคคลอื่นในการเข้าสู่ อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยผ่านระบบคอมพิวเตอร์ก็ตาม โดยให้มีแนวทางการปฏิบัติการดำเนินงานให้เกิดความชัดเจนถูกต้องในแนวทางเดียวกัน

๕.๒.๒ ความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีทั้งหมด ๓๐ มาตรา ซึ่งในบทเรียนนี้ จะกล่าวถึงหมวดที่ ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ เท่านั้น

หมวดที่ ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ ความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ

มาตรา ๕ การ เข้าถึงระบบคอมพิวเตอร์: ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่ มีมาตราการป้ องกัน การเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ การล่วงรู้มาตรการป้องกันการเข้าถึง : ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึง ระบบคอมพิวเตอร์ที่ ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแต่ ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ การ เข้าถึงข้อมูลคอมพิวเตอร์: ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่ มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกิน สี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ การ ดักข้อมูลโดยมิชอบ: ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อ ดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อ ประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ การแก้ไขเปลี่ยนแปลง ข้อมูลคอมพิวเตอร์ : ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือ เพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ ต้อง ระวางโทษจำคุกไม่เกินห้า ปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา ๑๐ รบกวน ขัดขวาง ระบบคอมพิวเตอร์ : ผู้ใดกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของ ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้อง ระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ สแปมเมล์ (Spam mail) : ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดย ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล ดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ การกระทำความผิดต่อ ประชาชนโดยทั่วไป / ความมั่นคง : ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชนไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันที หรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ต้องระวางโทษจำคุกไม่เกิน สิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศความปลอดภัยสาธารณะ หรือ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ที่มีไว้เพื่อประโยชน์สาธารณะ ต้อง ระวางโทษจำคุกตั้งแต่สามปี ถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปี ถึง ยี่สิบปี

มาตรา ๑๓ การจำหน่าย / เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด : ผู้ใดจำหน่าย หรือ เผยแพร่ชุดคำสั่ง ที่ จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด ตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่น บาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ นำเข้า / ปลอม / เท็จ / ภัยมั่นคง / ลามก / ส่งต่อข้อมูลคอมพิวเตอร์ : ผู้ใด กระทำความผิดที่ระบุ ไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความ เสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความ ตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการ ก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และ ข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ความรับผิดของผู้ให้บริการ: ผู้ใดให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด ตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำ ความผิดตามมาตรา ๑๔

มาตรา ๑๖ การเผยแพร่ภาพ ตัดต่อ / ดัดแปลง: ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกิน หกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหาย ได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

๕.๒.๓ สรุปบทลงโทษสำหรับผู้กระทำ ความผิดกฎหมายภายใต้ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ.๒๕๕๐

๕.๓ ตารางความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิด	โทษจำคุก	โทษปรับ
การเข้าถึงระบบคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยไม่ชอบ	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
การทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลงเพิ่มเติมข้อมูลคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่นโดยปกติสุข (Spam Mail)	ไม่มี	ไม่เกิน ๑๐๐,๐๐๐ บาท
การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
การกระทำต่อความมั่นคง -ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ -กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ - เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	 ไม่เกิน ๑๐ ปี ๓ ปี ถึง ๑๕ ปี ๑๐ ปี ถึง ๒๐ ปี	 ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐-๓๐๐,๐๐๐ บาท ไม่มี
การใช้ระบบคอมพิวเตอร์ท าความผิดอื่น (การเผยแพร่เนื้อหาอันไม่เหมาะสม)	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำ ความผิด ต้องระวางโทษ เช่นเดียวกับผู้กระทำ ความผิด ต้องระวางโทษ เช่นเดียวกับผู้กระทำ ความผิด การตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท

๕.๔ คำแนะนำเพื่อป้องกันการกระทำความผิด

● ไฟล์วอลส่วนตัว (Personal Firewall) ไฟล์วอลล์ส่วนตัวคือซอฟแวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัวซึ่งทำหน้าที่ป้องกันผู้บุกรุกหรือผู้ ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ส่วนตัวของเราหรือช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดี เช่น ไวรัส โทรจัน สปายแวร์ ถูกติดตั้งลงไปในเครื่องคอมพิวเตอร์ส่วนตัวโดยที่เราไม่ทราบหรือไม่รู้ตัว ดังนั้นเราควรติดตั้งไฟล์วอลล์ส่วนตัวโดยสามารถดาวน์โหลดได้จากเว็บ

● การสวมรอยบุคคล (Identity Theft) ในปัจจุบัน การขโมยและการฉ้อฉลนั้น สามารถกระทำได้กับเอกสารอิเล็กทรอนิกส์ที่อยู่ในเครื่อง คอมพิวเตอร์ ทั้งนี้เนื่องจากปัจจุบันเอกสารสำคัญที่ใช้ระบุตัวตนมากมายได้ถูกจัดเก็บไว้ในเครื่อง คอมพิวเตอร์และอาจเข้าถึงได้ โดยผู้บุกรุกโดยผ่านเครือข่ายอินเทอร์เน็ต การขโมยเอกสารสำคัญนั้นอาจนำไปสู่การสวมรอยเป็นตัวบุคคลผู้เป็นเจ้าของเอกสารนั้น และอาจใช้ในการดำเนินเรื่องต่าง ๆ แทนเจ้าของ โดยมิได้รับอนุญาตซึ่งเป็นการกระทำที่ผิดกฎหมาย เช่นการขโมยบัญชีผู้ใช้และรหัสผ่านเพื่อทำการล็อกอิน เข้าไปซื้อสินค้า ผลที่เกิดขึ้นต่อผู้ที่ถูกสวมรอย ได้แก่ เสียประวัติทางด้านการเงิน เสียชื่อเสียง และอื่นๆ คำแนะนำก็คือ ให้ระมัดระวังไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น ระวังการให้ข้อมูลเกี่ยวกับบัตรเครดิต เปลี่ยนรหัสผ่านบ่อย ๆ

● ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต (Instant Messaging, Chat Rooms, File Sharing) ห้องสนทนาและการใช้ข้อความฉับพลันได้มีการใช้งานกันอย่างแพร่หลาย ถึงแม้ว่าการสนทนาในทั้งสองรูปแบบจะมีประโยชน์อย่างมากในการแลกเปลี่ยนความคิดเห็นหรือข้อมูลต่างๆ แต่ถ้าไม่ได้เตรียมการป้องกันไว้ให้ดีแล้ว ผลลบก็อาจจะเกิดขึ้นได้ เช่น การติดไวรัสหรือโทรจัน การเปิดเผยข้อมูลส่วนตัว การแชร์ไฟล์เป็นรูปแบบหนึ่งของการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต ก็อาจเปิดโอกาสทำให้ผู้บุกรุกเข้ามาเอาไฟล์ในเครื่องของผู้ใช้งานไปได้ คำแนะนำ ให้หลีกเลี่ยงการส่งข้อความฉับพลัน การสนทนาใน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต เพราะอาจก่อให้เกิดการละเมิดความเป็นส่วนตัวได้

● อีเมล์หลอกลวง (Instant Scams) ปัจจุบันได้มีอีเมล์หลอกลวงให้ผู้รับอีเมล์หลงเชื่อซึ่งหลาย ๆ ครั้งทำให้เกิดความเสียต่อผู้รับอีเมล์ เช่น การเสียเงิน เสียเวลา ปัจจุบันองค์กร Federal Trade Commission (FTC) ของสหรัฐอเมริกาได้ระบุ อีเมล์ไว้ ๑๒ ประเภท ที่ผู้ใช้ต้องให้ความระมัดระวัง

๑. การสร้างโอกาสทางธุรกิจ อีเมล์นี้จะเสนอรายได้ก้อนใหญ่โดยไม่ต้องทำอะไรมาก

๒. อีเมล์การขายสินค้าที่มีกลุ่มผู้ใช้งานเป็นจำนวนมาก (Bulk E-mail) อีเมล์นี้จะเสนอรายชื่อกลุ่มผู้ใช้งานอีเมล์ซึ่งมีจำนวนมากและชักชวนว่าสามารถโฆษณาหรือขายสินค้าไปยังกลุ่มผู้ใช้งาน อีเมล์นี้ได้

๓. อีเมล์ลูกโซ่ชักชวนให้ผู้รับส่งเงินจำนวนเล็กน้อยไปยังผู้ส่งและส่งอีเมล์นี้ไปยังผู้อื่นต่อไป

๔. การทำงานที่บ้านโดยลงแรงเล็กน้อย อีเมล์นี้จะเสนอรายได้อย่างสม่ำเสมอ แต่ต้องจ่ายค่าธรรมเนียมแรกเข้าและทำตามที่อีเมล์ขอให้ทำ แต่ผู้รับไม่มีทางได้รับค่าตอบแทนใดๆ ทั้งสิน กลับคืน

๕. การรักษาสุขภาพและการควบคุมน้ำหนัก อีเมล์นี้จะเสนอยาประเภทต่างๆ ถ้าหลงเชื่อคำโฆษณา ซื้อผลิตภัณฑ์มาใช้ส่วนใหญ่แล้วจะเป็นการเสียเงินไปโดยเปล่าประโยชน์

๖. รายได้ก้อนโตโดยไม่ต้องเสียแรงมากนัก อีเมล์นี้จะเสนอวิธีร่ำรวยได้อย่างรวดเร็ว

๗. สินค้าฟรี อีเมล์นี้จะเสนอให้สินค้าฟรีโดยชำระเงินเพียงเล็กน้อย เช่น เพื่อเข้าเป็นสมาชิก

๘. โอกาสการลงทุนที่มีผลตอบแทนสูง อีเมล์นี้จะเสนอผลตอบแทนที่สูงกับการลงทุนที่ไม่มีความเสี่ยง เงินที่ลงทุนไปก็จะสูญไปโดยเปล่าประโยชน์

๙. ชุดอุปกรณ์เชื่อมต่อเคเบิลทีวี อีเมล์นี้ จะขายชุดอุปกรณ์สำหรับเชื่อมต่อเข้ากับเคเบิ้ลได้โดยไม่ต้อง เสียค่าสมาชิก ถึงแม้ว่าจะทำได้จริงแต่เป็นสิ่งที่ผิดกฎหมาย

๑๐. การให้เงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่าย ๆ ซึ่งสถาบันการเงินที่ถูกต้องตามกฎหมายจะไม่ใช้วิธีการ ส่งอีเมล์แบบนี้

๑๑. การเคลียร์สินเชื่อ อีเมล์นี้จะเสนอช่วยเคลียร์ข้อมูลสินเชื่อที่ติดลบในบัญชีธนาคาร การทำตามที่ เสนอถือเป็นการกระทำที่ผิดกฎหมาย

๑๒. การเสนอให้รางวัลไปเที่ยวฟรี อีเมล์จะเสนอว่าท่านเป็นผู้ที่ได้รับรางวัลไปเที่ยวฟรี ภายหลังก็จะ พบว่า ข้อเสนอนั้นไม่เป็นอย่างที่คิด หรือไม่ก็ต้องชำระเงินเพิ่มเติม คำแนะนำ คือ ให้ระมัดระวังโฆษณาชวนเชื่อในลักษณะดังกล่าว และ หมั่นติดตามประเภทของ อีเมล์หลอกลวงในแหล่งข้อมูลเพิ่มเติม

- ประเด็นทางกฎหมาย (Legal Issues) กิจกรรมบนอินเทอร์เน็ตทั่วไปที่ถือว่าเป็นการกระทำที่ผิดกฎหมาย ได้แก่
  - o การเล่นการพนัน
  - o การซื้ออาวุธปืน
  - o การซื้อขายยาเสพติด
  - o การนำเสนอสื่อลามกทุกประเภท
  - o การบุกรุกคอมพิวเตอร์หรือเครือข่าย
  - o การพัฒนาและการแพร่ไวรัสคอมพิวเตอร์
  - o การทำให้เครือข่ายหรือเครื่องคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานหรือให้บริการได้
  - o การสวมรอยบุคคลเพื่อทำการฉ้อฉล คำแนะนำ คือ ไม่ควรเข้าไปยุ่งเกี่ยวกับกิจกรรมที่ผิดกฎหมาย และ ปฏิบัติตามกฎหมายของ ประเทศในเรื่องทั่วๆ ไปและที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต รวมทั้งกฎหมายในระดับนานาชาติ ด้วย
- การเฝ้าดูการใช้งานอินเทอร์เน็ต (Monitoring Internet Usage) คำแนะนำสำหรับการใช้งานอินเทอร์เน็ตภายในองค์กร
  - o ให้ความรู้กับพนักงานเกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างสม่ำเสมอ
  - o จัดทำนโยบายการใช้งานอินเทอร์เน็ตขององค์กรเป็นลายลักษณ์อักษร โดยมีเนื้อหา ดังนี้
    - การใช้งานอินเทอร์เน็ตมีจุดประสงค์เพื่อผลประโยชน์ขององค์กรไม่ใช่ใช้เพื่อผลประโยชน์ ส่วนตัว
    - การใช้งานอินเทอร์เน็ตจะได้รับการดูแลอย่างใกล้ชิดจากผู้ดูแลระบบ
    - มีแนวทางการใชอีเมล์อย่างเหมาะสม คำแนะนำสำหรับการใช้อินเทอร์เน็ตจากที่บ้าน

o พ่อแม่ต้องให้ความรู้เกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างเหมาะสม

o ใช้ซอฟต์แวร์ตรวจสอบการเข้าเว็บไซต์สำหรับบุตรหลาน รวมทั้งกรองการเข้าเว็บบางเว็บที่ไม่เหมาะสม

o ติดตั้ง ICT House Keeper ป้องกันเว็บที่ไม่เหมาะสมสำหรับเยาวชน

● การหมิ่นประมาทหรือการทำให้ผู้อื่นเสื่อมเสียชื่อเสียง (Online Defamation) ข้อความทุกรูปแบบที่ใช้งานบนอินเทอร์เน็ต ต้องระวังไม่ให้เป็นข้อความอันเป็ นเท็จหรือก่อให้เกิด ความเสียหายต่อตัวบุคคลหรือองค์กรที่ถูกพาดพิงกล่าวถึง หรือ อ้างอิง

● สแปม (Spam) สแปม คืออีเมล์ที่เป็ นขยะ ผู้รับสแปมอาจจะต้องใช้เวลาในการจัดการกับสแปมจำนวนมากในแต่ ละวัน และ สแปมยังกีดขวางการทำงานของเมล์เซิฟเวอร์ทั่วโลก ซึ่งทำให้ทุกคนประสบกับปัญหาการ เชื่อมต่อที่ช้าลงและเสียค่าใช้จ่ายในการเชื่อต่อที่สูงขึ้น ถึงแม้ว่าจะไม่สามารถจัดการกับสแปมได้อย่าง เด็ดขาด แต่ก็สามารถลดระดับความรุนแรงลงได้ ดังนี้

o ไม่ส่งอีเมล์เพื่อตอบกลับสแปมที่ส่งมา การตอบกลับสแปมนั้นเท่ากับเป็นการยืนยันอีเมล์แอดเดรสของผู้รับว่ามีอยู่จริงและจะทำให้ผู้รับตกเป็นเป้าหมายที่ชัดเจนยิ่งขึ้น

o ใช้อีเมล์แอดเดรสประจำเพื่อติดต่อกับผู้ที่ติดต่ออยู่ด้วยเป็นประจำ เช่น ผู้ร่วมงาน ครอบครัว สำหรับการส่งอีเมล์เพื่อจุดประสงค์อื่น ๆ ให้ใช้อีเมล์แอดเดรสต่างหาก

o ใช้ตัวกรองสแปม ให้เลือกชนิดที่เหมาะสมกับโปรแกรมอีเมล์ที่ใช้งานอยู่ให้มากที่สุด

● สปายแวร์ (Spyware) สปายแวร์คือซอฟต์แวร์ใดๆ ที่ใช้ช่องทางการเชื่อมต่อกับอินเทอร์เน็ตในเครื่องคอมพิวเตอร์ของ ผู้อื่นใช้เพื่อแอบส่งข้อมูลส่วนตัวของผู้ใช้นั้นไปให้กับบุคคลหรือองค์กรหนึ่งโดยที่ผู้ใช้เองก็ไม่ทราบ โดย สปายแวร์ สามารถเข้าสู่เครื่องคอมพิวเตอร์ที่ใช้งานได้โดยผ่านทางไวรัสคอมพิวเตอร์ เว็บที่เข้าไปดู หรือ อีเมล์ที่เปิดอ่าน คำแนะนำ คือ สามารถดาวน์โหลดโปรแกรมตรวจสอบสปายแวร์มาใช้งานเช่นโปรแกรม “Ad-aware” (www.lavasoft.de)

ปฏิบัติตัวอย่างไรให้ปลอดภัยจากการกระทำความผิด

๑. ไม่ตัดต่อและเผยแพร่ภาพตัดต่อของผู้อื่น ที่ทำให้เขาเสียหายหรือเสียชื่อเสียง

๒. ก่อนดาวน์โหลดโปรแกรมหรือข้อมูลจากเว็บไซต์ ควรอ่านเงื่อนไขให้ละเอียดเสียก่อน

๓. ไม่ส่งต่อ (forward) อีเมล์ หรือคลิปวิดีโอภาพลามกอนาจารหรือข้อความที่ไม่เหมาะสม

๔. ไม่เผยแพร่ spam mail หรือไวรัส

๕. ไม่เปิดเผยมาตรการระบบคอมพิวเตอร์ให้ผู้อื่นล่วงรู้

๖. ไม่ขโมยข้อมูลระบบคอมพิวเตอร์ของผู้อื่น

๗. ระวังการ chat กับคนแปลกหน้า อย่าหลงเชื่อเขาง่าย ๆ

๘. อย่าลืมลงโปรแกรมป้องกันไวรัสและสปายแวร์

๙. ไม่แฮกระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่น

๑๐. ไม่ควรบันทึกรหัสผ่าน (Password) ไว้ในคอมพิวเตอร์ และควรเปลี่ยนรหัสผ่าน (password) ทุก ๆ ๓ เดือน

๑๑. ไม่แอบดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น

๑๒. ไม่นำเข้าข้อมูลหรือภาพลามกอนาจารเข้าไปในระบบคอมพิวเตอร์

๑๓. อย่าแอบเข้าใช้งานระบบคอมพิวเตอร์ของผู้อื่นโดยที่เจ้าของไม่อนุญาต

๑๔. ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนตัวผู้กระทำผิด

อาชญากรรมคอมพิวเตอร์

ความหมายของอาชญากรรมทางคอมพิวเตอร์ มี ๒ ประการ ได้แก่

๑. การกระทำใดๆ ก็ตาม ที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และทำให้ผู้กระทำได้รับผลตอบแทน

๒. การกระทำผิดกฎหมายใดๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์ มาประกอบการกระทำผิด และต้องใช้ผู้มีความรู้ทางคอมพิวเตอร์ ในการสืบสวน ติดตาม รวบรวมหลักฐาน เพื่อการดำเนินคดีจับกุม อาชญากรคอมพิวเตอร์จะก่ออาชญากรรมหลายรูปแบบ ซึ่งปัจจุบันทั่วโลกจัดออกเป็น ๙ ประเภท (ตามข้อมูลคณะอนุกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมคอมพิวเตอร์)

๑. การขโมยข้อมูลทางอินเตอร์เน็ต ซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ

๒. อาชญากรนำเอาระบบการสื่อสารมาปกปิดความผิดของตนเอง

๓. การละเมิดสิทธิ์ปลอมแปลงรูปแบบ เลียนแบบระบบซอฟต์แวร์โดยมิชอบ

๔. ใช้คอมพิวเตอร์แพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม

๕. ใช้คอมพิวเตอร์ฟอกเงิน

๖. อันธพาลทางคอมพิวเตอร์ที่เข้าไปก่อกวน ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟ ระบบการจราจร

๗. หลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม

๘. แทรกแซงข้อมูลแล้วนำข้อมูลนั้นมาเป็นประโยชน์ต่อตนโดยมิชอบ เช่น ลักลอบค้นหารหัสบัตร เครดิตของผู้อื่นมาใช้ดักข้อมูลทางการค้าเพื่อเอาผลประโยชน์นั้นเป็นของตน

