ภาคผนวก ก.

กรณีศึกษา : การพัฒนาระบบสำรองที่นั่งของธุรกิจการบิน 'SABRE system'

(อ้างอิง จากบทที่ 4 หัวข้อ 3)

การพัฒนาระบบสำรองที่นั่ง (Computer reservation system) ของสายการบิน American Airlines คือ SABRE system เป็นตัวอย่างของระบบที่มีความก้าวหน้า ผ่านคลื่นของการเปลี่ยนแปลงทั้ง 5 ขั้นตอน ดังที่กล่าวถึงในบทที่ 4 หัวข้อ 3

คลื่น 1 และ 2 : ระบบ SABRE ถูกพัฒนาขึ้นในช่วงกลางทศวรรษ 1960 เพื่อลดต้นทุนค่าใช้จ่ายของขั้นตอนการสำรองที่นั่ง และเพื่อลดทรัพย์สินของกิจการที่ต้องใช้เพื่อดำเนินการในขั้นตอนการสำรองที่นั่ง เพราะระบบผลักดันให้ American Airlines เปลี่ยนจากการทำงานแบบใช้แรงงาน (Manual - based) ไปสู่การใช้งานระบบคอมพิวเตอร์ (Computer - based) เป็นการใช้ระบบสารสนเทศเพื่อลดต้นทุนค่าใช้จ่ายลง

คลื่น 3 : ในกลางทศวรรษ 1970 American Airlines เสนอระบบดังกล่าวให้กับตัวแทนจำหน่าย (Travel agent) เพื่อช่วยให้ตัวแทนจำหน่ายเหล่านั้นสามารถสำรองที่นั่งโดยตรงผ่านเครื่องปลายทาง นอกจากนี้ American Airlines ยังเสริมระบบด้วยการเพิ่มหน้าที่สำคัญของตัวแทนจำหน่าย เช่น การเตรียมกำหนดการเดินทางท่องเที่ยวให้ลูกค้า เข้าไปในระบบด้วย ระบบ SABREทำให้ American Airlines อยู่ในตำแหน่งการแข่งขันเหนือสายการบินอื่น เพราะตัวแทนจำหน่ายพอใจกับระบบดังกล่าว ที่สามารถทำการสำรองที่นั่งได้โดยตรง ทำให้ตัวแทนจำหน่ายไม่หันเหไปใช้ระบบอื่น

คลื่น 4 : ในปลายทศวรรษ 1970 American Airlines ขยายระบบไปสู่การสำรองที่พักและรถเช่า ผ่านพันธมิตรที่เป็นผู้ให้บริการต่างๆ เหล่านี้ การขยายระบบดังกล่าวทำให้ American Airlines เปลี่ยนรูปแบบการดำเนินธุรกิจของตนเอง และส่งผลกระทบกับรูปแบบ ธุรกิจ สายการบินทั้งหมด เพราะเป็นการเปลี่ยนจากธุรกิจการบิน ไปเป็น ธุรกิจเดินทางท่องเที่ยว นอกจากนี้แล้ว American Airlines เพิ่มเติมองค์ประกอบที่ให้ผลในด้านการจัดการเข้าไปในระบบ SABRE โดยระบบสามารถจะปรับราคาที่นั่งได้คล่องตัวมากขึ้น ส่งผลให้ในด้านการจัดการสามารถเพิ่มพูนรายได้เข้าสู่กิจการได้มากขึ้น

CT 489 315

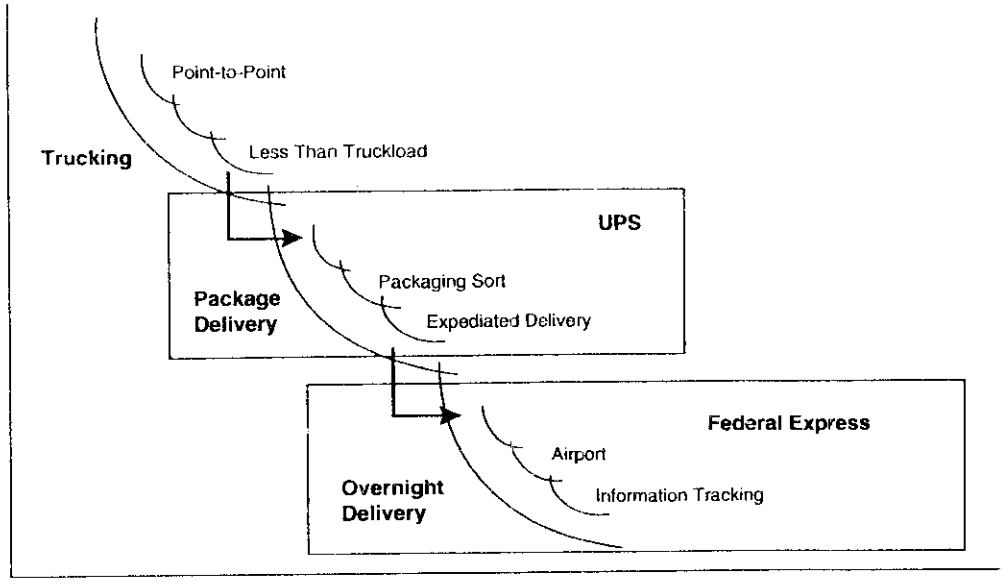
พูนรายได้เข้าสู่กิจการได้มากขึ้น

คลื่น 5 : ในทศวรรษ 1980 American Airlines ขยายระบบไปถึงผู้บริโภคใน 2 ด้านด้วยกัน คือ ด้านที่ 1 นำระบบ EAASY SABRE เข้ามาใช้งาน ระบบดังกล่าวเป็นระบบสำรองที่นั่งที่ผู้บริโภคสามารถทำการสำรองที่นั่งได้โดยตรงจากเครื่องพีซีของตนเอง ไม่ต้องผ่านบริษัทตัวแทนจำหน่าย ด้านที่ 2 American Airlines นำเสนอโปรแกรมสะสมระยะการเดินทาง ที่ชื่อ AAdvantage โปรแกรมนี้ช่วยกระตุ้นผู้ที่เดินทางบ่อยๆ ให้ใช้บริการของ American Airlines สะสมระยะการเดินทางเพื่อให้ได้ตั๋วฟรี นอกจากนี้ยังสร้างพันธมิตรกับบริษัทบัตรเครดิต Citibank ให้ผู้ที่ใช้บัตรเครดิต เพิ่มการสะสมระยะการเดินทางมากขึ้น

การพัฒนาระบบ 'SABRE' เป็นตัวอย่างที่แสดงให้เห็นอย่างชัดเจนว่า ผู้บริหารระดับสูงต้องเข้ามาเกี่ยวข้องเมื่อ 'SABRE' ก้าวเข้าไปสู่คลื่นลูกที่ 3 ซึ่งเป็นขั้นที่เป็นการใช้งานระบบสารสนเทศเพื่อสร้างเม็ดเงินเข้าสู่กิจการ และเมื่อขยายระบบ จนระบบเข้าถึงลูกค้าและผู้บริโภค ขั้นตอนการเปลี่ยนรูปแบบการใช้ประโยชน์ระบบสารสนเทศ ในคลื่น 4 และ 5 จำเป็นต้องขับเคลื่อนโดยผู้บริหารระดับสูงขององค์กร มิใช่เฉพาะแต่ผู้บริหารแผนกสารสนเทศเท่านั้น

ภาคผนวก ข.
กรณีศึกษา : อุตสาหกรรมการขนส่งสินค้า (Shipping industry)
(อ้างอิง จากบทที่ 4 หัวข้อ 4.1.1)

การนำเทคโนโลยีสารสนเทศมาเป็นเครื่องมือในการแข่งขัน ได้ทำให้มีการอธิบายถึงแนวคิดเกี่ยวกับคลื่นของการเปลี่ยนแปลง และ เส้นกราฟประสบการณ์การเรียนรู้ (แต่เดิมเส้นกราฟประสบการณ์การเรียนรู้แสดงให้เห็นว่าต้นทุนการใช้เทคโนโลยีใหม่จะลดลงเมื่อกิจการมีประสบการณ์กับเทคโนโลยีนั้นๆ เพิ่มมากขึ้น) Primozic et al ได้นำเสนอมุมมองใหม่เกี่ยวกับเส้นกราฟประสบการณ์การเรียนรู้ว่า ควรมีลักษณะเป็นกลุ่มของเส้นโค้งที่มีความต่อเนื่อง (set of connected curve) แทนที่จะเป็นเส้นโค้งต่อเนื่องเส้นเดียว (continuous curve) ดังรูป ข.1



รูป ข.1 คลื่นความเปลี่ยนแปลงในอุตสาหกรรมการขนส่ง

จากรูป ข.1 แต่ละเส้นโค้งแสดงถึงเทคโนโลยีที่มีพื้นฐานแตกต่างไปจากเดิมซึ่งอาจเป็นตัวสินค้า และกระบวนการผลิต การเปลี่ยนจากเส้นโค้งหนึ่งไปยังอีกเส้นโค้งหนึ่งจำเป็นต้องใช้การลงทุนเป็นจำนวนมาก แต่ก็จำเป็นต้องตัดสินใจลงทุนเพราะเป็นเทคโนโลยีที่ใช้เพื่อการแข่งขัน

กิจการซึ่งสามารถกำหนดตลาดใหม่ พร้อมกับเทคโนโลยีที่นำไปใช้กับตลาดใหม่ ก็จะเปลี่ยนไปสู่เส้นประสบการณ์เส้นใหม่ อย่างไรก็ตามในบางครั้งผู้บริหารอาจ ยึดติดกับประสบการณ์การเรียนรู้เดิม โดยไม่ได้มองหาเทคโนโลยีใหม่ เพื่อก้าวสู่ตลาดใหม่ ทำให้สูญเสียส่วนแบ่งการตลาดกับคู่แข่งที่ก้าวเข้าไปสู่เส้นประสบการณ์ใหม่

จากรูป ข.1 เป็นตัวอย่างเส้นประสบการณ์การเรียนรู้ในอุตสาหกรรมการขนส่ง ซึ่งเดิมมีการขนส่งสินค้าใน 2 รูปแบบ คือ บรรทุกเต็มพิกัดในจุดหนึ่งไปอีกจุดหนึ่ง กับ บรรทุกไม่เต็มพิกัด (Less than truckloads, LTL)

การขนส่งตามปริมาณภาชนะบรรจุ (Package delivery) เมื่อบริษัท United Parcel Service (UPS) ดำเนินธุรกิจขนส่งในลักษณะบรรทุกไม่เต็มพิกัดแต่เน้นการขนส่งตามปริมาณภาชนะบรรจุ เกิดส่วนแบ่งทางการตลาดใหม่ เป็นเส้นประสบการณ์การเรียนรู้ใหม่ และมีผลให้อุตสาหกรรมการขนส่งเกิดการเปลี่ยนแปลง บริษัท UPS เจริญเติบโตมีขนาดใหญ่กว่าบริษัทขนส่งเดิม เพราะบริษัท UPS สามารถให้บริการกับลูกค้าจำนวนมาก เทคโนโลยีที่ทำให้บริษัท UPS ประสบความสำเร็จ และทำให้เกิดเส้นประสบการณ์การเรียนรู้ใหม่ คือ การจัดเรียงภาชนะบรรจุสินค้าตามศูนย์กระจายสินค้าอย่างมีประสิทธิภาพ เพื่อให้ขนส่งได้ปริมาณมากที่สุดในแต่ละรอบการขนส่ง

การขนส่ง 24 ชั่วโมง (Overnight delivery) การขนส่งตามปริมาณการบรรจุของบริษัท UPS ไม่ได้รับประกันในเรื่องระยะเวลาการขนส่ง และ การติดตามข้อมูลในการขนส่ง บริษัท Federal Express เห็นช่องทางใน 2 ประเด็นนี้ จึงลงทุนกับเทคโนโลยีและก้าวเข้าไปสู่เส้นประสบการณ์การเรียนรู้ใหม่ สร้างลูกค้ากลุ่มใหม่กับการขนส่งข้ามคืน ในทำนองเดียวกันบริษัท Federal Express ได้กลุ่มลูกค้าที่ใหญ่ขึ้นกว่าบริษัท UPS บริษัท UPS และบริษัทอื่นต้องก้าวเข้าสู่การแข่งขันนี้ โดยลงทุนกับเทคโนโลยีที่จะรับประกันการขนส่ง และระบบที่สามารถติดตามสอบถามข้อมูลระหว่างการขนส่ง

บริการการจัดการสินค้าคงคลัง และระบบกระจายสินค้า บริษัท Federal Express ก้าวเข้าสู่เส้นประสบการณ์การเรียนรู้ใหม่ โดยใช้ระบบเครือข่ายการกระจายสินค้า และระบบสารสนเทศ ทำให้สามารถจัดการกับสินค้าคงคลังของลูกค้าซึ่งเป็นกิจการขนาดใหญ่ และรับประกันการขนส่งสินค้าตลอด 24 ชั่วโมง บริษัท Federal Express สามารถให้บริการในด้านสินค้าคงคลังและการกระจายสินค้าให้กับผู้ขายชิ้นส่วน ผู้ผลิต และ ผู้จำหน่ายสินค้าปลีกและส่ง การหาช่องทางการตลาดของการขนส่งสินค้าในรูปแบบต่างๆ ที่เกิดขึ้น มุ่งเน้นไปที่การจัดส่งสินค้าไปยังผู้บริโภคโดยตรง ซึ่งจัดเป็นตลาดที่ใหญ่ที่สุด

ภาคผนวก ค.

