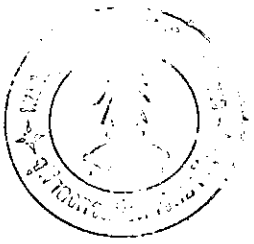


บทที่ 3

การจัดการด้านการควบคุมระบบคอมพิวเตอร์ซึ่งปฏิบัติงานในแบบ Online

เพื่ออำนวยการควบคุมระบบคอมพิวเตอร์ซึ่งปฏิบัติงานในแบบ Online อย่างมีประสิทธิภาพ จะต้องพิจารณาให้มีการควบคุม ดังต่อไปนี้

1. การควบคุมด้านการรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์

1.1 สถานที่ตั้ง ปัจจัยสำคัญที่ต้องระมัดระวังในการเลือกทำเลที่ตั้งของศูนย์คอมพิวเตอร์ ได้แก่

ก. อุทกภัย ถึงแม้ว่าน้อยครั้งที่จะปรากฏว่าอุทกภัยจะเป็นภัยต่ออุปกรณ์คอมพิวเตอร์ แต่ถ้าเกิดอุทกภัยขึ้นจริง การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ทำได้ยากลำบากกว่าอุปกรณ์อื่น ๆ ทั่วไป นอกจากนั้นในห้องคอมพิวเตอร์มักนิยมเดินสายไฟฟ้าแรงสูงไว้ใต้พื้นซึ่งอาจเกิดการลัดวงจรเป็นภัยอย่างร้ายแรงถ้าเกิดอุทกภัย ดังนั้นการเลือกทำเลที่ตั้งระบบคอมพิวเตอร์จะต้องระมัดระวังโอกาสที่จะเกิดอุทกภัยด้วย

ข. การสั่นสะเทือน อุปกรณ์คอมพิวเตอร์เป็นแผ่นจานแม่เหล็กทำงานด้วยความเร็วสูง ดังนั้นการสั่นสะเทือนนอกจากจะทำให้อุปกรณ์ดังกล่าวทำงานผิดพลาดยังอาจก่อให้เกิดขอเสียหายอย่างร้ายแรง การเลือกทำเลที่ตั้งอุปกรณ์คอมพิวเตอร์ควรจัดให้อยู่ห่างจากสิ่งที่ก่อให้เกิดการสั่นสะเทือน เช่น ทางรถไฟ ถนนซึ่งมีรถบรรทุกขนาดใหญ่วิ่งผ่าน หรือบริเวณที่มีการยกของมีน้ำหนักมาก

ค. อัคคีภัย อัคคีภัยเป็นภัยที่ร้ายแรงที่สุดที่ทำความเสียหายอย่างร้ายแรงต่อศูนย์คอมพิวเตอร์ ทั้งนี้เนื่องจากศูนย์คอมพิวเตอร์มักมีสายไฟฟ้าแรงสูง และ

มีวัสดุไวไฟมาก เช่น เทปแม่เหล็ก กระดาษพิมพ์ อุปกรณ์ประเภทสายไฟฟ้า กล่องพลาสติกบรรจุเทป และแผ่นจานแม่เหล็กเมื่อถูกอัคคีภัยจะก่อให้เกิดควันพิษซึ่งเป็นอันตรายต่อพนักงานที่ทำการดับไฟ ดังนั้นศูนย์คอมพิวเตอร์ควรจะอยู่ห่างจากทำเลที่เสี่ยงต่อการเกิดอัคคีภัย และควรมีอุปกรณ์เตือนอัคคีภัย เช่น เครื่องตรวจจับควันไฟ และอุปกรณ์ดับเพลิงอย่างพร้อมเพรียง อนึ่ง ข้อที่ควรระมัดระวังก็คือ ระบบการดับเพลิงโดยอัตโนมัติบางระบบนอกจากจะไม่สามารถป้องกันอัคคีภัยได้จริงแล้ว ยังอาจเป็นภัยต่ออุปกรณ์คอมพิวเตอร์ยิ่งกว่าอัคคีภัยเอง เช่น ระบบดับเพลิงแบบพ่นละอองน้ำจากเพดาน ถ้าเครื่องตรวจพบว่าอุณหภูมิในห้องสูงถึงขีดที่กำหนดไว้ ซึ่งมักปรากฏเสมอว่าเครื่องตรวจทำงานผิดพลาดพ่นละอองน้ำออกมาทำลายอุปกรณ์คอมพิวเตอร์ทั้ง ๆ ที่ไม่มีอัคคีภัยเกิดขึ้นจริง

1.2 <u>ระบบการจ่ายกระแสไฟ</u> (Power Supply) ระบบคอมพิวเตอร์ยุคใหม่ต้องการกระแสไฟในระหว่างการปฏิบัติงานน้อย แต่ต้องการกระแสไฟฟ้าซึ่งมีแรงดันไฟฟ้า (Voltage) คงที่ ทั้งนี้ เนื่องจากระบบคอมพิวเตอร์ยุคปัจจุบันประกอบด้วยวงจร Integrated Circuit (I.C.) ซึ่งไม่สามารถทนต่อการเปลี่ยนแปลงของแรงดันไฟฟ้าเกินกว่าพิกัดที่กำหนดไว้ ถ้ากระแสไฟฟ้าป้อนเข้าสู่ระบบคอมพิวเตอร์มีแรงดันไฟฟ้าขึ้นลงไม่คงที่ นอกจากจะทำให้ระบบคอมพิวเตอร์ทำงานผิดพลาดแล้ว ยังอาจทำให้อุปกรณ์เหล่านั้นเสียหายได้โดยง่าย โดยเฉพาะแผ่นจานแม่เหล็ก ซึ่งมักเสียหายถ้ามีแรงดันไฟฟ้า "กระตุก" การเดินสายไฟมายังห้องคอมพิวเตอร์ควรต่อตรงจากสายไฟฟ้าหลัก และไม่ควรมีการต่อไฟฟ้าแยกไปยังจุดอื่นอีก นอกจากนั้นควรจะมีระบบ Regulated Power Supply เพื่อปรับแรงดันไฟฟ้าให้คงที่ก่อนต่อเข้าสู่ระบบคอมพิวเตอร์

1.3 <u>การระมัดระวังวินาศภัย</u> นับตั้งแต่ปี ค.ศ. 1968 เป็นต้นมา

ได้เกิดการก่อวินาศภัยในศูนย์คอมพิวเตอร์หลายครั้ง เช่น [1]

ในปี ค.ศ. 1968 บุคคลลึกลับใช้อาวุธปืนยิงเครื่องคอมพิวเตอร์ IBM 1401 ใน State of Employment Office, Olympia, Washington

ในปี ค.ศ. 1972 บุคคลลึกลับใช้อาวุธปืนยิงผ่านหน้าต่างไปทำลายคอมพิวเตอร์ซึ่งใช้ใน Municipal Office ของเมือง Johannesburg ใน South Africa และ Honeywell Computer ของ New York Bank สหรัฐอเมริกา ถูกลอบทิ้งแทงด้วยของแหลมคม เช่น ไขควง ซึ่งค่าใช้จ่ายในการซ่อมแซมเป็นเงิน $ 589,000

ในระหว่างปี ค.ศ. 1970 ถึง 1975 ซึ่งเป็นช่วงที่มีการจลาจลระหว่างคนผิวขาวและผิวดำ และการต่อต้านสงครามเวียตนาม ปรากฏว่าศูนย์คอมพิวเตอร์ในมหาวิทยาลัยหลายแห่งที่รับงานวิจัยจากกระทรวงกลาโหมสหรัฐอเมริกาได้รับการโจมตีจากประชาชน

นอกจากนี้ศูนย์คอมพิวเตอร์ของ University of Wisconsin ที่ Army Mathematic Research Center ถูกวางระเบิด ทำให้มีคนตาย 1 คน บาดเจ็บสาหัส 3 คน และเกิดความเสียหายทางด้านอุปกรณ์เป็นจำนวนสูงมากกว่า $ 2.5 ล้าน รวมทั้งสูญเสียข้อมูลผลการวิจัยซึ่งสะสมมาเป็นเวลานานกว่า 20 ปี มีมูลค่าประเมินเป็นจำนวนสูงมากกว่า $ 16 ล้าน

ในปี ค.ศ. 1973 กลุ่มต่อต้านสงครามได้ใช้ระเบิดเพลิงขว้างใส่ศูนย์คอมพิวเตอร์ของ Fresno State College ในรัฐ California ทำให้อุปกรณ์เสียหายเป็นจำนวนสูงมากกว่า $ 1 ล้าน

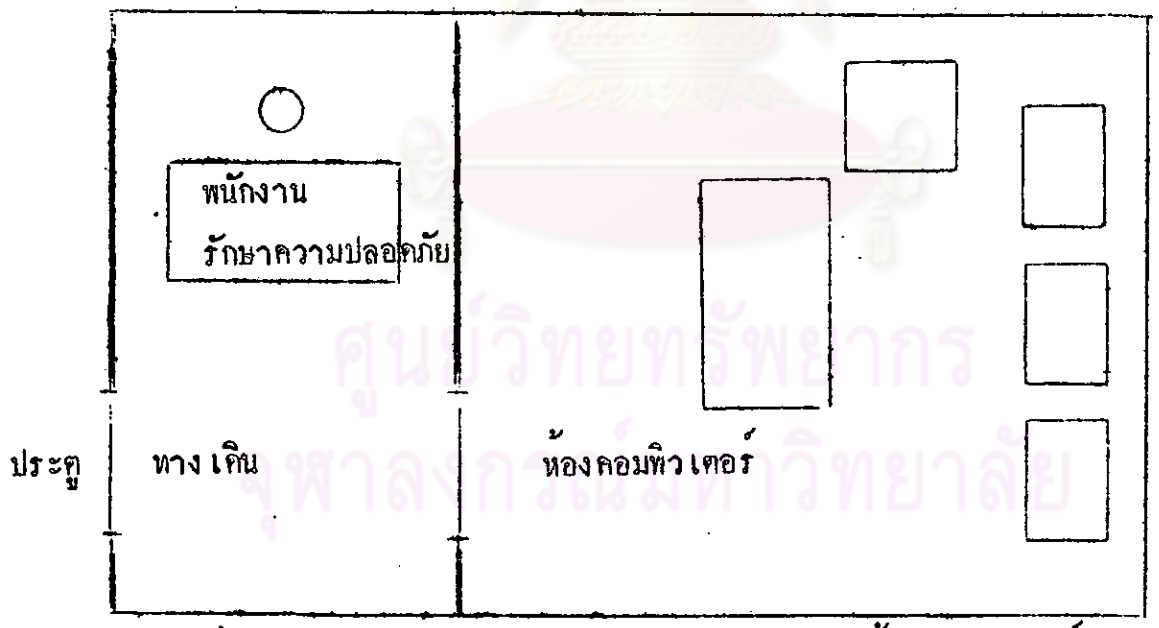
---

[1] Thomas Whiteside, Computer Capers, New York: The New American Library, Inc., 1979, p. 4-5.

ในปี ค.ศ. 1974 นักศึกษาผิวดำได้วางระเบิดเพลิงศูนย์คอมพิวเตอร์ของ New York University และขู่จะทำการระเบิดยกเว้นมหาวิทยาลัยฯ จะจ่ายเงิน $ 100,000 เป็นค่าประกันสมาชิกสมาคม Black Panther ที่ถูกคุมขัง แต่มหาวิทยาลัย ฯ รีบไปยังศูนย์คอมพิวเตอร์และถอดชนวนระเบิดได้ทันเวลา

จากตัวอย่างกรณีการเกิดวินาศภัยดังกล่าวมาแล้ว ศูนย์คอมพิวเตอร์ในปัจจุบันจึงนิยมตั้งในทำเลที่สามารถควบคุมเส้นทางการผ่านเข้าออกได้ง่าย ซึ่งต่างกับศูนย์คอมพิวเตอร์สมัยก่อน ซึ่งนิยมจัดทำในลักษณะตู้โชว์หรือที่เรียกว่า "Glass Palace" การผ่านเข้าออกศูนย์คอมพิวเตอร์จะมีการควบคุมในลักษณะที่เป็นด่าน ซึ่งอาจแบ่งเป็น 2 ประเภทคือ

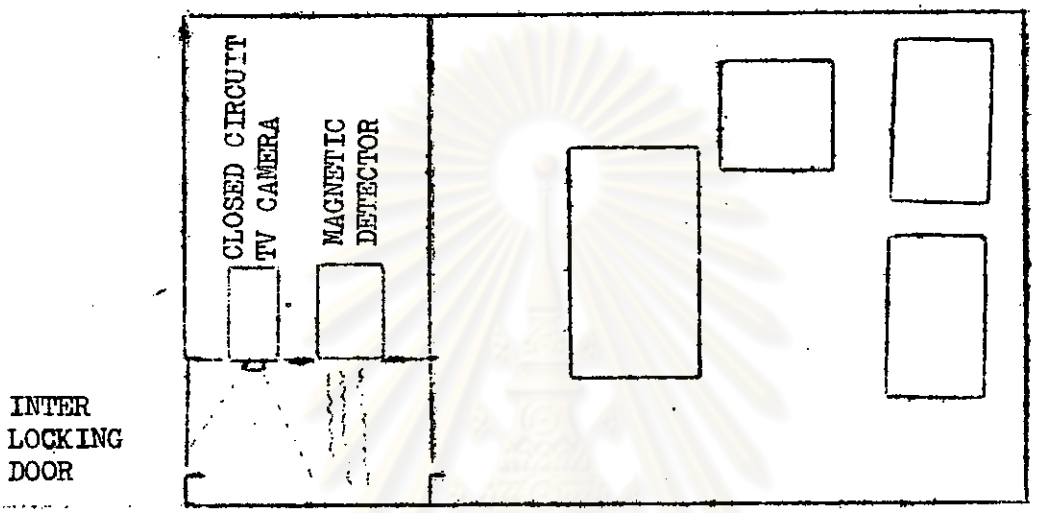
(1) ใช้ระบบควบคุมโดยพนักงานรักษาความปลอดภัย



แผนภาพที่ 3.1 การใช้พนักงานรักษาความปลอดภัยควบคุมห้องคอมพิวเตอร์

ผู้ที่จะผ่านเข้าไปยังศูนย์คอมพิวเตอร์จะต้องผ่านโต๊ะของพนักงานรักษาความปลอดภัย ซึ่งจะยอมให้เฉพาะผู้ที่มีอำนาจหน้าที่เท่านั้นผ่านเข้าไปได้

(2) ใช้ระบบควบคุมโดยอุปกรณ์อีเลคโทรนิค เช่น โทรทัศน์วงจรปิด ระบบกุญแจแบบรหัส หรือ Badge Reader



แผนภาพที่ 3.2 การใช้ระบบอุปกรณ์อีเลคโทรนิคควบคุมความปลอดภัยในห้องคอมพิวเตอร์

นอกจากการก่อวินาศภัยจะเกิดจากบุคคลภายนอกแล้ว บางครั้งวินาศภัยอาจเกิดจากบุคคลภายในเอง ซึ่งมักมีสาเหตุมาจากสภาพความกดดันในการทำงาน เช่น ในปี ค.ศ. 1972 คอมพิวเตอร์ของ National Farmers Union Service Corporation เมือง Denver ซึ่งรับทำการปฏิบัติข้อมูลของ Farmer Union Insurance ด้วยเครื่อง Burroughs 3500 เกิดขัดข้องถึง 56 ครั้ง และต้องเสียค่าซ่อมบำรุง $ 500,000 ต่อมาได้ใช้ระบบโทรทัศน์วงจรปิดจึงทราบว่าข้อขัดข้องเกิดจากพนักงานควบคุมเครื่องใช้กุญแจรถยนต์หย่อนลงในระบบแผ่นจานแม่เหล็ก ทำให้กระแสไฟฟ้าลัดวงจร ผู้กระทำผิดรับสารภาพว่าต้องการเพียงจะหยุดคอมพิวเตอร์ และในปี ค.ศ. 1974 พนักงานควบคุมคอมพิวเตอร์ของ Charlotte Liberty Mutual Life Insurance Company แห่ง Charlotte North Caroline ใช้อาวุธปืนยิงคอมพิวเตอร์เนื่องจากทำงานผิดพลาด

เพื่อป้องกันมิให้พนักงานของกิจการก่อวินาศภัยต่อระบบคอมพิวเตอร์

กิจการหลายแห่งจึงนิยมใช้ระบบ Buddy System กำหนดมิให้พนักงานอยู่ในห้องคอมพิวเตอร์ขณะใดขณะหนึ่งเพียงคนเดียว จะต้องมีบุคคลอื่นอยู่ด้วยอย่างน้อย 1 คน นอกจากนั้นกิจการหลายแห่งยังนิยมใช้ระบบ Badge Control Area กำหนดให้พนักงานที่ปฏิบัติงานในห้องคอมพิวเตอร์ติดแถบสี และกำหนดด้วยว่าพนักงานติดแถบสีแบบใดจะสามารถเข้าไปในบริเวณใดของห้องคอมพิวเตอร์ได้บ้าง ทั้งนี้เพื่อควบคุมมิให้ผู้ที่มิได้มีหน้าที่เกี่ยวข้องเข้าไปใกล้จุดสำคัญที่อาจเป็นภัยต่อระบบคอมพิวเตอร์และเพื่อป้องกันการก้าวก่ายหน้าที่ซึ่งกันและกันอีกด้วย

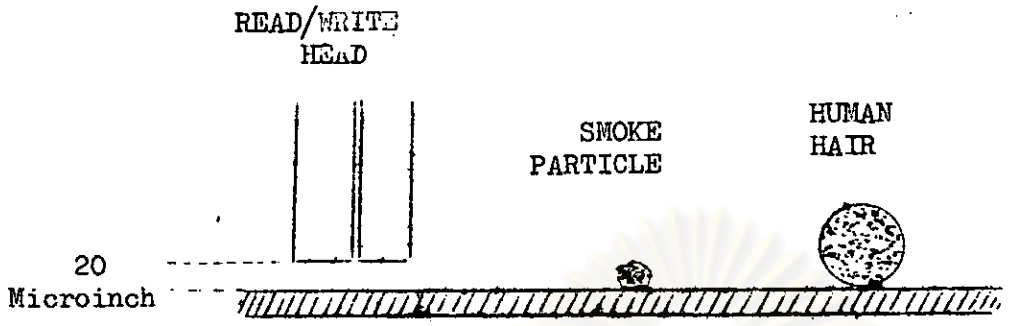
2. <u>การควบคุมด้านการรักษาความปลอดภัยของข้อมูล</u>

<u>การรักษาความปลอดภัยของวัสดุข้อมูล</u>

ในระบบคอมพิวเตอร์ ข้อมูลซึ่งถูกบันทึกในวัสดุข้อมูลประเภทแผ่นจานแม่เหล็กมีโอกาสที่จะเสื่อมสภาพได้ง่าย เนื่องจากความร้อน, ความชื้น, ฝุ่นละออง และสารแม่เหล็ก

<u>ความร้อนและความชื้น</u> ความร้อนอาจทำให้สภาพการเรียงตัวของจุดแม่เหล็กซึ่งมี Pattern เป็นรหัสแทนข้อมูลผิดสภาพจากเดิม ซึ่งในกรณีเช่นนี้มักเกิดจากการวางวัสดุข้อมูลถูกแสงอาทิตย์โดยตรงเป็นเวลานาน หรือเก็บวัสดุข้อมูลไว้ในบริเวณที่มีอากาศร้อน ส่วนความชื้นทำให้เกิด Oxide ในเนื้อสารแม่เหล็ก และไม่สามารถอ่านข้อมูลที่บันทึกไว้ได้ อย่างไรก็ดีวัสดุข้อมูลสามารถทนความร้อนได้สูงถึง 250 องศาฟาเรนไฮต์ในเวลานานพอสมควร แต่ถ้านำความร้อนและความชื้นมารวมกันจะเป็นอันตรายต่อวัสดุข้อมูลอย่างยิ่ง เช่น วัสดุข้อมูลอาจสูญเสียข้อมูลที่บันทึกไว้ถ้านำมาเก็บในที่มีอุณหภูมิเพียง 130 องศาฟาเรนไฮต์ แต่มีความชื้นร้อยละ 85 ดังนั้นเพื่อป้องกันการสูญเสียข้อมูล จึงต้องควบคุมการเก็บรักษาวัสดุข้อมูลโดยรัดกุม และสอดส่องห้ามการนำข้อมูลออกจากห้องคอมพิวเตอร์โดยไม่จำเป็น

แผนภาพที่ 3.3 ขนาดของฝุ่นละออง เมื่อเทียบกับช่องว่างของหัวอ่าน/บันทึก



ฝุ่นละออง ในระหว่างปฏิบัติงานหัวอ่าน/บันทึกของแผ่นจานแม่เหล็กจะลอยตัวเหนือพื้นผิวของแผ่นจานแม่เหล็กน้อยกว่า 20 Micro inch ด้วยความเร็วไม่ต่ำกว่า 140 ไมล์ต่อชั่วโมง ขณะที่ฝุ่นละอองจากควันบุหรี่มีขนาดเส้นผ่าศูนย์กลางประมาณ 25 Micro inch จะเห็นได้ว่าถ้ามีฝุ่นละอองแม้เพียงเล็กน้อย ย่อมทำให้พื้นผิวของแผ่นจานแม่เหล็กเสียสภาพการบันทึกข้อมูล หรือทำให้หัวอ่าน/บันทึกเสียหายได้ การจัดเก็บและการใช้งานแผ่นจานแม่เหล็กต้องคำนึงถึงเรื่องฝุ่นละอองเป็นอย่างมาก และควรมีข้อกำหนดห้ามการสูบบุหรี่ในห้องคอมพิวเตอร์ เพราะนอกจากจะก่อให้เกิดอัคคีภัยได้ง่ายแล้ว ยังอาจทำให้อุปกรณ์จัดเก็บข้อมูลขัดข้องได้ง่าย

อนึ่ง ความร้อน, ความชื้น และฝุ่นละอองยังเป็นอันตรายต่ออุปกรณ์คอมพิวเตอร์ส่วนอื่น ๆ ด้วย เพราะระบบวงจรของคอมพิวเตอร์ยุคปัจจุบันประกอบด้วยวงจรแบบ Integreated Circuit (I.C.) ซึ่งเป็นวงจรย่อส่วนขนาดเล็ก ความร้อนอาจทำให้ I.C. เสื่อมสภาพ และความชื้นรวมกับฝุ่นละอองอาจทำให้กระแสไฟฟ้าลัดวงจรใน I.C. ได้โดยง่าย

สารแม่เหล็ก ข้อมูลที่บันทึกในแผ่นจานแม่เหล็กอยู่ในสภาพการเรียงตัวของจุดแม่เหล็กเป็น pattern แทนข้อมูล ดังนั้นถ้ามีสารแม่เหล็กเคลื่อนผ่านในระยะใกล้ แรงดึงดูดของสารแม่เหล็กย่อมทำให้สภาพการเรียงตัวผิดไปจากเดิม ทำให้ข้อมูลที่บันทึกไว้เสียสภาพ การที่ข้อมูลถูกทำลายโดยสารแม่เหล็กอาจเกิดขึ้นได้ทั้งกรณีไม่เจตนาและเจตนากระทำให้เกิดความเสียหาย

กรณีที่ข้อมูลถูกทำลายด้วยสารแม่เหล็กโดยไม่เจตนามักเกิดขึ้นเนื่องจากเครื่องประดับหรือเครื่องใช้ของพนักงานในห้องคอมพิวเตอร์ได้กลายสภาพเป็นแม่เหล็กโดยไม่รู้ตัว และพนักงานได้เคลื่อนที่ผ่านวัสดุข้อมูล หรือกรณีซึ่งเกิดขึ้นที่ Chemical Bank ใน New York แผ่นจานแม่เหล็กที่ใช้เก็บข้อมูลบัญชีเงินฝากกระแสรายวันเกิดขัดข้องระหว่างการปฏิบัติงาน พนักงานซ่อมบำรุงได้ใช้ไฟฉายขนาดเล็กส่องดูวงจรภายในโดยไม่ระวังว่าตอนปลายของไฟฉายนั้นมีสภาพเป็นแม่เหล็ก ข้อมูลส่วนที่ไฟฉายเคลื่อนผ่านถูกทำลาย

กรณีที่ข้อมูลถูกทำลายด้วยสารแม่เหล็กด้วยเจตนากระทำให้เกิดความเสียหาย ได้แก่กรณีที่เกิดขึ้นในปี ค.ศ. 1970 บริษัทแห่งหนึ่งใน Cleveland, Ohio ไล่พนักงานออกจากงาน ในตอนบ่ายหลังจากพนักงานทุกคนในบริษัทออกไปรับประทานอาหาร พนักงานผู้นั้นได้แอบเข้าไปในห้องเก็บเทปแม่เหล็ก และใช้แท่งแม่เหล็กขนาดเล็กที่ซ่อนไว้ในมือทำลายข้อมูลที่สำคัญทั้งหมด บริษัทต้องจ้าง CPA (Certified Public Accountant) มาทำการสร้างข้อมูลทดแทนด้วยจำนวนเงินมากจนเกือบต้องเลิกกิจการ และ[1]บริษัทประกันภัยแห่งหนึ่งใน Hartford Connecticut พบว่าพนักงานหญิงสังกัดศูนย์คอมพิวเตอร์ผู้หนึ่งมีความสัมพันธ์กับพนักงานชาย 2 คน ซึ่งทำงานด้วยกันในเวลาเดียวกัน นอกจากจะก่อให้เกิดข้อวิวาทแล้ว ยังเป็นการขัดต่อระเบียบของบริษัท ผู้ตรวจการได้แจ้งให้พนักงานหญิงผู้นั้นออกจากงานภายใน 30 วัน โดยให้โอกาสหางานที่อื่นไปพลางก่อน หลังจากรับแจ้งพนักงานหญิงผู้นั้นได้ลักลอบลบข้อมูลสำคัญจากวัสดุข้อมูลซึ่งรวมทั้งข้อมูลจริงและข้อมูลสำรอง(Back up) แล้วจัดเก็บวัสดุข้อมูลให้ผิดจากตำแหน่งโดยปิดป้ายปลอม หลังจากพนักงานหญิงผู้นั้นออกจากบริษัท บริษัทต้องเสียค่าใช้จ่ายในการสร้างระบบข้อมูลใหม่เป็นจำนวนมากกว่า $ 10 ล้าน อย่างไรก็ตามบริษัทมิได้ดำเนินคดีกับผู้กระทำผิดซึ่งไม่อาจที่จะชดใช้ค่าเสียหายได้

---

[1]Ibid, p. 54.

I16624300

<u>การขโมยวัสดุข้อมูล</u> การขโมยวัสดุข้อมูลอาจเกิดจากทั้งกรณีไม่มีเจตนา หรือเจตนากระทำเพื่อเรียกร้องเงินค่าไถ่

กรณีการขโมยวัสดุข้อมูลโดยไม่เจตนาได้แก่ การที่ผู้เข้าชมศูนย์คอมพิวเตอร์ของบริษัทประกันภัยแห่งหนึ่งแล้วหยิบวัสดุข้อมูลกลับไปด้วยเพื่อเป็นที่ระลึก ซึ่งบริษัทประกันภัยต้องเสียค่าใช้จ่ายเป็นจำนวนมากในการสอบสวนเรียกคืน

กรณีการขโมยวัสดุข้อมูลโดยเจตนากระทำเพื่อเรียกร้องเงินค่าไถ่เกิดขึ้นเมื่อปี ค.ศ. 1973 ในประเทศเยอรมัน อดีตพนักงานควบคุมคอมพิวเตอร์ได้บุกรุกเข้าไปในศูนย์คอมพิวเตอร์ของบริษัทแห่งหนึ่งและขโมยวัสดุข้อมูลประเภทเทปแม่เหล็กซึ่งเก็บข้อมูลสำคัญทั้งข้อมูลจริงและข้อมูลสำรอง (Back up) ประมาณ 20 ม้วน และเรียกร้องเงินค่าไถ่ DM 200,000 บริษัทยินยอมจ่ายเงินค่าไถ่เนื่องจากคำนวนพบว่าการสร้างข้อมูลทดแทนจะต้องใช้เวลาและค่าใช้จ่ายมากกว่า[1] และในปี ค.ศ. 1977 หัวหน้าพนักงานพัฒนาโปรแกรมของ Imperial Chemical Industries, Ltd. ในกรุง Rotterdam ได้ขโมยวัสดุข้อมูลประเภทเทปซึ่งเก็บข้อมูล – ผลการปฏิบัติงานภาคพื้นยุโรปทั้งข้อมูลจริงและข้อมูลสำรอง (Back up) เพื่อเรียกร้องเงินค่าไถ่โดยกำหนดให้จ่ายเงินค่าไถ่ที่ Oxford Street ในกรุง London ตำรวจอังกฤษจับกุมผู้กระทำผิดได้ และอีกกรณีหนึ่งที่ Los Angeles Airport ในสหรัฐอเมริกา คนร้ายได้ขโมยเทปส่งมาจาก Bank of America 2 ม้วน เนื่องจากเข้าใจว่าบันทึกข้อมูลสำคัญทางด้านการเงิน และเรียกร้องเงินค่าไถ่ อย่างไรก็ตามธนาคารดังกล่าวปฏิเสธการจ่ายเงิน เพราะยังมีเทปข้อมูลสำรองเก็บไว้

---

[1] Ibid, p. 41.

