สงครามข้อมูลข่าวสารกับการประยุกต์ใช้

(ตอนที่ ๑)

(Information Warfare and Application)

น.อ.ภาณุฤทธิ์ ยุกตะทัต

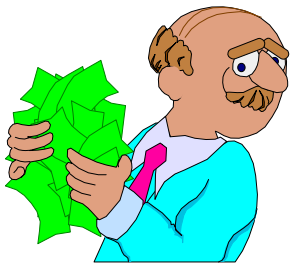
รองผู้อำนวยการกองวิชาวิศวกรรมเครื่องกลเรือ ฝ่ายศึกษา โรงเรียนนายเรือ

---

๑. สงครามข้อมูลข่าวสาร คืออะไร?

นิยามของคำว่าสงครามข้อมูลข่าวสาร (Information Warfare) ที่กำหนดโดยกระทรวงกลาโหมสหรัฐ หมายถึง "*Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks*."

สงครามข้อมูลข่าวสาร (Information Warfare) เป็นการต่อสู้อย่างหนึ่งที่กำลังเกิดขึ้นในปัจจุบันและกำลังทวีรุนแรงเพิ่มมากขึ้น ทั้งในด้านการทหารและทางพลเรือน เนื่องจากระบบการปฏิบัติงานของหน่วยงาน และองค์กรต่าง ๆ ของประเทศที่ได้รับการพัฒนาแล้ว มักจะใช้ระบบข้อมูลข่าวสารที่มีประสิทธิภาพ เป็นสื่อกลาง และเป็นหัวใจในการปฏิบัติงานได้อย่างถูกต้องและรวดเร็ว ซึ่งในความเป็นจริงแล้ว การประยุกต์ใช้ระบบข้อมูลข่าวสารนี้ก่อให้เกิดข้อดีต่อหน่วยงานหรือองค์กรนั้น ๆ อย่างมหาศาล เพียงแต่ว่าในตอนเริ่มออกแบบสร้างระบบในครั้งแรก โดยมากเรามักจะคำนึงถึงขีดความสามารถในการเข้าถึงข้อมูลต่าง ๆ ได้อย่างรวดเร็ว และให้คนหมู่มากสามารถเข้าถึงข้อมูลได้โดยง่าย มักจะไม่ค่อยคำนึงถึงการ ปกป้องข้อมูลที่ถูกส่งผ่านระบบสารสนเทศนั้น ๆ ดังนั้นการใช้งานระบบสารสนเทศในยุคต่อมาจึงมักเกิดปัญหาทางด้านการรักษาความปลอดภัย และการรั่วไหลของข้อมูลที่สำคัญ รวมทั้งระบบยังสามารถถูกโจมตีได้โดยง่ายอีกด้วย โดยทั่วไปเราจะแบ่งประเภทของการประยุกต์ใช้สงครามข้อมูลข่าวสารออกเป็น ๒ ประเภทคือ **Cyberwar** คือการประยุกต์ใช้ระบบข้อมูลข่าวสารเพื่อปฏิบัติการทางทหาร โดยมีจุดมุ่งหมาย ทางการทหาร (Military Objective) เป็นสำคัญ และ **Netwar** คือการรบกวน หรือการโจมตีระบบข้อมูลข่าวสารโดยมิได้มีจุดมุ่งหมายทางการทหารเป็นหลัก แต่มีจุดประสงค์อื่นที่ไม่เกี่ยวข้องกับการปฏิบัติการทางทหารเป็นจุดประสงค์หลัก



๒. ความเสียหายอันเกิดจากระบบข้อมูลข่าวสารที่ไม่ปลอดภัย

การที่หน่วยงานหรือองค์กรไม่สามารถที่จะรักษาความปลอดภัยในระบบข้อมูลข่าวสารได้อย่างมีประสิทธิภาพนั้น จะก่อให้เกิดความเสียหายอย่างใหญ่หลวง ตัวอย่างที่เห็นได้ชัดประการหนึ่งก็คือ กระทรวงการคลังของสหรัฐอเมริกา ซึ่งใช้ระบบการโอนเงินผ่านเครือข่ายแบบ ETF – Electronic Fund Transfer เป็นจำนวนถึง ๑.๗ ล้านล้านเหรียญ ในแต่ละปี และหากสมมติว่าระบบนี้มีการรั่วไหล หรือมีการโจมตีผ่านระบบนี้ขึ้นมา ก็จะเกิดความเสียหายอย่างใหญ่หลวงต่อระบบเศรษฐกิจในภาพรวมของสหรัฐอเมริกาเป็นอย่างยิ่ง ตัวอย่างของความเสียหายที่เกิดขึ้นกับระบบข้อมูลข่าวสารที่สำคัญ คือ

