บทที่ 9
ความมั่นคงและความปลอดภัยของระบบสารสนเทศ

1. ความอ่อนแอและความไม่มั่นคงของระบบสารสนเทศ

1.1 การคุกคามต่อฮาร์ดแวร์

1.2 การคุกคามต่อซอฟต์แวร์

1.3 การคุกคามต่อข้อมูล

2. ความมั่นคงของระบบสารสนเทศ

2.1 ความปลอดภัยของสถานที่

2.2 การควบคุมการเข้าถึง และใช้งานระบบ

2.3 การควบคุมการให้สิทธิในการใช้งาน

2.4 ความปลอดภัยในการปฏิบัติงาน

2.5 ความปลอดภัยในการใช้งานเครื่องไมโครคอมพิวเตอร์

3. สภาพแวดล้อมในการควบคุม

3.1 การควบคุมทั่วไป

3.1.1 การควบคุมการนำระบบไปใช้งาน

3.1.2 การควบคุมซอฟต์แวร์

3.1.3 การควบคุมฮาร์ดแวร์

3.1.4 การควบคุมการปฏิบัติงาน

3.1.5 การควบคุมความปลอดภัยของข้อมูล

3.1.6 การควบคุมในทางการบริหาร

3.2 การควบคุมงานประยุกต์

4. การกำหนดระดับความปลอดภัย

5. คำศัพท์

6. คำถามท้ายบท

CT 489 177

5. คำศัพท์

6. คำถามท้ายบท

บทที่ 9
ความมั่นคงและความปลอดภัยของระบบสารสนเทศ

ระบบคอมพิวเตอร์ ตลอดจนระบบสารสนเทศ มีบทบาทสำคัญมากทั้งในธุรกิจ ราชการ และชีวิตประจำวัน ทำให้เกิดความจำเป็นที่จะต้องปกป้องระบบสารสนเทศ และทำให้เกิดความมั่นใจว่าระบบมีความถูกต้อง และความน่าเชื่อถือ

1. ความอ่อนแอและความไม่มั่นคงของระบบสารสนเทศ

แต่เดิมข้อมูลเกี่ยวกับบุคลากร และองค์กร เป็นข้อมูลที่อยู่บนกระดาษ เอกสาร รายงาน ซึ่งจะมีการเก็บรักษา โดยกระจายอยู่ตามหน่วยงานต่างๆ ขององค์กร เมื่อมีระบบคอมพิวเตอร์เข้ามาช่วยทำให้งานต่างๆ ดำเนินไปโดยอัตโนมัติ ระบบสารสนเทศจะจัดการกับข้อมูลในแฟ้ม ข้อมูลเหล่านี้สามารถถูกเข้าถึงโดยกลุ่มคนทั้งภายใน และภายนอกองค์กร ผลที่ตามมาคือ ข้อมูลอัตโนมัติจะไวต่อการถูกทำลาย ถูกน้อฉล ความผิดพลาด และการใช้งานที่ไม่ถูกต้อง

เมื่อระบบคอมพิวเตอร์ไม่สามารถทำงานได้ตามที่ต้องการ กิจการซึ่งต้องพึ่งพาการทำงานของระบบคอมพิวเตอร์ จะพบว่าธุรกิจประสบกับความเสียหายมากมาย เช่น บริษัทนายหน้าค้าหุ้นแห่งหนึ่งเกิดความสูญเสียถึงชั่วโมงละ 6 ล้านเหรียญสหรัฐเมื่อระบบคอมพิวเตอร์หยุดทำงาน ดังนั้นยิ่งระบบคอมพิวเตอร์หยุดทำงานนานเท่าใด ความสูญเสียที่เกิดขึ้นก็จะมากขึ้นเป็นลำดับ และถ้าระบบหยุดทำงานเพียง 2-3 วัน อาจทำให้ธุรกิจบางแห่งไม่สามารถดำเนินงานต่อได้

ข้อมูลจำนวนมหาศาลที่ถูกเก็บในรูปแบบอิเล็กทรอนิกส์ จะเผชิญกับการถูกคุกคามในรูปแบบต่างๆ มากกว่าข้อมูลที่อยู่ในรูปแบบเดิม ดังตาราง 9.1

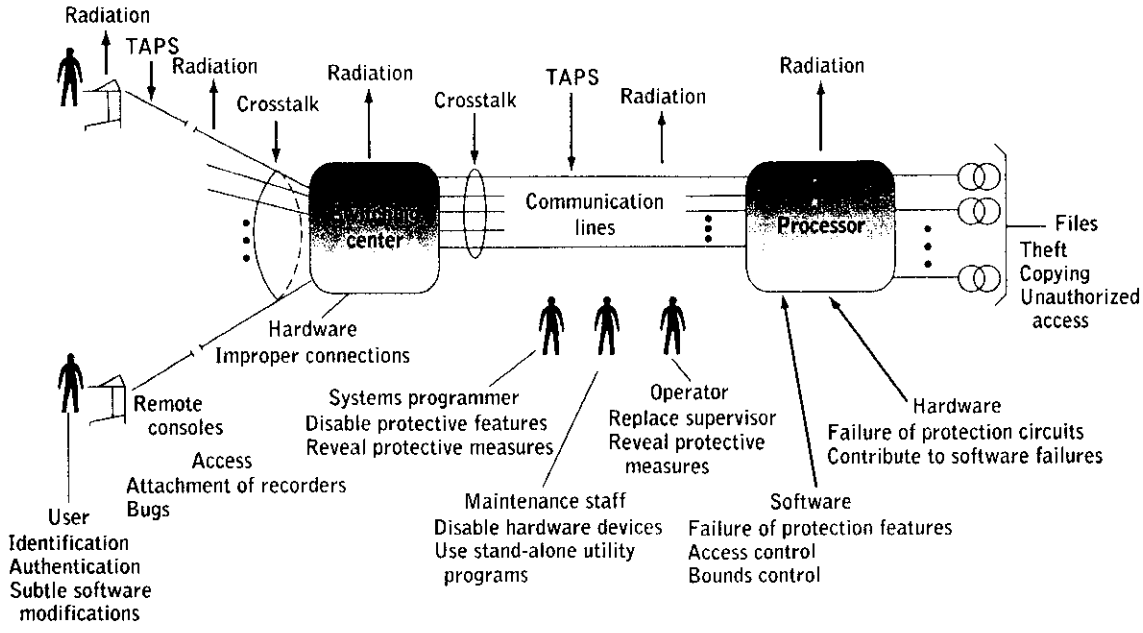
ตาราง 9.1 การคุกคามต่อระบบสารสนเทศ

ฮาร์ดแวร์ใช้งานไม่ได้	ไฟไหม้
ซอฟต์แวร์ใช้งานไม่ได้	ปัญหาด้านกระแสไฟฟ้า
พนักงาน	ความผิดพลาดของผู้ใช้
การบุกรุกเข้าใช้งานเครื่อง	การเปลี่ยนแปลงโปรแกรม
การขโมยข้อมูล บริหาร อุปกรณ์	ปัญหาในการสื่อสารทางไกล
เป็นต้น	

ระบบคอมพิวเตอร์มีความไม่มั่นคงต่อการคุกคามดังกล่าวเป็นพิเศษ เพราะ

- ระบบสารสนเทศที่ซับซ้อนไม่สามารถจะถอดแบบ หรือ จำลองโดยรูปแบบเดิมที่เป็นการใช้แรงงาน หรือ ทำด้วยมือได้
- กระบวนงานทางคอมพิวเตอร์เป็นกระบวนงานที่ไม่สามารถมองเห็นได้ และไม่สามารถที่จะตรวจสอบ หรือทำความเข้าใจได้โดยง่าย
- ถึงแม้ว่าโอกาสที่จะเกิดความหายนะต่อระบบอัตโนมัติไม่ได้สูงกว่าระบบรูปแบบเดิมที่ใช้แรงงาน หรือไม่ได้ใช้อุปกรณ์ในการดำเนินงานก็ตาม แต่ผลกระทบของความหายนะนั้นมีค่าสูงกว่ามาก ในบางกรณีข้อมูลทั้งหมดของระบบอาจถูกทำลาย และสูญเสียทั้งหมด
- ระบบสารสนเทศแบบเชื่อมตรง (on - line) ถูกเข้าถึงโดยตรงจากผู้ใช้จำนวนมาก ผู้ใช้ที่ได้รับสิทธิ อาจเข้าถึงส่วนของข้อมูลซึ่งผู้ใช้นั้นไม่ได้รับสิทธิ หรือผู้ใช้ที่ไม่ได้รับสิทธิก็อาจเข้าถึงระบบดังกล่าว

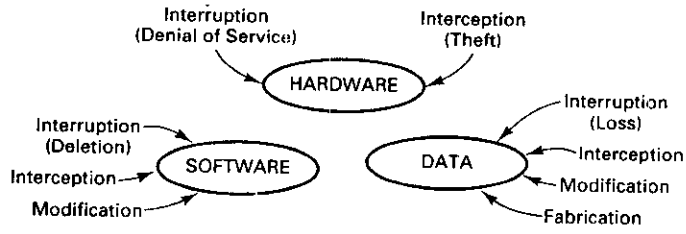
นอกจากนี้ความก้าวหน้าในด้านการสื่อสารทางไกล และซอฟต์แวร์ต่างๆ กลับเป็นส่วนที่ขยายความไม่มั่นคงของระบบให้สูงขึ้น เพราะด้วยเครือข่ายสื่อสารทางไกล ทำให้ระบบสารสนเทศในตำแหน่งต่างๆ สามารถเชื่อมต่อระหว่างกันได้ ดังนั้น การเข้าถึงโดยผู้ไม่ได้รับอนุญาต การใช้งานในทางที่ไม่ถูกต้อง หรือ การฉ้อฉล จึงไม่ได้จำกัดอยู่ในตำแหน่ง หรือในสถานที่เดียว แต่สามารถจะถูกดำเนินการจากที่ใดๆ ก็ตามในเครือข่าย ในความก้าวหน้าของเครือข่ายสื่อสารทางไกลซึ่งมีการใช้ฮาร์ดแวร์ ซอฟต์แวร์ และ องค์กรที่มีความซับซ้อน หลากหลาย ตลอดจนการจัดการบุคลากร ยิ่งทำให้เกิดการสร้างโอกาสและช่องทางที่จะแทรกแซง และดำเนินการเข้าถึงระบบได้มากขึ้น หรือความก้าวหน้าของการใช้เครือข่ายแบบไร้สายโดยใช้เทคโนโลยีของคลื่นวิทยุ ก็ทำให้ระบบง่ายต่อการแทรกแซงเช่นกัน เพราะคลื่นความถี่วิทยุสามารถที่จะกวาดตรวจได้ง่าย และท้ายสุดความก้าวหน้าที่ไม่อาจละเลยคือ เครือข่ายอินเทอร์เนต ซึ่งเป็นความก้าวหน้าที่ก่อให้เกิดปัญหาพิเศษ เพราะอินเทอร์เนตได้ถูกออกแบบมาให้ผู้คนทั่วไปในระบบหลากหลายสามารถเข้าถึงได้ง่าย ความไม่มั่นคงของเครือข่ายสื่อสารทางไกล แสดงดังรูป 9.2