๙. ใช้คอมพิวเตอร์แอบโอนเงินบัญชีผู้อื่นเข้าบัญชีตัวเอง นอกจากนั้นในส่วนของอินเทอร์เน็ต ยังมีรูปแบบการกระทำผิดอีกมาก เช่นการแอบขโมย โดเมนเนม, แอบใช้ รับ-ส่ง อีเมล์, แอบใช้บัญชีอินเทอร์เน็ต (เวลาการใช้งาน), การส่ง อีเมล์จำนวนมหาศาล ฯลฯ รวมทั้งการกระทำผิดแบบดั้งเดิมที่ใช้เทคโนโลยีอินเทอร์เน็ต เป็นเครื่องมือ เช่น ภาพลามกอนาจาร การค้าประเวณี การพนัน ใส่ร้ายป้ายสี หมิ่นประมาท ฯลฯ

๕.๕ กรณีศึกษาทางกฎหมายเทคโนโลยีสารสนเทศ

๑: นายจ้างหรือผู้บังคับบัญชา เปิด e-mail ลูกจ้างหรือผู้ใต้บังคับบัญชาอ่านได้หรือไม่? ในการใช้งาน e-mail ภายในองค์กรนั้น จะมีคำถามว่า ถ้าองค์กรนั้นๆ มีการกำหนด User name และ Password ให้กับคนในองค์กร แล้วถ้านายจ้างหรือผู้บังคับบัญชารู้ User name และ Password ของ คนในองค์กรแล้ว นายจ้างหรือผู้บังคับบัญชามีสามารถเปิดอ่าน e-mail ของลูกจ้างได้หรือไม่ ถ้าในประเทศ สหรัฐอเมริกา มีกฎหมายกำหนดไว้อย่างชัดเจนว่า นายจ้างหรือผู้บังคับบัญชาขององค์กรนั้นๆ สามารถ เปิดดูและตรวจสอบ e-mail ของลูกจ้างได้รวมทั้งสามารถดูแฟ้มข้อมูลต่างๆ ในฮาร์ดดิสก์คอมพิวเตอร์ของ บริษัทได้ หากเป็น e-mail ที่เป็นขององค์กร เพราะเป็น e-mail สำหรับการปฏิบัติงาน แต่หากเป็น e-mail อื่นที่ไม่ใช่ขององค์กร นายจ้างหรือผู้บังคับบัญชาไม่ได้รับอนุญาตให้เปิดอ่าน หากนายจ้างหรือ ผ้บังคับบัญชาละเมิดสิทธิ์ลูกจ้างสามารถฟ้องร้องนายจ้างหรือผู้บังคับบัญชาให้ชดใช้ค่าเสียหายทางแพ่งได้

๒: การ Copy รูปภาพ/ข้อความบนเว็บไซต์ของผู้อื่นมาใช้เป็นการละเมิดลิขสิทธิ์ทุกกรณีหรือ เปล่า? หากต้องทำการ copy รูปภาพหรือข้อความบนเว็บไซต์ของผู้อื่นมาใช้งาน จำเป็นต้องขออนุญาต เจ้าของเสียก่อน เพราะหากนำมาใช้โดยไม่ได้รับอนุญาตจะถือว่า ละเมิดลิขสิทธิ์ผิดกฎหมาย หากนำไปใช้ เพื่อการค้าอาจถูกฟ้องเป็นคดีแพ่งหรือคดีอาญาได้ อย่างไรก็ตามก็มีข้อยกเว้นสำหรับกรณีเพื่อการศึกษา โดยต้องมีการอ้างอิงและขออนญาตเจ้าของลิขสิทธิ์

๓: การหมิ่นประมาททางอินเทอร์เน็ต สามารถฟ้องร้องเอาผิดได้หรือไม่? หากมีการหมิ่นประมาทบุคคลผ่านทางอินเทอร์เน็ต สามารถฟ้องร้องได้ทั้งคดีอาญา และคดีแพ่ง ซึ่งตามกฎหมาย การหมิ่นประมาททางแพ่งหมายถึง “การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืน ความจริง และการกล่าวหรือไขข่าวนั้นทำให้เกิดความเสียหายแก่ชื่อเสียงเกียรติคุณ ทางทำมาหากินได้ ขัดขวางทางเจริญของบุคคลอื่น ซึ่งแม้ว่าผู้ที่หมิ่นประมาทจะไม่รู้ว่าข้อความที่ตนกล่าวหรือไขข่าวนั้นไม่จริง แต่หากว่าควรจะรู้ได้ก็ต้องรับผิดในความเสียหายที่เกิดขึ้น” ส่วนใหญ่คดีหมิ่นประมาทจะฟ้องร้องกันเป็นคดีแพ่ง และเรียกค่าเสียหายกันมากๆ เพื่อให้จำเลยเข็ดหลาบ คดีแพ่งเรื่องหมิ่นประมาท ในประเทศไทยยังมี ประเด็นที่น่าสนใจคือ เรื่องศาลที่จะฟ้องคดี คือโจทก์สามารถฟ้องคดีได้ที่ศาลที่จำเลยมีภูมิลำเนาอยู่ในเขต หรือศาลที่เป็นที่เกิดของเหตุในการฟ้องคดี ทางปฏิบัติที่เกิดขึ้นการหมิ่นประมาทโดยการโฆษณา หนังสือพิมพ์นั้นเนื่องจาก หนังสือพิมพ์มีการส่งไปขายทั่วประเทศ ฝ่ายผู้เสียหาย ซึ่งมักเป็นนักการเมือง อาจถือว่าความผิดเกิดขึ้นทั่วประเทศ จึงทำการตระเวนไปฟ้องตามศาลต่าง ๆ ทั่วประเทศ ส่งผลให้จำเลย ต้องตามไปแก้คดี กรณีที่

๔: การทำ Hyperlink อย่างไรไม่ให้ละเมิดลิขสิทธิ์? การอ้างอิงเว็บไซต์ของผู้อื่น มาใส่ไว้ในเว็บของเรา มีโอกาสละเมิดลิขสิทธิ์ หากมีการมองว่า เป็น การทำข้างนอกนั้นมีลิขสิทธิ์ แต่ถ้าการเชื่อมโยงนั้นเป็นการเชื่อมโยงต่อไปยังหน้าแรกของเว็บผู้อื่นก็สามารถ ได้แต่ควรขออนญาตเจ้าของลิขสิทธิ์ให้เรียบร้อย หากเป็นการเชื่อมโยงลึกลงไปถึงเนื้อหาส่วนอื่นของเว็บ ผู้อื่นจะถือเป็นการละเมิดลิขสิทธิ์ได้ ในกรณีที่ไม่ต้องการให้ใครนำเว็บของเราไปเชื่อมโยงอาจจะระบุไว้ที่ เว็บเลยว่า ไม่อนุญาตจะทำให้ผู้ที่เข้ามาเชื่อมโยง หากยังมีการละเมิดสิทธิ์ก็จะมีความผิดโดยไม่ต้อง ตีความ

๕: โหลดโปรแกรมหรือเพลงทางอินเทอร์เน็ตผิดกฎหมายหรือเปล่า? การ Download โปรแกรมทางอินเทอร์เน็ตมาใช้งานแบบถูกต้องตามกฎหมายโดยไม่ละเมิด ลิขสิทธิ์ ก็ต่อเมื่อโปรแกรมที่ผู้ใช้ Download มาใช้นั้น ถูกระบุว่าเป็นประเภท Freeware, Shareware สำหรับการโหลดเพลงทางอินเทอร์เน็ตสามารถทำได้โดยไม่เป็นการละเมิดลิขสิทธิ์หากได้รับอนุญาต แต่ โดยทั่วไปแล้วค่ายเพลงมักจะไม่อนุญาต ยกเว้นจะทำเพื่อการค้า ส่วนการ Upload เพลงขึ้นบน อินเทอร์เน็ตให้คนทั่วไปโหลดได้ฟรีๆเป็นการละเมิดลิขสิทธิ์ถือเป็นคดีอาญา

๖: ซื้อโปรแกรมลิขสิทธิ์มา copy แจกเพื่อนได้หรือเปล่า? การทำสำเนาหรือการ copy โปรแกรมคอมพิวเตอร์นั้น ตามกฎหมายลิขสิทธิ์เขาเรียกว่า “ทำซ้ำ" ซึ่งถือเป็นการละเมิดลิขสิทธิ์ แม้กฎหมายเขาจะมีข้อยกเว้นให้การทำสำเนาโดยเจ้าของโปรแกรมมีลิขสิทธิ์ ทำได้โดยไม่ผิดกฎหมาย แต่กฎหมายเขาจำกัดจำนวนสำเนาว่า ให้มีจำนวนตามสมควรเพื่อวัตถุประสงค์ในการบำรุงรักษาหรือป้องกันการสูญหาย คือทำสำเนาได้เฉพาะ backup ถ้าจะมา copy แจกเพื่อนๆ ทั้ง office ก็ถือว่า มีความผิดในเรื่องการละเมิดลิขสิทธิ์

ตัวอย่างลักษณะความผิดที่พบได้บ่อยในปัจจุบันสำหรับการใช้งานอินเทอร์เน็ต

๑. การส่งเมล์ก่อกวนหรือโฆษณาขายสินค้าหรือขายบริการ ประเภทป๊อปอัพ หรือพวกส่งอีเมล์ขยะ ที่เขาไม่ต้องการมีโทษปรับอย่างเดียวไม่เกิน ๑๐๐,๐๐๐ บาท โทษฐานก่อความรำคาญ

๒. การส่งเมล์ ใส่ร้ายป้ายสีคนอื่น ข่าวลือที่ก่อให้เกิดความวุ่นวาย การส่งภาพลามกอนาจาร ทั้งหลายรวมถึงการได้รับแล้วส่งต่อด้วย มีโทษเสมอกันคือ จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท ดังนั้นจึงไม่ควรส่งต่อเมล์ที่ไม่เหมาะสม

๓. การตัดต่อภาพของคนอื่น แล้วนำเข้าเผยแพร่ทางอินเตอร์เน็ต ทำให้เจ้าของภาพเสียหาย อับ อาย ต้องโทษจำคุกไม่เกิน ๓ ปีปรับไม่เกิน ๖๐๐, ๐๐๐ บาท แต่กฎหมายยกเว้นสำหรับผู้ที่ทำด้วยความ สุจริต จะไม่เป็นความผิด

๔. การ ใช้ username/password ของผู้อื่น Log in เข้าสู่ระบบ มีความผิดตามมาตรา ๕ ปรับไม่ เกิน ๑๐,๐๐๐ บาท จำคุกไม่เกิน ๖ เดือน ดังนั ้น ไม่ควรใช้user/password ของผู้อื่นและไม่ควรให้ผู้อื่นล่วงรู้ password ของตนเอง

๕. การโพสต์ข้อความตามกระทู้ต่างๆที่มีเนื้อหาไม่เหมาะสม เป็นเท็จ กระทบความมั่นคง หรือ ลามกอนาจาร มีความผิดตามมาตรา ๑๔ ปรับไม่เกิน ๑๐๐,๐๐๐ บาท จำคุกไม่เกิน ๕ ปีดังนั้นจึงควรใช้ วิจารณญาณในการแสดงความคิดเห็น และคำนึงถึงผลที่จะตามมา

จริยธรรมกับเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศมีผลกระทบต่อสังคมเป็นอย่างมาก โดยเฉพาะประเด็นจริยธรรมที่เกี่ยวกับระบบสารสนเทศที่จำเป็นต้องพิจารณารวมทั้งเรื่องความปลอดภัยของระบบสารสนเทศการใช้เทคโนโลยีสารสนเทศหากไม่มีกรอบจริยธรรมกำกับไว้แล้ว สังคมย่อมจะเกิดปัญหาต่าง ๆ ตามมาไม่สิ้นสุด รวมทั้ง ปัญหาอาชญากรรมคอมพิวเตอร์ด้วย ดังนั้นหน่วยงานที่ใช้ระบบสารสนเทศจึงจำเป็นต้องสร้างระบบความ ปลอดภัยเพื่อป้องกันปัญหาดังกล่าว

๑ กรอบความคิดเรื่องจริยธรรม หลักปรัชญาเกี่ยวกับจริยธรรม มีดังนี้ (Laudon & Laudon, ๑๙๙๙) R.O. Mason และคณะ ได้จำแนก ประเด็นเกี่ยวกับจริยธรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็ น ๔ ประเภทคือ ความเป็นส่วนตัว (Privacy) ความถูกต้องแม่นยำ (Accuracy) ความเป็นเจ้าของ (Property) และความสามารถในการเข้าถึง ได้ (Accessibility) (O'Brien, ๑๙๙๙: ๖๗๕; Turban, et al., ๒๐๐๑: ๕๑๒)

๑) ประเด็นความเป็นส่วนตัว (Information Privacy) คือ การเก็บรวบรวม การเก็บรักษา และการ เผยแพร่ ข้อมูลสารสนเทศเกี่ยวกับปัจเจกบุคคล หรือองค์กร ซึ่งเจ้าของข้อมูลหรือสารสนเทศนั้นๆ มีสิทธิที่จะไม่เผยแพร่ข้อมูลต่อสาธารณะ

๒) ประเด็นความถูกต้อง (Information Accuracy) ข้อมูลหรือสารสนเทศที่ดีต้องสามารถตรวจสอบถึงแหล่งที่มาได้ รวมถึงมีการตรวจสอบความถูกต้องก่อนที่จะทำการเผยแพร่ข้อมูลนั้นๆ

๓) ประเด็นของความเป็นเจ้าของ (Intellectual Property) คือกรรมสิทธิ์และมลู ค่าของข้อมูลสารสนเทศ (ทรัพย์สินทางปัญญา)

๔) ประเด็นของการเข้าถึงข้อมูล (Data Accessibility) คือเนื่องจากการเข้าถึงข้อมูลทำได้อย่าง ง่าย ทำให้เกิดการกำหนดสิทธิในการเข้าถึงข้อมูลสารสนเทศเพื่อความปลอดภัยของข้อมูล และสามารถตรวจสอบได้ว่าใครเป็นผู้บันทึก แก้ไขข้อมูลนั้นๆ การคุ้มครองความเป็นส่วนตัว (Privacy)

- ความเป็นส่วนตัวของบุคคลต้องได้ดุลกับความต้องการของสังคม
- สิทธิของสาธารณชนอยู่เหนือสิทธิความเป็นส่วนตัวของปัจเจกชน การคุ้มครองทางทรัพย์สินทางปัญญา ทรัพย์สินทางปัญญาเป็นทรัพย์สินที่จับต้องไม่ได้ที่สร้างสรรค์ขึ้นโดยปัจเจกชน หรือนิติบุคคล ซึ่ง อยู่ภายใต้ความคุ้มครองของกฎหมายลิขสิทธิ์กฎหมายความลับทางการค้า และกฎหมายสิทธิบัตร ลิขสิทธิ์(copyright) ตามพระราชบัญญัติ ลิขสิทธิ์พ.ศ. ๒๕๓๗ หมายถึง สิทธิ์แต่ผู้เดียวที่จะกระทำ การใดๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ซึ่งเป็นสิทธิ์ในการป้องกันการคัดลอกหรือทำซ้ำ ในงานเขียน งานศิลป์ หรืองานด้านศิลปะอื่น ตามพระราชบัญญัติดังกล่าวลิขสิทธิ์ทั่วไปมีอายุห้าสิบปีนนับแต่งานที่ได้ สร้างสรรค์ขึ้น หรือนับแต่ได้มีการโฆษณาเป็นครั้งแรกในขณะที่ประเทศสหรัฐอเมริกาจะมีอายุเพียง ๒๘ ปี สิทธิบัตร (Patent) ตามพระราชบัญญัติสิทธิบัตร พ.ศ. ๒๕๒๒ หมายถึง หนังสือสำคัญที่ออกให้เพื่อ คุ้มครองการประดิษฐ์ หรือการออกแบบผลิตภัณฑ์ ตามที่กฎหมายบัญญัติไว้ โดยสิทธิบัตรการประดิษฐ์มี อายุยี่สิบปี นับแต่วันขอรับสิทธิบัตร ในขณะที่ประเทศสหรัฐอเมริกาจะคุ้มครองเพียง ๑๗ ปี

๒ ประโยชน์ของการมีจริยธรรม

๑. ประโยชน์ต่อตนเอง ภาคภูมิใจ เป็นที่รักใคร่ เป็นคนดี

๒. ประโยชน์ต่อสังคม สบสุข ปรองดอง สามัคคี

๓. ประโยชน์ต่อประเทศชาติ ความเจริญรุ่งเรือง สามัคคี ความพัฒนา

๔. ประโยชน์ต่อองค์กรธุรกิจ ยกระดับมาตรฐานขององค์กร

๕. ประโยชน์ต่อการดำรงรักษาไว้ซึ่งจริยธรรม เผยแพร่ รักษาจริยธรรมไปสู่รุ่นต่อไป

๓ จริยธรรมของนักคอมพิวเตอร์

๑. มีความรับผิดชอบต่อการขายสินค้าและบริการ

๒. ทำงานด้วยความศรัทธา และจริงใจ

๓. รักษาผลประโยชน์ของผู้บริโภค

๔. นำเสนอคุณภาพสินค้าตามความจริง

๕. ไม่เผยแพร่สิ่งที่ก่อให้เกิดผลเสียต่อสังคม

๖. ทำตามกฎหมาย ข้อบังคับ ระเบียบของสังคม

๗. ทำประโยชน์ต่อสังคม

เอกสารอ้างอิง

1. Under Graduate Ctber Traning (Phase 1) In troduction to cyber Operations E3OQR17D1
2. สถานการณ์ไซเบอร์ของรัฐรอบโลก : http://csc.dist.mod.go.th/PDF/%E0%B8%82%E0%B8%B2%E0%B8%A7%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%8A%E0%B8%B2%E0%B8%AA%E0%B8%A1%E0%B8%9E%E0%B8%99%E0%B8%98/n_cy_inter581.aspx
3. The Threat of Cyber Warfare: The Case of China and ASEAN : http://www.researchgate.net/publication/275583255_The_Threat_of_Cyber_Warfare_The_Case_of_China_and_ASEAN
4. กฎหมายทางด้านเทคโนโลยีสารสนเทศ : http://www.informatics.buu.ac.th/885101/chapters/chapter_13.pdf

การรักษาความปลอดภัยระบบสารสนเทศ

สารบัญ

หัวข้อเรื่อง **หน้า**

บทที่ ๑
ภัยคุกคามต่อความปลอดภัยของข้อมูล

<u>ประเภทของภัยคุกคามต่อความปลอดภัยของข้อมูล</u>

๑ ผู้บุกรุก (Hacker)

หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก ดังนั้น องค์กรส่วนใหญ่ที่ใช้อินเทอร์เน็ตจึงให้ความสำคัญกับมาตรการป้องกัน Hacker

๒ ไวรัสคอมพิวเตอร์ (Computer Virus)

เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยาก ไวรัสคอมพิวเตอร์มีหลายประเภทและก่อให้เกิดความเสียหายต่อระบบได้หลายรูปแบบ ตั้งแต่สร้างความรำคาญ มีข้อความแปลก ๆ ปรากฏขึ้นมาเรื่อย ๆ บนหน้าจอ หรือแม้กระทั่งทำลายไฟล์ข้อมูลต่าง ๆ ให้ได้รับความเสียหาย