กรณีศึกษา : การแข่งขันด้านคุณภาพของบริษัท Federal Express

(อ้างอิง จากบทที่ 4 หัวข้อ 4.1.2)

บริษัท Federal Express เป็นผู้นำในกิจการขนส่งพัสดุภัณฑ์ เริ่มกิจการตั้งแต่ปีค.ศ.1973 มีรายได้ในปี 1990 เป็นเงิน 7.7 พันล้านเหรียญสหรัฐ จากการขนส่งพัสดุภัณฑ์ 1.5 ล้านชิ้นในแต่ละวัน ใช้พนักงาน 91,000 คน รถบรรทุก 31,000 คัน อากาศยาน 430 ลำ การใช้โปรแกรมคุณภาพของบริษัท เริ่มจาก บริษัทประกาศเป้าหมายของกิจการ คือ เป็นกิจการขนส่งสินค้าและพัสดุภัณฑ์ที่ให้การรับประกันระยะเวลาในการขนส่ง ตลอดจนสามารถให้ข้อมูลการขนส่งพัสดุ-ภัณฑ์แต่ละรายการอย่างถูกต้อง วัตถุประสงค์ของกิจการ คือ การสร้างความพอใจในการขนส่งพัสดุภัณฑ์ทุกครั้งกับลูกค้า จากเป้าหมาย และวัตถุประสงค์ดังกล่าว กิจการดำเนินการดังนี้

1. การปรับปรุงคุณภาพขององค์กร

โปรแกรมคุณภาพของกิจการเริ่มในต้นทศวรรษ 1980 เป็นวงจรคุณภาพในส่วนต่างๆ ของกิจการ กลางทศวรรษ 1980 กิจการซื้อโปรแกรมการฝึกอบรม เพื่อช่วยพัฒนา และทำการทดสอบแนวคิดด้านคุณภาพใน 2 ส่วน คือ ศูนย์บริการธุรกิจ และบัญชีผู้ขาย เมื่อ 2 ส่วนประสบผลสำเร็จ ก็ขยายโปรแกรมปรับปรุงคุณภาพไปทั่วทั้งกิจการในปี ค.ศ.1986 โปรแกรมคุณภาพมีหลักสำคัญ 5 ประการ คือ

1.1 โปรแกรมคุณภาพนี้เริ่มจากระดับสูงขององค์กร โดยนำผู้บริหารระดับสูงของกิจการเข้ารับการอบรมแนวคิดพื้นฐานด้านคุณภาพ และการจัดการคุณภาพ การอบรมเน้นที่ความสำคัญของกระบวนการเพื่อบรรลุคุณภาพในการบริการลูกค้า ตลอดจนความจำเป็นในการปรับปรุงกระ-บวนการอย่างต่อเนื่อง ผู้บริหารระดับสูงที่ผ่านการอบรมนี้แล้วจะเป็นผู้ให้การอบรมกับพนักงานระดับรองลงไป และถ่ายทอดการอบรมคุณภาพไปเป็นทอดๆ ใช้เวลาตั้งแต่ปี 1987 จนถึงปี 1989

2. เน้นการติดตามความล้มเหลวมากกว่าจะติดตามเปอร์เซ็นต์ความสำเร็จ การดำเนินงานที่ผ่านมา กิจการวัดคุณภาพจากอัตราเปอร์เซ็นต์ความสำเร็จ เช่น การขนส่งตรงเวลา การออกใบเรียกเก็บเงินอย่างถูกต้อง การแก้ปัญหาให้ลูกค้า ความพอใจของพนักงาน เป็นต้น เมื่อกิจการเริ่มโครงการนำร่องในปี 1985 จึงเริ่มเปลี่ยนเป็นการติดตามดูถึงส่วนที่ขาดหายไป หรือ ส่วนของความล้มเหลว และพบว่า เปอร์เซ็นต์เพียงเล็กน้อยเมื่อเปรียบเทียบกับอัตราความสำเร็จที่สูงถึง

98.5 เปอร์เซ็นต์นั้น ได้ปิดซ่อนจำนวนพัสดุภัณฑ์มากมายที่มีการสูญหาย ใบเรียกเก็บเงินจำนวนมากที่ไม่ถูกต้อง พัสดุภัณฑ์ที่เสียหาย และ คำถามของลูกค้าจำนวนมากที่ไร้คำตอบ เป็นต้น

3. การวัดโดยใช้มุมมองของลูกค้า กิจการแบ่งกลุ่มของความล้มเหลวออกเป็นรายการต่างๆ จากมุมมองของลูกค้า พร้อมคะแนนความรุนแรงแต่ละรายการ ความรุนแรงสูงสุด 10 คะแนน และ 1 คะแนนสำหรับความรุนแรงน้อยที่สุด แต่ละรายการได้แก่

- พัสดุภัณฑ์ไม่ได้รับการขนส่ง 10 คะแนน
- พัสดุภัณฑ์สูญหาย 10 คะแนน
- พัสดุภัณฑ์เสียหาย 10 คะแนน
- การขนส่งผิดวัน 5 คะแนน
- ต้องจัดการซ้ำ 5 คะแนน
- พัสดุภัณฑ์ไม่ระบุที่อยู่ 5 คะแนน
- การขนส่งช้า แต่ตรงวันที่กำหนด 1 คะแนน
- ลูกค้าต้องการให้ปรับปรุงใบกำกับการขาย 1 คะแนน

ความล้มเหลวแต่ละรายการจะถูกบันทึกในแต่ละวัน คูณด้วยน้ำหนักความรุนแรง แล้วรวมค่าทั้งหมดออกมา ตัวเลขดังกล่าวจะรายงานให้พนักงานทั้งหมดทราบในแต่ละอาทิตย์ พนักงานจะให้ความใส่ใจกับรายงานตัวเลข เพราะตัวเลขดังกล่าวจะสัมพันธ์กับค่าตอบแทน, ค่าแรง ของพนักงาน

4. ค่าตอบแทนของพนักงานขึ้นกับการปรับปรุงคุณภาพ ทั้งระดับผู้จัดการและพนักงานจะถูกวัดระดับค่าตอบแทน โดยใช้การปรับปรุงคุณภาพเป็นส่วนหนึ่งของดัชนีที่ใช้วัด รวมกับเป้าหมายที่กำหนดขึ้นในแต่ละไตรมาส ถ้าทำงานถึงเป้าหมายที่กำหนดทุกคนจะได้รับเงินพิเศษ เงินพิเศษนี้จึงเป็นรางวัลสำหรับการทำงานเป็นทีม ไม่ใช่เป็นรางวัลของแต่ละบุคคล ผลของการใช้โปรแกรมการจัดการคุณภาพ พบว่า ในช่วงปี 1988 ถึงปี 1990 ตัวเลขผลรวมความผิดพลาดลดลงถึง 20 เปอร์เซ็นต์ ในขณะที่จำนวนพัสดุภัณฑ์เพิ่มสูงขึ้น 42 เปอร์เซ็นต์

5. เป้าหมายหลัก คือ การค้นหา และแก้ไขสาเหตุที่แท้จริงของความล้มเหลว เหตุผลหลักในการติดตามความล้มเหลวที่เกิดขึ้น เพราะต้องการค้นหาสาเหตุที่แท้จริง ตลอดจนกระบวนการที่ไม่ถูกต้อง ไม่เหมาะสมที่ก่อให้เกิดความล้มเหลว Federal Express ได้ตั้งทีมดูแลคุณภาพเป็นทีมงานที่มาจากบุคลากรหลากหลายหน้าที่ โดยรับผิดชอบการลดจำนวนความล้มเหลวในรายการต่างๆ ที่กำหนดขึ้น ตัวอย่างเช่น ทีมงานที่รับผิดชอบเกี่ยวกับการพิสูจน์ทราบการขนส่งพัสดุ-

ภัณฑ์ ทีมงานนี้นำโดยรองประธานฝ่ายพัฒนาระบบ เพราะฝ่ายระบบสารสนเทศเป็นฝ่ายที่รับผิดชอบในการตรวจสอบลายเซ็นการรับพัสดุภัณฑ์ให้ตรงกับข้อมูลการออกใบเรียกเก็บเงิน จากฐานข้อมูลที่สำนักงานใหญ่ ทีมงานนี้มีจำนวน 10 คน ประกอบไปด้วยบุคลากรที่ได้รับผลกระทบจากความผิดพลาด หรือ ความล้มเหลวที่เกิดขึ้น หรือ เป็นบุคลากรที่สามารถจะเปลี่ยนแปลงเพื่อลดจำนวนตัวเลขความล้มเหลวลง ทีมงานได้แก่ ผู้จัดการสาขา 2 สาขา บุคลากรจากแผนกออกใบกำกับการขาย วิศวกรที่ใช้อุปกรณ์กราดตรวจด้วยแสง และบุคลากรในฝ่ายระบบสารสนเทศ ทีมงานจะพบกันเดือนละ 1 ครั้ง เพื่อตรวจสอบหาสาเหตุหลักของความผิดพลาดในแต่ละเดือน เช่น พนักงานส่งสินค้าไม่ได้ลายเซ็นผู้รับกลับมา ทีมงานมีหน้าที่กำกับให้การฝึกอบรมพนักงานส่งสินค้าย้ำเน้นถึงความสำคัญของกระบวนงานนี้ หรือ ถ้าสถานีใดมีจำนวนความผิดพลาดเกิดขึ้นสูง ทีมงานจะให้ผู้จัดการจากสถานีที่มีประสิทธิภาพดีกว่าเข้าไปช่วยแก้ปัญหา

การจัดการโปรแกรมคุณภาพใช้ทีมงานหลัก 40 คน ซึ่งปฏิบัติการแบบต่อเนื่อง ไม่ได้ทำงานเพื่อแก้ปัญหาใดปัญหาหนึ่งโดยเฉพาะ แต่จะเฝ้าสังเกตกระบวนการอย่างต่อเนื่อง ถ้ามีการเปลี่ยนแปลงคุณภาพอย่างกระทันหันเกิดขึ้น ทีมงานนี้จะทำหน้าที่หาสาเหตุ

บทบาทของระบบสารสนเทศ

ตัวบ่งชี้ที่แสดงถึงความสำคัญของระบบสารสนเทศที่ Federal Express ได้แก่ การที่หัวหน้าฝ่ายเทคโนโลยีสารสนเทศได้รับการเลื่อนตำแหน่งให้สูงขึ้นเป็น Chief Operating Officer และตัวบ่งชี้ที่แสดงให้เห็นว่าฝ่ายบริหารให้ความสนใจกับเทคโนโลยีสารสนเทศ ได้แก่ การกำหนดองค์ประกอบที่สำคัญยิ่งต่อความสำเร็จ (Critical success factors) ซึ่งเกี่ยวข้องกับเทคโนโลยีสารสนเทศ

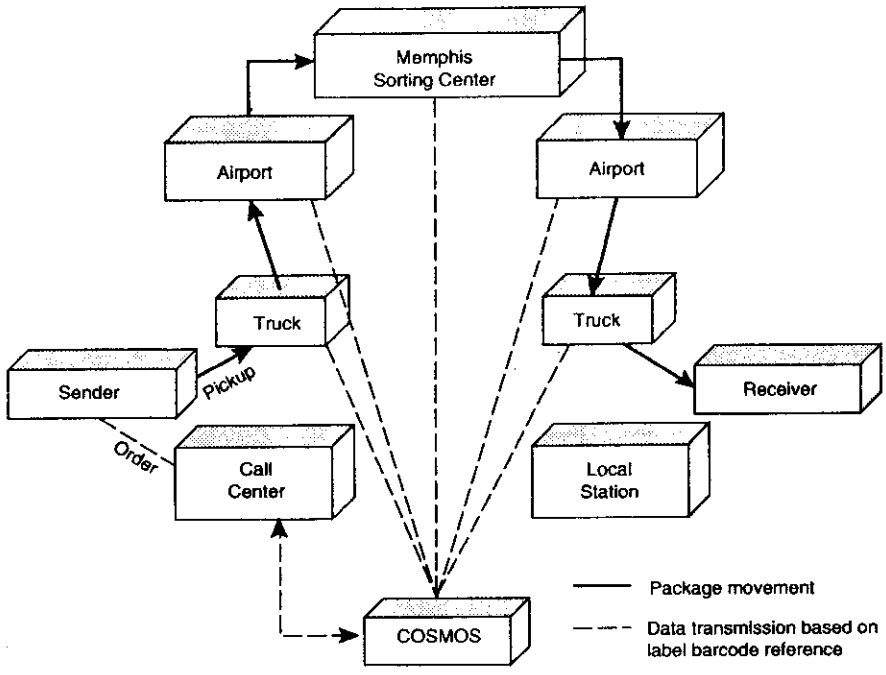
- การปรับปรุงคุณภาพอย่างต่อเนื่อง
- ปรับปรุงคุณค่าของการให้บริการ
- พยายามเข้าใกล้ลูกค้ามากขึ้น
- สร้างผลกำไรจากธุรกิจนานาชาติ
- สร้างการหมุนเวียนกระแสเงินสดให้แข็งแกร่ง

การเข้าไปมีส่วนร่วมหลักในโปรแกรมคุณภาพของฝ่ายเทคโนโลยีสารสนเทศ คือ COSMOS IIB system ซึ่งทำหน้าที่เก็บรวบรวมข้อมูลลำดับความรุนแรงของการปรับปรุงคุณภาพโดยอัตโนมัติ ระบบนี้มิได้ทำหน้าที่หลักเฉพาะระบบเชื่อมตรงในการแจ้งสถานะของพัสดุภัณฑ์

ให้แก่ลูกค้าทราบเท่านั้น แต่จะทำหน้าที่เป็นระบบป้อนกลับสำหรับพนักงาน เพื่อแจ้งให้พนักงานได้ทราบว่าการปรับปรุงคุณภาพการให้บริการลูกค้าเป็นอย่างไร อยู่ในระดับใด

COSMOS IIB system

เมื่อเริ่มก่อตั้งกิจการในปี 1973 Federal Express ก็ติดตั้งระบบคอมพิวเตอร์ ซึ่งได้รับการเพิ่มขีดความสามารถอย่างต่อเนื่องมาตลอด จนกลายเป็นระบบ COSMOS IIB ดังรูป ค.1



