# ความปลอดภัยของข้อมูล

# ข้อมูลสารสนเทศ เป็นสินทรัพย์สำคัญทางธุรกิจ ที่ต้องดูแลบำรุงรักษา และป้องกันอย่างดี ปัจจุบันบริษัทฯ ได้กำหนดความปลอดภัยระบบข้อมูลสารสนเทศ โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงาน และลดความเสี่ยงด้านความปลอดภัย ในระดับที่เหมาะสม และเกิดประสิทธิภาพต่อการทำงานสูงสุด

# บริษัทได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศ โดยให้มีการบริหารจัดการให้ระบบข้อมูลมีลักษณะคงความเป็น C I A  คือ

# 1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิเท่านั้น เข้าถึงเรียกดูข้อมูลได้ ต้องมีการควบคุมการเข้าถึง ข้อมูลเป็นความลับต้องไม่เปิดเผยกับผู้ไม่มีสิทธิ

# 2. ความถูกต้องแท้จริง (Integrity) มีเกราะป้องกันความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล และวิธีการประมวลผล ต้องมีการควบคุมความผิดพลาด ไม่ให้ผู้ไม่มีสิทธิมาเปลี่ยนแปลงแก้ไข

# 3. ความสามารถพร้อมใช้เสมอ (Availability) ให้บุคคลผู้มีสิทธิเท่านั้นเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ระบบล้มเหลว มีสมรรถภาพทำงานต่อเนื่อง ไม่ให้ผู้ไม่มีสิทธิมาทำให้ระบบหยุดการทำงาน

# ความปลอดภัยของข้อมูลสารสนเทศ (Information Security)

# บริษัทฯ มีนโยบายให้ความปลอดภัยและการรักษาความลับของข้อมูล โดยบริษัทฯ ใช้ระบบรักษาความปลอดภัยที่มีมาตรฐานสูงทั้งในด้านเทคโนโลยีและกระบวนการเพื่อป้องกันการโจรกรรมข้อมูลที่เป็นความลับ บริษัทฯ ได้กำหนดให้มีระบบความปลอดภัยที่มีประสิทธิภาพ เพื่อให้มั่นใจได้ว่าเว็บไซต์และข้อมูลของบริษัทฯ มีการรักษาความปลอดภัยที่ได้มาตรฐาน รวมถึงการเลือกใช้ Firewall System, Anti-Virus System ที่มีมาตรฐานความปลอดภัยสูง รวมทั้งได้ใช้เทคโนโลยี เข้ารหัสข้อมูลที่ระดับ 128 บิท (128 Bit Encryption) ซึ่งเป็นการเข้ารหัสข้อมูลระดับสูงสำหรับการทำธุรกรรมผ่านบริการทางอินเทอร์เน็ต นอกจากนี้ บริษัทฯ ยังกำหนดให้ลูกค้าต้องลงทะเบียนก่อนจึงจะสามารถใช้บริการได้

# บริษัทฯ ได้มีการเลือกใช้เทคโนโลยีระบบคอมพิวเตอร์ที่มีระบบการรักษาความปลอดภัยในขั้นพื้นฐานที่เป็นมาตรฐานสากลอยู่แล้ว และเสริมด้วยการทำงานด้านอุปกรณ์ความปลอดภัยเฉพาะอีกชั้น และโดยหลักการทั่วไปในการควบคุมและรักษาความปลอดภัยให้กับระบบข้อมูลข่าวสาร ได้แก่การควบคุมส่วนต่าง ๆ ของระบบอย่างรัดกุม วิธีการที่ใช้ในการควบคุมมีดังนี้

# 1.  การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control)   โดยมีระดับวิธีการ 3 วิธีคือ

# -  การควบคุมจากระบบภายในของซอฟต์แวร์ (Internal Program Control) คือการที่       โปรแกรมนั้นได้มีการควบคุมสิทธิการเข้าถึง และสิทธิในการใช้ข้อมูลภายในระบบ ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลภายในระบบเอง

# -  การควบคุมความปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) คือการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่าง ๆ ภายในระบบคอมพิวเตอร์ของผู้ใช้คนหนึ่ง และจำแนกแตกต่างจากผู้ใช้คนอื่น ๆ

# -  การควบคุมและการออกแบบโปรแกรม (Development Control) คือการควบคุมตั้งแต่การออกแบบ การทดสอบก่อนการใช้งานจริง

# 2. การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control)   โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาด ด้วยอุปกรณ์ภายในตัวเอง

# 3. การใช้นโยบายในการควบคุม (Policies)  โดยมีการประกาศใช้นโยบาย และการปรับปรุงนโยบายให้มีการทำงานสอดคล้องกับการดำเนินธุรกิจ และสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลบังคับใช้ทั้งองค์กร

# 4. การป้องกันทางกายภาพ (Physical Control)   การมีมาตรการการเข้าถึงศูนย์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์ที่สำคัญได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น รวมทั้งมีระบบสำรองข้อมูลอย่างสม่ำเสมอ มาตรการและอุปกรณ์ที่ใช้ในนโยบายระบบความปลอดภัย

# การจัดการด้านความปลอดภัยของระบบเครือข่าย Counter Service จะประกอบด้วยองค์ประกอบ 3 ส่วนดังนี้

# 1. โครงสร้างพื้นฐานด้านความปลอดภัย

# การติดตั้งระบบ Firewall บริษัทฯ ได้ติดตั้ง Firewall ซึ่งเป็นเทคโนโลยีที่ทำการป้องกันผู้บุกรุกเข้า-ออกระบบ และกำหนดโซนการให้บริการ การเข้าถึงข้อมูล ที่เหมาะสม - กำหนดขอบเขต และโซนการทำงานที่เหมาะสม - กำหนดบริการ และการเข้าถึงระบบสำหรับผู้ที่ได้รับอนุญาตเท่านั้น

# การติดตั้งระบบ Anti-Virus เพื่อทำการป้องกัน และกำจัดไวรัสที่มีการอัพเดตข้อมูลอย่างสม่ำเสมอ

# การติดตั้งระบบ SSL บริษัทฯ เลือกใช้ SSL เวอร์ชั่นล่าสุด ซึ่งบริษัท และธนาคารชั้นนำส่วนใหญ่เลือกใช้ เนื่องจากมีประสิทธิภาพในการรักษาความปลอดภัยขั้นสูง  หน้าที่ของ SSL คือ สลับที่ข้อมูลและแปลงเป็นรหัสตัวเลขทั้งหมด ยิ่งความละเอียดในการเข้ารหัสมีมากเท่าไร ความปลอดภัยก็ยิ่งสูงขึ้นเท่านั้น ระดับความละเอียดของการเข้ารหัสมีหน่วยเป็น บิท  โดยเว็บไซท์บริษัทฯ ได้ใช้การเข้ารหัสระดับ 128 บิท ซึ่งถือว่าเป็นระดับที่บริษัท และธนาคารชั้นนำของโลกใช้อยู่

# การติดตั้งระบบปฏิบัติการที่มีระดับความปลอดภัยที่ระดับ C2 โดยการติดตั้ง และเปิดใช้เฉพาะบริการที่เหมาะสม และจำเป็นเท่านั้น