- ไวรัสเลียนแบบ (Companion Virus) จะแอบแฝงตามไฟล์ต่าง ๆ และคอยสร้างไฟล์ขึ้นมาใหม่โดยเลียนแบบไฟล์ในระบบเดิม แล้วหลอกให้ระบบเรียกไฟล์ที่สร้างเลียนแบบขึ้นมาใช้งานแทนไฟล์จริง
- ไวรัสโปรแกรม (Program Virus) ถ้ามีการเรียกใช้ไฟล์ที่ติดไวรัสประเภทนี้ ก็จะทำให้ไวรัสแพร่เชื้อไปยังทุกไฟล์ที่สามารถติดต่อไปได้
- ไวรัสบู๊ต (Boot Virus) เป็นไวรัสที่คอยก่อกวนไฟล์สำคัญ ๆ ที่สำหรับเปิดเครื่องในตอนแรก ทำให้เราไม่สามารถบู๊ตเข้าสู่วินโดว์ได้
- ไวรัสหลบหลีก (Stealth Virus) จะหลบหลีกการตรวจจับจากโปรแกรมป้องกันไวรัส โดยจะขัดขวางการทำงานของโปรแกรมบางประเภทที่มีการป้องกันไวรัสด้วยการ copy ข้อมูลเดิมไว้ก่อน โดยไวรัสจะทำการแก้ไขชื่อไฟล์และไดเร็กทอรีที่ติดเชื้อ ทำให้โปรแกรมป้องกันไวรัสตรวจหาไฟล์ไม่เจอ
- ไวรัสหลอกลวง (Polymorphic Virus) จะแพร่กระจายเชื้อไปตามไฟล์ต่าง ๆ แล้วแสดงผลหลอกเหมือนว่ามีไวรัสหลายตัวในเครื่อง เพื่อให้โปรแกรมป้องกันไวรัสตรวจจับได้ยาก
- ไวรัสสองหน้า (Multipartite Virus) สามารถติดเชื้อได้ทั้งโปรแกรมและบู๊ตเซ็กเตอร์ได้พร้อม ๆ กัน ถือเป็นไวรัสที่มีความสามารถสูง
- ไวรัสมาโคร (Macro Virus) ทำการแพร่กระจายเชื้อเฉพาะไฟล์ที่เป็นเอกสารเท่านั้น เพื่อทำให้ข้อมูลที่เก็บไว้ในไฟล์เกิดความเสียหายหรือเปลี่ยนแปลงไป

๓. ความผิดพลาดของซอฟต์แวร์ (Bug)

ความผิดพลาดนั้นหมายถึง การทำงานในบางส่วนที่ไม่เป็นไปตามความต้องการหรือไม่ถูกต้อง

๔. อุบัติภัย (Disaster)

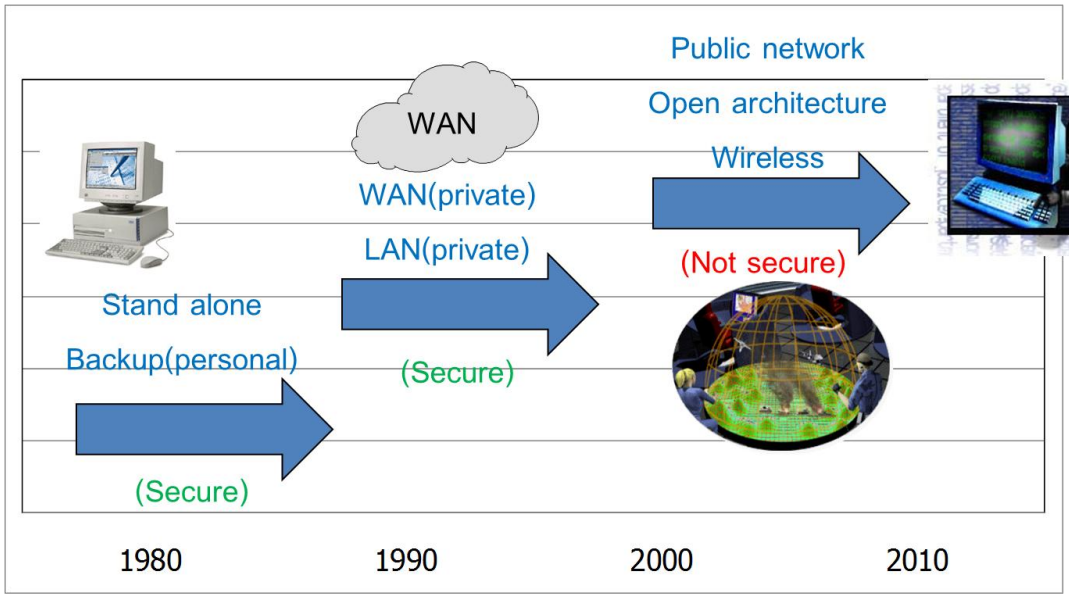
อุบัติภัยประเภทไฟไหม้ แหล่งจ่ายไฟล้มเหลว หรือภัยพิบัติอื่น ๆ ย่อมเกิดความเสียหายอย่างหลีกเลี่ยงไม่ได้ ดังนั้น จึงควรวางมาตรการป้องกันอุบัติภัยให้กับระบบคอมพิวเตอร์เป็นอย่างดี

๕. ความผิดพลาดในขั้นตอนการทำงานของระบบคอมพิวเตอร์

เนื่องจากระบบคอมพิวเตอร์มีโอกาสที่จะรับความเสียหายเข้ามาได้หลายทาง ตั้งแต่ส่วนการรับข้อมูลเข้ามาในระบบ เช่น การรับข้อมูลที่มีไวรัสคอมพิวเตอร์เข้ามา ส่วนของการทำงาน เช่น โปรแกรมทำงานในส่วนที่เกิด Bug พอดีหรือปัญหาจากฮาร์ดแวร์ ซึ่งความเสียหายของระบบเหล่านี้สามารถก่อความเสียหายให้กับองค์กรได้

บทที่ ๒
การรักษาความความปลอดภัยข้อมูลทางระบบคอมพิวเตอร์

การเชื่อมต่อในโลกยุคอินเทอร์เน็ต



Computer Network ความหมายคือ เครือข่ายคอมพิวเตอร์, ข่ายงานคอมพิวเตอร์ เป็นคำกล่าวโดยทั่ว ๆ ไปของการเชื่อมต่อสื่อสารกันระหว่างระบบคอมพิวเตอร์ ตั้งแต่ ๒ ระบบขึ้นไป หรือระหว่างเครื่องคอมพิวเตอร์กับเครื่องปลายทาง (Terminals) ทั้งหลาย เพื่อให้สามารถนำข้อมูล โปรแกรมรวมทั้งอุปกรณ์รอบข้างมาใช้งานร่วมกันได้ โดยมีอุปกรณ์ในระบบสื่อสารเป็นตัวเชื่อมโยง

ส่วนโซเชียลเน็ตเวิร์ค หรือ Social Network คือเครือข่ายสังคมออนไลน์ หรือการที่ผู้ใช้งานอินเตอร์เน็ตคนหนึ่งเชื่อมโยงกับเพื่อนอีกนับสิบ รวมไปถึงเพื่อนของเพื่อนอีกนับร้อย ผ่านผู้ให้บริการด้านโซเชียลเน็ตเวิร์ค (Social Network) บนอินเตอร์เน็ต เช่น Facebook, Blogger, Hi5, Twitter หรือ Tagged เป็นต้น การเชื่อมโยงดังกล่าว ทำให้เกิดเครือข่ายขึ้น เช่น เราสามารถรู้จักเพื่อนของเพื่อนเราได้ เป็นทอด ๆ ต่อไปเรื่อย ทำให้เกิดสังคมเสมือนจริงขึ้นมา สามารถสร้างคอนเน็คชั่นใหม่ ๆ ได้ง่าย และเมื่อเราแชร์ (Share) ข้อความหรืออะไรก็ตามลงไปในเครือข่าย ทุกคนในเครือข่ายก็สามารถรับรู้ได้พร้อมกัน และสามารถตอบสนองต่อสิ่งที่เราแชร์ได้ เช่น แสดงความคิดเห็น (Comment) กดไลค์ (Like) ซึ่งอาจจะแตกต่างกันออกไปตามแต่ละผู้ให้บริการ

ความโดดเด่นในเรื่องความง่ายของโซเชียลเน็ตเวิร์ค (Social Network) ทำให้ธุรกิจ และนักการตลาดสนใจที่จะใช้เป็นเครื่องมือในการประชาสัมพันธ์สินค้า และบริการ

ความหมายของสงครามไซเบอร์

สงครามไซเบอร์ (Cyber Warfare) คือ การใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำสงคราม สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด อาทิ

- การโจมตีเว็บ หรือบล็อคเว็บ
- การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต
- การเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้
- การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยำ
- การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก

ปัญหาการใช้ Thumb Drive

๑. นำมาซึ่งคอมพิวเตอร์ไวรัส - ในการนำ Thumb Drive เชื่อมต่อกับอุปกรณ์ ถ้าอุปกรณ์นั้น ๆ มีไวรัส ก็จะทำให้ Thumb Drive ที่ใช้งานติดไวรัสด้วย เมื่อนำThumb Drive ที่ติดไวรัสนั้นมาเชื่อมต่อกับระบบผู้ใช้งานเพื่อรับข้อมูลแล้ว ระบบก็จะติดไวรัสจาก Thumb Drive ตัวนั้นได้

๒. เป็นช่องทางรั่วไหลของข้อมูล - เมื่อนำ Thumb Drive มาใช้บันทึกข้อมูลทางราชการที่สำคัญแล้วThumb Drive นั้นได้สูญหายและตกไปอยู่ในมือของบุคคลภายนอกแล้วนั้น ข้อมูลทางราชการก็จะรั่วไหลไปสู่บุคคลภายนอก ซึ่งอาจส่งผลเสียภายหลัง

การรักษาความปลอดภัยข้อมูลเครือข่ายไร้สาย

หากมีการใช้เครือข่ายไร้สายทั้งในด้านยุทธการ และธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัส โดยต้องมีการขึ้นทะเบียนอุปกรณ์ (WiFi Access Point) เพื่อตรวจสอบและยืนยันความปลอดภัยจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อป้องกันการลักลอบใช้งานจากผู้ที่ไม่ได้รับอนุญาตทำให้ความลับทางราชการรั่วไหล

<u>วิธีการป้องกันภัยจากการการใช้งานระบบเครือข่ายไร้สาย</u>

หลักการในการใช้ระบบเครือข่ายไร้สายให้สะดวกและปลอดภัย

๑. ต้องมีการเข้ารหัสข้อมูล เช่น WEP, WPA, WPA version 2

๒. ต้องรีบเปลี่ยนรหัส (Default Password) ที่มากับอุปกรณ์ทั้งหมดให้เป็นของตนเองและต้องเก็บเป็นความลับ

๓. กำหนดระดับความแรงสัญญาณให้เหมาะสมกับพื้นที่ ๆ เปิดใช้งาน

๔. การแชร์ข้อมูลต้องมีการใช้รหัสผ่านเพื่อเข้าถึงข้อมูล

ระบบเข้ารหัส WEP กับ WPA

การเข้ารหัสข้อมูลมีอยู่ด้วยกันหลากหลายรูปแบบ เพื่อเพิ่มความปลอดภัยและความเหมาะสมในการใช้งาน โดยจะขออธิบายย่อ ๆ ดังนี้

๑. WEP คือ ใช้หลักการเข้ารหัสและถอดรหัสแบบ Symmetrical key มีความยาว ๖๔ หรือ ๑๒๘ บิต อย่างไรก็ตามกลไกการเข้ารหัสแบบ WEP นี้มีช่องโหว่อยู่มาก เพราะรหัสที่ใช้สามารถถูกถอดรหัสได้จากผู้ใช้งานโดยตรง นอกจากนี้ key ที่ใช้ในการเข้ารหัสก็ไม่มีการเปลี่ยนแปลงตลอดการใช้งาน

๒. WPA (Wi-Fi Protected Access) คือรูปแบบการเข้ารหัสที่มีความปลอดภัยสูงกว่าแบบ WEP เพราะใช้กลไกการเข้ารหัสและถอดรหัสแบบ TKIP (Temporal Key Integrity) ซึ่งเป็น key ชั่วคราวที่จะเปลี่ยนอยู่เรื่อย ๆ ร่วมกับ MIC (Message Integrity Code) เพื่อทำให้แน่ใจว่าข้อมูลที่อยู่ระหว่างการสื่อสารจะไม่ถูกปลอมแปลงจากผู้บุกรุก ทำให้ยากแก่การคาดเดาถอดรหัส

๓. WPA2 คือการรักษาความปลอดภัยระดับสูงสุดในปัจจุบันที่ถูกพัฒนาขึ้นโดยใช้กลไกการเข้ารหัสและถอดรหัสแบบ AES (Advanced Encryption Standard)

ระบบป้องกันมีหลายแบบดังที่กล่าวมาข้างต้น แต่ปัจจุบันแนะนำให้ใช้ WPA version 2 with AES (Advance Encryption Standard) ซึ่งเป็นระบบที่มีประสิทธิภาพมากที่สุด

นอกจากเทคนิคที่กล่าวมาข้างต้นนี้แล้ว ปัจจุบันยังมีวิธีการรักษาความปลอดภัยของระบบเครือข่ายไร้สายอีกหลายวิธีด้วยกัน ซึ่งจะต้องเลือกวิธีการให้เหมาะกับลักษณะและงบประมาณขององค์กรของตนเอง เพื่อให้เกิดประโยชน์และความคุ้มค่าสูงสุด

ข้อปฏิบัติและดำเนินการของผู้ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ

๑. ดำเนินการใด ๆ กับข้อมูลเฉพาะที่ได้รับอนุญาตแล้วเท่านั้น และต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

๒. ใช้ระบบสารสนเทศอย่างระมัดระวัง ถูกต้องตามกระบวนการรักษาความปลอดภัย และใช้ในกิจการงานที่ได้รับอนุญาต หรือได้รับมอบหมายเท่านั้น

๓. ตรวจสอบโปรแกรมประสงค์ร้ายก่อนนำมาใช้งานในระบบ

๔. ไม่นำโปรแกรมที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องกับภารกิจหน้าที่ ที่ได้รับมอบหมายเข้าสู่ระบบสารสนเทศ

๕. เก็บรักษาและใช้งานบัญชีผู้ใช้ (User Account) ซึ่งประกอบด้วยชื่อผู้ใช้ (user name) และรหัสผ่าน (Password) ให้เหมาะสม และเก็บรักษารหัสผ่าน (Password) ให้เป็นไปด้วยความปลอดภัย ไม่รั่วไหลถึงบุคคลอื่น

ข้อกำหนดขั้นต่ำของการกำหนดรหัสผ่าน (Password) ที่เหมาะสม

๑. มีความยาวอย่างน้อย ๘ ตัวอักษร

๒. ประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลขและอักขระพิเศษ

๓. จะต้องไม่มีข้อมูลเกี่ยวกับผู้ใช้ เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์จดจำรหัสผ่านแทนการเขียนบันทึก หากเจ้าของรหัสผ่านลืมรหัสผ่าน หรือต้องการแก้ไขให้เจ้าของรหัสผ่านแจ้งผู้ดูแลระบบ ให้ดำเนินการ

๔. ต้องเปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด หรือตามความเหมาะสม สำหรับระบบที่มีความสำคัญ

๕. ความรับผิดชอบในการใช้งาน Username และ Password เป็นของเจ้าของผู้ใช้งาน ต้องไม่โอนสิทธิหรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน ต้องไม่เปิดเผยรหัสผ่านให้แก่ผู้ใดทั้งสิ้น รวมถึงผู้ดูแลระบบสารสนเทศ

๖. สำหรับระบบสารสนเทศที่มีความสำคัญ ต้องไม่ใช้รหัสผ่านเดียวกันสำหรับเข้าถึงระบบทั่วไป

๗. ไม่ใช้รหัสผ่านร่วมกับผู้อื่นโดยเด็ดขาด แม้ว่าจะเป็นผู้ร่วมงานที่ต้องใช้แฟ้มข้อมูลเดียวกัน ทุกคนที่ได้รับอนุญาตจะต้องมีรหัสผ่านเป็นของตนเองในการเข้าใช้ข้อมูลดังกล่าว

สาเหตุที่ข้อมูลและสารสนเทศในระบบคอมพิวเตอร์ถูกคุกคามได้ง่าย

เหตุผลที่ข้อมูลและสารสนเทศในระบบคอมพิวเตอร์ถูกคุกคามจากภัยรูปแบบต่าง ๆ ได้ง่ายกว่าระบบข้อมูลในยุคเก่ามีหลายประการด้วยกัน

- ข้อมูลและสารสนเทศในระบบคอมพิวเตอร์มีความซับซ้อน
- กระบวนการทำงานของระบบคอมพิวเตอร์มองไม่เห็น
- ความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ขยายผลในวงกว้างกว่า
- ระบบข้อมูลคอมพิวเตอร์สามารถเข้าถึงได้จากบุคคลหลายฝ่าย
- ความก้าวหน้าของเทคโนโลยีสื่อสาร และซอฟต์แวร์เป็นผลให้การบุกรุกทำได้ง่ายขึ้น

บทที่ ๓
การรักษาความปลอดภัยของข้อมูล

เมื่อมีการนำคอมพิวเตอร์และระบบข้อมูลสารสนเทศเข้ามาใช้ การเก็บรวบรวมข้อมูลสารสนเทศขององค์กรก็เปลี่ยนรูปแบบไป ข้อมูลและสารสนเทศจะถูกเก็บเป็นไฟล์ และมีการจัดทำระบบข้อมูลส่วนกลางขององค์กร เพื่อให้การนำข้อมูลไปใช้งานง่าย และสะดวกมากขึ้น

เมื่อระบบเสียหายหรือไม่สามารถทำงานได้ตามปกติ เวลาและค่าใช้จ่ายที่ต้องใช้ในการแก้ปัญหาก็สูงตามไปด้วย นอกจากนี้เมื่อทุกคนทั้งในและนอกองค์กรสามารถเข้าถึงระบบข้อมูลได้ โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ เป็นเหตุให้ระบบข้อมูลถูกบุกรุกจากผู้ไม่ประสงค์ดีได้ง่าย นอกจากนี้ระบบคอมพิวเตอร์ยังต้องเผชิญกับภัยคุกคาม (Threat) ต่าง ๆ ได้ง่ายกว่าข้อมูลในรูปแบบเอกสารอีกด้วย

มาตรการในการรักษาความปลอดภัยของข้อมูล

ในยุคปัจจุบัน ข้อมูลข่าวสารไม่ได้อยู่เพียงในกระดาษหรือสื่อสิ่งพิมพ์แต่ยังมีการบันทึกไว้ในรูปแบบอื่นๆ ภายในระบบคอมพิวเตอร์ ซึ่งจะต้องมีวิธีการหรือมาตรการในการรักษาความปลอดภัยเช่นเดียวกัน มาตรการในการรักษาความปลอดภัยสามารถแบ่งออกเป็น ๓ มาตรการใหญ่ คือ

๑. มาตรการรักษาความปลอดภัยทางกายภาพ (Physical Security) เป็นมาตรการรักษาความปลอดภัยทั่วไปให้กับบุคคล สถานที่ และอุปกรณ์ ตลอดจนสื่อต่าง ๆ ที่บันทึกข้อมูลข่าวสาร เพื่อป้องกันไม่ให้ผู้บุกรุกเข้าถึงแหล่งข้อมูลได้ทางกายภาพ เช่น การสร้างรั้ว การเฝ้ายาม และการดำเนินงานด้านเอกสาร เป็นต้น ทั้งนี้รวมถึงการป้องกันการแพร่กระจายของคลื่นแม่เหล็กไฟฟ้าไม่ให้เล็ดลอดไปในสถานที่ที่ไม่เหมาะสม

๒. มาตรการรักษาความปลอดภัยทางระบบคอมพิวเตอร์ (Computing Security) เป็นมาตรการรักษาความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยตรง เน้นในการเข้าถึงและการใช้งานข้อมูลที่อยู่ในระบบสารสนเทศ ซึ่งจะต้องดำรงไว้ใน ๓ ลักษณะ คือ การรักษาความลับ (Confidential), การคงสภาพ (Integrity) และความพร้อมในการใช้งาน (Availability)

๒.๑ การรักษาความลับ (Confidential) เป็นการดำเนินการเพื่อให้สาระของข้อมูลข่าวสารได้ถูกเปิดเผยต่อบุคคล หรือ process ที่ได้รับอนุญาตเท่านั้น มาตรการนี้จะทำได้โดยวิธีการเข้ารหัส (Cryptography)

๒.๒ การคงสภาพ (Integrity) เป็นการยืนยันว่าข้อมูลที่ต้องการรักษาไม่ถูกเปลี่ยนแปลงไปจากของเดิมโดยผู้ที่ไม่ได้รับอนุญาต เนื่องจากในบางกรณีผู้บุกรุกไม่มีความประสงค์ที่จะรู้สาระของข้อมูลข่าวสาร แต่ต้องการทำให้ข่าวสารนั้นผิดไปจากสาระเดิม ซึ่งจะใช้การ Error Correction Code หรือ Integrity Check Sum เป็นต้น