รูป ค.1 COSMOS IIB - Federal Express

ระบบได้รับการติดตั้งที่ศูนย์ข้อมูลกลางที่เมือง Memphis ประกอบด้วยเครื่อง IBM 3090s 9 เครื่อง สำหรับจัดการกับ 14 ล้านธุรกรรมในแต่ละวัน ศูนย์ข้อมูลกลางนี้ถูกเชื่อมโดยใช้สถาปัตยกรรมเครือข่ายระบบของ IBM (IBM 's System Network Architecture, SNA) ผ่าน 56 kbps. ไปยังศูนย์ใหญ่ๆ 75 แห่ง และอีก 24 แห่งที่จัดการเกี่ยวกับการรับพัสดุภัณฑ์ของลูกค้า

การใช้ระบบเกิดขึ้นเมื่อ พนักงานของ Federal Express ใช้อุปกรณ์ที่เรียก SuperTracker

เป็นอุปกรณ์แบบมือถือ (Hand - held) สำหรับกราดตรวจ (Scan) รหัสแท่งที่อยู่บนหน้าบรรจุ-ภัณฑ์ การกราดตรวจนี้จะบันทึกวันและเวลาโดยอัตโนมัติ เมื่อพนักงานเก็บ SuperTracker เข้าที่ข้อมูลจะถูกส่งไปที่ศูนย์ข้อมูลส่วนกลาง โดยมีค่าเวลาล่วงผ่าน (Elapsed time) เฉลี่ยระหว่างการกราดตรวจไปจนถึงการบันทึกข้อมูลลงฐานข้อมูล เท่ากับ 4 นาที ดังนั้นทุกครั้งที่พัสดุภัณฑ์มีการเปลี่ยนมือ ไม่ว่าจะเป็นการขนส่งโดยรถขนส่ง หรือ ขนส่งทางอากาศ หรือ เมื่อขนส่งถึงศูนย์กระจายพัสดุภัณฑ์ รหัสแท่งจะถูกกราดตรวจ ซึ่งจะเป็นการปรับข้อมูลสถานะของพัสดุภัณฑ์ให้เป็นปัจจุบัน ดังนั้น ผู้ส่ง หรือ ผู้รับพัสดุภัณฑ์สามารถโทรศัพท์สอบถามสถานะของพัสดุภัณฑ์ได้ตลอดเวลา เมื่อพัสดุภัณฑ์เดินทางถึงที่หมายและมีการเซ็นรับของเรียบร้อย ก็จะมีการบันทึกเวลาและหลักฐานการรับพัสดุภัณฑ์

การปฏิบัติการที่เกิดขึ้นทั้งหมดนี้ ได้รับการสนับสนุนจาก COSMOS IIB system และข้อมูลที่มีการบันทึกไว้จะถูกนำไปวัด ความล้มเหลว หรือ ความผิดพลาดที่เกิดขึ้น ดังนั้นฝ่ายเทคโนโลยีสารสนเทศจึงมีบทบาทสำคัญในโปรแกรมการปรับปรุงคุณภาพ โดยให้ข้อมูลที่ถูกต้องทันต่อเวลากับพนักงาน เพื่อให้สามารถตรวจสอบได้ว่าอะไรที่จำเป็นต้องได้รับการแก้ไขปรับปรุง

ประโยชน์จากโปรแกรมคุณภาพ

Federal Express ตระหนักถึงประโยชน์ที่ได้รับจากโปรแกรมคุณภาพ เพราะโปรแกรมนี้พิสูจน์ให้เห็นถึงความสำคัญเท่าเทียมของคุณภาพ กับ การผลิต เพราะเมื่อกิจการมีตัวเลขของระดับความเสียหายต่ำสุด ก็เป็นช่วงที่ต้นทุนต่อพัสดุภัณฑ์มีค่าต่ำสุดเช่นเดียวกัน นอกจากนี้คุณภาพยังมีผลต่อวัฒนธรรมองค์กรด้วย Federal Express พบว่าโปรแกรมปรับปรุงคุณภาพทำให้เกิดการทำงานเป็นทีม และการทำงานร่วมกัน และคุณภาพกลายเป็นสิ่งที่ทุกคนให้ความใส่ใจตระหนักต่อเรื่องนี้ตลอด ในที่สุดพนักงานเริ่มค่อยๆ รู้สึกมีความรับผิดชอบต่อคุณภาพ ทั้งในสายงานของตนเอง และต่อองค์กรทั้งหมด

ภาคผนวก ง.
ความเป็นส่วนตัว (Privacy)
และการวัดทางชีวภาพ (Biometric measure)
(อ้างอิง จากบทที่ 9 หัวข้อ 2.2.2)

ความเป็นส่วนตัว (Privacy)

ความเป็นส่วนตัวนี้ สามารถถูกพิจารณาในหลายมุมมอง ทั้งในด้านสิทธิตามกฎหมาย หรือสิทธิตามหลักศีลธรรม จริยธรรม ความเป็นส่วนตัวนี้รวมถึง

1. ความเป็นส่วนตัวในร่างกาย ได้แก่ การโยกย้ายถ่ายเท และใช้ประโยชน์จากอวัยวะ เนื้อเยื่อ ของเหลวที่ได้จากร่างกาย โดยปราศจากการยินยอม

2. ความเป็นส่วนตัวในพฤติกรรม ครอบคลุมถึงพฤติกรรมการกระทำทั้งในที่ลับ และที่แจ้ง ตัวอย่างเช่น การลักลอบบันทึกเสียงในห้องน้ำหญิง ซึ่งไม่มีความผิดในทางกฎหมาย

3. ความเป็นส่วนตัวในการติดต่อสื่อสารกับบุคคลอื่นผ่านทางสื่อต่างๆ อย่างเป็นอิสระ โดยไม่ถูกลักลอบ ดักฟัง หรืออยู่ในสายตา หน่วยงาน องค์กร นิติบุคคลใด หรือ ปัจเจกบุคคล เช่น การลักลอบดักฟังโทรศัพท์

4. ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล เช่น ชื่อ ที่อยู่ ข้อมูลสุขภาพ ข้อมูลการเงิน ข้อมูลไบโอเมตริกซ์ ฯลฯ ที่เป็นการบ่งชี้ความเป็นตัวตนของปัจเจกบุคคล ย่อมต้องเป็นสมบัติของบุคคลนั้น ต้องไม่ถูกเผยแพร่ต่อบุคคลอื่น หน่วยงาน หรือ สาธารณชน และบุคคลย่อมมีสิทธิที่จะควบคุมการใช้ประโยชน์ แก้ไข เปลี่ยนแปลงข้อมูลข่าวสารส่วนบุคคลของตนได้

ตัววัดทางชีวภาพ หรือ ไบโอเมตริกซ์ (Biometric) หมายถึงวิธีการ หรือ เทคนิคในการตรวจสอบแยกแยะสิ่งมีชีวิต โดยวัดจากคุณลักษณะของสิ่งมีชีวิตนั้นๆ ในด้านคำจำกัดความไบโอเมตริกซ์ คือ เทคนิคอัตโนมัติต่างๆ ในการตรวจวัดคุณลักษณะทางกายภาพ (Physical Characteristics) พฤติกรรม (Behaviors) ตลอดจนร่องรอยอื่นๆ ในชีวิตประจำวัน (Personal traits) ของบุคคลที่มีชีวิต แล้วนำมาเปรียบเทียบกับคุณลักษณะนั้นๆ ที่ได้มีการบันทึกไว้ก่อนหน้านี้ในฐานข้อมูล เพื่อวัตถุประสงค์ในการแยกแยะ (Recognizing) บุคคลนั้นจากบุคคลอื่น สำหรับไบโอเมตริกซ์นั้น คุณลักษณะต่างๆ ไม่ว่าจะเป็นคุณลักษณะทางกายภาพ ทางพฤติกรรม หรือร่องรอยอื่นๆ ในชีวิตประจำวันของบุคคลต้องสามารถที่จะวัดในเชิงปริมาณได้ คุณลักษณะทาง

กายภาพนั้นส่วนใหญ่จะไม่แปรเปลี่ยนไปตามกาลเวลาในขณะที่คุณลักษณะทางพฤติกรรม หรือร่องรอยในชีวิตประจำวันอาจมีการเปลี่ยนแปลงไปตามกาลเวลา ตามการเรียนรู้ของเจ้าของได้ ดังนั้นไบโอเมตริกซ์ที่ใช้คุณลักษณะทางกายภาพมาเป็นตัววัดจึงได้รับความเชื่อถือมากกว่า ตัวอย่างคุณลักษณะทางกายภาพที่นำมาเป็นตัวบ่งชี้ทางไบโอเมตริกซ์ อย่างแพร่หลาย ได้แก่ ลายนิ้วมือ ม่านตา เส้นเลือดที่ผนังลูกตาดำ รูปพรรณสัณฐานของมือ โครงสร้างรูปหน้า ดังตาราง ง.1

ตาราง ง.1 ไบโอเมตริกซ์เทคโนโลยีที่ได้รับการพัฒนาจนเป็นผลิตภัณฑ์เชิงพานิชย์ นอกจากนี้ยังมีคุณลักษณะทางกายภาพอื่นๆ ที่กำลังศึกษา เช่น ลักษณะรอยย่นของข้อนิ้ว (Knuckle creases) คลื่นสมอง (Acoustic Head Resonance) หรือ กลิ่นตัว (Body Odors) เป็นต้น คุณสมบัติบางประการแปรเปลี่ยนไปตามกาลเวลา เช่น เสียงพูด ลายเซ็น (Hand - written signature) โดยพิจารณาพลวัตการใช้แป้นพิมพ์ (Keystroke dynamics)

ข้อมูลไบโอเมตริกซ์ต้องเก็บบันทึกจาก บุคคลที่ยังมีชีวิตอยู่เท่านั้น โดยระบบจะทำการตรวจเช็คความมีชีวิตของบุคคลด้วย ดังนั้นจึงไม่สามารถนำข้อมูลจากผู้ไม่มีชีวิตแล้วมาใช้งานได้ คุณสมบัติข้อนี้ทำให้เทคโนโลยีไบโอเมตริกซ์แตกต่างไปจากศาสตร์ทางด้านการชันสูตรศพ (Forensic Sciences)

ไบโอเมตริกซ์ถูกนำมาใช้เพื่อ การทำความรู้จัก หรือ แยกแยะตัวบุคคล โดยแบ่งการใช้งานออกมาได้เป็น 2 โอกาส คือ

1. การทวนสอบ เพื่อบ่งชี้ความเป็นตัวจริง (Verification) เป็นการเปรียบเทียบข้อมูลไบโอเมตริกซ์ที่เก็บได้ใหม่ (ณ จุดใช้งาน) กับข้อมูลของบุคคลนั้นที่ได้เคยลงทะเบียนไว้ เพื่อพิสูจน์ว่าบุคคลที่มากล่าวอ้างเป็นตัวจริง

2. การระบุ (Identification) ว่าบุคคลนั้นๆ เป็นใคร เป็นการเปรียบเทียบข้อมูลไบโอเมตริกซ์ที่เก็บใหม่ ณ จุดใช้งานกับข้อมูลไบโอเมตริกซ์ทั้งหมดที่มีอยู่ในฐานข้อมูลเพื่อพิสูจน์ว่าเจ้าของข้อมูล ณ จุดใช้งานเป็นใครในฐานข้อมูล

เทคโนโลยีไบโอเมตริกซ์จะใช้เทคนิคการทำงานแบบอัตโนมัติ ซึ่งมีขั้นตอน ดังนี้

1. เก็บตัวอย่างคุณลักษณะที่ต้องการวัด เช่น สแกนลายนิ้วมือออกมาเป็นภาพถ่ายลายนิ้วมือ

2. เก็บข้อมูลไบโอเมตริกซ์จากตัวอย่างที่สแกนได้ในข้อ 1 เช่น เก็บข้อมูลเชิงปริมาณจากภาพถ่ายลายนิ้วมือด้วยการคำนวณโดยใช้อัลกอริทึมเฉพาะ

3. เปรียบเทียบข้อมูลเชิงปริมาณที่วัดได้จากข้อ 2 กับข้อมูลที่ได้บันทึกไว้ก่อนหน้านี้ ซึ่ง