# การติดตั้งระบบ Web Server และการกำหนดค่าพารามิเตอร์ที่เหมาะสม

# 2. การตั้งค่าและใช้งานอย่างเหมาะสม (Hardening)

# Hardening

# Patch Management

# Authentication

# Backup

# 3. การตรวจสอบ (Audit)     การตรวจสอบการใช้งานทั่วไป

# มาตรการการรักษาความปลอดภัยของข้อมูล

|  |
| --- |
| ระบบรักษาความปลอดภัยของข้อมูลของพาณิชย์อิเล็กทรอนิกส์จึงต้องมีมาตรการดังต่อไปนี้                1. การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุ ตัวบุคคลที่ติดต่อว่าเป็น บุคคลตามที่ได้กล่าวอ้างไว้จริง และมีอำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง (เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ การใช้ระบบล็อกซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้น เป็นต้น)                2. การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้ (เปรียบเทียบได้กับ การปิดผนึกซองจดหมาย การใช้ชองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น)              3. การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้ (เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น เป็นต้น)               4. การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล (เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น)              เทคโนโลยีในการรักษาความปลอดภัย               1. ความปลอดภัยของเครือข่าย (Networks Security)                         - เพื่อปกป้องความปลอดภัยของเครือข่ายภายในองค์กรจากเครือข่ายภายนอกที่ไม่น่าเชื่อถือ                         - การใช้ firewalls               2. การพิสูจน์ตัวตน (Authentication)                         - เพื่อให้มั่นใจได้ว่าฝ่ายที่กาลังติดต่อด้วยนั้นเป็นบุคคลที่ถูกต้อง ไม่ใช่ผู้แอบอ้าง                          - การใช้รหัสผ่าน, การใช้ digital certificates, การใช้ smart card ที่เข้ารหัส, การใช้biometrics (เช่น ลายนิ้วมือ, ม่านตา)                3. การเข้ารหัส (Encryption)                          - ใช้ในการปกป้องข้อมูลที่ส่งผ่านเส้นทางสาธารณะ                          - SSL Protocol, Public-key cryptography                4. นโยบายและการจัดการระบบความปลอดภัย (Security Policy and Management)                          - ครอบคลุมถึงระบบการบริหารบุคคล วิธีการเข้าถึงตัว server และอื่น ๆ                          - เป็นส่วนสำคัญในการทำให้ระบบพาณิชย์อิเล็กทรอนิกส์ปลอดภัยอย่างแท้จริง              ความรู้เพิ่มเติม                  1. ลายมือชื่อดิจิทัล (Digital Signature) คือข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือชื่อของผู้ส่ง คุณสมบัติของลายมือชื่อดิจิทัล นอกจากจะสามารถ ระบุตัวบุคคล และเป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือหากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได                  2. ใบรับรองดิจิทัล (Digital Certificate) จะถูกนำมาใช้สำหรับยืนยันในตอนทำธุรกรรมว่าเป็นบุคคลนั้นๆจริง ตามที่ได้อ้างไว้ ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) ซึ่งรายละเอียดในใบรับรองดิจิทัลทั่วไปมีดังต่อไปนี้                      - ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อ องค์กร ที่อยู่                      - ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง                      - กุญแจสาธารณะของผู้ที่ได้รับการรับรอง                      - วันหมดอายุของใบรับรองดิจิทัล                      - ระดับชั้นของใบรับรองดิจิทัล ซึ่งมีทั้งหมด 4 ระดับ ในระดับ 4 จะมีกระบวนการตรวจสอบเข้มงวดที่สุด และต้องการข้อมูลมากที่สุด                      - หมายเลขประจำตัวของใบรับรองดิจิทัล                ประเภทของใบรับรองดิจิทัล แบ่งออกเป็น 3 ประเภท คือ                 1. ใบรับรองเครื่องแม่ข่าย                 2. ใบรับรองตัวบุคคล                     3. ใบรับรองสำหรับองค์รับรองความถูกต้อง |

# ความปลอดภัยของข้อมูล

# ข้อมูลที่ดีเป็นข้อมูลที่มีค่ามีราคา สามารถนำไปใช้ให้เกิดประโยชน์อย่างมากต่อกิจการขององค์กร

# และในมุมกลับกันอาจก่อให้เกิดโทษต่อองค์กรหรือบุคคลผู้ให้ข้อมูล ถ้าข้อมูลตกลงไปอยู่ในมือผู้ไม่ประสงค์ดี

# ดังนั้นความปลอดภัยของข้อมูล จึงเป็นเรื่องสำคัญที่จะต้องตระหนัก ความปลอดภัยของข้อมูล (data security)

# เป็นเรื่องที่เกี่ยวข้องกับการป้องกันไม่ให้ข้อมูลถูกทำลาย การรักษาความลับของข้อมูล

# และการป้องกันไม่ให้ข้อมูลถูกทำลาย การรักษาความลับของข้อมูล และการป้องกันการกระทำการทุจริตต่อข้อมูล

# ความไม่ปลอดภัยของข้อมูลมักมีสาเหตุจาก

# 1. ความผิดพลาดของระบบ ซึ่งอาจมีสาเหตุจากตัวเครื่องคอมพิวเตอร์ ได้แก่ เครื่องคอมพิวเตอร์เกิดขัดข้องในระหว่างการประมวลผลข้อมูล ซึ่งอาจทำให้ข้อมูลเกิดสูญเสียได้ นอกจากนี้อาจมีสาเหตุจากโปรแกรมที่ใช้ในการประมวลผลยังมีข้อผิดพลาดบางจุดซึ่งอาจทำให้ข้อมูลมีความผิดพลาดหรือสูญเสียได้เช่นกัน

# 2. อุบัติเหตุ เช่น ไฟไหม้ น้ำท่วม ทำให้ข้อมูลที่เก็บอยู่สูญเสียได้

# 3. บุคคลอาจทำให้ข้อมูลสูญเสีย เช่น มีการสั่งลบข้อมูล หรือบันทึกข้อมูลทับของเดิม หรือบุคคลอาจมีเจตนาร้ายต้องการทำให้ข้อมูลสูญเสีย เนื่องจากความโกรธแค้นจงใจทำลายข้อมูล

# 4. การขโมยข้อมูลซึ่งเป็นความลับเพื่อนำไปขายหรือให้คู่แข่ง ซึ่งสามารถทำได้ง่าย โดยแอบสำเนาลงบนแผ่นบันทึก

# 5. การกระทำทุจริตต่อข้อมูล เช่น มีการแก้ไขข้อมูลที่เกี่ยวข้องกับจำนวนเงิน เพื่อประโยชน์ของตัวเองหรือมีผู้รับจ้างให้กระทำการทุจริต

# 6. สาเหตุอื่น ๆ เช่น ความร้อนชื่น ฝุ่นละออง และสนามแม่เหล็ก

# การรักษาความปลอดภัยของข้อมูลที่อาจถูกทำลาย หรือเสียหายด้วยสาเหตุดังนี้

# 1. การรักษาความปลอดภัยของอุปกรณ์ระบบคอมพิวเตอร์

# 2. การทำสำเนาข้อมูล ในกรณีที่ข้อมูลอยู่ในแผ่นบันทึกอาจทำสำเนา ข้อมูลทั้งแผ่นโดยใช้คำสั่ง copy แต่ถ้าข้อมูลอยู่ในจานแม่เหล็กชนิดแข็งหรือกรณีที่มีข้อมูลเป็นจำนวนมากจะทำสำเนาโดยการใช้คำสั่ง backup ลงบนแผ่นบันทึกหรือในเทปแม่เหล็ก

# 3. การรักษาความลับของข้อมูล มาตรการแรกในการป้องกันคือ การควบคุมการเข้าไปใช้เครื่องคอมพิวเตอร์ โดยกำหนดว่าใครบ้างที่สามารถเข้าไปใช้เครื่องคอมพิวเตอร์ได้ มาตรการต่อมาคือ การกำหนดรหัสผ่าน (password) เพื่อผ่านเข้าไปใช้โปรแกรมหรือการเข้าถึงข้อมูล นอกจากนี้อาจจะมีการกำหนดขอบเขตเฉพาะแฟ้มข้อมูลเฉพาะแฟ้มบุคคลเฉพาะบุคคล ไม่มีสิทธิไปใช้หรือเปลี่ยนแปลงแก้ไขข้อมูลของแฟ้มรายได้ เป็นต้น