รูป 9.2 ความไม่มั่นคงของเครือข่ายสื่อสารทางไกล ในเครือข่ายสื่อสารทางไกลนั้นมีโอกาสที่จะเกิดการหยุดทำงานของฮาร์ดแวร์ ซอฟต์แวร์ ซึ่งเกิดจากระบบเอง ตลอดจนมีโอกาสที่โปรแกรมเมอร์ ผู้ปฏิบัติงาน พนักงานดูแลรักษาระบบ และผู้ใช้ ใช้งานอย่างไม่ถูกต้อง เช่น ลักลอบต่อสายสื่อสาร และสกัด หรือ ลักลอบดึงข้อมูลออกอย่างผิดกฎหมาย หรือการส่งผ่านด้วยความเร็วสูง ผ่านช่องทางการสื่อสารที่ใช้สายเคลียว ทำให้เกิดการรบกวนที่เรียก การแทรกสัญญาณข้ามวงจร (Crosstalk) เป็นต้น

ความไม่มั่นคงของระบบคอมพิวเตอร์ สามารถแบ่งพิจารณาออกเป็น 3 ส่วน ได้แก่

- การคุกคามต่อฮาร์ดแวร์
- การคุกคามต่อซอฟต์แวร์
- การคุกคามต่อข้อมูล



รูป 9.3 ความไม่มั่นคงของระบบคอมพิวเตอร์ใน 3 ส่วน

1.1 การคุกคามต่อฮาร์ดแวร์

ฮาร์ดแวร์เป็นส่วนที่ถูกคุกคามได้ง่าย เพราะ เป็นอุปกรณ์ เครื่องมือ ที่เห็นได้ง่ายชัดเจน แต่ในทางตรงกันข้าม ก็สามารถติดตั้งระบบการป้องกันได้ง่าย ความเสียหายที่เกิดขึ้นกับฮาร์ดแวร์ เช่น น้ำท่วม ไฟไหม้ แก๊ส ไฟลัดวงจร ความเสียหายเหล่านี้เป็นเหตุที่หลีกเลี่ยงยาก แต่สามารถป้องกันให้ความเสียหายลดลง นอกจากนี้ยังมีความเสียหายในรูปแบบอื่นๆ เช่น ผู้ใช้ทำน้ำ อาหาร หกหล่นไปที่ฮาร์ดแวร์ หนูกัดสายไฟ ฝุ่นละออง หรือก้นบุหรี่ เป็นต้น ความเสียหายเหล่านี้ยังเป็นความเสียหายที่เกิดขึ้นโดยไม่ตั้งใจ แต่ยังมีการคุกคามในรูปแบบที่เกิดขึ้นจากความประสงค์ร้ายต่อระบบ เกิดขึ้นด้วยความตั้งใจที่จะทำความเสียหายต่อระบบ โดยทำลายฮาร์ดแวร์ เช่น ใช้ระเบิด ทำให้เกิดไฟไหม้ ทำลายแผงวงจรไฟฟ้า ขโมยฮาร์ดแวร์ ฯลฯ ซึ่งมีได้มากมายหลายรูปแบบ การคุกคามหลากหลายรูปแบบที่เกิดขึ้น ทำให้ผู้บริหารศูนย์คอมพิวเตอร์ ต้องติดตั้งระบบรักษาความปลอดภัยในรูปแบบต่างๆ เพื่อป้องกันฮาร์ดแวร์

1.2 การคุกคามต่อซอฟต์แวร์

ดังที่ทราบกันดีว่าอุปกรณ์คอมพิวเตอร์จะไม่มีความหมาย ถ้าไม่มีซอฟต์แวร์ (ทั้งระบบปฏิบัติการ โปรแกรมอรรถประโยชน์ และโปรแกรมประยุกต์) ซอฟต์แวร์สามารถถูกทำลาย ถูกปรับเปลี่ยน ถูกลบทิ้ง ทั้งด้วยความตั้งใจ และความไม่ตั้งใจ การคุกคามเหล่านี้ก่อให้เกิดปัญหาต่อสภาพพร้อมใช้งานของซอฟต์แวร์ การคุกคามที่ลึกไปกว่านั้น คือ ซอฟต์แวร์ที่ใช้งานอยู่นั้น ถูกเปลี่ยนแปลง การคุกคามในรูปแบบนี้ยากในการตรวจสอบ เมื่อเปรียบเทียบกับการคุกคามต่อฮาร์ด-แวร์ ซึ่งสามารถมองเห็น หรือ ตรวจสอบทางกายภาพได้ แต่ในกรณีของซอฟต์แวร์นั้น การปรับเปลี่ยนโปรแกรมต้นฉบับเพียง 1 บรรทัด อาจไม่สามารถตรวจพบได้ เพราะโปรแกรมยังคงสามารถ

ทำงานหลักๆ ได้ในรูปแบบเดิม

การลบซอฟต์แวร์ทิ้ง อาจเกิดขึ้นจากความเผอเรอของนักเขียนโปรแกรมที่ลบแฟ้มบางแฟ้มทิ้งโดยไม่ตั้งใจ หรือ ทำสำเนาเก็บแฟ้มที่ผิดไว้ แต่ลบแฟ้มที่ถูกต้องทิ้งไป เนื่องจากซอฟต์แวร์เป็นสิ่งที่มีมูลค่าสูง สำคัญต่อการทำงาน ต่อระบบสารสนเทศ ทำให้ต้องกำหนดการควบคุมการเข้าถึงโดยผ่านกระบวนการที่เรียก การจัดการโครงแบบ (Configuration management) เพื่อให้ซอฟต์แวร์ไม่ถูกลบทิ้ง ไม่ถูกทำลาย หรือ ไม่ถูกแทนที่ด้วยความไม่ตั้งใจ

การปรับเปลี่ยนซอฟต์แวร์ เป็นการปรับเปลี่ยนโปรแกรมที่กำลังทำงาน เพื่อให้การทำงานของโปรแกรมผิดพลาด หรือ ไม่ทำงาน ซอฟต์แวร์สามารถถูกปรับเปลี่ยนการทำงานโดยการเปลี่ยนแปลงรหัสเพียงเล็กน้อย ความเสียหายที่เกิดขึ้นกับโปรแกรมอาจเกิดขึ้นเมื่อโปรแกรมเริ่มใช้งาน หรือ เมื่อโปรแกรมทำงานไปได้ระยะหนึ่งแล้วจึงเกิดความไม่เที่ยงตรง ขึ้นกับว่าเปลี่ยนแปลงโปรแกรมในจุดใด ตำแหน่งใด

ในกรณีที่โปรแกรมทำงานไปได้ระยะหนึ่ง การปรับเปลี่ยนจะมีความซับซ้อนได้มาก เช่น การทำให้โปรแกรมทำงานเป็นปกติโดยส่วนใหญ่ แต่จะทำงานผิดปกติ เมื่อเข้าสู่สภาวะแวดล้อมที่กำหนด ตัวอย่างเช่น พนักงานซึ่งมีความโกรธแค้น ไม่พอใจบริษัท อาจเข้าไปปรับเปลี่ยนโปรแกรมสำคัญ เพื่อให้สามารถเข้าถึงส่วนที่เป็นวันที่ของระบบ และให้หยุดการทำงานโดยทันทีหลังจากวันที่ 1 เดือนกรกฎาคม โดยพนักงานคนนี้วางแผนว่าจะลาออกในวันที่ 1 เดือนพฤษภาคม และไปทำงานที่แห่งใหม่ ห่างไกลจากที่เดิม ก่อนเดือนกรกฎาคม เป็นต้น

การเปลี่ยนแปลงซอฟต์แวร์อีกรูปแบบหนึ่ง คือ ขยายหน้าที่ของโปรแกรม เพื่อให้เกิดผลข้างเคียงจากโปรแกรมนั้นๆ เช่น โปรแกรมซึ่งแสดงโครงสร้างรายการแฟ้มที่เป็นของผู้ใช้ อาจมีการปรับเปลี่ยนการป้องกันโดยยินยอมให้ผู้ใช้อื่นสามารถเข้าถึงแฟ้มเหล่านั้นได้

การจัดประเภทในการปรับเปลี่ยนซอฟต์แวร์ รวมถึง

- ตัวลวง หรือ ม้าโทรจัน (Trojan horse) เป็นโปรแกรมที่แสดงให้เห็นว่ากำลังทำหน้าที่หนึ่ง แต่แฝงการทำงานอีกหน้าที่หนึ่งไว้
- ไวรัสคอมพิวเตอร์ (Virus) เป็นรูปแบบเฉพาะของม้าโทรจัน และสามารถแพร่กระจายความเสียหายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ
- ประตูกับดัก (Trapdoor) เป็นโปรแกรมที่มีจุดทางเข้าลับ

การขาดการควบคุม หรือ การควบคุมไม่พอเพียง จะทำให้มีการสร้างโปรแกรมใหม่ๆ ติดตั้งโปรแกรมเข้าสู่ระบบ ใช้งานโปรแกรมเหล่านั้น แล้วก่อให้เกิดปัญหาความปลอดภัยของระบบ

การขโมยซอฟต์แวร์ การคุกคามรูปแบบนี้รวมถึงการทำสำเนาซอฟต์แวร์โดยไม่ได้รับอนุญาต ผู้เขียนและผู้จัดจำหน่ายซอฟต์แวร์ควรได้รับค่าชดเชย หรือค่าตอบแทนในการใช้ซอฟต์-แวร์อย่างยุติธรรม

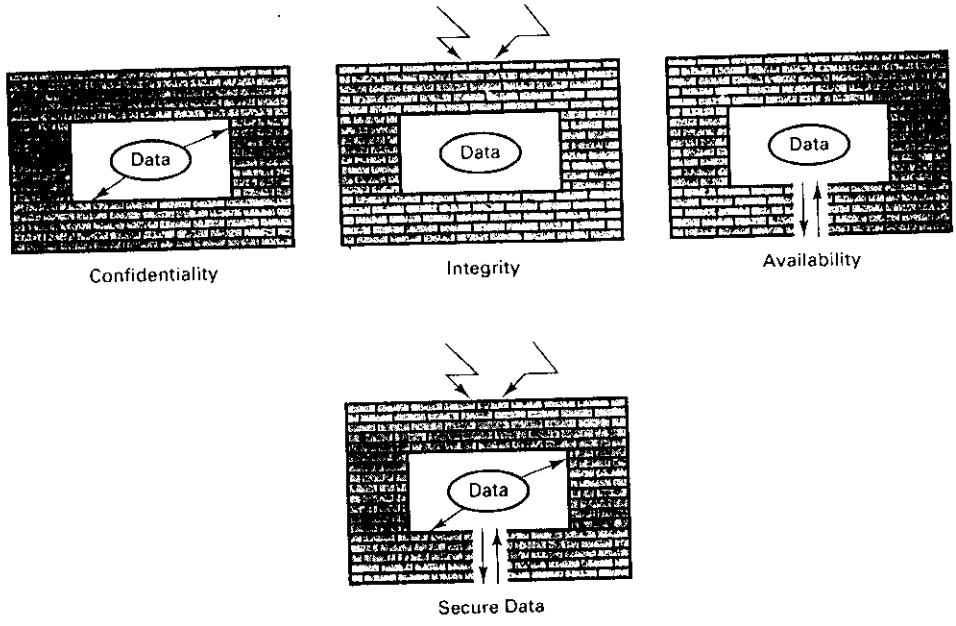
1.3 การคุกคามต่อข้อมูล

ในด้านความปลอดภัยของฮาร์ดแวร์ จะเป็นความเกี่ยวข้องของบุคลากรที่เป็นทีมงานของศูนย์คอมพิวเตอร์ ส่วนความปลอดภัยของซอฟต์แวร์เป็นปัญหาที่ใหญ่ขึ้น เพราะขยายขอบเขตไปสู่ผู้เขียนโปรแกรม และนักวิเคราะห์ระบบ ซึ่งทำหน้าที่เป็นผู้สร้าง และปรับเปลี่ยนโปรแกรม โดยในแต่เดิมนั้นโปรแกรมจะถูกเขียนขึ้นด้วยภาษาเฉพาะของนักคอมพิวเตอร์ เพื่อป้องกันการใช้ประโยชน์ถ้าโปรแกรมมีการรั่วไหลออกไปสู่ภายนอก แต่การคุกคามต่อข้อมูล เป็นปัญหาที่กระจายกว้าง และเป็นปัญหาหนักกว่าการคุกคามฮาร์ดแวร์ และ ซอฟต์แวร์ เพราะเป็นสิ่งที่บุคคลทั่วไปสามารถอ่านสามารถทำความเข้าใจ และใช้ประโยชน์ได้ โดยเนื้อแท้แล้วข้อมูลไม่ได้เป็นสิ่งที่มีมูลค่า แต่เมื่อถูกนำไปใช้งานในรูปแบบต่างๆ ทำให้ข้อมูลกลายเป็นสิ่งที่มีคุณค่าและมูลค่า แม้ว่ามูลค่านั้นจะวัดได้ยาก เช่น ข้อมูลทางการตลาด ถูกเผยแพร่ไปสู่คู่แข่งทางการค้า หรือ ข้อมูลทางการเงินของกิจการ หรือ ข้อมูลเกี่ยวกับเส้นทาง หมายกำหนดการของเที่ยวบินต่างๆ