ไบโอเมตริกซ์	รายละเอียด	ข้อดี	ข้อเสีย
เรตินาสแกน	ภาพสแกนการจัดเรียงของเส้นเลือดดำ (vein pattern) ที่ผนังชั้นในสุดของลูกตา	เรตินาจะมีรูปแบบไม่เปลี่ยนแปลงตลอดชั่วอายุคน จึงทำให้บ่งชี้ตัวบุคคลได้อย่างแม่นยำ	จะต้องแนบลูกตาให้ติดกับอุปกรณ์ (ประมาณ 3 นิ้ว) ทำให้ไม่สะดวกกับการใช้งานในที่สาธารณะ เพราะถือว่าต้องมีการล่วงล้ำทางกายภาพ
ไอริส	เก็บภาพพื้นผิวด้านที่มองเห็นของไอริสโดยใช้กล้องวิดีโอมาตรฐาน	ไม่ต้องล่วงล้ำทางกายภาพเพราะกล้องสามารถสแกนไอรสได้ในระยะห่างประมาณ 2-3 ฟุต	อุปกรณ์มีราคาค่อนข้างแพง อีกทั้งต้องการเนื้อที่ในการเก็บข้อมูลค่อนข้างมาก และเนื่องจากเป็นส่วนที่เกี่ยวข้องกับดวงตาจึงอาจจะไม่ได้รับการยอมรับจากสาธารณะชนเท่าที่ควร
ลายนิ้วมือ	ออปติคอลสแกนลักษณะเส้นลายนิ้วมือ	เป็นที่ยอมรับโดยทั่วไปว่าลายนิ้วมือของคนจะเป็นหนึ่งเดียว และไม่ซ้ำกับลายนิ้วมือของคนอื่นในโลกนี้	ต้องวางนิ้วมือติดกับเครื่องสแกนเนอร์ซึ่งเสี่ยงต่อการติดเชื้อ และร่องรอยลายนิ้วมือที่หลงเหลืออยู่บนเครื่อง หรือรอยมีดบาดอาจสร้างปัญหาได้ ทั้งยังให้ภาพลักษณ์ว่ามีความเกี่ยวข้องกับอาชญากรรม
โครงสร้างของมือและนิ้ว	ออปติคอลสแกนรูปร่างมือและนิ้ว (สามมิติ) ซึ่งจะบันทึกความกว้าง ความยาว และความหนาของมือและนิ้ว	สะดวกต่อการใช้งาน และใช้เนื้อที่ในการเก็บข้อมูลไม่มากนัก	ไม่มีคุณสมบัติที่เป็นหนึ่งเดียว เช่นเดียวกับลายนิ้วมือ หรือเรตินา อีกทั้งบาดแผลบนมือก็สามารถทำให้เป็นอุปสรรคได้เหมือนกัน
ภาพถ่ายใบหน้า	รหัสดิจิทัลที่แปลงจากภาพถ่ายใบหน้า	สะดวกและไม่ต้องมีการล่วงล้ำทางกายภาพ	คนที่หน้าคล้ายกันอาจทำให้อุปกรณ์สับสนได้ และใบหน้าคนก็เปลี่ยนไปตามกาลเวลาด้วย นอกจากนั้นการไว้หนวดเคราก็สามารถที่จะหลอกเครื่องให้เข้าใจผิดได้แล้ว
เสียงพูด	รหัสดิจิทัลที่แปลงจากสัญญาณเสียงพูดแบบอะคูสติก	ใช้งานได้ดีกับเครื่องโทรศัพท์ โดยสามารถตรวจความแตกต่างระหว่างเสียงพูดสดกับเสียงที่อัดเทป หรือการเลียนเสียงพูดได้	เสียงคนอาจเปลี่ยนแปลงได้อีกทั้งเสียงรบกวนรอบข้างก็อาจเป็นอุปสรรคต่อความแม่นยำ และยังต้องใช้เนื้อที่ในการเก็บข้อมูลมาก
พลวัตของลายเซ็น	การเก็บข้อมูลคุณลักษณะต่างๆ ของลายเซ็น ไม่ว่าจะเป็นการจรดปากกา การลากลายเส้น ความเร็ว น้ำหนักและทิศทางของลายเส้น	สะดวกและง่ายต่อการใช้งานเพราะผู้ใช้คุ้นเคยกับการเซ็นชื่ออยู่แล้ว	หากมีการเปลี่ยนแปลงลายเซ็นก็จะต้องให้เครื่องเรียนรู้ใหม่ ทำให้ไม่สามารถประกันความแม่นยำได้ดีเท่าที่ควร

ตาราง ง.1 ไบโอเมตริกซ์เทคโนโลยีที่ได้รับการพัฒนาจนเป็นผลิตภัณฑ์เชิงพาณิชย์

อาจบันทึกไว้ในฐานข้อมูลกลาง หรือบันทึกบนบัตรอัจฉริยะ

4. พิจารณาผลการเปรียบเทียบว่าถูกต้องตรงกันหรือไม่

5. ตัดสินว่าเป็นบุคคลนั้นจริง หรือ บุคคลนี้เป็นใคร

การนำเทคโนโลยีไบโอเมตริกซ์มาใช้กับงานต่างๆ เช่น

1. ควบคุมการผ่านเข้า-ออก อาคารสถานที่ หรือ ควบคุมการผ่านชายแดน โดยใช้เครื่องกราดตรวจ มือ นิ้ว หรือ โครงสร้างรูปหน้า

2. รักษาความปลอดภัยของระบบคอมพิวเตอร์ ใช้การตรวจสอบลายนิ้วมือ ม่านตา โครงสร้างใบหน้า พลวัตการพิมพ์

3. การทำธุรกรรม เช่น ใช้การกราดตรวจม่านตา (Iris scanning) การรู้จำรูปหน้า (Facial recognition) มาใช้กับเครื่องฝากถอนเงินอัตโนมัติ แทนการใช้รหัส

4. จัดการฐานข้อมูลอาชญากรและนักโทษ

5. ควบคุมการลงเวลาทำงาน เช่น ใช้การกราดตรวจมือเพื่อลงเวลาเข้าออกพนักงาน

6. ป้องกันการโกงใช้โทรศัพท์เคลื่อนที่

การนำไบโอเมตริกซ์มาใช้เพื่อบ่งชี้ความเป็นตัวตนที่แท้จริงของบุคคลมากขึ้น ความเสี่ยงในการถูกคุกคามความเป็นส่วนตัวก็มากขึ้นเช่นกัน ไบโอเมตริกซ์จึงมีความเกี่ยวข้องกับความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล เช่น การดำเนินชีวิตประจำวันสามารถถูกตรวจสอบได้ง่ายว่ากระทำกิจกรรมใดบ้างในแต่ละวัน นอกจากนั้นข้อมูลในรูปดิจิทัลสามารถทำซ้ำหรือถ่ายโอนผ่านทางเครือข่ายคอมพิวเตอร์ไปสู่บุคคลอื่น หรือสู่สาธารณชนได้ง่าย และไวต่อความเสียหายมากกว่าข้อมูลรูปแบบอื่น

อย่างไรก็ตามตัววัดทางชีวภาพ ถูกนำมาใช้ประโยชน์ในการระบุตัวบุคคลที่แท้จริงกว้างขวาง เพราะยังเป็นตัววัดที่ลอกเลียนปลอมแปลงได้ยากขึ้น เช่น การเข้าถึงสถานที่หวงห้าม โดยตรวจสอบลายนิ้วมือ การเข้าถึงข้อมูลส่วนบุคคล ข้อมูลสำคัญที่เป็นความลับ ตัววัดทางชีวภาพเมื่อนำมาใช้ร่วมกับเทคโนโลยีอื่น เช่น การใช้บัตรอัจฉริยะและเทคโนโลยีการเข้ารหัสข้อมูล วิธีการนี้ข้อมูลตัววัดทางชีวภาพจะถูกเข้ารหัสและเก็บบันทึกไว้บนบัตรอัจฉริยะ โดยที่ ณ จุดใช้งานการตรวจสอบการระบุตัวตนจะทำโดยการถอดรหัสข้อมูลตัววัดทางชีวภาพที่บันทึกไว้บนบัตรด้วยตัววัดทางชีวภาพที่กราดตรวจใหม่จากตัวบุคคล ถ้าเข้ากันได้ แสดงว่าผ่านขั้นตอนการตรวจสอบความเป็นตัวจริง รูปแบบนี้เป็นตัวอย่างการตรวจสอบความเป็นตัวจริง (Verification) ของบุคคลเท่านั้น ยังไม่สามารถระบุได้ว่าบุคคลนั้นเป็นใคร (Identification) ถ้าต้องการระบุความ

เป็นตัวตนต้องตรวจสอบกับข้อมูลส่วนบุคคลที่บันทึกไว้ล่วงหน้าบนฐานข้อมูลกลาง

ดังนั้นการนำเทคโนโลยีมาใช้งาน จำเป็นต้องมีกฎ และ ระเบียบต่างๆ ในสังคม ที่มีการปรับปรุงแก้ไขให้เหมาะสม สามารถรองรับหลักการกว้างๆ สำหรับการใช้ตัววัดทางชีวภาพได้ ได้แก่

1. การแจ้งให้ทราบล่วงหน้า การจัดเก็บข้อมูลส่วนบุคคลต้องกระทำเปิดเผย แจ้งให้ทราบโดยทั่วกัน มิใช่ลักลอบเก็บ

2. การเข้าถึงข้อมูลตัววัดทางชีวภาพ บุคคลย่อมมีสิทธิที่จะตรวจสอบข้อมูลตัววัดทางชีวภาพของตนที่เก็บอยู่ในฐานข้อมูล และมีสิทธิที่จะรับรู้ว่าข้อมูลนั้นๆ ของตนถูกนำไปใช้งานอย่างไร โดยที่ผู้จัดเก็บข้อมูลตัววัดทางชีวภาพจะต้องเปิดเผยแนวทางการจัดการเกี่ยวกับความเป็นส่วนตัว (Privacy practices) ต่อสาธารณะ

3. การแก้ไขข้อมูลตัววัดทางชีวภาพ บุคคลย่อมมีสิทธิในการแก้ไขปรับปรุงหรือเปลี่ยนแปลงรายการข้อมูลตัววัดทางชีวภาพของตนได้

4. การยินยอม เจ้าของต้องได้รับแจ้งล่วงหน้าเกี่ยวกับการใช้ข้อมูลโดยปกติ และถ้าจะมีการใช้นอกเหนือจากที่มีการแจ้ง จะต้องได้รับการยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลก่อนการใช้งาน

5. ความปลอดภัยและความน่าเชื่อถือ หน่วยงานที่จัดเก็บข้อมูลตัววัดทางชีวภาพ ต้องมีระบบการจัดเก็บฐานข้อมูลที่น่าเชื่อถือ ตลอดจนมีการรักษาความปลอดภัย

สำหรับประเทศไทย ตัววัดทางชีวภาพยังถูกนำมาใช้ค่อนข้างน้อย และมักเป็นไปเฉพาะในภาคราชการเท่านั้น เช่น การเก็บทะเบียนประวัติอาชญากรพร้อมตัวอย่างลายนิ้วมือทั้ง 10 นิ้ว สำหรับภาคเอกชน จะเป็นการนำเทคโนโลยีนี้มาใช้ควบคู่กับเทคโนโลยีอื่น เช่น บัตรอัจฉริยะ และเทคโนโลยีการเข้ารหัสข้อมูล เพื่อใช้กับงานด้านการเงิน การธนาคาร เพราะงานเหล่านี้ต้องการความปลอดภัยของข้อมูลส่วนบุคคล (Security of personal data) และความเป็นส่วนตัวของเจ้าของบัตรค่อนข้างสูง

ในการเก็บทะเบียนประวัติอาชญากร ที่กองทะเบียนประวัติอาชญากร ของสำนักงานตำรวจแห่งชาติ มีระบบตรวจสอบลายนิ้วมืออัตโนมัติ (Automated Fingerprints Identification System, AFIS) ใหญ่เป็นอันดับสองในเอเชีย รองจากประเทศญี่ปุ่น เก็บฐานข้อมูลทะเบียน-ประวัติคนร้ายทั่วประเทศพร้อมตัวอย่างลายนิ้วมือสิบนิ้วมากกว่า 4 ล้านระเบียน (มิถุนายน 2541) ฐานข้อมูลนี้หน่วยราชการอื่นสามารถใช้ในการอ่านข้อมูลได้ (Read only) เช่น สำนักงานคณะ-

กรรมการป้องกันและปราบปรามยาเสพติด กองตรวจคนเข้าเมือง เป็นต้น

โครงการจีเน็ต หรือ Government Information Network เป็นโครงการที่จะสนับสนุนให้หน่วยงานภาครัฐได้มีการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและเอกสารราชการกันทางเครือข่ายคอมพิวเตอร์ เชื่อมโยงข้อมูล ระหว่างหน่วยงานภาครัฐเข้าด้วยกัน โครงการนี้ได้มีการวางมาตรฐานระดับความปลอดภัยของการเข้าถึงข้อมูล ตลอดจนการส่งผ่านข้อมูลที่มีความไวต่อความเสียหายกับระบบราชการ และ/หรือ ความมั่นคงของประเทศ โดยกำหนดให้ใช้บัตรอัจฉริยะควบคู่ไปกับข้อมูลตัววัดทางชีวภาพ จึงเป็นทางเลือกหนึ่งของมาตรการการรักษาความปลอดภัยของข้อมูล มาตรการนี้สร้างความมั่นใจใน ความเป็นตัวจริง (Authentication) ของเอกสาร ที่ส่งโดยผู้มีอำนาจ (Authorized personnel) ในเอกสารที่ผ่านมาทางเครือข่ายอินเทอร์เน็ต และการควบคุมการเข้าถึง (Accessibility) เอกสารที่ต้องการความปลอดภัยค่อนข้างสูง ก็สามารถใช้มาตรการนี้ในการแสดงความเป็นตัวจริง (Identity) ของผู้ที่ต้องการเข้าถึงเอกสาร ว่าเป็นผู้มีสิทธิในการเข้าดู หรือ ทำการแก้ไข

จากพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช 2540 ดังแสดงในหน้า 331 – 333 เป็นกฎหมายไทยฉบับแรกๆ ที่มีการกล่าวถึงการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติฉบับนี้ ข้อมูลข่าวสารส่วนบุคคลซึ่งเก็บรักษาไว้โดยหน่วยราชการถือเป็นส่วนหนึ่งของข้อมูลข่าวสารของราชการ ซึ่งหน่วยงานราชการมิได้เป็นเจ้าของโดยตรง การเปิดเผยดังกล่าวเป็นจุดเริ่มต้น ซึ่งมีหลักการที่ดี แต่ยังขาดความชัดเจนในทางปฏิบัติ ถ้ามีการใช้เทคโนโลยีไบโอเมตริกซ์อย่างกว้างขวางมากขึ้น ก็ต้องมีการปรับปรุงแก้ไขพระราชบัญญัติเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคล ในด้าน