# กระบวนการรักษาความปลอดภัยข้อมูล การรักษาความปลอดภัยของข้อมูลนั้นเป็นกระบวนการในเชิงรุกเพื่อบริหารความเสี่ยง (Risk Management) แต่ที่ผ่านมาโดยส่วนใหญ่การรักษาความปลอดภัยจะเป็นแบบเชิงรับ กล่าวคือ องค์กรจะรอให้มีเหตุการณ์เกิดขึ้นก่อนแล้วค่อยหาวิธีการที่จะป้องกันเหตุการณ์นั้น ซึ่งการทำเช่นนี้อาจเกิดความเสียหายกับองค์การมากเกินคาดก็ได้ การจัดการในเชิงรุกนั้นเป็นขั้นตอนที่ทำก่อนที่จะเกิดเหตุการณ์ขึ้น ถ้าการรักษาความปลอดภัยนั้นเป็นแบบเชิงรับ ค่าใช้จ่ายของระบบการรักษาความปลอดภัยนั้นไม่สามารถประเมินได้ค่าใช้จ่ายการรักษาความปลอดภัย = ค่าความเสียหายเมื่อเกิดเหตุการณ์ + ค่าใช้จ่ายในการติดตั้งระบบป้องกัน ค่าใช้จ่ายการรักษาความปลอดภัย = ค่าใช้จ่ายในการติดตั้งระบบป้องกัน ข้อสังเกตจากสมการทั้งสองข้างบนก็คือ ค่าความเสียหายที่เกิดจากเหตุการณ์นั้นอาจมีค่ามากกว่าค่าใช้จ่ายในการติดตั้งระบบเพื่อป้องกันเหตุการณ์มาก ทำให้ค่าใช้จ่ายในการรักษาความปลอดภัยนั้นลดลงอย่างเห็นได้ชัด การเตรียมการล่วงหน้าก่อนที่จะเกิดเหตุการณ์ขึ้นเป็นนโยบายเชิงรุกสำหรับการรักษาความปลอดภัยข้อมูลขององค์กร กระบวนการในการรักษาความปลอดภัยข้อมูลขององค์กรนั้นเป็นกระบวนการที่ต้องทำอย่างต่อเนื่อง ซึ่งประกอบด้วย ๕ ขั้นตอนหลักคือ • การประเมินความเสี่ยง (Risk Assessment) • กำหนดนโยบาย (Policy) • การติดตั้งระบบป้องกัน (Implementation) • การฝึกอบรม (Training) • การตรวจสอบ (Audit) แต่ละขั้นตอนนั้นมีความสำคัญต่อกระบวนการรักษาความปลอดภัยข้อมูลขององค์กรอย่างไรก็ตามเพื่อให้กระบวนการนี้ได้ผล และมีประสิทธิภาพในการป้องกันเหตุการณ์ต่างๆ องค์กรจะต้องทำทุกขั้นตอนควบคู่กันไป การบริหารความเสี่ยง การรักษาความปลอดภัยนั้นจะเกี่ยวข้องกับการบริหารความเสี่ยงอย่างใกล้ชิด ถ้าไม่เข้าใจเกี่ยวกับความเสี่ยงขององค์กรแล้ว การใช้ทรัพยากรขององค์กรเพื่อการรักษาความปลอดภัยนั้นอาจมากเกินความจำเป็นหรือน้อยกว่าที่ควรจะเป็นก็ได้  ความเสี่ยงนั้นประกอบด้วย ๒ ส่วน คือ จุดอ่อนหรือช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) ที่จะใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่นั้น เมื่อมีการประเมินความเสี่ยง เราจึงจำเป็นที่จะต้องเข้าใจจุดอ่อน และภัยคุกคามขององค์กรก่อน เมื่อรวมจุดอ่อน และภัยคุกคามก็จะกลายเป็นความเสี่ยงนั่นเอง ดังนั้น ถ้าไม่มีจุดอ่อนก็จะไม่มีความเสี่ยง หรือถ้าไม่มีคัยคุกคามก็จะไม่มีความเสี่ยงเช่นกัน จุดอ่อนหรือช่องโหว่ (Vulnerability) คือ ช่องทางที่อาจใช้สำหรับการโจมตีได้จุดอ่อนหรือช่องโหว่ อาจมีในระบบคอมพิวเตอร์และเครือข่าย ซึ่งเป็นช่องทางให้ผู้ไม่ประสงค์ดีสามารถเจาะเข้าระบบหรือเครือข่ายได้ จุดอ่อนนั้นมีหลายระดับขึ้นอยู่กับความยากง่าย และระดับความชำนาญทางด้านเทคนิคที่จะสามารถใช้ประโยชน์จากมันได้ นอกจากนี้ผลกระทบที่เกิดจากการใช้ประโยชน์จากจุดอ่อนดังกล่าวก็จะนับรวมเข้าไปด้วย ยกตัวอย่างเช่น จุดอ่อนประเภทที่ง่ายต่อการเจาะเข้าซึ่งอาจเป็นเพราะสคริปต์ (Script) ที่ใช้สำหรับเจาะเข้าระบบนั้นหาได้ง่าย และเมื่อทำสำเร็จผู้บุกรุกสามารถควบคุมระบบได้ทั้งหมด จุดอ่อนประเภทนี้ก็จะจัดว่ามีความอันตรายในระดับสูง ในทางตรงข้ามถ้าเป็นจุดอ่อนประเภทที่ต้องใช้ความชำนาญสูง และอาจต้องใช้ทรัพยากรจำนวนมากในการเจาะเข้าระบบ ถ้าเจาะเข้าระบบได้แล้วแต่ได้ข้อมู่ลที่ไม่ถือว่าสำคัญมากนัก จุดอ่อนประเภทนี้ก็ถือได้ว่ามีอัตรายในระดับต่ำ จุดอ่อนนั้นไม่ได้มีกับเฉพาะระบบคอมพิวเตอร์ และเครือข่ายเท่านั้น แต่จะรวมถึงทางด้านกายภาพ พนักงาน และข้อมูล หรือทรัพย์สินที่ไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์ด้วย ภัยคุกคาม (Threat) คือสิ่งที่อาจจะเกิดขึ้นและมีอันตรายต่อทรัพย์สินขององค์กร ภัยคุกคามนั้นประกอบด้วย ๓ ส่วนคือ • เป้าหมาย (Target) : ด้านของการรักษาความปลอดภัยที่อาจถูกโจมตี • ผู้โจมตี (Agent) : คนหรือองค์กรที่เป็นแหล่งที่มาของภัยคุกคาม • เหตุการณ์ (Event) : สิ่งที่เกิดขี้นและก่อให้เกิดความเสียหาย เพื่อให้เข้าใจภัยคุกคามต่อองค์กรอย่างแน่ชัดนั้นควรศึกษาองค์ประกอบทั้งสามส่วนของภัยคุกคามให้แน่ชัดก่อน เป้าหมายของการโจมตีในที่นี้ หมายถึง องค์ประกอบด้านต่างๆ ของการรักษาความปลอดภัยที่กล่าวถึงก่อนหน้าคือ ความลับ ความคงสภาพ และความพร้อมใช้งาน ซึ่งภัยคุกคามแต่ละด้านนั้นขึ้นอยู่กับเหตุผลหรือแรงจูงใจ ผู้โจมตี คือ ผู้ที่กระทำการใดๆ ที่ก่อให้เกิดผลทางด้านลบกับองค์กร ผู้โจมตีในที่นี้ต้องมีคุณสมบัติ ๓ ข้อต่อไปนี้ • การเข้าถึง (Access) : ผู้โจมตีต้องสามารถเข้าถึงเป้าหมายได้ • ความรู้ (Knowledge) : ความรู้หรือข้อมูลเกี่ยวกับเป้าหมายที่ผู้โจมตีทราบ • แรงจูงใจ (Motivation) : เหตุผลที่เอเย่นต์มีสำหรับการโจมตี ภัยคุกคามเกิดขึ้นเมื่อผู้โจมตีมีความรู้เกี่ยวกับเป้าหมาย และสามารถเข้าถึงได้ด้วยแรงจูงใจ บนพื้นฐานของทั้ง ๓ อย่าง ผู้โจมตีอาจเป็นบุคคลดังต่อไปนี้ • พนักงาน ซึ่งสามารถเข้าถึงระบบ และมีความรู้เกี่ยวกับระบบ เพราะเป็นสิ่งที่จำเป็นสำหรับการทำงาน คำถามสำหรับพนักงานคือ เขามีแรงจูงใจที่จะทำอันครายต่อระบบขององค์กรหรือไม่ นี่ไม่ได้หมายความว่า พนักงานทุกคนจะตกเป็นผู้ต้องสงสัยเมื่อเกิดเหตุการณ์ขึ้น แต่ก็ไม่ควรมองข้ามเมื่อมีการวิเคราะห์ความเสี่ยง • พนักงานเก่า ซึ่งคุ้นเคยกับระบบเป็นอย่างดีเนื่องจากเคยทำงานที่นั่นมาก่อน บางบริษัทหรือองค์กรนั้นอาจมีกระบวนการที่ยังหละหลวมอยู่เมื่อพนักงานออกจากงาน ทำให้พนักงานเก่าบางคนที่ออกไปแล้วอาจยังมีสิทธิ์ที่จะสามารถเข้าถึงระบบได้ • แฮคเกอร์ เป็นบุคคลที่มีแรงจูงใจที่จะทำอันตรายให้บริษัทเสมอจะด้วยความสามารถใดก็แล้วแต่ แฮคเกอร์นั้นอาจจะมีหรือไม่มีความรู้ หรือมีข้อมูลเกี่ยวกับระบบ และเครือข่ายขององค์กรก็ได้ การเข้าถึงระบบนั้นอาจผ่านช่องโหว่ หรือจุดอ่อนที่ระบบยังคงมีอยู่ก็ได้ • ศัตรูหรือคู่แข่ง เป็นกลุ่มที่ต้องการจะรู้ข้อมูลขององค์กรเสมอ เช่น คู่แข่งด้านการค้าอาจต้องการทำลายศักยภาพของคู่แข่งเพื่อให้ได้เปรียบทางด้านการค้า เหตุการณ์ หมายถึง วิธีการที่ผู้โจมตีอาจทำอันตรายต่อองค์กร เช่น แฮคเกอร์อาจทำอันตรายโดยการแก้ไขหน้าเว็บไซต์ขององค์กร ยกตัวอย่างเช่น • การใช้บัญชีผู้ใช้ในทางที่ผิด หรือเกินกว่าที่ได้รับอนุญาต • การแก้ไขข้อมูลที่สำคัญทั้งที่ตั้งใจและที่ไม่ได้ตั้งใจ • การเจาะเข้าระบบโดยไม่ได้รับอนุญาต • การทำลายระบบโดยไม่ได้ตั้งใจ • การรบกวนระบบสื่อสารข้อมูลทั้งภายในและภายนอก • การบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต การประเมินความเสี่ยง แนวทางในการประเมินภัยคุกคาม และความเสี่ยงขององค์กร ปัจจุบันมีเครื่องมือหลายประเภทที่ใช้สำหรับงานนี้ ซึ่งบางซอฟต์แวร์ก็ฟรีบางซอฟต์แวร์ก็ต้องซื้อ อย่างไรก็ตามเครื่องมือต่างๆ เหล่านี้ถูกใช้งานเพื่อตอบคำถามต่อปนี้ • เราต้องการจะปกป้องอะไร • ใครหรืออะไรที่เป็นภัยคุกคาม จุดอ่อน หรือช่องโหว่ • จะเกิดความเสียหายมากน้อยเท่าใดเมื่อถูกโจมตีจุดอ่อน หรือช่องโหว่เหล่านั้น • มูลค่าทรัพย์สินขององค์กรมีอะไรบ้างและเท่าไร • เราจะป้องกันหรือแก้ไขช่องโหว่ หรือจุดอ่อนได้อย่างไร ผลที่จะได้จากการประเมินความเสี่ยงคือ ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด เพื่กปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ปกติ ก่อนที่จะสามารถตอบคำถามเหล่านี้ได้องค์กรจะต้องประเมินความเสี่ยงก่อน ซึ่งสามารถทำได้โดยการใช้ทรัพยากรภายในหรือภายนอกก็ได้ การประเมินความเสี่ยงนั้นต้องอาศัยความร่วมมือจากทุกฝ่าย ถ้าม่ได้รับความร่วมมืออาจทำให้การประเมินความเสี่ยงนั้นไม่ได้ผลหรือไม่มีประสิทธิภาพ ขั้นตอนที่สำคัญของการประเมินความเสี่ยงคือ ๑. กำหนดขอบเขต ๒. เก็บรวบรวมข้อมูล ๓. วิเคราะห์นโยบายและระเบียบปฏิบัติ ๔. วิเคราะห์ภัยคุกคาม (Threat Analysis) ๕. วิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability Analysis) ๖. ประเมินความเสี่ยง การกำหนดขอบเขตเป็นขั้นตอนที่สำคัญที่สุดของกระบวนการ เนื่องจากขอบเขตเป็นสิ่งที่กำหนดว่าอะไรที่จะทำหรือไม่ทำในระหว่างการประเมิน และเป็นการระบุว่าอะไรที่เราจะปกป้อง ความสำคัญของสิ่งที่เราพยายามจะปกป้อง และจะปกป้องถึงระดับไหนและละเอียดเพียงใด นอกจากนี้การกำหนดขอบเขตยังเกี่ยวข้องกับว่าระบบใด หรือแอพพลิเคชันใดที่จะถูกประเมินบ้าง การเก็บรวบรวมข้อมูลนั้นควรทำสิ่งต่อไปนี้ • เซอร์วิสแพ็คหรือแพตช์ที่ติดตั้งในแต่ละเครื่อง • เซอร์วิสที่ให้บริการ เช่น เว็บ, เมล์, FTP เป็นต้น • ประเภทและเวอร์ชั่นของระบบปฏิบัติการ • แอพพลิเคชันที่รันผ่านเครือข่าย • ห้องหรือสถานที่ติดตั้งระบบ • สิทธิ์ในการเข้าออกห้องคอมพิวเตอร์ • การสแกนพอร์ตที่เปิด • การให้บริการไวร์เลสแลน • การทดสอบระบบ IDS • การทดสอบระบบโทรศัพท์ • การทดสอบไฟร์วอลล์ • การสำรวจเครือข่าย ข้อมูลเกี่ยกับจุดอ่อน หรือช่องโหว่ของระบบเฉพาะ หรือโปรแกรมเฉพาะสามารถหาได้จากหายแหล่ง เช่น • //www.securityfocus.com : ให้บริการข้อมูลเกี่ยวกับจุดอ่อนและช่องโหว่ต่างๆ • //www.incidents.org : ให้บริการข้อมูลเกี่ยวกับภัยต่างๆ ในปัจจุบัน • //www.packetstormsecurity.org : เว็บไซต์ที่รวบรวมข้อมูลเกี่ยกับเครื่องมือ ช่องโหว่ และข้อแนะนำในการป้องกัน • //www.sans.org : เว็บไซต์ที่ให้ข้อมูลเกี่ยวกับการฝึกอบรมด้านการรักษาความปลอดภัย และได้รวบรวมเอกสารทางด้านนี้มากมาย นอกจากนี้ยังมีระบบแจ้งเตือนภัยบนอินเทอร์เน็ตด้วย • //www.cert.org : เว็บไซต์ที่ให้ข้อมูลเกี่ยวกับภัยคุกคามบนอินเทอร์เน็ต พร้อมข้อแนะนำในการป้องกันและแก้ไขช่องโหว่ต่างๆ ที่ค้นพบ การวิเคราะห์นโยบายและระเบียบปฏิบัติ  การทบทวนและวิเคราะห์นโยบาย และระเบียบปฏิบัติขององค์กรที่ประกาศใช้งานในปัจจุบันเป็นการตรวจสอบดูว่าองค์กรนั้นจัดอยู่ในระดับใดของมาตรฐานความปลอดภัย  การวิเคราะห์ช่องโหว่จุดประสงค์ของการวิเคราะห์ช่องโหว่ (Vulnerability Analysis) นั้นก็เพื่อเป็นการทดสอบสถานภาพขององค์กรในปัจจุบันว่าล่อแหลมต่อการถูกโจมตี หรือถูกทำลายมากน้อยแค่ไหน หรือเป็นการทดสอบ การรักษาความลับ ความคงสภาพ และความพร้อมใช้งานของข้อมูลที่สำคัญขององค์กร และนอกจากนี้ยังเป็นการทดสอบว่าเครื่องมือหรือระบบที่ใช้สำหรับป้องกัน และรักษาความปลอดภัยนั้นมีประสิทธิภาพเพียงพอหรือไม่ ปัจจุบันมีเครื่องมือหลายประเภทที่สามารถใช้สำหรับการวิเคราะห์ช่องโหว่หรือจุดอ่อนของระบบ เช่น • Nessus (www.nessus.org) • GFI LANGuard (www.gfi.com) • Retina (www.eeye.com) • SAINT (www.saintcorporation.com) ปัญหาส่วนใหญ่ที่เกิดจากการใช้เครื่องมือเหล่านี้คือ การวิเคราะห์ข้อมูลที่ได้ เนื่องจากเครื่องมือส่วนใหญ่จะรายงานข้อมูลไม่สมบูรณ์มากนัก ยังต้องอาศัยการวิเคราะห์จากผุ้ที่ใช้เครื่องมือเหล่านี้ ดังนั้น ผู้ที่ใช้เครื่องมือเหล่านี้จำเป็นที่จะต้องมีความรู้เกี่ยวกับเรื่องการรักษาความปลอดภัยค่อนข้างมาก