ทั้งฮาร์ดแวร์และซอฟต์แวร์ มีอายุการใช้งานยาวนาน โดยมีมูลค่าค่อยๆ ลดลงตามระยะเวลา ส่วนมูลค่าข้อมูลอาจจะสูง แต่ข้อมูลบางประเภทจะมีอายุการใช้งาน หรือ อยู่ในความสนใจเพียงช่วงสั้นๆ เช่น นักวิเคราะห์จะวิเคราะห์สภาวะเศรษฐกิจของประเทศออกมาเป็นระยะ ซึ่งจะเผยแพร่ข้อมูลการวิเคราะห์ออกสู่สาธารณะตามวันเวลาที่กำหนดล่วงหน้า แต่ก่อนที่จะถึงวันที่กำหนด การเข้าถึงข้อมูลดังกล่าวอาจสร้างผลกำไร เช่น ข้อมูลดังกล่าวกระทบต่อตลาดหุ้น ดังนั้น ถ้าการวิเคราะห์ข้อมูลเสร็จสิ้น 24 ชั่วโมง ก่อนเผยแพร่สู่สาธารณะ และนักวิเคราะห์ระบบต้องการส่งผ่านข้อมูลนี้ให้กับนักวิเคราะห์อีกคนหนึ่งเพื่อทำการตรวจสอบ การกำหนดระบบการป้องกันข้อมูลในส่วนนี้จะถูกกำหนดเพียง 24 ชั่วโมงเท่านั้น เพราะหลังจาก 24 ชั่วโมงแล้ว ข้อมูลนี้ก็ไม่ได้เป็นความลับอีกต่อไป

รูป 9.4 แสดงถึงความปลอดภัยของข้อมูลใน 3 ด้าน

183



รูป 9.4 ความปลอดภัยของข้อมูลใน 3 ด้าน ได้แก่

ความลับของข้อมูล (Confidentiality) ได้แก่ การป้องกันข้อมูลจากการเปิดเผยโดยไม่ได้รับอนุญาต

บูรณภาพ (Integrity) ได้แก่ การป้องกันข้อมูลจากการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

ความพร้อมใช้งาน (Availability) ได้แก่ การป้องกันการปฏิเสธ การเข้าถึงข้อมูลที่ได้รับอนุญาต

2. ความมั่นคงของระบบสารสนเทศ

ความมั่นคงในที่นี้หมายถึง นโยบาย กระบวนงาน และวิธีทางเทคนิค ที่จะป้องกัน การเข้าถึงโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขโมย และความเสียหาย ฯลฯ ต่อระบบสารสนเทศ ความมั่นคงของระบบสารสนเทศนี้ สามารถจะเสริมสร้างโดยใช้เทคนิคและเครื่องมือต่างๆ เพื่อป้อง

กัน ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่ายสื่อสาร และ ข้อมูล

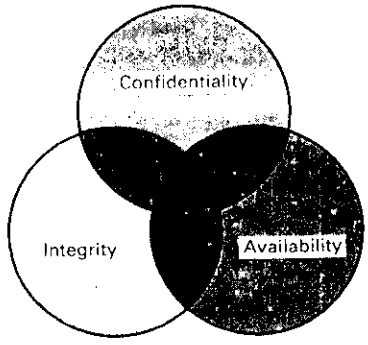
เป้าหมายของการรักษาความมั่นคงของระบบสารสนเทศ ประกอบด้วย การบำรุงรักษาลักษณะ 3 ประการ ได้แก่ ความเชื่อมั่น (Confidentiality) บูรณภาพ (Integrity) และ สภาพพร้อมใช้งาน (Availability) ดังรูป 9.5

ความเชื่อมั่น (Confidentiality) หมายถึง ทรัพย์สินของระบบคอมพิวเตอร์จะถูกเข้าถึงได้เฉพาะผู้ได้รับสิทธิเท่านั้น รูปแบบของการเข้าถึง เป็นการเข้าถึงในการอ่าน ได้แก่ การอ่าน (reading) การดู (viewing) การพิมพ์ (printing) หรือเป็นเพียงการรู้ว่ามีข้อมูล หรือมีสิ่งนั้นอยู่ในระบบ ในบางครั้งความเชื่อมั่นนี้อาจเรียกว่า ความลับ (Secrecy) หรือ ภาวะส่วนตัว (Privacy)

บูรณภาพ (Integrity) หมายถึง ทรัพย์สินของระบบคอมพิวเตอร์ สามารถได้รับการปรับปรุงเฉพาะจากผู้มีอำนาจ หรือ ผู้ที่มีสิทธิ หรือ ได้รับการปรับปรุงเฉพาะในรูปแบบที่ได้รับสิทธิเท่านั้น การปรับปรุงในที่นี้ รวมถึง การเขียน การเปลี่ยนแปลง การเปลี่ยนสถานะ การลบ และ การสร้าง

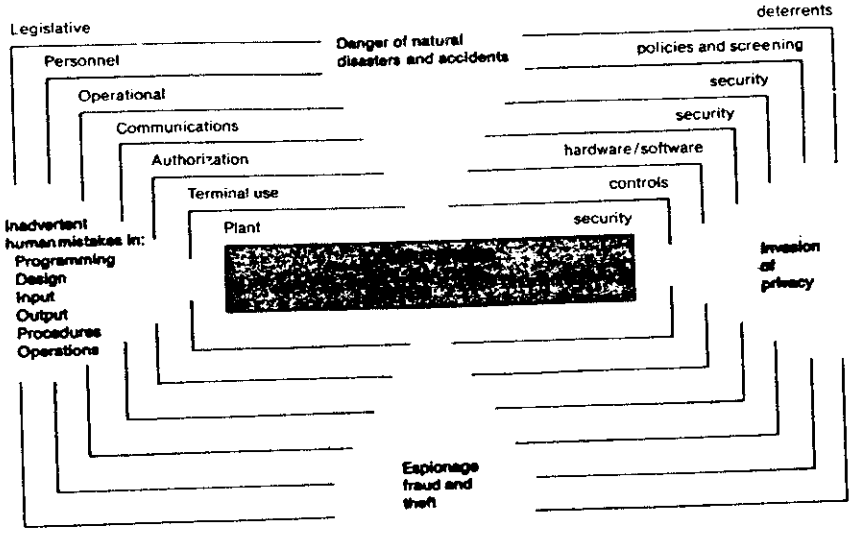
คำว่าบูรณภาพ มีความหมายได้หลากหลาย เช่น ความถูกต้อง การไม่เปลี่ยนแปลง การเปลี่ยนแปลงเฉพาะในรูปแบบที่ได้รับการยอมรับ การเปลี่ยนแปลงเฉพาะจากผู้ที่มีสิทธิ การเปลี่ยนแปลงจากเฉพาะกระบวนงานที่ได้รับอนุญาต ความต้องกัน (Consistency) ความต้องกันภายในผลลัพธ์ที่มีความหมายและถูกต้อง เป็นต้น

สภาพพร้อมใช้งาน (Availability) หมายถึง ทรัพย์สินของระบบคอมพิวเตอร์พร้อมให้ผู้ที่ได้รับอนุญาต เข้าถึงได้ ผู้ที่ได้รับอนุญาตไม่ควรจะถูกขัดขวางจากการเข้าถึงส่วนใดๆ ของระบบที่บุคคลนั้นได้รับสิทธิในการเข้าถึง สภาพพร้อมใช้งานนี้ในบางครั้งเป็นที่เข้าใจในทางตรงกันข้าม คือ การปฏิเสธในการบริการ ความหมายของสภาพพร้อมใช้งานนี้ มีความหลากหลาย เช่น การมีอยู่ของวัตถุ หรือ บริการในรูปแบบที่ใช้งานได้ มีกำลังความสามารถที่ตอบสนองต่อความต้องการได้ การให้เวลาอย่างพอเพียง หรือ การให้บริการอย่างถูกเวลา อย่างเหมาะสม เป็นต้น ดังนั้นเป้าหมายของสภาพพร้อมใช้งาน คือ การตอบสนองอย่างทันเวลา การจัดสรรอย่างเหมาะสม ทนต่อความผิดพร่อง (Fault tolerance) และ การใช้งานได้



รูป 9.5 ความสัมพันธ์ระหว่างความเชื่อมั่น (Confidentiality) บูรณภาพ (Integrity และ สภาพพร้อมใช้งาน (Availability)

การออกแบบระบบความปลอดภัยเพื่อป้องกันระบบสารสนเทศจากภัยคุกคามรูปแบบต่างๆ โดยกำหนดการควบคุมเป็นลำดับขั้น ดังรูป 9.6



รูป 9.6 ลำดับขั้นของการควบคุม

2.1 ความปลอดภัยของสถานที่

การป้องกันและรักษาความปลอดภัยหลายรูปแบบสามารถกำหนดตั้งแต่ในขั้นการก่อสร้าง หรือ การต่อเติมเปลี่ยนแปลงอาคาร เพื่อป้องกันระบบคอมพิวเตอร์จากการบุกรุกแบบผิดกฎหมาย การถูกทำลายจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ตัวอย่างเช่น การติดระบบล๊อคที่ประตู หน้าต่าง ติดตั้งปุ่มสัญญาณเตือนภัย การติดตั้งอุปกรณ์ตรวจจับควัน หรือ อุปกรณ์ดับไฟอัตโนมัติ

2.2 การควบคุมการเข้าถึงและใช้งานระบบ

ในกรณีที่อุปกรณ์ต่างๆ อยู่ที่ศูนย์คอมพิวเตอร์ การควบคุมการเข้าถึงวิธีการหนึ่งก็คือ การควบคุมไม่ให้บุคคลที่ไม่มีสิทธิเข้ามาใช้งาน เข้ามาในบริเวณศูนย์คอมพิวเตอร์ วิธีการต่างๆ ที่ช่วยป้องกันผู้ที่ไม่มีสิทธิ ได้แก่ ล๊อคประตู รั้วไฟฟ้า สุนัขเฝ้ายาม จุดตรวจ เป็นต้น