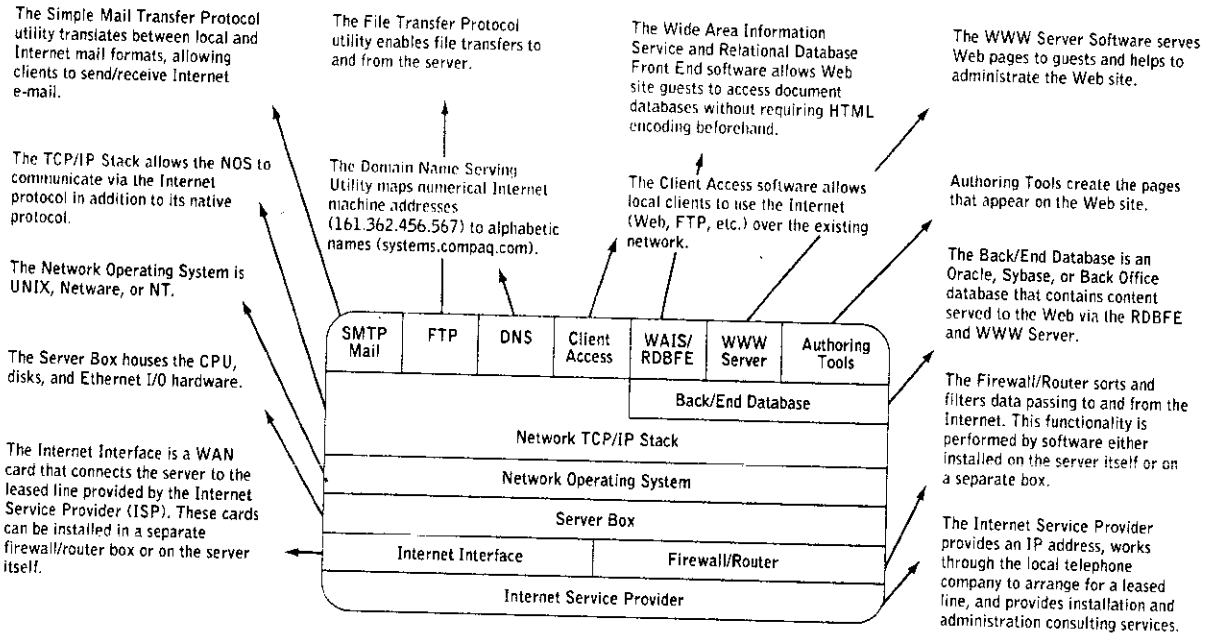
1. ความรับผิดชอบ (Accountability) มีผู้ที่ดูแลการดำเนินการขององค์กรในส่วนที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคล

2. ความเปิดเผย (Openness) ให้สาธารณชนรับทราบเกี่ยวกับการมีฐานข้อมูลข่าวสารส่วนบุคคลไว้ในครอบครอง ประกาศนโยบายที่เกี่ยวข้องกับการจัดการข้อมูล

3. วัตถุประสงค์ (Purposes) ของการเก็บข้อมูลข่าวสารส่วนบุคคล

4. การยินยอม (Consent) เจ้าของข้อมูลต้องรับรู้ และให้การยินยอมในการจัดเก็บ ใช้หรือเปิดเผยข้อมูล

5. ข้อจำกัดในการจัดเก็บ (Collection limitation) เก็บข้อมูลข่าวสารส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ (ไม่เก็บเกินกว่าที่จำเป็น)



รูปที่ จ.3 องค์ประกอบของเครื่องให้บริการอินเทอร์เน็ต

ที่มา : Compaq Computer Corporation

2. การคุกคามต่อระบบเครือข่าย

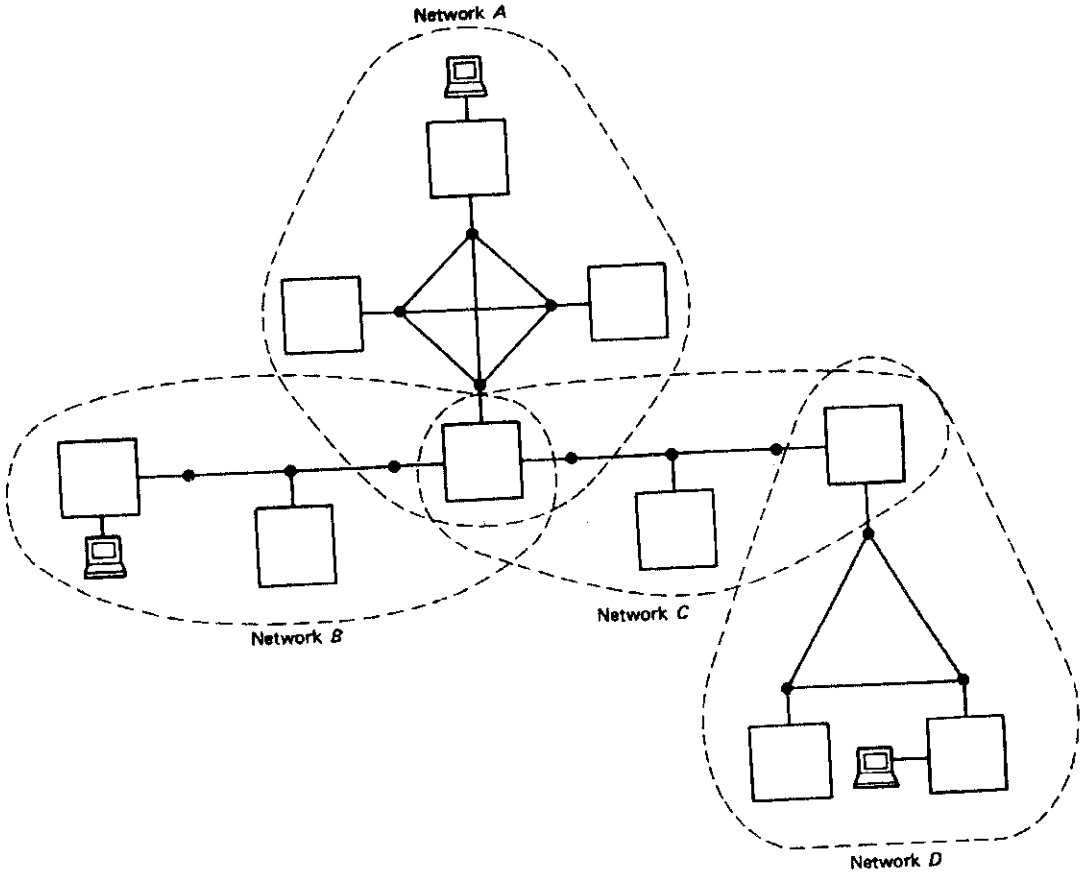
2.1 ประเด็นพิจารณาเกี่ยวกับความมั่นคงในระบบเครือข่าย

ระบบเครือข่ายเผชิญกับปัญหาความมั่นคง ความปลอดภัยมากขึ้น เพราะ

1. การใช้งานร่วม ระบบเครือข่ายเป็นการใช้ทรัพยากร และภาระงานร่วมกัน จากผู้ใช้จำนวนมาก

2. ความซับซ้อนของระบบ ระบบปฏิบัติการที่ใช้ในระบบเครือข่ายมีความซับซ้อนมากกว่าระบบปฏิบัติการในเครื่องเดี่ยว

3. ไม่มีกรอบที่แน่นอน การขยายของเครือข่ายทำให้ขอบเขตของเครือข่ายไม่แน่นอน เครื่องแม่ข่าย 1 เครื่อง อาจเป็นจุดต่อ (Node) บน 2 เครือข่ายที่ต่างกัน ดังนั้น ทรัพยากรของเครือข่ายหนึ่งอาจถูกเข้าถึงโดยผู้ใช้จากอีกเครือข่ายหนึ่ง ดังรูป จ.4



รูป จ.4 ขอบเขตเครือข่ายที่ไม่แน่นอน

4. มีจุดที่ถูกคุกคามได้มากมาย ความไม่มีขอบเขตที่แน่นอนของเครือข่าย เครื่องแม่ข่ายไม่ได้ถูกเข้าถึงเฉพาะจากลูกข่ายในเครือข่ายเดียว ผู้บริหารเครือข่ายไม่สามารถกำหนดการควบคุมไปถึงเครือข่ายอื่นๆ ได้

5. การคุกคามไม่ได้เกิดขึ้น ณ ตำแหน่งใดตำแหน่งหนึ่ง แต่สามารถจะถูกคุกคามจากที่ใดๆ ก็ได้

6. ผู้ใช้เครือข่ายไม่ทราบ และไม่สามารถควบคุมเส้นทางการติดต่อสื่อสารที่เกิดขึ้นได้

2.2 การวิเคราะห์การคุกคามต่อความมั่นคง

ในเครือข่ายนั้น

(1) จุดต่อเฉพาะที่ (Local nodes) เชื่อมต่อผ่าน

(2) สายสื่อสารเฉพาะที่ (Local communications links) ไปยัง

(3) เครือข่ายเฉพาะที่ (Local area network, LAN) ซึ่งมี

(4) ส่วนเก็บข้อมูลเฉพาะที่ (Local data storage),

(5) การประมวลผลเฉพาะที่ (Local processes) และ

(6) อุปกรณ์เฉพาะที่ต่างๆ (Local devices) เครือข่ายเฉพาะที่นี้จะเชื่อมต่อไปยัง

(7) เกตเวย์เครือข่าย (Network gateway) ซึ่งให้การเข้าถึงผ่าน

(8) สายสื่อสารเครือข่าย (Network communications links) ไปยัง

(9) ทรัพยากรควบคุมเครือข่าย (Network control resources)

(10) ตัวจัดเส้นทางเครือข่าย (Network routers) และ

(11) ทรัพยากรเครือข่าย (network resources) เช่น ฐานข้อมูล

การคุกคามต่างๆ ที่เกิดขึ้น คือ

- การขวาง ยึด ข้อมูลในระหว่างเส้นทาง
- การเข้าถึงโปรแกรม หรือข้อมูลที่เครื่องแม่ข่ายระยะไกล
- การปรับเปลี่ยนโปรแกรม หรือข้อมูลที่เครื่องแม่ข่ายระยะไกล
- การปรับเปลี่ยนข้อมูลในระหว่างเส้นทาง
- การปิดกั้นเส้นทางที่ข้อมูลเดินทาง
- การปิดกั้นเส้นทางทุกเส้นทาง

3. การควบคุมความมั่นคงของเครือข่าย

เครื่องมือที่มีประสิทธิภาพที่ช่วยควบคุมความมั่นคง และปลอดภัยของเครือข่าย ได้แก่

3.1 **การเข้ารหัสลับ** (Encryption)

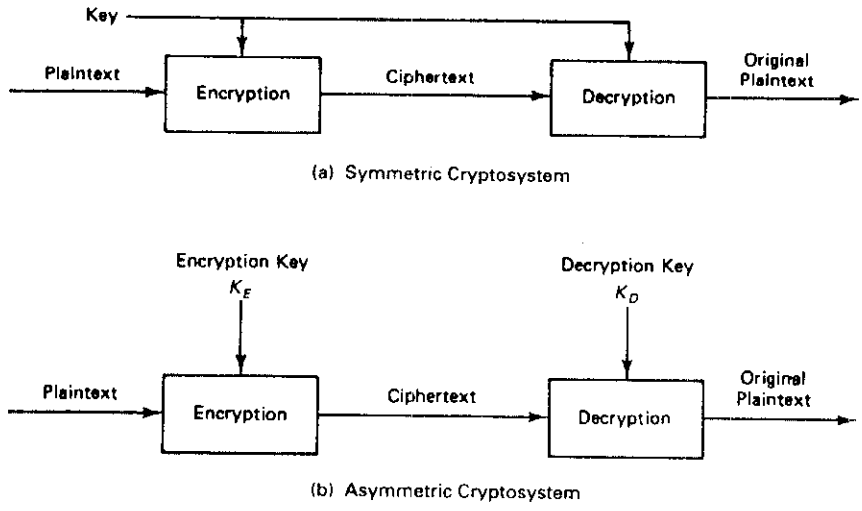
เป็นกระบวนการเข้ารหัสข้อความเพื่อไม่ให้ข้อความดังกล่าวเป็นที่เปิดเผย ส่วนการถอดรหัสลับ (Decryption) เป็นกระบวนการย้อนกลับ เปลี่ยนจากข้อความเข้ารหัสกลับไปเป็นรูปแบบปกติ (โดยมากมักจะใช้คำศัพท์ Encode Decode Encipher และ Decipher แทนคำว่า Encrypt และ Decrypt)

รูปแบบเดิมของข้อความเรียกว่า Plaintext ส่วนรูปแบบของข้อมูลที่เข้ารหัสลับแล้วเรียก Ciphertext ดังรูป จ.5

รูป จ.5 การเข้ารหัสลับ

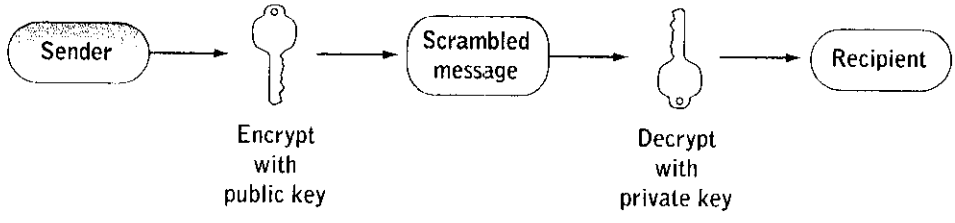
3.1.1 อัลกอริทึมการเข้ารหัสลับ (Encryption Algorithms)

อัลกอริทึมการเข้ารหัสลับรูปแบบหนึ่งคือ การใช้กุญแจ (Key, K) ดังนั้น ข้อความที่เข้ารหัสลับแล้ว จะขึ้นกับข้อความเดิม และค่า K ถ้ากุญแจในการเข้ารหัส และถอดรหัสเหมือนกัน จะเรียกว่า เป็นการเข้ารหัสลับสมมาตร (Symmetric encryption) ดังรูป จ.6 (a) แต่ถ้ากุญแจการเข้ารหัสมาเป็นคู่กับกุญแจการถอดรหัส จะเรียกว่าเป็น การเข้ารหัสลับอสมมาตร (Asymmetric encryption) ดังรูป จ.6 (b)



รูป จ.6 การเข้ารหัสลับโดยใช้กุญแจเข้ารหัส

การเข้ารหัสที่เป็นที่นิยมเรียก 'Public key' encryption หรือการเข้ารหัสโดยใช้กุญแจสาธารณะ ดังแสดงในรูป จ.7