มาตรการควบคุมด้านการรักษาความปลอดภัยของข้อมูล

การป้องกันวัสดุข้อมูลเสื่อมสภาพอันเนื่องมาจากความร้อน ความชื้น และฝุ่นละอองอาจทำได้โดยการจัดระบบปรับอากาศ และระบบควบคุมความชื้นที่เหมาะสม นอกจากนั้นเพื่อป้องกันการทำลายข้อมูลด้วยสารแม่เหล็ก หรือการขโมยเพื่อเรียกร้องค่าไถ่ ควรมีระบบป้องกันการเข้าออกในศูนย์คอมพิวเตอร์ดังได้กล่าวมาแล้ว การป้องกันการลักลอบนำสารแม่เหล็กเข้าไปในห้องคอมพิวเตอร์อาจกระทำได้โดยติดตั้งอุปกรณ์ตรวจจับสารแม่เหล็กในช่องทางเข้าสู่ห้องคอมพิวเตอร์ นอกจากนั้นยังควรใช้ระบบ Buddy System และ Bedge Control Area เพื่อป้องกันการเจตนาทำลายข้อมูลควบคู่ไปด้วย

สิ่งที่ควรระมัดระวังเป็นพิเศษคือ กรณีที่มีคำสั่งให้พนักงานออกจากงาน เนื่องจากพนักงานได้รับคำสั่งให้ออกจากงานอาจมีความโกรธแค้นต่อกิจการ จนชักนำให้เกิดการทำลายข้อมูล ดังนั้นในทางปฏิบัติ การมีคำสั่งให้พนักงานในศูนย์คอมพิวเตอร์ออกจากงานมักจะกระทำโดยฉับพลัน และไม่เปิดโอกาสให้พนักงานผู้นั้นกลับเข้าไปยังห้องคอมพิวเตอร์อีก หรือถ้ามีความจำเป็นหลีกเลี่ยงไม่ได้มักจะต้องจัดพนักงานอื่นควบคุม บางครั้งการมีคำสั่งให้ออกจากงานอาจกระทำโดยย้ายพนักงานผู้นั้นไปยังแผนกอื่นซึ่งไม่เกี่ยวกับการปฏิบัติข้อมูลชั่วคราวจนกว่าจะมีคำสั่งให้ออกจากงาน

เมื่อมีคำสั่งให้พนักงานในศูนย์คอมพิวเตอร์ออกจากงาน ควรเรียกกุญแจ, บัตร และเครื่องหมายอื่น ๆ ที่ใช้ในการเข้าออกศูนย์คอมพิวเตอร์คืน ระบบป้องกัน เช่น กุญแจ password ควรมีการเปลี่ยนแปลง และพนักงานผู้อื่นควรได้รับการแจ้งให้ทราบโดยพลันเพื่อให้ช่วยระมัดระวังการทำลายข้อมูล

ถึงแม้จะมีมาตรการควบคุมด้านการรักษาความปลอดภัยของข้อมูลรัดกุมเพียงใดก็ตาม แต่โอกาสที่ข้อมูลจะสูญเสียมีอยู่เสมอ เช่น เกิดจากการพลั้งเผลอ ข้อมูลย่อมเป็นหัวใจสำคัญในการดำเนินกิจการ ดังนั้น จึงต้องระมัดระวังเป็นกรณีพิเศษ มาตรการที่สำคัญในด้านการรักษาความปลอดภัยของข้อมูลที่ละเลยเสียไม่ได้

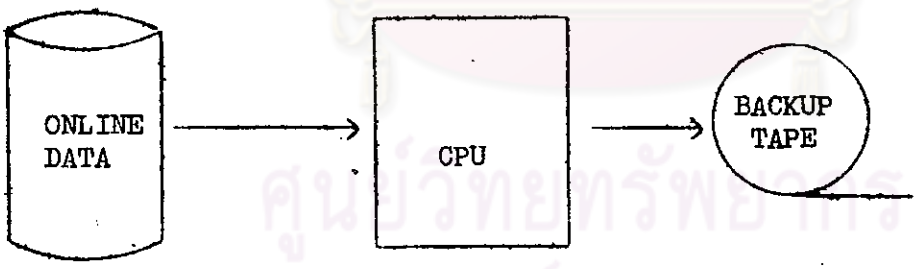
ประการหนึ่ง คือการสร้างระบบ ข้อมูลสำรอง (Back up System)

ระบบการสร้างข้อมูลสำรอง คือการ Copy ข้อมูลที่ใช้อยู่ถ่ายทอดไปจัดเก็บไว้ในวัสดุข้อมูลอื่นเพื่อเป็นข้อมูลสำรอง ในกรณีที่ข้อมูลจริงเกิดเสื่อมสภาพหรือสูญหายจะได้สามารถนำข้อมูลสำรองนั้นมาใช้แทนข้อมูลจริงต่อไป

วิธีการ Back up ข้อมูล

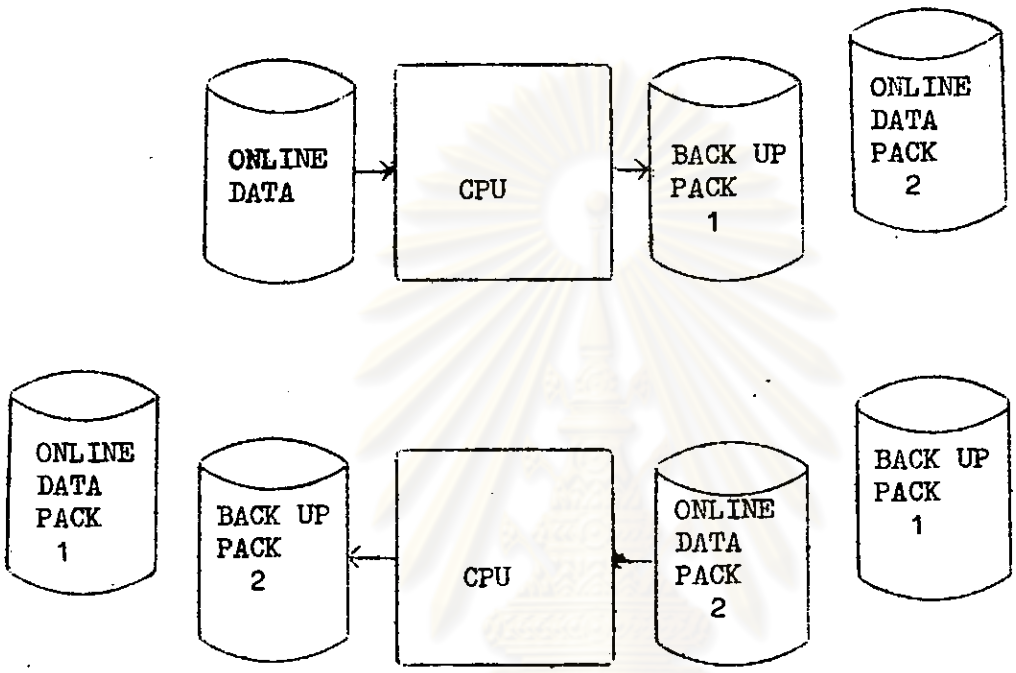
ในการปฏิบัติข้อมูลแบบ Online ข้อมูลที่ใช้ในการปฏิบัติงานประจำวันมักบันทึกอยู่ในแผ่นจานแม่เหล็กเป็นส่วนใหญ่ วิธีการ Back up ข้อมูลย่อมขึ้นอยู่กับอุปกรณ์ซึ่งกิจการใช้อยู่

ตัวอย่างวิธีการ Back up ข้อมูล



แผนภาพที่ 3.4 การ Back up ข้อมูลใน Disk Pack 1 Unit สู่ Tape

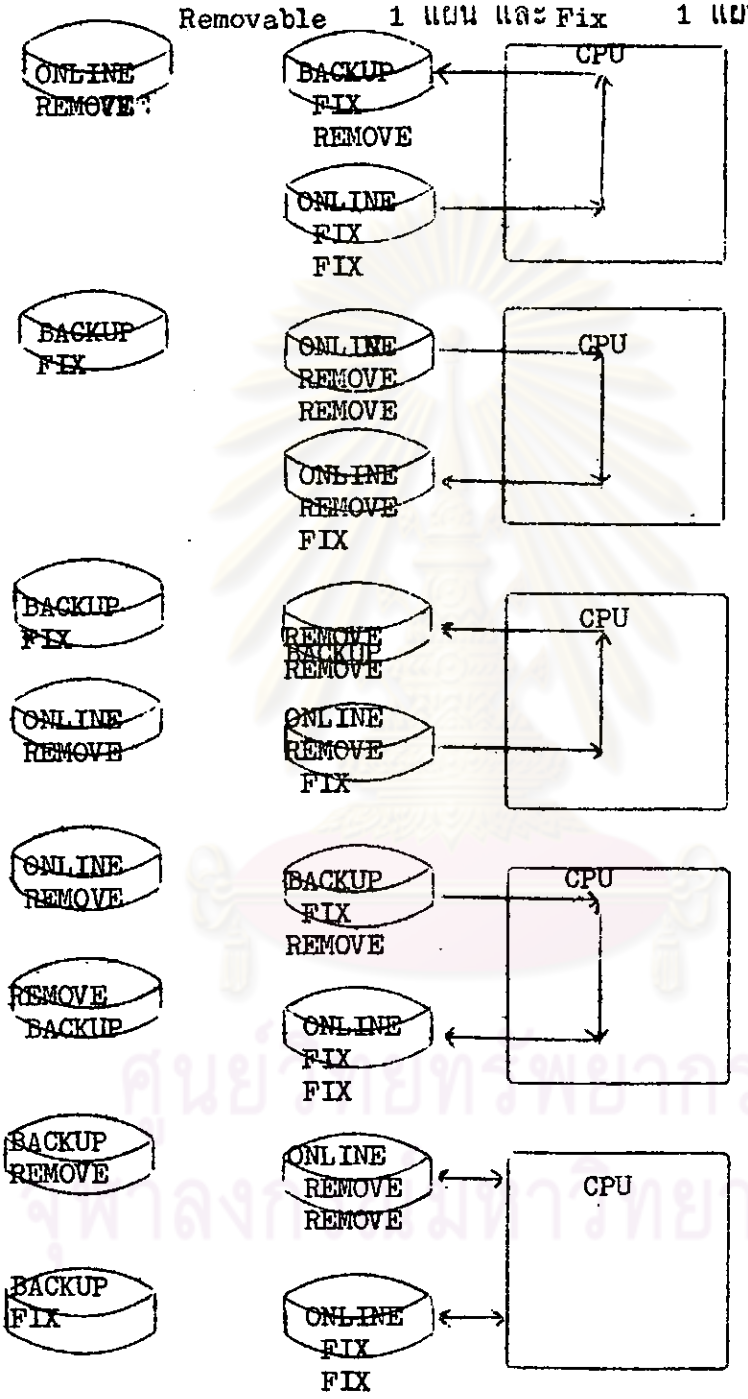
ก. ถ้าในระบบคอมพิวเตอร์มีอุปกรณ์จัดเก็บข้อมูลประเภท Disk Pack 1 Unit หรือ Fixed Disk และเทป การ Back up ข้อมูลอาจทำโดย Dump ข้อมูล Online จาก Disk Pack ไปเก็บยังเทปที่ใช้ Back up



แผนภาพที่ 3.5 การ Back up ข้อมูลใน Disk Pack 2 Unit

ข. ถ้าในระบบคอมพิวเตอร์ประกอบด้วย Disk Pack 2 Unit การ Back up สามารถกระทำโดย Dump ข้อมูลจาก Drive หนึ่งไปยังอีก Drive หนึ่งที่เตรียม Back up Pack ไว้เมื่อเสร็จสิ้นก็จะทำการ Dump ข้อมูลในทางกลับกัน

แผนภาพที่ 3.6 การ Back up ข้อมูลจาก Catridge Disk ซึ่งประกอบด้วย Removable 1 แผน และ Fix 1 แผน



ค. ถ้าในกรณีที่ในระบบคอมพิวเตอร์ประกอบด้วย Catridge Disk ซึ่งมีแผ่นหนึ่งเป็น Fixed Disk และอีกแผ่นหนึ่งเป็น Removable Disk การ Back up อาจกระทำโดย

(1) ถอดแผ่น Removable ออกและทำการ Back up ข้อมูลจากแผ่น Fixed ใน Blank Catridge

(2) Dump ข้อมูล Online จากแผ่น Removable ไปยังแผ่น Fixed

(3) Dump ข้อมูลจากแผ่น Fixed มาเป็นข้อมูล Back up ของแผ่น Removable

(4) Dump ข้อมูล Back up จากแผ่น Fixed มาบันทึกในแผ่น Fixed

(5) นำข้อมูล Online จากแผ่น Removable กลับเข้าที่เดิม

ข้อควรระมัดระวังในระบบการ Back up ข้อมูล

1. ระเบียบปฏิบัติในเรื่องการ Back up จะต้องกำหนดระยะเวลาในการ Back up ไว้อย่างแน่นอน เช่น ทุกสิ้นวันทำการ หรือทุกสัปดาห์ และจะต้องมีการตรวจตราให้มีการปฏิบัติตามระเบียบปฏิบัติอย่างเคร่งครัด ตัวอย่างกรณีที่มักเกิดขึ้นก็คือ พนักงานในศูนย์คอมพิวเตอร์มักปฏิบัติตามระเบียบอย่างเคร่งครัดในระยะแรก แต่เนื่องจากขั้นตอนการ Back up ยุ่งยากและใช้เวลานาน จึงมักจะละเลย ซึ่งจะก่อให้เกิดความเสียหายอย่างมากในกรณีที่ข้อมูลจริงเกิดเสียหาย

อนึ่ง ผู้บริหารควรหลีกเลี่ยงวิธีปฏิบัติในด้านการ Back up บางวิธีซึ่งแม้จะกระทำได้แต่ยุ่งยากมากในทางปฏิบัติ เช่น ระบบการ Back up โดยใช้วิธี Dump ข้อมูลจาก Fixed Disk มา Back up ใน Diskette ซึ่งเป็น Disk ขนาดเล็ก สมมติว่ามีข้อมูลจัดเก็บใน Fixed Disk 10 MB (10 ล้านตัวอักษร)

ในขณะที่ Diskette มีความจุแผ่นละ 0.25 MB (250,000 ตัวอักษร) จะต้องใช้ Diskette ในการ Back up ถึง 40 แผ่น ซึ่งถ้าใช้เวลาในการ Dump แผ่นละ 5 นาที จะต้องใช้เวลาทั้งสิ้น 200 นาที หรือประมาณ $3\frac{1}{2}$ ชั่วโมง ถ้าระบบการ Back up ไม่สะดวกในทางปฏิบัติหรือใช้เวลามากเกินสมควร มักปรากฏอยู่เสมอที่ผู้ปฏิบัติงานละเลยการปฏิบัติตามระเบียบปฏิบัติในการ Back up ที่วางไว้

2. ข้อมูล Back up ควรจะจัดเก็บแยกจากข้อมูลจริงที่ใช้อยู่ประจำวัน เช่นแยกเก็บในสาขาหรืออาคารหลังอื่น ทั้งนี้เพื่อป้องกันมิให้ทั้งข้อมูลจริงและข้อมูล Back up ถูกทำลายในเวลาเดียวกัน กรณีที่เกิดอัคคีภัยหรือวินาศภัย

3. ในบางครั้งแม้จะมี Back up Disk File ก็ตาม แต่ผู้ใช้อาจทำลายข้อมูล Back up นั้นด้วยความรู้เท่าไม่ถึงการ ตัวอย่าง เช่น ในกรณีที่ Disk Drive เกิดขัดข้องเนื่องจากหัวอ่าน/บันทึกครูดกับพื้นผิวแผ่นจานแม่เหล็กจนคดงอและข้อมูลเสียหาย เมื่อเกิดข้อขัดข้องผู้ใช้มักรีบ Load แผ่น Back up สู่ Disk ที่ขัดข้องโดยไม่สืบสวนสาเหตุของข้อขัดข้องเสียก่อน ทำให้ Back up Disk พลอยถูกทำลายจากหัวอ่าน/บันทึกที่ผิดปกติไปด้วย ดังนั้นจึงควรวางกฎเกณฑ์ไว้ว่าในกรณีที่เกิดข้อขัดข้องใน Disk Drive โดยไม่ทราบสาเหตุแน่ชัด ควรจะปรึกษากับพนักงานซ่อมบำรุงก่อน และควรมีแผ่นจานแม่เหล็กทดสอบเตรียมไว้ เพื่อทดสอบว่าข้อขัดข้องเกิดจากหัวอ่าน/บันทึกผิดปกติหรือไม่ ก่อนที่จะทำการ Load แผ่น Back up ถ้าพบว่าข้อขัดข้องไม่ได้เกิดจากหัวอ่าน/ บันทึกผิดปกติ ก่อนจะใช้ข้อมูลจากแผ่น Back up ควรจะทำการ Dump ข้อมูลจากแผ่น Back up เพื่อ Back up ไว้อีกชั้นหนึ่ง

ในการปฏิบัติข้อมูลแบบ Online ซึ่งทำการ Update ข้อมูลที่จัดเก็บไว้ตลอดเวลา ในกรณีที่สูญเสียข้อมูลในระหว่างช่วงเวลาปฏิบัติงานถึงแม้จะมีข้อมูล Back up แต่ก่อนจะนำข้อมูล Back up นั้นมาใช้งานต่อเนื่องอาจต้องทำการ Update ข้อมูลที่มีการเปลี่ยนแปลงระหว่างช่วงเวลานับจากมีการ Back up จนถึงช่วงที่เกิดการสูญเสียข้อมูลเสียก่อน ดังนั้นจะต้องมีการวางมาตรการ Recovery ความเสียหายที่เกิดขึ้น เพื่อให้สามารถปฏิบัติงานปกติต่อไปได้ในเวลาที่สั้นที่สุด

แผนภาพที่ 3.7 การ Recovery

วิธีการ Recovery ง่าย ๆ ก็คือ จัดเตรียมโปรแกรม Update ในแบบ Batch ไว้ และนำรายการ Transaction ประจำวันมา Update Back up File จนได้ข้อมูลที่เป็นปัจจุบัน อนึ่ง ถ้าเป็นไปได้ควรบันทึก Transaction File ไว้ใน Disk Drive แยกจาก Unit ที่บันทึก Master File เพื่อป้องกันข้อมูลรายการ Transaction ถูกทำลายไปพร้อมกับข้อมูลใน Master File

3. <u>การควบคุมด้านการป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยผู้ไม่มีอำนาจหน้าที่</u>

มักจะปรากฏอยู่เสมอที่มีผู้ลักลอบใช้อุปกรณ์คอมพิวเตอร์ทั้ง ๆ ที่ไม่มีอำนาจหน้าที่เพื่อผลประโยชน์ส่วนตน เช่น ใช้คอมพิวเตอร์ทำการปฏิบัติข้อมูลให้แก่บุคคลภายนอก มาตรการป้องกันดังกล่าวมีหลายระดับดังนี้

3.1 Physical Lock ได้แก่ การใช้ระบบกุญแจป้องกันมิให้ผู้ไม่มีกุญแจสามารถใช้อุปกรณ์คอมพิวเตอร์ได้ เช่น มีระบบกุญแจและป้องกันการเข้าสู่ห้องคอมพิวเตอร์ และป้องกันการใช้อุปกรณ์ต่าง ๆ ในระบบ Online การใช้คอมพิวเตอร์ไม่จำเป็นต้องเข้าสู่ห้องคอมพิวเตอร์เสมอไป เพราะ Terminal ได้ติดตั้งกระจัดกระจายอยู่ตามส่วนงานต่าง ๆ และผู้ใช้ Terminal อาจสั่งงานคอมพิวเตอร์โดยตรงเสมือนอยู่ในห้องคอมพิวเตอร์ ดังนั้น Terminal จะต้องมีระบบPhysical Lock ที่รัดกุม เช่น มีระบบกุญแจ 2 ดอก Supervisor จะเก็บรักษากุญแจไว้ดอกหนึ่ง ซึ่งจะเปิด Lock เมื่อเริ่มเวลาทำงานและปิด Lock เมื่อสิ้นเวลาทำงาน และOperator ที่ใช้ Terminal นั้น เก็บไว้ดอกหนึ่ง Operator จะต้องเปิด Lock เมื่อจะใช้ Terminal นั้น ซึ่งถ้า Supervisor ไม่เปิด Lock ไว้ก่อน Operator จะไม่สามารถใช้ Terminal นั้นได้

3.2 หลังจากผ่านขั้นตอน Physical Lock แล้ว ก่อนที่ผู้ใช้จะสามารถใช้คอมพิวเตอร์จะต้องผ่านขั้นตอนแสดงตนให้ระบบคอมพิวเตอร์รับรู้เพื่อสามารถตรวจสอบได้ว่า ผู้ใช้นั้นมีสิทธิใช้ระบบคอมพิวเตอร์เพียงใด เพื่อให้สามารถดำเนินงานตามมาตรการนี้ได้เมื่อเริ่มติดตั้งระบบคอมพิวเตอร์ในขั้น System Generation ผู้ควบคุมจะต้องกำหนด Parameter ว่าผู้ใดบางมีสิทธิในการใช้ระบบคอมพิวเตอร์และมีสิทธิใช้เพียงใด

User Identification	Password	Group Code	Security Level	Primary Task Program
01	NYUX	01	Z	
DON	TDBN	02	A	INV 01
TUK	XC26	03	P	
PAD	NC3Z	04	A	REC 01

ตารางที่ 3.1 Authorized Table

ในการกำหนด Parameter ผู้ควบคุมจะระบุว่าผู้ใช้แต่ละรายมี User Identification และ Password อะไรสังกัดอยู่ในผู้ใช้กลุ่มไหน มี Security Level ในการอ่านหรือแก้ไขข้อมูลที่บันทึกไว้ในแผ่นจานแม่เหล็กได้เพียงใด และมี Primary Task Program ซึ่งหมายถึงโปรแกรมที่ผู้ใช้รายนั้นสามารถปฏิบัติอะไรบ้าง คอมพิวเตอร์จะจัดทำ Authorized Table และบันทึกไว้ในแผ่นจานแม่เหล็ก ผู้ควบคุมจะแจ้ง Password ให้แก่ผู้มีอำนาจหน้าที่ในการปฏิบัติข้อมูลหรือพัฒนาโปรแกรมแต่ละรายตามขอบเขตหน้าที่รับผิดชอบ ดังนั้น เฉพาะผู้ใช้ซึ่งได้รับมอบหมายเท่านั้นจึงจะทราบ Password และเป็น Password ที่มีขอบเขตกำหนดอำนาจหน้าที่เฉพาะงาน

เมื่อผู้ต้องการใช้คอมพิวเตอร์ผ่านขั้นตอน Physical Lock แล้ว จะต้องพิมพ์ User Identification และ Password ประจำตัวผ่าน Terminal ระบบคอมพิวเตอร์จะอ่าน Authorized Table เข้าสู่ส่วนความจำและตรวจสอบว่ามี User Identification นั้น ปรากฏใน Authorized Table หรือไม่ และ Password ถูกต้องหรือไม่ ถ้าทุกอย่างถูกต้องก็จะตรวจดูว่ามี Primary Task ระบุไว้หรือไม่ ถ้ามีก็จะปฏิบัติงานตามโปรแกรมที่ระบุ ถ้าไม่มี Primary Task ระบุย่อมแสดงว่าผู้ใช้รายนั้นสามารถปฏิบัติงานที่เกี่ยวกับการพัฒนาโปรแกรมและ File Handling

ข้อที่ควรระวังของการใช้ระบบ Password ก็คือ Password อาจรั่วไหลได้ง่าย ซึ่งถ้าผู้ใดก็ตามสามารถล่วงรู้ Password ย่อมสามารถสั่งให้คอมพิวเตอร์ปฏิบัติงานเท่ากับผู้เป็นเจ้าของ Password ทุกประการ Password อาจรั่วไหลได้ด้วยเหตุต่อไปนี้

(1) เกิดจากความไม่ระมัดระวังในการเก็บรักษา Password เช่น ในกรณีตัวอย่าง นักเรียน High School วิทยาลัยแห่งหนึ่งในสหรัฐอเมริกาพบกระดาษจด Password ของพนักงานพัฒนาระบบประจำวิทยาลัยในถังขยะ จึงได้ใช้ Password นั้นใช้เวลาของคอมพิวเตอร์จำนวนมากในการเล่น Computer Game

(2) เกิดจากความสนิทสนม ส่วนตัวระหว่างผู้ที่ทราบ Password และผู้ที่ต้องการทราบ Password หรือบางครั้งผู้ที่ต้องการทราบ Password อาจเชื่อมโยง Password ในแบบ Jigsaw Puzzle ดังเช่นตัวอย่างในกรณี Jerry Neal Schneider[1] ได้เดินผ่านที่ทิ้งขยะของ Pacific Telephone & Telegraph Company(PT & TC) ใน Los Angeles ตั้งแต่เป็นนักเรียน High School เขาสังเกตเห็นแบบฟอร์มการขอเบิกพัสดุโทรศัพท์ ตลอดจนคู่มือการเบิกพัสดุทิ้งอยู่ จึงพยายามศึกษาวิธีการขอเบิกพัสดุทางโทรศัพท์

ระบบการเบิกพัสดุของบริษัทฯ เป็นระบบอัตโนมัติ ผู้ได้รับมอบหมายให้เบิกพัสดุจะแจ้ง Password ไปยังศูนย์คอมพิวเตอร์ของบริษัทฯ โดย Remote Terminal ผ่านสายโทรศัพท์ไปยังคอมพิวเตอร์ IBM 360 คอมพิวเตอร์จะตรวจสอบ Password ซึ่งถ้าถูกต้องก็จะให้ผู้ที่มีPassword แจ้งรายการอุปกรณ์โทรศัพท์ที่ขอเบิกตลอดจนสถานที่และเวลาสั่งของ จากนั้นคอมพิวเตอร์จะส่งรายการขอเบิกนี้พิมพ์แจ้งไปยังหน่วยพัสดุ ซึ่งจะจัดพัสดุที่ขอเบิกส่งไปยังสถานที่และเวลาซึ่งนัดหมายไว้ต่อไป ราคาพัสดุที่เบิกจะลงบัญชีโครงการ (Project) ที่เจ้าของ Password สังกัดอยู่ ระบบการเบิกพัสดุนี้บริษัทฯ กล่าวว่าช่วยให้การดำเนินงานตามโครงการติดตั้งโทรศัพท์คลอบคลุมทั้งรัฐ California ของบริษัทฯ ดำเนินไปอย่างมีประสิทธิภาพและรวดเร็ว

ต่อมา Schneider เข้าศึกษาในคณะวิศวกรรมศาสตร์ใน University of California at Los Angeles (UCLA) ทำให้เข้าถึงกลไกของระบบคอมพิวเตอร์และระบบรหัสลับมากขึ้น เขาพยายามสนิทสนมกับพนักงานของบริษัทฯ ตลอดจนสัมภาษณ์พนักงานเหล่านั้นในฐานะนักศึกษาเตรียมเขียนวิทยานิพนธ์ในหัวข้อเรื่อง Computerized Warehouse System ทำให้ Schneider สามารถเชื่อมโยงระบบ Password ในการเบิกพัสดุได้ทั้งหมด

---

[1] Ibid, p. 37.

ในเดือนมิถุนายน ค.ศ. 1971 Schneider ซื้อ Termenal แบบเดียวกับที่บริษัทฯ ใช้ และทดลองส่ง Password เพื่อขอเบิกพัสดุโทรศัพท์มีมูลค่า $ 300,000 ให้ส่งไปยังจุดที่นัดหมาย ซึ่งปรากฏว่าได้ผล

Schneider ได้ตั้งบริษัทชื่อ Los Angeles Telephone & Telegraph Company เพื่อขายอุปกรณ์โทรศัพท์ซึ่งยักยอกจาก PT & TC ผ่านทางระบบการเบิกโดยใช้ Password ตลอดมา และกิจการได้ขยายขึ้นจนมีโกดังเก็บของขนาด 6,000 ตารางฟุต และมีพนักงานในสังกัด 10 คน

ในเดือนมกราคม ค.ศ. 1972 Schneider ให้พนักงานผู้หนึ่งออกจากงาน พนักงานผู้นั้นได้นำเรื่องไปแจ้งตำรวจ จากการสอบสวนพบว่าพัสดุโทรศัพท์ที่ Schneider ยักยอกในช่วงเวลา 2 ปีที่ผ่านมามีมูลค่าประมาณหลายล้านเหรียญสหรัฐ แต่พนักงานอัยการสามารถหาหลักฐานพิสูจน์ต่อศาลได้เพียง $ 5,000 เขาได้รับคำตัดสินจำคุก 60 วัน แต่ถูกจองจำเพียง 40 วัน เนื่องจากประพฤติดี

หลังจากพ้นโทษ Schneider ได้ตั้งบริษัทที่ปรึกษาทางด้านรักษาความปลอดภัยของระบบข้อมูลคอมพิวเตอร์ และยังได้แต่งหนังสือเกี่ยวกับอาชญากรรมที่ได้กระทำ ซึ่งบริษัทสร้างภาพยนตร์ขอซื้อสิทธิ์เพื่อนำไปสร้างภาพยนตร์โดยให้ค่าตอบแทนที่สูง

(3) ระบบ Password อาจรั่วไหลเนื่องจากจุดอ่อนในโปรแกรม Operating System เอง ตัวอย่างเช่น ระบบการใช้ Authorized Table ที่ผ่านมา เนื่องจาก Authorized Table ถูกจัดเก็บในแผ่นจานแม่เหล็ก ดังนั้นผู้ที่ต้องการทราบ Password อาจใช้ Utility Routine ทำการ Dump ข้อมูลในแผ่นจานแม่เหล็กเพื่อทราบถึง Password ที่บันทึกใน Table หรืออาจใช้ Routine ที่ใช้ Maintenance Table ทำการแก้ไข Authorized Table เพื่อผลในทางทุจริต เช่นเพิ่ม Password สำหรับผ่านเข้าสู่ระบบ แล้วแก้ไข Security Level ของบาง Password

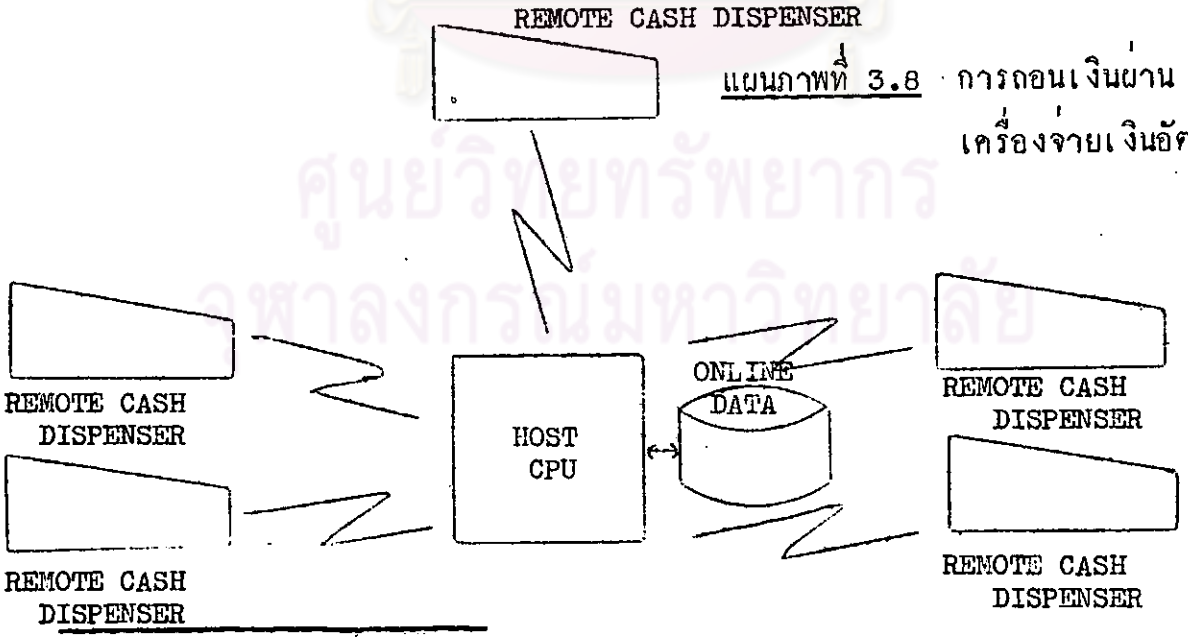
เนื่องจากการใช้ระบบ Password เพื่อ Identify ผู้ใช้ต่อระบบคอมพิวเตอร์มีจุดอ่อนในด้านที่รั่วไหลได้ง่าย ในระบบที่มีการระมัดระวังอย่างเคร่งครัดจึงนิยมใช้วิธีอื่นประกอบด้วยเช่น

- ใช้ Badge/Card Reader ซึ่งอ่านเครื่องหมายและบัตรที่ออกให้ผู้ใช้แต่ละราย และตรวจสอบว่า Badge/Card Reader นั้น ถูกต้องหรือไม่

- ตรวจคุณสมบัติทางร่างกายของผู้ใช้ เช่น ลายนิ้วมือหรือคลื่นเสียง แล้วเปรียบเทียบกับข้อมูลเกี่ยวกับผู้ใช้ที่จัดเก็บไว้ว่าตรงกัน

ข้อที่ควรสังวรณ์ก็คือ ไม่ว่าจะมีระบบป้องกันการ Access อุปกรณ์คอมพิวเตอร์รัดกุมเพียงใดก็ตาม ผู้ที่จงใจทุจริตย่อมหาทางผ่านมาตรการป้องกันโดยวิธีที่แยบยลได้เสมอ

[1]ในปี ค.ศ. 1974 วิศวกรไฟฟ้าชาวฝรั่งเศสผู้หนึ่งถูกจับในข้อหาขโมยเงินประมาณ F.Fr. 60,000 จากเครื่องจ่ายเงินอัตโนมัติในเมืองใหญ่ของฝรั่งเศส 4 เมือง



แผนภาพที่ 3.8 การถอนเงินผ่านเครื่องจ่ายเงินอัตโนมัติ

[1]Ibid, p. 56.