- บริษัท MCI ซึ่งเป็นบริษัทยักษ์ใหญ่ในแวดวงของการสื่อสาร ถูกลักขโมยบัตรเครดิต ก่อให้เกิดความเสียหายเป็นมูลค่าถึง ๕๐ ล้านเหรียญ
- ระบบคอมพิวเตอร์ของกระทรวงกลาโหมสหรัฐอเมริกา ถูกโจมตี และถูกทำให้ไม่สามารถใช้งานได้หลายครั้ง แต่ครั้งที่น่าสนใจคือได้มีการสนับสนุนปฏิบัติการนี้อย่างลับ ๆ จากองค์กรอาชญากรรมข้ามชาติ หรือสายลับของฝ่ายตรงข้าม
- ในเดือน ม.ค.๒๕๔๖ ไวรัส MyDoom ซึ่งเป็นหนอนคอมพิวเตอร์ ได้ถูกแพร่เข้ามาทาง E-mail และทำให้เกิดการร้องขอ (Request) ไปยังเว็บไซต์เป้าหมาย จนกระทั่งเกิดความหนาแน่นในช่องทางสื่อสารของระบบเครือข่าย จนกระทั่งระบบล้ม
- ในเดือน เม.ย.๒๕๔๖ ไวรัส Sasser ได้ถูกแพร่เข้ามาทำลายเครื่องแม่ข่ายกว่า ๑๘๐ ล้านเครื่องทั่วโลก โดยมุ่งเน้นเครื่องที่ใช้ระบบปฏิบัติการ Microsoft Windows 2003 Server ก่อให้เกิดความเสียหายคิดเป็นมูลค่าหลายร้อยล้านเหรียญ

๓. ส่วนประกอบของระบบสงครามข้อมูลข่าวสาร

เนื่องจากระบบข้อมูลข่าวสาร เป็นระบบที่มีความสลับซับซ้อนเป็นอย่างมาก เพราะจะประกอบด้วยเทคโนโลยีหลายส่วนมาประกอบกันเป็นระบบ ดังนั้นหากเราต้องพิจารณาในเรื่องของการทำสงคราม ข้อมูลข่าวสาร เราจะต้องพิจารณาให้ครบในทุกมุมมอง ซึ่งมีส่วนประกอบที่สำคัญ ดังนี้

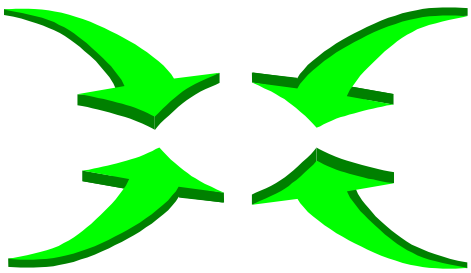
๓.๑ Information Collection : ก่อนที่จะมีการปฏิบัติการใด ๆ จะต้องมีการเก็บรวบรวมข้อมูลที่จำเป็นเสียก่อน จึงจะสามารถทำการตัดสินใจปฏิบัติการใด ๆ ได้อย่างมีประสิทธิภาพ ขั้นตอนการทำงานในชั้นนี้ก็จะรวมถึง การวางแผนในการเสาะหาข้อมูล การปฏิบัติงานตามแผนที่วางไว้ และสุดท้ายก็คือการติดตามผลการปฏิบัติ ซึ่งในการสืบเสาะหาข้อมูลสิ่งสำคัญที่ต้องคำนึงถึงสำหรับข้อมูลที่ได้มานั้นก็คือ ข้อมูลจะต้องถูกต้องและครบถ้วน อีกทั้งยังต้องเป็นข้อมูลที่ทันสมัยต่อเหตุการณ์ด้วย