๒.๓ ความพร้อมในการใช้งาน (Availability) เป็นการรักษาความพร้อมในการใช้งานของข้อมูลเช่น ข้อมูลบัญชีเงินฝากของลูกค้าธนาคาร หรือข้อมูลสำคัญต่าง ๆ ที่ต้องพร้อมใช้งานในเวลาที่ต้องการ ซึ่งในบางครั้งเป็นข้อมูลที่สามารถเปิดเผยให้สาธารณชนรับทราบได้ เพื่อประโยชน์ในการประชาสัมพันธ์ หรือการเผยแพร่ในวงกว้าง เช่น ข้อมูลการท่องเที่ยว การแบ่งปันข้อมูล หรือ การติดต่อแบบ Social Network เป็นต้น โดยใช้วิธีการ Back Up ต่าง ๆ หรือการทำ Redundant Array of Independent Disk: RIAD รวมทั้งการเตรียมที่ตั้งสำรองในยามฉุกเฉิน

๓. มาตรการรักษาความปลอดภัยทางระเบียบกฎเกณฑ์ (Rule and Regulations) ในโลกแห่งความเป็นจริงแล้ว ไม่มีอุปกรณ์ หรือสิ่งกีดขวางใด ๆ จะสามารถรักษาความปลอดภัยของข้อมูลข่าวสารได้สมบูรณ์ หากไม่ได้ควบคุมการใช้งานของมนุษย์ การละเมิดในระบบรักษาความปลอดภัยนั้นส่วนมากจะมีคนในองค์กรมีส่วนเกี่ยวข้องโดยเสมอ ดังนั้นจึงขาดไม่ได้ที่จะต้องมีมาตรการทางด้านระเบียบกฎเกณฑ์มารองรับหรือควบคุมการใช้งาน(Authentication) ของบุคลากรภายในองค์กร ตลอดไปถึงการออกกฎหมาย (Law) ด้านการรักษาความปลอดภัยของประเทศ เพื่อป้องกันอาชญากรรมคอมพิวเตอร์ที่จะเกิดขึ้นในสังคมปัจจุบัน อีกทั้งต้องกำหนดให้มีการบันทึกการใช้งาน (Log) ของระบบสารสนเทศ เพื่อใช้ในการตรวจสอบ (Audit) และหาผู้ละเมิดมาลงโทษ

การรักษาความปลอดภัยฐานข้อมูล (Database Security)

การรักษาความปลอดภัยฐานข้อมูล มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึงการเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

๑. ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย และหากเป็นข้อมูลที่มีชั้นความลับ ต้องมีการเข้ารหัสในการจัดเก็บที่เหมาะสม โดยใช้รูปแบบการเข้ารหัสตามมาตรฐานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศกำหนด

๒. ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ และจัดให้มีแฟ้มลงบันทึกเข้าออกและการใช้งาน (Audit Log) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

๓. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

๔. ต้องมีการจัดทำแผนสำรองและกู้ข้อมูลที่เหมาะสม และหากเป็นข้อมูลเกี่ยวกับงานด้านยุทธการต้องมีการสำรองข้อมูลอย่างน้อย ๒ ชุด โดยเก็บไว้ในพื้นที่ปฏิบัติงาน ๑ ชุดและเก็บไว้ห่างจากจุดที่มีการติดตั้งใช้อีก ๑ ชุด สำหรับระบบอื่น ๆ ให้กำหนดตามความเหมาะสม

บทที่ ๔
กลยุทธ์และการควบคุมรักษาความปลอดภัย

กลยุทธ์การรักษาความปลอดภัย

๑. ค้นหาภัยคุกคาม

เพื่อหาคำตอบออกมาให้ได้ก่อน ว่าภัยที่สามารถคุกคามความปลอดภัยข้อมูลขององค์กรนั้นมีทางไหนบ้าง เพื่อให้มองเห็นถึงภัยคุกคามที่จะเกิดขึ้นกับองค์กรได้รอบด้าน

๒. อธิบายถึงความเสี่ยงต่อภัยคุกคาม

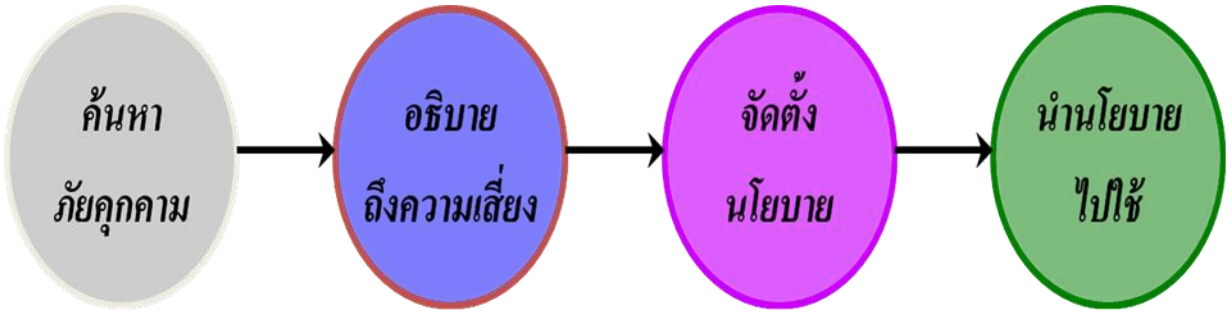
มาพิจารณากันต่อว่าภัยคุกคามที่อาจจะเกิดขึ้นนั้นก่อให้เกิดผลเสียอย่างไร ร้ายแรงแค่ไหน และมีผลต่อส่วนใดขององค์กรบ้าง รวมถึงหนทางที่ภัยคุกคามเหล่านั้นจะเข้ามายังองค์กรเพื่อหาวิธีป้องกัน

๓. จัดตั้งนโยบายการรักษาความปลอดภัย

หน่วยงานรักษาความปลอดภัยข้อมูลขององค์กรจะต้องนำข้อมูลซึ่งได้จากขั้นตอนที่ผ่าน ๆ มารวบรวม วิเคราะห์ หาทางป้องกันและตั้งนโยบายที่จะใช้เพื่อรักษาความปลอดภัยของข้อมูลจากภัยคุกคามเหล่านั้น

๔. นำนโยบายไปใช้

การนำนโยบายรักษาความปลอดภัยมาใช้พร้อมกับพยายามวัดประสิทธิภาพของนโยบายที่นำมาปฏิบัติอยู่เสมอ เพื่อปรับปรุงแก้ไขให้ทันต่อรูปแบบภัยคุกคามที่เปลี่ยนแปลงไปเสมอ



การควบคุมความปลอดภัยของข้อมูล

การควบคุมความปลอดภัยของข้อมูล ต้องมีมาตรการหรือการควบคุมความปลอดภัยที่มีประสิทธิภาพ ประกอบด้วย นโยบาย วิธีปฏิบัติ และกระบวนการขององค์กร ในการรักษาข้อมูลให้มีความถูกต้องและน่าเชื่อถือ

ปัจจุบันภัยคุกคามมาจากหลายทาง และยังส่งผลต่อระบบคอมพิวเตอร์ร้ายแรงขึ้น การควบคุมความปลอดภัยจึงถูกนำมาพิจารณาตั้งแต่ช่วงแรกของการพัฒนาระบบการควบคุมความปลอดภัยของระบบคอมพิวเตอร์แบ่งออกเป็น ๒ ประเภท คือ

๑. ควบคุมทั่วไป (General control) เป็นการควบคุมความปลอดภัยของข้อมูลในทุกฝ่ายที่มีการใช้คอมพิวเตอร์ หรือพูดง่าย ๆ ก็คือ มาตรการร่วมที่ใช้กันทั้งองค์กร

- ควบคุมความปลอดภัยของข้อมูลตั้งแต่กระบวนการพัฒนาระบบ (Implementation control)
- ควบคุมความปลอดภัยของซอฟต์แวร์ (Software Control)
- ควบคุมความปลอดภัยของฮาร์ดแวร์ (Hardware Control)
- ควบคุมความปลอดภัยของระบบคอมพิวเตอร์ (Computer Operation Control)
- ควบคุมความปลอดภัยของข้อมูล (Data Security Control)
- ควบคุมมาตรฐาน (Administrative Control)

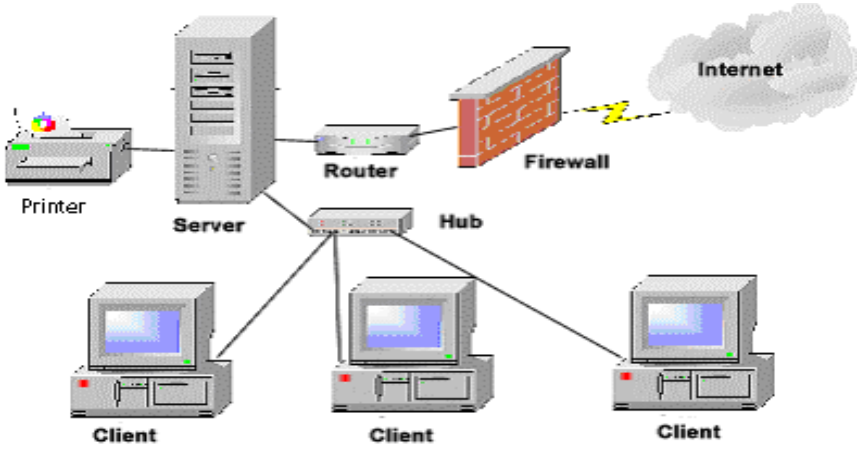
๒. ควบคุมเฉพาะโปรแกรม (Application Control) เป็นการควบคุมเฉพาะแต่ละโปรแกรม เช่น ระบบบัญชี ระบบการจ่ายเงิน หรือระบบการสั่งซื้อ เป็นต้น ดังนั้นมาตรการที่ใช้จึงแตกต่างกันไปตามแต่ละแผนก

- ควบคุมอินพุต (Input Control)
- ควบคุมกระบวนการ (Process Control)
- ควบคุมเอาต์พุต (Output Control)

การควบคุมความปลอดภัยบนอินเทอร์เน็ต

เนื่องมาจากความเสียหายที่เกิดขึ้นจากการคุกคามทางอินเทอร์เน็ตแพร่กระจายได้อย่างรวดเร็ว มาตรการที่นำมาใช้ในการป้องกันภัยคุกคามทางอินเทอร์เน็ตก็คือ Firewall โดย Firewall เป็นตัวกลางระหว่างเครือข่ายภายในองค์กร (LAN) กับเครือข่ายนอกองค์กรอย่าง WAN หรืออินเทอร์เน็ต

หน้าที่ Firewall ก็คือ ป้องกันการสื่อสารทั้งจากภายนอกที่จะเข้ามายังเครือข่ายภายใน และจากเครือข่ายภายในที่จะออกสู่อินเทอร์เน็ต โดย Firewall จะตรวจสอบข้อมูลที่จะเข้ามา เช่น ชื่อ หมายเลขไอพี (IP Address) และลักษณะเฉพาะอื่น ๆ ให้ถูกต้องหรือปลอดภัยตามมาตรฐานที่ผู้ดูแลเครือข่าย (Network Administrator) กำหนดไว้ จึงจะได้รับอนุญาตให้สื่อสารถึงกันได้



Firewall การป้องกันภัยคุกคามทางอินเทอร์เน็ต

การนำการรักษาความปลอดภัยข้อมูลข่าวสารไปใช้งาน (Information Security Implementation)

การพิจารณานำการรักษาความปลอดภัยข้อมูลข่าวสารของระบบสารสนเทศไปใช้งานนั้น จะต้องทำอย่างรอบคอบเนื่องจากเป็นสิ่งที่ใช้ทรัพยากรค่อนข้างสูงในหลาย ๆ ด้าน ทั้งอุปกรณ์ บุคคล และงบประมาณ ซึ่งในบางครั้งสามารถแทนที่ด้วยมาตรการอื่น ๆ เช่น การรักษาความปลอดภัยสถานที่ หรือการใช้กฎระเบียบ เป็นต้น ในการพิจารณานั้นสามารถแบ่งเป็นขั้นตอนพื้นฐานได้ ดังนี้

๑. การสำรวจการทำงานและนโยบายขององค์กร (Security Policy) ในเรื่องการรักษาความปลอดภัยของข้อมูลข่าวสารนั้นเป็นเรื่องของนโยบายขององค์กร ซึ่งผู้บริหารจะต้องเป็นผู้ริเริ่ม และกำกับดูแล ดังนั้นในขั้นตอนแรกจะต้องทราบถึงนโยบายขององค์กร และสำรวจทำความเข้าใจระบบการทำงาน หรือการบริหารข้อมูลภายในองค์กร และการแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น ๆ ที่ทำธุรกิจร่วมกัน ตลอดจนการปฏิสัมพันธ์กับลูกค้า เพื่อให้ได้ความต้องการที่แท้จริงในด้านการรักษาความปลอดภัยของข้อมูล การแบ่งกลุ่มระดับความสำคัญข้อมูล การแบ่งกลุ่มผู้ใช้งานข้อมูล และกำหนดลักษณะการใช้งานข้อมูล เช่น การเน้นในด้านการรักษาความลับ (Confidential Base), การเน้นในด้านการรักษาสภาพข้อข้อมูล (Integrity Base) หรือการแยกข้อมูลตามผลประโยชน์ (Conflict of Interest) เป็นต้น

๒. การเลือกใช้แบบจำลองของการรักษาความปลอดภัย (Security Model) เมื่อสามารถกำหนดลักษณะการใช้งานของข้อมูลได้แล้ว ขั้นตอนต่อไปจะเป็นการสร้างแบบจำลองของการรักษาความปลอดภัย เนื่องจากการใช้งานข้อมูลบนระบบสารสนเทศเป็นการทำงานโดยอัตโนมัติระหว่าง Processor หลายตัว จำเป็นต้องมีกฎเกณฑ์ (Criteria) ที่แน่นอนชัดเจน โดยเฉพาะในเรื่องสิทธิในการเข้าถึง (Access) และการใช้งาน (Manipulate) ข้อมูลของกลุ่มผู้ใช้งานที่ได้รับอำนาจ (Authority) หรือระดับของชั้นความลับ (Security Level) ในการเข้าถึงข้อมูลที่ต่างกัน ตัวแบบจำลองนี้เองจะเป็นการกำหนดว่า Process หรือผู้ใช้ใดสามารถเข้าถึง (Access) ใช้งานข้อมูลในลักษณะใด เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความปลอดภัยตามขั้นตอนที่ ๑ เช่น Bell-LaPadula Model “No Read Up & No Write Down”, Biba Model or Biba Integrity Model “No Write Up & No Read Down” หรือ Brewer and Nash model “Chinese Wall Model or Firewall” เป็นต้น

๓. การศึกษาและประเมินค่าผลิตภัณฑ์ในตลาด (Security Product Study and Evaluation) หลังจากที่สามารถกำหนดแบบจำลองของการรักษาความปลอดภัยของข้อมูลได้แล้ว จะต้องทำการหาผลิตภัณฑ์ที่สามารถตอบสนองความต้องการให้สามารถทำงานได้อย่างเหมาะสม ซึ่งต้องคำนึงถึงความเป็นมาตรฐาน (Standard) และความไม่เป็นมาตรฐาน (Non-standard) ประกอบกัน โดยแต่ละประเภทจะมีข้อดีและข้อเสียที่ต่างกัน และนำมาประเมินค่าการใช้งานในระบบว่าครบถ้วนหรือไม่ ในบางครั้งการรักษาความปลอดภัยของข้อมูลในระบบหนึ่งอาจต้องให้วิธีการมากกว่าหนึ่งวิธี และผลิตภัณฑ์มากกว่าหนึ่งผลิตภัณฑ์ ดังนั้นในการศึกษาและเลือกใช้ต้องคำนึงถึงการบูรณาการสิ่งต่าง ๆ เหล่านี้ด้วย สิ่งที่ได้อีกประการหนึ่งในขั้นตอนนี้คือประมาณการค่าใช้จ่ายที่จะใช้ในการรักษาความปลอดภัยของระบบ

๔. การประเมินความเสี่ยง และการบริหารความเสี่ยง (Risk Assessment and Management) เป็นที่แน่นอนว่าในโลกธุรกิจ ต้องพยายามเพิ่มกำไร โดยการลดต้นทุน และเพิ่มมูลค่าสินค้า สำหรับการรักษาความปลอดภัยแล้วไม่ว่าจะทำด้วยมาตรการใด ๆ ก็ตามเป็นการเพิ่มต้นทุนทั้งสิ้น ดังนั้นผู้บริหารที่ดีจะต้องประเมินความเสี่ยง หรือมูลค่าความเสียหาย หากไม่มีป้องกันเป็นวงเงินเท่าไร และมีโอกาสเป็นไปได้มากน้อยเพียงไร และนำมาเปรียบเทียบกับค่าใช้จ่ายในการป้องกันว่าเหมาะสมกันหรือไม่ ทั้งนี้องค์กรจะต้องบริหารความเสี่ยงให้อยู่ในระดับที่เหมาะสมกับค่าใช้จ่ายที่ลงทุนไป

๕. การนำไปใช้ (Security Implementation) เมื่อได้ข้อสรุปในการประเมินและบริหารความเสี่ยงแล้วจะเป็นขั้นตอนในการนำระบบรักษาความปลอดภัยไปใช้งาน ซึ่งสามารถทำได้ใน ๒ ลักษณะ คือ แบบใช้หน่วยงานภายใน และ แบบใช้หน่วยงานภายนอก โดยมีการกำกับดูแลโดยผู้บริหารระดับสูงขององค์กร

๖. การตรวจสอบและประเมินค่าความปลอดภัยขององค์กร (Security Inspection and Audit) เป็นขั้นตอนที่สำคัญมากในการนำระบบการรักษาความปลอดภัยข้อมูลข่าวสารไปใช้งาน เป็นการตรวจสอบหาจุดอ่อน หรือช่องทางในการละเมิด โดยจะเน้นในการกำกับดูแลการทำงานของบุคลากรให้เป็นไปตามระเบียบหรือกฎเกณฑ์ที่กำหนดไว้ โดยคณะผู้ตรวจสอบต้องรายงานผลการทำงานให้ผู้บริหารสูงสุดทราบโดยตรง

ระเบียบกองทัพอากาศ

ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

พ.ศ. ๒๕๕๒

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. ๒๕๕๒”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ การดำเนินการรักษาความปลอดภัยตามระเบียบนี้ให้ยึดถือและปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕ ระเบียบกระทรวงกลาโหมว่าด้วยการรักษาความปลอดภัยหน่วยกรรมวิธีข้อมูลอัตโนมัติ พ.ศ.๒๕๒๘ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ เป็นมูลฐาน

ข้อ ๔ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. ๒๕๔๓

บรรดาระเบียบ และคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัด หรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

สำหรับมาตรการรักษาความปลอดภัยอื่นใดที่มิได้กล่าวไว้ในระเบียบนี้ ให้ยึดถือตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

ข้อ ๕ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานราชการ และลูกจ้างของกองทัพอากาศ ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ

ข้อ ๖...

ข้อ ๖ ในระเบียบนี้

๖.๑. “ระบบสารสนเทศ” (Information System) หมายความว่า ระบบที่ประกอบด้วย คน ระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร ข้อมูล และกระบวนการ (Process) โดยกระบวนการนั้นได้แก่ วิธีการในการเก็บข้อมูล ประมวลผลข้อมูลเพื่อที่จะเปลี่ยนข้อมูลให้เป็นสารสนเทศ และเผยแพร่ข้อมูลให้อยู่ในลักษณะของสารสนเทศของผู้ใช้ต้องการ

๖.๒ “คอมพิวเตอร์” (Computer) หมายความว่า เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถในการคำนวณอัตโนมัติตามคำสั่ง ส่วนที่ใช้ประมวลผลเรียกว่าหน่วยประมวลผล ชุดของคำสั่งที่ระบุขั้นตอนการคำนวณเรียกว่าโปรแกรมคอมพิวเตอร์ ผลลัพธ์ที่ได้ออกมานั้นอาจเป็นได้ทั้ง ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่น ๆ โดยอาจมีลักษณะเป็น คอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์เคลื่อนที่ โทรศัพท์แบบฉลาด (Smart Phone) ตลอดจน ระบบคอมพิวเตอร์ฝังตัว (Embedded Computer) เป็นต้น

๖.๓ “ภัย” (Threat) หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยคน (Person) สิ่งต่าง ๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ ตามความต้องการของภัย นั้น

๖.๔ “ความอ่อนแอ” (Vulnerability) หมายความว่า จุดอ่อน หรือข้อบกพร่องใด ๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกัน สามารถนำไปใช้ประโยชน์ เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้น ๆ ได้

๖.๕ “ความเสี่ยง” (Risk) หมายความว่า โอกาสของการเกิดภัยในรูปแบบที่เหมาะกับความอ่อนแอ ที่มีอยู่ของระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากัน ในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศ แต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด

๖.๖ “ประเมินความเสี่ยง” (Risk Assessment) หมายความว่า กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

๖.๗ “ระบบสื่อสารข้อมูล” (Data Communication System) หมายความว่า ระบบที่ประกอบด้วยผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล เช่น ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น ทั้งระบบวงจรมีสายและไร้สาย

๖.๘ “ระบบ...