การวิเคราะห์ความเสี่ยง จุดมุ่งหมายของการประเมินค่าความเสี่ยงภัยของข้อมูลนั้นประกอบด้วย • เพื่อประเมินค่าของทรัพย์สินประเภทข้อมูล • เพื่อประเมินค่าความเสี่ยงภัยต่อความลับ ความคงสภาพ และความพร้อมใช้งานของทรัพย์สินข้อมูล • เพื่อตรวจสอบและค้นหาจุดอ่อน หรือช่องโหว่ของระบบในขณะนั้น • เพื่อประเมินความเสี่ยงขององค์กรที่เกี่ยวกับทรัพย์สินประเภทข้อมูล • เพื่อแนะนำวิธีปฏิบัติต่อข้อมูลเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ • เพื่อใช้เป็นข้อมูลเกี่ยวกับการวางรากฐานสำหรับการสร้างระบบการรักษาความปลอดภัย การประเมินสถานการณ์ในปัจจุบันขององค์กรนั้น แบ่งออกได้เป็น ๕ ระดับ ดังนี้ • การวิเคราะห์ความเสี่ยงในระดับระบบ (System-Level Vulnerability Assessment) : เป็นการประเมินเพื่อหาจุดอ่อนของคอมพิวเตอร์แต่ละเครื่องที่ใช้งานในองค์กร และการตรวจสอบระบบเพื่อให้ทราบว่าระบบดังกล่าวสามารถบังคับให้เป็นไปตามนโยบายการรักษาความแลอดภัยในขณะนั้นหรือไม่ • การวิเคราะห์ความเสี่ยงในระดับเครือข่าย (Network-Level Risk Assessment) : เป็นการประเมินค่าความเสี่ยงต่อภัยต่างๆ ของระบบคอมพิวเตอร์ และเครือข่ายทั่วทั้งองค์กร รวมถึงโครงสร้างระบบการจัดการข้อมูลขององค์กร • การวิเคราะห์ความเสี่ยงระดับองค์กร (Organization-Wide Risk Assessment) : เป็นการวิเคราะห์ และประเมินความเสี่ยงของทั้งองค์กรโดยรวมเพื่อระบุถึงภัยต่อข้อมูลขององค์กรโดยตรง วิเคราะห์และค้นหาจุดอ่อนของการปฏิบัติ และจัดการข้อมูลขององค์กร โดยจะต้องเก็บข้อมูลในที่จัดเก็บในทุกรูปแบบไม่ว่าจะเป็นการจัดเก็บทางด้านกายภาพ เช่น บนกระดาษ หรือในรูปแบบของอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์ • การตรวจสอบ (Audit) : เป็นการตรวจสอบนโยบายการรักษาความปลอดภัย และตรวจวิเคราะห์ว่าองค์กรได้ปฏิบัติ หรือมีการบังคับใช้นโยบายเหล่านั้นหรือไม่ • การทดสอบเจาะเข้าระบบ (Penetration Test) : เป็นการทดสอบการเจาะเข้าระบบเพื่อทดสอบความสามารถขององค์กรในการตอบโต้ต่อการบุกรุก การทดสอบประเภทนี้ควรทำกับเฉพาะองค์กรที่มีระบบการรักษาความปลอดภัยที่ค่อนข้างแข็งแกร่ง เพราะการทดลองเจาะเข้าระบบอาจสร้างความเสียหายให้กับองค์กรก็ได้ การสำรวจเครือข่าย โดยปกติแล้วระบบเครือข่ายขององค์กรเป็นจุดที่สามารถเข้าถึงข้อมูลขององค์กรได้ง่ายที่สุด การสำรวจนั้นก็เริ่มจากการตรวจดูผังระบบเครือข่าย และตรวจหาแต่ละจุดที่สามารถเชื่อมต่อเข้าเครือข่ายได้ ข้อควรระวังอย่างหนึ่งคือ บ่อยครั้งที่ผังระบบเครือข่ายนั้นอาจม่ได้มีการปรับปรุงให้ทันสมัย เนื่องจากเครือข่ายอาจมีการเปลี่ยนแปลงอยู่บ่อยๆ และบางทีอาจไม่ได้เก็บข้อมูลเหล่านี้ไว้ในรูปแบบของเอกสาร ดังนั้น นอกจากการตรวจสอบผังระบบเครือข่ายในรูปแบบของเอกสารแล้ว ควรใช้ซอฟต์แวร์ที่สามารถสแกนเครือข่ายเพื่อให้ได้ผังเครือข่ายที่ทันสมัยด้วย ในการตรวจสอบนั้นควรตรวจดูตำแหน่งของเซิร์ฟเวอร์ คอมพิวเตอร์ ลิงค์ที่เชื่อมต่อไปยังอินเทอร์เน็ต การเชื่อมต่อเครือข่ายด้วยโมเด็ม และการเชื่อมต่อระยะไกลกับหน่วยงานอื่น ในระหว่างการวิเคราะห์ผังเครือข่าย และการสัมภาษณ์กับผู้ดูแลระบบเครือข่ายนั้นควรเก็บรวบรวมข้อมูลดังต่อไปนี้ • ประเภทและจำนวนของระบบต่างๆ ที่ใช้ในเครือข่าย • ประเภทและเวอร์ชันระบบปฏิบัติการที่ใช้งานในองค์กร • โทโปโลยีของเครือข่ายรวมถึง ฮับ สวิตช์ เราท์เตอร์ และอุปกรณ์เครือข่ายอื่นๆ • ลิงค์ที่เชื่อมต่อเข้ากับอินเทอร์เน็ต • ประเภท จำนวน และเวอร์ชันของไฟร์วอลล์ • ประเภทจองระบบการเชื่อมต่อระยะไกล หรือรีโมทแอ็กเซส • โทโปโลยีของเครือข่าย WAN • จุดที่เชื่อมต่อเครือข่ายของหน่วยงานที่อยู่อีกที่ที่อยู่ไกล • จุดที่เชื่อมต่อเข้าเครือข่ายของหน่วยงานอื่นที่เกี่ยวข้อง • ตำแหน่งของเซิร์ฟเวอร์ต่างๆ เช่น เว็บเซิร์ฟเวอร์ เมลเซิร์ฟเวอร์ และดีเอ็นเอสเซิร์ฟเวอร์ เป็นต้น • โปรโตคอลต่างๆ ที่ใช้ในระบบเครือข่าย • ใครที่มีหน้าที่ในการควลคุม และดูแลระบบเครือข่ายด้บ้าง เมื่อได้สำรวจโครงสร้างของเครือข่ายแล้วให้สำรวจกลไกในการควบคุม และป้องกันเครือข่ายซึ่งรวมถึงสิ่งต่อไปนี้ • การควบคุมการเข้าถึงเราท์เตอร์ (Access Control List) และกฏของไฟร์วอลล์ของทุกๆ จุดที่เชื่อมต่อเข้ากับอินเทอร์เน็ต • ระบบการพิสูจน์ตัวตนเพื่อเข้าถึงเครือข่ายจากระยะไกล (Remote Access) • กลไกการป้องกันสำหรับการเข้าถึงเครือข่ายขององค์กรอื่น • กลไกการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่ายหรือที่จัดเก็บไว้ในระบบ • กลไกการเข้ารหัสข้อมูลของคอมพิวเตอร์เคลื่อนที่ • ระบบป้องกันไวรัสบนเซิร์ฟเวอร์ คอมพิวเตอร์ และระบบอีเมล • การป้องกันและรักษาความปลอดภัยของเซิร์ฟเวอร์ต่างๆ การรักษาความปลอดภัยทางด้านกายภาพ การตรวจสอบระบบการรักษาความปลอดภัยทางกายภาพนั้นควรตรวจสอบสิ่งต่อไปนี้ • ประเภทของระบบป้องกัน และรักษาความปลอดภัยของสถานที่ อาคาร ห้องทำงาน เอกสาร อุปกรณ์จัดเก็บข้อมูล เช่น เทป ซีดี ซิปไดร์ว เป็นต้น และดาต้าเซ็นเตอร์ • ใครที่เก็บกุญแจหรือบัตรรูดเข้าออก หรือใครที่สามารถเปิดประตูได้บ้าง • นอกจากดาต้าเซ็นเตอร์แล้วมีพื้นที่อื่นหรือไม่ที่สำคัญกับระบบ นอกจากนี้ต้องมีการตรวจสอบเส้นทางสายสัญญาณที่ติดตั้งภายในอาคาร และจุดที่สายสัญญาณเข้าถึงอาคาร เนื่องจากพื้นที่เหล่านี้อาจเป็นจุดที่สามารถแท็ปสายสัญญาณเพื่อดักจับข้อมูลที่วิ่งอยู่บนสายสัญญาณได้ เพราะฉะนั้นพื้นที่เหล่านี้ควรเพิ่มเข้าไปในรายการที่เป็นพื้นที่เสี่ยงด้วย การรักษาความปลอดภัยทางด้านกายภาพนั้นจะรวมถึงระบบไฟฟ้า ระบบควบคุมสภาวะแวดล้อม เช่น อุณหภูมิ เป็นต้น ระบบป้องกันอัคคีภัย ซึ่งควรรวบรวมข้อมูลดังต่อไปนี้ • ระบบไฟฟ้าของสถานที่ และอาคารมีแหล่งที่มาอย่างไร • ระบบไฟฟ้าของดาต้าเซ้นเตอร์เป็นอย่างไร • ระบบไฟฟ้าสำรองหรือ UPS สามารถรองรับการทำงานของระบบได้นานเท่าใดเมื่อไฟฟ้าดับ • ระบบใดบ้างที่ใช้งาน UPS • ใครจะได้รับรายงานบ้างเมื่อเกิดไฟฟ้าขัดข้อง • ระบบควบคุมสภาพแวดล้อมของดาต้าเซ็นเตอร์เป็นอย่างไรบ้าง • ใครจะได้รับแจ้งเมื่อระบบควบคุมสภาพแวดล้อมไม่ทำงาน • ระบบป้องกันอัคคีภัยของดาต้าเซ็นเตอร์เป็นอย่างไรบ้าง นโยบายและระเบียบปฏิบัติ องค์กรส่วนใหญ่จะมีนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับการรักษาความปลอดภัยอยู่แล้ว ในระหว่างการประเมินนั้นควรตรวจสอบ และเก็บรวบรวมข้อมูลเกี่ยวกับสิ่งต่อไปนี้ • นโยบายการรักษาความปลอดภัยทั่วไป • นโยบายการรักษาความปลอดภัยข้อมูล • แผนการฟื้นฟูหลังเกิดภัยร้ายแรง เช่น น้ำท่วม ไฟไหม้ เป็นต้น • แผนการตอบโต้เมื่อเกิดเหตุการณ์ • นโยบายและระเบียบปฏิบัติสำหรับการสำรองข้อมูล • คู่มือปฏิบัติงานของพนักงาน • ขั้นตอนการปฏิบัติเมื่อจ้างพนักงานใหม่ • ขั้นตอนการปฐมนิเทศสำหรับพนักงานใหม่ • นโยบายการรักษาความปลอดภัยของไฟร์วอลล์ • นโยบายการสื่อสารข้อมูลระยะไกล • ผังระบบเครือข่าย • ผังการจัดองค์กร • นโยบายข้อมูล (Information Policy) : กำหนดว่าข้อมูลใดมีความสำคัญ และข้อมูลเหล่านี้ ซึ่งประกอบด้วย การจัดเก็บ การถ่ายโอน และการทำลาย นโยบายน้จะเป็นสิ่งที่เป็นพื้นฐานเพื่อตอบคำถามที่ว่า “ทำไม” ของการรักษาความปลอดภัย • นโยบายการรักษาความปลอดภัย (Security Policy) : กำหนดเกี่ยวกับระบบควบคุมทางด้านเทคนิคกับระบบคอมพิวเตอร์ต่างๆ นโยบายการรักษาความปลอดภัยนี้จะเป็นสิ่งที่ตอบคำถามว่า “อะไร” ของการรักษาความปลอดภัย • นโยบายการใช้งาน (Usage Policy) : กำหนดนโยบายขององค์กรเกี่ยวกับการใช้งานคอมพิวเตอร์ที่ถูกต้องและเหมาะสม • การสำรอง (Backup Policy) : กำหนดความจำเป็นเกี่ยวกับการสำรองระบบคอมพิวเตอร์ • ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการบัญชีผู้ใช้ (Account Management Procedure) : กำหนดขั้นตอนการปฏิบัติเมื่อต้องเพิ่มบัญชีผู้ใช้ใหม่ และการลบทิ้งบัญชีผู้ใช้ที่ไม่ได้ใช้งานแล้ว • ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ (Incident Handling Procedure) : กำหนดจุดมุ่งหมายและขั้นตอนเกี่ยวกับการจัดการกับเหตุการณ์ที่เกิดขึ้นเกี่ยวกับข้อมูล • แผนการฟื้นฟูหลังภัยร้ายแรง (Disaster Recovery Plan) : กำหนดแผนสำหรับฟื้นฟูหรือกู้คืนระบบคอมพิวเตอร์หลังจากที่เกิดภัยธรรมชาติหรือภัยที่เกิดจากมนุษย์ การกำหนดนโยบายต่างๆ นั้นอาจเกี่ยวข้องกับการเมือง ซึ่งอาจจะต้องใช้พนักงานจากหลายหน่วยงานย่อยร่วมกันกำหนดนโยบายให้เหมาะสม บุคคลที่เป็นคีย์แมนจะเป็นคนที่ทำให้การกำหนดนโยบายนั้นประสบความสำเร็จมากที่สุด การออกแบบและติดตั้งระบบรักษาความปลอดภัย ในการบังคับใช้นโยบายการรักษาความปลอดภัยให้ได้ผลนั้น ต้องเกี่ยวข้องกับการจัดหาเครื่องมือเทคนิค และระบบควบคุมการเข้าถึงทางกายภาพ พร้อมทั้งอาจต้องจ้างเจ้าหน้าที่รักษาความปลอดภัยเพิ่ม การบังคับใช้นั้นอาจต้องมีการคอนฟิกระบบใหม่ซึ่งอาจไม่ได้อยู่ในการควบคุม และดูแลของฝ่ายรักษาความปลอดภัย ในกรณีนี้ในการติดตั้งซอฟต์แวร์ระบบการรักษาความปลอดภัยนั้นต้องเกี่ยวข้องกับผู้ดูแลระบบและผู้ดูแลเครือข่ายด้วย ตรวจสอบดูว่าการติดตั้งแต่ละระบบนั้นมีผลต่อสภาพแวดล้อมโดยรวมอย่างไร และมีผลกระทบต่อระบบควบคุมอื่นอย่างไร ยกตัวอย่างเช่น การเพิ่มระบบการรักษาความปลอดภัยทางด้านกายภาพนั้น อาจมีผลทำให้ความจำเป็นในการเข้ารหัสข้อมูลนั้นน้อยลงหรือในทางกลับกัน หรือการติดตั้งไฟร์วอลล์อาจช่วยลดช่องโหว่หรือจุดอ่อนของระบบได้ทันที ระบบรายงานการรักษาความปลอดภัย ระบบรายงานการรักษาความปลอดภัย จะเป็นกลไกที่ช่วยให้ฝ่ายรักษาความปลอดภัยทราบถึงการปฏิบัติตามนโยบายของพนักงานทั่วไป และเป็นสิ่งที่ใช้ติดตามสถานภาพในปัจจุบันเกี่ยวกับจุดอ่อนโดยรวมขององค์กรด้วย  การเฝ้าระวังการใช้งานระบบ การมอนิเตอร์การใช้งานระบบเป็นกลไกที่ใช้สำหรับการตรวจสอบการปฏิบัติตามนโยบายการใช้งานของพนักงาน ซึ่งอาจจะรวมถึงซอฟต์แวร์ที่ใช้มอนิเตอร์การใช้งานอินเทอร์เน็ต จุดมุ่งหมายของการมอนิเตอร์ก็เพื่อตรวจดูว่าพนักงานคนใดที่ชอบฝ่าฝืนนโยบายขององค์กรบ่อยๆ บางซอฟต์แวร์อาจสามารถป้องกันการเข้าถึงได้และเก็บล็อคเกี่ยวกับความพยายามที่จะฝ่าฝืนไว้ ซอฟต์แวร์บางตัวอาจสามารถลบเกมที่ติดตั้งบนเครื่องได้ หรืออาจเก็บล็อคเกี่ยวกับการติดตั้งโปรแกรมใหม่เข้าไปในระบบก็ได้ การสแกนช่องโหว่ของระบบ การสแกนระบบเพื่อค้นหาจุดอ่อนได้กลายเป็นหัวข้อที่สำคัญเกี่ยวกับการรักษาความปลอดภัย การติดตั้งระบบปฏิบัติการโดยดีฟอลต์นั้นจะมีโพรเซสที่ไม่จำเป็นต้องถูกติดตั้งด้วย และรวมถึงจุดอ่อนและช่องโหว่ด้วย ในขณะที่การตรวจสอบเพื่อค้นหาจุดอ่อน และช่องโหว่ของระบบนั้นเป็นเรื่องที่ง่ายเมื่อใช้เครื่องมือที่มีในปัจจุบัน แต่การแก้ปัญหานั้นเป็นเรื่องที่ยากและต้องใช้เวลา การปฏิบัติตามนโยบาย การบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัยนั้น เป็นเรื่องที่ต้องใช้เวลาพอสมควร การตรวจสอบว่ามีการปฏิบัติตามนโยบายนั้นมี ๒ วิธีคือ แบบอัตโนมัติ และแบบทำด้วยมือ แบบที่ไม่อัตโนมัตินั้นผู้รักษาความปลอดภัยต้องคอยตรวจเช็คทุกระบบเพื่อดูว่ามีการฝ่าฝืนนโยบายหรือระเบียบหรือไม่ โดยอาจตรวจสอบล็อคไฟล์ หรืออาจใช้เครื่องมืออื่นเพื่อมอนิเตอร์เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ วิธีนี้เป็นวิธีที่ใช้เวลามาก และมีโอกาสที่จะเกิดข้อผิดพลาดขึ้นเยอะ บางองค์กรอาจสุ่มเลือกบางระบบเพื่อสแกนวิธีนี้อาจจะช่วยลดเวลาในการทำแต่ก็เป็นวิธีที่ไม่สมบูรณ์ ระบบพิสูจน์ทราบตัวตน ระบบพิสูจน์ทราบตัวตน (Authentication Systems) เป็นกลไกที่ใช้ตรวจสอบผู้ใช้ที่ต้องการล็อกอินเข้าใช้งานระบบหรือเครือข่าย นอกจากนี้ยังเป็นกลไกสำหรับตรวจสอบการเข้าสถานที่ที่ต้องห้ามด้วย ในการตรวจสอบเพื่อพิสูจน์ทราบนั้นอาจใช้รหัสผ่าน สมาร์ทการ์ด หรือไบโอเมติกก็ได้  การรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ต การติดตั้งระบบรักษาความปลอดภัยสำหรับการใช้งานอินเทอร์เน็ตนั้นเป็นระบบที่ต้องใช้ไฟร์วอลล์ และ VPN (Virtual Private Network) ซึ่งอาจต้องเปลี่ยนโครงสร้างของเครือข่าย บางทีสิ่งที่สำคัญที่สุดเกี่ยวกับการรักษาความปลอดภัยอินเทอร์เน็ตคือ ตำแหน่งของการติดตั้งระบบควบคุมการเข้าถึง เช่น ไฟร์วอลล์ ซึ่งต้องติดตั้งระหว่างอินเทอร์เน็ตและเครือข่ายภายใน ถ้าไม่มีระบบป้องกันนี้ระบบที่อยู่ภายในเครือข่ายก็ถูกเปิดให้สามารถถูกโจมตีได้ตลอดเวลา การติดตั้งไฟร์วอลล์นั้นไม่ใช่เป็นเรื่องง่าย ซึ่งบางครั้งอาจรบกวนการใช้งานอินเทอร์เน็ตของผู้ใช้ภายในด้วย ระบบตรวจจับและป้องกันการบุกรุก ระบบตรวจจับการบุกรุกหรือ IDS (Intrusion Detection System) เป็นระบบเตือนภัยของเครือข่ายสัญญาณเตือนขโมย เป็นระบบที่ใช้สำหรับตรวจจับผู้ไม่ประสงค์ดีที่พยายามจะบุกรุกเข้าสถานที่ต้องห้าม IDS ก็ทำงานคล้ายกันโดยจะแยกแยะได้ระหว่างการเข้าถึงส่วนของเครือข่ายที่ต้องห้ามที่ได้รับอนุญาตหรือเป็นการเข้ามาโดยผิดปกติ IDS นั้นมีหลายประเภท การเลือกใช้งานนั้นก็ขึ้นอยู่กับความเสี่ยงและทรัพยากรที่มีอยู่ขององค์กร IDS อาจต้องใช้ทรัพยากรค่อนข้างมากจากฝ่ายรักษาความปลอดภัย ระบบตรวจจับการบุกรุกที่รู้จักกันมากที่สุดคือ ซอฟต์แวร์ป้องกันไวรัส ซึ่งซอฟต์แวร์นี้ควรต้องติดตั้งลงในคอมพิวเตอร์ทุกเครื่องรวมถึงเซิร์ฟเวอร์ด้วย ซอฟต์แวร์ป้องกันไวรัสเป็น IDS ที่ใช้ทรัพยากรน้อยที่สุด IDS อื่นๆ ประกอบด้วย • การตรวจสอบล็อคไฟล์ด้วยมือ • การตรวจสอลล็อคไฟล์แบบอัตโนมัติ • Host-based IDS • Network-based IDS การเข้ารหัสข้อมูล การเข้ารหัสข้อมูลหรือเอ็นคริพชัน (Encryption) เป็นวิธีที่ใช้ปกป้องความลับ (Confidentiality) ของข้อมูล กลไกในการเข้ารหัสข้อมูลนั้นอาจใช้สำหรับป้องกันข้อมูลในระหว่างที่ส่งผ่านเครือข่ายหรือระหว่างที่จัดเก็บในอุปกรณ์จัดเก็บข้อมูล เช่น ฮาร์ดดิสก์ เป็นต้น ในการเลือกใช้การเข้ารหัสแต่ละวิธีนั้นมี ๒ สิ่งที่ต้องพิจารณาคือ • อัลกอริธึม (Algorithms) • การบริหารคีย์ (Key Management) เมื่อติดตั้งระบบการเข้ารหัสข้อมูลนั้น จุดประสงค์ของการเข้ารหัสข้อมูลนั้นจะเป็นสิ่งที่จะกำหนดการเลือกอัลกอริธึม การเข้ารหัสแบบไพรเวทคีย์เอ็นคริพชัน (Private Key Encryption) จะทำงานเร็วกว่าพับลิกคีย์เอ็นคริพชัน (Public Key Encryption) อย่างไรก็ตามไพรเวทคีย์เอ็นคริพชันไม่สามารถใช้สำหรับการพิสูจน์ตัวตน เช่น ดิจิตอลซิกเนเจอร์ (Digital Signature) ได้ ในการเลือกอัลกอริธึมนั้นควรเลือกที่เป็นที่รู้จักดี ซึ่งได้มีการทดสอบอย่างเปิดเผยมาแล้วว่ามีประสิทธิภาพดี เพราะถ้าใช้อัลกอริธึมที่ไม่รู้จักกับระบบนั้นอาจมีช่องโหว่หรือจุดอ่อนในตัวก็ได้ ในการติดตั้งกลไกสำหรับเข้ารหัสข้อมูลนั้นจะมีบางส่วนที่เกี่ยวข้องกับการจัดการคีย์ สำหรับการเข้ารหัสแบบจุดต่อจุด (Point-to-Point) ซึ่งโดยส่วนใหญ่จะใช้การเข้ารหัสแบบไพรเวทคีย์เอ็นคริพชันนั้น ระบบต้องมีการอัพเดตคีย์เป็นประจำ ส่วนระบบที่ต้องใช้การเข้ารหัสแบบพับลิกคีย์เอ็นครพชัน ซึ่งต้องมีการแจกจ่ายใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ไปยังผู้ใช้จำนวนมากทำให้ปัญหานั้นยุ่งยากกว่า เมื่อต้องติดตั้งระบบนี้ควรต้องกำหนดให้มีเวลาสำหรับทดสอบการจัดการคีย์ด้วย ข้อควรระวังอย่างหนึ่งคือโปรแกรมทดลองนั้นส่วนใหญ่จะมีข้อกำหนดเกี่ยวกับจำนวนผู้ใช้ ในขณะที่เมือต้องติดตั้งใช้งานจริงนั้นจะเกี่ยวข้องกับผู้ใช้จำนวนที่มากกว่ามาก องค์กรไม่สามารถจะป้องกันข้อมูลที่สำคัญขององค์กรได้โดยปราศจากความร่วมมือจากพนักงานขององค์กรทุกคน การจัดการฝึกอบรมเพื่อรับทราบนั้นก็เป็นการแจ้งข้อมูลที่จำเป็นให้พนักงานแต่ละคนทราบ การฝึกอบรมนั้นอาจจัดเป็นในลักษณะของการประชุม หรือการตีพิมพ์ผ่านสื่อต่างๆ ขององค์กร เช่น วารสาร หรือปิดประกาศในที่ต่างๆ วิธีที่ดีที่สุดคือ การใช้ทั้ง ๓ วิธีควบคู่กันไปและต้องทำเป็นประจำด้วย Audit (การตรวจสอบ) การตรวจสอบ (Audit) นั้นเป็นขั้นตอนสุดท้ายของกระบวนการรักษาความปลอดภัย หลังจากที่ได้ประเมินสถานการณ์ขององค์กรแล้วก็กำหนดนโยบาย และระเบียบปฏิบัติ ติดตั้งระบบรักษาความปลอดภัยที่จำเป็น ฝึกอบรมเจ้าหน้าที่และพนักงานทั่วไป ท้ายสุดคือการตรวจสอบว่ามีการฝ่าฝืนนโยบายและระเบียบปฏิบัติหรือไม่ เมื่อเรากล่าวถึงการตรวจสอบเกี่ยวกับด้านการรักษาความปลอดภัยนั้นเรามักจะหมายถึงการตรวจสอบ ๓ ประเภทต่อไปนี้ • การตรวจสอบการปฏิบัติตามนโยบาย • การประเมินโครงการใหม่ๆ • การตรวจสอบการเจาะระบบ (Penetration Test)