๓.๒ Information Protection : เมื่อหน่วยปฏิบัติการได้รับข้อมูลข่าวสารมาแล้ว ขั้นตอนต่อไปที่มีความสำคัญก็คือ การปกป้องข้อมูลเหล่านั้นในแง่ของไม่ให้เกิดการรั่วไหลไปสู่มือของฝ่ายตรงกันข้าม และการป้องกันไม่ให้ข้อมูลที่สำคัญเหล่านั้นถูกทำลายลงโดยฝ่ายตรงกันข้าม ดังนั้นสิ่งสำคัญที่ต้องปฏิบัติก็คือ การป้องกันจุดอ่อน (Vulnerability) ของระบบข้อมูลข่าวสารนั้น ๆ เพื่อมิให้ศัตรูสามารถใช้จุดอ่อนที่มีอยู่นั้นได้

๓.๓ Information Denial : คือการทำให้ศัตรูหรือฝ่ายตรงกันข้าม ไม่สามารถที่จะใช้ระบบข้อมูลข่าวสารนั้น ๆ ในการปฏิบัติงานได้ การปฏิเสธการใช้งานของฝ่ายตรงกันข้ามนี้สามารถทำได้ ๒ อย่าง คือ การโจมตีระบบข้อมูลข่าวสารโดยตรง หรือการลวงให้ข้อมูลข่าวสารที่ไม่ถูกต้องแก่ศัตรู

๓.๔ Information Management : สิ่งหนึ่งที่สำคัญก็คือ ระบบการจัดการที่ใช้ในการจัดการกับข้อมูลข่าวสาร ต้องเป็นระบบที่ดี เพราะหากระบบการจัดการไม่ดีแล้วนั้น ก็ยากที่จะประสบความสำเร็จในการทำสงครามทางด้านข้อมูลข่าวสาร ในปัจจุบันการใช้ระบบข้อมูลข่าวสารมักจะใช้ปรัชญาแบบ Decentralized ซึ่งมีผลให้การใช้ระบบนั้นมีความรวดเร็วและยากต่อการโจมตี แต่อย่างไรก็ตามขั้นตอนในการใช้งาน และการตรวจสอบก็จะต้องระมัดระวังเป็นพิเศษ เนื่องจากข้อมูลมีการกระจายออกไปยังส่วนต่าง ๆ นั่นเอง และระบบการจัดการที่ดีนั้นจะต้องคำนึงถึงว่า ข้อมูลนั้นอยู่ที่ใด อยู่กับใคร และมีขั้นตอนการใช้และการปกป้องที่ดีเพียงพอ หรือไม่

๓.๕ Information Transport : สิ่งที่เป็นหัวใจสำคัญอย่างยิ่งของระบบข้อมูลข่าวสารนั้นก็คือการขนส่งข้อมูลข่าวสารอย่างถูกต้อง รวดเร็ว และปลอดภัย ซึ่งระบบการขนส่งข้อมูลข่าวสารจะต้องอาศัยความเป็นหนึ่งเดียวกัน (Homogeneous) ในด้านการประสานงานระหว่างส่วนต่าง ๆ แทบจะทั้งหมดในระบบ ความรวดเร็วเป็นส่วนประกอบที่สำคัญอย่างยิ่งยวดในการตอบสนองการปฏิบัติการที่ทันต่อเหตุการณ์ (Responsiveness) หากระบบการขนส่งข้อมูลข่าวสารนี้มีข้อบกพร่อง หรือไม่สมบูรณ์แล้ว ก็จะทำให้ง่ายต่อการโจมตี หรือขโมยข้อมูลจากฝ่ายตรงกันข้ามได้



๔. การปฏิบัติในการทำสงครามข้อมูลข่าวสาร

ตัวอย่างที่เกี่ยวกับการปฏิบัติงานด้านการทำสงครามข้อมูลข่าวสาร มีดังต่อไปนี้

๔.๑ Electronic Warfare (EW) ประกอบด้วยส่วนประกอบที่สำคัญ คือ การโจมตีทางด้านอิเล็กทรอนิกส์ การสนับสนุนทางด้านอิเล็กทรอนิกส์ และการป้องกันทางด้านอิเล็กทรอนิกส์ การทำสงครามอิเล็กทรอนิกส์นั้นจะยังผลให้เกิดการปฏิเสธการใช้งานของฝ่ายตรงข้ามต่อข้อมูลที่จำเป็น