สำหรับในระบบเชื่อมตรง ซึ่งใช้การสื่อสารทางไกล ความมั่นคงของระบบเป็นปัญหาที่ใหญ่ และยุ่งยากกว่า เพราะไม่สามารถควบคุมการเข้าถึงในจุดที่ใช้งานได้ ดังนั้นจึงต้องใช้การระบุตัวบุคคลที่จะเข้าใช้งาน และ บุคคลนั้นได้รับสิทธิในการใช้งานหรือไม่ การระบุ (Identification) สามารถใช้

1. ผู้ใช้มี หรือ ใช้อะไรในการระบุ เช่น บัตรประจำตัว กุญแจ
2. ผู้ใช้เป็นใคร เช่น การวัดทางชีวภาพ หรือ ลักษณะทางกายภาพ
3. ผู้ใช้รู้อะไร เช่น รหัสผ่าน (Password)

2.2.1 บัตร หรือ กุญแจ

การล๊อคเครื่องซึ่งต้องใช้กุญแจเปิดจึงจะสามารถใช้งานเครื่องได้ หรือการใช้บัตร เพื่อระบุผู้ใช้ โดยการเสียบบัตรที่เครื่องอ่านบัตร เมื่อผู้ใช้ต้องการใช้งาน รูปแบบของบัตรมีหลายรูปแบบ เช่น บัตรพลาสติก เป็นบัตรที่คล้ายบัตรเครดิต ซึ่งจะมีแถบแม่เหล็กติดอยู่ที่ด้านหน้า หรือ ด้านหลัง บัตรที่เรียกว่า Proximity card เป็นบัตรที่มีวงจรไฟฟ้าถูกประกบอยู่ภายใน เครื่องอ่านบัตรชนิดนี้ต้องมีทั้งตัวส่งผ่านสัญญาณ และ ตัวรับสัญญาณ บัตรแสง (Optical card) เป็นบัตรที่บรรจุข้อมูลในรูปของจุดแสง ซึ่งต้องใช้ลำแสงพิเศษในการอ่านข้อมูล เช่น แสงอินฟราเรด (Infrared light) บัตรเก่ง (Smart card) เป็นบัตรที่มีชิพวงจรรวมบรรจุอยู่ภายใน ชิพนี้จะมีหน่วยความจำบรรจุรายละเอียดของเจ้าของบัตร และ ไมโครโพรเซสเซอร์ ด้วย

ข้อเสียของการใช้บัตร หรือ กุญแจ คือ บัตร หรือ กุญแจ อาจสูญหาย ถูกขโมย หรือถูกปลอม ซึ่งทำให้ผู้ถือบัตรอาจไม่ได้เป็นเจ้าของบัตร หรือ ผู้ได้รับสิทธิที่แท้จริง เพราะบัตร หรือ

กุญแจ ไม่ได้สัมพันธ์โดยตรงกับผู้ถือ ดังนั้น จึงมักใช้รหัสผ่านควบคู่กับบัตร หรือกุญแจ ด้วย

2.2.2 ระบบการวัดทางกายภาพ (Biometric systems)

ระบบควบคุมการใช้งานอุปกรณ์บางระบบ ระบุผู้ใช้ โดยใช้การวัดลักษณะทางกายภาพของผู้ใช้ เช่น ใช้อุปกรณ์กราดตรวจ ตรวจสอบมือของผู้ใช้ แล้วทำการเปรียบเทียบกับข้อมูลของผู้ที่ได้รับอนุญาตใช้งานที่ทำการเก็บไว้ก่อนหน้านี้ ถ้าตรงกับข้อมูลที่มีการเก็บไว้ ก็จะอนุญาตให้เข้าใช้งาน

ตัวอย่างคุณลักษณะทางกายภาพที่นำมาใช้เพื่อระบุตัวบุคคล ได้แก่ ลายนิ้วมือ ม่านตา เส้นเลือดที่ผนังลูกตาดำ รูปพรรณสัณฐานของมือ โครงสร้างรูปหน้า นอกจากนี้ยังมีคุณลักษณะทางกายภาพอื่นๆ อีกที่ยังอยู่ระหว่างการศึกษาความเป็นไปได้ในการนำมาใช้งาน และพัฒนาเป็นทางเลือกใหม่ เช่น ลักษณะรอยย่นของข้อนิ้ว (Knuckle creases) คลื่นสมอง (Acoustic head resonance) หรือ กลิ่นตัว (Body orders)

ข้อมูลทางกายภาพของบุคคลต้องเป็นบันทึกจากบุคคลที่ยังมีชีวิตอยู่เท่านั้น โดยอุปกรณ์เก็บข้อมูลจะมีระบบตรวจสอบความมีชีวิตของบุคคลด้วย ซึ่งทำให้เทคโนโลยีนี้ต่างจากศาสตร์ทางด้านการชันสูตรศพ (Forensic science)

การใช้ลักษณะทางกายภาพถูกนำมาใช้เพื่อวัตถุประสงค์ในการทำความรู้จัก หรือ แยกแยะตัวบุคคล สามารถแบ่งการใช้งานออกเป็น 2 ส่วน คือ

1. บ่งชี้ความเป็นตัวจริง (Verification) เป็นการเปรียบเทียบข้อมูลไบโอเมตริกที่เก็บ ณ จุดใช้งาน กับข้อมูลของบุคคลนั้นที่เคยลงทะเบียนไว้ เพื่อพิสูจน์ว่าเป็นบุคคลนั้นจริง

2. เพื่อระบุว่าบุคคลนั้นเป็นใคร (Identification) เป็นการเปรียบเทียบข้อมูลไบโอเมตริกที่เก็บ ณ จุดใช้งาน กับข้อมูลไบโอเมตริก ทั้งหมดในฐานข้อมูล เพื่อพิสูจน์ว่าเป็นบุคคลที่เป็นเจ้าของข้อมูล

การใช้ลายนิ้วมือ หรือ ลายฝ่ามือ ในการระบุผู้ใช้ เป็นการใช้ระบบการรู้จำ และการจับคู่

การตรวจสอบลายเซ็น เป็นการตรวจวัดการเคลื่อนที่ของปลายปากกาสัมพันธ์กับเวลาที่ใช้ โดยใช้ปากกาลวด หรือ เซ็นบนแผ่นที่ไวต่อการรับสัญญาณ

การตรวจสอบเสียง โดยทำการบันทึกเสียงของผู้ใช้ในรูปสัญญาณแอนะล็อก (Analog) แล้วปรับเป็นสัญญาณดิจิทัล (Digital) เพื่อระบุถึงรูปแบบเสียงของผู้ใช้ที่ได้รับสิทธิ จากนั้นเมื่อผู้มีความต้องการใช้งาน ก็จะใช้กระบวนการจับคู่ เปรียบเทียบกับเสียงที่บันทึกไว้ในหน่วยความจำของระบบ

ระบบการควบคุมโดยลักษณะทางชีวภาพ เป็นระบบที่ได้รับความสนใจจากหลายๆ สาขา

อาชีพ เช่น ตำรวจ จึงเป็นเทคโนโลยีที่มีการพัฒนามาเป็นเวลาหลายปี ถึงแม้ว่าเทคโนโลยีมีความก้าวหน้า สามารถแจกแจงรูปแบบที่ซับซ้อนได้ก็ตาม ระบบการรู้จำแบบ (Pattern recognition) ก็ยังไม่ได้ปราศจากปัญหา คือ เมื่อเปรียบเทียบแล้วอยู่ในรูปแบบที่ต่ำกว่าเงื่อนไข ตัวอย่างเช่น มือซึ่งมีแผลพุพอง ถูกไฟไหม้ มีรอยบาด หรือ เหงื่อ จะรบกวนต่อการเปรียบเทียบลายนิ้วมือ หรือในการตรวจสอบเสียง ปัญหาด้านสุขภาพ และอารมณ์ ก็มีผลทำให้เสียงของผู้ใช้เปลี่ยนแปลงไปจากรูปแบบที่บันทึกไว้ ดังนั้น เพื่อลดปัญหานี้อาจใช้การตรวจสอบทางชีวภาพหลายรูปแบบเปรียบเทียบกัน เช่นวิเคราะห์ทั้งเสียง และ มือ แต่การแก้ปัญหานี้ทำให้เสียค่าใช้จ่ายที่สูงขึ้นตามไปด้วย (รายละเอียดเกี่ยวกับความเป็นส่วนตัว (Privacy) และ การบ่งชี้ด้วยลักษณะทางชีวภาพ (Biometric measure) ในภาคผนวก ง.)

2.2.3 รหัสผ่าน

การใช้รหัสผ่าน เป็นวิธีการหนึ่งที่ได้รับความนิยมสูง เช่น การใช้รหัสผ่านในการเข้าถึงระบบรับ-จ่ายเงินอัตโนมัติ (เอทีเอ็ม) (Automatic teller machine, ATM)

ปัญหาของการใช้รหัสผ่าน อยู่ที่การขาดความระมัดระวังในการใช้งานรหัสผ่านของผู้ใช้ เช่น ผู้ใช้จดรหัสผ่านเก็บไว้ในกระเป๋าเงิน หรือ เขียนไว้ที่เครื่อง หรือ กำหนดรหัสผ่านที่คาดเดาได้ง่าย เช่น วันเกิด เลขที่บ้าน ชื่อลูก ชื่อสัตว์เลี้ยง หรือ คำทั่วไป เช่น 'God' 'Genius' หรือแม้แต่รหัสผ่านที่มีความซับซ้อนที่ได้จากการสุ่มของเครื่องคอมพิวเตอร์ก็ตาม ก็ยังสามารถใช้เครื่องคอมพิวเตอร์ค้นหารหัสดังกล่าวได้

ทางเลือกทางหนึ่งในการแก้ปัญหาการล่วงรู้รหัสผ่าน คือ การใช้รหัสผ่านแบบใช้ครั้งเดียว (One - time password) โดยผู้ใช้ที่ได้รับอนุญาตแต่ละคนจะได้รับรายการของรหัสผ่านที่สุ่มเลือกมาแล้ว วิธีในการเลือกรหัสผ่านที่จะใช้ครั้งต่อไป จะต้องเป็นที่ตกลงกันระหว่างผู้ใช้แต่ละคนกับคอมพิวเตอร์ รายการรหัสผ่านที่สุ่มเลือกมาแล้วจะต้องถูกเก็บอย่างปลอดภัย ต่อมาได้มีการนำระบบรหัสผ่านอีกรูปแบบหนึ่งมาใช้ในท้องตลาด โดยทำการสร้างรหัสผ่านเฉพาะให้กับผู้ใช้แต่ละรายในแต่ละครั้งที่ผู้ใช้ต้องการเข้าถึงระบบ ลักษะการทำงานที่เกิดขึ้น คือ ที่หน่วยงานแม่ข่ายจะมีตัวควบคุมศูนย์กลาง และมีตัวสร้างรหัสผ่าน (Password generator) แบบสุ่มสำหรับผู้ใช้แต่ละราย จากนั้นระบบทำงานโดย เมื่อผู้ใช้ต้องการเข้าถึงเครื่องเมนเฟรม ผู้ใช้จะป้อนชื่อ หรือ รหัสประจำตัวผ่านทางแผงแป้นอักขระ (Keyboard) เครื่องจะให้ 'Challenge number' กลับมาให้ผู้ใช้ หมายเลขที่ได้กลับมานี้เป็นข้อมูลเข้าสำหรับตัวสร้างรหัสผ่านของผู้ใช้ เมื่อผู้ใช้ป้อนหมายเลขที่ได้รับเข้าไปสู่ตัว