รูป จ.7 Public key encryption

การเข้ารหัสโดยใช้กุญแจสาธารณะ จะใช้กลุ่มของกุญแจสาธารณะ (Public key) และกุญแจส่วนตัว (Private key) ทำการเข้ารหัสข้อมูล ก่อนจะส่ง แล้วจึงถอดรหัสเมื่อข้อมูลไปถึงผู้รับ ผู้ส่งข้อมูลจะระบุกุญแจสาธารณะของผู้รับในสารบบ (Directory) และใช้กุญแจสาธารณะนั้นนำข้อมูลเข้ารหัส ข้อมูลถูกส่งในลักษณะที่เข้ารหัสแล้วเข้าสู่เครือข่าย เมื่อข้อมูลเข้ารหัสมา

ถึงผู้รับ ผู้รับจะใช้กุญแจส่วนตัวเพื่อถอดรหัสข้อมูลแล้วอ่านข้อความนั้นๆ

การเข้ารหัสเป็นประโยชน์อย่างมากในการช่วยปกป้องข้อมูลต่างๆ ในเครือข่ายอินเทอร์-เน็ต และเครือข่ายสาธารณะอื่นๆ เพราะเครือข่ายทั้ง 2 รูปแบบมีความปลอดภัยน้อยกว่าเครือข่ายส่วนตัว การเข้ารหัสช่วยป้องกันการส่งผ่านข้อมูลการชำระเงิน เช่น ข้อมูลบัตรเครดิต เป็นต้น

ข้อความเดียวกันถ้าเปลี่ยนกุญแจเข้ารหัส ก็จะได้การเข้ารหัสลับที่แตกต่างกันออกไป การวิจัยเพื่อศึกษาการเข้ารหัสลับ และการถอดรหัสลับ เรียกว่า Cryptology

รูปแบบหลักในการเข้ารหัสลับ ได้แก่ การแทนค่า (Substitutions) คือ ตัวอักษรแต่ละตัวถูกเปลี่ยนแปลงไปเป็นตัวอักษรอื่น และ การสลับตำแหน่ง (Transpositions) คือ เปลี่ยนแปลงลำดับของตัวอักษร

3.1.2 การถอดรหัสลับ

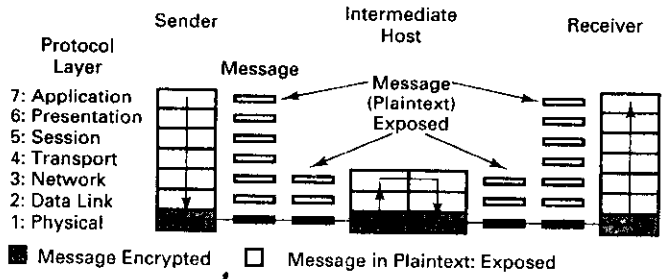
หมายถึงการทำลายการเข้ารหัสลับ เป็นการพยายามหาความหมายของข้อความที่เข้ารหัสลับ หรือ พยายามหาอัลกอริทึมการถอดรหัสที่เข้าคู่กับอัลกอริทึมการเข้ารหัสโดยมีรูปแบบที่แตก-ต่างกัน คือ

- พยายามทำลายข้อความเดี่ยว
- พยายามหารูปแบบของข้อความที่เข้ารหัสลับ เพื่อที่จะสามารถถอดรหัสข้อความต่อๆ ไปโดยใช้อัลกอริทึมการถอดรหัส
- พยายามหาจุดอ่อนในอัลกอริทึมเข้ารหัสลับ

3.1.3 การเข้ารหัสลับสำหรับเครือข่าย

สำหรับระบบเครือข่ายนั้น การเข้ารหัสลับอาจดำเนินการระหว่างแม่ข่ายของเครือข่ายหรือระหว่างงานประยุกต์ และยังต้องคำนึงถึงกุญแจที่ใช้งานด้วย เพราะกุญแจเข้ารหัสจะต้องส่งให้กับทั้งผู้ส่งและผู้รับอย่างปลอดภัย

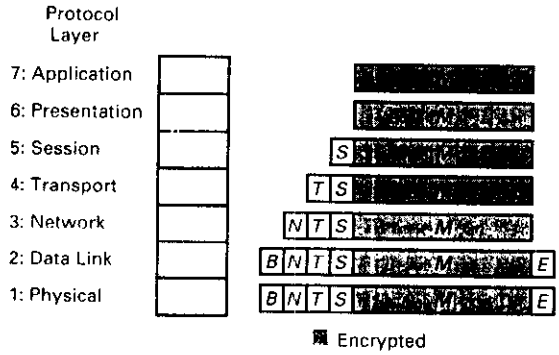
รูปแบบการเข้ารหัสสำหรับเครือข่าย ได้แก่ Link encryption โดยข้อมูลจะถูกเข้ารหัสก่อนที่ระบบจะถูกเชื่อมต่อทางกายภาพ การเข้ารหัสนี้จะเกิดขึ้นในขั้นที่ 1 หรือขั้นที่ 2 ใน OSI model ส่วนการถอดรหัสเกิดขึ้นเมื่อการสื่อสารผ่านไปที่คอมพิวเตอร์เครื่องรับ ดังรูป ข.8



รูป จ.8 Link encryption

การเข้ารหัสนี้ช่วยป้องกันข้อมูลในระหว่างการส่งผ่านระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง แต่ข้อความจะอยู่ในรูปแบบปกติในขณะที่อยู่ที่แม่ข่าย

อีกรูปแบบของการเข้ารหัสสำหรับเครือข่าย คือ End-to-End Encryption เป็นการรักษาความปลอดภัยจากด้านหนึ่งของการส่งผ่านข้อมูลไปจนถึงอีกด้านหนึ่งซึ่งรับข้อมูล การเข้ารหัสนี้สามารถดำเนินการโดยฮาร์ดแวร์ ระหว่างผู้ใช้และแม่ข่าย หรือ ดำเนินการโดยซอฟต์แวร์ที่ทำงานอยู่บนเครื่องแม่ข่าย ซึ่งไม่ว่าในกรณีใดก็ตามการเข้ารหัสจะเกิดในระดับสูงสุดของ OSI model ดังรูป จ.9



รูป จ.9 End-to-End Encryption

เนื่องจากการเข้ารหัสเกิดขึ้นก่อนหน้าการกำหนดเส้นทาง และการส่งผ่านข้อมูล ดังนั้นข้อมูลข้อความจะถูกส่งผ่านในรูปที่ถูกเข้ารหัสแล้วตลอดเครือข่าย รูปแบบนี้จึงครอบคลุมในกรณีที่ถ้าระดับล่างของOSI Model เกิดความผิดพลาด และข้อมูลถูกเปิดเผย แต่ยังจะรักษาความปลอดภัยของข้อมูลได้

CT 489

3.2 **การควบคุมการเข้าถึง** (Access control)

การเข้ารหัสจะถูกใช้เพื่อป้องกันข้อมูลภายในเครือข่าย อย่างไรก็ตาม ยังต้องคำนึงถึงการเข้าถึงข้อมูล โปรแกรม และทรัพยากรอื่นๆ ของเครือข่าย ในระบบเครือข่าย ผู้ใช้ หรือ แม้แต่ผู้บริหารเครือข่ายอาจไม่ทราบว่ามีผู้ใช้ใดบ้างที่เชื่อมต่ออยู่ในเครือข่ายเดียวกัน ดังนั้นในสภาพแวดล้อมของเครือข่าย การควบคุมการเข้าถึง จะต้องป้องกันระบบของเครือข่ายและป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตผ่านจากระบบหนึ่งของเครือข่าย เพื่อเข้าถึงระบบอื่นๆ ของเครือข่าย

3.2.1 การป้องกันช่องทาง (Port protection)

โดยปกติแล้ว ในระบบคอมพิวเตอร์เดี่ยวนั้น การระบุตัวผู้ใช้ก็เป็นสิ่งที่ทำได้ยาก แต่เมื่อผู้ใช้สามารถต่อเข้าระบบโดยการโทรศัพท์นั้น ยิ่งทำให้การระบุตัวผู้ใช้ยากขึ้นอีกมาก การเข้าถึงช่องทางโดยการต่อโทรศัพท์ จึงเป็นจุดที่ไม่มั่นคงจุดใหญ่ของระบบเครือข่าย จึงจำเป็นต้องมีการป้องกันช่องทาง และใช้เทคนิคนี้ร่วมกับเทคนิคฮาร์ดแวร์ และเทคนิคการบริหารหลายรูปแบบ

1. การเรียกกลับอัตโนมัติ (Automatic call-back) ในระบบเรียกกลับอัตโนมัติ เมื่อผู้ใช้ที่ได้รับอนุญาตต่อโทรศัพท์เข้าสู่ระบบคอมพิวเตอร์ หลังจากที่ระบุตัวผู้ใช้เองแล้ว ระบบคอมพิวเตอร์ จะตรวจสอบหมายเลขโทรศัพท์จากรายการเลขหมายที่มีอยู่ แล้วเรียกกลับไปตามหมายเลขที่ระบุไว้ ซึ่งถ้าผู้ใช้มีหลายเครื่องในหลายสถานที่ จะต้องแจ้งหมายเลขทั้งหมดไว้กับระบบ เมื่อต้องการต่อเข้าระบบจากเครื่องใด ก็แจ้งหมายเลขนั้นไป ถ้าระบบตรวจสอบหมายเลขแล้วไม่ตรงกับในรายการที่ระบุไว้ ระบบจะเตือนไปที่เจ้าหน้าที่รักษาความปลอดภัยของระบบ

2. สร้างสิทธิการเข้าถึงที่แตกต่างกัน (Differentiated access rights) ข้อมูลที่สำคัญสามารถได้รับการปกป้องโดยจำกัดตำแหน่งในการเข้าถึง โดยการเข้าถึงข้อมูลสำคัญจะต้องเข้าถึงจากสถานที่ที่ปลอดภัยเท่านั้น เช่น พนักงานขายสามารถโทรศัพท์และป้อนข้อมูลการขายเข้าสำนักงาน แต่ข้อมูลสำคัญ เช่น การพยากรณ์ยอดขาย หรือ โครงสร้างราคา ข้อมูลเหล่านี้จะเข้าถึงได้จากเฉพาะภายในสำนักงานเท่านั้น

3.3 **การระบุตัวตน** (Authentication)

หมายถึงความสามารถของแต่ละฝ่ายที่ทำธุรกรรมต่อกัน สามารถระบุอัตลักษณ์ (Identity) ของอีกฝ่ายหนึ่งได้ ธุรกรรมที่เกิดขึ้นในสมัยก่อนจะใช้ลายเซ็นเพื่อระบุตัวตน แต่ธุรกรรมปัจจุบันหลีกเลี่ยงการใช้ลายเซ็น เช่น ธนาคารอิเล็กโทรนิกส์ จะใช้เครือข่ายส่วนตัวที่มีการปกป้องเป็นอย่างดี สามารถบันทึกและพิสูจน์การจ่ายเงินของผู้จ่ายได้

พระราชบัญญัติ

ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

.....

หมวด ๓

ข้อมูลข่าวสารส่วนบุคคล

มาตรา ๒๑ เพื่อประโยชน์แห่งหมวดนี้ "บุคคล" หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทย

มาตรา ๒๒ สำนักข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานของรัฐแห่งอื่นตามที่กำหนดในกฎกระทรวงอาจออกระเบียบ โดยความเห็นชอบของคณะกรรมการกำหนดหลักเกณฑ์ วิธีการและเงื่อนไขที่มิให้นำบทบัญญัติวรรคหนึ่ง (๓) ของมาตรา ๒๓ มาใช้บังคับกับข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานดังกล่าวก็ได้

หน่วยงานของรัฐแห่งอื่นที่จะกำหนดในกฎกระทรวงตามวรรคหนึ่งนั้น ต้องเป็นหน่วยงานของรัฐซึ่งการเปิดเผยประเภทข้อมูล ข่าวสารส่วนบุคคลตามมาตรา ๒๓ วรรคหนึ่ง (๓) จะเป็นอุปสรรคร้ายแรงต่อการดำเนินการของหน่วยงานดังกล่าว

มาตรา ๒๓ หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

(๑) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงาน ของหน่วยงานของรัฐให้สำเร็จ ตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(๒) พยายามเก็บข้อมูลข่าวสาร โดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของ บุคคลนั้น

(๓) จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(๔) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(๕) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสาร โดยตรงจากเจ้าของข้อมูลหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณี

ที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจ หรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคล ทั่วไปทราบ ข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ

มาตรา ๒๔ หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่น หรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผย ดังต่อไปนี้

(๑) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(๒) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(๓) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคล ไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(๔) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(๕) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา ๒๖ วรรคหนึ่ง เพื่อการตรวจดูคุณค่าใน การเก็บรักษา

(๖) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็น คดีประเภทใดก็ตาม

(๗) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(๘) ต่อศาลและเจ้าหน้าที่ของรัฐหนือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(๙) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (๓) (๔) (๕) (๖) (๗) (๘) และ (๙) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้ กับข้อมูลข่าวสารนั้นตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

มาตรา ๒๕ ภายใต้บังคับมาตรา ๑๔ และมาตรา ๑๕ บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้น หรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา ๙ วรรคสอง และวรรคสาม มาใช้บังคับ โดยอนุโลม การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้น มอบหมายก็ได้ ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า ในกรณีที่หน่วยงาน

ของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวัน นับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ ต่อคณะกรรมการและไม่ว่ากรณีใดๆ ให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา ๒๓ มาตรา ๒๔ และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถหรือเจ้าของข้อมูลที่ถึงแก่กรรมแล้วได้

6. ข้อจำกัดการใช้งาน การเปิดเผย และการเก็บไว้ในครอบครอง (Use, Disclosure, Retention Limitation) ไม่ใช้ข้อมูลเกินวัตถุประสงค์ที่แจ้งไว้ในตอนแรกตามความยินยอมของเจ้าของข้อมูล และไม่เก็บรักษาข้อมูลไว้นานเกินความจำเป็น

7. การรักษาความปลอดภัย (Safeguards) มีการรักษาความปลอดภัยที่เหมาะสมกับความเสี่ยงต่อการสูญเสีย การเข้าถึง การทำลาย การใช้ การแก้ไขดัดแปลง หรือ เปิดเผยข้อมูลโดยมิชอบ ต้องมีสถานที่ บุคลากร งบประมาณ พอเพียงต่อการประกันความปลอดภัย