๔.๒ C2W (Command and Control Warfare) คือการปฏิบัติการเพื่อต่อต้านการทำงานของระบบ หรือหน่วยงานบังคับบัญชาของฝ่ายตรงข้าม

๔.๓ Direct Energy (Lasers, Particle Beams, High-power Microwaves) สามารถที่จะนำมาใช้เพื่อการทำลายระบบ Software และ Hardware ของฝ่ายตรงข้ามได้

๔.๔ Unauthorized Access คือ การเจาะระบบข้อมูลข่าวสารของฝ่ายตรงข้ามเพื่อล้วงความลับของฝ่ายตรงข้ามโดยไม่ให้รู้ตัว

๔.๕ Intrusion คือการเจาะระบบฝ่ายตรงข้ามโดยมีวัตถุประสงค์ร้ายในการวางกับดัก หรือการใช้ Malicious Program เพื่อทำลายระบบข้อมูลข่าวสารของฝ่ายตรงข้าม

๔.๖ Modification, Substitution and Destruction คือการเปลี่ยนแปลง หรือแกล้งดัดแปลงแก้ไขข้อมูลข่าวสาร โดยมีวัตถุประสงค์เพื่อการลวงฝ่ายตรงข้าม

๔.๗ Signal Intelligence คือ การตรวจสอบการทำงานโดยละเอียดของระบบการปฏิบัติงานของฝ่ายตรงข้ามว่ามีการทำงานอย่างไร ในเวลาใด ขนาดของการทำการวิเคราะห์ข้อมูลเป็นอย่างไร เป็นต้น ซึ่งข้อมูลเหล่านี้บางครั้งจะมีความสำคัญเป็นอย่างมากต่อ Intelligence Information

๔.๘ Spoofing คือการเติมใส่โปรแกรม หรือข้อมูลเข้าไป เพื่อจุดประสงค์ในการขโมยความลับของข้อมูลนั้นๆ

๔.๙ Masquerading คือการปลอมแปลงเข้าไปในระบบโดยการแกล้งว่าเป็นผู้ใช้ที่ได้รับอนุญาตที่ถูกต้อง

๔.๑๐ Deception คือการเพิ่มความไม่แน่นอนทางด้านความถูกต้องของข้อมูลให้แก่ข้อมูลข่าวสารของฝ่ายตรงข้าม ยังผลให้ฝ่ายตรงข้ามใช้ข้อมูลข่าวสารได้ยาก และมีข้อผิดพลาด

๔.๑๑ Psychological Operations (PSYOPS) คือการป้อนข้อมูลข่าวสารที่ผิดพลาดเพื่อเป็นการลวง และยังผลให้ฝ่ายตรงข้ามมีการตัดสินใจที่ผิดพลาด

๔.๑๒ Denial of Service คือการปฏิเสธการใช้งานของระบบข้อมูลข่าวสารของฝ่ายตรงข้าม

๕. การประยุกต์ใช้ไวรัสคอมพิวเตอร์ (Computer Viruses) ในระบบสงครามข้อมูลข่าวสาร

ในปัจจุบันการใช้ไวรัสคอมพิวเตอร์สามารถที่จะก่อให้เกิดความเสียหายให้กับระบบคอมพิวเตอร์เน็ตเวิร์คได้อย่างมหาศาลในระยะเวลาอันรวดเร็ว ดังนั้นจึงก่อให้เกิดระบบการสงครามชนิดใหม่ขึ้นมาในสาขาของระบบการทำสงครามอิเล็กทรอนิกส์ โดยการใช้โปรแกรม Microcode จำพวกนี้ เพื่อจุดประสงค์ในการทำลายระบบข้อมูลข่าวสารของฝ่ายตรงข้าม หากจะเปรียบเทียบไวรัสคอมพิวเตอร์กับระบบการทำสงครามอิเล็กทรอนิกส์แบบเก่า ๆ นั่นคือ ECM (Electronic Counter Measure) แล้ว ไวรัสคอมพิวเตอร์จะมีการทำงานคล้ายๆ กับระบบ ECM เพียงแต่ว่าระบบ ECM นั้นมุ่งเน้นที่จะทำลาย หรือรบกวนระบบการรับสัญญาณของฝ่ายตรงข้ามเท่านั้น ในขณะที่ไวรัสคอมพิวเตอร์มุ่งเน้นที่จะทำลายส่วนที่สำคัญของระบบ ไม่ว่าจะเป็นหน่วยประมวลผลของระบบปฏิบัติการนั้น ๆ หรือระบบการขนส่งข้อมูล ตารางต่อไปนี้จะแสดงการเปรียบเทียบระหว่างระบบทั้งสอง