เครื่องจ่ายเงินอัตโนมัติมีสภาพคล้ายกับ Terminal ติดตั้งอยู่ในย่านชุมนุมชนเพื่ออำนวยความสะดวกให้ลูกค้าธนาคารสามารถถอนเงินในวันสุดสัปดาห์หรือเมื่อมีความจำเป็นต้องใช้เงินกระทันหันโดยไม่ต้องไปเบิกเงินที่ธนาคาร เมื่อลูกค้าต้องการเบิกเงินจะต้องสอดบัตรที่ธนาคารออกให้เฉพาะบุคคล ในบัตรจะมีเครื่องหมายรหัสลับซึ่งเครื่องจ่ายเงินอัตโนมัติจะตรวจจับ Pattern ของรหัส แล้วส่งข้อมูลไปยังศูนย์คอมพิวเตอร์เพื่อตรวจว่า Pattern นั้นถูกต้องหรือไม่ ถ้า Pattern ไม่ถูกต้องคอมพิวเตอร์จะส่งสัญญาณกลับมายังเครื่องจ่ายเงินให้เก็บบัตรใบนั้นไว้ แต่ถ้าพบว่าเป็นบัตรที่ถูกต้องก็จะส่งสัญญาณให้เครื่องจ่ายเงินอัตโนมัติคืนบัตรให้ลูกค้าและส่งสัญญาณให้ลูกค้า Key รหัสลับของบัญชีเงินฝาก ข้อมูลจะถูกส่งไปยังคอมพิวเตอร์ตรวจสอบว่า ยอดคงเหลือในบัญชีลูกค้ามีพอหรือไม่ ถ้ายอดคงเหลือมีเพียงพอเครื่องจะปลดปล่อยซองบรรจุเงินประมาณ F.Fr. 50-100 ตามที่ลูกค้าเบิกให้แก่ลูกค้า และ Update ยอดคงเหลือในบัญชีเงินฝาก

ผู้ทุจริตได้ขอเปิดบัญชีเงินฝากที่ให้บริการดังกล่าวเพื่อให้ได้รับบัตรถอนเงิน ผู้ทุจริตพยายามศึกษา Pattern ของรหัสจนเข้าใจระบบรหัสที่ใช้และทำบัตรปลอมขึ้น ผู้ทุจริตได้ใช้วิธีการเพื่อที่จะทราบถึงตัวเลขรหัสลับของบัญชีเงินฝากที่ธนาคารออกให้แก่ลูกค้าแต่ละราย โดยโทรศัพท์ถึงลูกค้ารายใหญ่ของธนาคารที่คาดว่าจะมีเงินคงเหลือในบัญชีจำนวนมาก และอ้างว่าเป็นพนักงานของธนาคารต้องการเปลี่ยนเลขหมายรหัสลับของบัญชีลูกค้าใหม่เพื่อเหตุผลในด้านรักษาความปลอดภัย การเปลี่ยนหมายเลขใหม่จะกระทำโดยเพิ่มหมายเลขพิเศษขึ้นอีก 1 หลักต่อท้ายหมายเลขเดิม จากนั้นผู้ทุจริตจะแกล้งซักซ้อมความเข้าใจถึงตัวเลขรหัสใหม่กับลูกค้า โดยให้ลูกค้าอ่านหมายเลขรหัสทั้งหมด ผลปรากฏว่าทุกครั้งที่ทำการสอบถามลูกค้าทุกรายได้ให้ความร่วมมือในการแจ้งรหัสลับของตนเป็นอย่างดี

ด้วยการใช้บัตรปลอมที่จัดเตรียมและรหัสลับของบัญชีเงินฝากที่สอบถามจากลูกค้า ผู้ทุจริตได้ทำการเบิกเงินจากเครื่องจ่ายเงินอัตโนมัติในเมืองใหญ่ ๆ ของฝรั่งเศส

4 เมือง ในที่สุดผู้ทุจริตถูกจับได้เนื่องจากเครื่องจ่ายเงินอัตโนมัติเครื่องหนึ่งขัดข้องไม่คืนบัตรปลอมให้ผู้ทุจริต พนักงานควบคุมของธนาคารพบบัตรปลอมในเครื่อง จึงได้ดักซุ่มอยู่บริเวณเครื่องจ่ายเงินอัตโนมัตินั้น วันรุ่งขึ้นผู้ทุจริตได้กลับไปเพื่อทดลองใหม่และถูกจับกุมดำเนินคดี

การลักลอบใช้อุปกรณ์คอมพิวเตอร์เพื่อผลประโยชน์ในทางทุจริตมักเกิดจากบุคคลภายในศูนย์คอมพิวเตอร์เองซึ่งอาจมีอำนาจหน้าที่ในการใช้คอมพิวเตอร์ หรือทราบจุดอ่อนของระบบ Password อยู่แล้ว เช่นตัวอย่างกรณีที่อดีตพนักงานของ Mamufacturing Data System Inc. แห่ง Ann Arbor, Michigan ซึ่งทำกิจการ Computer Service Center ได้ใช้รหัสลับที่ทางบริษัทออกให้ลูกค้าใช้เวลาของคอมพิวเตอร์ทำการประมวลผลข้อมูลให้ W & R Tool เป็นการส่วนตัวเป็นเวลาทั้งสิ้น 143 ชั่วโมง คิดเป็นค่าใช้จ่าย $ 15,000 ซึ่งต่อมาถูกจับและถูกดำเนินคดี

มาตรการที่นิยมใช้ในการป้องกันการใช้อุปกรณ์คอมพิวเตอร์เพื่อประโยชน์ในทางทุจริตอีกประการหนึ่งก็คือ Run Control Log โดยกำหนดให้คอมพิวเตอร์บันทึกไว้ว่าได้ปฏิบัติอะไรให้แก่ผู้ใดตั้งแต่เวลาใดถึงเวลาใด รายงานนี้อาจพิมพ์ออกสู่ภายนอกโดย Console Printer ตลอดเวลา หรือบันทึกไว้ในแผ่นจานแม่เหล็กเพื่อรอการ List ออกมาในภายหลังก็ได้

```
NEC/300 ONLINE
LOGMSC - 10:55:54 EDT FRIDAY 10/17/80
10:56:41 INVR LOG ON
10:58:26 ACRE LOG ON
11:02:42 INVR LOG OFF TIME: 6 MIN 01
```

แผนภาพที่ 3.9 Control Log Report

ผู้มีหน้าที่ควบคุมจะต้องตรวจตรา Control Log Report มิให้มีการแก้ไขเปลี่ยนแปลงและตรวจสอบว่าผู้ใช้แต่ละรายมีหน้าที่ในการใช้คอมพิวเตอร์ในช่วงเวลาที่ปรากฏในรายงานจริงหรือไม่ ช่วงเวลาที่ใช้ปฏิบัติงานดังกล่าวนานกว่าที่ควรจะเป็นหรือไม่

4. <u>การควบคุมด้านการรักษาความลับของข้อมูล</u>

การขโมยข้อมูลซึ่งเป็นความลับที่บันทึกไว้ในระบบคอมพิวเตอร์เพื่อนำไปหาผลประโยชน์ได้เป็นพฤติกรรมที่แพร่หลายในปัจจุบัน เช่น [1]พนักงานควบคุมเครื่องคอมพิวเตอร์ 3 คนของบริษัทขาย Encyclopedia Britamica ได้ร่วมมือ List รายชื่อลูกค้าและนำไปขายให้บริษัทคู่แข่งและบริษัทประเภทขายสินค้าทางไปรษณีย์ (Mailing List) ทั่วไป ซึ่งเจ้าหน้าที่ของบริษัทผู้เสียหายได้ประเมินราคาของข้อมูลว่าไม่ต่ำกว่า $ 1 ล้าน

ใน ค.ศ. 1973 พนักงานควบคุมเครื่องคอมพิวเตอร์ของ Illinois Driver Registration Bureau ได้รับการติดสินบนจากบุคคลภายนอกเป็นเงิน $ 10,000 ให้ลักลอบ List รายชื่อและที่อยู่ของผู้ขับขี่ยานพาหนะซึ่งมีมูลค่าต่อธุรกิจขายสินค้าทางไปรษณีย์ประมาณ $ 70,000

ใน ค.ศ. 1971 พนักงานตำรวจในชิคาโกถูกจับในข้อหา List ข้อมูลอาชญากรรมจากศูนย์คอมพิวเตอร์ National Crime Information Center ของ F.B.I. เพื่อนำไปขายให้นักสืบเอกชนและสำนักงานทนายความ

ในประเทศนอร์เวย์ พนักงานควบคุมเครื่องคอมพิวเตอร์ของ Health Service ถูกจับในข้อหา List ข้อมูลเกี่ยวกับผู้ป่วยเรื้อรังเพื่อขายให้พนักงานขายของบริษัทผลิตยาไปติดต่อผู้ป่วย

นอกจากข้อมูลที่เป็นความลับจะเป็นเป้าหมายของการทุจริตเพื่อหาผลประโยชน์แล้ว

---

[1] Ibid, p. 48-49.

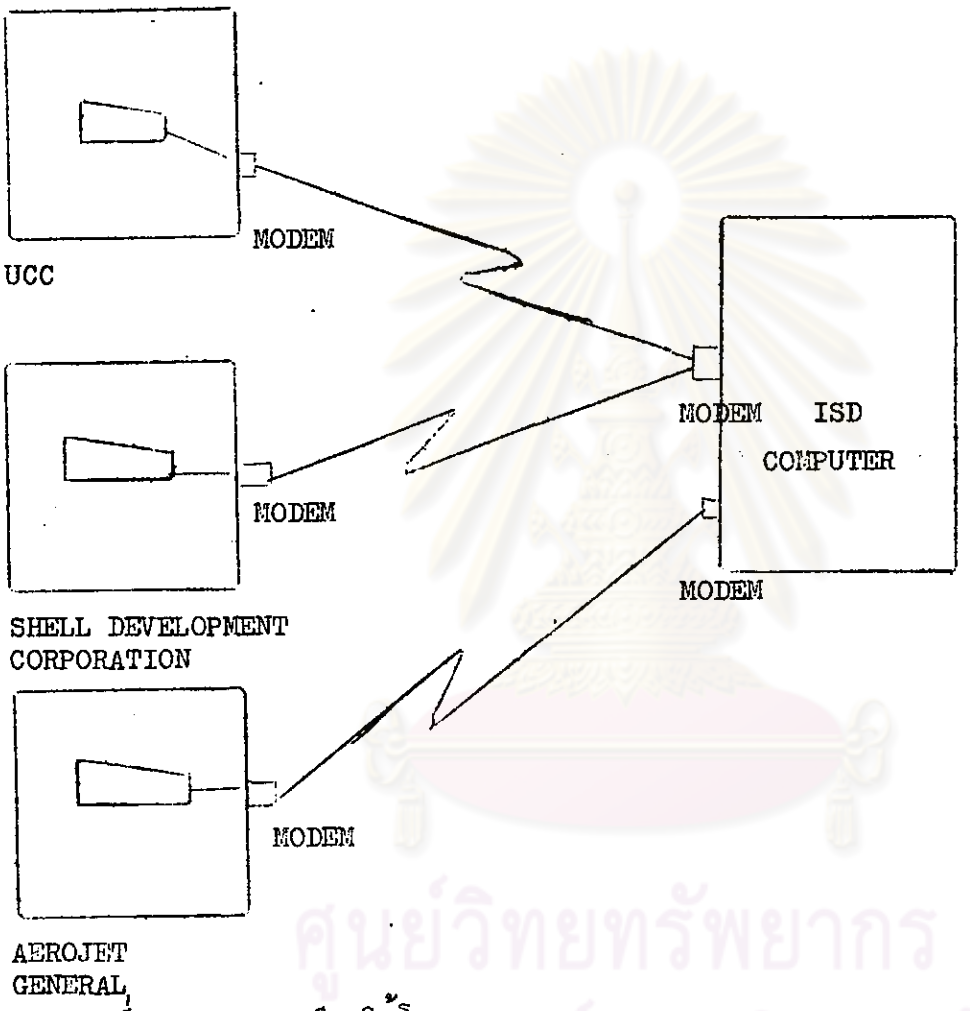
โปรแกรมควบคุมการทำงานของคอมพิวเตอร์ก็เป็นเป้าหมายของการทุจริตด้วย ตัวอย่างเช่น [1]บริษัท University Computing Company (U.C.C.) แห่ง Palo Alto, California ประกอบธุรกิจประเภท Computer Service Center ให้บริการเช่าเวลาคอมพิวเตอร์แก่กิจการทั่วไป มีรายได้ประมาณปีละ $ 100 ล้าน U.C.C. มีคู่แข่งขันที่สำคัญที่ดำเนินธุรกิจประเภทเดียวกัน คือบริษัท Information System Design Inc. (I.S.D.) แห่ง Oakland, California บริษัท I.S.D. นับเป็นบริษัทที่ก่อตั้งภายหลังมีรายได้ประมาณปีละ $ 1 ล้าน แต่มีความสามารถพัฒนาโปรแกรม PLOT/TRANS โปรแกรมนี้สามารถ Plot graph จากผลการคำนวณทางวิศวกรรมซึ่งลูกค้าที่ใช้บริการส่งมาจาก Remote Terminal โดยใช้ Remote Terminal แห่งนั้นเอง ระบบ PLOT/TRANS ช่วยอำนวยความสะดวกและลดค่าใช้จ่ายในการประมวลผลข้อมูลให้แก่ลูกค้า เพราะสามารถ Plot graph ด้วย Terminal ธรรมดาและให้บริการที่รวดเร็วแก่ Terminal ของลูกค้าที่อยู่ห่างไกล ดังนั้น ระบบนี้จึงช่วยให้เทคนิคของ I.S.D. ก้าวหน้ากว่า U.C.C.จึงพยายามพัฒนาระบบเช่นนี้เช่นกัน แต่ยังไม่ประสบผลสำเร็จ บริษัททั้งสองแข่งขันการให้บริการแก่ลูกค้าสำคัญคือ Shell Development Corporation แห่ง Emeryville และ Aerojet General แห่ง Sacramento แต่ I.S.D. อยู่ในฐานะได้เปรียบในการแข่งขันการให้บริการลูกค้าเนื่องจากระบบ PLOT/TRANS ดังกล่าว

พนักงานพัฒนาโปรแกรมอาวุโสของ U.C.C. คือ Eli Bart พยายามที่จะดึงความลับของโปรแกรม PLOT/TRANS โดยใช้ Terminal ที่ U.C.C. ทำการ Access ระบบคอมพิวเตอร์ของ I.S.D. การที่จะติดต่อกับระบบคอมพิวเตอร์ของ I.S.D. ได้ ประการแรกจะต้องทราบหมายเลขโทรศัพท์ที่ I.S.D. กำหนดให้ลูกค้าแต่ละรายใช้ติดต่อระหว่าง Terminal ของลูกค้ากับคอมพิวเตอร์ของ I.S.D. และหมายเลขนี้ไม่ปรากฏในสมุดโทรศัพท์ ประการที่สองจะต้องทราบ Password

---

[1] Ibid, p. 43.

ของลูกค้าที่ I.S.D. กำหนดให้ลูกค้าแต่ละราย และประการที่สามจะต้องทราบชื่อรหัสของโปรแกรม PLOT/TRANS เพื่อสามารถเรียกใช้โปรแกรม



แผนภาพที่ 3.10 การเรียกใช้โปรแกรมงานจาก Remote Terminal

Eli Bart ทราบความลับของหมายเลขโทรศัพท์คู่สายระหว่าง Termenal ของบริษัท Shell Development Corporation และ Password ซึ่ง I.S.D. ออกให้บริษัท Shell โดยการเข้าไปสนิทสนมกับพนักงานของบริษัท Shell ซึ่งเป็นลูกค้าของทั้ง U.C.C. และ I.S.D. สำหรับชื่อรหัสของโปรแกรม PLOT/TRANS ปรากฏว่า Eli Bart ได้จากเพื่อนซึ่งทำงานในบริษัท Aerojet General ซึ่งเป็นลูกค้าของ I.S.D. และใช้ระบบ PLOT/TRANS

ในวันที่ 19 มกราคม ค.ศ. 1970 Eli Bart ได้ใช้ Terminal ในสำนักงานใหญ่ของ U.C.C. ทำการ Access คอมพิวเตอร์ของ I.S.D. โดยทำเสมือนเป็น Terminal ของบริษัท Shell Development Coporation และสั่งให้คอมพิวเตอร์ของ I.S.D. ส่งโปรแกรม PLOT/TRANS มาพิมพ์ ณ Terminal ของ U.C.C.

ถึงแม้ความพยายามของ Eli Bart ในการได้ความลับของโปรแกรม PLOT/TRANS จะเป็นผลสำเร็จ แต่รายการนี้ได้ถูกบันทึกใน Control Log ของคอมพิวเตอร์ I.S.D. เพื่อเรียกเก็บเงินจากบริษัท Shell Development Corporation เป็นค่าบริการใช้คอมพิวเตอร์ ซึ่งบริษัท Shell Development Corporation ได้ปฏิเสธการจ่ายเงินตามรายการดังกล่าว เนื่องจากไม่เคยใช้บริการในลักษณะนี้มาก่อน

พนักงานของบริษัท I.S.D. ได้ดำเนินการสอบสวนกรณีดังกล่าว และเพ่งเล็งมายัง U.C.C. ในวันที่ 19 กุมภาพันธ์ ศกเดียวกัน เจ้าหน้าที่ตำรวจและพนักงานของบริษัท I.S.D. ใช้หมายค้นทำการตรวจสอบข้อมูลในส่วนความจำและอุปกรณ์จัดเก็บข้อมูลของระบบคอมพิวเตอร์ บริษัท U.C.C. นับว่าเป็นหมายค้นส่วนความจำของคอมพิวเตอร์ครั้งแรกในประวัติศาสตร์ หลังจากใช้เวลา List ข้อมูล 9 ชั่วโมง จึงได้พบว่าโปรแกรม PLOT/TRANS ที่ขโมยมาจากบริษัท I.S.D. ได้ถูกถ่ายทอดเก็บไว้ในเทปแม่เหล็ก และตรวจพบเอกสารลายมือของ Eli Bart เขียนบันทึกวิธีการ Access ระบบคอมพิวเตอร์ของ I.S.D.

Eli Bart ถูกฟ้องศาลในข้อหาขโมยความลับทางการค้าซึ่งประเมินว่ามีมูลค่าไม่ต่ำกว่า $ 1 ล้าน และได้รับโทษปรับ $ 5,000 รวมทั้งรอลงอาญา 3 ปี บริษัท U.C.C. ถูกฟ้องในฐานะจำเลยร่วม และต้องชดใช้ค่าเสียหายให้บริษัท I.S.D. เป็นเงิน $ 300,000

โปรแกรมอีกประเภทหนึ่งซึ่งมักเป็นเป้าหมายของการขโมยความลับ คือ โปรแกรมที่ใช้ในการถอดแบบแปลนของสิ่งปลูกสร้าง ผู้ใช้จะต้องแจ้ง Parameter ของสิ่งก่อสร้าง เช่น ขนาดของสิ่งก่อสร้าง ลักษณะ จำนวนชั้น จำนวนประตู หน้าต่าง วัสดุที่ใช้ ฯลฯ คอมพิวเตอร์จะคำนวนประมาณราคาก่อสร้างจากข้อมูลที่ได้รับ เพื่อผู้ใช้จะนำราคานั้นประกอบการพิจารณายื่นประมูลรับเหมาก่อสร้างต่อไป ถ้าหาก โปรแกรมรั่วไหลไปยังบริษัทคู่แข่ง ย่อมทำให้บริษัทคู่แข่งสามารถตัดราคาประมูลใน Margin ที่ต่ำกว่าเพียงเล็กน้อย

มาตรการในการรักษาความลับของข้อมูลและโปรแกรมมักแฝงอยู่ในระบบ Operating System เช่นเดียวกับระบบ Access Control เมื่อผู้ใช้ต้องการ Allocate เนื้อที่ในแผ่นจานแม่เหล็กเพื่อบันทึกข้อมูลหรือโปรแกรม จะต้องทำการ Key in แจ้ง Parameter ของ File หรือโปรแกรมที่ต้องการบันทึกนั้น ๆ ใน Parameter นอกจากจะระบุขนาด ประเภท และข้อมูลอื่น ๆ เกี่ยวกับ File แล้ว ยังต้องระบุว่า File นั้นสังกัด Group อะไร ซึ่งหมายถึง File นั้นเป็น File ในสังกัดหน่วยงานใด มี Security Level อะไร Parameter จะถูกบันทึกใน File Directory ของแผ่นจานแม่เหล็ก

ใน Authorized Table ได้แบ่งผู้ใช้ออกเป็น 2 กลุ่มคือ

ก. กลุ่มผู้ใช้ซึ่งมี Primary Task โดยระบุชื่อโปรแกรม หลังจากผ่านขั้นตอน Identified ถูกต้องแล้ว คอมพิวเตอร์จะ Load โปรแกรมนั้นเข้าสู่ส่วนความจำ ผู้ใช้มีสิทธิปฏิบัติงานเฉพาะที่กำหนดในโปรแกรมนี้

ข. ผู้ใช้ซึ่งไม่มี Primary Task ระบุไว้ หมายความถึงผู้ใช้ซึ่งมีสิทธิใช้ Command ต่าง ๆ ของ Operating System ในงานเกี่ยวกับการพัฒนาโปรแกรมและ File Handling ในรูปแบบต่าง ๆ

User Identification	Password	Group Code	Security Level	Primary Task Program
OI	NTUK	OI	Z	
DON	TDBN	02	A	INV MAST
TUK	XC26	02	P	
PAD	NC32	03	A	RECOI

Authorized Table

File Name	Group Code	Security Level	Location Information
G/L	OI	B	
INV MAST	02	A	
INV TRANS	02	A	
INV CONTROL	02	B	
REC MAST	03	A	

File Directory

G/L
INV MAST
INV TRANS
INV CONTROL
REC MAST

Information Store-in

แผนภาพที่ 3.11 แสดงโปรมแกรมและข้อมูลที่ผู้ใช้เฉพาะรายที่กำหนดไว้ใน **Authorized Table**

ถ้าผู้ใช้ประเภทนี้ต้องการปฏิบัติงานเกี่ยวกับข้อมูลใดที่บันทึกไว้ในแผ่นจานแม่เหล็กหลังการ Allocate จะต้องสั่งให้คอมพิวเตอร์ทำการ Open File โดยการอ้างชื่อ File คอมพิวเตอร์จะอ่าน File Directory เพื่อตรวจว่ามี File ชื่อที่ผู้ใช้ต้องการอ่านหรือไม่ และ Group Code ตรงกับ Group Code ของผู้ใช้ Password นั้นตามที่ระบุใน Authorized Table หรือไม่ ถ้าตรงกันจะตรวจสอบต่อไปว่า Security Level ของ File นั้นตามที่ระบุใน File Directory มีระดับสูงกว่า Security Level ของผู้ใช้รายนั้นหรือไม่ ถ้าพบว่าไม่สูงกว่าก็จะทำการ open File เปิดโอกาสให้ผู้ใช้รายนั้นนำข้อมูลจาก File มาปฏิบัติงาน ตัวอย่างเช่น ผู้ใช้ซึ่งมี Password EDBN ต้องการจะปฏิบัติงานเกี่ยวกับ File ชื่อ INV MAST หลังจากที่ Key in Password เพื่อให้คอมพิวเตอร์ตรวจสอบกับ Authorized Table แล้ว ถ้ามีการปฏิบัติงานซึ่งเกี่ยวข้องกับ File ชื่อ INV MAST คอมพิวเตอร์จะตรวจจาก File Directory เพื่อตรวจสอบว่า Group Code ของ File ซึ่งเท่ากับ 02 ตรงตาม Group Code ของผู้ใช้เจ้าของ Password หรือไม่ และ Security Level ของผู้ใช้สูงกว่า Security Level ของ File หรือไม่ จะสังเกตได้ว่าผู้ใช้ซึ่งมีรหัส Password EDBN สามารถปฏิบัติเกี่ยวกับ File เฉพาะ File ชื่อ INV MAST และ INV TRANS แต่ไม่สามารถปฏิบัติงานเกี่ยวกับ File ชื่อ G/L และ REC MAST เพราะ File ทั้งสองสังกัดอยู่คนละ Group Code รวมทั้งไม่สามารถปฏิบัติงานที่เกี่ยวข้องกับ File ชื่อ INV CONTROL ที่ถึงแม้จะมี Group Code เดียวกับผู้ใช้ แต่มีระดับ Security Level สูงกว่า

จุดอ่อนของระบบป้องกันความลับของข้อมูลมีสาระเช่นเดียวกับระบบป้องกันการใช้อุปกรณ์ระบบคอมพิวเตอร์ กล่าวคือ อาจมีการแก้ไข Authorized Table เพื่อให้ผู้ที่ต้องการ Access ข้อมูลมีโอกาส Access ข้อมูลที่ต้องการ หรือมีการลักลอบ Dump ข้อมูล ระบบควบคุมการ Access ข้อมูลขึ้นอยู่กับ Operating System ดังนั้นอาจมีการ Manipulate Routine ใน Operating System

ให้ทำการ Bypass ขั้นตอนการตรวจสอบก่อนจะทำการ Open File หรืออาศัยจุดอ่อนของ Operating System เองเพื่อ Bypass ขั้นตอนการตรวจสอบเหล่านี้ ใน [1] Routine Operating System ของ IBM S/370 ประกอบด้วยคำสั่งประมาณ 6 ล้านคำสั่ง ซึ่งถ้าพิมพ์ List ในกระดาษต่อเนื่องจะได้ Listing ยาวอย่างน้อย 15 ไมล์ ดังนั้นถ้าผู้ทุจริตมีความรู้เกี่ยวกับ Operating System เป็นอย่างดีทำการแก้ไขคำสั่งของ Routine เพื่อผลในทางทุจริต ยอมยากที่จะตรวจพบ ในคำสั่งทั้ง 6 ล้านคำสั่งนี้ย่อมมีคำสั่งที่เป็นจุดอ่อนซึ่งผู้เชี่ยวชาญสามารถอาศัยจุดอ่อนเหล่านี้ทำการ Access ข้อมูล ข้อเท็จจริงในการพัฒนา Operating System ประการหนึ่งคือ Routine Operating System ส่วนมากพัฒนาโดยผู้เชี่ยวชาญมาตั้งแต่การพัฒนาระบบ Operating System ของคอมพิวเตอร์ Generation ที่ 2 ซึ่งส่วนมากของระบบปฏิบัติข้อมูลแบบ Batch Processing ในขณะที่คอมพิวเตอร์ในปัจจุบันปฏิบัติงานในแบบ Online ดังนั้นแนวความคิด (Concept) ในการรักษาความปลอดภัยได้เปลี่ยนไปซึ่งผู้พัฒนา Operating System อาจไม่พัฒนาเทคนิคให้ทันต่อเหตุการณ์

การขโมยความลับทางด้านข้อมูลและโปรแกรมส่วนมากผู้ทุจริตสามารถกระทำด้วยวิธีง่าย ๆ อาศัยจุดอ่อนในวิธีปฏิบัติ เช่น กรณีบริษัท University Computing Company ขโมยโปรแกรม PLOT/TRANS จากบริษัท Information System Design Inc., หรือผู้ทุจริตเป็นพนักงานในกิจการที่ถูกขโมยความลับซึ่งมักมีอำนาจในการ Access ข้อมูลนั้น ๆ อยู่แล้ว ดังนั้นผู้ควบคุมจะต้องสอดส่องวิธีปฏิบัติเรื่องการรักษาความลับของ Password และการใช้อุปกรณ์คอมพิวเตอร์นอกเหนือจากการปฏิบัติงานปกติโดยไม่มีเหตุผลสมควร รวมทั้งการควบคุมในด้าน Output Control ซึ่งจะได้กล่าวถึงต่อไป

---

[1] Ibid, p. 123.