๖.๘ “ระบบคอมพิวเตอร์” (Computer System) หมายความว่า ระบบที่ประกอบด้วยส่วนเครื่อง (Hardware) ส่วนชุดคำสั่ง (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware) ที่ใช้ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ

๖.๙ “สารสนเทศ” (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๖.๑๐ “พื้นที่ใช้งานระบบสารสนเทศ” (Information System Workspaces) หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือเตรียมข้อมูลเก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้ง เครื่องคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งประจำโต๊ะทำงาน

๖.๑๑ “เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสาร หรือการส่งข้อมูลกันระหว่างระบบสารสนเทศของกองทัพอากาศ ทั้งระบบสารสนเทศเพื่อการสนับสนุน (Support Information System: SIS) และระบบสารสนเทศเพื่อการยุทธ (Combat Information System: CIS) ตัวอย่างเช่น ระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link: TDL) ระบบป้องกันทางอากาศอัตโนมัติ (Royal Thai Air Defense System: RTADS) ระบบบัญชาการและควบคุมทางอากาศ (Air Command and Control System : ACCS) ระบบสารสนเทศเพื่อการบริหาร (Management Information System: MIS) ของส่วนราชการต่าง ๆ ระบบสารสนเทศสำหรับผู้บังคับบัญชาระดับสูง (Executive Information System: EIS) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๖.๑๒ “สารสนเทศที่กำหนดชั้นความลับ” หมายความว่า สารสนเทศในรูปข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึงหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึก ประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่ หรือเตรียมจะใช้ ตลอดจนวัสดุ หรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

๖.๑๓ “การรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า การดำเนินการเพื่อให้ระบบสารสนเทศมีคุณสมบัติดังนี้ มีการรักษาความลับของข้อมูล (Confidentiality) ให้เข้าถึงได้สำหรับผู้ที่มีสิทธิเท่านั้น มีการคงสภาพความถูกต้อง และความน่าเชื่อถือของข้อมูล (Integrity) โดยไม่มีการเปลี่ยนแปลงจากผู้ไม่มีสิทธิ และการเปลี่ยนแปลงที่ผิดพลาดจากผู้มีสิทธิ มีสภาพพร้อมใช้งาน (Availability) สามารถให้บริการต่อเนื่องอย่างมีเสถียรภาพ และเมื่อเกิดปัญหาสามารถกู้กลับคืนมาได้

๖.๑๔ “คณะ...

๖.๑๔ “คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า คณะกรรมการที่ได้รับการแต่งตั้งจากผู้บังคับบัญชา เพื่อช่วยในการบริหารและจัดดำเนินการงานด้านการรักษาความปลอดภัยระบบสารสนเทศของหน่วยงาน หรือของระบบตามสายงาน

๖.๑๕ “นายทหารรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า นายทหารสัญญาบัตรที่ได้รับการคัดเลือกและแต่งตั้ง ให้เป็นนายทหารรักษาความปลอดภัยระบบสารสนเทศ

๖.๑๖ “ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ” หมายความว่า ผู้ที่เกี่ยวข้องกับการจัดการระบบสารสนเทศในด้านต่าง ๆ เช่น ผู้บริหารระบบ (System Administrator) ผู้บริหารฐานข้อมูล (Database Administrator) ผู้บริหารเครือข่าย (Network Administrator) ผู้เขียนโปรแกรม (Programmer)

ข้อ ๗ ให้เจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ รักษาการให้เป็นไปตามระเบียบนี้ และมีอำนาจกำหนดระเบียบปลีกย่อย คู่มือ คำแนะนำ หรือรายการปฏิบัติ โดยไม่ขัดหรือแย้งกับระเบียบนี้ได้ตามความจำเป็น

หมวด ๑
กล่าวทั่วไป
ส่วนที่ ๑
ความมุ่งหมาย

ข้อ ๘ ระเบียบนี้มีความมุ่งหมายเพื่อ

๘.๑ กำหนดหลักการ และมาตรการป้องกันภัยของระบบสารสนเทศของกองทัพอากาศ

๘.๒ พิทักษ์รักษา และป้องกันสารสนเทศที่กำหนดชั้นความลับ มิให้รั่วไหล หรือรู้ไปถึงหรือตกไปอยู่กับบุคคลผู้ไม่มีอำนาจหน้าที่ที่จะต้องทราบ

๘.๓ พิทักษ์รักษา และป้องกันการก่อวินาศกรรมแก่ระบบสารสนเทศของกองทัพอากาศในส่วนที่เป็นระบบคอมพิวเตอร์ และระบบสื่อสารข้อมูล

ส่วนที่ ๒
การแบ่งมอบความรับผิดชอบในการดำเนินงานด้านการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๙ เพื่อให้การดำเนินงานในการรักษาความปลอดภัยระบบสารสนเทศที่มีประสิทธิภาพ จึงแบ่งมอบความรับผิดชอบดังนี้

๙.๑ ให้...

๙.๑ ให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ในฐานะส่วนราชการที่ทำหน้าที่ฝ่ายอำนวยการด้านเทคโนโลยีสารสนเทศและสงครามสารสนเทศ ซึ่งรวมถึง การรักษาความปลอดภัยระบบสารสนเทศ มีหน้าที่รับผิดชอบ กำหนดมาตรการ แนวทางปฏิบัติ ตรวจสอบ แจ้งเตือนภัยที่เกี่ยวข้องกับระบบสารสนเทศในกองทัพอากาศ

๙.๒ ให้ส่วนราชการที่รับผิดชอบระบบในสายงานต่าง ๆ กำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งนายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ โดยแบ่งออกเป็น ๒ ประเภท ดังนี้

๙.๒.๑ นายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่รับผิดชอบ ในการดูแลรักษาความปลอดภัยระบบสารสนเทศที่มีการติดตั้งใช้งานภายในกองทัพอากาศ ทั้งระบบสารสนเทศเพื่อการบริหาร และระบบสารสนเทศเพื่อการยุทธ

๙.๒.๒ นายทหารรักษาความปลอดภัยระบบสารสนเทศและคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วย มีหน้าที่รับผิดชอบ ในการดูแลรักษาความปลอดภัยระบบสารสนเทศเฉพาะภายในหน่วยงานตนเอง แต่หากระบบ นั้นมีการเชื่อมต่อกับระบบสารสนเทศของระบบงาน ก็จะทำหน้าที่ตามที่คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงานกำหนด

ข้อ ๑๐ การกำหนดชั้นความลับของสารสนเทศ ให้เป็นไปตามกฎหมาย หรือระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ หรือระเบียบอื่นใดที่กำหนดไว้เป็นอย่างอื่น

หมวด ๒
การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศ และการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ
(Physical Security and Administrative Security)

ข้อ ๑๑ การรักษาความปลอดภัยสภาพแวดล้อมของระบบสารสนเทศและการจัดการด้านการรักษาความปลอดภัยระบบสารสนเทศ เป็นมาตรการรักษาความปลอดภัยทางด้านกายภาพ บุคคล และการจัดการของระบบสารสนเทศ ที่ช่วยสนับสนุนให้เกิดความปลอดภัยในสภาพแวดล้อมของระบบสารสนเทศที่กำลังดำเนินการป้องกันอยู่ในขณะนั้น

ส่วนที่ ๑

การรักษาความปลอดภัยเกี่ยวกับบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ

(Personnel Security)

ข้อ ๑๒ การรักษาความปลอดภัยเกี่ยวกับบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ มีความมุ่งหมาย เพื่อตรวจสอบบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และเพื่อกำหนดระดับความไว้วางใจที่ให้ปฏิบัติหน้าที่เกี่ยวกับข้อมูล ซึ่งเป็นความลับของทางราชการ ตลอดจนควบคุมบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๓ ให้ส่วนราชการต้นสังกัดดำเนินการตรวจสอบความไว้วางใจโดยละเอียดผ่านกรมข่าวทหารอากาศ และให้หัวหน้าส่วนราชการนั้น ๆ รับรองความไว้วางใจบุคคล ก่อนที่จะมอบหมายให้บุคคลใดปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ โดยยึดถือผลการตรวจสอบประวัติ และพฤติการณ์ของบุคคลนั้น เป็นแนวทางการพิจารณาตามที่เห็นสมควร ในกรณีจำเป็นเร่งด่วนหัวหน้าส่วนราชการอาจรับรองความไว้วางใจบุคคลได้ โดยไม่ต้องรอผลการตรวจสอบประวัติ โดยมีเงื่อนไขว่าหากผลการตรวจสอบประวัติปรากฏว่าผู้นั้นมีประวัติ หรือพฤติการณ์ไม่เหมาะสม ให้ผู้ที่ได้รับการมอบหมายพ้นจากการปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศทันที

บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศโดยตรง เข้ามาทำงานเป็นประจำภายในพื้นที่ใช้งานระบบสารสนเทศ เช่น เจ้าหน้าที่รับ - ส่งหนังสือราชการ พนักงานทำความสะอาด หรือบุคคลอื่น ๆ ต้องทำการตรวจสอบประวัติ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ข้อ ๒๕ ด้วย และให้กำหนดช่วงเวลาทำงานที่แน่นอนของบุคคลดังกล่าว ในระหว่างนั้น ต้องมีเจ้าหน้าที่ประจำพื้นที่ใช้งานระบบสารสนเทศควบคุมดูแลอยู่ด้วยอย่างน้อย ๑ คน

ข้อ ๑๔ ให้ส่วนราชการชี้แจงในเรื่องการรักษาความปลอดภัยตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และเรื่องการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ ตามระเบียบนี้ แก่บุคคลที่จะปฏิบัติในหน้าที่เกี่ยวกับระบบสารสนเทศ

นายทหารรักษาความปลอดภัยระบบสารสนเทศ ตามข้อ ๙ ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ หรือระบบสารสนเทศ โดยจะต้องผ่านการอบรมเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศมาก่อน และจะต้องไม่ได้รับมอบหมายให้รับผิดชอบต่อภารกิจอื่นที่เป็นอุปสรรค หรือเป็นภัยต่อการรักษาความปลอดภัยระบบสารสนเทศ เมื่อได้รับมอบหมายให้ปฏิบัติหน้าที่การรักษาความปลอดภัยระบบสารสนเทศแล้วต้องปฏิบัติหน้าที่ด้วยความซื่อสัตย์ อดทน เสียสละ

ข้อ ๑๕...

ข้อ ๑๕ ให้ส่วนราชการที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศจัดทำทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศตามระดับความไว้วางใจที่แต่ละบุคคลได้รับอนุมัติ และสำเนาส่งให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ทราบด้วย

ข้อ ๑๖ เมื่อบุคคลใดพ้นจากหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ส่วนราชการนั้นตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ และสำเนาส่งให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ทราบด้วย

ข้อ ๑๗ ให้หัวหน้าส่วนราชการ หรือผู้ที่ได้รับมอบหมาย หรือนายทหารรักษาความปลอดภัยระบบสารสนเทศ ชี้แจงให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศได้ทราบถึงความเสียหายต่อความมั่นคงของชาติ ทัณฑ์ทางวินัยในการเปิดเผยความลับของทางราชการ รวมทั้งโทษตามกฎหมายในการเปิดเผยความลับของทางราชการแก่บุคคลผู้ไม่มีหน้าที่เกี่ยวข้องทราบ

ข้อ ๑๘ เมื่อบุคคลใดจะเข้าปฏิบัติหน้าที่ หรือพ้นหน้าที่เกี่ยวกับระบบสารสนเทศ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับเมื่อเข้ารับตำแหน่งหรือหน้าที่ (รปภ.๑๗) หรือใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๑๘) แล้วแต่กรณี ตามที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ข้อ ๒๘, ๒๙, ๓๑ และข้อ ๕๕

ข้อ ๑๙ บุคคลอื่นใดไม่สามารถอ้างยศ ตำแหน่ง หรืออำนาจ เพื่อขอทราบ หรือให้ได้มาซึ่งข้อมูลที่ตนไม่ได้รับอนุญาต

ข้อ ๒๐ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ควบคุม ดูแล และตรวจสอบสิทธิการเข้าถึงระบบสารสนเทศต่าง ๆ ในขอบเขตที่รับผิดชอบ

บุคคลที่จะเข้าใช้ระบบสารสนเทศจะต้องได้รับอนุญาตจากผู้มีอำนาจหน้าที่ก่อน และการเข้าถึงระบบสารสนเทศต้องคำนึงถึงความปลอดภัยของระบบสารสนเทศเป็นหลัก

บุคคลที่ไม่มีอำนาจหน้าที่ จะอนุญาตให้บุคคลอื่นเข้าถึงระบบสารสนเทศไม่ได้

ข้อ ๒๑ หากเจ้าหน้าที่ หรือบุคคลผู้ใดมีพฤติการณ์ไม่น่าไว้วางใจหรืออาจเป็นภัยต่อระบบสารสนเทศ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ รีบรายงานตามลำดับชั้นถึง กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อดำเนินการตามมาตรการรักษาความปลอดภัยและข้อกฎหมายที่เกี่ยวข้องต่อไป

ส่วนที่ ๒...

ส่วนที่ ๒

การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ

(Building and Workspace Security)

ข้อ ๒๒ การรักษาความปลอดภัยอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันภัยเกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศ เพิ่มเติมจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ระเบียบกระทรวงกลาโหมว่าด้วยการรักษาความปลอดภัยหน่วยกรรมวิธีข้อมูลอัตโนมัติ พ.ศ.๒๕๒๘ และระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒

ข้อ ๒๓ ให้ส่วนราชการกำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศอื่นใด เป็นพื้นที่หวงห้าม โดยพิจารณาตามความสำคัญว่าจะต้องพิทักษ์รักษาสิ่งที่เป็นความลับของระบบสารสนเทศในระดับใด โดยกำหนดเป็น “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” แล้วแต่กรณี

พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยินและการมองเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง ทั้งนี้รวมถึงการบันทึกภาพจากกล้องวงจรปิด และให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่งด้วย

ให้ส่วนราชการพิจารณากำหนดมาตรการป้องกันเพิ่มเติมให้เหมาะสม เช่น ห้ามนำอุปกรณ์สื่อสาร ถ่ายภาพ หรืออุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ได้ (Removable Storage Device) เข้าไปภายใน “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ”

ข้อ ๒๔ การปฏิบัติในเวลาฉุกเฉิน

๒๔.๑ อาคาร สถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศที่จัดให้มีเวร - ยามรักษาการณ์เพื่อพิทักษ์รักษาระบบสารสนเทศโดยเฉพาะแล้ว ให้ถือว่าเป็นการปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ ข้อ ๖๔

๒๔.๒ ให้ส่วนราชการเจ้าของอาคาร สถานที่ จัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ แผนเผชิญเหตุ (Contingency Plan) โดยเตรียมอุปกรณ์สนับสนุนในการเคลื่อนย้าย และทำลายไว้ให้พร้อมที่จะปฏิบัติได้ทันท่วงที และชี้แจงให้เจ้าหน้าที่ผู้เกี่ยวข้องเข้าใจวิธี และขั้นตอนปฏิบัติ โดยยึดแนวทางปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยการรักษาการณ์ พ.ศ.๒๕๔๒ ข้อ ๗

๒๔.๓...

๒๔.๓ หากสถานการณ์รุนแรงจนไม่สามารถพิทักษ์รักษาระบบสารสนเทศให้ปลอดภัยได้ ให้ใช้แผนการเคลื่อนย้าย และแผนการทำลายระบบสารสนเทศในเวลาฉุกเฉิน

๒๔.๔ เพื่อมิให้ส่วนใดส่วนหนึ่งของระบบสารสนเทศที่กำหนดชั้นความลับตกไปอยู่ในความครอบครองของฝ่ายตรงข้าม หรือผู้ไม่มีอำนาจหน้าที่ ให้ทำลายตามลำดับความสำคัญชั้นลับที่สุดก่อน

๒๔.๕ ให้ส่วนราชการเจ้าของอาคาร สถานที่ กำหนดมาตรการการป้องกันอัคคีภัย พร้อมจัดเตรียมอุปกรณ์ในการดับเพลิง สำหรับระบบคอมพิวเตอร์ มาตรการป้องกันภัยธรรมชาติพร้อมจัดเตรียมอุปกรณ์ป้องกันภัยธรรมชาติสำหรับระบบคอมพิวเตอร์ จัดเตรียมสถานที่ วัสดุ อุปกรณ์ที่จำเป็นสำหรับการฟื้นฟูระบบ รวมทั้งสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัย

ส่วนที่ ๓
การจัดการการรักษาความปลอดภัยระบบสารสนเทศ
(Information System Security Management)

ข้อ ๒๕ การจัดการการรักษาความปลอดภัยระบบสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดแนวทางการจัดการสำหรับผู้เกี่ยวข้องในระดับของส่วนราชการ และกองทัพอากาศ ในการพิจารณามาตรการควบคุม และป้องกันภัยระบบสารสนเทศที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ

ข้อ ๒๖ การกำหนดมาตรการ หรือระบบการรักษาความปลอดภัย ต้องผ่านการประเมินความเสี่ยง (Risk Assessment) ความอ่อนแอ (Vulnerability) ภัย (Threat) ระบบสารสนเทศ เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับสภาพแวดล้อมของแต่ละระบบ โดยการทำแผนจัดการความเสี่ยง (Risk Management Plan)

ข้อ ๒๗ การรักษาความปลอดภัยระบบสารสนเทศ ต้องดำเนินการป้องกันให้ถึงระดับที่สมดุลกับความเสี่ยงของระบบสารสนเทศที่ประเมินได้

ข้อ ๒๘ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ในฐานะหน่วยงานที่รับผิดชอบงานด้านการรักษาความปลอดภัยระบบสารสนเทศ มีหน้าที่ดังนี้

๒๘.๑ กำหนดและรักษานโยบายการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

๒๘.๒ เสนอแนะการแต่งตั้งนายทหารรักษาความปลอดภัยระบบสารสนเทศตามข้อ ๙

๒๘.๓...

๒๘.๓ กำหนดหน้าที่รับผิดชอบเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ

๒๘.๔ ประเมินความเสี่ยงของระบบสารสนเทศ เพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๒๘.๕ พัฒนาหลักการ และกระบวนการด้านการรักษาความปลอดภัยระบบสารสนเทศและประสานงานด้านการรักษาความปลอดภัยระบบสารสนเทศกับกองบัญชาการกองทัพไทยและหน่วยงานอื่นที่เกี่ยวข้อง

๒๘.๖ สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๗ ให้มีการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องกับระบบสารสนเทศ

๒๘.๙ ดำเนินการตรวจเยี่ยม เพื่อทำการตรวจสอบความปลอดภัยของระบบสารสนเทศ (IT Security Audit) เพื่อพิจารณาให้คำแนะนำ ติดตามและประเมินผลในการปฏิบัติตามนโยบายและแผนการรักษาความปลอดภัยระบบสารสนเทศ

๒๘.๑๐ รายงานอันตรายที่อาจเกิดขึ้น หรือที่เกิดขึ้นแล้วกับระบบสารสนเทศของกองทัพอากาศ ให้แก่ผู้บัญชาการทหารอากาศ หรือผู้ที่ได้รับมอบหมายจากผู้บัญชาการทหารอากาศ

๒๘.๑๑ ตรวจสอบหาหลักฐาน เมื่อมีการละเมิดเพื่อการดำเนินการทางกฎหมายต่อไป

ข้อ ๒๙ นายทหารรักษาความปลอดภัยระบบสารสนเทศ ซึ่งแต่งตั้งโดยหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ มีหน้าที่ดังนี้

๒๙.๑ นายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่

๒๙.๑.๑ กำหนดมาตรการป้องกันสำหรับพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยตาม ข้อ ๒๓ ตามผลการประเมินความเสี่ยงของระบบสารสนเทศ และแจ้งให้ผู้เกี่ยวข้องทราบ

๒๙.๑.๒ ควบคุม ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของระบบงาน

๒๙.๑.๓ ควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบสารสนเทศให้เป็นไปตามความมุ่งหมายของทางราชการ

๒๙.๑.๔...