	ECM แบบเดิม	**ไวรัสคอมพิวเตอร์**
ระบบเป้าหมาย	ระบบตรวจจับ (Sensor) ระบบควบคุม ระบบสื่อสาร	ระบบคอมพิวเตอร์ และ ระบบเครือข่าย คอมพิวเตอร์
เป้าหมายสำคัญ	ส่วนรับสัญญาณ	ส่วนควบคุม การปฏิบัติงาน (Processor)
การโจมตีโดยการรบกวนระบบ	ใช้ Noise ใช้ Deception Signals	ใช้การลวง (Deception) ใช้วิธีการสร้างการรบกวนระบบ
การนำไปปฏิบัติ	ใช้ระบบอนาล็อกเป็นส่วนใหญ่	ใช้ระบบดิจิตอล

๖. การป้องกันพื้นฐาน

เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลจากระบบข้อมูลข่าวสาร หรือจากระบบสารสนเทศ ทางกระทรวงกลาโหมสหรัฐได้มีการนำมาตรฐานเทคโนโลยี TEMPEST มาใช้เพื่อเป็นการปกป้องการรั่วไหลของข้อมูล จากการลอบดักฟังข้อมูลที่เรียกว่า “Electromagnetic Eavesdropping” ข้อมูลที่รั่วไหลได้ในลักษณะนี้ ก็เนื่องมาจากอุปกรณ์ที่ใช้ในการวิเคราะห์ข้อมูลข่าวสาร มักจะปล่อยสัญญาณแม่เหล็กไฟฟ้าที่บ่งบอกถึงข้อมูลที่กำลังทำการวิเคราะห์เหล่านั้นออกมา ดังนั้นเทคโนโลยี TEMPEST จึงถูกนำมาใช้ในการป้องกันการรั่วไหลของข้อมูลในลักษณะดังกล่าว อย่างไรก็ตามถึงแม้ว่าประเทศไทยยังไม่มีการนำ

เทคโนโลยี TEMPEST มาใช้ในการป้องกันการรั่วไหลของข้อมูล แต่กระทรวงกลาโหม โดยกองบัญชาการทหารสูงสุดได้มีการกำหนดมาตรฐานการรักษาความปลอดภัยเทคโนโลยีสารสนเทศของกองทัพไทยไว้ในระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พุทธศักราช ๒๕๔๖ โดยจำแนกเป็นการรักษาความปลอดภัยส่วนประกอบต่าง ๆ ๙ ประการของระบบสารสนเทศ ดังนี้

๖.๑ มาตรฐานการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

๖.๑.๑ มาตรฐานการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ให้บริการ หรือเครื่องแม่ข่าย (Server)

๖.๑.๒ ต้องกำหนดให้มีการทำ Network Segmentation เพื่อให้เกิด Server Security Zone เช่น การแบ่ง Segment ที่เป็น External Public Services, Internal Non Critical Services และ Internal Critical Services ออกจากกัน และจัดให้มีการตรวจจับการบุกรุกเข้าสู่ระบบที่เป็น Critical Application อย่างสม่ำเสมอ

๖.๑.๓ ต้องมีบันทึกการ Hardening หรือ Configuration set up ของอุปกรณ์ Server ทุกครั้งที่ติดตั้ง Critical Application หรือเมื่อมีการเปลี่ยนแปลง

๖.๑.๔ ต้องมีบันทึกการติดตั้ง Service Patch ทุกครั้ง

๖.๑.๕ System Administrator ต้องไม่ใช้ Default Username / Default Password

๖.๑.๖ ต้องไม่เปิดเผย OS version, Service Patch version ให้แก่บุคคลภายนอก

๖.๑.๗ มาตรฐานการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

กำหนดแผนการบำรุงรักษาและซ่อมบำรุงระบบคอมพิวเตอร์

- บำรุงรักษาและซ่อมบำรุงโดยกำลังพลที่มีความรู้ด้านฮาร์ดแวร์โดยตรงภายในเหล่าทัพตามระดับความสามารถที่มี
- บำรุงรักษาโดยส่วนราชการเจ้าของอุปกรณ์ ได้แก่การทำความสะอาดสัปดาห์ละ ๑ ครั้ง เปลี่ยนหมึกพิมพ์ตามวาระ
- บำรุงรักษาโดยจัดจ้างเอกชนตามวงรอบที่กำหนดในสัญญา ดูแลการทำงานของเครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบให้สามารถใช้งานได้โดยต่อเนื่อง
- ซ่อมบำรุงโดยจัดจ้างเอกชนในกรณีที่ชำรุดเสียหาย

๖.๒ มาตรฐานการรักษาความปลอดภัยด้านซอฟต์แวร์

มาตรฐานการรักษาความปลอดภัยด้านซอฟต์แวร์ในที่นี้จะเน้นถึงมาตรฐานการรักษาความปลอดภัยระบบสารสนเทศ โดยการรักษาความปลอดภัยระบบสารสนเทศไม่สามารถจะกำหนดเป็นมาตรฐานได้ชัดเจน เช่นเดียวกับสารสนเทศด้านเทคนิคอื่นๆ เนื่องจากการรักษาความปลอดภัยในระบบหนึ่งจะใช้ มาตรฐานเดียวกันกับอีกระบบหนึ่งได้ไม่ทั้งหมด ดังนั้นในการรักษาความปลอดภัยระบบสารสนเทศใด ๆ จะต้องมีทั้งมาตรฐานทางด้านเทคนิคพื้นฐานที่เหมาะสมกับแต่ละระบบ และมาตรการ

รองรับต่าง ๆ เพื่อให้ ข้อมูลมีความถูกต้อง ไม่เกิดการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตซึ่งจะทำให้ข้อมูลหรือความลับไม่รั่วไหล ให้พิจารณาถึงลักษณะและสิทธิ์ในการเข้าถึงระบบสารสนเทศของผู้ใช้ในแต่ละระดับ โดยกำหนดดังนี้

๖.๒.๑ ต้องมีรหัสผ่านในการเข้าสู่ระบบงานอย่างน้อย ๑ ระดับ

๖.๒.๒ ต้องพิจารณาเกี่ยวกับการออกแบบการรักษาความปลอดภัยระบบสารสนเทศพร้อมการพัฒนาระบบสารสนเทศตั้งแต่ขั้นตอนแรกของการออกแบบระบบจนถึงการนำระบบงานไปใช้

๖.๒.๓ ผู้พัฒนาระบบ (Developer) มีสิทธิ์ในการเข้าถึงระบบและข้อมูลที่เกี่ยวข้องกับงานที่กำลังพัฒนาเท่านั้น ต้องไม่มีสิทธิ์ในการเข้าสู่ระบบที่ใช้งานเป็นประจำ (Production)

๖.๒.๔ ต้องทดสอบความปลอดภัย (Security Acceptance Test) ก่อนติดตั้งระบบงานเป็นลักษณะ Production

๖.๒.๕ Application Administrator ต้องมีบัญชีรายชื่อ (account) ของผู้มีสิทธิ์เข้าถึงระบบงานและดำเนินการตรวจสอบความทันสมัยและความถูกต้องของบัญชีรายชื่ออย่างสม่ำเสมอและต้องยกเลิกบัญชี รายชื่อของผู้ที่หมดหน้าที่ในการปฏิบัติงานนั้น ๆ

๖.๒.๖ ต้องแบ่งความรับผิดชอบระหว่างผู้พัฒนาระบบ กับผู้บริหารระบบตามที่ได้กำหนดไว้ในหน้าที่ความรับผิดชอบของตำแหน่ง

๖.๒.๗ การแลกเปลี่ยนข้อมูลในระบบสารสนเทศภายในส่วนราชการและระหว่างส่วนราชการให้เลือกใช้ฮาร์ดแวร์หรือซอฟต์แวร์ในการรักษาความปลอดภัยที่เหมาะสมกับระบบของหน่วย แต่จะต้องสามารถแลกเปลี่ยนข้อมูลซึ่งกันและกันได้โดยมีระบบการรักษาความปลอดภัยที่เพียงพอ

๖.๒.๘ ให้มีการจัดทำ Log file / การสำรอง / การกู้คืนสภาพซอฟต์แวร์ระบบงาน และทดสอบอย่างน้อยปีละ ๔ ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบงาน

(โปรดติดตามฉบับหน้า)