5. การควบคุมด้าน Tele Communication

ในการปฏิบัติข้อมูลแบบ Online มักเกี่ยวข้องกับการรับ-ส่งข้อมูลระหว่างคอมพิวเตอร์และ Terminal ที่อยู่ห่างไกล มาตรการที่ใช้ในการควบคุมการรับ-ส่งข้อมูลอาจแบ่งเป็น 2 ประเภทคือ

ก. มาตรการควบคุมความถูกต้องของการรับ-ส่งข้อมูล

ข. มาตรการป้องกันการรั่วไหลของข้อมูลระหว่างการรับ-ส่ง

มาตรการควบคุมความถูกต้องของการรับ ส่งข้อมูล

ในการรับ-ส่งข้อมูลในระยะไกล เช่น ผ่านสายโทรศัพท์สาธารณะ การส่งข้อมูลจะส่งเป็น Bit ในสภาพของ Pulse Train ที่มีส่วนผสมของ Pulse เป็น Pattern แทนข้อมูล ซึ่งยิ่งระยะห่างไกลเท่าใด โอกาสที่ Pulse Train จะเปลี่ยนรูปยิ่งมีมากเพียงนั้น เป็นผลให้ข้อมูลที่รับ-ส่งผิดพลาด สำหรับสาเหตุที่ Pulse Train เปลี่ยนรูปอาจเกิดจากคุณภาพของสายไฟที่เป็นเส้นการรับ-ส่งข้อมูล และคลื่นรบกวนต่าง ๆ

มาตรการควบคุมความถูกต้องของการรับ-ส่งข้อมูลที่นิยมใช้กันได้แก่ ระบบ Error-detecting Code ซึ่งประกอบด้วยเทคนิคการใช้ Parity Check โดยเติม Bit พิเศษที่ทำให้จำนวน Bit ที่เป็น Pattern แทนข้อมูลต้องประกอบด้วยจำนวน Bit เป็นคู่หรือเป็นคี่เสมอ ถ้ากำหนดไว้ว่าจำนวน Bit ในกลุ่มของรหัสจะต้องเป็นคู่เสมอ ถ้าส่วนที่รับข้อมูลตรวจพบว่าจำนวน Bit ใน Pattern มิได้เป็นคู่ก็จะตัดสินได้ว่ามีข้อผิดพลาดในการรับ-ส่งข้อมูล ระบบควบคุมการรับ-ส่งข้อมูลจะดำเนินการดังต่อไปนี้

ก. สั่งให้ส่วนที่ส่งข้อมูลส่งข้อมูลเดิมมาใหม่

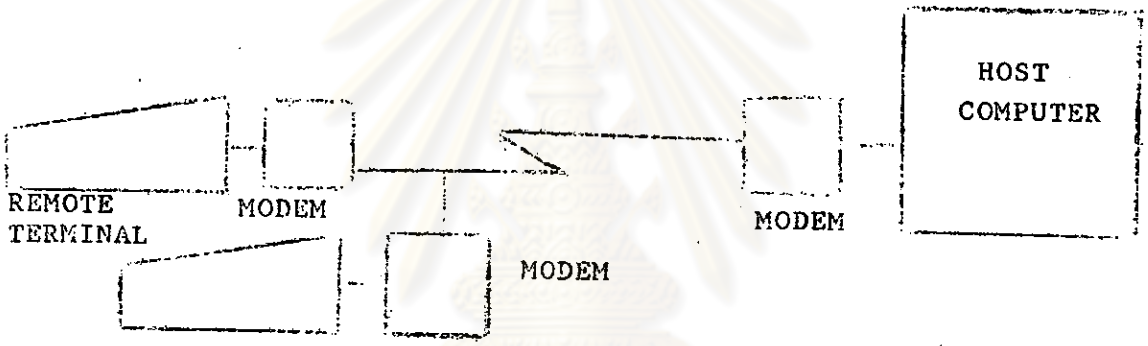
ข. พยายามลดความเร็วในการส่งข้อมูลลง

ค. หยุดการรับ–ส่งข้อมูลชั่วคราว และพยายามที่จะรับ–ส่งข้อมูลใหม่

ง. แจ้ง Error Message แก่ผู้ใช้ และหยุดการรับ–ส่งข้อมูล

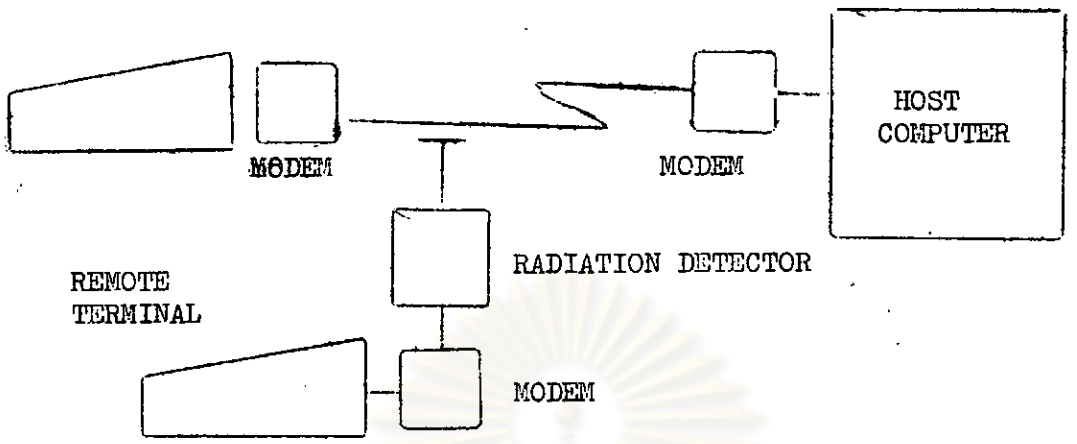
<u>มาตรการป้องกันการรั่วไหลของข้อมูลระหว่างการรับ–ส่ง</u>

การรับ–ส่งข้อมูลในแบบ Tele Communication ต้องระมัดระวังการรั่วไหลของข้อมูลมากกว่าปกติ โอกาสที่ผู้ทุจริตทราบข้อมูลในระหว่างการรับ–ส่งประกอบด้วยเทคนิคที่สำคัญ 2 แบบ คือ



<u>แผนภาพที่ 3.12</u> การตรวจจับข้อมูลโดยวิธี Wire Tapping

ก. Wire Tapping การลักลอบตรวจจับข้อมูลกระทำโดยเชื่อมเส้นทางการรับ–ส่งข้อมูลเพื่อดัก Pulse Train เข้าสู่คอมพิวเตอร์ของผู้ทุจริต ดังนั้น ข้อมูลที่ส่งจาก Remote Terminal หรือส่งจากคอมพิวเตอร์จะถูกส่งมายังคอมพิวเตอร์ของผู้ทุจริตด้วย



แผนภาพที่ 3.13 การตรวจจับข้อมูลด้วยวิธี Radiation

ข. ใช้วิธีตรวจจับ Radiation โดยวิธีนี้ผู้ทุจริตมิได้ต่อเชื่อมระบบคอมพิวเตอร์ของผู้ทุจริตเข้ากับเส้นทางการรับ-ส่งข้อมูลโดยตรง แต่ใช้เครื่องมือตรวจจับสัญญาณที่ส่งในเส้นทางการรับ-ส่งข้อมูล ดังได้กล่าวมาแล้วว่าการรับ ส่งข้อมูลกระทำในรูปของ Pulse Train ซึ่งมีสภาพการไหลของกระแสไฟฟ้าเป็น Pattern แทนข้อมูล การไหลของกระแสไฟฟ้าเหนี่ยวนำให้เกิดคลื่นแม่เหล็กไฟฟ้า ดังนั้นเครื่องตรวจจับคลื่นแม่เหล็กไฟฟ้าจะตรวจจับ Pattern ของคลื่นและเปลี่ยนกลับให้อยู่ในสภาพของ Pulse Train

การขโมยความลับของข้อมูลที่รับ-ส่งแบบ Tele Communication บางครั้งทำความเสียหายให้แก่ธุรกิจอย่างมาก เช่น [1]รายบริษัทน้ำมันแห่งหนึ่งในสหรัฐอเมริกาได้สำรวจแหล่งน้ำมันใน North Slope, Alaska เพื่อประมูลขอสัมปทานพื้นที่ในการขุดเจาะ หลังจากนักธรณีวิทยาได้ทดลองขุดเจาะจะส่งผลการสำรวจไปยังศูนย์คอมพิวเตอร์ของสำนักงานใหญ่ใน New York ซึ่งอยู่ห่างหลายพันไมล์โดยผ่านระบบโทรศัพท์ คอมพิวเตอร์สำนักงานใหญ่จะวิเคราะห์ข้อมูลและส่งผลในด้านโอกาสที่จะพบน้ำมัน ตลอดจนจำนวนเงินที่ควรยื่นประมูลเพื่อขอสัมปทานกลับมายัง Terminal ที่ Alaska เป็นที่น่าสังเกตว่า บริษัทดังกล่าวแพ้การประมูล

---

[1] Ibid, p. 42.

ต่อบริษัทคู่แข่งขันติดต่อกันหลายครั้งในจำนวนเงินที่ต่างกันน้อยมาก หลังจากการสอบสวน พบว่าบริษัทคู่แข่งได้ใช้เครื่องมืออิเลคโทรนิคทำการ Wire Tapping สายโทรศัพท์ที่ใช้ในการรับ–ส่งข้อมูลระหว่าง Remote Terminal และคอมพิวเตอร์ ณ สำนักงานใหญ่ ผลเสียหายประเมินแล้วหลายล้านเหรียญสหรัฐ

มาตรการป้องกันความลับของข้อมูลซึ่งรับ–ส่งในแบบ Tele Communication

การป้องกัน Wire Tapping และ Radiation ในทางปฏิบัติไม่สามารถกระทำได้อย่างมีประสิทธิภาพ ดังนั้นมาตรการป้องกันจะเน้นถึงการใช้เทคนิคซึ่งเรียกว่า Cryptograph

เทคนิคของ Cryptograph คือการเปลี่ยนข้อมูลที่จะส่งด้วยวิธีการที่กำหนดไว้ก่อนเพื่อให้กลายเป็นข้อมูลที่ผู้ไม่ทราบวิธีการถอดรหัสไม่อาจถอดความหมาย เทคนิคการใช้ Cryptograph มีหลายแบบ แต่ที่ใช้กันอย่างแพร่หลายประกอบด้วย

1. Substitution ซึ่งใช้วิธีเปลี่ยนตัวเลขและตัวอักษรของข่าวสาร[1] โดยมีกฎเกณฑ์แน่นอน เช่น อาจกำหนดว่า ในการเข้ารหัส Cryptograph จะให้เปลี่ยนอักษร E ให้กลายเป็นตัวอักษร X และในทำนองเดียวกันกำหนดว่า R = O A = M, N = 3, D = A และ Y =N ถ้าต้องการส่งข้อความว่า YEAR ENDED ผู้ส่งจะต้องดำเนินการเข้ารหัสโดยเปลี่ยนตัวอักษรในข้อความที่จะส่งแต่ละตัวตามกฎเกณฑ์กำหนด ซึ่งจะกลายเป็นข้อความว่า NXMO X3AXA ข้อความนี้แม้จะรั่วไหลในระหว่างการรับ–ส่ง แต่ถ้าผู้ทราบข้อมูลนี้ไม่รู้ถึงกฎเกณฑ์ในการเข้ารหัสย่อมไม่สามารถถอดความหมายของข้อความได้

ในการส่งข้อมูล ผู้ส่งอาจพัฒนาโปรแกรมที่ใช้ในการเข้ารหัสในลักษณะที่กล่าวและใช้โปรแกรมนั้นเข้ารหัสเสียก่อนซึ่งถึงแม้จะถูก Wire Tapping ผู้ทุจริตอาจ

---

[1] James Martin, Security, Accuracy and Privacy in Computer Systems, Englewood Cliffs, New Jersey : Prentice-Hall, Inc.,1973, p.208.

ไม่ทราบถึงความหมาย เมื่อส่งข้อมูลถึงปลายทางระบบคอมพิวเตอร์ปลายทางจะใช้โปรแกรมถอดความหมายรหัสตามกฎเกณฑ์การเข้ารหัสเพื่อให้ได้ข้อมูลที่มีความหมายต่อไป

2. Transposition ใช้วิธีการเข้ารหัสโดยเปลี่ยนตำแหน่งของตัวอักษรในข้อมูลตามกฎเกณฑ์ที่กำหนด

3. Arithmetic Manipulation ใช้วิธีการเข้ารหัสโดยใช้กฎเกณฑ์การคำนวณ เช่น หารข้อมูลที่เป็นตัวเลขทุกตัวด้วย 2.356 และส่งผลหารเป็นข้อมูล ซึ่งผู้รับข้อมูลจะต้องถอดรหัสโดยคูณข้อมูลที่ได้รับด้วย 2.356

4. Repetitive Addition of a Key ใช้วิธีการเข้ารหัสโดยรวมข้อมูลที่จะส่งกับข้อมูลอื่น ๆ ที่ไม่มีความหมาย

นอกจากนี้ยังมีเทคนิคพิเศษในการใช้ Cryptograph อีกหลายแบบซึ่งผู้ใช้อาจคิดค้นให้เหมาะสมกับสภาพการใช้งาน

เทคนิคการใช้ Cryptograph ในปัจจุบันมิได้จำกัดอยู่เพียงการรับ-ส่งข้อมูล แต่ได้เริ่มมีบทบาทอย่างกว้างขวางในการเปลี่ยนข้อมูลความลับที่จัดเก็บในแผ่นจานแม่เหล็กด้วยวิธีดังกล่าวเพิ่มมากขึ้นวิธีการเข้า-ถอดรหัสนอกจากจะใช้โปรแกรม Software แล้ว ปัจจุบันยังมีการออกแบบ Hardware สำหรับใช้ในการนี้โดยเฉพาะเพื่อให้ง่ายต่อการใช้และเพิ่มความเร็วในการทำงานอีกด้วย

อย่างไรก็ตาม การใช้วิธี Cryptograph มิได้หมายความว่าสามารถป้องกันความลับรั่วไหลได้สมบูรณ์ โปรแกรมเข้า-ถอดรหัสอาจรั่วไหลได้เช่นเดียวกับโปรแกรมอื่น หรือถ้าผู้ทุจริตมีเวลาและความพยายามอย่างพอเพียงย่อมสามารถถอดรหัสโดยสังเกตจับ Pattern ของข้อมูลหรือใช้คอมพิวเตอร์ช่วยในการถอดรหัส

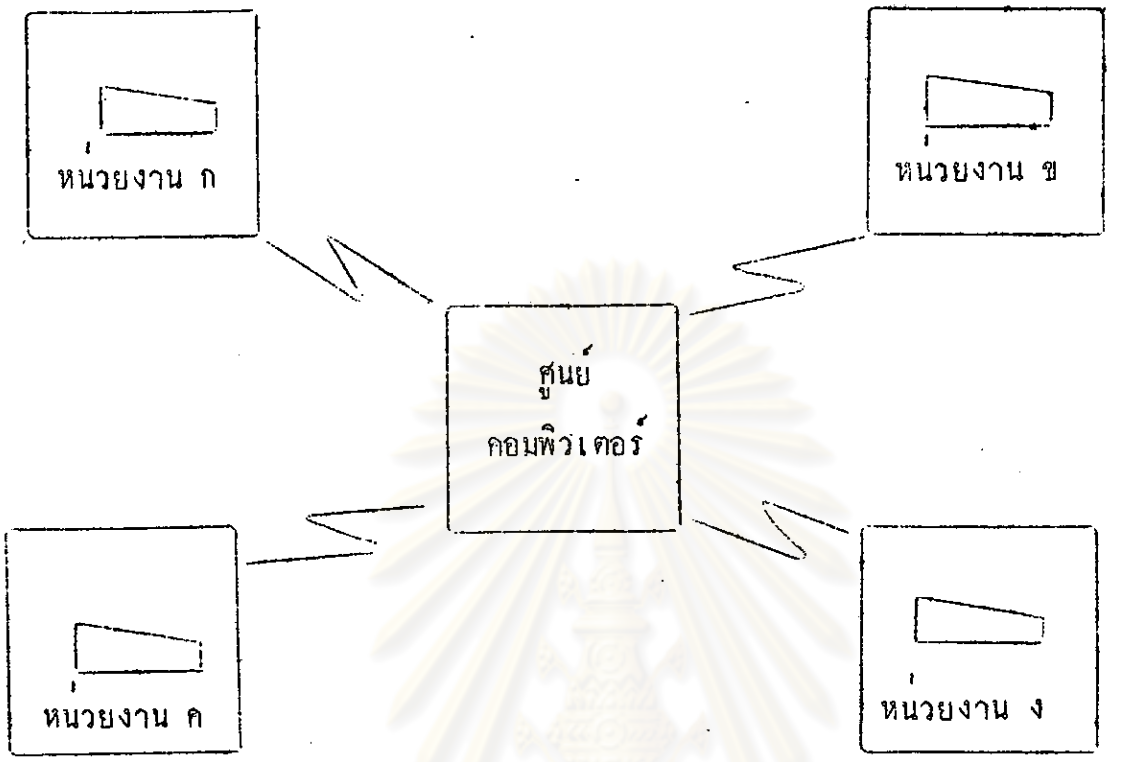
6. <u>การควบคุมด้านการจัดองค์การของศูนย์คอมพิวเตอร์</u>

ตามหลักการควบคุมภายในที่ดี ขอบเขตอำนาจหน้าที่ของผู้ปฏิบัติงานต้องมีการแบ่งแยกกันโดยชัดเจนระหว่าง

ก. ผู้มีอำนาจหน้าที่ในการปฏิบัติงาน
ข. ผู้บันทึกข้อมูลผลของการปฏิบัติงาน
ค. ผู้เก็บรักษาทรัพย์สิน

เมื่อพิจารณาโดยส่วนรวมหน้าที่ของศูนย์คอมพิวเตอร์โดยทั่วไปก็คือ บันทึกข้อมูลผลของการปฏิบัติงาน ดังนั้นอำนาจหน้าที่ของศูนย์คอมพิวเตอร์จะต้องไม่เกี่ยวกับอำนาจหน้าที่ในการปฏิบัติงานของกิจการโดยตรง และต้องไม่เกี่ยวข้องกับการดูแลรักษาทรัพย์สินโดยตรงเช่นกัน

ลักษณะการปฏิบัติข้อมูลในแบบ Online ทำให้ศูนย์คอมพิวเตอร์ต้องเกี่ยวข้องโดยตรงกับหน่วยงานต่าง ๆ ที่มีระบบปฏิบัติข้อมูลเชื่อมโยงกับศูนย์คอมพิวเตอร์นั้น สำหรับการปฏิบัติข้อมูลในแบบ Batch Processing ศูนย์คอมพิวเตอร์มักจะรับผิดชอบในการปฏิบัติข้อมูลตั้งแต่ต้นจนจบขบวนการ โดยหน่วยงานต่าง ๆ ต้องส่งข้อมูลมายังศูนย์คอมพิวเตอร์แต่ในการปฏิบัติข้อมูลในแบบ Online ซึ่ง Terminal ติดตั้งแยกอยู่ในแผนกต่าง ๆ ส่วนใหญ่พนักงานของส่วนงานต่าง ๆ จะทำการ Update และดูแลระบบข้อมูลของส่วนงานนั้น ๆ เอง ศูนย์คอมพิวเตอร์มีหน้าที่เพียงอำนวยความสะดวกให้แก่หน่วยงานผู้ใช้ เช่น ดูแลรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ตลอดจนควบคุมการพิมพ์รายงานประจำวันหรือประจำงวดซึ่งมีปริมาณการพิมพ์จำนวนมาก



แผนภาพที่ 3.14 แสดงศูนย์คอมพิวเตอร์และหน่วยงานที่มีระบบปฏิบัติข้อมูลเชื่อมโยงกับศูนย์คอมพิวเตอร์

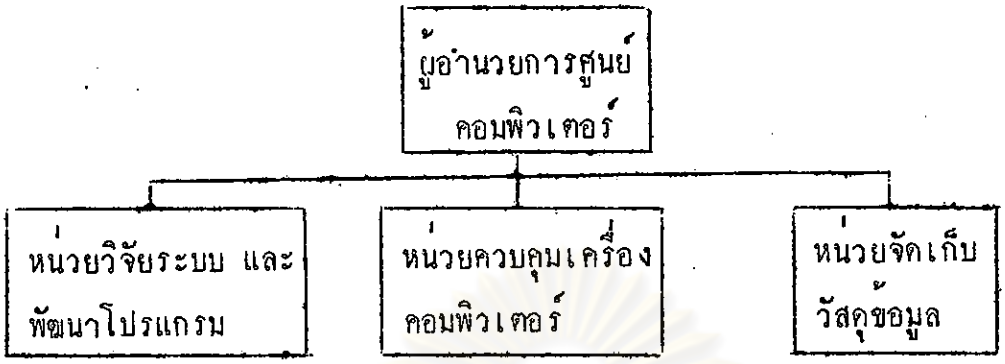
โดยทั่วไปแล้วศูนย์คอมพิวเตอร์จะเป็นหน่วยงานอิสระหรืออาจจะสังกัดหน่วยประมวลบัญชี การจัดองค์การและการแบ่งแยกหน้าที่ในศูนย์คอมพิวเตอร์จะมีการแบ่งแยกหน้าที่ระหว่าง

ก. ผู้มีหน้าที่วางระบบและพัฒนาโปรแกรม (System Designer And Programmer)

ข. ผู้มีหน้าที่ควบคุมเครื่องคอมพิวเตอร์ (Operator)

ค. ผู้มีหน้าที่เก็บรักษาข้อมูล (Librarian)

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย



แผนภาพที่ 3.15 การจัดการองค์การในศูนย์คอมพิวเตอร์

การปฏิบัติข้อมูลในแบบ Batch Processing มักมีข้อกำหนดห้ามมิให้พนักงานพัฒนาโปรแกรมดำเนินการใช้คอมพิวเตอร์ หรือยุ่งเกี่ยวกับวัสดุข้อมูลที่อยู่ในระหว่างการใช้งาน เพราะเกรงว่าพนักงานพัฒนาโปรแกรมซึ่งรู้ขั้นตอนของโปรแกรมดีอาจจะ Manipulate โปรแกรมหรือข้อมูลเพื่อผลในทางทุจริต ในการใช้คอมพิวเตอร์ปฏิบัติงานในแบบ Online การแบ่งแยกเช่นนี้อาจทำได้ยากในทางปฏิบัติ เพราะในการพัฒนาโปรแกรม Online แบบ Interactive พนักงานพัฒนาโปรแกรมจะต้องใช้ Terminal ติดต่อกับคอมพิวเตอร์ระหว่างการปฏิบัติงาน และอยู่ในขอบข่ายที่อาจ Access ข้อมูลที่บันทึกในแผ่นจานแม่เหล็กซึ่งเชื่อมโยงอยู่ในระบบคอมพิวเตอร์โดยตรง ดังนั้นจะเห็นได้ว่า การควบคุมป้องกันการทุจริตโดยอาศัยหลักการแบ่งแยกขอบเขตอำนาจหน้าที่ในระบบ Online ทำได้ยากกว่าระบบการปฏิบัติข้อมูลแบบ Batch Processing

7. การควบคุมพนักงานซึ่งเกี่ยวข้องกับการปฏิบัติข้อมูล

ลักษณะสำคัญประการหนึ่งของการปฏิบัติข้อมูลด้วยระบบคอมพิวเตอร์ทั้งแบบ Batch Processing หรือ Online Processing ก็คือ ถ้ามีข้อผิดพลาดในระหว่างการปฏิบัติงาน การแก้ไขย่อมทำได้ยาก ดังนั้นผู้ที่จะปฏิบัติข้อมูลจะต้องคัดเลือกจากผู้ที่มีความละเอียดรอบคอบในการทำงานเป็นพิเศษ และมีความรู้ในด้านคอมพิวเตอร์พอเพียงที่จะแก้ไขปัญหาเฉพาะหน้าได้ตามสมควร

ในการปฏิบัติข้อมูลแบบ Online สิ่งที่ต้องระมัดระวังเป็นพิเศษก็คือ การรักษาความลับของข้อมูล เพราะโอกาสที่ข้อมูลที่เป็นความลับจะรั่วไหลออกสู่ภายนอกมีมากกว่าระบบการใช้บุคคลปฏิบัติข้อมูล วิธีการปฏิบัติซึ่งสมควรยึดถือแบบหนึ่งก็คือ การให้ผู้เกี่ยวข้องกับการปฏิบัติข้อมูลลงนามในเอกสารห้ามการเปิดเผยความลับของกิจการ

ถึงแม้การลงนามในเอกสารจะมิได้เป็นสิ่งประกันว่าจะไม่มีการทุจริตในการเปิดเผยความลับของข้อมูล แต่อย่างน้อยก็เป็นการซักซ้อมความเข้าใจในด้านนโยบายการรักษาความลับด้านข้อมูลของกิจการ

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

[1] POLICY

CONFIDENTIAL INFORMATION

NON-USE/NON-DISCLOSURE AGREEMENT

In the normal conduct of business, officers and employees of the company have access to and deal with privileged information that belongs to the company and that the company considers to be sensitive or confidential.

All such uses and disclosures of privileged information are prohibited during and following employment with the company.

- Customer names, addresses, sales data, engineering data, and specifications.
- Supplier names and prices of raw materials.
- Product cost, discount, profitability, and unpublished price data.
- Business plans pertaining to: new products, advertising and sales campaigns, mergers/acquisitions/joint ventures, real estate needs, plant closings, and layoffs.
- Computer system software, application programs, and security features.
- Trade secrets, formulas, proprietary processes, and research findings.
- Financial information: budgets, division performance, sales, profit and loss, balance sheet, earnings projections, and inventory data.

- All "insider information" which has not been released to the general public or investment community.
- Collective bargaining strategies and negotiation data.
- Shareholder names, addresses, and holdings.
- Personnel data such as : pay, performance, promotion, background,medical,names,and addresses.

The undersigned acknowledges that he has read and understands this policy, knows that compliance is a condition of employment, realizes that it is his obligation to obtain official authorization before using or disclosing confidential information, and understands that any failure to comply may result in immediate dismissal, in addition to legal action by the company and others.

Sign._____date_____

แผนภาพที่ 3.16 ตัวอย่างเอกสารห้ามเปิดเผยความลับของกิจการ

---

[1] Leonard I.Krauss/Aileen MacGahan, Computer Fraud and Countermeasures : Englewood Cliff. New Jersey, Prentice-Hall,Inc., 1979, p.66.