8. คุณภาพของข้อมูล (Data quality) ข้อมูลส่วนบุคคลต้องมีความถูกต้อง ครบถ้วน และทันสมัย กับการใช้งานตามวัตถุประสงค์

9. การมีส่วนร่วมของเจ้าของข้อมูล (Individual participation) เจ้าของข้อมูลมีสิทธิเรียกดูรายละเอียดการใช้งาน หรือการเปิดเผยข้อมูลของตน สามารถตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูล รวมทั้งขอแก้ไขได้ตามความเหมาะสม

CT 489 333

ภาคผนวก จ.
ความมั่นคงและความปลอดภัยในระบบเครือข่าย

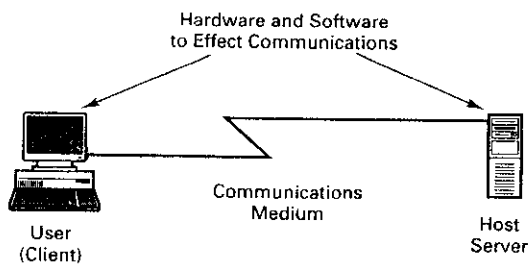
1. **แนวคิดพื้นฐานของระบบเครือข่าย**
2. **การคุกคามต่อระบบเครือข่าย**
   2.1 ประเด็นพิจารณาเกี่ยวกับความมั่นคงในระบบเครือข่าย
   2.2 การวิเคราะห์การคุกคามความมั่นคง
3. **การคุกคามความมั่นคงของเครือข่าย**
   3.1 การเข้ารหัสลับ (Encryption)
   3.2 การควบคุมการเข้าถึง (Access control)
   3.3 การระบุตัวตน (Authentication)
   3.4 บูรณภาพของข้อมูล (Message integrity)
4. **Firewall**
   4.1 ตัวกลั่นกรองเส้นทาง (Screening routers)
   4.2 Proxy gateway
   4.3 Guard
5. **ความปลอดภัยกับพานิชย์อิเล็คทรอนิกส์** (Electronic commerce)
6. **คำศัพท์**

ภาคผนวก จ.
ความมั่นคงและความปลอดภัยในระบบเครือข่าย

ถึงแม้ว่าในความเป็นจริงแล้ว การแยกนโยบาย กับกลไก การทำงาน เป็นหลักการที่สำคัญในเรื่องของความมั่นคงและความปลอดภัยก็ตาม แต่ในบทนี้จำเป็นต้องเชื่อมโยงระหว่างนโยบายกับการคุกคามต่อเทคโนโลยีเฉพาะ เพราะการคุกคามต่อระบบเครือข่ายนั้นเกิดขึ้นในจุดที่แตกต่างกัน บนพื้นฐานทางเทคโนโลยีที่แตกต่างกันด้วย การควบคุมที่เกิดขึ้นจึงต้องสัมพันธ์กับเทคโนโลยีนั้นๆ (อย่างไรก็ตาม เนื้อหาในบทนี้เป็นเพียงส่วนหนึ่งของการบริหารการจัดการศูนย์คอมพิวเตอร์ ดังนั้นจึงเป็นเพียงบริบทกว้างๆ เท่านั้น รายละเอียดควรศึกษาจากหนังสือที่เกี่ยวกับความมั่นคงและความปลอดภัยโดยเฉพาะ)

1. แนวคิดพื้นฐานของระบบเครือข่าย

เครือข่าย (Network) คือ อุปกรณ์ 2 ชิ้นขึ้นไป เชื่อมต่อผ่านสื่อรูปแบบต่างๆ โดยมีฮาร์ดแวร์และซอฟต์แวร์ ที่ทำให้การสื่อสารสมบูรณ์ ดังรูป จ.1



รูป จ.1 รูปแบบเครือข่ายพื้นฐาน

ในบางกรณี อุปกรณ์ด้านหนึ่งจะเป็นเครื่องคอมพิวเตอร์ (ซึ่งเรียก เครื่องให้บริการ (Server) ส่วนอุปกรณ์อีกด้านหนึ่งจะเป็นอุปกรณ์นำเข้า/นำออก (ซึ่งเรียก เครื่องรับบริการ (Client) เครื่องรับบริการขั้นต่ำสุดจะเป็นแผงแป้นอักขระเพื่อนำเข้าข้อมูล และหน้าจอสำหรับ

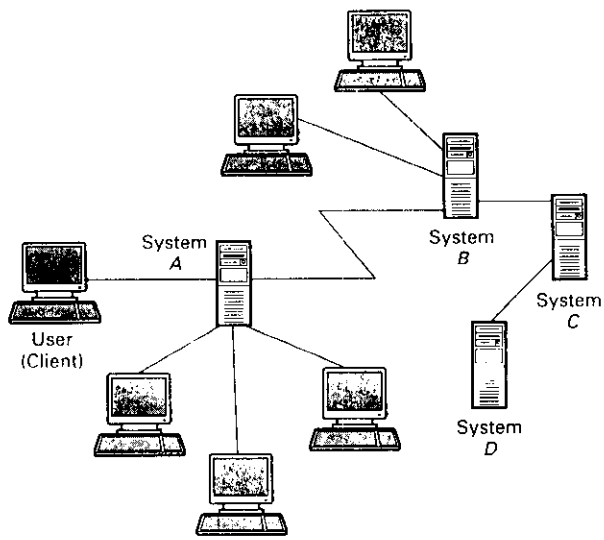
นำออกข้อมูล รูป จ.1 เป็นเพียงรูปที่สื่อตามคำจำกัดความเท่านั้น แต่ในความเป็นจริงระบบเครือข่ายจะมีความซับซ้อน โดย

- อุปกรณ์นำเข้า/นำออก มักจะเป็นเครื่องไมโครคอมพิวเตอร์ หรือ สถานีงาน ซึ่งจะทำให้เครื่องรับบริการมีพื้นที่หน่วยเก็บ และมีความสามารถในการประมวลผลสูงขึ้น

- ระบบเครือข่ายโดยปกติไม่ได้มีเครื่องให้บริการ 1 เครื่อง ต่อเชื่อมกับเครื่องรับบริการ 1 เครื่อง แต่จะเป็น เครื่องให้บริการหลายเครื่อง เชื่อมต่อกับเครื่องรับบริการหลายเครื่องเช่นกัน

- ผู้ใช้ในระบบไม่ได้ตระหนักว่าในขณะที่ใช้งานนั้น มีการสื่อสารข้อมูลจากผู้ใช้มากมายเกิดขึ้นในระบบ

ระบบเครือข่ายที่เกิดขึ้นโดยทั่วไป ดังรูป จ.2



รูป จ.2 ระบบเครือข่ายทั่วไปที่มีความซับซ้อน

การสื่อสารที่เกิดขึ้นนั้น ข้อมูลจะเดินทางผ่านสื่อรูปแบบต่างๆ ได้แก่ สายลวดเกลียวคู่ (Twisted pair) สายลวด Coaxial (Coax) ใยแก้วนำแสง (Optical fiber) หรือ คลื่นไมโครเวฟ ดาวเทียม

การสื่อสารระหว่างอุปกรณ์ที่มีความแตกต่างกัน จึงต้องกำหนดรูปแบบข้อตกลงในการติดต่อสื่อสารที่เรียกว่า โพรโทคอล (Protocol) ได้แก่ การเชื่อมต่อระหว่างระบบเปิด หรือ โอเอสไอ (Open system interconnection, OSI) โพรโทคอลควบคุมการส่งผ่าน และ โพรโทคอล

อินเทอร์เน็ต (Transmission Control Protocol and Internet Protocol, TCP/IP)

รูปแบบในการเชื่อมต่ออุปกรณ์ หรือ Topology พื้นฐาน ได้แก่ เครือข่ายแบบบัส (Bus) แบบวงแหวน (Ring) และแบบดาว (Star) รูปแบบการเชื่อมต่อนี้มีผลต่อความมั่นคง และความปลอดภัยของระบบเครือข่าย ระบบเครือข่ายที่ใหญ่ที่สุดและเป็นที่รู้จักกันดีคือ อินเทอร์เน็ต ซึ่งเป็นการเชื่อมต่อเครือข่ายต่างๆ รอบโลกเข้าด้วยกัน อินเตอร์เน็ตอาศัยพื้นฐานเทคโนโลยีแบบระบบรับ/ให้บริการ (Client/Server system) สามารถใช้ในการสื่อสารข้อมูลทั้งภายใน และภายนอกองค์กร องค์ประกอบของเครื่องให้บริการอินเตอร์เน็ต ดังรูป ข.3

การเชื่อมต่อเข้ากับอินเทอร์เน็ต หรือ การส่งผ่านข้อมูลผ่านเครือข่ายภายใน และเครือข่ายภายนอก ต้องมีการรักษาความปลอดภัยเป็นพิเศษ

3.4 **บูรณภาพของข้อมูล** (Message integrity)

คือความสามารถที่ทำให้เกิดความแน่ใจว่าข้อมูลที่มีการส่งไปนั้นไม่ถูกทำลายหรือ ถูกเปลี่ยนแปลง

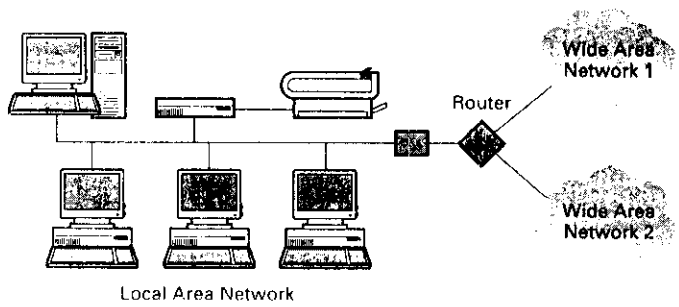
4. Firewall

Firewall เป็นระบบรักษาความปลอดภัย ประกอบด้วยฮาร์ดแวร์ และ ซอฟต์แวร์ที่กั้นระหว่างเครือข่ายภายในองค์กร และเครือข่ายภายนอก วัตถุประสงค์ของ Firewall คือ กั้นสิ่งไม่ดีทั้งหลายให้อยู่ภายนอกสภาพแวดล้อมที่ปกป้องไว้ ป้องกันเครือข่ายส่วนตัวจากผู้บุกรุกภายนอก โดยการทำงานของ Firewall อาจเป็นการป้องกันการเข้าถึงจากภายนอก (แต่ยินยอมให้เกิดการผ่านจากภายในไปสู่ภายนอก) หรือ ยินยอมให้เข้าถึงเฉพาะจากตำแหน่งที่กำหนด หรือจากผู้ใช้ที่กำหนด หรือจากกิจกรรมที่กำหนด

รูปแบบการรักษาความปลอดภัยที่เรียกว่าเป็น Firewall ได้แก่

4.1 **ตัวกลั่นกรองเส้นทาง** (Screening routers)

เป็นรูปแบบที่ง่ายที่สุด และในบางสถานการณ์ รูปแบบนี้จะมีประสิทธิภาพสูงสุด การทำงานของตัวกลั่นกรองเส้นทาง คือ เครื่องแม่ข่ายจะไม่ติดต่อโดยตรงกับเครือข่ายระยะไกล แต่จะเชื่อมต่อกับตัวจัดเส้นทาง (Router) ซึ่งเป็นคอมพิวเตอร์ที่จัดเส้นทางการสื่อสารไปยังเป้าหมาย ตัวจัดเส้นทางจะรับกลุ่ม (Packet) ข้อมูล แต่ละกลุ่ม พิจารณาตารางเส้นทาง แล้วส่งผ่านกลุ่มข้อมูลไปยังช่องทางต่างๆ ซึ่งจะรับและส่งไปยังจุดหมายปลายทาง ดังรูป จ.10



รูป จ.10 ตัวจัดเส้นทางเชื่อมเครือข่ายเฉพาะที่เข้ากับ 2 เครือข่ายระยะไกล

4.2 **Proxy gateway**

ในรูปแบบแรก ตัวกลั่นกรองเส้นทางจะพิจารณาเฉพาะส่วนแรก หรือ ส่วนหัวของกลุ่มข้อมูลเท่านั้น แต่ไม่ได้พิจารณาภายในกลุ่มข้อมูล ดังนั้น ตัวกลั่นกรองเส้นทางจะส่งผ่านอะไรก็ตามไปยังช่องทางที่กำหนด โดยยึดกฎเกณฑ์ว่ายินยอมให้ภายในเชื่อมต่อไปยังช่องทางนั้นๆ ในรูปแบบที่ 2 Proxy gateway เป็น Firewall ที่จำลองผลกระทบของงานประยุกต์ เพื่อที่งานประยุกต์จะรับเฉพาะสิ่งที่ถูกต้อง

Proxy gateway ทำงานเป็นงานประยุกต์เทียม เช่น เมื่อมีการส่งไปรษณีย์อิเล็กทรอนิกส์ มีกระบวนการส่ง และกระบวนการรับ สื่อสารกันโดยโพรโทคอลที่กำหนดกฎเกณฑ์ในการส่งผ่านไปรษณีย์ แล้วจึงส่งผ่านข้อความ Proxy gateway จะบุกรุกไปที่ส่วนกลางของโพรโทคอลการแลกเปลี่ยน เป็นเสมือนจุดหมายปลายทางโดยผู้ส่งอยู่ภายนอก Firewall และเป็นเสมือนผู้ส่งของการสื่อสารโดยมีจุดหมายปลายทางที่แท้จริงอยู่ภายใน Proxy ในส่วนกลางจะทำหน้าที่กลั่นกรองไปรษณีย์ที่มีการส่งผ่าน ให้แน่ใจว่ามีเฉพาะส่วนที่ยอมรับให้การยินยอมเท่านั้นที่ผ่านไปที่จุดหมายปลายทาง ความแตกต่างของ Proxy gateway กับตัวกลั่นกรองเส้นทาง คือ Proxy จะตีความโพรโทคอลไปยังงานประยุกต์ เพื่อควบคุมการทำงานผ่าน Firewall โดยอาศัยพื้นฐานว่าทุกอย่างในโพรโทคอลต้องโปร่งใส ไม่ใช่เฉพาะส่วนหัวของข้อมูลเท่านั้น