สร้างรหัสผ่าน ตัวสร้างรหัสผ่านจะใช้อัลกอริทึมการเข้ารหัสลับ (Cryptographic algorithm) และกุญแจลับ (กลุ่มข้อมูลเฉพาะสำหรับตัวสร้างรหัสผ่านแต่ละตัว) ทำการสร้างรหัสผ่านแบบใช้ครั้งเดียว ผู้ใช้จึงนำรหัสผ่านที่ได้นี้ป้อนเข้าระบบอีกครั้ง ตัวควบคุมศูนย์กลางก็จะทำการคำนวณรหัสผ่านที่ถูกต้อง ถ้าตรงกันจึงอนุญาตให้ผู้ใช้เข้าถึงระบบได้

ระบบการจัดการรหัสผ่านดังกล่าวมีความยุ่งยาก เพราะรหัสผ่านถูกเปลี่ยนแปลงในทันที มีช่วงระยะเวลาเพียงสั้นๆ ที่จะต้องป้อนรหัสผ่านที่ถูกต้องเข้าไป นอกจากนี้ระบบควบคุมยังเป็นระบบที่ขึ้นกับโพรโทคอล (Protocol) ซึ่งเป็นปัญหาต่อผู้ใช้ที่พยายามเข้าระบบในเครือข่ายที่มีโพรโทคอลแตกต่างกัน ส่วนข้อดีต่อผู้ใช้คือ ตัวสร้างรหัสผ่านสามารถพกพาไปใช้งานในที่ต่างๆ สะดวก และง่ายต่อการใช้งาน

2.3 การควบคุมการให้สิทธิในการใช้งาน

นอกเหนือจากระบบที่ระบุผู้ใช้งานแล้ว ยังมีระบบควบคุมที่ติดตั้งเพื่อตรวจสอบว่าผู้ใช้ได้รับสิทธิในการเข้าถึงแฟ้ม และฐานข้อมูล หรือไม่ และสิทธิในการเข้าถึงของผู้ใช้อยู่ในระดับใด เช่น สิทธิในการอ่าน การเขียน หรือ การปรับปรุงข้อมูล

2.3.1 สารบบข้อมูล (Data directory)

คอมพิวเตอร์สามารถถูกโปรแกรมให้อ้างถึงแมทริกซ์ความปลอดภัยสารบบข้อมูล (Data directory security matrix) เพื่อกำหนดรหัสความปลอดภัยที่ใช้ในการเข้าถึงส่วนย่อยข้อมูลเฉพาะที่อยู่ในแฟ้มก่อนที่จะประมวลงานของผู้ใช้ ถ้าผู้ใช้ไม่สามารถระบุระดับการเข้าถึง และใช้งาน ให้ชัดเจน ระบบก็จะปฏิเสธการเข้าถึงของผู้ใช้

คอมพิวเตอร์อาจถูกโปรแกรมให้อ้างถึงตารางที่ระบุระดับการเข้าถึง หรือ ช่วงเวลาที่อนุญาตให้เข้าถึง เช่น เครื่องที่ผู้บริหารฐานข้อมูลใช้งานเป็นเครื่องเดียวที่ได้รับสิทธิในการเข้าถึงแฟ้มและโปรแกรมทั้งหมด และเป็นเครื่องเดียวที่สามารถเข้าถึงแมทริกซ์ระบบรักษาความปลอดภัย ดังตาราง 9.7

ตาราง 9.7 สารบบการเข้าถึง

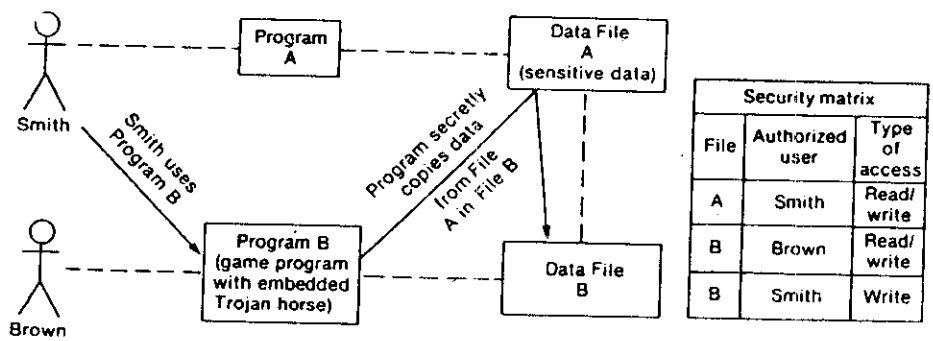
User identification: *076–835–5623*
Access limitation: *13 hours (of CPU time for current fiscal year)*
Account Number: *A55842*

Data elements	*Type of access*	*Security level*	*Terminal number*	*Time lock*
Customer number	Read	10	04	08 00–17 00
Invoice number	Read	10	04	08 00–17 00
Cash receipt	Read/write	12	06	08 00–12 00

การกำหนดระดับในการเข้าถึงของบุคลากรแต่ละคนในองค์กรเป็นงานที่ยาก เพราะข้อมูลและสารสนเทศเป็นสิ่งที่สำคัญ มีค่า และสามารถถูกนำไปใช้งานได้หลากหลาย ตลอดจนสิทธิในการเข้าถึงเป็นสัญลักษณ์ที่บ่งบอกสถานะของบุคลากรด้วย ซึ่งทำให้พนักงานอยากได้สิทธิในการเข้าถึง ถึงแม้ว่าจะไม่มีความจำเป็น หรือความต้องการใช้งานข้อมูลเหล่านั้น ผู้กำหนดระดับในการเข้าถึงจึงมักต้องตระหนักว่า การออกแบบระบบรักษาความปลอดภัยเพื่อป้องกันข้อมูลที่เป็นความลับ และทรัพยากรคอมพิวเตอร์ที่มีค่านั้นอาจมีผลทำให้พนักงานในองค์กรเกิดความขัดแย้ง หรือมีปัญหาต่อกัน

2.3.2 ใจกลางระบบความปลอดภัย (Security kernel)

สำหรับในระบบผู้ใช้หลายคน (Multiuser system) ข้อมูลในแฟ้มสามารถถูกลักลอบนำไปใช้งานได้โดยการติดตั้งโปรแกรมม้าโทรจัน การดำเนินงานของโปรแกรมนี้ แสดงดังรูป 9.8



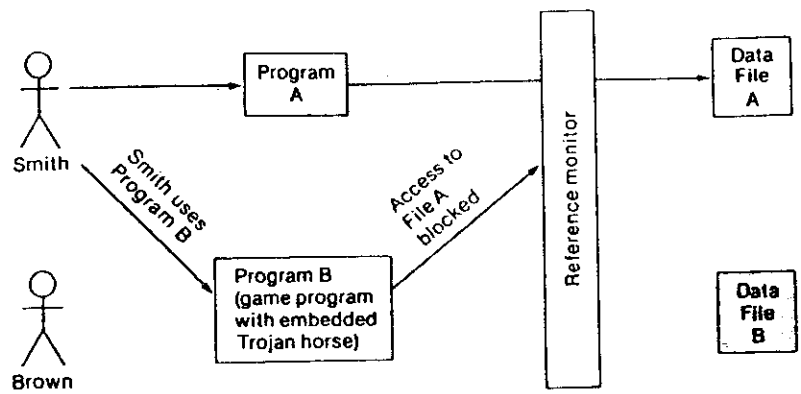
รูป 9.8 การลักลอบนำข้อมูลไปใช้งานโดยโปรแกรมม้าโทรจัน

จากรูป 9.8 สมมติว่า Smith ได้รับสิทธิการเข้าถึงข้อมูลในแฟ้ม A แบบอ่าน/เขียนได้ ในขณะที่ Brown ต้องการเข้าถึงแฟ้ม A เช่นกัน แต่ไม่ได้รับสิทธินั้น Brown สามารถเข้าถึงระบบได้เท่านั้น Brown จึงสร้างแฟ้ม B ขึ้น ซึ่ง Brown มีสิทธิในการอ่าน/เขียนแฟ้ม B นี้ และกำหนดรายการควบคุมการเข้าถึงเพื่อยินยอมให้โปรแกรมที่ Smith ใช้งานสามารถที่จะเขียนลงบนแฟ้ม B ได้ (โดย Smith ไม่ได้รับการบอกกล่าวเกี่ยวกับสถานการณ์นี้)

จากนั้น Brown จะสร้างโปรแกรมซึ่งคาดว่า Smith จะเข้ามาใช้งาน เช่น โปรแกรมเกมส์

โปรแกรมนี้จะซ่อนคำสั่งลับ หรือ ม้าโทรจันไว้ เพื่อให้คอมพิวเตอร์ทำสำเนาแฟ้มข้อมูลจากแฟ้ม A แล้วเขียนข้อมูลนั้นลงบนแฟ้ม B ในขณะที่ Smith เล่นเกมส์ (โปรแกรมม้าโทรจันที่ได้รับการออกแบบให้สามารถตรวจพบได้ว่า Smith เป็นผู้ใช้งาน) แมทริกซ์ระบบรักษาความปลอดภัยไม่สามารถหลีกเลี่ยงการจู่โจมนี้ เพราะ Smith ได้รับสิทธิการเข้าถึงแฟ้ม A ดังนั้นถึงแม้ว่าสารบบจะไม่ให้สิทธิ Brown ในการเข้าถึงแฟ้ม A แต่ข้อมูลลับจากแฟ้ม A สามารถถูกทำสำเนาไปยังอีกแฟ้มหนึ่ง ซึ่ง Brown ได้รับสิทธิในการเข้าถึง รูปแบบดังกล่าวทำให้สามารถหลีกเลี่ยงระบบรักษาความปลอดภัยได้

แต่แนวคิดในเรื่องใจกลางระบบความปลอดภัย เป็นแนวคิดที่พัฒนาเพื่อแก้ไขโปรแกรมม้าโทรจัน 'ใจกลาง' นี้หมายถึงกลไกฮาร์ดแวร์/ซอฟต์แวร์ ซึ่งใช้ตัวเฝ้าสังเกตอ้างอิง (Reference monitor) ตัวเฝ้าสังเกตอ้างอิงนี้เป็นองค์ประกอบระบบที่ตรวจสอบการอ้างอิงแต่ละรายการ โดยตรวจสอบ ผู้ใช้ หรือ โปรแกรม กับ เป้าหมายที่ผู้ใช้ หรือ โปรแกรมเข้ามาใช้งาน ได้แก่ แฟ้ม อุปกรณ์ หรือโปรแกรม พร้อมทั้งระบุว่าการเข้าถึงนั้นถูกต้องตามนโยบายการรักษาความปลอดภัยของระบบหรือไม่ ดังรูป 9.9



รูป 9.9 ตัวเฝ้าสังเกตอ้างอิงสกัดการจู่โจมของโปรแกรมม้าโทรจัน

จากรูป 9.9 สมมติว่าการรักษาความปลอดภัยมี 2 ระดับ ระดับแรกยินยอมการเข้าถึงข้อมูลสำคัญ (Data file A) อีกระดับยินยอมการเข้าถึงเฉพาะข้อมูลที่ไม่สำคัญ (Data file B) ตัวเฝ้าสังเกต

ความปลอดภัยดำเนินตามกฎเกณฑ์ที่ระบุว่า ผู้ใช้ หรือโปรแกรมไม่สามารถจะอ่านแฟ้มในระดับความปลอดภัยที่สูงกว่า และไม่สามารถเขียนลงบนแฟ้มที่มีระดับความปลอดภัยที่ต่ำกว่า

เนื่องจาก Smith Program A และ File A มีระดับความปลอดภัยสูง Smith สามารถเข้าถึงแฟ้ม A ในขณะที่ Brown ไม่สามารถทำได้ เมื่อ Smith ซึ่งไม่ทราบถึงกลไกโปรแกรมม้าโทรจันที่ Brown ใส่ไว้ โปรแกรมจะเข้ายึดระดับความปลอดภัยของ Smith อย่างไรก็ตามตัวเฝ้าสังเกตอ้างอิงจะปิดกั้นคอมพิวเตอร์จากการใช้คำสั่งจู่โจม เพราะแฟ้ม B มีระดับความปลอดภัยต่ำกว่าแฟ้ม A

2.3.3 เครื่องเสมือน (Virtual Machine)

เป็นแนวคิดต่อการรักษาความปลอดภัยสำหรับสภาพแวดล้อมผู้ใช้หลายคน ที่แตกต่างไปจากเดิม ด้วยโครงสร้างระบบนี้ ผู้ใช้แต่ละรายจะบรรจุ และใช้งานสำเนาระบบปฏิบัติการของตนเอง ผลที่เกิดขึ้น คือ เป็นการแยกผู้ใช้แต่ละรายออกจากกลุ่มผู้ใช้ ถึงแม้ว่าจะเป็นการใช้อุปกรณ์เครื่องจักรเดียวกันทางกายภาพ เพราะเครื่องเสมือนแต่ละเครื่องสามารถถูกดำเนินการในระดับความปลอดภัยที่แตกต่างกัน

2.4 ความปลอดภัยในการปฏิบัติงาน

วิธีการควบคุมเพื่อป้องกันระบบสารสนเทศในระหว่างการประมวลผลได้กล่าวไว้ในบทที่ 10 สำหรับในส่วนนี้จะย้ำเน้นถึงกลยุทธการบริหารทั่วไปเพื่อป้องกันระบบโดยรวม เช่น ในระหว่างการเปลี่ยนระบบ คือหลังจากที่ระบบใหม่ผ่านการทดสอบเพื่อยอมรับ (Acceptance test) และพร้อมที่จะปฏิบัติงาน ระบบจะเกิดความอ่อนแอไม่มั่นคงต่อการบุกรุก เพราะพนักงานซึ่งขาดประสบการณ์กับระบบใหม่ จะไม่ตระหนักถึงการละเมิดต่อความปลอดภัยระบบ ในขณะเดียวกันช่างเทคนิค ซึ่งกำลังเหนื่อยอ่อนต่อการเปลี่ยนแปลงไปสู่ระบบใหม่ ก็จะมีความเอาใจใส่ในเรื่องความปลอดภัยต่ำกว่าปกติ ผลก็คืออาจเกิดการเปลี่ยนแปลงกระบวนงาน ข้อมูล และ โปรแกรมโดยไม่มีผู้ล่วงรู้ หรือสังเกตเห็น ดังนั้นในระหว่างการเปลี่ยนระบบ ผู้มีประสบการณ์จึงให้คำแนะนำว่าควรเพิ่มระดับความปลอดภัยให้สูงขึ้นในขั้นตอนนี้

สำหรับการปฏิบัติงานในแต่ละวัน ก็ต้องระมัดระวังในการตรวจสอบบันทึก รายงาน หรือพฤติกรรมที่ผิดปกติ กิจการโดยส่วนใหญ่จะกำหนดตารางการตรวจสอบการทำงานเป็นระยะๆ ด้วย (รายละเอียดในบทที่ 10) บางกิจการอาจว่าจ้างนักสืบเอกชนเพื่อตรวจสอบความปลอดภัย ถึงแม้ว่าการกระทำดังกล่าวอาจส่งผลในทางลบต่อขวัญกำลังใจของพนักงานก็ตาม ยิ่งไปกว่านั้นมีรายงาน

กล่าวถึงบางกรณีที่กิจการทำการว่าจ้างบุคคลซึ่งติดทัณฑ์บน ข้อหาการใช้โปรแกรมในการฉ้อโกง หรือทำผิดกฎหมาย มาสร้าง พัฒนา ตรวจสอบระบบรักษาความปลอดภัยของกิจการ เพราะ บุคคลที่รู้ว่าจะทำลายระบบได้อย่างไรนั้น จะรู้ว่าควรจะป้องกันระบบได้อย่างไรด้วย

แต่อย่างไรก็ตามการติดตั้งระบบรักษาความปลอดภัยที่ดีที่สุด ก็ไม่สามารถหลีกเลี่ยงความเสียหายที่เกิดจากภัยธรรมชาติ และ ผู้ประสงค์ร้ายก็ใช้อุบายเล็ดลอดการควบคุมบ่อยจนเกินกว่าจะรับประกันได้ว่าจะมีภูมิคุ้มกันระบบต่อการคุกคามเหล่านั้น ส่วนหนึ่งที่ช่วยลดทอนความเสียหายทางการเงินในบางกรณี คือ การทำประกัน แต่ส่วนสำคัญของการรักษาความปลอดภัยในการปฏิบัติงาน คือ การวางแผนสำหรับ การกู้คืน (Recovery) สิ่งที่สูญเสีย สูญหาย ไม่ว่าจะเป็นข้อมูล โปรแกรม หรือ ฮาร์ดแวร์ และทำให้ระบบสามารถกลับสู่การทำงานได้อย่างรวดเร็ว สิ่งนี้เป็นความรับผิดชอบของผู้จัดการ ผู้บริหารโดยผู้ขายอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ต่างๆ สามารถให้การสนับสนุนในด้านคู่มือ รายการตรวจสอบ เพื่อช่วยในการวางแผนการสร้างใหม่ หรือการกู้ระบบ

ในการวางแผนว่าควรดำเนินกระบวนงานใดบ้างเมื่อเกิดความเสียหาย หรือ เมื่อระบบหยุดทำงาน ฝ่ายบริหารต้อง

- กำหนดโครงแบบทรัพยากรขั้นต่ำที่จำเป็นต่อการปฏิบัติงาน
- ระบุว่าบันทึก ข้อมูลใดมีความสำคัญ
- กำหนดลำดับความสำคัญของงาน (กำหนดกำลังความสามารถในการทำงานที่ลดลง งานใดที่ต้องผ่านการประมวลผล เวลาครบวงงานใดบ้างที่สำคัญ)
- มอบหมายความรับผิดชอบในการกู้คืน (กำหนดว่าใครเป็นผู้ที่มีอำนาจในการเคลื่อนย้ายทรัพยากรขององค์กร)

ในกรณีที่สถานที่ อุปกรณ์ในการทำงานเกิดความเสียหายอย่างหนัก ต้องวางแผนเกี่ยวกับการกำหนดสถานที่สำรอง ซึ่งไม่ควรจะอยู่ในจุดเดียวกัน เพราะการกำหนดระบบสำรองไว้ในอาคารหรือสถานที่เดียวกัน อาจเกิดความเสียหายพร้อมกันทั้ง 2 ที่ แต่การกำหนดสถานที่สำรองห่างไกลออกไปจากที่เดิม ก็เป็นการเพิ่มความยากลำบากในการติดต่อสื่อสารเข้ากับปัญหาในการกู้คืนระบบ กิจการซึ่งมีการประมวลผลแบบกระจายโดยทั่วไปจะยังคงสามารถทำงานได้ถ้าการเชื่อมต่อเครือข่ายหนึ่งหยุดทำงาน ส่วนกิจการซึ่งใช้ระบบรวมศูนย์จำเป็นต้องมีสถานที่ทำงานสำรองไว้ แนวทางแก้ไขแนวทางหนึ่งคือ ทำข้อตกลงช่วยเหลือซึ่งกันและกันกับกิจการอื่น โดยกิจการที่เป็นคู่สัญญากันตกลงที่จะยอมรับภาระงานเพิ่มมากขึ้น (เช่น ทำงานเป็น 3 ช่วง) เมื่อคู่สัญญาเกิดความจำเป็น ในกรณีของการทำข้อตกลงกับกิจการอื่นนั้น ต้องแก้ปัญหาเกี่ยวกับความเข้ากันของระบบของทั้ง 2 กิจ-

การ และต้องดูแลรักษาแฟ้มสำรองสำหรับสถานที่สำรองด้วย

ผู้ตรวจสอบบางคนแนะนำว่าควรมีการทดสอบเพื่อตรวจสอบประสิทธิภาพของการวางแผนต่อความเสียหาย เข้าเป็นส่วนหนึ่งของกระบวนงานในการตรวจสอบปกติด้วย ทุกๆ กิจการควรมีการวางแผนสำหรับดำเนินการเมื่อระบบหยุดทำงาน และพนักงานควรจะได้รับทราบถึงขั้นตอนที่ควรทำเมื่อเกิดเหตุฉุกเฉินขึ้น อาจทำเป็นบันทึกช่วยจำ หรือเป็นคู่มืออย่างละเอียด ขึ้นกับสภาพและความซับซ้อนของธุรกิจ

2.5 ความปลอดภัยในสภาพการใช้งานไมโครคอมพิวเตอร์

ถึงแม้ว่าสำหรับการใช้งานไมโครคอมพิวเตอร์จะมีปริมาณข้อมูลน้อยกว่าการใช้งานเครื่องเมนเฟรม แต่ก็ยังจำเป็นต้องป้องกันการสูญหายของข้อมูลทั้งด้วยเจตนา หรือ โดยความบังเอิญ มาตรการที่กล่าวมาสามารถใช้ได้ทั้งสภาวะแวดล้อมสำหรับไมโครคอมพิวเตอร์และสภาพการใช้เครื่องเมนเฟรม และเครื่องมินิคอมพิวเตอร์

อย่างไรก็ตามมีองค์ประกอบหลายประการที่เป็นปัญหาเฉพาะต่อการใช้เครื่องไมโครคอมพิวเตอร์ เช่น ผู้ใช้เครื่องไมโครคอมพิวเตอร์จำนวนมาก ไม่ใช่บุคลากรทางด้านคอมพิวเตอร์ ทำให้ขาดความตระหนักถึงการรักษาความปลอดภัย หรือ ไม่มีการวางแผนรองรับสถานการณ์ฉุกเฉิน หรือ ขาดกระบวนงานสำรอง หรือ ไม่มีการเตรียมหลักฐานการทดสอบ เป็นต้น

นอกจากนี้ทั้งฮาร์ดแวร์ และซอฟต์แวร์ของไมโครคอมพิวเตอร์ก็ง่ายต่อการขโมย หรือลักลอบใช้งาน ดังนั้นจึงควรเก็บข้อมูล โปรแกรม ในสื่อเก็บที่พกพาได้ เพื่อเก็บไว้ในที่ปลอดภัย ใช้ล็อค กุญแจ รหัสผ่าน การเข้ารหัส (Encryption) ฯลฯ เพื่อช่วยในการรักษาความปลอดภัย