ระเบียบปฏิบัติอื่น ๆ ซึ่งใช้ควบคุมพนักงานที่เกี่ยวข้องกับการปฏิบัติข้อมูล

ก. ระเบียบปฏิบัติในด้านการหมุนเวียนสับเปลี่ยนงาน (Job Rotation) พนักงานที่ปฏิบัติหน้าที่ในตำแหน่งเดิมติดต่อเป็นเวลานานย่อมมีโอกาสที่จะทุจริตมากกว่าการปฏิบัติหน้าที่ในระยะเวลาอันสั้น หรือไม่ทราบระยะเวลาที่แน่นอน ทั้งนี้เนื่องจากการปฏิบัติหน้าที่ในตำแหน่งเดิมติดต่อกันเป็นเวลานานย่อมมีโอกาสหาช่องทางทุจริตมากกว่าและสามารถหาลู่ทางในการปิดบังพฤติกรรมทุจริตอย่างต่อเนื่อง การหมุนเวียนสับเปลี่ยนหน้าที่นอกจากจะทำให้การปิดบังร่องรอยพฤติกรรมทุจริตทำได้ยากแล้ว ยังมีข้อดีในการลดความเบื่อหน่ายของพนักงานที่ทำงานเดียวกันซ้ำซาก และเปิดโอกาสให้พนักงานได้รับความรู้และประสบการณ์ใหม่ ๆ ทำให้สามารถปฏิบัติงานแทนกันได้ถ้าพนักงานผู้หนึ่งผู้ใดลาออกจากงานโดยกระทันหัน

การหมุนเวียนสับเปลี่ยนหน้าที่ควรกระทำอย่างสม่ำเสมอ และอยู่ในความดูแลของผู้ควบคุมอย่างใกล้ชิด หมายกำหนดการสับเปลี่ยนหน้าที่ไม่ควรประกาศให้ทราบล่วงหน้า ทั้งนี้เพื่อให้ผู้ทุจริตไม่สามารถวางแผนในการปิดบังพฤติกรรมทุจริตล่วงหน้า

ข. ระเบียบปฏิบัติในด้านการลาพักผ่อนของพนักงาน การกำหนดวันลาพักผ่อนของพนักงานโดยกิจการเป็นมาตรการป้องกันมิให้พนักงานที่ทุจริตสามารถปิดบังร่องรอยพฤติกรรมอย่างต่อเนื่อง การบังคับให้พนักงานลาพักผ่อนติดต่อกันในช่วงเวลาที่นานพอสมควรโดยไม่กำหนดวันลาล่วงหน้า ทำให้การวางแผนปิดบังการทุจริตล่วงหน้าทำได้ยาก และร่องรอยมักปรากฏแก่พนักงานที่ปฏิบัติหน้าที่แทนชั่วคราว

8. การควบคุมด้านการวางระบบงาน (System Designs)

การวางระบบงานถือเป็นหัวใจสำคัญของความสำเร็จในการปฏิบัติข้อมูล ถ้าระบบที่วางไว้มีจุดอ่อนหรือข้อบกพร่องไม่เหมาะสมในทางปฏิบัติย่อมเป็นการยากที่ระบบปฏิบัติข้อมูลนั้นจะดำเนินไปอย่างราบรื่น และมักจะเป็นสาเหตุให้เกิดการทุจริตได้ง่าย

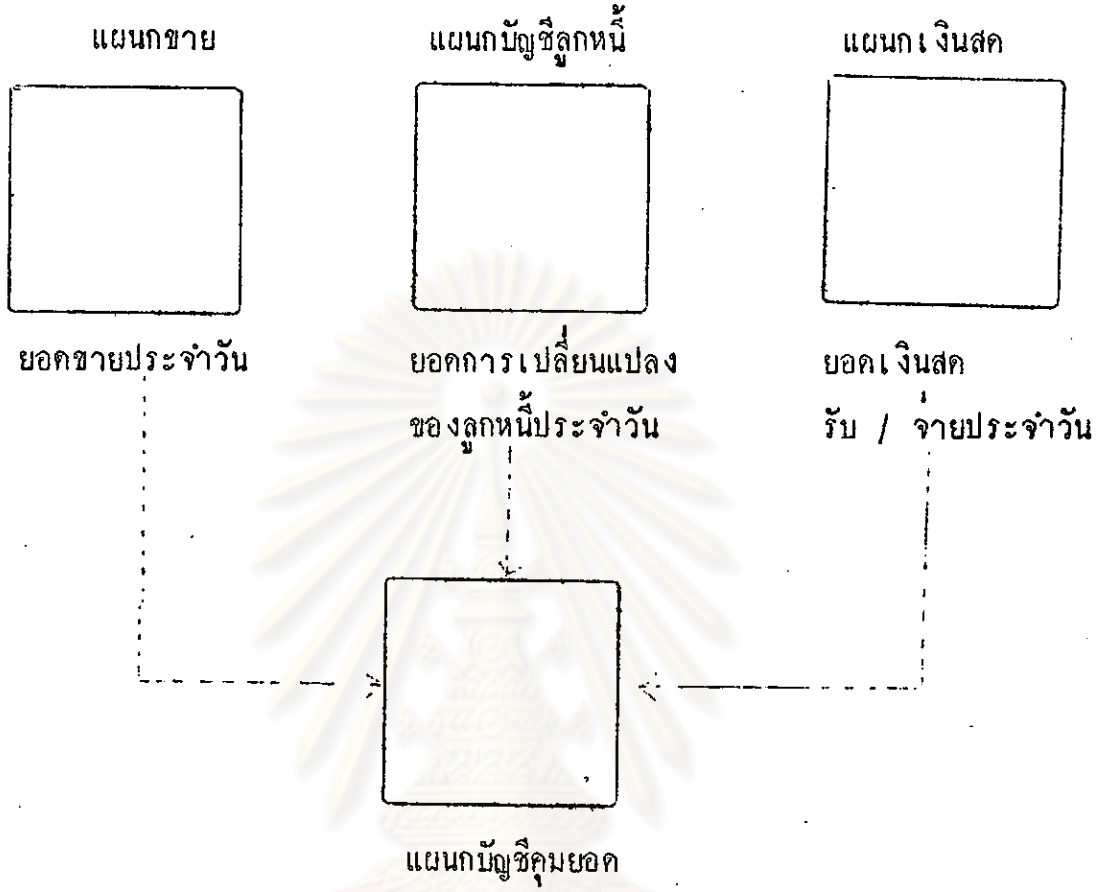
ปัจจัยสำคัญสำหรับการวางระบบประกอบด้วย

ก. <u>ความซับซ้อนของระบบงาน</u> ก่อนที่ทำการตัดสินใจวางระบบงาน จะต้องประเมินความสามารถของพนักงานที่จะปฏิบัติงานตามระบบนั้น ๆ มักปรากฏอยู่เสมอที่ผู้วางระบบพยายามสร้างระบบที่มีประสิทธิภาพโดยเน้นเรื่องความสะดวกในการทำงานของระบบคอมพิวเตอร์ และการประหยัดเนื้อที่จัดเก็บข้อมูลในอุปกรณ์ Mass Storage เช่น พยายามใช้ระบบข้อมูลในลักษณะที่เป็นรหัส ใช้ระบบ File ที่มีโครงสร้างซับซ้อน หรือใช้ระบบ Data Base ผลที่เกิดขึ้นก็คือแม้ระบบนั้นจะเป็นระบบที่คอมพิวเตอร์สามารถทำงานได้เร็ว ประหยัดเนื้อที่ในการจัดเก็บข้อมูล แต่ซับซ้อนเกินกว่าที่พนักงานซึ่งส่วนมากไม่มีพื้นความรู้อย่างพอเพียงสามารถเข้าใจระบบได้ จึงมักปฏิบัติงานตามที่ได้รับมอบหมายด้วยความคลุมเคลือหรือละเลยต่อระบบนั้นทั้งสิ้น หรือสร้างระบบที่ไม่เป็นทางการขึ้นแทน ฉะนั้น ไม่ว่าผู้ใช้จะเลือกทางใดก็ตาม ย่อมถือได้ว่าเป็นจุดเริ่มแห่งความล้มเหลวในระบบดังกล่าว

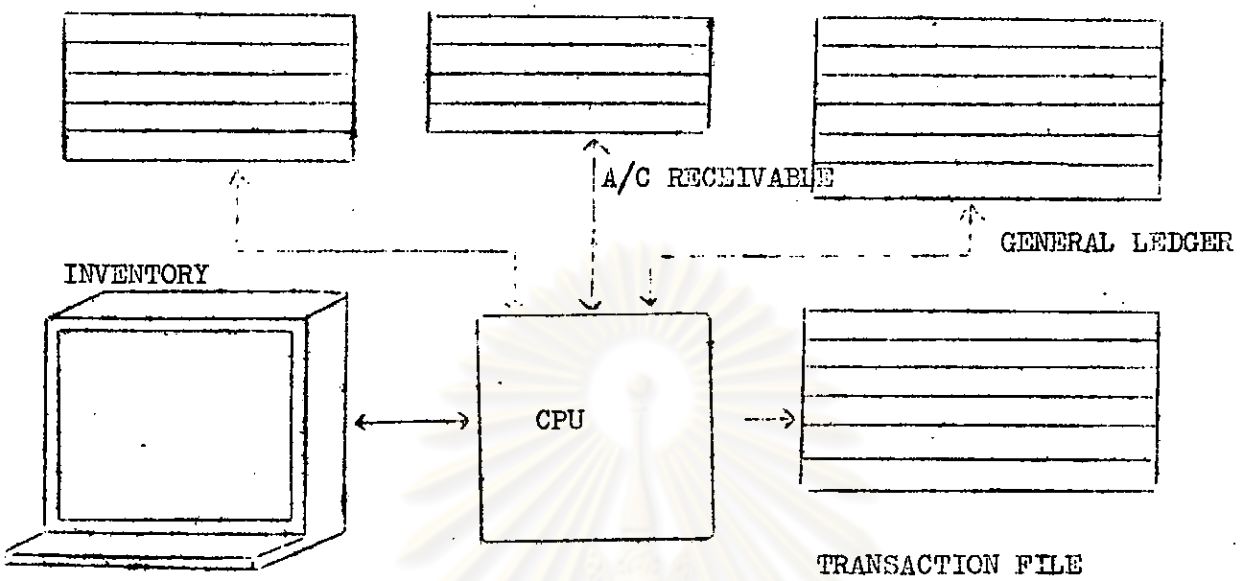
ระบบปฏิบัติข้อมูลอย่างง่าย ๆ ซึ่งถึงแม้เป็นระบบที่ขาดประสิทธิภาพในแง่วิชาการคอมพิวเตอร์ แต่ถ้าเป็นระบบที่ผู้ใช้เข้าใจและยอมรับในฐานะเครื่องมือช่วยในการปฏิบัติงานและส่งเสริมความสามารถของผู้ใช้ ย่อมดีกว่าระบบที่มีประสิทธิภาพสูงสุดในแง่วิชาการคอมพิวเตอร์แต่ซับซ้อนเกินกว่าที่ผู้ใช้จะเข้าใจ

ข. <u>ระบบยืนยันความถูกต้องซึ่งกันและกัน</u> (Dual Control) ระบบบัญชีคู่ซึ่งใช้ในกิจการโดยทั่วไปเป็นระบบที่เน้นการควบคุมความถูกต้องของการปฏิบัติงานโดยแบ่งแยกหน้าที่ในการบันทึกข้อมูล ซึ่งสามารถนำผลของการปฏิบัติงานมาสอบทานยืนยันความถูกต้องซึ่งกันและกัน ทั้งนี้เพื่อสามารถตรวจจับความผิดพลาดและป้องกันการทุจริต

แผนภาพที่ 3.17 แสดงการแบ่งแยกหน้าที่ในการบันทึกข้อมูลในระบบบัญชีคู่



ตัวอย่างเช่น ในกิจการจำหน่ายสินค้า แผนกขายจะรับผิดชอบในการวางระบบเอกสารการขายประจำวัน แผนกบัญชีลูกหนี้จะรวบรวมรายการเกี่ยวกับการเพิ่มยอดหรือลดยอดลูกหนี้รายตัว แผนกเงินสดจะรับผิดชอบบันทึกรายการรับ/จ่ายเงินสดทุกสิ้นวันทั้ง 3 แผนกจะส่งรายละเอียดและรายการสรุปยอดมายังแผนกบัญชีคุมยอดเพื่อลงรายการในบัญชีแยกประเภท แผนกบัญชีคุมยอดสามารถพิสูจน์ความถูกต้องเบื้องต้นในการรวบรวมรายละเอียดการดำเนินงานและรายการสรุปยอดด้านการขายประจำวัน – จากสมการบัญชีง่าย ๆ รายการเดบิทเงินสดจากการขายสินค้าประจำวันรวมกับรายการเดบิทลูกหนี้ประจำวัน จะต้องเท่ากับรายการเครดิตยอดขายประจำวัน ถ้าพบว่าสมการบัญชีดังกล่าวไม่เท่ากัน จะทำให้ยอดดุลในงบทดลองไม่เท่ากัน แผนกบัญชีคุมยอดย่อมทราบได้ว่ามีข้อผิดพลาดในการรวบรวมและบันทึกข้อมูล ซึ่งจะดำเนินการตรวจสอบแก้ไขต่อไป

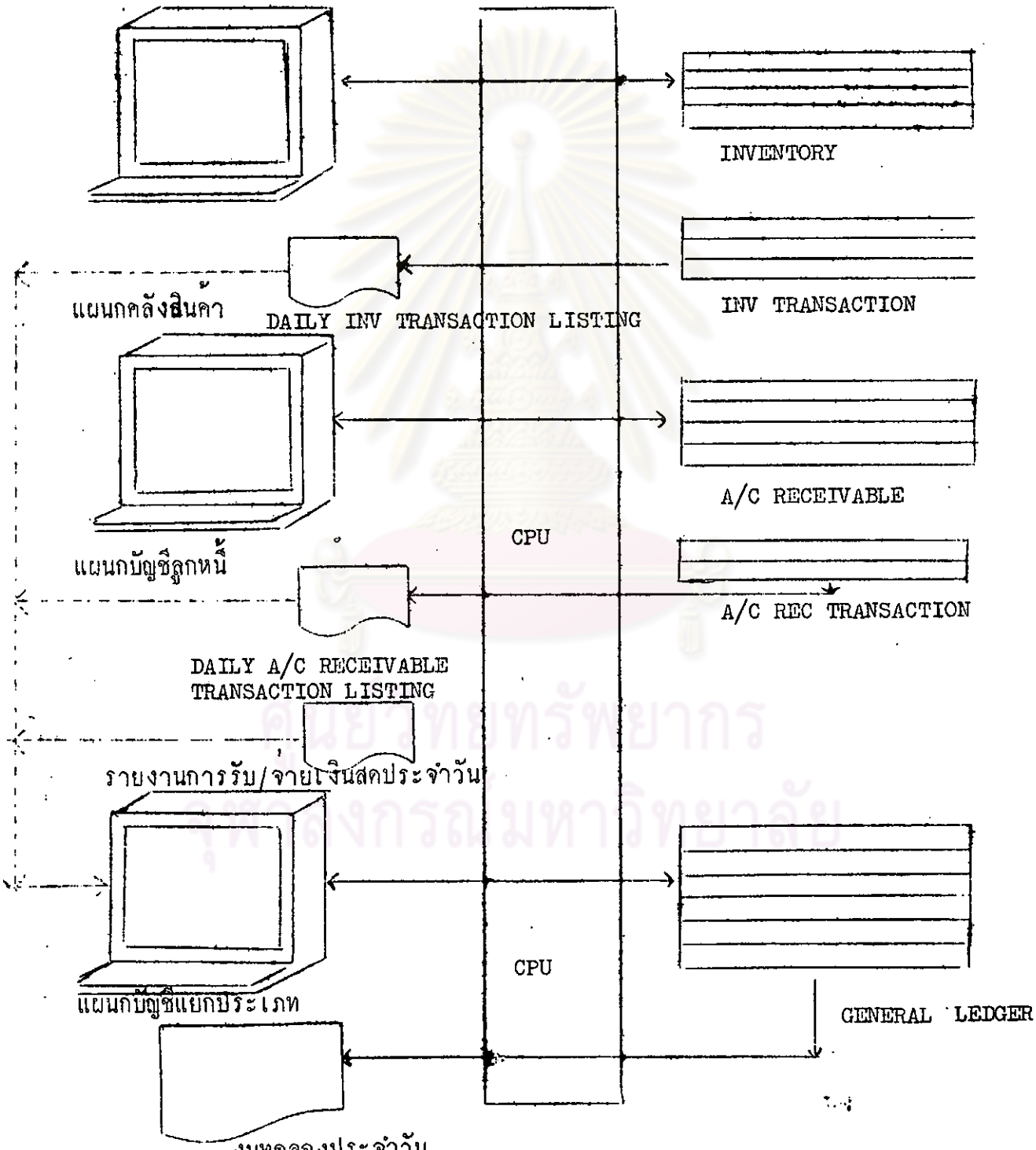


แผนภาพที่ 3.18 การออกแบบระบบงานในแบบที่ไม่มีการยืนยันความถูกต้องซึ่งกันและกัน

บางครั้งการออกแบบระบบกระทำโดยเน้นความสะดวกในการ Update เป็นสำคัญโดยมิได้คำนึงถึงระบบควบคุมยืนยันความถูกต้องซึ่งกันและกันอย่างพอเพียง เช่น เราอาจออกแบบระบบซึ่งถ้ามีรายการขายเกิดขึ้น พนักงานขายสามารถ Key in รายการ Transaction นั้นไปทำการ Update ข้อมูลใน Inventory Master File, Account Receivable File และ General Ledger File ตามประเภทรายการ Transaction ที่เกิดขึ้นได้ในการ Key in เพียงครั้งเดียว จะเห็นได้ว่าถึงแม้ระบบในลักษณะเช่นนี้จะง่ายต่อการ Update ข้อมูล แต่มีข้อเสียที่สำคัญคือ ถ้าพนักงานขาย Key in ข้อมูลผิดพลาดซึ่งจะเกิดจากเจตนาทุจริตหรือไม่ก็ตาม การตรวจสอบยอมทำได้ยาก เพราะยอดดุลในระบบบัญชี General Ledger และรายละเอียดของบัญชีย่อยจะอยู่ในดุลและสัมพันธ์กันตลอดมา

การออกแบบระบบที่สามารถควบคุมความถูกต้องโดยอาศัยหลักการยืนยันยอดซึ่งกันและกันอาจทำได้ โดยแบ่งให้แต่ละหน่วยงานรับผิดชอบการ Update ข้อมูลเฉพาะส่วนที่อยู่ในความรับผิดชอบของหน่วยงานนั้น เช่น แผนกขายมีสิทธิ Update

เฉพาะ Inventory Master File แผนกบัญชีลูกหนี้มีสิทธิ Update เฉพาะ Account Receivable Master File เท่านั้น ทุกสิ้นวันทำการแผนกขายและบัญชีลูกหนี้จะ List รายละเอียด



แผนภาพที่ 3.19 การแบ่งแยกความรับผิดชอบการ Update ข้อมูล

และจัดทำยอดสรุปรายการ Transaction ส่งไปแผนกประมวลบัญชี เช่นเดียวกับแผนกเงินสดจะสรุปรายการรับ/จ่ายนั้นแยกตามประเภทจากทะเบียนเงินสดประจำวัน แผนกบัญชีคุมยอดจะ Key in รายการสรุปเพื่อ Update General Ledger Master File แล้วพิมพ์(List)รายการงบทดลองประจำวัน ซึ่งถ้าทุกอย่างดำเนินไปอย่างถูกต้อง ยอดดุลของงบทดลองประจำวันจะอยู่ในดุล แต่ถ้ามีข้อผิดพลาดในการ Update ข้อมูลเกิดขึ้น การที่งบทดลองไม่อยู่ในดุลจะเป็นเครื่องเตือนให้พิจารณาทำการทดสอบหาข้อผิดพลาด

ถึงแม้การออกแบบระบบซึ่งสามารถควบคุมความถูกต้องโดยอาศัยหลักการยืนยันยอดซึ่งกันและกันจะทำให้ต้องยุ่งยากในการ Enter รายการ Transaction เดียวกันหลายครั้ง ทำให้ใช้เวลาในการปฏิบัติข้อมูลมาก แต่การมีระบบเตือนเมื่อมีความผิดพลาดเกิดขึ้น ย่อมทำให้สามารถแน่ใจในความถูกต้องขั้นต้นของระบบและป้องกันการทุจริตซึ่งอาจเกิดขึ้น

ค. <u>รายละเอียดประกอบการปฏิบัติข้อมูล</u> (Audit Trail)

STOCK CARD

INV NO 1003

NAME PEN (BLUE)

DATE	IN/OUT	UNIT	COST
01-01-80	BD	200	5.00
02-01-80	+100	300	5.00
05-01-80	-80	220	5.00

<u>แผนภาพที่ 3.20</u> แผ่นบัญชีในระบบปฏิบัติข้อมูลแบบใช้บุคคล

ในระบบปฏิบัติข้อมูลแบบใช้บุคคล โดยลงรายการในแผ่นบัญชี รายการที่ลงในแผ่นบัญชีย่อมเป็น Audit Trail ที่ต่อเนื่องและง่ายต่อการตรวจสอบ ตัวอย่างเช่น ถ้าจะตรวจสอบความถูกต้องของยอดคงเหลือ-พัสดุรายการใดรายการหนึ่ง ผู้ทำการตรวจสอบอาจนำเอกสารเบื้องต้น เช่น ใบรับ/ใบเบิกพัสดุมาทำการผ่านรายการกับรายการในแผ่นบัญชีเพื่อตรวจสอบว่า การลงรายการครบถ้วนถูกต้องหรือไม่ ทดสอบการคำนวณออกยอดคงเหลือว่าถูกต้องเพียงใด และผู้ตรวจสอบอาจวิเคราะห์ประวัติรายการเปลี่ยนแปลงต่อเนื่องที่ปรากฏในแผ่นบัญชีว่ามีรายการที่ผิดปกติหรือไม่

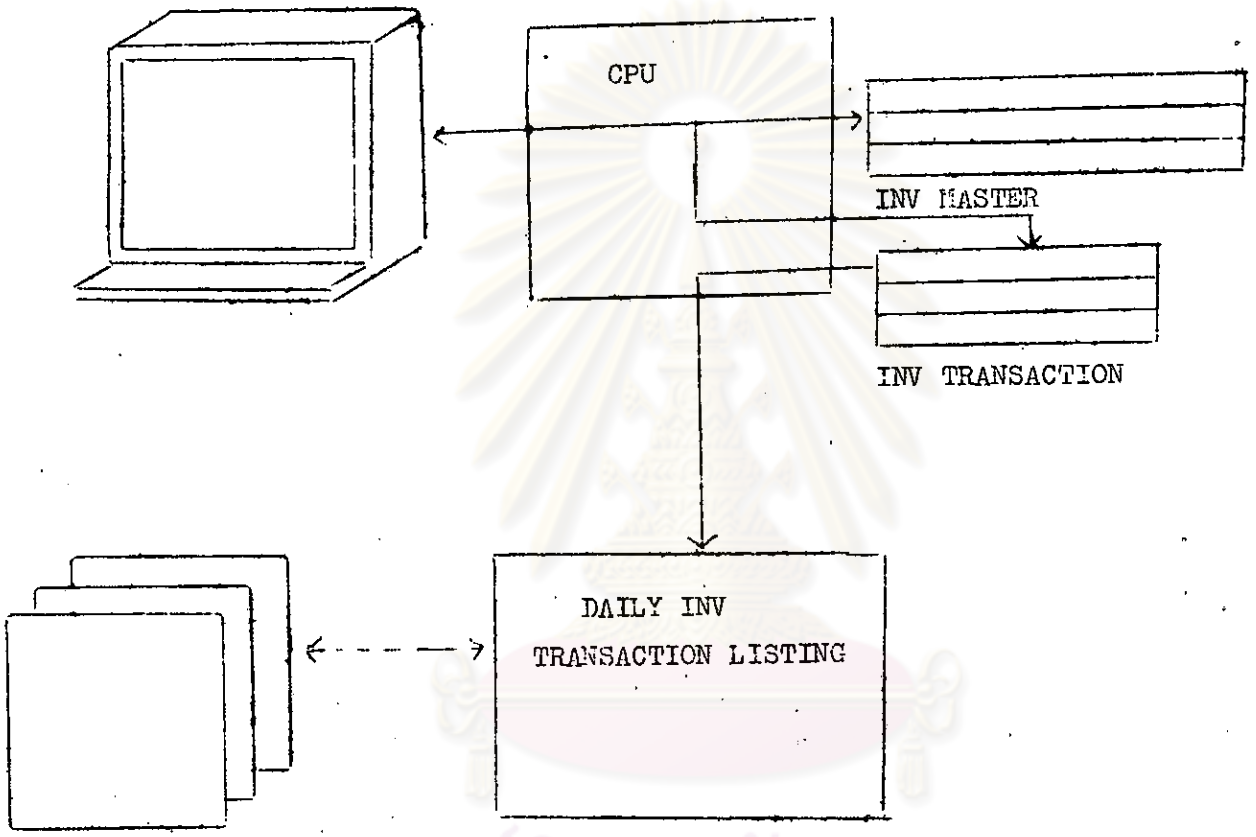
ในการปฏิบัติข้อมูลแบบ Online ซึ่งบันทึกข้อมูลในแผ่นจานแม่เหล็ก ผู้ออกแบบระบบจะต้องคำนึงถึงการประหยัดเนื้อที่จัดเก็บข้อมูลและความง่ายในการปฏิบัติงาน

MASTER RECORD	TRANSACTION HISTORY 1	2	3

แผนภาพที่ 3.21 โครงสร้างของ Inventory Master File

ตัวอย่างเช่น ถ้าจะออกแบบโครงสร้างของ Inventory Master File ให้สามารถบันทึก Audit Trail ต่อเนื่องเช่นเดียวกับการบันทึกรายการ Transaction ในแผ่นบัญชีลักษณะโครงสร้างของ Inventory Master File อาจมีลักษณะดังภาพ ถ้า File นี้มีโครงสร้างของ File เป็นแบบ Index ซึ่งนิยมกำหนดให้แต่ละ Record มีความยาวเท่ากัน (Fixed Lenght Record) เพื่อง่ายต่อการ Handle ปัญหาที่เกิดขึ้นก็คือจะกันเนื้อที่ใช้สำหรับรายการ Transaction กี่รายการต่อ 1 Record ถ้าเนื้อที่ใช้สำหรับรายการ Transaction มากเกินไป จำนวนรายการ Transaction ของพัสดุแต่ละรายการอาจไม่เท่ากัน พัสดุบางรายการมี Transaction มาก บางรายการมีน้อย สำหรับพัสดุที่มีรายการ Transaction น้อย เนื้อที่ที่กันไว้ก็จะเป็นเนื้อที่ที่ไม่ถูกนำมาใช้ประโยชน์คุ้มค่า ในทางตรงข้ามถ้ากันเนื้อที่

ไว้น้อยเกินไป ก็อาจไม่เพียงพอสำหรับพัสดุที่มีรายการ Transaction มาก จะเห็นได้ว่าการออกแบบระบบให้คงรักษา Audit Trail เช่นเดียวกับแผ่นบัญชีเป็นเรื่องที่ยุ่งยากทั้งในด้านการพัฒนาโปรแกรมและการ Maintenance File



แผนภาพที่ 3.22 แสดงการ List รายการ Transaction ตรวจสอบกับเอกสารเบื้องต้น

เพื่อความสะดวกในการออกแบบโครงสร้างของ File และง่ายต่อการพัฒนาโปรแกรม Audit Trail ของการปฏิบัติงานในแบบ Online มักอยู่ในรูปของการบันทึกรายละเอียดของรายการ Transaction ที่นำไป Update Master File ไว้ใน Transaction File และทุกสิ้นวันจะทำการ List รายการ Transaction มาตรวจสอบกับเอกสารเบื้องต้นว่าครบถ้วนและถูกต้องตรงกันหรือไม่

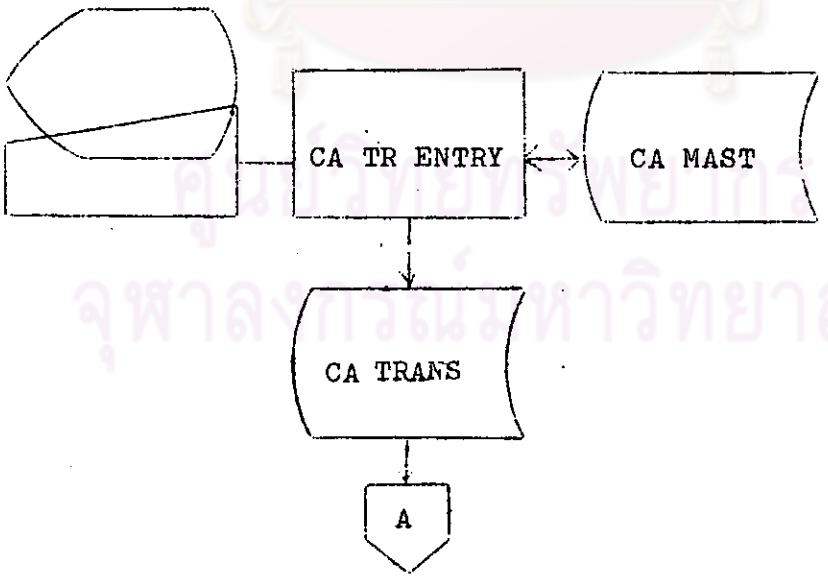
ในการปฏิบัติข้อมูลแบบ Online ข้อมูลที่ผ่านการ Update เช่น ยอดคงเหลือของพัสดุที่มีรายการเปลี่ยนแปลงจะถูกบันทึกแทนที่ยอดคงเหลือเดิม ดังนั้นจึงไม่อาจตรวจสอบผลของการ Update โดยการกระทบยอดคงเหลือเดิมกับรายการเปลี่ยนแปลงและยอดคงเหลือใหม่ ดังเช่น Audit Trail ที่ปรากฏในแผ่นบัญชี การที่จะเชื่อถือว่ายอดคงเหลือหลังการ Update ถูกต้องเพียงใด ย่อมขึ้นอยู่กับความเชื่อถือในความถูกต้องของโปรแกรมที่ใช้ Update โดยตั้งสมมุติฐานว่า ถ้าพิสูจน์ได้ว่าโปรแกรมถูกต้องและดำเนินการ Update อย่างถูกต้อง ผลที่ได้จากการ Update ย่อมถูกต้อง

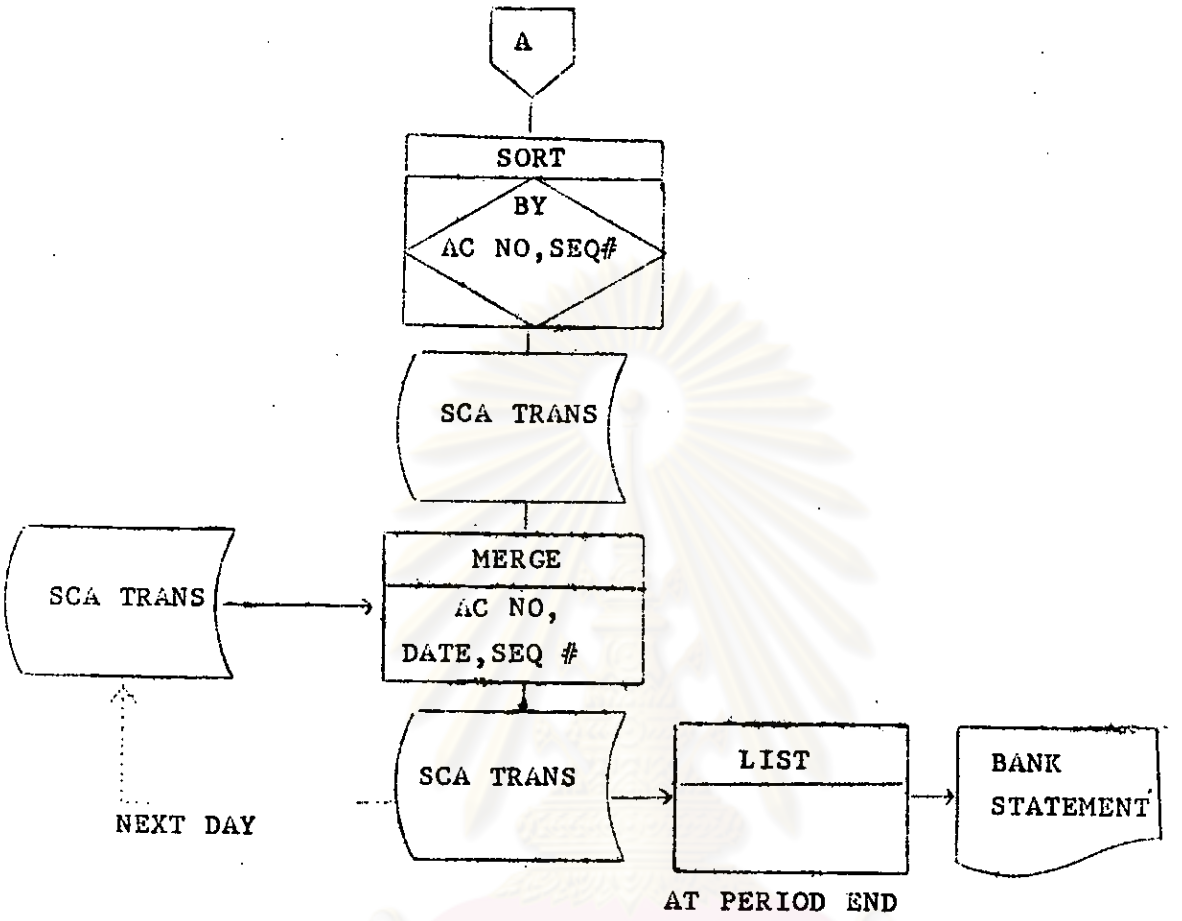
ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

การแสดงรายละเอียดประกอบการ Update อาจทำได้โดยการขยายขนาดของ Transaction Record เพื่อเก็บยอดคงเหลือยกมาและยอดคงเหลือยกไปของรายการที่ถูก Update

สำหรับรายการ Update บางรายการซึ่งมีระบบการคำนวณที่ซับซ้อนและต้องการเก็บรายละเอียดการคำนวณไว้เป็นหลักฐานเช่น รายการคำนวณดอกเบี้ยบัญชีเงินเบิกเกินบัญชีของธนาคารพาณิชย์ซึ่งอัตราดอกเบี้ยที่ใช้ในการคำนวณสำหรับลูกค้าบางรายอาจมีถึง 4 อัตรา รายงานแสดงรายละเอียดการคำนวณอาจเป็นสิ่งจำเป็นต่อการตรวจสอบ

การปฏิบัติข้อมูลบางประเภทอาจมีความจำเป็นจะต้องมีรายงานแสดงรายการ Update เรียงตามลำดับต่อเนื่องเสมือนรายการที่แสดงในแผ่นบัญชี เช่น รายงาน Bank Statement ของบัญชีกระแสรายวันที่ธนาคารต้องส่งให้ลูกค้า การจัดเตรียมรายงานลักษณะดังกล่าวอาจกระทำได้โดย System Flowchart ต่อไปนี้