๒๙.๑.๔ ควบคุม กำกับ ดูแลการเข้าใช้เครือข่ายระบบสารสนเทศในส่วนที่เกี่ยวข้องให้เป็นไปตามหน้าที่ความรับผิดชอบกำหนด และแจ้งให้นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วยทราบ

๒๙.๑.๕ รับผิดชอบการตรวจสอบไวรัสคอมพิวเตอร์ รวมทั้งมาตรการป้องกันและการปรับแก้ไข

๒๙.๑.๖ ศึกษา ค้นคว้า และติดตามข้อมูลข่าวสารเกี่ยวกับการค้นพบจุดอ่อนของระบบต่าง ๆ หรือภัยรูปแบบใหม่ ๆ ของระบบสารสนเทศ เพื่อปรับปรุงมาตรการป้องกันให้ทันสมัยเสมอ

๒๙.๑.๗ พัฒนากระบวนการรักษาความปลอดภัยร่วมกับกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๒๙.๑.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องภายในส่วนราชการ

๒๙.๑.๙ ให้คำแนะนำกับผู้เกี่ยวข้องให้มีความรู้และปฏิบัติตามกระบวนการรักษาความปลอดภัย

๒๙.๑.๑๐ ให้คำแนะนำกับคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงานในการจัดทำแผนต่าง ๆ ที่เกี่ยวข้อง

๒๙.๒ นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วย มีหน้าที่

๒๙.๒.๑ กำหนดมาตรการป้องกันสำหรับพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยตาม ข้อ ๒๓ ตามผลการประเมินความเสี่ยงของระบบสารสนเทศ และแจ้งให้ผู้เกี่ยวข้องทราบ

๒๙.๒.๒ ควบคุม ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ทั้งหมดของส่วนราชการ และหากมีการเชื่อมต่อกับระบบสารสนเทศของระบบงาน ต้องปฏิบัติตามคำแนะนำของนายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงานโดยเคร่งครัด

๒๙.๒.๓ ควบคุมและตรวจสอบการติดตั้งโปรแกรมเข้าสู่ระบบสารสนเทศให้เป็นไปตามความมุ่งหมายของทางราชการ

๒๙.๒.๔ ควบคุม กำกับ ดูแลการเข้าใช้เครือข่ายระบบสารสนเทศให้เป็นไปตามที่ส่วนราชการเจ้าของระบบสารสนเทศนั้น ๆ กำหนด

๒๙.๒.๕ รับผิดชอบการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมประสงค์ร้ายอื่น ๆ รวมทั้งมาตรการป้องกันอื่น ๆ และการปรับแก้ไข

๒๙.๒.๖ ศึกษา ค้นคว้า และติดตามข้อมูลข่าวสารเกี่ยวกับการค้นพบจุดอ่อนของระบบต่าง ๆ หรือภัยรูปแบบใหม่ ๆ ของระบบสารสนเทศ เพื่อปรับปรุงมาตรการป้องกันให้ทันสมัยเสมอ

๒๙.๒.๗...

๒๙.๒.๗ ปฏิบัติตามกระบวนการรักษาความปลอดภัยตามคำแนะนำของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๒๙.๒.๘ ตรวจสอบให้มีการปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยที่เกี่ยวข้องภายในส่วนราชการ

๒๙.๒.๙ ให้คำแนะนำกับผู้เกี่ยวข้องให้มีความรู้และปฏิบัติตามกระบวนการรักษาความปลอดภัย

ข้อ ๓๐ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ มีองค์ประกอบและหน้าที่ ดังนี้

๓๐.๑ องค์ประกอบของคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ

๓๐.๑.๑ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน ซึ่งแต่งตั้งโดย หัวหน้าส่วนราชการ ผู้รับผิดชอบระบบ ประกอบด้วย

๓๐.๑.๑.๑ หัวหน้าส่วนราชการ หรือ รองหัวหน้าส่วนราชการผู้รับผิดชอบระบบ เป็นประธาน

๓๐.๑.๑.๒ หัวหน้าหน่วยขึ้นตรงของส่วนราชการผู้รับผิดชอบระบบ เป็นกรรมการ

๓๐.๑.๑.๓ นายทหารรักษาความปลอดภัยระบบสารสนเทศของระบบงาน เป็นกรรมการและเลขานุการ

๓๐.๑.๑.๔ ผู้เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศตามข้อ ๓๑ โดยพิจารณาตามความเหมาะสม เป็นกรรมการ

๓๐.๑.๒ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วย ซึ่งแต่งตั้งโดยหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ ประกอบด้วย หัวหน้าส่วนราชการ หรือรองหัวหน้าส่วนราชการเป็นประธาน และมีกรรมการ ตามจำนวนที่เหมาะสมโดยมีนายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วย เป็นกรรมการ และเลขานุการ

๓๐.๒ หน้าที่ของคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ

๓๐.๒.๑ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของระบบงาน มีหน้าที่

๓๐.๒.๑.๑ จัดทำแผนจัดการความเสี่ยงสำหรับระบบสารสนเทศของระบบงาน

๓๐.๒.๑.๒ กำหนดมาตรการรักษาความปลอดภัยเฉพาะสำหรับระบบสารสนเทศของระบบงานตามแผนใน ข้อ ๓๐.๒.๑.๑ หรือตามที่ได้รับการแนะนำ

๓๐.๒.๑.๓...

๓๐.๒.๑.๓ จัดทำแผนที่เกี่ยวข้อง ดังนี้

๓๐.๒.๑.๓(๑) แผนการสำรองข้อมูลของระบบสารสนเทศ

๓๐.๒.๑.๓(๒) แผนฟื้นฟูระบบสารสนเทศ

๓๐.๒.๑.๓(๓) แผนป้องกันภัยธรรมชาติของระบบสารสนเทศ

๓๐.๒.๑.๓(๔) แผนป้องกันอัคคีภัยของระบบสารสนเทศ

๓๐.๒.๑.๓(๕) แผนเผชิญเหตุ (Contingency Plan)

๓๐.๒.๑.๓(๖) แผนป้องกันภัยที่ส่วนราชการนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

๓๐.๒.๑.๔ จัดทำแผนผัง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของระบบงาน

๓๐.๒.๑.๕ จัดทำรายการอุปกรณ์ สถานภาพการใช้งานและผู้รับผิดชอบ

๓๐.๒.๑.๖ กำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์แต่ละหน่วยงาน โดยให้มีหน้าที่ ดูแล บำรุงรักษา ป้องกันภัย ตรวจสอบความพร้อมใช้งานตลอดจนควบคุมการใช้งานอุปกรณ์ให้เป็นไปตามที่กำหนดไว้

๓๐.๒.๒ คณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของหน่วยมีหน้าที่

๓๐.๒.๒.๑ จัดทำแผนจัดการความเสี่ยงสำหรับระบบสารสนเทศของหน่วย

๓๐.๒.๒.๒ กำหนดมาตรการรักษาความปลอดภัยเฉพาะสำหรับระบบสารสนเทศของระบบงานตามข้อมูลจากแผนใน ข้อ ๓๐.๒.๒.๑ หรือตามที่ได้รับการแนะนำ

๓๐.๒.๒.๓ จัดทำแผนที่เกี่ยวข้องตามความเหมาะสมดังนี้

๓๐.๒.๒.๓(๑) แผนการสำรองข้อมูลของระบบสารสนเทศ

๓๐.๒.๒.๓(๒) แผนฟื้นฟูระบบสารสนเทศ

๓๐.๒.๒.๓(๓)...

๓๐.๒.๒.๓(๓) แผนป้องกันภัยธรรมชาติของระบบสารสนเทศ

๓๐.๒.๒.๓(๔) แผนป้องกันอัคคีภัยของระบบสารสนเทศ

๓๐.๒.๒.๓(๕) แผนเผชิญเหตุ (Contingency Plan)

๓๐.๒.๒.๓(๖) แผนป้องกันภัยที่ส่วนราชการนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

๓๐.๒.๒.๔ จัดทำแผนผัง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของหน่วย

๓๐.๒.๒.๕ จัดทำรายการอุปกรณ์ สถานภาพการใช้งานและผู้รับผิดชอบ

๓๐.๒.๒.๖ กำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์แต่ละหน่วยงาน โดยให้มีหน้าที่ ดูแล บำรุงรักษา ป้องกันภัย ตรวจสอบความพร้อมใช้งานตลอดจนควบคุมการใช้งานอุปกรณ์ให้เป็นไปตามที่กำหนดไว้

ข้อ ๓๑ ผู้ปฏิบัติหน้าที่ด้านระบบสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ นอกจากจะต้องมีความรู้และได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามผนวก ก แล้วให้มีหน้าที่ดังนี้

๓๑.๑ ผู้บริหารระบบ (System Administrator) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตเข้าถึงระบบคอมพิวเตอร์ได้ วางระบบป้องกันการเข้าถึงในระบบสารสนเทศให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ โดยกำหนดให้มีกระบวนการพิสูจน์ทราบ(Authentication) กำหนดสิทธิ (Authorization) และบันทึกปูมใช้งานที่เหมาะสม(Audit Log) นอกจากนั้นต้องมีหน้าที่ในการปฏิบัติตามแผนสำรองและกู้ข้อมูล โดยหากเป็นเครือข่ายด้านยุทธการควรต้องกำหนดกระบวนการพิสูจน์ทราบที่ใช้มากกว่า password หรือเป็น Multi-Factor Authentication เช่น การใช้ Smart Card หรือ การอ่านลายนิ้วมือ

๓๑.๒ ผู้บริหารฐานข้อมูล (Database Administrator) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตเข้าถึงฐานข้อมูลได้ วางระบบป้องกันการเข้าถึงฐานข้อมูลให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับ คงสภาพและสร้างสภาพพร้อมใช้งานให้ฐานข้อมูล

๓๑.๓ ผู้บริหารเครือข่าย (Network Administrator) มีหน้าที่ดำเนินการเพื่อให้ผู้ได้รับอนุญาตสามารถเข้าถึงระบบเครือข่ายได้ วางระบบป้องกันการเข้าถึงเครือข่ายให้พ้นจากผู้ไม่เกี่ยวข้อง รักษาความลับโดยการเลือกใช้การเข้ารหัสที่เหมาะสม คงสภาพและสร้างสภาพพร้อมใช้งานให้ระบบเครือข่าย

รวมถึง...

รวมถึงดูแลการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ ทางกายภาพให้ตรงตามการใช้งานที่ได้กำหนดไว้

๓๑.๔ ผู้เขียนโปรแกรม (Programmer) มีหน้าที่ดำเนินการให้ผู้ใช้ที่ได้รับอนุญาตสามารถเข้าถึงโปรแกรมได้ ตรวจหาข้อบกพร่อง หรือสิ่งอื่นใดที่เป็นภัยต่อโปรแกรม เพื่อกำจัดก่อนนำเข้าสู่ระบบสารสนเทศ

ข้อ ๓๒ ผู้ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ ต้องปฏิบัติและดำเนินการ ดังนี้

๓๒.๑ ดำเนินการใด ๆ กับข้อมูลเฉพาะที่ได้รับอนุญาตแล้วเท่านั้น และต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

๓๒.๒ ใช้ระบบสารสนเทศอย่างระมัดระวัง ถูกต้องตามกระบวนการรักษาความปลอดภัย และใช้ในกิจการงานที่ได้รับอนุญาต หรือได้รับมอบหมายเท่านั้น

๓๒.๓ ตรวจสอบโปรแกรมประสงค์ร้ายก่อนนำมาใช้งานในระบบ

๓๒.๔ ไม่นำโปรแกรมที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องกับภารกิจหน้าที่ ที่ได้รับมอบหมายเข้าสู่ระบบสารสนเทศ

๓๒.๕ เก็บรักษาและใช้งานบัญชีผู้ใช้ (User Account) ซึ่งประกอบด้วยชื่อผู้ใช้ (user name) และรหัสผ่าน (Password) ให้เหมาะสม และเก็บรักษารหัสผ่าน (Password) ให้เป็นไปด้วยความปลอดภัย ไม่รั่วไหลถึงบุคคลอื่น

ข้อ ๓๓ ผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ของหน่วยงานตามที่ได้รับการมอบหมายจากคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ ต้องปฏิบัติและดำเนินการ ดังนี้

๓๓.๑ ดำเนินการหน้าที่ตาม ข้อ ๓๐.๒.๑.๖

๓๓.๒ ดูแลการใช้งานอุปกรณ์คอมพิวเตอร์ในพื้นที่ที่รับผิดชอบ

๓๓.๓ ดูแลสภาพแวดล้อมการใช้งานให้เหมาะสม

ข้อ ๓๔ การกำหนดรหัสผ่าน (Password) ที่เหมาะสมสำหรับผู้ใช้ทุกระดับมีข้อกำหนดขั้นต่ำดังนี้

๓๔.๑ มีความยาวอย่างน้อย ๘ ตัวอักษร

๓๔.๒ ประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลขและอักขระพิเศษ

๓๔.๓ จะต้องไม่มีข้อมูลเกี่ยวกับผู้ใช้ เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์จดจำรหัสผ่านแทนการเขียนบันทึก หากเจ้าของรหัสผ่านลืมรหัสผ่าน หรือต้องการแก้ไขให้เจ้าของรหัสผ่านแจ้งผู้ดูแลระบบ ให้ดำเนินการ

๓๔.๔...

๓๔.๔ ต้องเปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด หรือตามความเหมาะสม สำหรับระบบที่มีความสำคัญ

๓๔.๕ ความรับผิดชอบในการใช้งาน Username และ Password เป็นของเจ้าของผู้ใช้งาน ต้องไม่โอนสิทธิหรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน ต้องไม่เปิดเผยรหัสผ่านให้แก่ผู้ใดทั้งสิ้น รวมถึงผู้ดูแลระบบสารสนเทศ

๓๔.๖ สำหรับระบบสารสนเทศที่มีความสำคัญ ต้องไม่ใช้รหัสผ่านเดียวกันสำหรับเข้าถึงระบบทั่วไป

๓๔.๗ ไม่ใช้รหัสผ่านร่วมกับผู้อื่นโดยเด็ดขาด แม้ว่าจะเป็นผู้ร่วมงานที่ต้องใช้แฟ้มข้อมูลเดียวกัน ทุกคนที่ได้รับอนุญาตจะต้องมีรหัสผ่านเป็นของตนเองในการเข้าใช้ข้อมูลดังกล่าว

หมวด ๓
การรักษาความปลอดภัยระบบคอมพิวเตอร์
(Computer System Security)

ข้อ ๓๕ การรักษาความปลอดภัยระบบคอมพิวเตอร์ เป็นมาตรการควบคุมและป้องกันเพื่อยืนยันถึงความถูกต้อง สิทธิการเข้าใช้ ความลับ และความพร้อมใช้งานของสารสนเทศที่ดำเนินการ หรือที่เก็บรักษาในระบบคอมพิวเตอร์

ส่วนที่ ๑
การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์
(Computer Equipment Security)

ข้อ ๓๖ การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์ มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ การรั่วไหล และความเสียหายของข้อมูลที่เกิดจากจุดอ่อน หรือข้อบกพร่องของอุปกรณ์คอมพิวเตอร์ หรือซอฟต์แวร์ที่เกี่ยวข้อง รวมทั้งสร้างสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์

ข้อ ๓๗ อุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศของทุกหน่วย หรือทุกชุด ต้องมีการกำหนดผู้รับผิดชอบ และจัดทำรายละเอียดที่จำเป็น เช่น ผู้ที่ได้รับอนุญาตให้เข้าใช้ การใช้งาน ตลอดจนระดับของการป้องกัน เป็นต้น

ข้อ ๓๘...

ข้อ ๓๘ การจัดเก็บสิ่งบันทึกที่สามารถแสดงผล หรือสื่อความเป็นสารสนเทศที่มีชั้นความลับได้ เช่น จานบันทึก ซีดีรอม และอื่น ๆ ที่นำมาแสดงผลโดยระบบคอมพิวเตอร์ได้ หากแสดงชั้นความลับไว้ในที่ดังกล่าวไม่ได้ ให้พิทักษ์รักษาตามชั้นความลับนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ และห้ามมิให้ผู้ใดมีการใช้งานสื่อบันทึกข้อมูลที่เคลื่อนที่ได้ (Removable Storage Devices) ในสายงานที่เกี่ยวข้องกับงานด้านยุทธการที่มีชั้นความลับ เว้นแต่ผู้ที่ได้รับอนุญาตจากหัวหน้าหน่วยงานที่เกี่ยวข้องเป็นลายลักษณ์อักษร และหากมีการกระทำความผิดเกี่ยวข้องกับสื่อบันทึกข้อมูลที่เคลื่อนที่ได้นั้น เจ้าของผู้ลงทะเบียนต้องรับผิดชอบ

ข้อ ๓๙ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ตรวจสอบอุปกรณ์ที่นำมาติดตั้งใหม่ทุกครั้ง ว่าได้มาตรฐานในการรักษาความปลอดภัย สำหรับอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่แล้ว ให้ตรวจสอบทุกรอบ ๓ เดือน หรือเมื่อมีเหตุอันควรแก่การตรวจสอบ และรายงานให้หัวหน้าส่วนราชการทราบเมื่อสิ้นสุดระยะเวลาการตรวจสอบ

ข้อ ๔๐ การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เข้า - ออก นอกพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการ หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะการทำงานของอุปกรณ์เปลี่ยนแปลงไป จะต้องแจ้งและขออนุญาตตามลำดับชั้นถึงนายทหารรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ และให้ผู้รับผิดชอบพื้นที่ใช้งานระบบสารสนเทศของส่วนราชการตรวจสอบความปลอดภัยก่อนการเคลื่อนย้ายทุกครั้ง

ข้อ ๔๑ ก่อนนำอุปกรณ์คอมพิวเตอร์ไปซ่อมบำรุง หรือจำหน่ายขายซากให้บุคคลภายนอกกองทัพอากาศ หรือนำอุปกรณ์คอมพิวเตอร์กลับไปใช้ในงานของภารกิจใหม่ภายหลังจากใช้ในงานของภารกิจอื่น ๆ มาแล้ว หรือต้องการทำลายข้อมูล เมื่อหมดความจำเป็นในการใช้งานแล้ว หรือเป็นการโอนสิทธิการถือครองอุปกรณ์คอมพิวเตอร์ในลักษณะอื่น ๆ ต้องทำลายข้อมูลทั้งหมดที่มีชั้นความลับตั้งแต่ “ลับ” ขึ้นไปที่อยู่ในอุปกรณ์ดังกล่าวไม่ให้สามารถกู้คืนมาใช้งานได้อีก

ในกรณีที่นำอุปกรณ์คอมพิวเตอร์ไปซ่อมภายนอกกองทัพอากาศ และมีการเปลี่ยนชิ้นส่วน เพื่อทดแทนชิ้นส่วนที่ชำรุดเสียหาย ให้นายทหารรักษาปลอดภัยระบบสารสนเทศของส่วนราชการที่ดำเนินการซ่อมบำรุงติดตามนำชิ้นส่วนดังกล่าวกลับมาดำเนินการให้ถูกต้องต่อไป

ส่วนที่ ๒
การรักษาความปลอดภัยการโปรแกรม
(Program Security)

ข้อ ๔๒ การรักษาความปลอดภัยการโปรแกรม มีความมุ่งหมาย เพื่อขจัดการใช้ประโยชน์จากจุดอ่อน หรือข้อบกพร่องของโปรแกรมในการทำอันตรายระบบสารสนเทศ

ข้อ ๔๓...

ข้อ ๔๓ ผู้พัฒนาโปรแกรมเพื่อนำไปใช้ในระบบสารสนเทศ ต้องพัฒนาโปรแกรมตามหลักวิชาการที่ยอมรับโดยทั่วไป และยินยอมให้ทำการตรวจสอบได้ตลอดเวลา รวมทั้งแสดงรายละเอียดที่จำเป็นต่อการรักษาความปลอดภัยไว้ที่รหัสต้นทาง (Source Code) เช่น ชื่อผู้เขียน วัน เดือน ปีที่เขียน หรือปรับปรุง วัตถุประสงค์ ระดับการป้องกัน สำหรับข้อมูลที่จำเป็นต้องใช้ในการพัฒนา เช่น ความสัมพันธ์ที่สามารถเชื่อมโยงไปถึงโปรแกรมหรือข้อมูลลับอื่น ๆ หรือผู้ที่ได้รับอนุญาตให้นำโปรแกรมไปใช้งานได้ให้เพิ่มเติมไว้ในเอกสารคู่มือ

ผู้พัฒนาโปรแกรมทั้งที่เป็นบุคลากรทางคอมพิวเตอร์ของกองทัพอากาศและบุคคลภายนอกที่รับจัดทำโปรแกรมให้กองทัพอากาศ ต้องคำนึงถึงความปลอดภัยในทุกขั้นตอนของการพัฒนาโปรแกรม รวมทั้งรับผิดชอบต่อการรักษาความลับของข้อมูลและความถูกต้องของโปรแกรม จัดทำเอกสารหรือคู่มือประกอบการใช้งานสำหรับผู้พัฒนาโปรแกรมและผู้ใช้ และพัฒนาโปรแกรมให้ตรงตามวัตถุประสงค์ของทางราชการเท่านั้น ให้ใช้เฉพาะซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันโปรแกรมประสงค์ร้าย หากเป็นโปรแกรมสำเร็จรูป เช่น โปรแกรมระบบปฏิบัติการ หรือ โปรแกรมสำนักงาน ต้องมีการปรับปรุงให้ทันสมัยตลอดเวลาเพื่ออุดช่องโหว่และเป็นการป้องกันโปรแกรมประสงค์ร้าย

ข้อ ๔๔ การพัฒนาโปรแกรมประยุกต์ให้ส่วนราชการ ผู้มีสิทธิและอำนาจในสารสนเทศนั้นเป็นผู้พิจารณาคุณสมบัติของผู้ที่สามารถใช้งานโปรแกรมดังกล่าวได้ตามสิทธิ

หมวด ๔
การรักษาความปลอดภัยระบบสื่อสาร
(Data Communication Security)

ข้อ ๔๕ การรักษาความปลอดภัยระบบสื่อสาร เป็นมาตรการควบคุมและป้องกันเพื่อยืนยันถึงความถูกต้องของการโอน การแลกเปลี่ยนสารสนเทศ หรือการติดต่อกันในลักษณะใดลักษณะหนึ่งผ่านทางระบบสื่อสารข้อมูลว่าได้กระทำโดยผู้มีอำนาจหน้าที่และป้องกันผู้ไม่เกี่ยวข้องเข้าถึงระบบสื่อสาร

ข้อ ๔๖ การรักษาความปลอดภัยเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ (Computer Network Security) เป็นการรักษาความปลอดภัยระบบสื่อสาร มีความมุ่งหมาย เพื่อกำหนดมาตรการควบคุมและป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต ความลับรั่วไหลการบิดเบือน และการทำลายสารสนเทศในระหว่างส่งผ่านทางระบบเครือข่ายคอมพิวเตอร์

ข้อ ๔๗ ส่วนราชการเจ้าของเรื่องสารสนเทศในเครือข่ายระบบสารสนเทศ ผู้มีสิทธิและอำนาจในสายงาน ที่มีการติดต่อแลกเปลี่ยนสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นผู้พิจารณาคุณสมบัติ

ของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึง และดำเนินการกับสารสนเทศดังกล่าว รวมทั้งพิจารณาระดับของการป้องกันที่ต้องการ โดยหากมีการแลกเปลี่ยนกับหน่วยงานนอกกองทัพอากาศ ต้องได้รับการตรวจสอบระดับความปลอดภัยที่เหมาะสมจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๔๘ การส่งสารสนเทศที่มีชั้นความลับผ่านระบบเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุมัติจากเจ้าของเรื่องสารสนเทศ ผู้มีสิทธิและอำนาจในสายงาน ที่กำหนดชั้นความลับนั้นก่อน เมื่อได้รับอนุมัติแล้ว สารสนเทศกำหนดชั้นความลับจะต้องส่งเข้ารหัส (Encryption) โดยมาตรฐานที่ได้รับการรับรองแล้วจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ผู้มีสิทธิและอำนาจในสายงานสามารถกำหนดระเบียบปฏิบัติของการเข้าใช้ที่สอดคล้องกับระเบียบนี้

ข้อ ๔๙ หากมีการใช้เครือข่ายไร้สายทั้งในด้านยุทธการ และธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัส โดยต้องมีการขึ้นทะเบียนอุปกรณ์ (WiFi Access Point) เพื่อตรวจสอบและยืนยันความปลอดภัยจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ข้อ ๕๐ ห้ามมิให้เครือข่ายทางด้านยุทธการเชื่อมต่อกับระบบอินเทอร์เน็ตหรือระบบอื่น ๆ ของหน่วยงานภายนอกกองทัพอากาศ ยกเว้นแต่ที่ได้รับการตรวจสอบและเห็นชอบจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

หมวด ๕
การรักษาความปลอดภัยสารสนเทศ
(Information Security)

ข้อ ๕๑ การรักษาความปลอดภัยสารสนเทศ เป็นมาตรการป้องกันสารสนเทศที่อยู่ในระบบจากการเข้าถึง ด้วยการรักษาความลับไม่ให้รั่วไหล การคงสภาพข้อมูล และการสร้างสภาพพร้อมใช้งานให้แก่ผู้มีสิทธิ รวมถึงมาตรการป้องกันอื่น ๆ ที่จำเป็น

ส่วนที่ ๑
การรักษาความปลอดภัยฐานข้อมูล
(Database Security)

ข้อ ๕๒ การรักษาความปลอดภัยฐานข้อมูล มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึงการเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

ข้อ ๕๓...

ข้อ ๕๓ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย และหากเป็นข้อมูลที่มีชั้นความลับ ต้องมีการเข้ารหัสในการจัดเก็บที่เหมาะสม โดยใช้รูปแบบการเข้ารหัสตามมาตรฐานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศกำหนด

ข้อ ๕๔ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ และจัดให้มีแฟ้มลงบันทึกเข้าออกและการใช้งาน (Audit Log) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

ข้อ ๕๖ ต้องมีการจัดทำแผนสำรองและกู้ข้อมูลที่เหมาะสม และหากเป็นข้อมูลเกี่ยวกับงานด้านยุทธการต้องมีการสำรองข้อมูลอย่างน้อย ๒ ชุด โดยเก็บไว้ในพื้นที่ปฏิบัติงาน ๑ ชุดและเก็บไว้ห่างจากจุดที่มีการติดตั้งใช้อีก ๑ ชุด สำหรับระบบอื่น ๆ ให้กำหนดตามความเหมาะสม

ส่วนที่ ๒
การจัดการสารสนเทศ
(Information Management)

ข้อ ๕๗ การจัดการสารสนเทศ มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันและควบคุมการใช้สารสนเทศที่มีชั้นความลับในรูปแบบต่าง ๆ

ข้อ ๕๘ ให้ผู้มีส่วนเกี่ยวข้องกับการแสดงชั้นความลับของสารสนเทศ ปฏิบัติดังนี้

๕๘.๑ สารสนเทศที่จัดทำในรูปแบบเอกสารหรือรายงาน ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับกึ่งกลางหน้าทั้งด้านบน และด้านล่างของทุกหน้าเอกสารที่มีชั้นความลับนั้น โดยใช้ตัวอักษรที่มีขนาดใหญ่กว่าที่ใช้ในข้อความปกติ และใช้สีหรือความเข้มของตัวอักษรที่มีขนาดใหญ่

๕๘.๒ สารสนเทศที่จัดทำในรูปแบบ ภาพเขียน เรขา ภาพถ่าย แผนที่ แผนภูมิ แผนผัง ให้แสดงหรือพิมพ์ตัวอักษรตามชั้นความลับ เช่นเดียวกับ ข้อ ๕๘.๑ โดยให้แสดงชั้นความลับให้ปรากฏเห็นได้ชัดเจน หรือแสดงไว้ใกล้ชื่อภาพ หรือมาตราส่วน

๕๘.๓ ในการแสดง นำเสนอ หรือพูดถึงสารสนเทศที่มีชั้นความลับ ให้ผู้แสดงหรือผู้พูดแจ้งให้ผู้ดู หรือผู้ฟังทราบชั้นความลับที่กำหนดของสารสนเทศนั้น ๆ หากแสดงภาพฉายบนจอภาพให้แสดงชั้นความลับด้วยอักษร ทั้งก่อนและเมื่อเสร็จสิ้นการแสดง การนำเสนอหรือพูดแล้ว

๕๘.๔...

๕๘.๔ สารสนเทศที่กำหนดชั้นความลับ จะต้องวางระบบป้องกันมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าถึงและแก้ไข ลบล้าง หรือทำลายโดยพลการ และหากมีข้อมูลที่เป็นชั้นความลับหลายชั้นความลับอยู่ในแฟ้มข้อมูลเดียวกัน ให้กำหนดชั้นความลับสูงสุดของสารสนเทศนั้นไว้ที่แฟ้มข้อมูลดังกล่าว

ข้อ ๕๙ การจัดทำซ้ำ หรือจัดทำสำเนาข้อมูลสารสนเทศที่กำหนดชั้นความลับ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากเจ้าของเรื่องสารสนเทศ ที่กำหนดชั้นความลับนั้น และให้รวมหมายถึงการสั่งงานระบบคอมพิวเตอร์ให้จัดการพิมพ์ออกเป็นเอกสารลับนั้นด้วย

ข้อ ๖๐ การปรับ และยกเลิกชั้นความลับของสารสนเทศ ให้เจ้าของสารสนเทศตรวจสอบอยู่เสมอว่าชั้นความลับของสารสนเทศที่กำหนดไว้แต่เดิมยังจำเป็นต้องใช้อยู่หรือไม่ เพราะสารสนเทศอาจลดชั้น เพิ่มชั้นหรือยกเลิกชั้นความลับได้ตามความจำเป็น และควรลดชั้นลงทุกโอกาสเท่าที่กระทำได้เพื่อลดภาระในการรักษาความปลอดภัย

ข้อ ๖๑ สารสนเทศที่ได้รับจากรัฐบาลต่างประเทศ หรือองค์การระหว่างประเทศ หากรัฐบาลหรือองค์การนั้น ๆ ได้กำหนดชั้นความลับไว้ จะต้องปฏิบัติต่อสารสนเทศนั้นเท่าเทียมกับสารสนเทศที่กำหนดชั้นความลับ

ข้อ ๖๒ การเผยแพร่ข้อมูล ข่าวสาร หรือสารสนเทศใด ๆ ของทางราชการผ่านสื่อทางระบบสารสนเทศให้เป็นไปตามระเบียบ คำสั่งของส่วนราชการและกองทัพอากาศที่เกี่ยวข้อง โดยให้มีการเผยแพร่เท่าที่จำเป็นตามพระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ อีกทั้งให้บุคลากรของกองทัพอากาศระมัดระวังการให้ข้อมูลผ่านช่องทางที่ไม่เป็นทางการด้วย โดยให้ยึดถือตามแนวทางของกฎหมาย ดังกล่าวเช่นกัน

ข้อ ๖๓ สารสนเทศที่กำหนดชั้นความลับ “ลับที่สุด” และ “ลับมาก” ที่ใช้ร่วมกันระหว่างส่วนราชการต้องแบ่งระดับการเข้าถึงสารสนเทศตามหน้าที่ของผู้ใช้

ข้อ ๖๔ สารสนเทศที่อยู่ในระบบคอมพิวเตอร์ หากสารสนเทศเป็นร่าง หรือสำเนาของเอกสารที่มีชั้นความลับ จะต้องแสดงชั้นความลับเช่นเดียวกับเอกสารต้นฉบับ ในกรณีที่เอกสารต้นฉบับได้ดำเนินการทำลายแล้วให้ลบทิ้งสารสนเทศที่อยู่ในระบบคอมพิวเตอร์นั้นด้วย โดยการทำลายแบบไม่ให้สามารถกู้ข้อมูลกลับคืนได้ภายหลัง

ข้อ ๖๕ กุญแจเพื่อการเข้าและถอดรหัสลับ (Encryption and Decryption Key) ทุกชนิดที่ใช้ในการเข้ารหัสระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป ต้องจำกัดการเข้าถึงเท่าที่จำเป็น โดยมีขนาดของกุญแจ (จำนวน bit) ที่เหมาะสมและควรเปลี่ยนตามวาระ ดังนี้

๖๕.๑...

๖๕.๑ ตามห้วงระยะเวลาอย่างน้อย ๓ เดือนต่อหนึ่งครั้ง หรือ ตามความจำเป็นหากเกี่ยวข้องกับงานด้านยุทธการ แต่ต้องไม่กำหนดระยะเวลาที่แน่นอนได้

๖๕.๒ เมื่อมีการเปลี่ยนเจ้าหน้าที่ที่เกี่ยวข้องกับการเข้ารหัส พร้อมทั้งสั่งยกเลิกกุญแจเพื่อเข้าและถอดรหัสลับ (Encryption and Decryption Key) เดิม

๖๕.๓ เมื่อความลับรั่วไหลหรือสงสัยว่าความลับรั่วไหล

ข้อ ๖๖ รหัสผ่าน (Password) ของผู้ใช้ ที่ใช้ในระบบสารสนเทศให้จัดเป็นสารสนเทศที่มีชั้นความลับ “ลับ” ขึ้นไป และให้ผู้ใช้ทุกคนปฏิบัติตามวิธีการรักษาความปลอดภัยเกี่ยวกับรหัสผ่านประจำตัว

หมวด ๖
การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ข้อ ๖๗ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีความมุ่งหมาย เพื่อให้เป็นแนวทางปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ และลดความเสียหายที่เกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลยให้เหลือน้อยที่สุด พร้อมทั้งตรวจสอบ ค้นหาสาเหตุ ผลเสียหายเพื่อปรับปรุงมาตรการป้องกันการละเมิดที่จะเกิดขึ้นซ้ำอีกกับกำหนดวิธีดำเนินการต่อผู้ละเมิดการรักษาความปลอดภัย

ข้อ ๖๘ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีดังนี้

๖๘.๑ เมื่อตรวจพบ หรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ หรือมีสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ ให้รีบรายงานผู้บังคับบัญชา และนายทหารรักษาความปลอดภัยระบบสารสนเทศทราบโดยเร็วที่สุด

๖๘.๒ ให้นายทหารรักษาความปลอดภัยระบบสารสนเทศ ดำเนินการดังนี้

๖๘.๒.๑ รายงานขั้นต้นต่อ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อการค้นหาและพิสูจน์หลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์ (Computer Forensic) หากพบว่าเป็นการละเมิดต่อสารสนเทศที่มีชั้นความลับให้แจ้ง กรมข่าวทหารอากาศ ในฐานะสายวิทยาการรักษาความปลอดภัยทราบด้วย

๖๘.๒.๒ ลดความเสียหายเบื้องต้น โดยการระงับใช้ แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิดนั้น หากเป็นสารสนเทศที่มีชั้นความลับจะต้องแจ้งให้เจ้าของเรื่องสารสนเทศที่มีชั้นความลับนั้นทราบ เพื่อพิจารณายกเลิกชั้นความลับ

๖๘.๒.๓...

๖๘.๒.๓ สำรวจความเสียหายที่เกิดจากการละเมิด ตรวจสอบสาเหตุและจุดอ่อน หรือข้อบกพร่องที่ก่อให้เกิดการละเมิดโดยให้มีผู้แทนจาก กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ และกรมข่าวทหารอากาศร่วมในการตรวจสอบสาเหตุด้วย

๖๘.๒.๔ รายงานเหตุการณ์ที่เกิดขึ้นให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

๖๘.๒.๕ หากปรากฏหลักฐาน หรือสงสัยว่าระบบสารสนเทศถูกจารกรรม ให้รายงานให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ เพื่อแก้ไขโดยเร็วที่สุด

ข้อ ๖๙ หน้าที่และความรับผิดชอบของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ มีดังนี้

๖๙.๑ แจ้งให้ส่วนราชการเจ้าของสารสนเทศร่วม ทราบโดยเร็วที่สุด

๖๙.๒ แต่งตั้งคณะกรรมการร่วมกับส่วนราชการที่มีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ เพื่อดำเนินการสืบสวนสอบสวนหาตัวผู้รับผิดชอบและผู้กระทำผิดโดยเร็วที่สุด

๖๙.๓ แจ้งให้ส่วนราชการต้นสังกัด ลงโทษผู้รับผิดชอบและผู้กระทำผิดต่อการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ ตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบ หรือส่งตัวผู้กระทำผิดไปดำเนินการตามกฎหมายแล้วแต่กรณี

๖๙.๔ สั่งให้แก้ไขข้อบกพร่อง และป้องกันมิให้เกิดเหตุการณ์ซ้ำขึ้นอีก

ข้อ ๗๐ หน้าที่และความรับผิดชอบของส่วนราชการที่มีผู้ละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

๗๐.๑ ลงโทษหรือลงทัณฑ์ทางวินัยกับผู้ละเมิด และผู้รับผิดชอบต่อการละเมิดดังกล่าวตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำขึ้นอีก ในกรณีผู้ละเมิดเป็นบุคคลภายนอกกองทัพอากาศ ให้หน่วยเกี่ยวข้องดำเนินการตามกฎหมายต่อไป

๗๐.๒ หากก่อให้เกิดความเสียหายต่อทางราชการอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป

๗๐.๓ พิจารณาข้อมูลสารสนเทศที่มีชั้นความลับ รหัสประมวลลับ (Code) กุญแจเข้าและถอดรหัสที่อยู่ในความรับผิดชอบ หากได้รับความเสียหาย รั่วไหล หรือได้รับความกระทบกระเทือน ต้องดำเนินการแก้ไขโดยเร็วที่สุด

๗๐.๔ กำหนดมาตรการป้องกันเพิ่มเติม เพื่อขจัดความเสียหายที่จะเกิดการละเมิดซ้ำหรือเปลี่ยนแปลงวิธีการปฏิบัติ ยกเลิกโปรแกรม และอื่น ๆ

๗๐.๕...

๗๐.๕ หากก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และต้องเสียค่าใช้จ่ายในการกู้คืนมา ให้ส่วนราชการเรียกร้องค่าเสียหายส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้ระบบด้วย

ข้อ ๗๑ ในกรณีที่มีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ อันก่อให้เกิดความเสียหายต่อระบบสารสนเทศของกองทัพอากาศอย่างร้ายแรง ให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ สั่งการแก้ไข เปลี่ยนแปลงระบบ แผนงาน และวิธีปฏิบัติได้ตามความจำเป็นและความเหมาะสม

ข้อ ๗๒ เพื่อให้การดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศตามระเบียบนี้เป็นไปด้วยความเรียบร้อยและรวดเร็ว ให้คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง มีความหมายตามผนวก ข

ประกาศ ณ วันที่ ๒๐ พฤศจิกายน พ.ศ.๒๕๕๒

(ลงชื่อ) พลอากาศเอก อิทธพร ศุภวงศ์

(อิทธพร ศุภวงศ์)

ผู้บัญชาการทหารอากาศ

การแจกจ่าย ผบ.ทอ., รอง ผบ.ทอ., ปธ.คปษ.ทอ., ผช.ผบ.ทอ., เสธ.ทอ., ปษ.พิเศษ ทอ., หน.คณะนายทหารฝ่ายเสนาธิการประจำผู้บังคับบัญชา, รอง เสธ.ทอ., ผช.เสธ.ทอ., สน.ผบ.ทอ., สน.รอง ผบ.ทอ., สน.ปธ.คปษ.ทอ., สน.ผช.ผบ.ทอ., สน.เสธ.ทอ., สน.รอง เสธ.ทอ., สน.ผช.เสธ.ทอ., สน.ปษ.ทอ., สน.ผทค.ทอ., ผนน.บก.ทอ., นขต.ทอ. และ นขต.ทสส.ทอ.

สำเนาถูกต้อง

น.อ.

(ธคุณ มุ่งเพียร)

รอง จก.ทสส.ทอ.

๒๗ พ.ย.๕๒

นางเสมอดาว ฯ พิมพ์/ทาน

น.อ.ณัฐพล ฯ ตรวจ

ผนวก ก

หน้าที่การรักษาความปลอดภัยระบบสารสนเทศแบ่งตามบทบาท

๑. ผู้บริหารระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอฟต์แวร์ระบบเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๑.๑ บริหารและดูแลอุปกรณ์คอมพิวเตอร์ ซึ่งเป็นแม่ข่ายบริการแก่หน่วยต่าง ๆ ของส่วนราชการ

๑.๒ ควบคุมและตรวจสอบการใช้งานระบบ

๑.๓ ตรวจสอบ ควบคุม ดูแล การบำรุงรักษาระบบ

๑.๔ รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งาน

๒. ผู้บริหารฐานข้อมูล (Database Administrator) มีความรู้ด้านการจัดการฐานข้อมูลระบบคอมพิวเตอร์เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๒.๑ ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดู

๒.๒ เลือก ตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๒.๓ รักษาความปลอดภัยฐานข้อมูล เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ฐานข้อมูล

๒.๔ ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๒.๕ ควบคุม และบริการการใช้งานฐานข้อมูล

๓. ผู้บริหารเครือข่าย (Network Administrator) มีความรู้ด้านฮาร์ดแวร์ การสื่อสารข้อมูลและอุปกรณ์ในระบบเครือข่ายเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๓.๑ กำหนดเลขที่อยู่ไอพี (IP Address) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการโดยประสานกับส่วนราชการหรือผู้บริหารระบบเครือข่ายคอมพิวเตอร์ของกองทัพอากาศ

๓.๒ กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้ภายในเครือข่ายที่รับผิดชอบ

๓.๓ ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๓.๔ ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย

๓.๕ รักษาความปลอดภัยระบบเครือข่าย เช่น รักษาความลับ ความคงสภาพกำหนดการเข้ารหัส และความพร้อมใช้งานให้ระบบเครือข่าย

๔. ผู้เขียน...

๔. ผู้เขียนโปรแกรม (Programmer) มีความรู้เรื่องระบบคอมพิวเตอร์ การเขียนโปรแกรมคอมพิวเตอร์และฐานข้อมูลเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๔.๑ เขียนและพัฒนาโปรแกรมที่ได้รับมอบหมาย

๔.๒ จัดหาข้อมูลเพื่อทดสอบโปรแกรม

๔.๓ ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

๔.๔ รักษาความปลอดภัยโปรแกรม เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งานให้โปรแกรม

ผนวก ข

คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

๑. Account ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: บัญชีผู้ใช้

อธิบายความหมาย

: เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกัน มีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกัน เพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชี หรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

๒. Application ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การประยุกต์

อธิบายความหมาย

: งานที่ทำด้วยโปรแกรมคอมพิวเตอร์ หรือระบบคอมพิวเตอร์เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ เช่น งานออกแบบโครงสร้างทางวิศวกรรม งานพยากรณ์ทางธุรกิจ งานด้านการจัดการสถานพยาบาล เป็นต้น การประยุกต์ มีความหมายรวมถึงโปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) และซอฟต์แวร์ประยุกต์ (Application Software)

๓. Computer Network ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: เครือข่ายคอมพิวเตอร์, ข่ายงานคอมพิวเตอร์

อธิบายความหมาย

: เป็นคำกล่าวโดยทั่ว ๆ ไปของการเชื่อมต่อสื่อสารกันระหว่างระบบคอมพิวเตอร์ตั้งแต่ ๒ ระบบขึ้นไป หรือระหว่างเครื่องคอมพิวเตอร์กับเครื่องปลายทาง (Terminals) ทั้งหลาย เพื่อให้สามารถนำข้อมูล โปรแกรมรวมทั้งอุปกรณ์รอบข้างมาใช้งานร่วมกันได้ โดยมีอุปกรณ์ในระบบสื่อสารเป็นตัวเชื่อมโยง

๔. Decryption / Encryption ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: การถอดรหัสลับ / เพื่อการเข้ารหัสลับ

อธิบายความหมาย

: การถอดรหัสลับ (Decryption)

(๑) กระบวนการนำข้อความ (Message) ที่ผ่านการเข้ารหัสลับ (Encrypted) แล้วมาแปลงกลับให้เป็นข้อความดั้งเดิม (Original Meaningful Message) หรือข้อความธรรมดา (Plaintext) เป็นความหมายที่ตรงกันข้ามกับคำว่า การเข้ารหัสลับ

(๒) กระบวน...

(๒) กระบวนการที่ตรงข้าม คือ การแปลงข้อความที่เข้ารหัสลับแล้วให้กลับไปอยู่ในรูปแบบปกติ คำที่มีความหมายเหมือนกันคือ เข้ารหัส (Encode) และถอดรหัส (Decode) หรือ เข้ารหัส (Encipher) และถอดรหัส (Decipher) ซึ่งใช้แทนคำว่า เข้ารหัส (Encrypt) และถอดรหัส (Decrypt) และเรียกระบบที่มีการเข้ารหัสลับและถอดรหัสลับว่า ระบบการเข้ารหัสลับ (Cryptosystem)

: การเข้ารหัสลับ (Encryption)

(๑) เป็นขบวนการเข้ารหัสให้ข้อความเพื่อทำให้ไม่ทราบความหมายที่แท้จริงของข้อความดังกล่าว

(๒) กระบวนการเข้ารหัส (Encode) หรือการเข้ารหัสลับ (Encryption) ให้แก่ข้อมูล (Data) ใด ๆ ก็ตามซึ่งต้องการรหัสเฉพาะเจาะจง (Specific Code) หรือ กุญแจ (Key) สำหรับการแปลงให้กลับมาเป็นข้อมูลดั้งเดิม (Original data)

(๓) เป็นการเข้ารหัสข้อมูลสื่อสาร (Communication Data)

๕. Decryption Key / Encryption Key ยังไม่มีการกำหนดไว้ในศัพท์คอมพิวเตอร์ฉบับราชบัณฑิตยสถาน

: กุญแจเพื่อการถอดรหัสลับ / กุญแจเพื่อการเข้ารหัสลับ

อธิบายความหมาย

: เป็นคำศัพท์สำหรับการเข้ารหัสแบบกุญแจสาธารณะ (Public Key System) ประกอบด้วยไฟล์คอมพิวเตอร์คู่หนึ่ง คือ กุญแจสาธารณะ (Public Key) ใช้ในการเข้ารหัสลับ ซึ่งไฟล์สำหรับการเข้ารหัสคือ Encryption Key และ กุญแจลับ (Secret Key) ใช้เมื่อถอดรหัสลับ ซึ่งไฟล์สำหรับการถอดรหัสคือ Decryption Key

๖. Hardware ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. ส่วนเครื่อง, ฮาร์ดแวร์

: ๒. ส่วนอุปกรณ์, ฮาร์ดแวร์

อธิบายความหมาย

: ระบบคอมพิวเตอร์ส่วนที่เป็นอุปกรณ์ทางกายภาพ เช่น อิเล็กทรอนิกส์ แม่เหล็ก และเครื่องจักรกล แสดงให้เห็นถึงความแตกต่างของฮาร์ดแวร์และซอฟต์แวร์ ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์เช่นเดียวกัน

๗. Log File ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: แฟ้มลงบันทึกเข้าออก

อธิบายความหมาย

: เป็นการบันทึกการปฏิบัติทั้งหมดของอุปกรณ์ที่เกี่ยวข้องกับการประมวลผลข้อมูล (Data Processing Equipment) จะบันทึกงานทุกงานหรือการดำเนินการ (Run) ตามลำดับที่เกิดขึ้น เวลาเริ่มต้นและสิ้นสุดของแต่ละงาน รวมทั้งกิจกรรมที่ทำ ทั้งนี้เพื่อนำมาตรวจสอบความถูกต้องของการใช้งานได้ในภายหลัง

๘. Malicious Code ยังไม่กำหนดความหมายไว้ในศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: โปรแกรมประสงค์ร้าย

อธิบายความหมาย

: โปรแกรมหรือส่วนของโปรแกรมที่สร้างขึ้น และเผยแพร่โดยผู้มีเจตนาร้ายมุ่งทำลายอย่างใดอย่างหนึ่งต่อสิ่งที่เป็นเป้าหมาย โดยทั่วไปโปรแกรมประสงค์ร้ายจะแบ่งตามลักษณะ การแพร่กระจายและการกระทำได้ ๕ ประเภท คือ

๘.๑ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมหรือส่วนของโปรแกรมที่ผู้เขียนมีวัตถุประสงค์ในการทำลายอย่างใดอย่างหนึ่ง หนทางเข้าสู่ระบบคอมพิวเตอร์โดยการเกาะติดกับโปรแกรมที่ใช้งานทั่ว ๆ ไปภายในระบบคอมพิวเตอร์และทำให้โปรแกรมเป้าหมายที่อาศัยอยู่นั้นกลายเป็นโปรแกรมประสงค์ร้ายด้วย ไวรัสคอมพิวเตอร์แพร่กระจายโดยสำเนาตัวเอง (Copy) ไปเกาะติดกับโปรแกรมต่าง ๆ เพื่อให้โปรแกรมเหล่านั้นนำพาไปยังส่วนต่าง ๆ ของระบบเพื่อจะได้แพร่กระจายไปสู่โปรแกรมอื่น ๆ ที่ยังไม่มีโปรแกรมไวรัสเกาะอยู่ ซึ่งการแพร่กระจายจะเป็นลักษณะทวีคูณ ทำลายเป้าหมายได้ทุกรูปแบบตามเจตนาของผู้เขียนโปรแกรม ไวรัสคอมพิวเตอร์มักจะแบ่งประเภทตามแหล่งที่อาศัยภายในระบบหรือโปรแกรมที่จะกระทำการโดยเฉพาะ เช่น ไวรัสในส่วนการปลุกเครื่อง (Boot Sector Virus) มาโครไวรัส (Macro Virus) เป็นต้น ไวรัสคอมพิวเตอร์จะกระทำการ (Active) ได้ก็ต่อเมื่อโปรแกรมเป้าหมายที่โปรแกรมไวรัสอาศัยอยู่มีการดำเนินการ (Run/Process)

๘.๒ หนอน (Worm) เป็นโปรแกรมที่สามารถสำเนาตัวเอง (Copy) ให้แพร่กระจายในระบบเครือข่าย และสามารถกระทำการ (Active) ต่าง ๆ ได้โดยลำพัง ไม่ต้องอาศัยโปรแกรมอื่น ๆ ในการนำพาไปยังส่วนต่าง ๆ ของระบบ ทำลายระบบโดยการสำเนาตัวเองเพิ่มขึ้นเรื่อย ๆ จนระบบไม่สามารถทำงานต่อไปได้

๘.๓ ตัวลวง...

๘.๓ ตัวลวง หรือ ม้าโทรจัน (Trojan Horse) เป็นโปรแกรม หรือส่วนของโปรแกรมที่ถูกนำมาซ่อนไว้ในโปรแกรมใช้งานโปรแกรมใดโปรแกรมหนึ่งภายในระบบโดยผู้ใช้ไม่ทราบและคิดว่าเป็นโปรแกรมที่ใช้งานตามปกติ มักกระทำโดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องกับการบำรุงรักษาโปรแกรม เช่น โปรแกรมม้าโทรจันที่แทรกมากับบท (คำสั่ง) ลงบันทึกเข้า (Login Script) ที่รอให้บริการแก่ผู้ใช้ที่ต้องการเข้าสู่ระบบใดระบบหนึ่ง โดยการใส่บัญชีผู้ใช้และรหัสผ่าน ซึ่งนอกจากทำหน้าที่ตรวจสอบความถูกต้องแท้จริงในการเข้าระบบของผู้ใช้แล้วยังแอบสำเนาบัญชีผู้ใช้และรหัสผ่านดังกล่าวเก็บไว้ใช้ประโยชน์ส่วนตัวในภายหลัง

ม้าโทรจันไม่สามารถเคลื่อนย้ายหรือสำเนาตัวเองได้ บางครั้งใช้เป็นที่พรางตัวของโปรแกรมประสงค์ร้ายอื่น ๆ มักเป็นไปในลักษณะของการเชิญชวนให้เกิดความสนใจและนำโปรแกรมดังกล่าวบรรจุเข้าในระบบ ซึ่งผู้ใช้เองที่นำม้าโทรจันเข้าสู่ระบบโดยไม่เจตนา เช่น เกมส์คอมพิวเตอร์ (Computer Game) โปรแกรมอรรถประโยชน์ (Utility Program) ภาพอนาจาร (Nude) เป็นต้น ซึ่งโปรแกรมเหล่านี้เมื่อบรรจุเข้าระบบได้แล้วก็อาจแพร่ไวรัสหรือโปรแกรมประสงค์ร้ายอื่น ๆ ได้

๘.๔ กับดัก (Trap Door) เป็นโปรแกรมที่สร้างให้มีหนทางลับหรืออภิสิทธิ์ในการเข้าสู่ระบบ โปรแกรมหรือข้อมูลเป้าหมายได้เฉพาะบุคคล และตลอดเวลาที่ต้องการ โดยปกติมีวัตถุประสงค์ให้ผู้ควบคุมระบบใช้เป็นทางเข้าเพื่อดูแล บำรุงรักษา หรือตรวจสอบระบบ เช่น โปรแกรมของเครื่องรับจ่ายเงินอัตโนมัติ (Automatic Teller Machine) กำหนดให้รหัสผ่าน ๙๙๙๙ เป็นรหัสผ่านที่สามารถเข้าถึงการบันทึกเข้าออก (Log) ของรายการเปลี่ยนแปลง (Transaction) ยอดเงินฝากเข้าลูกค้า

กับดักกระทำได้โดยผู้พัฒนาโปรแกรมหรือบุคคลอื่นที่เกี่ยวข้องในช่วงที่กำลังพัฒนาโปรแกรมซึ่งอาจสร้างทางลับเพื่อหาประโยชน์อย่างใดอย่างหนึ่งจากระบบในภายหลังจากตัวอย่างข้างต้นเมื่อสามารถเข้าสู่แฟ้มบันทึกเข้าออก (Log File) ของรายการเปลี่ยนแปลงได้แล้วอาจสร้างโปรแกรมให้มีการโอนเงินหลังจุดทศนิยมจากรายการเปลี่ยนแปลงมาสะสมไว้ในบัญชีลับบัญชีใดบัญชีหนึ่งได้

๘.๕ ระเบิด (Bomb) เป็นโปรแกรมที่มีเจตนาร้ายอย่างใดอย่างหนึ่ง จะดำเนินการเมื่อมีเหตุการณ์ตรงตามเงื่อนไขเกิดขึ้น ได้แก่ เงื่อนไขเวลา วันที่ หรือเงื่อนไขอื่น ๆ เช่น โปรแกรมกำหนดให้จัดรูปแบบจานบันทึกแบบแข็ง (Format Hard Disk) เมื่อมีผู้เข้าใช้ระบบที่มีบัญชีผู้ใช้ขึ้นต้นด้วยอักษร “ S” ครบ ๕๐ ครั้ง เป็นต้น

อย่างไรก็ตามปัจจุบันโปรแกรมประสงค์ร้ายได้มีการพัฒนาความสามารถในการทำลาย และการหลบหลีกการตรวจจับของโปรแกรมป้องกันต่าง ๆ อยู่เสมอ ดังนั้นในอนาคตจะปรากฏโปรแกรมประสงค์ร้ายในรูปแบบที่มีการผสมผสานกันหลาย ๆ ประเภทมากยิ่งขึ้น

๙. Password ความหมาย ในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: รหัสผ่าน

อธิบายความหมาย

: เป็นชุดของตัวอักษรหรือคำพิเศษ (Special Word) หรือวลี (Phase) ซึ่งให้สิทธิในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน นอกจากนี้รหัสผ่านยังเป็นเครื่องมือรักษาความปลอดภัยที่ใช้แสดงต่อระบบคอมพิวเตอร์เพื่อให้การรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้ และตรวจสอบสิทธิในการใช้งานระบบ (Access to its Resources) ดังนั้นจึงต้องมีการกำหนดระเบียบปฏิบัติให้ผู้ใช้สามารถจัดการรหัสผ่านของตนเองได้อย่างปลอดภัยและถูกต้อง

๑๐. Program ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ๑. โปรแกรม, ชุดคำสั่ง

: ๒. สร้างโปรแกรม

อธิบายความหมาย

: เป็นชุดคำสั่งที่ต่อเนื่องกันเป็นลำดับเพื่อให้คอมพิวเตอร์ประมวลผลในลักษณะที่ต้องการ อาจอยู่ในรูปของการเขียนโปรแกรมด้วยภาษาระดับสูง (High-Level) ซึ่งต้องผ่านการแปลความหมายให้เป็นรหัสจุดหมาย (Object Code) ก่อน คอมพิวเตอร์จึงประมวลผลได้ หรืออาจอยู่ในรูปของรหัสจุดหมาย (Object Code) ซึ่งสามารถสั่งให้คอมพิวเตอร์ประมวลผลได้โดยตรง โปรแกรมคอมพิวเตอร์โดยทั่วไป แบ่งเป็น ๒ ประเภท คือ

- โปรแกรมระบบ (System Program) ได้แก่ โปรแกรมระบบปฏิบัติการ (Operating System Program) โปรแกรมบรรจุ (Loader, Loading Program) ตัวแปลโปรแกรม หรือโปรแกรมแปลโปรแกรมหรือคอมไพเลอร์ (Compiler) เป็นต้น โปรแกรมเหล่านี้ช่วยอำนวยความสะดวกในการใช้งานคอมพิวเตอร์

- โปรแกรมประยุกต์ หรือโปรแกรมใช้งาน (Application Program) เป็นโปรแกรมที่สร้างขึ้นโดยมีวัตถุประสงค์เพื่อการใช้งานในลักษณะใดลักษณะหนึ่งโดยเฉพาะ เช่น โปรแกรมประมวลผลคำ (Word Processing) - สารบรรณ - ธุรการ โปรแกรมทางธุรกิจ - การเงิน - การธนาคาร โปรแกรมเกี่ยวกับงานวิจัย - การศึกษา - การพยากรณ์ โปรแกรมควบคุมการทำงานของอุปกรณ์ - เครื่องมือเฉพาะอย่าง เป็นต้น โปรแกรมเหล่านี้มักจะเขียนด้วยภาษาระดับสูง และใช้ประโยชน์เพียงกลุ่มผู้ใช้บางกลุ่มเท่านั้น รวมทั้งต้องมีการปรับปรุงเปลี่ยนแปลงโปรแกรมเพื่อให้ใช้งานได้ทันสมัยอยู่เสมอ

๑๑. Removable Storage Devices สื่อบันทึกข้อมูลที่เคลื่อนที่ได้ หมายถึง อุปกรณ์เชื่อมต่อใด ๆ ที่สามารถเก็บข้อมูลได้ เช่น External Hard Disk, USB Drive, เครื่องเล่น MP3, หรือ อื่น ๆ

๑๒. Software...

๑๒. Software ความหมายในภาษาไทยตามศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน

: ส่วนชุดคำสั่ง ซอฟต์แวร์

อธิบายความหมาย

: เป็นคำที่ใช้เรียกโปรแกรมหรือโปรแกรมคอมพิวเตอร์โดยทั่วไป ต้องการแสดงให้เห็นถึงความแตกต่างระหว่าง ฮาร์ดแวร์ และซอฟต์แวร์ซึ่งเป็นองค์ประกอบของระบบคอมพิวเตอร์

: เป็นคำสั่งที่อยู่ในรูปภาษาเครื่อง (Machine Language) ซึ่งเป็นภาษาระดับต่ำ (Low-Level) ที่หน่วยประมวลผลกลางของคอมพิวเตอร์สามารถเข้าใจและประมวลผลตามคำสั่งนั้นได้ทันที โดยทั่วไปมี ๒ ประเภท คือ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System Software) และซอฟต์แวร์ประยุกต์ (Application Software)