4.3 **Guard**

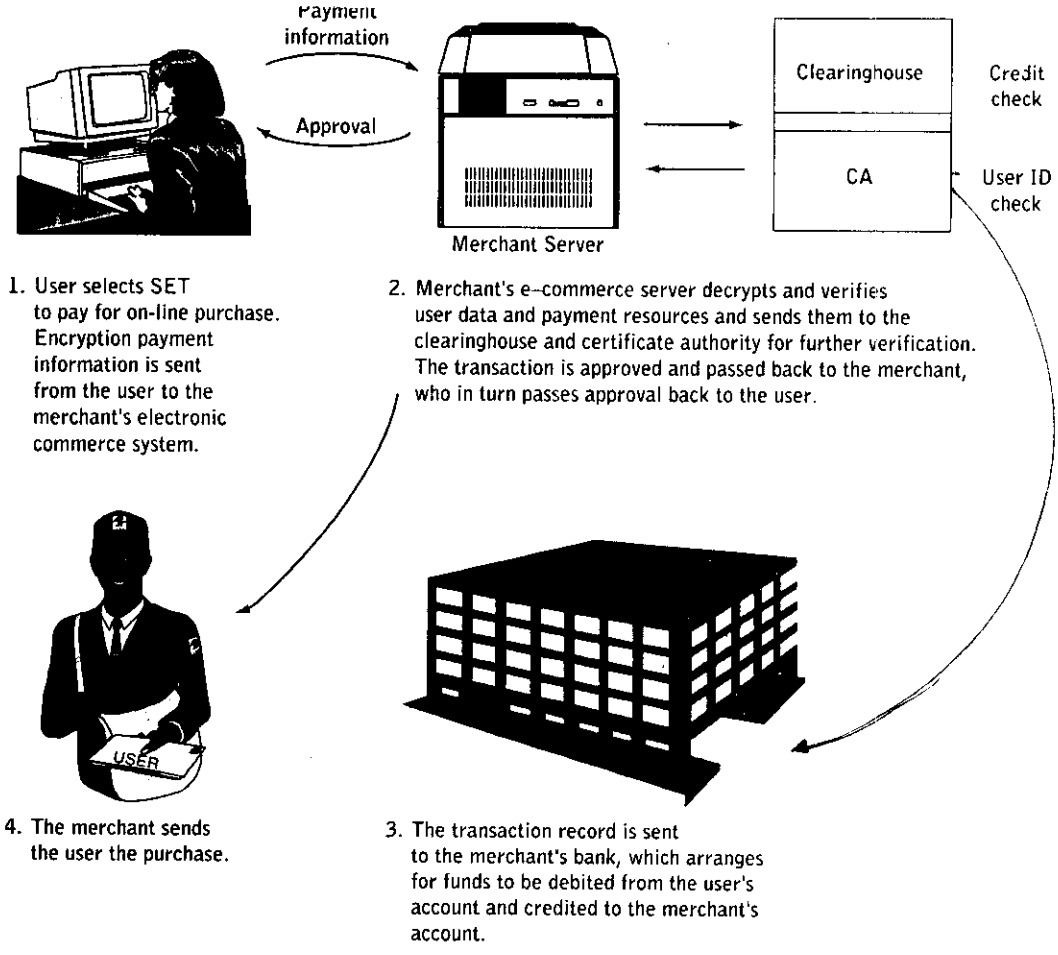
Guard เป็น Proxy firewall ที่ซับซ้อน โดย guard จะรับข้อมูลโพรโทคอล ตีความและส่งผ่านข้อมูลโพรโทคอลเดิม หรือ ที่แตกต่าง ซึ่งอาจให้ผลในรูปแบบเดิม หรือให้ผลที่แตกต่างออกไป Guard จะทำหน้าที่ตัดสินใจว่าบริการใดที่จะดำเนินการ

5. การรักษาความปลอดภัยกับพานิชย์อิเล็กทรอนิกส์ (Electronic commerce)

เทคโนโลยีความก้าวหน้าในการติดต่อสื่อสาร ทำให้เครือข่ายสื่อสารถูกนำมาใช้เป็นประโยชน์กับธุรกิจ เป็นการค้าทางอิเล็กทรอนิกส์ สิ่งสำคัญสำหรับพานิชย์อิเล็กทรอนิกส์ คือ ขั้นตอนการชำระเงิน เพราะจะต้องมีระบบรักษาความปลอดภัยในการชำระเงิน ซึ่งได้มีการพัฒนาระบบชำระเงินอิเล็กทรอนิกส์เป็นพิเศษ โดยบริษัทที่ดำเนินธุรกิจบัตรเครดิตทั้งหลาย ได้แก่ VISA International, MasterCard International, American Express และธนาคารต่างๆ ระบบการรักษาความปลอดภัยดังกล่าว เช่น

1. **Secure Electronic Transaction (SET)** เป็นโพรโทคอลสำหรับเข้ารหัสข้อมูลการ

ชำระเงินด้วยบัตรเครดิตผ่านเครือข่ายอินเทอร์เน็ต และเครือข่ายเปิดอื่นๆ ขั้นตอนการใช้งานนั้น ผู้ใช้จะได้รับใบรับรองดิจิทัล และกระเป๋าเงินดิจิทัล จากธนาคารที่ผู้ใช้ใช้บริการ ซึ่งจะทำหน้าที่เป็นเสมือนตัวกลางสำหรับธุรกรรมพานิชย์อิเล็กทรอนิกส์ โดยกระเป๋าเงินและใบรับรองที่ได้รับจากธนาคารนั้นจะเป็นตัวที่ระบุผู้ใช้ และบัตรเครดิตที่ใช้ เมื่อผู้ใช้ซื้อของจาก Web site และเลือกใช้วิธีการจ่ายเงินระบบ SET เครื่องให้บริการของผู้ขายจะส่งสัญญาณผ่านทางอินเทอร์เน็ตไปยังกระเป๋าดิจิทัลของผู้ใช้ จากนั้นกระเป๋าดิจิทัลจะเข้ารหัสข้อมูลการจ่ายเงิน และส่งข้อมูลไปยังผู้ขาย ผู้ขายจะทำการตรวจสอบว่าข้อมูลนั้นเป็นกลุ่มข้อมูล SET หรือไม่ แล้วใส่ใบรับรองดิจิทัลเข้าไปที่ข้อความ ทำการเข้ารหัส แล้วส่งข้อมูลไปยังสำนักหักบัญชี และผู้ออกใบรับรองเพื่อตรวจสอบข้อมูล สำนักหักบัญชีเป็นผู้ให้การยอมรับหรือปฏิเสธธุรกรรมนั้นๆ ตามสถานะเครดิตของผู้ซื้อ สำนักหักบัญชีส่งข้อมูลผ่านอินเทอร์เน็ตไปยังผู้ขาย และกลับไปที่กระเป๋าเดินทางของผู้ใช้ ธุรกรรมนี้จะถูกส่งไปที่ธนาคารของผู้ขาย ซึ่งจะจัดการโอนเงินจากผู้ซื้อไปยังผู้ขาย ดังรูป จ.11



รูป จ.11 ขั้นตอนการทำงานของ SET

อธิบายขั้นตอนการทำงาน

1. เมื่อผู้ใช้เลือกวิธีการจ่ายเงินแบบ SET สำหรับการซื้อในระบบเชื่อมตรง (On-line) ผู้ใช้จะส่งข้อมูลการจ่ายเงินที่เข้ารหัสแล้วไปยังระบบพานิชย์อิเล็กทรอกนิกส์ของผู้ขาย
2. เครื่องให้บริการพานิชย์อิเล็กทรอนิกส์ของผู้ขายจะถอดรหัสข้อมูล ตรวจสอบข้อมูลและการจ่ายเงินของผู้ใช้ แล้วส่งไปยังสำนักหักบัญชี เพื่อตรวจสอบขั้นต่อไป ธุรกรรมที่ได้รับการยินยอมแล้วจะถูกส่งกลับไปยังผู้ขาย ซึ่งจะเป็นผู้ส่งการยินยอมไปที่ผู้ซื้อ
3. ข้อมูลธุรกรรมจะถูกส่งไปยังธนาคารที่ผู้ขายใช้บริการ ธนาคารจะเป็นผู้ที่จัดการโอนเงินจากบัญชีของผู้ซื้อไปยังบัญชีผู้ขาย
4. ผู้ขายจัดส่งให้ผู้ซื้อ

2. **CyberCash/Checkfree Wallet** รูปแบบนี้จะไม่ใช้ซอฟต์แวร์ของลูกค้าเพื่อเข้ารหัสส่งต่อธุรกรรม และข้อมูลบัตรเครดิต ผ่านทาง Web site ไปยังผู้ขายสินค้าบนเครือข่าย แต่ผู้ขายจะเป็นผู้ส่งข้อมูลไปยังเครื่องให้บริการ CyberCash เครื่องให้บริการจะเก็บข้อมูลไว้ภายใต้กำแพงไฟ (Firewall) ทำการถอดรหัส แล้วส่งไปยังธนาคารที่ผู้ขายใช้บริการ ธนาคารจะส่งการร้องขอเป็นผู้มีสิทธิ ไปยังธนาคารที่ออกบัตรเครดิต เมื่อธนาคารที่ออกบัตรเครดิตตรวจสอบข้อมูลและให้การยินยอม หรือปฏิเสธการจ่ายเงิน ธนาคารที่ออกบัตรเครดิตจะส่งข้อมูลดังกล่าวไปยัง CyberCash CyberCash รับข้อมูลและส่งกลับไปยังผู้ขาย กระบวนการดังกล่าวหลีกเลี่ยงมิให้ผู้ขายรู้และเก็บหมายเลขบัตรเครดิตของลูกค้า ซึ่งช่วยเพิ่มระดับความปลอดภัยของระบบให้สูงขึ้น

3. **E-cash หรือ Electronic cash** Electronic cash เป็นเงินตราในรูปแบบอิเล็กทรอนิกส์ที่เคลื่อนไหวอยู่นอกเครือข่ายเงินตราปกติ (เครือข่ายเงินตราปกติ ได้แก่ ธนบัตร เหรียญ เช็ค บัตรเครดิต) เป็นเงินตราที่ไม่ได้อยู่ในบทบัญญัติของ Federal Reserve System (เป็นระบบการธนาคารของสหรัฐอเมริกา) ผู้ใช้จะได้รับซอฟต์แวร์ตัวรับบริการ และสามารถแลกเปลี่ยนเงินกับผู้ใช้ E-cash อื่นๆ ผ่านเครือข่ายอินเทอร์เน็ต เมื่อมีลูกค้าซื้อสินค้าในระบบเชื่อมตรง E-cash ซอฟต์แวร์จะสร้างเงินในปริมาณที่ผู้ใช้ระบุ และใส่ซองเสมือนส่งไปยังธนาคาร ธนาคารที่รับซองเสมือนก็จะถอนจำนวนเงินตามที่ระบุจากบัญชีของลูกค้า ปิดแสตมป์บนซองเพื่อยืนยันมูลค่าจำนวนเงิน และส่งกลับไปยังผู้ใช้ เมื่อผู้ใช้รับซองกลับไป ก็จะสามารถใช้จำนวนเงินนั้นได้

3. **Virtual PIN** First Virtual Internet Payment System เป็นระบบที่ใช้แนวคิดต่างจากแนวคิดอื่นๆ เพราะระบบนี้จะหลีกเลี่ยงการสร้างระบบความปลอดภัยในการส่งข้อมูลผ่าน

เครือข่ายอินเทอร์เน็ตโดยสิ้นเชิง แต่จะให้ลูกค้าขอหมายเลขระบุบุคคล ซึ่งเป็นหมายเลขเฉพาะแต่ละบุคคล เรียกว่า VirtualPIN หมายเลขเฉพาะ หรือ VirtualPIN นี้สามารถใช้กับ Site ใดก็ได้ VirtualPIN จะถูกเก็บไว้กับหมายเลขบัตรเครดิตในคอมพิวเตอร์ที่ไม่ได้ต่อผ่านเครือข่ายหรือต่อแบบเชื่อมตรง และมีเฉพาะ First Virtual เท่านั้นที่สามารถเข้าถึงข้อมูลได้ เมื่อลูกค้ามีการซื้อสินค้าผ่านทางอินเทอร์เน็ต จะมีเฉพาะ VirtualPIN ของลูกค้าเท่านั้นที่เดินทางอยู่ในเครือข่าย ในการชำระเงิน ผู้ขายจะส่ง VirtualPIN ของผู้ขายพร้อมกับ VirtualPIN ของผู้ซื้อไปยัง First Virtual จากนั้น First Virtual จะส่งไปรษณีย์อิเล็กทรอนิกส์ไปยังลูกค้าเพื่อยืนยันการขาย ถ้าลูกค้าให้การยอมรับธุรกรรมนั้น First Virtual ก็จะประมวลผลธุรกรรม และยืนยันไปยังผู้ขาย ผู้ขายจึงจะจัดส่งสินค้าไปยังผู้ซื้อ

5. **NetCheck** เป็นระบบการชำระเงินที่ใช้เช็คอิเล็กทรอนิกส์ โดยเช็คเหล่านี้จะผ่านการเข้ารหัสพร้อมลายเซ็นที่สามารถตรวจสอบได้ และใช้สำหรับการชำระเงินในพานิชย์อิเล็กทรอนิกส์

6. คำศัพท์

Access control
Authentication
Automatic call – back
Ciphertext
Client
Cybercash
Decryption
E – cash
Electronic commerce
Encryption
End – to – End encryption
Firewall
Guard
Link encryption
Plaintext
Port protection
Private key
Protocol
Proxy gateway
Public key
Server
SET
TCP/IP