แผนภาพที่ 3.23 แสดง Flowchart การจัดทำรายงาน Bank Statement ของบัญชีกระแสรายวัน (Current Account)

การเตรียมรายงานในลักษณะดังกล่าวมีขั้นตอนที่ยุ่งยากโดยเฉพาะการ Sort ข้อมูลเป็นขั้นตอนที่ใช้เวลามาก ดังนั้น รายงานประเภทนี้จึงมักจัดเตรียมเมื่อมีความจำเป็นโดยแท้จริงเท่านั้น

จะเห็นได้ว่าในการปฏิบัติข้อมูลในแบบ Online ยิ่งมีการเตรียม Audit Trail ที่รัดกุมต่อเนื่องเพียงใด ระบบการปฏิบัติข้อมูลจะยิ่งซับซ้อนเพิ่มขึ้นเพียงนั้น ผู้ออกแบบระบบจะต้องตัดสินใจหาจุดสมดุลย์ระหว่างการมี Audit Trail ที่พอเพียงและพิจารณาค่าใช้จ่ายว่าคุ้มกันหรือไม่

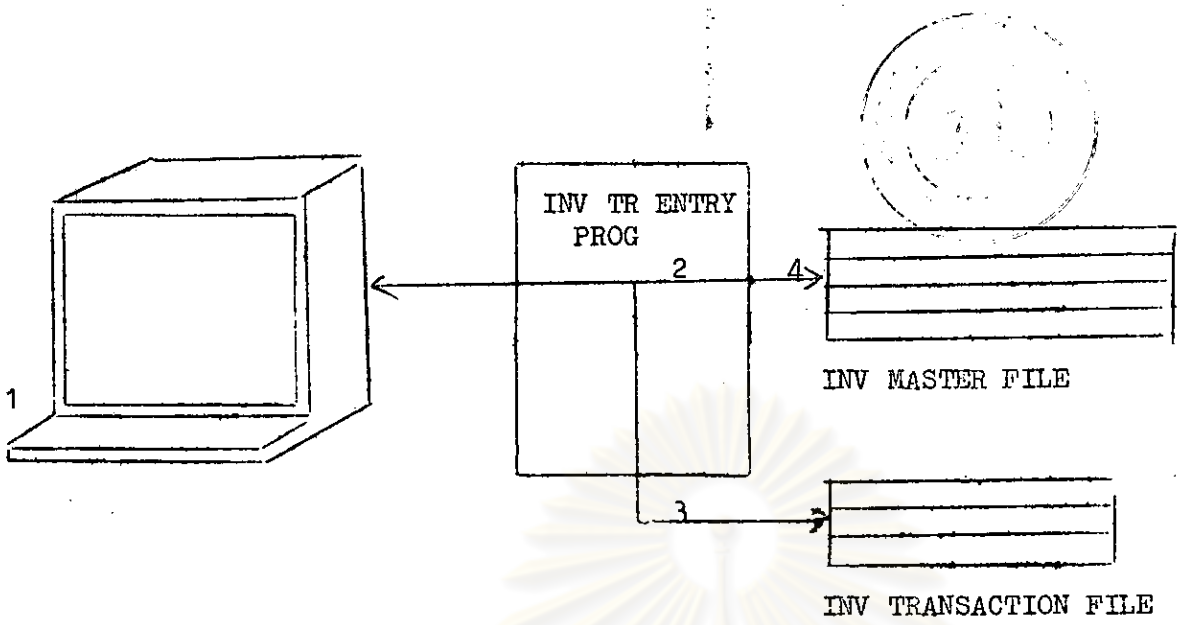
ง. การเตรียมพร้อมสำหรับข้อขัดข้อง เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เป็นเครื่องจักรกลซึ่งเหมือนกับเครื่องจักรกลทั่วไปที่อาจขัดข้องโดยไม่สามารถคาดหมายล่วงหน้า การขัดข้องอาจเกิดจากสภาวะแวดล้อม เช่น กระแสไฟฟ้า ภัยธรรมชาติ เป็นต้น รวมทั้งเกิดจากตัวเครื่องคอมพิวเตอร์และอุปกรณ์เอง การมีมาตรการที่รัดกุมเพื่อเตรียมพร้อมสำหรับข้อขัดข้องจะช่วยลดความเสียหายที่อาจเกิดขึ้น มาตรการดังกล่าวได้แก่

- Check Point and Recovery
- Graceful Degration

Check Point and Recovery การปฏิบัติข้อมูลแบบ Batch Processing ซึ่ง Master Record เดิมที่ถูกนำมา Update มิได้ถูกเปลี่ยนแปลงแก้ไข เมื่อมีข้อขัดข้องเกิดขึ้น เช่น ไฟฟ้าดับระหว่างปฏิบัติงาน การ Recovery ทำได้ง่าย โดยการ Reprocess ข้อมูลใหม่ทั้งหมด อย่างไรก็ตามถ้า File มีขนาดใหญ่ การ Reprocess ข้อมูลตั้งแต่ต้นย่อมสิ้นเปลืองเวลา ดังนั้นจึงนิยมแบ่งกลุ่มของ Record เป็นส่วน ๆ (Segment หรือ Block) และ ณ จุดสุดท้ายของแต่ละส่วนที่ผ่านการ Process แล้วจะทำเครื่องหมาย Check Point ในกรณีที่มีข้อขัดข้องเกิดขึ้นการ Reprocess อาจทำเฉพาะส่วนที่ต่อจาก Check Point ก็คือส่วนที่ยังคงค้างการ Process นั่นเอง

ในระบบการปฏิบัติงานแบบ Online ซึ่งข้อมูลถูก Update โดยวิธีบันทึกแทนที่ (Replace) ข้อมูลเดิม การจัดทำ Check Point เป็นสิ่งจำเป็น ถ้ามีข้อขัดข้องเกิดขึ้นระหว่างการปฏิบัติงานระบบ Check Point จะแสดงให้เห็นว่าการปฏิบัติงานได้ทำไปถึงจุดใด การ Recovery จะทำในลักษณะใด

เพื่อแสดงความสำคัญของระบบ Check Point and Recovery จะแสดงตัวอย่างง่าย ๆ ดังนี้



แผนภาพที่ 3.24 ลำดับขั้นตอนการ Update ข้อมูลใน Inventory Master File

ลำดับขั้นตอนการ Update ข้อมูลใน Inventory Master File มีดังนี้

(1) พนักงาน Key in รายการ Transaction ผ่าน Terminal

(2) คอมพิวเตอร์อ่าน Record ที่มีรายการ Transaction จาก Inventory Master File

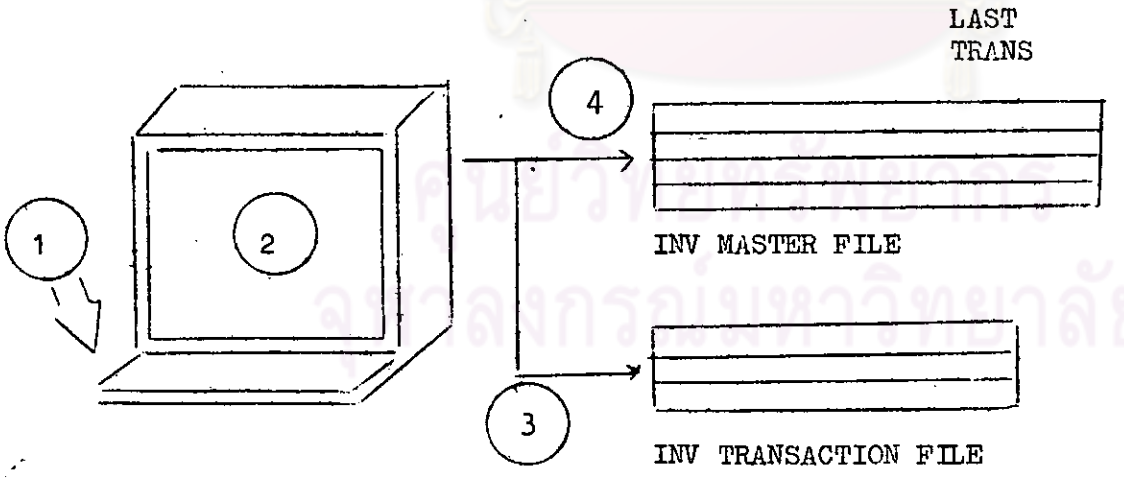
(3) บันทึกรายการ Transaction เก็บไว้ใน Daily Transaction File

(4) Replace Record ที่อ่านจาก Inventory Master File ด้วยข้อมูลที่ผ่านการ Update แล้ว

ถ้าไฟฟ้าดับในระหว่างช่วงลำดับที่ (1) และ (2) การ Update ยังไม่เกิดขึ้น แต่ถ้าไฟฟ้าดับเมื่อเสร็จงานในลำดับที่ (3) แต่ยังไม่เสร็จสิ้นงานในลำดับที่ (4) จะมีรายการ Transaction นี้ปรากฏใน Transaction File แต่ไม่มีการ Update Master File และถ้าไฟฟ้าดับหลังจากเสร็จสิ้นงานในลำดับที่ (4) แล้ว การ Update จะเสร็จสิ้นสมบูรณ์

จะเห็นได้ว่าถ้าไม่มีระบบ Check Point ที่ดีพนักงานซึ่งปฏิบัติข้อมูลจะไม่มีทางทราบเลยว่า การ Update ที่ยังค้างอยู่ได้เสร็จสิ้นไปเพียงใดโดยเฉพาะเมื่อเกิดข้อขัดข้องหลังจากเสร็จสิ้นงานในลำดับที่ (3) ไปแล้ว ถ้าพนักงานพิมพ์(List)รายการ Transaction จาก Transaction File มาตรวจสอบพบว่ามีรายการ Transaction นั้น บันทึกไว้อาจเข้าใจว่าการ Update เสร็จสิ้นสมบูรณ์ จึงข้ามไปปฏิบัติงานอื่นต่อ ทั้งนี้โดยข้อเท็จจริงแล้วข้อขัดข้องได้เกิดขึ้นก่อนที่จะเริ่มปฏิบัติงานในลำดับที่ (4) ซึ่งข้อมูลใน Master File ยังไม่ได้ Update ในทางตรงข้ามถ้าพนักงานเข้าใจว่ายังไม่ได้ Update Master File จึงทำการ Reupdate ซึ่งตามข้อเท็จจริงแล้วข้อขัดข้องเกิดขึ้นหลังจากเสร็จสิ้นงานในลำดับที่ (4) ในกรณีนี้ข้อมูลใน Master File จะถูก Update ซ้ำ

การสร้างระบบ Check Point อาจทำโดยวิธีบันทึกรายละเอียดรายการ Transaction สุดท้าย (Last Transaction Identifier) ไว้ใน Master File Record ทุกครั้งที่ทำการ Replace



แผนภาพที่ 3.25 การสร้างระบบ Check Point โดยบันทึกรายการรายละเอียดรายการ Transaction สุดท้าย

หลังจากมีข้อขัดข้องเกิดขึ้นการ Recovery จะกระทำโดย

(1) อ่าน Transaction Record สุดท้าย และตรวจว่าเป็นรายการ Transaction ของ Record ใดใน Master File

(2) อ่าน Record นั้นจาก Master File ตรวจดูว่า Last Transaction Identifier ตรงกันหรือไม่

- ถ้าตรงกันแสดงว่าการ Update ได้ทำจนเสร็จสิ้นขบวนการ
- ถ้าไม่ตรงกันแสดงว่ายังไม่ได้มีการ Replace Master Record การ Recovery อาจทำโดยทำการ Update Master Record นั้นใหม่ตามรายละเอียดใน Transaction Record จนสิ้นขบวนการ

รายละเอียดในเรื่อง Check Point and Recovery ให้ศึกษาเรื่องการควบคุมการปฏิบัติงาน ซึ่งจะได้กล่าวถึงต่อไป

<u>ระดับการ Recovery</u>

(1) ถ้าข้อขัดข้องที่เกิดขึ้นไม่ทำให้ข้อมูลถูกทำลาย การ Recovery ทำได้โดยใช้วิธีการ Check Point ดังได้กล่าวมาแล้ว

(2) ถ้าข้อขัดข้องที่เกิดขึ้นทำให้ข้อมูลถูกทำลาย

ก. ถ้าข้อขัดข้องเกิดขึ้นในขณะยังไม่มีการ Update เกิดขึ้น อาจใช้ข้อมูล Back up Load เข้าสู่ระบบ และรวบรวมรายการ Transaction ที่ยังค้างการ Update มาปฏิบัติ

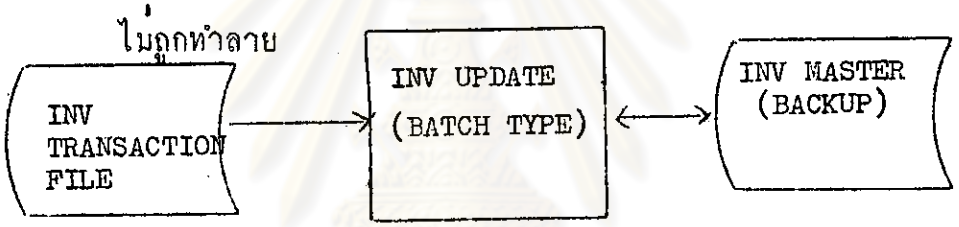
ข. ถ้าข้อขัดข้องเกิดขึ้นเมื่อมีการ Update ข้อมูลบางส่วนแล้ว

- ถ้าทั้ง Master File และ Transaction File

ถูกทำลาย การ Recovery จะทำโดยใช้ข้อมูล Back up มาทำการ Update ใหม่ตามวิธีปกติ

– ถ้า Master File ถูกทำลายแต่ Transaction File ไม่ถูกทำลาย การ Recovery อาจทำโดยใช้ Master File ที่ Back up ไว้ Load เข้าสู่ระบบและทำการ Update ข้อมูลกับ Transaction File ในแบบ Online Batch เพื่อไม่ต้อง Key in รายการ Transaction เข้าสู่คอมพิวเตอร์ใหม่

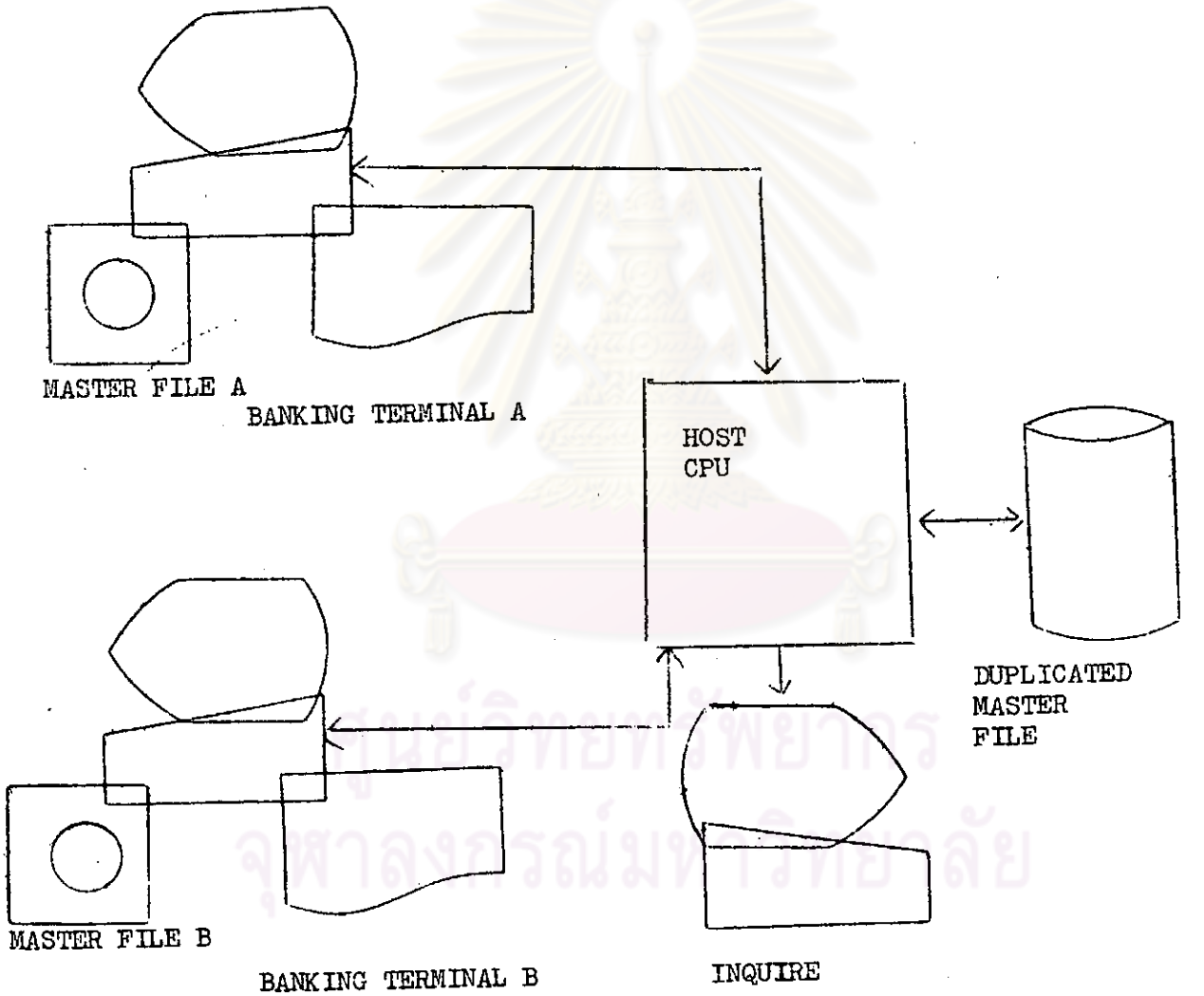
<u>แผนภาพที่ 3.26</u> การ Recovery เมื่อ Master File ถูกทำลายแต่ Transaction ไม่ถูกทำลาย



– ถ้า Master File ไม่ถูกทำลาย แต่ Transaction File ถูกทำลาย การ Recovery อาจทำโดยใช้ Master File Back up มาทำการ Update ใหม่ทั้งหมดหรือทำการ Updata Master File เดิมต่อไป และสร้าง Transaction ส่วนที่ขาดไปภายหลัง

<u>Graceful Degration</u> การปฏิบัติข้อมูลบางประการ เช่น การ Update ข้อมูลของระบบ Inventory ถ้ามีข้อขัดข้องเกิดขึ้นผู้ใช้อาจหยุดการปฏิบัติงานไว้ชั่วคราว จนกว่าทุกอย่างถูกแก้ไขจนคืนเข้าสู่ภาวะปกติจึงปฏิบัติงานต่อไป โดยรวบรวมรายการ Transaction ที่ค้าง Update มาปฏิบัติข้อมูลจนทันต่อการเปลี่ยนแปลง อย่างไรก็ตามมีระบบการปฏิบัติข้อมูลบางประเภทซึ่งการหยุดปฏิบัติงานจะก่อให้เกิดความเสียหายอย่างร้ายแรง เช่น การปฏิบัติข้อมูลในระบบเงินฝากกระแสรายวันของธนาคารพาณิชย์ ดังนั้น ในการออกแบบระบบจะต้องเตรียมมาตรการให้สามารถปฏิบัติงานต่อไปได้ถึงแม้จะไม่สมบูรณ์เช่นในภาวะปกติ

การเตรียมการสำหรับ Graceful Degration หมายถึงจะต้องเตรียมมาตรการฉุกเฉิน ซึ่งเรียกว่า Fall Back Procedure เพื่อให้แก้ไขระดับการปฏิบัติงานโดยอาจตัดส่วนที่ไม่สำคัญในขั้นตอนการทำงานออกตามความจำเป็น แต่การปฏิบัติงานบางส่วนยังดำเนินต่อไป ซึ่งเรียกว่า Fail Softly



แผนภาพที่ 3.27 การออกแบบระบบที่มีการเตรียมสำหรับ Graceful Degration

ตัวอย่างเช่น การปฏิบัติข้อมูลในระบบบัญชีเงินฝากกระแสรายวันของธนาคารไทยทนุ จำกัด Banking Terminal แต่ละ Unit มีสภาพเป็นคอมพิวเตอร์แบบ Subsystem โดยมีจอภาพ, เครื่องพิมพ์, CPU บัตรบัญชีเงินฝาก และ Mass Storage ประเภท Diskette เพื่อจัดเก็บ Master File โดย Banking Terminal แต่ละ Unit สามารถทำงานในลักษณะ Stand Alone ทุก Banking Terminal จะต่อเชื่อมกับระบบคอมพิวเตอร์ใหญ่ (Main CPU) โดยมี Duplicated Master File ใน Mass Storage ประเภท Fixed Disk การ Update ข้อมูลจะกระทำทั้งใน Master File ของ Banking Terminal และใน Duplicated Master File ของ Main CPU เพื่อให้สามารถเชื่อมโยงระบบการ Inquire ข้อมูล นอกจากนั้น Transaction Record จะถูกส่งมาจัดเก็บใน Mass Storage ของ Main CPU เพื่อสามารถจัดทำรายงานเช็คเคลียริ่งประจำวัน

Fall Back Procedure จะประกอบด้วยลำดับขั้นดังนี้

ก. ถ้า Main CPU หรือเส้นทางเชื่อมโยงข้อมูลระหว่าง Banking Terminal และ CPU ขัดข้อง Banking Terminal จะยังปฏิบัติงานเป็นปกติ โดยทำการตัด (Bypass) ขั้นตอนการส่งข้อมูลไป Update Duplicated Master File ใน Main CPU และงดการส่ง Transaction Record

งานที่หยุดชะงักในกรณีนี้ก็คือ การ Inquire อาจทำได้ไม่สมบูรณ์เพราะไม่ได้มีการ Update Duplicated Master File และรายงานเช็คเคลียริ่งไม่อาจกระทำได้

ข. ถ้า Banking Terminal บางหน่วยขัดข้องอาจพิจารณาใช้ Banking Terminal ของระบบเงินฝากที่มีการเคลื่อนไหวน้อยเช่น Banking Terminal ของระบบเงินฝากประจำปฏิบัติงานทดแทน

ก. ถ้าอุปกรณ์ทุกส่วนขัดข้อง การปฏิบัติงานจะยังคงดำเนินต่อไปโดยลง

รายการในบัตรบัญชีเงินฝากในแบบ Manual และนำรายการที่เกิดขึ้นในระหว่างนั้นมาผ่าน (Post) เข้าสู่ระบบคอมพิวเตอร์เมื่อแก้ไขอุปกรณ์ที่ขัดข้องเข้าสู่ภาวะปกติแล้ว

ข้อควรระวังก็คือ ถึงแม้จะมีการเตรียมมาตรการFall Back Procedure ไว้ดีเพียงใดก็ตาม แต่ถ้าไม่ได้มีการชี้แจงให้ผู้ปฏิบัติงานเข้าใจ หรือซักซ้อมการใช้มาตรการโดยสม่ำเสมอแล้ว ในกรณีเกิดข้อขัดข้องขึ้นจริงพนักงานอาจไม่สามารถปฏิบัติตาม Fall Back Procedure ได้อย่างมีประสิทธิภาพ

9. <u>การควบคุมด้านการทำเอกสารประกอบระบบงาน</u> โดยเหตุที่เทคนิคการใช้ระบบคอมพิวเตอร์ปฏิบัติข้อมูลมักจะยุ่งยากซับซ้อน ดังนั้น การจัดทำเอกสารประกอบ — ระบบงานจึงเป็นสิ่งจำเป็นอย่างยิ่ง ประโยชน์ของการทำเอกสารประกอบระบบงาน ได้แก่

ก. เป็นสิ่งเชื่อมโยงช่วยให้ผู้บริหารเข้าใจจุดมุ่งหมาย, ขั้นตอนการปฏิบัติงาน และมาตรการควบคุม

ข. ช่วยให้ผู้มีหน้าที่วิเคราะห์และออกแบบระบบงาน, พนักงานพัฒนาโปรแกรม ตลอดจนพนักงานซึ่งปฏิบัติงานมีสิ่งอ้างอิงในการปฏิบัติงาน และสามารถวางแนวทางในการปรับปรุงระบบงานได้โดยง่าย

ค. ช่วยให้ผู้ตรวจสอบทั้งภายในและภายนอกเข้าใจระบบงาน ทำให้สามารถวางแนวการตรวจสอบอย่างมีประสิทธิภาพ

ง. ช่วยในการกำหนดมาตรฐานการปฏิบัติงาน

การละเลยไม่ควบคุมให้มีการจัดทำเอกสารประกอบระบบงานโดยเหมาะสมย่อมแสดงให้เห็นถึงระบบการควบคุมที่อ่อนแอ และการละเลยของผู้บริหารตั้งแต่เบื้องต้น

เอกสารประกอบระบบงานอาจแบ่งตามขั้นตอนของการเตรียมงานดังนี้

ก. เอกสารประกอบระบบงานที่จัดเตรียมในขั้นวางระบบงาน ได้แก่

- System Flowchart ซึ่งแสดงขั้นตอนของการปฏิบัติข้อมูลในด้านของระบบงานส่วนรวม
- Record Layout แสดงถึงโครงสร้างของ Record ในแต่ละ File
- Display และ Report Layout แสดงถึงรูปแบบของข้อมูลที่จะแสดงในจอภาพ หรือจัดพิมพ์ในรูปของรายงาน

นอกจากนี้ยังอาจมี Document Form Layout ซึ่งแสดงถึงรูปแบบเอกสารเบื้องต้นที่จะใช้ในแต่ละขั้นตอน

ข. เอกสารประกอบระบบงานซึ่งจัดเตรียมในขั้นการพัฒนาโปรแกรม ได้แก่

- Program Run Sheet ซึ่งแสดงถึงรายละเอียดเกี่ยวกับโปรแกรมโดยทั่วไป
- Program Flowchart ซึ่งแสดงรายละเอียดขั้นตอนของคำสั่งในโปรแกรม
- Program Listing

สำหรับเอกสารประกอบระบบงาน ซึ่งจะยกตัวอย่างระบบงานของ Inventory System ง่าย ๆ ในแบบ Online โดยย่อส่วนจากระบบที่ใช้จริง ดูได้จากภาคผนวก ก

10. <u>การควบคุมด้านการพัฒนาโปรแกรม</u>

จุดประสงค์ของการควบคุมด้านการพัฒนาโปรแกรมได้แก่ การควบคุมให้โปรแกรมที่ดำเนินการพัฒนาเป็นไปตาม Program Specification ที่กำหนด ดังนั้น ในขั้นตอนระหว่างการพัฒนาโปรแกรมผู้ดำเนินงานจะต้องติดต่อประสานงานกับ

ผู้ทำหน้าที่พัฒนาโปรแกรมโดยใกล้ชิด และควรมีการทดสอบความถูกต้องของโปรแกรมที่อยู่ระหว่างการพัฒนาเป็นระยะถ้าสามารถกระทำได้ เพื่อสามารถตรวจพบข้อผิดพลาดและดำเนินการแก้ไขได้ทันท่วงที

คอมพิวเตอร์จะทำงานถูกต้องหรือไม่ขึ้นอยู่กับโปรแกรมที่พัฒนา ก่อนที่จะใช้โปรแกรมใดปฏิบัติงานจะต้องมีการทดสอบจนกว่าจะแน่ใจว่าโปรแกรมนั้นสามารถปฏิบัติงานกับรายการ Transaction ทุกประเภทที่อาจเกิดขึ้นได้โดยถูกต้อง

การควบคุมให้มีการทดสอบโปรแกรมอย่างเหมาะสมเป็นช่วงงานที่สำคัญยิ่งในการพัฒนาระบบงาน วิธีการทดสอบความถูกต้องของโปรแกรมซึ่งนิยมใช้กันโดยทั่วไปได้แก่ การใช้ Test Data

<u>การจัดเตรียม Test Data</u>

การจัดเตรียม Test Data คือการสร้างระบบข้อมูลที่จะทำการทดสอบในลักษณะของระบบจำลอง สมมุติรายการ Transaction ทุกประเภทเท่าที่อาจจะเป็นไปได้นำมาทดสอบปฏิบัติข้อมูล และศึกษาผลของการปฏิบัติงานเพื่อพิสูจน์ว่าโปรแกรมที่ทำการทดสอบสามารถปฏิบัติงานได้ถูกต้องหรือไม่

ขั้นตอนของการจัดเตรียม Test Data

(1) ศึกษาระบบงานและ Program Flowchart ที่จะทำการทดสอบเพื่อใช้เป็นพื้นฐานในการจัดเตรียม Test Data

(2) จัดเตรียม Working Paper เพื่อสร้าง File จำลอง, รายการ Transaction แบบต่าง ๆ

(3) สร้างระบบ File จำลอง

(4) ดำเนินการทดสอบโดยทดลองนำรายการ Transaction ที่จัดเตรียมมา Update กับ File จำลอง.

(5) ตรวจสอบผลของการปฏิบัติงาน ซึ่งถ้าพบข้อผิดพลาดจะต้องทำรายการแสดงรายละเอียดข้อผิดพลาดและสาเหตุเพื่อรายงานให้ผู้ทำการพัฒนาโปรแกรมดำเนินการแก้ไข

ตัวอย่างของ Test Data ให้ดูจากภาคผนวก ข.

ข้อแนะนำในการจัดเตรียม Test Data

Test Data ควรมีรายการ Transaction ซึ่งครอบคลุมถึงสภาวะต่อไปนี้

1. Out of Sequence Condition เป็นการทดสอบด้าน Identification comparision routines ในโปรแกรม วิธีทดสอบอาจทำได้ง่ายโดยจัดลำดับ Test Data ให้ไม่เรียงลำดับกันตามเงื่อนไขที่วางไว้ เช่น ในการปฏิบัติข้อมูลแบบ Batch Processing รายการเงินเดือนมักเรียงลำดับรายการปฏิบัติข้อมูลตามหมายเลขประจำตัวพนักงาน ถ้าการเรียงลำดับหมายเลขของ Test Data ไม่เป็นไปตามเงื่อนไข โปรแกรมที่ใช้จะต้องตรวจพบและรายงานความผิดพลาด

2. Out of limit Condition คือ การทดสอบเงื่อนไขที่ตั้งไว้ว่ารายการเปลี่ยนแปลงหรือมูลค่าของรายการใดจะต้องไม่มากกว่าข้อกำหนดที่ตั้งไว้ เช่น ในการปฏิบัติบัญชี บัญชีเงินเดือนมักมีการกำหนดว่าการเปลี่ยนแปลงของอัตราเงินเดือนจะต้องไม่มากเกินร้อยละ 10 ของอัตราเงินเดือนเดิม

3. การเปรียบเทียบทาง Logic ในรายการระหว่าง Master File และ Transaction File ซึ่งผลของการเปรียบเทียบจะกำหนดเส้นทางที่ทำการ.