3. สภาพแวดล้อมในการควบคุม

การควบคุมประกอบด้วย วิธีการ นโยบาย และ กระบวนงานทางองค์กร ที่ทำให้เกิดความมั่นใจในความปลอดภัยของทรัพย์สินองค์กร ความถูกต้องและความน่าเชื่อถือของข้อมูล และการปฏิบัติงานที่เป็นมาตรฐาน

ในอดีตที่ผ่านมาการควบคุมระบบสารสนเทศถูกดำเนินการในขั้นตอนท้ายๆ คือก่อนที่จะเริ่มใช้งานระบบ ก่อนที่จะติดตั้งระบบ แต่ในปัจจุบัน เมื่อคนเริ่มตระหนักถึงความสำคัญของสารสนเทศ และต้องพึ่งพาใช้งานระบบสารสนเทศ ทำให้ประเด็นการควบคุมถูกดำเนินการเป็นส่วนหนึ่งในขั้นตอนการออกแบบระบบ ระบบคอมพิวเตอร์ถูกควบคุมโดย 2 ส่วนร่วมกัน คือ การควบคุมทั่วไป และ การควบคุมงานประยุกต์

3.1 การควบคุมทั่วไป

หมายถึงการควบคุมการออกแบบ การรักษาความปลอดภัย การใช้งานโปรแกรมคอมพิวเตอร์ และความปลอดภัยของแฟ้มข้อมูลโดยทั่วไปทั้งองค์กร โดยภาพรวมแล้วการควบคุมทั่วไปใช้กับงานประยุกต์ที่ใช้งานระบบคอมพิวเตอร์ทั้งหมด การประสานระหว่างซอฟต์แวร์ระบบ และกระบวนงานในแบบที่ใช้แรงงาน

การควบคุมทั่วไป คือ การควบคุมทั้งหมดที่ให้เกิดความมั่นใจในประสิทธิภาพของการปฏิบัติงานของกระบวนงานที่ได้รับการโปรแกรม การควบคุมทั่วไป ได้แก่

3.1.1 การควบคุมในการนำระบบไปใช้งาน

เป็นการตรวจสอบกระบวนการพัฒนาระบบในขั้นตอนต่างๆ เพื่อให้เกิดความมั่นใจว่ากระบวนการต่างๆ ได้รับการควบคุม และการจัดการอย่างเหมาะสม การตรวจสอบการพัฒนาระบบควรเป็นการค้นหาจุดที่ควรได้รับการทบทวนในขั้นตอนต่างๆ ของการพัฒนา ซึ่งช่วยให้ผู้ใช้ และฝ่ายบริหาร สามารถยอมรับ หรือ ไม่ยอมรับ กับการนำระบบไปใช้งาน

การตรวจสอบการพัฒนาระบบควรพิจารณาระดับความเกี่ยวข้องของผู้ใช้ในแต่ละขั้นตอน และตรวจสอบการใช้วิธีวิเคราะห์ทางการเงินในขั้นการศึกษาความเป็นไปได้ ตลอดจนค้นหาการใช้เทคนิคในการควบคุม และประเมินคุณภาพ ในการพัฒนาโปรแกรม การเปลี่ยนจากระบบเก่าไปสู่ระบบใหม่ การทดสอบ และ การจัดทำเอกสารประกอบระบบ เอกสารสำหรับผู้ใช้ และเอกสารในการปฏิบัติงาน

3.1.2 การควบคุมซอฟต์แวร์

เป็นการเฝ้าสังเกตการใช้งานซอฟต์แวร์ระบบ และป้องกันการเข้าถึงโปรแกรมซอฟต์แวร์ซอฟต์แวร์ระบบ โดยไม่ได้รับอนุญาต ซอฟต์แวร์ระบบเป็นจุดควบคุมที่สำคัญ เพราะเป็นส่วนที่ทำหน้าที่ควบคุมโปรแกรมทั้งหมดซึ่งทำหน้าที่ประมวลผลข้อมูล และแฟ้มข้อมูลโดยตรง

3.1.3 การควบคุมฮาร์ดแวร์

เป็นการทำให้เกิดความมั่นใจว่าฮาร์ดแวร์ได้รับการดูแลความปลอดภัย และมีการตรวจสอบการทำงานที่ผิดปกติของฮาร์ดแวร์ ฮาร์ดแวร์ต้องได้รับการดูแลรักษาความปลอดภัยจากการเข้าถึงโดยเฉพาะผู้ได้รับสิทธิเท่านั้น ตลอดจนได้รับการป้องกันจากไฟไหม้ อุณหภูมิเกินเกณฑ์ปกติ และ

ความชื้น องค์กรที่พึ่งพาใช้งานอุปกรณ์คอมพิวเตอร์เป็นหลักต้องมีระบบสำรองสำหรับกรณีฉุกเฉินที่อาจเกิดขึ้น

3.1.4 การควบคุมการปฏิบัติงาน

เป็นการควบคุมการปฏิบัติงานของแผนกคอมพิวเตอร์ และช่วยให้เกิดความมั่นใจว่ากระบวนงานที่โปรแกรมไว้สำหรับเก็บและประมวลผลข้อมูลเป็นไปอย่างถูกต้องและแน่นอน การควบคุมการปฏิบัติงานนี้ครอบคลุมถึงการจัดเตรียมงานที่จะประมวลผล ซอฟต์แวร์ปฏิบัติงานและกระบวนงานในการทำสำรองและกู้คืนการประมวลผลที่ผิดปกติ

ผู้ที่รับผิดชอบกับการควบคุมการปฏิบัติงานจะต้องจัดทำเอกสารเกี่ยวกับคำสั่งในการให้คอมพิวเตอร์ทำงาน มีการทบทวน และ ให้การยอมรับ การควบคุมซอฟต์แวร์ปฏิบัติการจะรวมถึง การออกแบบกระบวนงานในส่วนที่ใช้แรงงานทั้งเพื่อป้องกันและตรวจหาข้อผิดพลาด ตลอดจนพัฒนาคำสั่งพิเศษสำหรับการทำสำรอง และการกู้คืน เพื่อที่เมื่อฮาร์ดแวร์ หรือ ซอฟต์แวร์ ไม่ทำงาน หรือ ทำงานผิดพลาด กระบวนการกู้คืนสำหรับโปรแกรมการผลิต ซอฟต์แวร์ระบบ และแฟ้มข้อมูล จะไม่สร้างการเปลี่ยนแปลงที่ผิดพลาดในระบบ

3.1.5 การควบคุมความปลอดภัยของข้อมูล

เพื่อให้เกิดความแน่ใจว่า แฟ้มข้อมูลที่มีค่าทางธุรกิจไม่ว่าจะเป็นข้อมูลที่อยู่บนจานแม่เหล็ก หรือ เทปแม่เหล็ก จะไม่ถูกเข้าถึง เปลี่ยนแปลง หรือ ทำลาย โดยไม่ได้รับอนุญาต การควบคุมนี้ต้องดำเนินการทั้งกับแฟ้มข้อมูลที่กำลังใช้งาน และเมื่อแฟ้มข้อมูลเหล่านั้นถูกเก็บไว้เพื่อการใช้งาน

เมื่อข้อมูลสามารถจะถูกนำเข้าโดยตรงผ่านเครื่องปลายทาง จึงต้องมีการป้องกันการนำเข้าข้อมูลที่ไม่ได้รับอนุญาต ตัวอย่างเช่น ใบลดหนี้สามารถถูกเปลี่ยนให้ตรงกับใบกำกับการขายในแฟ้ม ในกรณีเช่นนี้ ต้องมีการพัฒนาระบบรักษาความปลอดภัยหลายระบบ ได้แก่

- จำกัดการเข้าใช้เครื่อง เพื่อให้พนักงานเฉพาะผู้ที่ได้รับอนุญาตเข้าใช้งานเท่านั้น
- การให้รหัสผ่านกับเฉพาะผู้ที่ได้รับสิทธิในการใช้งานซอฟต์แวร์ ผู้ที่ไม่มีรหัสผ่านจะไม่สามารถเข้าสู่ระบบได้
- พัฒนากลุ่มรหัสผ่าน และเข้มงวดกับการรักษาความปลอดภัยสำหรับระบบ และงานประยุกต์เฉพาะงาน เช่น ซอฟต์แวร์รักษาความปลอดภัยของข้อมูลสามารถจำกัดการเข้าถึงแฟ้มเฉพาะบางแฟ้ม เช่น แฟ้มสำหรับระบบบัญชีลูกหนี้ สามารถจำกัดรูปแบบการเข้า

ถึงเพื่อที่จะให้เฉพาะผู้ได้รับอนุญาตเท่านั้นที่จะสามารถปรับข้อมูลในแฟ้มเฉพาะเหล่านี้ได้ บุคคลอื่นอาจได้รับสิทธิเฉพาะการอ่านข้อมูล หรือ อาจจะถูกปฏิเสธการเข้าถึงแฟ้มเฉพาะเหล่านั้น

แบบต่างๆ ที่ยินยอมให้มีการสอบถามข้อมูล หรือ การรายงานโดยตรง ต้องมีการรักษาความปลอดภัยของแฟ้มข้อมูล ดังรูป 9.10

Employee Identification
Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2
User: Divisional Personnel Manager

Location: Division 1

Employee Identification
Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

รูป 9.10 ตัวอย่างการรักษาความปลอดภัยในระบบบุคลากร

จากรูป 9.10 แสดงถึงการรักษาความปลอดภัยที่ให้กลุ่มผู้ใช้ 2 กลุ่ม ที่เข้าใช้ฐานข้อมูล

บุคลากรแบบเชื่อมตรง โดยข้อมูลในฐานข้อมูลบางส่วน เป็นข้อมูลส่วนบุคคลที่ไม่ควรเปิดเผย หรือควรเก็บเป็นความลับ เช่น เงินเดือน ผลตอบแทน ประวัติทางการแพทย์ กลุ่มผู้ใช้กลุ่มแรกเป็นพนักงานที่ทำหน้าที่ปฏิบัติงานกับข้อมูล เช่น นำเข้าข้อมูลพนักงานเข้าสู่ระบบ พนักงานเหล่านี้สามารถจะปรับปรุงระบบให้เป็นปัจจุบัน แต่จะไม่สามารถอ่าน หรือ ปรับเปลี่ยนข้อมูลลับ เช่น เงินเดือน ประวัติทางการแพทย์ ข้อมูลผลประโยชน์ กลุ่มผู้ใช้กลุ่มที่ 2 ได้แก่ ผู้จัดการแผนก กลุ่มนี้จะถูกกำหนดให้ไม่สามารถปรับข้อมูล แต่สามารถอ่านข้อมูลทั้งหมดของพนักงานในแผนก ซึ่งรวมทั้งเงินเดือน ประวัติทางการแพทย์ ด้วย ดังนั้นในทั้ง 2 กรอบ ในการรักษาความปลอดภัยจะได้รับการกำหนด และดูแลรักษา โดยระบบรักษาความปลอดภัยข้อมูล

3.1.6 การควบคุมในทางการบริหาร

เป็นมาตรฐาน กฎเกณฑ์ กระบวนงาน และ การควบคุมวินัย เพื่อให้เกิดความมั่นใจว่า การควบคุมทั่วไป และ การควบคุมงานประยุกต์ ได้รับการปฏิบัติ และใช้งานอย่างถูกต้องเหมาะสม การควบคุมการบริหารการจัดการที่สำคัญ คือ 1. แบ่งแยกหน้าที่ 2. นโยบายและกระบวนงานถูกเขียนออกมาอย่างชัดเจน 3. การดูแล การตรวจตรา

การแบ่งแยกหน้าที่ หมายถึง การออกแบบหน้าที่งานเพื่อลดความเสี่ยงที่จะเกิดความผิด-พลาด หรือ การดำเนินการที่เป็นการฉ้อโกงทรัพย์สินขององค์กร โดยบทบาทความรับผิดชอบของแต่ละคนจะแตกต่างกันออกไป ตามปกติแล้ว แผนกสารสนเทศจะรับผิดชอบกับแฟ้มข้อมูล และโปรแกรม ส่วนผู้ใช้จะรับผิดชอบเกี่ยวกับการสร้างธุรกรรมต่างๆ เช่น การชำระเงิน เป็นต้น

การเขียนนโยบาย และกระบวนงาน จะเป็นการกำหนดมาตรฐานอย่างเป็นทางการสำหรับควบคุมการทำงานของระบบสารสนเทศ กระบวนงานควรจะเขียนขึ้นอย่างเป็นทางการ และได้รับมอบอำนาจจากผู้บริหารระดับที่เหมาะสม พร้อมระบุความรับผิดชอบ

การดูแล ตรวจตรา เป็นขั้นตอนที่ทำให้เกิดความมั่นใจว่า การควบคุมระบบสารสนเทศได้ดำเนินการตามที่ควรจะเป็น เพราะถึงแม้จะมีการออกแบบการควบคุมที่ดี แต่ขาดการดูแลตรวจตรา มาตรการการควบคุมก็อาจถูกละเลยมองข้ามไป หรือเป็นแค่ทางผ่านเท่านั้น

3.2 การควบคุมงานประยุกต์

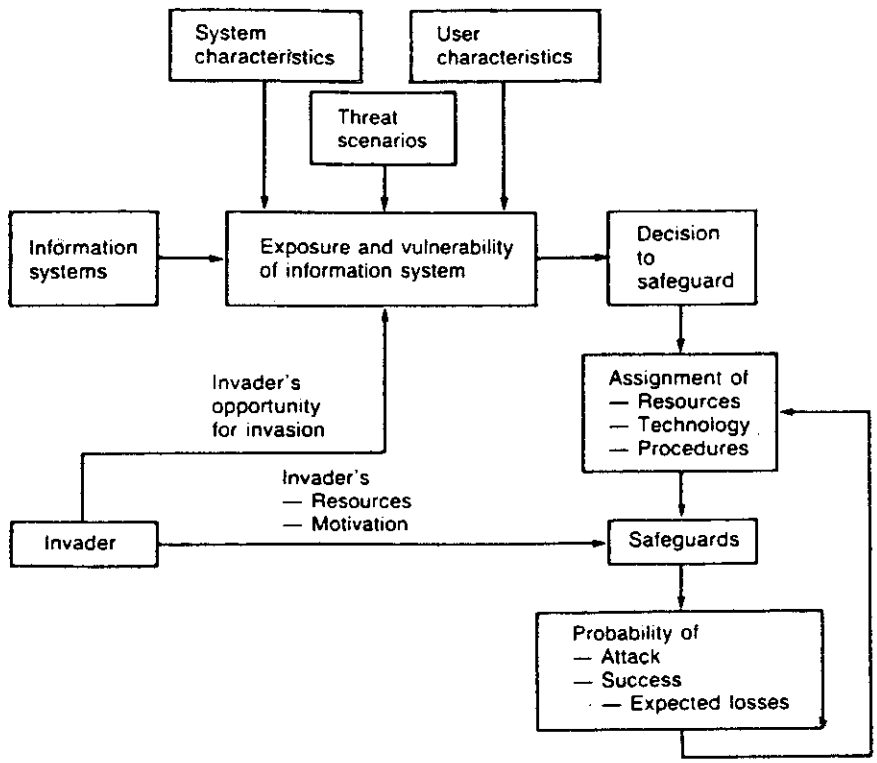
การควบคุมงานประยุกต์ เป็นการควบคุมเฉพาะภายในงานประยุกต์ทางด้านคอมพิวเตอร์แต่ละงาน เช่น ระบบค่าแรง หรือ การประมวลผลใบสั่งสินค้า การควบคุมงานประยุกต์นี้รวมเอากระ-บวนงานทั้งที่เป็นอัตโนมัติ และเป็นระบบใช้แรงงาน เพื่อให้เกิดความมั่นใจว่า เฉพาะข้อมูลที่ได้รับ

อนุญาตเท่านั้นที่ได้รับการประมวลผลจากงานประยุกต์อย่างสมบูรณ์ และถูกต้อง การควบคุมสำหรับแต่ละงานประยุกต์รวมถึงลำดับการประมวลผลทั้งหมด

การควบคุมงานประยุกต์ แบ่งออกเป็น การควบคุมสิ่งเข้า การควบคุมการประมวลผล และการควบคุมสิ่งออก (รายละเอียดศึกษาในบทที่ 10)

4. การกำหนดระดับความปลอดภัย

การรักษาความปลอดภัยเป็นสิ่งที่มีค่าใช้จ่ายเกิดขึ้น ทั้งค่าใช้จ่ายในด้านอุปกรณ์รักษาความปลอดภัย และบุคลากรที่ใช้ในการรักษาความปลอดภัย นอกจากนี้ยังมีค่าใช้จ่ายที่ไม่สามารถจะประมาณเป็นจำนวนเงินได้ เช่น ความไม่พอใจของพนักงาน เพราะการรักษาความปลอดภัยอาจทำให้กระบวนการทำงานล่าช้า หยุดชะงัก หรือขาดความสะดวกในการทำงาน ตลอดจนพนักงานเสียขวัญกำลังใจในการทำงาน ดังนั้นการกำหนดระดับความปลอดภัยควรกำหนดในระดับใด ผู้บริหารจะต้องวิเคราะห์ความเสี่ยง (Risk) ว่าระบบมีความอ่อนแอต่อความเสียหาย ต่อการประมวลผลล่าช้า ต่อการฉ้อโกง ต่อการเปิดเผยข้อมูล มากน้อยเพียงใด รูป 9.11 แสดงถึงองค์ประกอบในการประเมินความเสียหายจากการบุกรุกระบบ



รูป 9.11 องค์ประกอบในการประเมินความเสียหายเมื่อระบบถูกบุกรุก

ในการประเมินความเสี่ยง ต้องพิจารณาถึงลักษณะของระบบ และลักษณะของผู้ใช้ ดังรูป 9.11 วิธีการหนึ่งในการคำนวณมูลค่าความเสียหายจากการที่ระบบถูกบุกรุก มีสูตรในการคำนวณ คือ

$$\text{Expected loss} = L \times P_A \times P_B$$

L = Potential loss

P_A = Probability of attack

P_B = Probability of success

บริษัทประกัน หรือ บริษัทผู้ขายอุปกรณ์ เครื่องมือ สามารถช่วยผู้บริหารในการกำหนดค่าของ L ส่วนค่าความน่าจะเป็นทั้ง 2 ค่า กำหนดได้ยาก ดังนั้นแทนที่จะกำหนดเป็นค่าที่ชัดเจน ก็จะใช้การกำหนดเป็นค่าความเสี่ยงสัมพันธ์ (ความเสี่ยงสูง ปานกลาง หรือ ต่ำ) แล้วจึงกำหนดค่าตัวเลขลงในแต่ละความเป็นไปได้ที่สัมพันธ์กันเหล่านี้ เช่น 0.8 0.5 และ 0.2 ตามลำดับ ก็สามารถจะคำนวณค่าความเสียหายจากสูตรดังกล่าว เช่น

Exposure	L	x P_A	x P_B	= Expected loss
1	500,000	1.0	0.2	100,000
2	200,000	0.6	0.5	60,000
3	50,000	0.2	0.8	8,000
Total Expected loss				168,000

ค่าที่ได้เป็นค่าความเสียหายในแต่ละกรณี ค่ารวมของค่าความเสียหายจะเป็นมูลค่าความเสี่ยงทั้งหมดต่อระบบ ถ้าค่าความเป็นไปได้ P_A และ P_B เป็นค่าความเป็นไปได้ของปี ค่าความเสียหายที่คำนวณก็จะเป็นค่าความเสียหายต่อปี

การใช้สูตรนี้จะช่วยฝ่ายบริหารในการกำหนดว่าการเพิ่มระดับการรักษาความปลอดภัยนั้นคุ้มกับค่าความเสียหายหรือไม่ อย่างไรก็ตามสูตรที่ใช้ในการคำนวณเป็นเพียงค่าประมาณ เพราะอุตสาหกรรมคอมพิวเตอร์เป็นอุตสาหกรรมที่นับว่าใหม่ และมีการเปลี่ยนแปลงสูง รวดเร็ว จึงไม่มีข้อมูลในอดีตยาวนานพอที่จะคำนวณค่าความน่าจะเป็นที่น่าเชื่อถือ นอกจากนั้นข้อมูลเกี่ยวกับการถูกคามระบบรักษาความปลอดภัยของกิจการต่างๆ มักจะไม่ได้รับการเปิดเผย เพราะจะทำให้กิจการขาดความเชื่อมั่น ข้อมูลส่วนนี้จึงไม่สมบูรณ์เช่นกัน และประการสุดท้ายบุคลากรที่ทำหน้าที่ออก-แบบระบบรักษาความปลอดภัยมักจะไม่ตระหนักถึงเล่ห์เหลี่ยม และเทคนิคของอาชญากรคอมพิว-

CT 489

201

เตอร์ที่พยายามทำลายระบบรักษาความปลอดภัย ดังนั้นจึงไม่สามารถจะวางแผนรับมือกับอาชญากรเหล่านี้ ได้พอเพียง หรือเท่าทัน

5. คำศัพท์

Availability	Secrecy
Confidential	Security kernel
Data directory	Smart card
Identification	Trapdoor
Integrity	Trojan horse
Password	Virtual machine
Privacy	Virus

6. คำถามท้ายบท

1. การรักษาความปลอดภัยในส่วนใดที่ทำได้ยาก : ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล เพราะเหตุใด
2. เทคนิคที่ใช้ในการระบุตัวบุคคล ใช้เทคนิคใดบ้าง ข้อดี และข้อเสียของแต่ละเทคนิค
3. ความเป็นส่วนตัว (Privacy) สำคัญอย่างไร
4. ความเป็นส่วนตัวของข้อมูล กับความจำเป็นในการเข้าถึงข้อมูล ขัดแย้งกันหรือไม่ เพราะเหตุใด
5. รหัสผ่านคืออะไร รหัสผ่านสามารถป้องกันการคุกคามระบบได้มากน้อยเพียงใด เพราะเหตุใด
6. เหตุใดการกำหนดระดับความปลอดภัยสูง จึงอาจสร้างความไม่พอใจให้กับผู้ใช้ระบบ
7. ในองค์กรธุรกิจซึ่งข้อมูลมีความสำคัญต่อคู่แข่งสูง ควรกำหนดระบบในการรักษาความปลอดภัยอะไรบ้าง
8. บทบาทหน้าที่ของผู้บริหารแผนกสารสนเทศเกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ เป็นอย่างไร
9. จงอธิบายเกี่ยวกับ คำต่างๆ ต่อไปนี้ โดยสังเขป :- Virus, Trojan horse, Trapdoor
10. Verification กับ Identification แตกต่างกันอย่างไร