# ความปลอดภัยของข้อมูล

# ข้อมูลที่ดีเป็นข้อมูลที่มีค่ามีราคา สามารถนำไปใช้ให้เกิดประโยชน์อย่างมากต่อกิจการขององค์กร และในมุมกลับกันอาจก่อให้เกิดโทษต่อองค์กรหรือบุคคลผู้ให้ข้อมูล ถ้าข้อมูลตกลงไปอยู่ในมือผู้ไม่ประสงค์ดี ดังนั้นความปลอดภัยของข้อมูล จึงเป็นเรื่องสำคัญที่จะต้องตระหนัก ความปลอดภัยของข้อมูล (data security) เป็นเรื่องที่เกี่ยวข้องกับการป้องกันไม่ให้ข้อมูลถูกทำลาย การรักษาความลับของข้อมูล และการป้องกันไม่ให้ข้อมูลถูกทำลาย การรักษาความลับของข้อมูล และการป้องกันการกระทำการทุจริตต่อข้อมูล ความไม่ปลอดภัยของข้อมูลมักมีสาเหตุจาก

# •  ความผิดพลาดของระบบ ซึ่งอาจมีสาเหตุจากตัวเครื่องคอมพิวเตอร์ ได้แก่ เครื่องคอมพิวเตอร์เกิดขัดข้องในระหว่างการประมวลผลข้อมูล ซึ่งอาจทำให้ข้อมูลเกิดสูญเสียได้ นอกจากนี้อาจมีสาเหตุจากโปรแกรมที่ใช้ในการประมวลผลยังมีข้อผิดพลาดบางจุดซึ่งอาจทำให้ข้อมูลมีความผิดพลาดหรือสูญเสียได้เช่นกัน

# •  อุบัติเหตุ เช่น ไฟไหม้ น้ำท่วม ทำให้ข้อมูลที่เก็บอยู่สูญเสียได้

# •  บุคคลอาจทำให้ข้อมูลสูญเสีย เช่น มีการสั่งลบข้อมูล หรือบันทึกข้อมูลทับของเดิม หรือบุคคลอาจมีเจตนาร้ายต้องการทำให้ข้อมูลสูญเสีย เนื่องจากความโกรธแค้นจงใจทำลายข้อมูล

# •  การขโมยข้อมูลซึ่งเป็นความลับเพื่อนำไปขายหรือให้คู่แข่ง ซึ่งสามารถทำได้ง่าย โดยแอบสำเนาลงบนแผ่นบันทึก

# •  การกระทำทุจริตต่อข้อมูล เช่น มีการแก้ไขข้อมูลที่เกี่ยวข้องกับจำนวนเงิน เพื่อประโยชน์ของตัวเองหรือมีผู้รับจ้างให้กระทำการทุจริต

# •  สาเหตุอื่น ๆ เช่น ความร้อนชื่น ฝุ่นละออง และสนามแม่เหล็ก

# **การรักษาความปลอดภัยของข้อมูลที่อาจถูกทำลาย หรือเสียหายด้วยสาเหตุต่าง ๆ ดังกล่าวนั้นอาจทำได้ดังนี้**

# •  การรักษาความปลอดภัยของอุปกรณ์ระบบคอมพิวเตอร์

# •  การทำสำเนาข้อมูล ในกรณีที่ข้อมูลอยู่ในแผ่นบันทึกอาจทำสำเนา ข้อมูลทั้งแผ่นโดยใช้คำสั่ง copy แต่ถ้าข้อมูลอยู่ในจานแม่เหล็กชนิดแข็งหรือกรณีที่มีข้อมูลเป็นจำนวนมากจะทำสำเนาโดยการใช้คำสั่ง backup ลงบนแผ่นบันทึกหรือในเทปแม่เหล็ก

# •  การรักษาความลับของข้อมูล มาตรการแรกในการป้องกันคือ การควบคุมการเข้าไปใช้เครื่องคอมพิวเตอร์ โดยกำหนดว่าใครบ้างที่สามารถเข้าไปใช้เครื่องคอมพิวเตอร์ได้ มาตรการต่อมาคือ การกำหนดรหัสผ่าน (password) เพื่อผ่านเข้าไปใช้โปรแกรมหรือการเข้าถึงข้อมูล นอกจากนี้อาจจะมีการกำหนดขอบเขตเฉพาะแฟ้มข้อมูลเฉพาะแฟ้มบุคคลเฉพาะบุคคล ไม่มีสิทธิไปใช้หรือเปลี่ยนแปลงแก้ไขข้อมูลของแฟ้มรายได้ เป็นต้น

# **การรักษาความปลอดภัยของข้อมูล**

# อีเมลเซิร์ฟเวอร์ หรือ อีเมลโฮสติ้ง จะมีข้อมูลที่เป็นความลับสูง และเป็นแหล่งโจมตีแรกๆ ของเหล่า Hacker ดังนั้นการเข้ารหัสจึงเป็นส่วนสำคัญเพื่อปกป้องไม่ให้ข้อมูลขององค์กรรั่วไหลได้

# **Data Encryption 5 ส่วนดังนี้**

# 1. การเข้ารหัสระหว่างผู้ใช้ (User) และ อีเมลโฮสติ้ง (Email Hosting)      เข้ารหัสการเชื่อมต่อ 256-Bits ผ่าน SSL/TLS รองรับผ่าน Web Mail, MS Outlook, thunderbird และมือถือทุกรุ่น

# 2. การเข้ารหัสระหว่างอีเมลโฮสติ้ง (Email Hosting) และ อีเมล์โฮ้สติ้ง (Email Hosting)     การรับส่งข้อมูลระหว่างเครื่องเซิร์ฟเวอร์ โดยการรับข้อมูลหรือส่งข้อมูลจะส่งผ่านการเข้ารหัส SSL/TLS

# 3. การเข้ารหัสระหว่างเครือข่ายลูก (Node Server)      ลูกข่ายหรือ Relay Server และ Storage Area Network เขื่อมต่อผ่านการเข้ารหัสเพื่อความปลอดภัย ด้วยการเข้ารหัสขนาด 256-Bits AES

# 4. การเข้ารหัสผ่านผู้ใช้ (Password Encryption)      ใช้การเข้ารหัสผู้ใช้ SHA ซึ่งเป็นการเข้ารหัสสูงสุดซึ่งยากต่อการถอดรหัส โดยหลายผู้ให้บริการละเลยถึงความสำคัญของการเข้ารหัสนี้

# 5. การเข้ารหัสข้อมูลอีเมล (Data Encryption)      ระบบใช้การเข้ารหัส Storage AES-256 algorithm โดยจะสามารถเปิดได้ที่เครื่องที่ระบุไว้เท่านั้น ทำให้ป้องกันการโจรกรรมข้อมูลได้เป็นอย่างดี