ปฏิบัติข้อมูล เช่น มีการเปรียบเทียบว่าถ้ารายการใดใน Master File มากกว่า เท่ากับ หรือน้อยกว่ารายการใน Transaction File จะเลือกเส้นทางปฏิบัติข้อมูลต่างกัน

4. ระบบควบคุมการนำมาตราวัดที่ต่างกันมาเปรียบเทียบ เช่น นำรายการที่วัดเป็นปอนด์มาใช้กับรายการที่ควรวัดเป็นกิโลกรัม

5. ข้อมูลที่ไม่สมบูรณ์ ไม่ถูกต้อง หรือขาดหายบางส่วน

6. ระบบป้องกันการใช้ Master File หรือ Transaction File ผิด

7. มีการใช้อักษรใน Data Field ที่ควรเป็นตัวเลข หรือมีการใช้ตัวเลขในที่ควรเป็นตัวอักษร

8. จำนวนตัวอักษรหรือตัวเลขใน Data Field หนึ่ง ๆ มีมากกว่าหรือน้อยกว่าที่กำหนดไว้ หรือที่ควรเป็น

9. Logical Condition โปรแกรมที่ใช้ควรทำหน้าที่ตรวจสอบความเกี่ยวพันทาง Logic ของข้อมูลที่เกี่ยวพันกันโดยสม่ำเสมอ

10. กรณีที่ Transaction Code หรือข้อมูลใน Transaction Data แตกต่างไปจากที่กำหนดไว้

การทดสอบในขั้นสุดท้ายควรจะกระทำกับการปฏิบัติงานจริง ๆ และควรกระทำโดยมิให้ผู้พัฒนาโปรแกรมมีส่วนรวม เพื่อทดสอบว่าสามารถนำโปรแกรมนั้นมาใช้โดยอิสระปราศจากการช่วยเหลือของผู้พัฒนาโปรแกรมหรือไม่

ในกรณีที่เป็นการเปลี่ยนแปลงจากระบบการใช้บุคคลปฏิบัติข้อมูลเป็นระบบปฏิบัติข้อมูล

โดยคอมพิวเตอร์ มักนิยมปฏิบัติข้อมูลโดยใช้ระบบเดิมควบคู่กับระบบคอมพิวเตอร์ซึ่งพัฒนาใหม่ระยะหนึ่งก่อน (Parallel Run) จนกว่าจะแน่ใจว่าระบบคอมพิวเตอร์สามารถปฏิบัติงานโดยถูกต้องจึงยกเลิกระบบเดิม

<u>การทำเอกสารประกอบโปรแกรมที่ใช้</u>

เช่นเดียวกับการควบคุมด้านการวางระบบงาน รายละเอียดทุกขั้นพร้อมทั้งสำเนาเอกสารควรรวบรวมเก็บเป็นแฟ้มเฉพาะโปรแกรมหนึ่ง ๆ (Program Run Book) รายละเอียดของเอกสารประกอบควรรวมถึงนโยบายในการใช้โปรแกรม, ผู้มีสิทธิ์ใช้ รายการทดสอบและรายการเปลี่ยนแปลงแก้ไข และประเภทของข้อมูลที่เกี่ยวข้อง การทำเอกสารประกอบโปรแกรมโดยละเอียดนอกจากจะช่วยให้สามารถตรวจสอบโปรแกรมโดยสะดวกแล้ว ยังเป็นการง่ายที่ผู้อื่นจะรับช่วงงานต่อจากผู้เขียนโปรแกรมคนปัจจุบันถ้าหากมีความจำเป็นต้องมีการเปลี่ยนแปลง

รายละเอียดที่ควรรวบรวมใน Program Run Book ประกอบด้วย

1. จุดประสงค์ของโปรแกรม
2. Flowchart ประกอบโปรแกรม
3. Listing ของโปรแกรม
4. Computer Operating Instruction
5. เอกสารประกอบการทดสอบโปรแกรม
6. ตัวอย่างของรายงานที่ได้จากโปรแกรม

<u>การควบคุมการเปลี่ยนแปลงโปรแกรมที่ใช้</u>

ผลของความเจริญเติบโตขององค์การย่อมทำให้ต้องปรับปรุงที่ใช้ให้เหมาะสมกับสถานะการณ์อยู่เสมอ วางระเบียบปฏิบัติให้รัดกุมเพื่อป้องกันการเปลี่ยนแปลงโปรแกรมเพื่อผลในการทุจริต ดังนั้นจะต้อง

Request For Program Change

To Date

Description of service being requested

Date desired

Requested by	Name	Title	Phone
	Dept.		

Space below for data-processing use only

Program name Program No.

Change approved by Date

Estimated starting date	Documentation	By	Date
Estimated completion date	1. Source corrected		
Assigned to:	2. New program listing		
Released to operations _____ By	3. New program tested		
Department notified _____ By	4. Resulted approved		
Department notified _____ By	5. Flowcharts corrected		
Effective date of change	6. Other manuals changed		
	7. Operating instr. changed		
	8. Old listing destroyed		
	9. Old object destroyed		
	10. Accepted by librarian		

Distribution:
Original to Data Processing
Second copy returned to department by Data Processing
Third copy retained by department for follow-up

แผนภาพที่ 3.2 ตัวอย่างแบบฟอร์มการขอเปลี่ยนแปลงแก้ไขโปรแกรม

1. ต้องเขียนอธิบายความมุ่งหมายในการเปลี่ยนแปลงโดยชัดแจ้ง และต้องได้รับอนุมัติในหลักการจากผู้รับผิดชอบ การเปลี่ยนแปลงหลักต้องได้รับความเห็นชอบจาก System Designer และคณะกรรมการเสียก่อน การเปลี่ยนแปลงย่อยอาจต้องการเพียงความเห็นชอบจากหน่วยงานผู้ใช้ที่เกี่ยวข้องเท่านั้น การเขียนคำอธิบายความมุ่งหมายของการเปลี่ยนแปลงเป็นลายลักษณ์อักษรจะช่วยป้องกันการเข้าใจผิดและเป็นการแสดงถึงประวัติของโปรแกรมด้วย

2. การทำการเปลี่ยนแปลงแก้ไขควรอยู่ในความรับผิดชอบของผู้วิจัยระบบและผู้เขียนโปรแกรมเท่านั้น ผู้มีหน้าที่ทางด้านควบคุมเครื่องไม่ควรเกี่ยวข้องโดยเด็ดขาด การแบ่งแยกเช่นนี้ก็เพื่อป้องกันมิให้ผู้ควบคุมเครื่องรู้รายละเอียดของโปรแกรมใช้การ Intervention การทำงานของเครื่องเพื่อทุจริต อนึ่ง บางแห่งยินยอมให้ผู้ควบคุมเครื่องมีอำนาจในการแก้ไขโปรแกรมเล็ก ๆ น้อย ๆ ได้เอง การอนุญาตเช่นนั้นยากต่อการควบคุมให้อยู่ในขอบเขตและก่อให้เกิดปัญหาในการรักษาเอกสารรายละเอียดให้เป็นปัจจุบัน (Up-to-date)

3. นอกจากจะต้องทำรายละเอียดการเปลี่ยนแปลงแล้ว โปรแกรมที่เปลี่ยนแปลงแก้ไขจะต้องได้รับการทดสอบโดยหน่วยงานอิสระไม่เกี่ยวข้องกับหน่วยงานที่ทำการเปลี่ยนแปลง

4. หลังจากเสร็จสิ้นการเปลี่ยนแปลงและการทดสอบแล้ว จะต้องบันทึกรายการในทะเบียนคุมการเปลี่ยนแปลง และควรจะมีการวางระเบียบโดยเคร่งครัดให้ผู้ควบคุมเครื่อง จะใช้แต่โปรแกรมที่ผ่านขั้นตอนการสร้างและการเปลี่ยนแปลงโดยถูกต้องครบถ้วนเท่านั้น

5. เอกสารที่เกี่ยวกับการเปลี่ยนแปลงทั้งหมดต้องเก็บรักษารวมไว้ในแฟ้ม

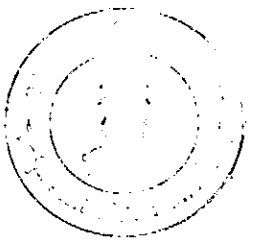
11. <u>การควบคุมด้านการปฏิบัติข้อมูล</u>

การควบคุมด้านการปฏิบัติข้อมูลอาจแบ่งเป็น 3 ส่วนคือ

ก. การควบคุมทางด้าน Input

ข. การควบคุมทางด้าน Processing

ค. การควบคุมทางด้าน Output



ก. <u>การควบคุมทางด้าน Input</u>

โดยปกติ Source Data หรือข้อมูลดิบเบื้องต้นจะเป็นจุดอ่อนของระบบคอมพิวเตอร์ซึ่งควรได้รับการเพ่งเล็งเป็นพิเศษ การทดสอบความถูกต้องของระบบงานหรือโปรแกรมอาจจะกระทำนาน ๆ ครั้ง แต่ปัญหาเกี่ยวกับ Input Data จะต้องได้รับการตรวจสอบอย่างสม่ำเสมอ ไม่ว่าระบบคอมพิวเตอร์หรือโปรแกรมที่วางไว้จะดีเพียงใดก็ตาม ถ้า Input Data ไม่ถูกต้องตั้งแต่แรกแล้วผลลัพธ์ย่อมไม่ถูกต้อง การควบคุมทางด้าน Input Data นี้ ถือเป็นหัวใจสำคัญของระบบคอมพิวเตอร์ จะสังเกตไว้ว่าระบบคอมพิวเตอร์ขององค์การใดจะประสบผลสำเร็จหรือล้มเหลวก็มักมีผลเกี่ยวเนื่องมาจาก Input Data เสียเป็นส่วนใหญ่ มีคำกล่าวว่า "Like humans, computers are what they eat" หรือ "Garbage in, garbage out"

ข้อมูลที่ Input เข้าสู่ระบบคอมพิวเตอร์ ส่วนใหญ่จะผิดพลาดด้วยเหตุ 3 ประการ คือ

1. สูญหาย
2. ได้รับการบันทึกผิดตั้งแต่จุดเริ่มต้น หรือได้รับการถ่ายทอดเป็น Machine Readable Form ผิด
3. ถูกแก้ไขหรือเพิ่มเติมเพื่อผลในทางทุจริต

มีวิธีการหลายอย่างที่ได้ถูกนำมาใช้เพื่อช่วยในการควบคุมความถูกต้องของการ Input วิธีพื้นฐานประกอบด้วย

1. การจัดพิมพ์เลขลำดับล่วงหน้าในเอกสารเบื้องต้นที่จะใช้บันทึกรายการ Input Data จะช่วยให้ทราบว่ามีเอกสารเบื้องต้นรายการใดขาดหายไปบ้างหรือไม่ โดยสามารถตรวจจากการเรียงลำดับของเอกสารที่นำมาเป็น Input ในเอกสารเบื้องต้นบางประเภทนิยมพิมพ์เป็นชุดและเย็บเป็นเล่ม เช่น ใบรับพัสดุ ใบเบิกพัสดุ ซึ่งเมื่อนำไปบันทึกรายการ Transaction จะบันทึกเป็นชุดโดยมีสำเนาตามจำนวนที่กำหนด เมื่อนำส่งรายการรับหรือเบิกพัสดุเพื่อทำการ Input อย่างน้อยควรมีสำเนาเหลือในเล่มทำให้ทราบได้ว่าใบรับพัสดุ ใบเบิกพัสดุแผ่นใดถูกนำไปบันทึกรายการ ผู้ควบคุมสามารถตรวจสอบได้ว่ารายการที่เกิดขึ้นได้ถูกนำไป Input ครบถ้วนหรือไม่ โดยเทียบใบรับพัสดุ ใบเบิกพัสดุที่เป็น Input กับสำเนาในเล่ม นอกจากนั้นอาจมีข้อกำหนดว่าใบรับพัสดุ ใบเบิกพัสดุใบใดถูกยกเลิกจะต้องนำมาเย็บติดในเล่ม เพื่อป้องกันการสับสนและสะดวกในการตรวจสอบ

2. เพื่อลดความผิดพลาดในการบันทึกรายการในเอกสารเบื้องต้น ควรที่จะออกแบบเอกสารเบื้องต้นให้ง่ายต่อการบันทึกรายการ เอกสารเบื้องต้นที่ได้รับการออกแบบมาอย่างดีย่อมช่วยในการทดสอบความถูกต้องเบื้องต้นของข้อมูล เช่น ส่วนที่จะใช้กรอกหมายเลขพัสดุในใบเบิกพัสดุอาจพิมพ์เป็นช่อง ๆ มีจำนวนช่องเท่ากับจำนวนหลักของหมายเลขพัสดุ ถ้ามีการบันทึกหมายเลขพัสดุจำนวนหลักมากหรือน้อยกว่าข้อกำหนดจะทราบข้อผิดพลาดได้ทันที (ดูตัวอย่างของเอกสารเบื้องต้นในภาคผนวก ก ประกอบ)

นอกจากนี้ยังนิยมออกแบบให้เอกสารเบื้องต้นซึ่งใช้บันทึกรายการแต่ละประเภทมีสีต่างกัน เช่น ใบรับพัสดุใช้สีขาว และใบเบิกพัสดุใช้สีแดง เป็นต้น หมายเลขที่กำกับเอกสารเบื้องต้นแต่ละแบบอาจกำหนดให้ตัวเลขนำต่างกันเป็นช่วง เช่น เอกสารที่เป็น

ใบรับพัสดุมีหมายเลขกำกับเริ่มจาก 0001 – 5999 และเอกสารซึ่งเป็นใบเบิกพัสดุมีหมายเลขกำกับตั้งแต่ 6000– 99999 เป็นต้น เพื่อประโยชน์ในการตรวจสอบ Relative Checking ซึ่งจะได้กล่าวถึงต่อไป

การออกแบบเอกสารเบื้องต้นจะต้องคำนึงถึงขั้นตอนในการ Input ข้อมูลด้วย และถ้าใช้วิธี Input ผ่าน Terminal แบบจอภาพ (CRT) ควรจะต้องออกแบบจอภาพให้สัมพันธ์กัน เพื่อป้องกันมิให้สับสนในการ Input ข้อมูลซึ่งโดยมากจะนิยม Input ข้อมูลจากเอกสารเบื้องต้นในลักษณะเดียวกับธรรมชาติการอ่านเริ่มจากด้านซ้ายมือไปสู่ด้านขวามือ และจากบันทัดบนสู่บันทัดล่างถัดไป

อนึ่ง การออกแบบจอภาพซึ่งใช้ในการ Input ข้อมูล ตามปกติจะออกแบบให้ทำการ Display โครงร่างรูปแบบของเอกสารเบื้องต้นเสียก่อน และเว้นช่องไว้สำหรับให้ผู้ใช้ Input รายละเอียดในขณะทำการ Input (ดูตัวอย่างของจอภาพในภาคผนวก ก ประกอบ)

ถึงแม้จะออกแบบเอกสารเบื้องต้นและจอภาพดีเพียงใดก็ตาม แต่ข้อผิดพลาดในการบันทึกรายการย่อมเกิดขึ้นได้เสมอซึ่งมักจะเกิดจากความไม่ระมัดระวังในการบันทึก ดังนั้น โปรแกรมที่ทำหน้าที่รับข้อมูลที่ผู้ใช้ทำการ Input ข้อมูลควรจะต้องได้รับการออกแบบให้สามารถทำการตรวจสอบความถูกต้องเบื้องต้นเท่าที่จะทำได้ ซึ่งเรียกว่า Edit Function แฝงอยู่ในโปรแกรม (ดู Program Flowchart INV TR ENTRY ในภาคผนวก ก ประกอบ)

Edit Function อาจแบ่งเป็นประเภทได้ดังนี้

- <u>Reasonableness, Range & Limit Checking</u> เป็นการตรวจสอบความสมเหตุสมผลและช่วงของข้อมูลเท่าที่สามารถเป็นได้ เช่น ถ้ากำหนดให้ TR Code

มีได้เพียง 4 แบบ ดังนั้น ถ้าทำการ Input ข้อมูลที่เป็น TR Code เกินกว่าตัวเลขที่มีใช่ 1 – 4 แสดงว่ามีข้อผิดพลาดในการ Input ซึ่งโปรแกรมจะต้องตรวจสอบและทำการ Display Error Message ในกรณีที่ทำการ Input ข้อมูลโดยใช้ Terminal เพื่อเตือนให้ผู้ใช้ทำการ Input ทราบข้อผิดพลาดและดำเนินการแก้ไข มิฉะนั้นจะไม่ยอมให้ทำการ Input รายการ Transaction นี้

- Relative Checking เป็นการตรวจสอบความสัมพันธ์ระหว่างข้อมูลที่ทำการ Input เช่น ถ้ากำหนดว่ารายการรับพัสดุหรือรายการยกเลิกรายการรับซึ่งมี TR Code เท่ากับ 1 และ 3 เอกสารใบรับจะต้องมีหมายเลขตั้งแต่ 1 – 5999 และรายการเบิกพัสดุหรือรายการยกเลิกรายการเบิกซึ่งมี TR Code เท่ากับ 2 และ 4 เอกสารใบเบิกจะต้องมีหมายเลขตั้งแต่ 6000 ขึ้นไป ดังนั้น ถ้าทำการ Input รายการ TR Code เป็น 1 แต่ระบุหมายเลขเอกสารเบื้องต้นเกินกว่า 5999 ย่อมแสดงว่ามีข้อผิดพลาดซึ่งโปรแกรมจะตรวจสอบและ Display Error Message

- Sequence Checking เป็นการตรวจสอบการเรียงลำดับของข้อมูลที่ทำการ Input เช่น ในเอกสารใบรับหรือใบเบิกพัสดุมีรายการรับหรือเบิกพัสดุหลายรายการ ในการ Input รายการ Transaction แต่ละรายการ จะต้องระบุหมายเลขรายการในเอกสาร (TLINE) ซึ่งโปรแกรมจะตรวจสอบว่าเรียงตามลำดับหรือไม่ ซึ่งถ้าพบว่าไม่เรียงตามลำดับจะ Display Warning Message

- Calculation Checking เป็นการตรวจสอบความถูกต้องในการคำนวณ เช่น ในการ Input รายการรับพัสดุจากเอกสารเบื้องต้นจนหมดรายการในใบหนึ่ง ๆ ผู้ทำการ Input จะต้อง Key-in มูลค่าของพัสดุที่ได้รับทั้งสิ้นในเอกสารใบนั้นเพื่อทำการตรวจสอบกับรายการมูลค่าสะสมที่คอมพิวเตอร์ทำการคำนวณซึ่งถ้าพบว่าไม่ตรงกัน ย่อมแสดงว่ามีข้อผิดพลาดเกิดขึ้น

- Check Digit ข้อมูลบาง Field เป็นข้อมูลที่มีความสำคัญต่อความถูกต้องของการปฏิบัติข้อมูล เช่น Inventory Number ในระบบ Inventory ซึ่งใช้เป็น Key Field ในการ Update ข้อมูลใน Inventory Master File ถ้าทำการ Input รายการ Transaction โดยระบุ Inventory Number ผิด ความผิดพลาดอย่างร้ายแรงย่อมบังเกิดขึ้น เพราะจะทำให้มีการ Update ผิดบัญชี ดังนั้น ในการออกแบบหมายเลข Key Field จึงนิยมที่จะสร้าง Check Digit แฝงไว้ใน Key Field นั้น เพื่อตรวจจับความผิดพลาดในการ Input ข้อมูล ที่อาจเกิดขึ้น

หลักการของ Check Digit ก็คือกำหนดหลักเกณฑ์ที่แน่นอนในการสร้าง Check Digit. สำหรับข้อมูลที่เป็น Identification แต่ละรายการ และถือ Check Digit ที่สร้างขึ้นเป็นส่วนหนึ่งของข้อมูลนั้น ในภายหลังถ้ามีการ Input ข้อมูล Field นั้นเข้าสู่ระบบคอมพิวเตอร์ โปรแกรมจะทำการสร้าง Check Digit และเปรียบเทียบว่า Check Digit สร้างใหม่ตรงกับ Check Digit ที่แฝงอยู่ในข้อมูลหรือไม่ ซึ่งถ้าตรงกันก็แสดงว่า ข้อมูลที่นำมา Input. ถูกต้อง แต่ถ้าไม่ตรงกันแสดงว่าน่าจะมีข้อผิดพลาดเกิดขึ้น

เทคนิคที่ใช้ในการสร้าง Check Digit. มีหลายวิธี ซึ่งต่อไปนี้จะยกตัวอย่างวิธีง่าย ๆ ที่ใช้กันโดยทั่วไปเพื่อเป็นแนวทาง

ในการ Input ข้อมูลเพื่อสร้าง Inventory Master File (INV CREATE) ข้อมูลที่เป็น Key Field ได้แก่ Inventory Number ซึ่งเป็นตัวเลข 4 หลัก ในโปรแกรมที่ใช้สร้าง Master File จะทำการสร้าง Check Digit สำหรับ Inventory Number ของพัสดุแต่ละรายการโดยวิธีการดังนี้

สมมุติจะทำการสร้าง Check Digit. ของพัสดุหมายเลข 1001 มีขั้นตอนดังนี้

(1) ทำการแยกตัวเลขแต่ละหลักซึ่งประกอบเป็นหมายเลขพัสดุออกเป็นส่วน ๆ — 1 0 0 1

(2) คูณหมายเลขพัสดุแต่ละส่วนจากขวามาซ้ายด้วยเลขที่มีค่าเพิ่มขึ้นเป็นลำดับ โดยตั้งต้นจากเลข 1 — X X X X / 4 3 2 1

(3) บวกผลลัพธ์ที่ได้แต่ละส่วนเข้าด้วยกัน — 4+0+0+1

(4) ถ้าผลลัพธ์ที่ได้เป็นตัวเลขไม่เกิน 1 หลัก ให้นำไปลบจาก 10 แต่ถ้าเกิน 1 หลักให้ตัดเฉพาะหลักแรกนำไปลบจาก 10 ผลลัพธ์ที่ได้คือ Check Digit — =5 / 10-5=5

(5) นำผลลัพธ์ที่ได้มาต่อท้ายหมายเลขพัสดุเดิม — 1 0 0 1 5

สมมุติว่าภายหลังเมื่อทำการ Input รายการ Transaction พนักงานได้ทำการ Input ข้อมูลรายการนี้เป็น 10105 ซึ่งอาจเกิดจากการ Key-in ผิดหรือได้รับการบันทึกในเอกสารเบื้องต้นผิด

โปรแกรม INV TR ENTRY จะทำการตรวจสอบหา CHeck Digit ของ Inventory Number แต่ละรายการที่ได้รับการ Input โดยใช้วิธีการเช่นเดียวกับการสร้าง Check Digit

(1) แยกตัวเลขซึ่งกำหนดให้เป็น Check Digit ออกจากหมายเลขพัสดุ — 1010 ----> 5

(2) ทำการแยกตัวเลขแต่ละหลักซึ่งประกอบเป็นหมายเลขพัสดุออกเป็นส่วน ๆ — 1 0 1 0

(3) คูณหมายเลขพัสดุแต่ละส่วนจากขวามาซ้ายด้วยเลขที่มีค่าเพิ่มขึ้นเป็นลำดับ โดยตั้งต้นจากเลข 1 — X X X X / 4 3 2 1

4+0+2+0

(4) บวกผลลัพธ์ที่ได้แต่ละส่วนเข้าด้วยกัน =6

(5) ถ้าผลลัพธ์ที่ได้เป็นตัวเลขไม่เกิน 1 หลักให้นำไปลบ จาก 10 แต่ถ้าเกิน 1 หลักให้ตัดเฉพาะหลักแรก นำไปลบจาก 10 ผลลัพธ์ที่ได้คือ Check Digit 10-6=4

(6) เปรียบเทียบ Check Digit ที่ระบุใน Inventory Number ที่เป็น Input ซึ่งได้แก่ 5 กับ Check Digit ที่คำนวณได้ใหม่ซึ่งได้แก่ 4 จะเห็นได้ว่า Check Digit ไม่ตรงกัน แสดงว่ามีข้อผิดพลาดในการ Input ข้อมูล โปรแกรมจะสั่งให้คอมพิวเตอร์ Display Error Message เตือนผู้ใช้ที่ทำการ Input

การใช้ Check Digit นิได้หมายความว่าจะสามารถป้องกันความผิดพลาดได้เสมอไป ตัวอย่างเช่น การใช้วิธีการดังได้กล่าวมาแล้ว Inventory Number 1001 และ 5000 จะมี Check Digit เหมือนกัน อย่างไรก็ตามโอกาสที่พนักงานจะไม่ระมัดระวังจนถึงกับป้อนข้อมูลผิดพลาดในแบบแตกต่างกันมากในโอกาสประจวบเหมาะเช่นนี้ย่อมมีน้อยมาก

Flowchart ของโปรแกรม INV TR ENTRY ในภาคผนวก ก ได้แฝง Edit Function ไว้ในโปรแกรมดังนี้

- เมื่อทำการ Input "TR CODE" จะกำหนดในโปรแกรมให้ทำการตรวจสอบ Range ซึ่งจะต้องอยู่ระหว่าง 1 – 4

- เมื่อทำการ Input "DOCUMENT NUMBER" โปรแกรมจะตรวจสอบ Relationship ตามข้อกำหนด ถ้าเป็นรายการรับพัสดุและรายการ Reverse

รายการรับพัสดุ (TR CODE = 1 และ 3 ตามลำดับ) หมายเลขเอกสารเบื้องต้นจะต้องน้อยกว่า 6000 แต่ถ้าเป็นรายการเบิกพัสดุและรายการ Reverse รายการเบิกพัสดุ (TR CODE = 2 และ 4 ตามลำดับ) หมายเลขเอกสารเบื้องต้นจะต้องไม่น้อยกว่า 6000 หากพบว่าความสัมพันธ์ระหว่าง TR Code และ Document Number ไม่เป็นไปตามข้อกำหนด ย่อมชี้ให้เห็นว่ามีข้อผิดพลาดเกิดขึ้น

– ทุกครั้งที่ทำการ Input รายการรับพัสดุ, รายการเบิกพัสดุแต่ละรายการจะต้อง Input หมายเลขรายการ (หมายเลขบันทึกในเอกสารเบื้องต้น) จะกำหนดให้โปรแกรมทำหน้าที่ตรวจสอบว่าเรียงตามลำดับ (Sequence Checking) หรือไม่ ถ้าไม่เรียงตามลำดับอาจแสดงว่ามีการ Input ข้ามรายการ

– เมื่อทำการ Input หมายเลขพัสดุ (INV NO) จะทำการ Check Digit ว่าถูกต้องหรือไม่เพื่อป้องกันการ Update ผิด Record

– ถ้าเป็นรายการเบิกพัสดุ หรือรายการ Reverse รายการรับพัสดุ (TR CODE 2 และ 3 ตามลำดับ) จำนวนในรายการ Transaction จะต้องไม่เกินจำนวนพัสดุคงเหลือใน Record ทั้งนี้เพื่อป้องกันมิให้จำนวนพัสดุคงเหลือติดลบหลังการ Update ซึ่งเป็นการตรวจสอบ Reasonableness

– ถ้าเป็นรายการรับพัสดุ (TR CODE = 1), รายการ Reverse รายการรับพัสดุ (TR CODE = 3) หรือรายการ Reverse รายการเบิก (TR CODE = 4) ซึ่งจะต้อง Input ข้อมูลที่เป็น Cost จะกำหนดในโปรแกรมให้ทำการตรวจสอบ Range ของ TCOST ที่ Input จะต้องต่างจาก Cost เดิมที่บันทึกใน Record ไม่เกิน 20 % ซึ่งถ้าพบว่าต่างมากกว่านั้น จะ Display Warning Message

– ถ้าเป็นรายการรับพัสดุ (TR CODE = 1) จะต้อง Input ยอดรวมจำนวนเงินที่ปรากฏในเอกสารเบื้องต้นซึ่งจะต้องตรงกับที่คอมพิวเตอร์ทำการคำนวณ ถ้าไม่ตรงกันย่อมชี้ให้เห็นว่ามีข้อผิดพลาดซึ่งอาจเกิดจากการ Input ผิดพลาด หรือการเขียนจำนวนเงินในเอกสารเบื้องต้นผิดพลาด

การมี Edit Function ที่ดีแฝงอยู่ในโปรแกรมเท่ากับเป็นการกำหนดให้คอมพิวเตอร์ทำหน้าที่ตรวจสอบความถูกต้องเบื้องต้นของข้อมูลที่ทำการ Input เปรียบเสมือนเป็น Checker นั่นเอง อย่างไรก็ตามมีข้อผิดพลาดอีกเป็นจำนวนมากที่ Edit Function ไม่สามารถตรวจพบเช่น รายการที่ผิดสมเหตุสมผลหรืออยู่ภายในข้อกำหนดที่วางไว้ ดังนั้น เมื่อเสร็จสิ้นการ Input รายการ Transaction ควรที่จะพิมพ์ (List) รายการ Transaction ออกพิมพ์ในรูปของรายงาน (Report) เพื่อนำมาตรวจสอบกับเอกสารเบื้องต้นว่าถูกต้องตรงกันหรือไม่

การทุจริตทางด้าน Input มักเกิดจากการแก้ไขรายการ Input และรายการ Input ปลอมดังกรณีตัวอย่างต่อไปนี้

[1]ในปี ค.ศ. 1972 พนักงาน Data Entry ของ Board of Election, New York ถูกจับในข้อหาเพิ่มรายชื่อผู้ที่ยังไม่มีสิทธิ์ออกเสียงเลือกตั้งหลายร้อยชื่อใน File ของผู้ที่สิทธิ์ออกเสียงเพื่อร่วมมือทุจริตในการเลือกตั้ง

[2]ในปี ค.ศ. 1974 พนักงานศูนย์คอมพิวเตอร์ของ New York Department

---

[1] Thomas Whiteside, Computer Capers, New York: The New American Library, Inc., 1979. p. 50.

[2] Ibid, p. 48.

of Motor Vehicle ได้ถูกจับในข้อหาเพิ่มชื่อของผู้สอบผ่านการขอรับใบขับขี่ File รายชื่อที่เพิ่มส่วนมากเป็นผู้อพยพต่างชาติ ซึ่งไม่ผ่านการทดสอบสายตา, ข้อเขียนและการทดสอบขับขี่ในถนน (Road Test) ผู้กระทำผิดสารภาพว่า ร่วมมือกับโรงเรียนสอนขับรถยนต์ และได้รับค่าจ้างประมาณ $ 200 – 400 ต่อราย ทำให้มีรายได้จากการทุจริตประมาณ $ 300,000

สตรีชราผู้หนึ่งนำเช็ค Tax Refund ของ Internal Revenue Service (IRS) ไปขอเบิกเงินที่ธนาคารแห่งหนึ่งใน Southern California โดยมีหลักฐานการขอรับเงินไปแสดงอย่างครบถ้วน อย่างไรก็ตามพนักงานของธนาคารจำได้ว่าสตรีชราผู้นั้นยังชีพด้วยเงินสวัสดิการประกันสังคม จึงไม่ควรที่จะได้รับ Tax Refund อีก ดังนั้น พนักงานได้รายงานข้อสงสัยไปยังสำนักงาน IRS จากการสอบสวนพบว่าหลานของสตรีชราผู้นั้นซึ่งทำงานในฐานะพนักงาน Data Entry ของสำนักงาน IRS California ได้เพิ่มชื่อของสตรีชราผู้นั้นใน File ผู้มีสิทธิ์ได้รับ Tax Refund และส่งไปพิมพ์เช็คสั่งจ่ายที่ศูนย์คอมพิวเตอร์ของสำนักงานใหญ่ IRS ใน West Virginia

การทุจริตทางด้าน Input ทั้ง 3 รายกระทำโดยเพิ่มข้อมูลใน File โดยไม่มีเอกสารเบื้องต้นสนับสนุน ดังนั้น ถ้ามีการพิมพ์(List) รายการที่ทำการ Input สู่คอมพิวเตอร์นำมาตรวจสอบกับเอกสารเบื้องต้นอย่างรอบคอบแล้ว ย่อมสามารถตรวจพบการทุจริตในกรณีดังกล่าว

บางกรณีการทุจริตทางด้าน Input ได้กระทำอย่างซับซ้อน เช่น ในกรณีตัวอย่าง[2] Stephen Hattner พนักงาน Teller แห่ง Union Dime Saving

---

[1] Ibid, p. . 69–70.

[2] Ibid, p.19–25.

Bank สาขา Park Avenue, New York ยักยอกเงินลูกค้าเงินฝากในระหว่าง ปี ค.ศ. 1970 – 1973 เป็นจำนวนเงิน $ 1.5 ล้าน Stephen Hattner ดำเนินการยักยอกเงินจากบัญชีเงินฝากประจำที่ลูกค้านำมาเปิดบัญชี โดยในครั้งแรกจะ Input ข้อมูลเข้าเครื่องคอมพิวเตอร์ตรงตามจำนวนที่ลูกค้านำฝากเพื่อให้คอมพิวเตอร์พิมพ์รายการในสมุดคู่ฝาก จากนั้นเมื่อลูกค้ากลับไปแล้ว Stephen Hattner จะลงรายการ Reverse รายการฝากนี้และแก้ไขยอดเงินนำฝากให้น้อยลง เช่น ถ้าลูกค้านำเงินมาฝาก $ 10,000 จะยกเลิกรายการฝากนี้โดยทำการ Reverse และ Input รายการใหม่เป็น $ 1,000 ซึ่งทำให้ดูเสมือนการ Input ครั้งแรกเป็นรายการที่ผิดพลาดเนื่องจากพิมพ์ตัวเลขผิดพลาด Stephen Hattner จะบันทึกรายการที่ยักยอกไว้อย่างละเอียด ซึ่งถ้าลูกค้าที่ถูกยักยอกมาถอนเงินก็จะนำเงินที่ยักยอกไว้บางส่วนจ่ายให้แก่ลูกค้า อย่างไรก็ตามรายการถอนเงินมีน้อยมากเนื่องจากลูกค้าที่ถูกยักยอกส่วนใหญ่เป็นคนชราซึ่งฝากเงินบำเหน็จบำนาญเพื่อหวังดอกเบี้ยเลี้ยงชีพ ในวันสิ้นงวดบัญชีซึ่งต้องมีการพิมพ์ใบยืนยันยอดเงินคงเหลือในบัญชีแจ้งไปยังลูกค้า Stephen Hattner อาศัยจุดอ่อนในระบบการพิมพ์ใบยืนยันยอดเงินฝากธนาคารซึ่งกำหนดให้ทำการพิมพ์ใบยืนยันยอดบัญชีเงินฝากออมทรัพย์ต่างวันกับการพิมพ์ใบยืนยันยอดเงินฝากประจำ คือ เงินฝากออมทรัพย์จะถือยอด ณ วันสิ้นงวด และเงินฝากประจำจะถือยอด 2 วันหลังจากวันสิ้นงวด เขาทำการโอนยอดเงินจากบัญชีเงินฝากออมทรัพย์ของลูกค้าบางรายมาเป็นรายการฝากในบัญชีเงินฝากประจำที่ได้ทำการยักยอก เพื่อให้ยอดเงินในใบยืนยันยอดคงเหลือในสมุดคู่ฝาก ซึ่งหลังจากที่พิมพ์ใบยืนยันยอดแล้วเขาจะทำการโอนกลับไปยังบัญชีออมทรัพย์ดังเดิม

หลังจากที่ทำการยักยอกเงินจากลูกค้าในช่วงเวลา 3 ปี เป็นจำนวนเงินมากกว่า $ 1.5 การทุจริตได้ถูกเปิดเผยเนื่องจากเจ้าหน้าที่ตำรวจจับเจ้ามือการพนันจากการค้นตัวเจ้ามือการพนันพบรายชื่อลูกค้ารายใหญ่ซึ่งมีชื่อของ Stephen Hattner

รวมอยู่ด้วย จากรายละเอียดการรับแทงปรากฏว่า Stephen Hattner เป็นผู้ที่เสียพนันมากที่สุด บางวันเสียพนันถึง $ 30,000 ทั้งนี้ทำให้เจ้าหน้าที่ตำรวจสงสัยว่า Stephen Hattner นำเงินจากที่ใดมาเล่นการพนัน จึงทำการสอบสวนและสามารถเปิดเผยการทุจริตครั้งนี้

ต่อมา Stephen Hattner ได้รับคำตัดสินจำคุก 20 เดือนในข้อหายักยอกเงิน $ 1.5 ล้าน แต่จำคุกจริงเพียง 15 เดือนเนื่องจากประพฤติดี

กรณีทุจริตของ Stephen Hattner เกิดขึ้นโดยอาศัยจุดอ่อนในระบบการควบคุมที่ยินยอมให้ผู้มีหน้าที่รับเงินเป็นผู้บันทึกรายการรับเงินเองทุกสิ้นวัน

ในด้านการแบ่งแยกหน้าที่ เมื่อทำการ List รายละเอียด Transaction ประจำวันผู้ควบคุมไม่ได้ให้ความสนใจกับรายการ Reverse รายการรับฝากเงินของพนักงานรายนี้ ซึ่งมีรูปแบบการ Reverse ที่ผิดปกติเกิดขึ้นเป็นประจำ นอกจากนั้นวิธีการพิมพ์ใบยืนยันยอดเงินฝากยังหละหลวมโดยยินยอมให้มีการพิมพ์ใบยืนยันยอดเงินฝากออมทรัพย์และเงินฝากประจำต่างวันกัน เป็นการเปิดโอกาสให้สามารถโอนยอดเงินระหว่างกัน สิ่งที่ต้องระวังเป็นพิเศษก็คือ การแก้ไขยอดคงเหลือใน Record ที่บันทึกในระบบคอมพิวเตอร์สามารถทำได้อย่างรวดเร็วและไม่ทิ้งร่องรอยใด ๆ ไว้ ทั้งนี้ต่างจากระบบการบันทึกข้อมูลในแผ่นบัญชี ซึ่งทำได้ยากกว่าและมีร่องรอย Audit Trail ปรากฏอยู่ง่ายต่อการตรวจสอบความผิดปกติ

บางครั้งผู้บริหารของกิจการเป็นผู้สร้าง Input ปลอมเพื่อใช้เป็นเครื่องมือแสดงฐานะของกิจการให้ดูมั่นคงกว่าข้อเท็จจริง หรือเพื่อหลอกลวงบริษัทอื่นที่เกี่ยวข้อง เช่น กรณีตัวอย่างที่เกิดใน [1] Equity Funding Corporation , New York

---

[1] Ibid, p. 11-18.

ระหว่างปี ค.ศ. 1969 – 1973 Equity Funding Corp. เป็นบริษัทดำเนินกิจการประกันชีวิต เมื่อขายประกันได้จะขายกรมธรรม์บางรายต่อให้บริษัทอื่นรับช่วงในฐานะ Reinsurance ในการขายกรมธรรม์ต่อให้บริษัทอื่น Equity Fund Corp. ได้ค่าธรรมเนียมจากบริษัทที่รับช่วง อย่างไรก็ตามถึงแม้จะขายกรมธรรม์ให้บริษัทรับช่วงไปแล้ว แต่การจ่ายเงินค่าประกันประจำปีลูกค้าที่เอาประกันยังจ่ายต่อ Equity Funding Corp. ซึ่งจะนำส่งผลประโยชน์ที่ได้ให้กับบริษัทรับช่วงอีกต่อหนึ่ง

นับแต่ปี ค.ศ. 1969 Stanley Goldblum ประธานกรรมการของบริษัทฯ สั่งให้พนักงานสร้างกรมธรรม์ปลอม Input สู่ระบบคอมพิวเตอร์โดยใช้รหัสว่ากรมธรรม์จัดเตรียมโดย Department 99 ทั้งนี้เพื่อให้ฐานะของบริษัทเจริญเติบโตกว่าความเป็นจริง ซึ่งมีผลให้หุ้นของบริษัทฯ มีมูลค่าสูงขึ้นในตลาดหลักทรัพย์ และให้ขายกรมธรรม์ปลอมนั้นต่อให้บริษัทรับช่วง ทำให้ได้ค่าธรรมเนียมและผลประโยชน์ตอบแทนอื่น ๆ เป็นเงิน $ 1,175,000 เฉพาะในปี ค.ศ. 1972 กรมธรรม์ปลอมทั้งสิ้นมีมูลค่าทางบัญชีสูงถึง $ 14.5 ล้าน (จากกรมธรรม์ทั้งหมด 97,000 รายการ เป็นกรมธรรม์ปลอม 64,000 รายการ)

ในเดือนมีนาคม ค.ศ. 1973 Raymond Dirk อดีตพนักงานของ Equity Funding Corp. ซึ่งถูกไล่ออก ได้แจ้งการทุจริตที่เกิดขึ้นต่อ New York State Insurance Department และ New York Stock Exchange หลังการสอบสวน ผู้บริหารของ Equity Funding Corp. ได้รับการตัดสินให้จำคุก

ข้อที่น่าสังเกตก็คือ การปิดบังการทุจริตมิให้ผู้ควบคุมจาก New York State State Insurance และผู้สอบบัญชีตรวจพบกระทำโดยเตรียมการตั้งแต่ขั้น Input ข้อมูล ทั้งนี้รายการที่เป็นกรมธรรม์ปลอมจะมีรหัสกำกับว่า "Issued by Department 99" เมื่อผู้ควบคุมจาก New York State Insurance หรือผู้ตรวจสอบบัญชีมาตรวจสอบ

มักกำหนดให้ทำการ List กรมธรรม์ตามเงื่อนไขที่กำหนดเพื่อนำไปสุ่มตรวจสอบกับผู้เอาประกัน โปรแกรม List รายการกรมธรรม์ที่ Equity Funding Corp. จัดเตรียมจะแฝงไว้ด้วยคำสั่งที่ให้ข้ามรายการซึ่ง "Issued by Department 99" ทำให้รายการกรมธรรม์ปลอมไม่มีโอกาสถูก List ออกมาตรวจสอบ

อนึ่ง ในปัจจุบันกิจการต่าง ๆ มีแนวโน้มที่จะใช้ระบบการ Input ข้อมูลในลักษณะกึ่งอัตโนมัติเพื่อความรวดเร็วในการปฏิบัติงาน เช่น การใช้ระบบ MICR (Magnetic Ink Character Reader) โดยการพิมพ์ข้อมูลที่จะ Input เข้าสู่ระบบคอมพิวเตอร์ในลักษณะที่เครื่องอ่าน MICR สามารถอ่านข้อมูลที่พิมพ์อยู่ได้โดยตรง บางครั้งการใช้ระบบ Input ข้อมูลในลักษณะดังกล่าวโดยไม่ทำการตรวจสอบอย่างรอบคอบอาจกลายเป็นช่องทางให้ผู้ทุจริตฉวยโอกาสดำเนินการฉ้อโกงได้ ดังกรณีตัวอย่าง[1] ชายผู้หนึ่งเปิดบัญชีเงินฝากกระแสรายวันกับธนาคารแห่งหนึ่งใน Washington D.C. สหรัฐอเมริกา ทำให้ได้สมุดเช็คและใบนำฝากเงินจำนวนมาก ในใบนำฝากเงินและสมุดเช็คด้านล่างจะมีรหัสตัวเลขซึ่งพิมพ์ในระบบ MICR แสดงหมายเลขบัญชี หลังจากที่ได้ศึกษาระบบรหัสและรูปแบบของใบนำฝากเงินเป็นอย่างดีแล้ว ชายผู้นั้นได้พิมพ์ใบนำฝากเงินปลอมในลักษณะเหมือนกับใบนำฝากเงิน ซึ่งธนาคารเตรียมไว้ที่เคาน์เตอร์สำหรับผู้ที่มีความประสงค์จะฝากเงิน แต่มิได้นำใบนำฝากเงินที่ธนาคารออกให้มา ใบนำฝากเงินในแบบนี้จะไม่มี MICR หมายเลขบัญชีบันทึกไว้ ซึ่งถ้าลูกค้านำฝากโดยใช้ใบนำฝากเงินในลักษณะนี้ พนักงานของธนาคารจะใช้เครื่องพิมพ์ MICR พิมพ์หมายเลขบัญชีเพิ่มให้ในเวลาที่ทำการพิมพ์จำนวนเงินในใบนำฝากและนำใบนำฝากไปเข้าเครื่องอ่าน MICR เพื่อทำการ Update ยอดเงินในบัญชีของลูกค้ารายนั้น

ผู้ทุจริตได้พิมพ์ใบนำฝากเงินปลอมโดยบันทึกหมายเลขบัญชีของผู้ทุจริตในแบบ

---

[1] Ibid, p. 29.

MICR กำกับอยู่ด้วย และแอบนำไปไว้รวมกับใบนำฝากที่ธนาคารเตรียมไว้ให้ลูกค้าที่เคาน์เตอร์ เมื่อลูกค้าที่ต้องการจะฝากเงินแต่ไม่ได้นำใบนำฝากเงินของตนมาก็จะหยิบใบนำฝากเงินปลอมนี้ กรอกจำนวนเงินที่จะนำฝากและส่งให้พนักงานเคาน์เตอร์นับเงินและประทับตราลงนามรับรองพร้อมทั้งคืนสำเนาให้ลูกค้า ใบนำฝากเงินจะถูกส่งต่อให้แก่พนักงานซึ่งจะให้เครื่องพิมพ์ MICR พิมพ์จำนวนเงินและเลขที่บัญชี ถ้าใบนำส่งเงินฝากนี้ไม่มีหมายเลขบัญชีพิมพ์ด้วย MICR ปรากฏอยู่ ปรากฏว่าในขั้นตอนของการพิมพ์จำนวนเงินพนักงานที่พิมพ์ตรวจดูใบนำฝากเงินนั้นมีหมายเลขบัญชีของผู้ทุจริตพิมพ์อยู่แล้ว จึงพิมพ์ MICR เฉพาะจำนวนเงินฝากในใบนำฝาก และส่งเข้าสู่เครื่องอ่าน MICR เพื่อทำการ **Update** ยอดคงเหลือในบัญชีของลูกค้า ดังนั้น ผลที่เกิดขึ้นก็คือจำนวนเงินในใบนำฝากปลอมจะถูกส่งไป Update เพิ่มยอดคงเหลือของผู้ทุจริต ซึ่งผู้ทุจริตได้ถอนเงินทั้งสิ้นในเวลาใกล้ปิดทำการและหลบหนีไป

กรณีเช่นนี้เกิดขึ้นใน New York และ Boston ในช่วงเวลาใกล้เคียงกัน

การทุจริตโดยอาศัยจุดอ่อนของระบบ Input ในแบบอัตโนมัติอีกกรณีหนึ่งเกิดขึ้นกับธนาคารใน New York ชายผู้หนึ่งเปิดบัญชีกระแสรายวันกับธนาคารหลายแห่งในเวลาใกล้เคียงกัน ต่อมาผู้ทุจริตได้ซื้อเครื่องพิมพ์เช็คซึ่งสามารถพิมพ์ MICR เพื่อพิมพ์เช็คปลอมของ Chemical Bank แห่ง New York แต่ในส่วนที่เป็นหมายเลข MICR ซึ่งแสดงว่าเป็นเช็คของธนาคารใด ผู้ทุจริตได้พิมพ์หมายเลขประจำของ Bank of American แห่ง Los Angeles ไว้แทน[1]

ต่อมาผู้ทุจริตได้กรอกจำนวนเงินในเช็คปลอมเหล่านั้นและนำฝากเข้าบัญชีกับธนาคารที่เปิดบัญชีไว้ ซึ่งพนักงานธนาคารที่รับฝากจะลงรายการเป็น Clearing Check

---

1 Ibid, p. 30

ของ Local Area ซึ่งจะถอนเงินได้ในวันทำการถัดไปถ้าเช็คนั้นไม่ถูกคืนจาก Chemical Bank

เช็คปลอมได้ถูกส่งไปยัง Federal Reserve Bank เพื่อทำการ Clearing เครื่องแยกเช็คของ Federal Reserve Bank ซึ่งแยกเช็คโดยการอ่าน MICR ได้แยกเช็คปลอมเพื่อส่งไปเรียกเก็บเงินจาก Bank of America แห่ง Los Angeles ตามหมายเลขธนาคารที่พิมพ์ในระบบ MICR แทนที่จะเป็น Chemical Bank เช็คปลอมได้ถูกส่งไปยัง Los Angeles ซึ่งจะใช้เวลาประมาณ 2 วัน เมื่อเช็คถูกส่งไปถึง Bank of America พนักงานธนาคารได้ตรวจพบว่าเป็นเช็คของ Chemical Bank แห่ง New York ทำให้เข้าใจว่าคงจะเกิดความผิดพลาดในการแยกเช็ค จึงส่งเช็คปลอมกลับไปยัง Federal Reserve Bank ที่ New York ซึ่งใช้เวลาอีก 2 วัน

เนื่องจากเช็คไม่ได้ถูกคืนจาก Chemical Bank ในวันทำการถัดไปนับจากวันนำฝาก ดังนั้น ธนาคารซึ่งผู้ทุจริตนำเช็คฝากเข้าบัญชีจึงถือว่าเช็คนั้นเป็นเช็คที่เรียกเก็บเงินได้ หลังจากผู้ทุจริตเบิกเงินนำฝากตามเช็คปลอมเป็นจำนวนกว่า $ 1 ล้าน แล้วได้หลบหนีไป

ข. การควบคุมทางด้าน Processing

ความมุ่งหมายของการควบคุมในด้านนี้ก็เพื่อให้การปฏิบัติข้อมูลกระทำโดยผู้มีอำนาจหน้าที่และใช้โปรแกรมที่ผ่านการทดสอบความถูกต้องและได้รับการรับรองแล้วเท่านั้น ทั้งนี้เพื่อป้องกันมิให้มีการใช้โปรแกรมที่ถูกสร้างหรือดัดแปลงแก้ไขจากโปรแกรมเดิมทำการปฏิบัติข้อมูลเพื่อผลในทางทุจริต

การทุจริตทางด้านการปฏิบัติข้อมูลเนื่องมาจากโปรแกรมซึ่งมักเกิดขึ้นเสมอได้แก่

1. การทุจริตเกิดขึ้นจากการใช้โปรแกรมที่ผู้ทุจริตจัดทำขึ้นเพื่อลักลอบแก้ไขหรือ List ข้อมูลที่จัดเก็บในระบบ เช่น กรณีที่เกิดขึ้นใน TRW Credit Data of Anaheim, California สหรัฐอเมริกา ซึ่งเป็นบริษัทที่ดำเนินกิจการในด้านรวบรวมข้อมูลเกี่ยวกับฐานะการเงิน (Credit Status) ของประชากรประมาณ 50 ล้านคนในสหรัฐอเมริกา เพื่อให้บริการด้านข่าวสารและข้อมูลประวัติทางด้านสินเชื่อของบุคคลต่าง ๆ แก่ธนาคารและกิจการ Credit Card ซึ่งเป็นสมาชิก โดยเฉพาะอย่างยิ่ง American Express และ Master Change ตอมาคณะลูกขุนแห่ง Los Angeles ได้ฟ้องพนักงานของ TRW Credit Data of Anaheim ข้อหารับแก้ไขประวัติทางด้านสินเชื่อของบุคคลที่มีประวัติไม่เป็นที่น่าพึงพอใจให้กลายเป็นบุคคลที่มีประวัติทางด้านสินเชื่อดี โดยได้รับค่าจ้างประมาณรายละ $ 300 – 1,500 ซึ่งผลจากการแก้ไขประวัติด้านสินเชื่อได้ก่อให้เกิดหนี้สูญในกิจการ Credit Card จำนวนมหาศาล

ในระหว่างปี ค.ศ. 1968 – 1972 พนักงานในศูนย์คอมพิวเตอร์ของ FBI ถูกสอบสวนในข้อหาว่ามีการรับจ้างแก้ไขประวัติอาชญากรรมของบุคคลต่าง ๆ ที่จัดเก็บไว้

2. การทุจริตเกิดขึ้นจากการใช้โปรแกรมที่ผู้ทุจริตสร้างขึ้น หรือดัดแปลงจากโปรแกรมเดิมเพื่อหักเงินจากบัญชีอื่นครั้งละจำนวนน้อย และนำมาเข้าบัญชีของผู้ทุจริต หรือเรียกวิธีการนี้ว่า Salami

ผู้ทุจริตเป็นพนักงานศูนย์คอมพิวเตอร์ของธนาคารได้จัดทำโปรแกรมเพื่อหักเงินจากบัญชีกระแสรายวันของลูกค้าธนาคารเฉพาะรายที่เป็นเอกชนครั้งละไม่เกิน $ 1 มาเข้าบัญชีของผู้ทุจริต โปรแกรมได้รับการออกแบบให้ทำการตรวจเช็คมิให้บัญชีใดถูกหักเงินเกินกว่าปีละ 3 ครั้ง การทุจริตนี้ได้ดำเนินไปเป็นเวลานาน เนื่องจากการหักบัญชีกระทำโดยไม่ทิ้งร่องรอยใด ๆ เลย และลูกค้าที่เป็นเอกชนทั่วไปมักไม่สนใจเงินจำนวนน้อยที่ขาดหายไป เพราะคิดว่าเป็นค่าบริการที่ธนาคารหักจากบัญชี และไม่คุ้มค่า

ที่จะไปธนาคารเพื่อสอบถาม คนส่วนมากมักเชื่อคอมพิวเตอร์ และคิดว่าตนเองคำนวณยอดเงินคงเหลือผิด

พนักงานของโรงงานตัดเย็บเสื้อผ้าที่ New York ได้โปรแกรมให้คอมพิวเตอร์หักภาษี ณ ที่จ่ายออกจากเช็คเงินเดือนของพนักงานทุกคนในบริษัทเกินกว่าปกติ และให้นำเงินที่หักนี้ส่งเป็นภาษีของผู้ทุจริต ซึ่งเมื่อสิ้นปีผู้ทุจริตจะได้รับเงินจาก Internal Revenue Service จำนวนมากในรูปของภาษีคืน (Tax Return)

พนักงานพัฒนาโปรแกรมของบริษัทขายสินค้าทางไปรษณีย์ได้โปรแกรมให้คอมพิวเตอร์หักบัญชีค่านายหน้าของพนักงานขายคนอื่นคนละจำนวนน้อยไปเข้าบัญชีปลอมในชื่อ Zwana (เหตุที่ใช้ชื่อ Zwana เนื่องจากในการปฏิบัติข้อมูลเพื่อคำนวณค่านายหน้าที่พนักงานแต่ละคนจะได้รับในรอบเดือน จะทำเรื่องตามลำดับชื่อซึ่ง Zwana จะเป็นชื่อสุดท้าย) การทุจริตได้ดำเนินไปอย่างราบรื่นเป็นเวลา 3 ปี จนในที่สุดได้ถูกเปิดเผย เนื่องจากบริษัทได้จัดงานเลี้ยงพนักงานขายและจะแจกรางวัลพิเศษแก่พนักงานขายชื่อแรกและชื่อสุดท้ายในบัญชีรายชื่อ ปรากฏว่า Zwana ซึ่งเป็นชื่อสุดท้ายไม่มีตัวตน

3. การทุจริตเกิดขึ้นจากผู้ทุจริตแฝงคำสั่งให้คอมพิวเตอร์ข้ามขั้นตอนในโปรแกรมเพื่อผลในทางทุจริตหรือที่เรียกว่า TROSAN HORSE

พนักงานพัฒนาโปรแกรมแห่ง National City Bank แห่ง Mineapolis สหรัฐอเมริกา ซึ่งได้รับมอบหมายให้พัฒนาโปรแกรมปฏิบัติข้อมูลเงินฝากกระแสรายวัน ได้แฝงคำสั่งประเภท Condition Branch ในโปรแกรมเพื่อให้คอมพิวเตอร์ปฏิบัติงานข้ามขั้นตอนการตรวจเช็คจำนวนคงเหลือในบัญชีถ้าเป็นการเบิกเงินจากบัญชีซึ่งผู้ทุจริตเปิดไว้ ทำให้ผู้ทุจริตสามารถสั่งจ่ายเงินจากบัญชีนั้นในจำนวนเกินกว่ายอดคงเหลือจำนวนเท่าใดก็ได้ การทุจริตได้ถูกเปิดเผยเนื่องจากระบบคอมพิวเตอร์ขัดข้อง จึงต้อง

ทำการ Update ยอดคงเหลือด้วยมือ ทำให้เสมียนธนาคารคนหนึ่งสังเกตพบการทุจริต

การป้องกันการทุจริตทางด้านการปฏิบัติข้อมูลต้องใช้มาตรการหลายด้านประกอบกัน เพื่อป้องกันมิให้ผู้ทุจริตมีโอกาสใช้โปรแกรมที่จัดเตรียมลักลอบทำการปฏิบัติข้อมูลเพื่อผลทางทุจริต จะต้องมีการควบคุมด้านการป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับมอบหมายอย่างเคร่งครัดโดยใช้มาตรการดังได้กล่าวแล้วในตอนต้น โปรแกรมใช้งานจะต้องได้รับการพิมพ์(List)ออกมาตรวจเทียบกับโปรแกรมที่ผ่านการทดสอบความถูกต้องและได้รับการรับรอง เพื่อค้นหาข้อแตกต่างที่ผู้ทุจริตอาจทำการแก้ไขอยู่เสมอ และการตรวจสอบควรจะกระทำในลักษณะไม่แจ้งให้ทราบล่วงหน้า (Surprise Request)

ค. การควบคุมทางด้าน Output

จุดมุ่งหมายของการควบคุมทางด้าน Output ก็เพื่อให้แน่ใจว่าผู้มีหน้าที่เกี่ยวข้องที่ได้รับมอบหมายเท่านั้นที่ได้รับ Output Report ในช่วงเวลาที่เหมาะสม

การทุจริตทางด้าน Output ที่มักเกิดขึ้นอยู่เสมอก็คือ รายงานที่เป็น Output ได้รับการบิดเบือนแก้ไขเพื่อปิดบังการทุจริต หรือทำให้ผู้ใช้รายงานเข้าใจผิดในข้อเท็จจริง รายงานที่เป็น Output ถูกทำลาย หรือถูกนำไปขายแก่บุคคลอื่นที่ต้องการทราบความลับ

มาตรการที่ใช้ในการควบคุมด้าน Output ประกอบด้วย

1. เอกสาร Output ที่มีความสำคัญ เช่น เช็คเงินเดือนที่พิมพ์โดยคอมพิวเตอร์ การพิมพ์หมายเลขลำดับล่วงหน้าและมีทะเบียนคุมหมายเลขซึ่งสามารถตรวจสอบความสัมพันธ์ระหว่างหมายเลขในทะเบียนคุมและหมายเลขเอกสารที่ถูกนำไปพิมพ์เป็น Output อยู่เสมอ

2. ควรมีทะเบียนคุมการจัดพิมพ์รายงานต่าง ๆ ซึ่งศูนย์คอมพิวเตอร์จัดพิมพ์ในทะเบียนควรระบุชื่อรายงาน, จำนวนที่จัดพิมพ์, ชื่อผู้สั่งพิมพ์และผู้รับรายงาน วันและเวลาที่พิมพ์แล้วเสร็จ ชื่อผู้ที่นำส่งรายงานไปยังผู้รับและวันเวลาที่นำรายงานไปส่ง ชื่อผู้รับรายงานและเวลาที่ได้รับ ทั้งนี้ ผู้ทำการควบคุมจะต้องตรวจสอบช่วงเวลาที่ใช้ในการนำส่งรายงานที่พิมพ์แล้วเสร็จว่าใช้เวลาในการนำส่งนานผิดปกติหรือไม่ เพื่อป้องกันการนำรายงานนั้นไปใช้ในทางทุจริต เช่น ทำการ Copy ข้อมูลในรายงานที่เป็นความลับออกสู่ภายนอก

3. รายงานที่เป็นความลับควรมีมาตรการในการจัดเก็บและการทำลายเมื่อหมดความต้องการใช้งานอย่างแน่นอนและควบคุมให้มีการปฏิบัติตามระเบียบที่กำหนดไว้

4. ควรจะสอบถามผู้รับรายงานถึงความถูกต้องของรายงานอยู่เสมอ

ข้อสรุปสำหรับมาตรการที่ใช้ในการควบคุมด้านต่าง ๆ ที่กล่าวมาแล้วก็คือ มาตรการและระเบียบควบคุมต่าง ๆ ที่กำหนดไว้ไม่ว่าจะรัดกุมหรือดีเพียงใดก็ตาม แต่ถ้าไม่มีการบังคับใช้อย่างจริงจัง หรือไม่มีการควบคุมให้ปฏิบัติตามกฎเกณฑ์ที่วางไว้อย่างเคร่งครัดแล้ว กฎเกณฑ์ระเบียบต่าง ๆ จะมีค่าเพียงเศษกระดาษเท่านั้น

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย