<u>คาบ 8 ความมั่นคงปลอดภัยข้อมูลและการจัดวางข้อมูล</u>

ดร.ยรรยง เต็งอำนวย

เมื่อได้กล่าวถึงสถาปัตยกรรมข้อมูลไปในคาบที่แล้ว คาบนี้จะได้เน้นเรื่องความมั่นคงปลอดภัยของข้อมูลหรือ Data Security **<u>Slide 1</u>** ซึ่งจำเป็นอย่างยิ่งต่อองค์กรสมัยใหม่ที่อาศัยข้อมูลและสารสนเทศสูงมาก จนเรียกได้ว่าไม่อาจขาดสิ่งนี้ไปได้เลย อีกส่วนหนึ่งซึ่งจะเน้นในคาบนี้คือการให้ผู้เรียนเข้าใจถึงการ "จัดวาง" ข้อมูลหรือ Data Placement ว่าจะวางข้อมูลที่มีอยู่ขององค์กรในลักษณะใด จะรวมไว้ที่เดียวตรงส่วนกลาง หรือจะปล่อยให้กระจัดกระจายไปตามที่ต่างๆ ซึ่งการจัดวางข้อมูลนี้เป็นประเด็นที่เริ่มมีความสำคัญต่อองค์กรมากขึ้นเรื่อยๆ เมื่อทุกส่วนทุกหน่วยงานย่อยขององค์กรเริ่มใช้ระบบสารสนเทศเพื่อการเพิ่มพูนประสิทธิภาพของการทำงานกันมากขึ้น

สำหรับองค์กรแล้ว ข้อมูลมีความสำคัญเสมอ แต่ในปัจจุบันข้อมูลถูกบรรจุเข้าไปในระบบสารสนเทศมากขึ้นเรื่อยๆ และผนวกสัมพันธ์กับระบบงานการดำเนินธุรกิจอย่างใกล้ชิด ทำให้ข้อมูลหลักเปลี่ยนจากรูปแบบของเอกสารกระดาษไปเป็นเอกสารอิเล็กทรอนิกส์

ดังนั้นในองค์กรสมัยใหม่ ข้อมูลที่มีอยู่ในระบบสารสนเทศจึงมีความสำคัญยิ่งยวดเพราะแทบจะไม่มีสำเนาหรือสำรองอยู่ในรูปของกระดาษอย่างสมัยก่อนที่เริ่มใช้คอมพิวเตอร์กัน ความเสียหายอันอาจเกิดต่อข้อมูลที่เก็บไว้ในระบบสารสนเทศจึงเป็นเรื่องที่ร้ายแรงมาก จนอาจกล่าวได้ว่าข้อมูลเป็นโครงสร้างพื้นฐานหรือ infrastructure แบบหนึ่ง ไม่ต่างจากเซิร์ฟเวอร์และเครือข่ายขององค์กร **<u>Slide 2</u>**

การที่ข้อมูลเป็นอิเล็กทรอนิกส์อย่างเต็มรูปแบบทำให้ความเสียหายที่เกิดขึ้นกับข้อมูลเป็นเรื่องร้ายแรง เพราะไม่อาจหามาทดแทนได้โดยง่าย ไม่เหมือนกับวัสดุอุปกรณ์และสินทรัพย์ประเภทอื่นที่สามารถหาซื้อมาเปลี่ยนส่วนที่เสียหายชำรุดหรือถูกโจรกรรมได้ไม่ยากนัก หากข้อมูลขององค์กรเสียหายและไม่อาจกู้คืนได้ องค์กรจะได้รับความเสียหายหนักเพราะไม่มีข้อมูลที่ต้องใช้ในการดำเนินงานขององค์กร องค์ประกอบอื่นจะไม่อาจมาทดแทนหรือผ่อนหนักเป็นเบาได้หากข้อมูลถูกทำลาย ให้สังเกตว่าความเสียหายของข้อมูลนั้นไม่จำเป็นต้องเป็นเพราะฮาร์ดดิสก์ถูกทำลายไปพร้อมกับข้อมูล แต่อาจเป็นเพราะข้อมูลถูกผู้ร้ายสำเนาออกไป คือข้อมูลรั่วไหล หรืออาจโดนผู้ไม่ประสงค์ดีเข้ามาทำการแก้ไขทำให้ผิดพลาด หรืออาจถูกผู้ร้ายเข้ามาแก้ไขรหัสผ่านหรือเข้ารหัสลับข้อมูลสำคัญทำให้องค์กรไม่อาจใช้ประโยชน์ข้อมูลที่มีอยู่ได้ เช่นนี้ถือเป็นความเสียหายต่อข้อมูลทั้งสิ้น

การทำให้ข้อมูลมีความมั่นคงปลอดภัยนั้นแบ่งเป็นด้านกายภาพหรือ Physical Security และด้านตรรกหรือ Logical Security

ความมั่นคงทางกายภาพสำหรับข้อมูลนั้นแบ่งเป็นสามส่วนด้วยกัน **Slide 3** คือด้านสื่อหรือ media สำหรับใช้เก็บข้อมูล เช่น อุปกรณ์จำพวกฮาร์ดดิสก์ ด้านอุปกรณ์หรือ Equipment สำหรับบรรจุสื่อที่ใช้เก็บข้อมูลเหล่านั้น เช่นตู้อุปกรณ์หรือ Rack และด้านสถานที่หรือห้องสำหรับการจัดวางอุปกรณ์

ในส่วนของความมั่นคงปลอดภัยของสื่อหรือ Media ที่ใช้เก็บข้อมูลนั้น แม้จะมีสื่อหลายประเภทในปัจจุบัน แตกต่างกันไปทั้งในด้านราคา ความรวดเร็ว ความจุ แต่สื่อที่เป็นพื้นฐานเป็นหลักในการเก็บข้อมูลที่เป็นที่ยอมรับกันโดยทั่วไปคือฮาร์ดดิสก์ **Slide 4** ซึ่งมีพัฒนาการด้วยความรวดเร็วใกล้เคียงกับที่กำหนดไว้ในกฎของคุณมัวร์ กล่าวคือกฎของมัวร์นั้นกำหนดให้ระบบวงจรฮาร์ดแวร์ของคอมพิวเตอร์มีพัฒนาการเพิ่มพูนเป็นสองเท่าในทุก 18 เดือน ส่วนของฮาร์ดดิสก์นั้นจะเพิ่มพูนเป็นสองเท่าในทุกๆ 12 เดือนเท่านั้นเอง จึงเป็นสื่อที่ได้รับความนิยมอย่างสูง

ปัจจุบันฮาร์ดดิสก์นิยมใช้ในลักษณะของออนไลน์ คือเสียบทำงานอยู่กับระบบตลอดเวลา ไม่มีการถอดออกเก็บแยกต่างหาก ทั้งนี้เพื่อให้สอดคล้องกับสภาพการใช้งานของระบบสารสนเทศที่ต้องให้บริการตลอดเวลาทุกวัน และการให้บริการเหล่านั้นจำต้องอาศัยข้อมูลในภาพกว้างขององค์กรมากขึ้น จึงต้องมีข้อมูลขององค์กรทั้งหมดออนไลน์พร้อมให้ใช้อยู่เสมอ

ปัญหาคือสื่อเป็นอุปกรณ์เก็บข้อมูลทางกายภาพ มีส่วนที่เป็นกลไกเคลื่อนไหว ดังนั้นจึงมีความเสื่อมที่สูงกว่าระบบที่ไม่มีส่วนเคลื่อนไหวเป็นธรรมชาติธรรมดาอยู่เอง ด้วยเหตุนี้เมื่อมีการนำฮาร์ดดิสก์มาใช้จำต้องคำนึงถึงวันที่ฮาร์ดดิสก์นั้นจะเสียหายพังไป ซึ่งอาจอยู่ในระดับของ 2-3 ปีหรืออาจ 5-10 ปีขึ้นกับคุณภาพของอุปกรณ์ แต่อย่างไรก็ตามอายุการใช้งานของอุปกรณ์ที่มีการผลิตเป็นจำนวนมากนั้นจะไม่แน่นอนเป็นเรื่องของสถิติ ดังนั้นไม่อาจระบุได้อย่างชัดเจนว่าฮาร์ดดิสก์แต่ละตัวนั้นจะเสียเมื่อใดในกี่ปี ดังนั้นต้องมีสำรองข้อมูลหรือ Backup เอาไว้อย่างแน่นอน โดยองค์กรอาจคำนึงถึงหลักการที่เรียกว่า LOCKSS ซึ่งย่อมาจาก Lots of Copies Keep Stuff Safe หรือหมายถึงหากมีสำเนาของข้อมูลอยู่หลายชุดก็จะทำให้ข้อมูลนั้นมีโอกาสเสียหายโดยสิ้นเชิงน้อยลง

แต่การมีหลายสำเนาหรือมีสำรองอยู่มากนั้น เป็นธรรมดาที่ต้องสิ้นเปลืองเนื้อที่ในการเก็บ การบำรุงดูแลรักษา และข้อมูลหลายสำเนาก็อาจเกิดความคลาดเคลื่อนไม่ตรงกันระหว่างสำเนา เกิดเป็น inconsistency ได้ นอกจากนั้นเมื่อมีหลายสำเนากระจายอยู่ตามที่ต่างๆ ย่อมทำให้เกิดความเสี่ยงสูงขึ้นที่ข้อมูลจะรั่วไหลจากสำเนาที่ได้รับการปกป้องไม่เพียงพอ เช่นการทำสำเนาชุดหนึ่งไปเก็บไว้ที่บ้านของผู้อำนวยการฝ่ายซึ่งล่อแหลมที่จะโดนโจรกรรมได้ เป็นต้น

นอกจากนั้นอาจจำต้องมีการเก็บสำเนาเป็นสำรองไว้แบบ Off-line Backup เนื่องด้วยสำเนาที่ on-line ทุกชุดนั้นหากมีการปกป้องไม่ดีพอจะทำให้ไวรัสคอมพิวเตอร์แพร่ไปถึงทุกสำเนาเหล่านั้นได้ คือหากไวรัสสามารถเข้าไปเปลี่ยนแปลงสำเนาได้ชุดหนึ่ง สำเนาชุดที่เหลือจะได้รับการแก้ไขอันประสงค์ร้ายเหล่านั้นไปด้วยเพราะเป็นสภาพการออกแบบให้คงค่าของข้อมูลไว้ให้ตรงกันทุกสำเนาอยู่แล้ว การเก็บข้อมูลไว้เป็น Off-line Backup จะช่วยลดโอกาสการแพร่ของไวรัสหรือโปรแกรมประสงค์ร้ายในลักษณะนี้ได้ไม่มากก็น้อย

รูปใน **Slide 5** แสดงถึงการมีอายุของสื่อต่างๆ ในรูปเป็นแผ่นดีวีดีที่คุณภาพต่ำและมีการเก็บรักษาไม่ดีพอ ทั้งเรื่องของอุณหภูมิและความชื้น ทำให้แผ่นสารที่ปิดไว้เพื่อบันทึกข้อมูลมีอาการเสื่อมและสลายเป็นดวงอย่างเห็นได้ชัด ไม่อาจนำข้อมูลเหล่านั้นกลับมาใช้ได้อีก แผ่นที่เห็นในรูปนี้มีอายุเพียงปีเศษเท่านั้นก็เสื่อมสภาพแล้ว เกิดเป็นดวงๆ ไปทั่ว หากเป็นแผ่นที่ใช้สำหรับเก็บสำรองข้อมูลหรือ backup จะเห็นได้ทันทีว่าข้อมูลขององค์กรนั้นอยู่สภาวะที่ล่อแหลมมากทีเดียว

สภาพการณ์ของอายุที่จำกัดของสื่อนั้น ไม่ได้เกิดเพียงแต่แผ่นดีวีดีหรือฮาร์ดดิสก์เท่านั้น แต่รวมไปถึงสื่อทุกประเภท ไม่ว่าจะเป็นเทปแม่เหล็ก diskette thumb drive ไม่ว่าจะมีคุณภาพดีเพียงใด สื่อเหล่านั้นต่างมีอายุการใช้งานด้วยกันทั้งสิ้น ไม่ว่าจะในด้านของเนื้อสารที่เสื่อมสภาพทางกายภาพแม้จะไม่ได้ใช้งานโดยเก็บวางไว้เฉยๆ ก็ตาม หรือการเสื่อมสภาพของข้อมูลที่บรรจุอยู่แม้สภาพทางกายภาพจะดีอยู่ก็ตาม รวมไปถึงการที่สื่อนั้นเกิดล้าสมัยเมื่อเวลาผ่านไป อย่างเช่น diskette ขนาดใหญ่ของสมัยก่อนที่มีเส้นผ่านศูนย์กลางถึง 8 นิ้ว ในปัจจุบันไม่อาจหาเครื่องที่จะอ่านแผ่นขนาดนั้นได้อีกต่อไป เช่นนี้จะทำให้ข้อมูลในแผ่นที่อาจมีการเก็บรักษาไว้เป็นอย่างดีไม่อาจนำมาใช้งานได้

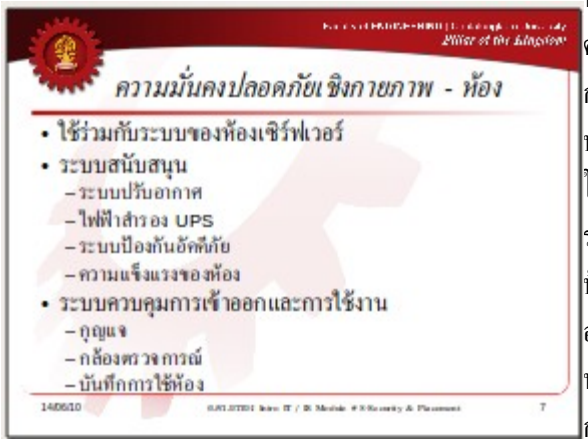
ในส่วนของอุปกรณ์สำหรับบรรจุใส่สื่อที่ใช้เก็บข้อมูลนั้น ควรต้องคำนึงถึงความมั่นคงปลอดภัยในเชิงกายภาพอย่างสูง เช่น ควรใช้อุปกรณ์ที่ดี มียี่ห้อ เพราะอุปกรณ์ประเภทนี้จะยึดมาตรฐานการผลิตในระดับสากล ทำให้มีความมั่นคงปลอดภัยคงทนต่อการใช้งานได้ในระดับที่ดี **Slide 6**

นอกจากนี้ควรใช้อุปกรณ์ฮาร์ดดิสก์ประเภทที่เป็น RAID หรือ Redundant Array of Inexpensive Disk หมายถึงการนำฮาร์ดดิสก์ราคาย่อมเยาว์มาเรียงกันเป็นตับเพื่อให้เป็นสำรองซึ่งกันและกัน จะช่วยให้ยืดอายุการใช้งานของฮาร์ดดิสก์ทั้งตับนั้นได้ยาวนานกว่าอายุของฮาร์ดดิสก์แต่ละลูก ซึ่งลักษณะของ RAID นี้มีอยู่หลายรูปแบบ หลายมาตรฐาน และทั้งยังมีการเปลี่ยนแปลงเพิ่มเสริมเมื่อระบบวงจรควบคุมได้รับการพัฒนามากขึ้นด้วย ให้ผู้เรียนศึกษาถึงรูปแบบของ RAID ประเภทต่างๆ เพื่อจะได้นำไปใช้ประโยชน์ในการเลือกซื้ออุปกรณ์ประเภทนี้

อีกส่วนหนึ่งของอุปกรณ์คือตู้ใส่อุปกรณ์มาตรฐานที่เรียกว่า Rack Cabinet มาตรฐานนั้นกำหนดทั้งขนาดและอุปกรณ์ประกอบที่จำเป็นเช่นระบบจ่ายไฟฟ้า เต้าเสียบ พัดลมระบายความร้อน และอย่างหนึ่งที่มักละเลยคือการมีฝาหรือประตูตู้ปิดให้เป็นสัดส่วนพร้อมกุญแจเพื่อเพิ่มความปลอดภัยให้กับอุปกรณ์ในตู้อีกชั้นหนึ่ง

กุญแจตู้อุปกรณ์นี้เป็นสิ่งที่มักมองข้ามกันไปเนื่องด้วยความไม่สะดวกในการใช้งานหรือการซ่อมบำรุง แต่เนื่องจากตู้อุปกรณ์เหล่านี้อยู่ในห้องเซิร์ฟเวอร์ขนาดใหญ่ มีพนักงานทั้งขององค์กรและพนักงานจากบริษัทภายนอกเข้าออกอยู่แทบจะตลอดเวลา จึงทำให้เป็นจุดอ่อนหากมีผู้ไม่ประสงค์ดีเข้าไปในห้อง

ความมั่นคงปลอดภัยเชิงกายภาพในระดับที่สามนั้นคือความมั่นคงปลอดภัยของห้องเซิร์ฟเวอร์ที่ใช้บรรจุอุปกรณ์เก็บข้อมูลนั่นเอง **Slide 7** ซึ่งโดยปกติแล้วจะอาศัยพ่วงระบบการรักษาความมั่นคงปลอดภัยของเซิร์ฟเวอร์ไปด้วย กระนั้นก็สมควรกล่าวถึงองค์ประกอบที่ควรคำนึงถึงสำหรับความมั่นคงปลอดภัยระดับนี้ไว้ด้วย



ในระดับห้องแล้วต้องมีระบบสนับสนุนต่างๆ ที่เหมาะสม ทั้งระบบปรับอากาศ ระบบไฟฟ้าสำรองหรือระบบ UPS ระบบป้องกันอัคคีภัย รวมไปถึงความแข็งแรงทนทานของห้อง ไม่อาจเจาะทะลุเข้ามาทางผนัง พื้น หรือฝ้าเพดานได้โดยง่าย นอกจากความมั่นคงปลอดภัยของห้องแล้ว ระบบที่ดีต้องมีกุญแจหรือ key card สำหรับการผ่านเข้าออก โดยอาศัยกล้องตรวจการณ์เป็นมาตรการป้องกันอีกชั้นหนึ่ง รวมถึงการมีบันทึกการเข้าใช้ห้องและการเข้าถึงข้อมูลในทางกายภาพ เช่นการทำ backup ประจำสัปดาห์ หรือการเปลี่ยนฮาร์ดดิสก์ลูกที่เสียพัง เช่นนี้เป็นต้น

ในส่วนของความมั่นคงในเชิงตรรกหรือ Logical Security **Slide 8** อาจใช้มาตรการการเข้ารหัสลับหรือ Data Encryption ต่อข้อมูลที่เก็บไว้และทำการถอดรหัสลับคืนเมื่อต้องการใช้งาน แต่การใช้รหัสลับนั้นมีข้อเสียหลายประการเช่น ข้อมูลที่เข้ารหัสนั้นแม้จะไม่อาจอ่านหรือใช้ได้โดยผู้ที่ไม่มีสิทธิ์แต่ก็สามารถถูกทำลายให้เสียหายใช้การไม่ได้โดยผู้ไม่ประสงค์ดี นอกจากนั้นข้อมูลในยุคสมัยใหม่นี้สามารถเข้าถึงได้โดยผ่านเครือข่าย ไม่จำต้องเข้าไปใกล้แหล่งที่เก็บข้อมูล ดังนั้นแม้จะได้มีการเข้ารหัสลับแล้วก็ตามแต่ผู้ไม่ประสงค์ดียังสามารถเข้าถึงข้อมูลเหล่านั้นได้ จึงต้องมีมาตรการในการปิดกั้นหรือหน่วงเหนี่ยวไม่ให้ผู้ไม่ได้รับสิทธิ์เข้าไปใกล้ข้อมูลผ่านเครือข่ายได้ นอกจากนั้นต้องมีบุคลากรที่ไว้วางใจได้ให้เป็นผู้ถือกุญแจ ไม่เช่นนั้นหากกุญแจรหัสลับรั่วไหลออกไปหรือผู้ถือกุญแจมีเจตนาร้ายก็สามารถเข้าถึงข้อมูลจากระยะไกลได้

ดังนั้นเพื่อเป็นการป้องกันอีกชั้นหนึ่ง ระบบสารสนเทศขององค์กรขนาดใหญ่จะใช้ Security Token เป็นกุญแจทางกายภาพอีกชั้นหนึ่งในการควบคุมการเข้าถึงข้อมูล โดยใช้กุญแจที่เป็นกายภาพเช่น Key Card หรือบัตรผ่านพิเศษที่ต้องไปสอดลงในอุปกรณ์อ่านบัตรที่กำหนดจุดไว้ตายตัว แม้เพื่อการอ่านหรือบันทึกข้อมูลต่างๆ โดยมีเจ้าหน้าที่เฝ้าจุดอ่านกุญแจเหล่านั้นสำหรับข้อมูลหรือระบบงานที่มีชั้นความลับสูง เป็นการป้องกันการล้วงความลับหรือขโมยข้อมูลผ่านทางเครือข่ายได้

ไม่ว่าองค์กรจะปกป้องข้อมูลจากความเสียหายหรือการโจรกรรมด้วยการเข้ารหัสลับหรือการใช้กุญแจกายภาพที่มีความมั่นคงปลอดภัยสูงอย่างไรก็ตาม ข้อมูลยังอาจเกิดเสียหายได้จากเหตุอันไม่คาดฝันเช่นภัยพิบัติ อัคคีภัย ต่างๆ เหล่านี้ได้ องค์กรจึงต้องมีการสำรองข้อมูลเป็น Backup ไว้เผื่อความเสียหายทุกประเภท โดยควรแยกข้อมูลที่สำรองไว้นี้ให้อยู่ภายนอกองค์กรหรืออยู่ห่างออกไป ในเชิงกายภาพ จากข้อมูลสำเนาที่เป็นตัวจริง เช่นอยู่คนละอาคาร แต่จากสภาพการณ์ที่ผ่านมาจะพบว่าภัยพิบัติอาจมีผลต่อกลุ่มอาคารในบริเวณที่ทำการเดียวกันได้โดยสิ้นเชิง ดังนั้นจึงควรเก็บสำรองข้อมูลไว้ในที่ทำการที่ห่างไกลแยกออกไป **Slide 9**

มาตรการทางตรรกในการปกป้องข้อมูลอีกอย่างหนึ่งคือการปิดบังข้อมูลสำคัญหรือเรียกว่า Data Masking คือการให้ใช้ข้อมูลเพียงบางส่วน ไม่ใช่ทั้งหมด เช่นสำหรับผู้ที่ไม่เกี่ยวข้อง เช่นเจ้าหน้าที่ call center ก็ให้เห็นเฉพาะเลขสี่หลักท้ายของเลขรหัสบัตรเครดิตเพื่อใช้ตรวจสอบตัวตนของผู้ถือบัตรที่โทรศัพท์เข้ามารับบริการ เช่นนี้เป็นต้น

มาตรการรักษาความมั่นคงปลอดภัยอีกประการหนึ่งสำหรับข้อมูลนั้นอยู่ตรงที่ต้องคำนึงถึงข้อมูลในลักษณะที่ครบวงจรชีพของมัน กล่าวคือนับแต่ได้รับหรือป้อนข้อมูลเข้าสู่ระบบ การใช้งาน การแก้ไขเปลี่ยนแปลง และสุดท้ายคือการเกษียณข้อมูลนั้นออกจากระบบไป ในระบบงานที่ดีหรือสำคัญจะไม่มีการเกษียณข้อมูลใดๆ ข้อมูลทุกชิ้นจะถูกเก็บไว้อย่างถาวรเพื่อการอ้างอิงในอนาคต แต่ในความเป็นจริงนั้นข้อจำกัดด้านเนื้อที่ของสื่อในการเก็บข้อมูลทำให้องค์กรต้องทิ้งหรือลบข้อมูลออกจากระบบ ซึ่งการจำหน่ายข้อมูลทิ้งนี้จำต้องได้รับการตรวจตรา การลงบันทึกที่เหมาะสม เพื่อกันการรั่วไหลของข้อมูลผ่านกระบวนการจำหน่ายทิ้งนี้

นอกจากนั้นสื่อบันทึกข้อมูลที่ถูกจำหน่ายทิ้งก็เช่นกัน เมื่อระบบอุปกรณ์เกิดเสียหายหรือหมดอายุหรือถูกทดแทนด้วยอุปกรณ์รุ่นใหม่ จำต้องให้แน่ใจว่าข้อมูลที่บรรจุอยู่ภายในนั้นถูกลบออกอย่างหมดจดแล้ว เพราะมีกรณีตัวอย่างที่นักวิจัยของมหาวิทยาลัยในต่างประเทศทำวิจัยด้านความมั่นคงปลอดภัยของข้อมูลโดยกว้านซื้อเครื่องคอมพิวเตอร์เก่าๆ ที่ขายทอดตลาดนำมาวิเคราะห์พบข้อมูลสำคัญขององค์กรหลายแห่งที่ติดมากับเครื่องเก่าเหล่านี้

ประเด็นเกี่ยวเนื่องกับความมั่นคงปลอดภัยของข้อมูลอีกประการหนึ่งคือการใช้งาน Thumb Drive หรือ Flash Drive ซึ่งเป็นหน่วยความจำขนาดเล็กเท่านิ้วหัวแม่มือ จึงเรียกว่า Thumb Drive คือเป็นฮาร์ดดิสก์ขนาดนิ้วมือนั้นเอง หน่วยความจำแบบนี้กำลังเป็นที่นิยมอย่างมากเพราะมีราคาถูก ความจุสูงขึ้นอย่างรวดเร็วปีต่อปี และยังมีขนาดกระทัดรัด พกพาไปมาได้ อีกทั้งยังเป็นหน่วยความจำกลุ่มเดียวกับที่ใช้ในกล้องถ่ายรูปแบบดิจิตอลทั่วไป เป็นวิวัฒนาการด้านเทคโนโลยีหน่วยความจำที่มีผลกระทบอย่างสูงต่อวงการ **Slide 10**

ปัญหาของหน่วยความจำแบบนี้คือการที่มีความจุสูง ซึ่ง Thumb Drive สมัยใหม่จุถึง 32 GB ในราคาเพียงพันกว่าบาทเท่านั้น แต่ขณะเดียวกันมีขนาดเล็กมาก บางแบบก็เล็กจนสามารถซ่อนในกระเป๋าสตางค์ในช่องใส่เงินเหรียญหรือสามารถซ่อนไว้ในปากของผู้ไม่ประสงค์ดีได้ด้วยซ้ำไป ความที่เล็กกระทัดรัด ใช้สะดวกนี้ ทำให้หน่วยงานทั้งหลายนิยมเอามาใช้เป็นอุปกรณ์เก็บข้อมูล สำรองข้อมูล แลกเปลี่ยนข้อมูล หรือใช้ในการส่งและรับข้อมูลระหว่างองค์กร แทนการใช้แผ่นดีวีดีหรือแผ่นซีดีกันแล้ว แต่ในลักษณะเดียวกับแผ่นดีวีดีหรือซีดี Thumb Drive สามารถวางทิ้งไว้บนโต๊ะหรือในกระเป๋าเอกสาร สามารถใส่กระเป๋าเสื้อแล้วก้มลงทำหล่นหาย หรือวางลืมทิ้งไว้ที่โต๊ะในร้านกาแฟหลังจากนั่งทำงานเสร็จ เหล่านี้ทำให้มีโอกาสที่ข้อมูลขององค์กรจะรั่วไหลผ่านสื่อบันทึกที่มีเทคโนโลยีสูงเช่นนี้ได้ ควบคุมการรั่วไหลนี้ได้ยากมาก ดังนั้นองค์กรใหญ่ๆ ที่ระมัดระวังเกี่ยวกับข้อมูลขององค์กร เช่นทางทหาร จะมีนโยบายห้ามใช้ Thumb Drive เหล่านี้โดยสิ้นเชิง หรือ

ห้ามไม่ให้เครื่องคอมพิวเตอร์ไม่ว่าจะเป็นแบบตั้งโต๊ะหรือแบบโน้ตบุ๊ค ห้ามไม่ให้มี USB port สำหรับเสียบ Thumb Drive โดยเด็ดขาด
แต่ไม่ว่าจะใช้มาตรการอย่างไร หน่วยความจำบนสื่อสมัยใหม่ที่สะดวกและมีความจุสูงในราคาย่อมเยาว์เช่นนี้ก็ยากที่จะห้ามใช้ได้ เนื่องจากความสะดวกและมีประสิทธิภาพสูงด้วยประการทั้งปวง ดังนั้นองค์กรจึงควรคำนึงถึงปัญหานี้ให้ดี และมีนโยบายหรือมาตรการที่เหมาะสมออกมาเพื่อเป็นการประนีประนอมระหว่างการรักษาความมั่นคงปลอดภัยและประโยชน์ใช้สอยจากเทคโนโลยีสมัยใหม่

ตัวอย่างของ Thumb Drive เป็นดัง **Slide 11** โดยรูปทางด้านซ้ายมือนั้นเป็นลักษณะของผลิตภัณฑ์ที่คุ้นเคยกันดีอยู่ มีลักษณะเป็นแท่งยาวราวสองนิ้วสามารถถอดฝาให้เห็น jack เสียบเข้าช่อง USB ได้

แต่เนื่องจากเทคโนโลยีนี้เกาะตามพัฒนาการแบบกฎของคุณมัวร์อย่างเต็มที่ ทำให้เป็นวงจรอิเล็กทรอนิกส์ขนาดเล็กที่มีสมรรถนะสูง ความจุเป็นหลายสิบกิกกาไบต์ ขนาดจำกัดอยู่ที่ขนาดของ jack เสียบช่อง USB ที่มีขนาดมาตรฐาน ดังนั้นในภาพทางด้านขวาจะเป็น Thumb Drive ที่ตัดส่วนประกอบที่ไม่จำเป็นออกจนเกือบหมด เหลือเพียงส่วนที่บรรจุ memory chip ที่เป็นวงจรขนาดเล็กกับส่วนที่เป็น jack สำหรับเสียบช่อง USB เท่านั้น จึงมีขนาดรูปร่างที่บางเฉียบและเล็กกระทัดรัดอย่างมาก แลเห็นเป็นแผ่นบางๆ คีบอยู่กับปลายนิ้วได้
พัฒนาการอันน่ามหัศจรรย์ของ Thumb Drive นั้นทำให้มันมีประโยชน์อย่างสูงล้ำ แต่ในขณะเดียวกันก็เป็นปัญหาด้านความมั่นคงปลอดภัยของข้อมูลสำหรับองค์กรอย่างมากเช่นกัน

ไม่ว่าจะอย่างไรก็ตาม ความจำเป็นในการระแวดระวังความมั่นคงปลอดภัยของข้อมูลนั้นเป็นความจำเป็นขององค์กรสมัยใหม่ที่เปลี่ยนมุมมองจากการเป็น "เจ้าของ" ข้อมูลมาเป็น "ผู้ดูแล" ข้อมูล ดังนั้นข้อมูลที่องค์กรเก็บไว้ในความเป็นจริงคือข้อมูลของลูกค้าที่มา "ฝาก" ไว้กับองค์กรเพื่อประโยชน์ในการทำนิติกรรมกับองค์กร
ดังนั้นในระดับสากล **Slide 12** จึงมีการออกกฎหมายและข้อบังคับรวมทั้งมาตรฐานต่างๆ มาเพื่อให้ชี้ชัดลงไปในประเด็นของความมั่นคงปลอดภัยของข้อมูลและสารสนเทศที่องค์กรเก็บรักษาไว้ให้ลูกค้าของตน เช่นในประเทศอังกฤษมีกฎหมายว่าด้วยการคุ้มครองข้อมูลหรือ Data Protection Act ซึ่งให้ความคุ้มครองข้อมูลของเจ้าของ เช่น Credit Rating หรือความน่าเชื่อถือทางการเงินของบุคคลทั่วไปที่เป็นลูกค้าของสถาบันการเงินอย่างธนาคารหรือบริษัทบัตรเครดิต ซึ่งหากข้อมูลเหล่านี้รั่วไหลออกไปย่อมทำให้เกิดความเสียหายต่อชื่อเสียงของบุคคลผู้นั้นได้ เป็นต้น

หรือในมาตรฐานโลก ISO/IEC 17799 ซึ่งระบุถึงมาตรฐานด้านความมั่นคงปลอดภัยของสารสนเทศหรือ Information Security ได้กำหนดว่าข้อมูลทุกตัวในระบบสารสนเทศขององค์กรต้องมีการกำหนดผู้รับผิดชอบในเรื่องความถูกต้องและเรื่องความมั่นคงปลอดภัยของข้อมูลนั้นๆ อย่างชัดเจน ทั้งนี้เพื่อให้แน่ใจว่าข้อมูลมีผู้ที่ระแวดระวังอย่างดี มิใช่เป็นข้อมูลที่มี

การใช้งานแต่ปล่อยให้เป็น "ภาระ" ขององค์กรซึ่งไม่มีตัวตน ซึ่งการกำหนดมาตรฐานเช่นนี้หมายถึงจะมีการระแวดระวังในระดับที่ถี่ถ้วนมากขึ้นโดยผู้ที่รับผิดชอบ

อีกประเด็นหนึ่งที่สำคัญเกี่ยวข้องกับระบบความมั่นคงปลอดภัยของข้อมูลหรือระบบงานสารสนเทศก็ตาม คือความสามารถของระบบและข้อมูลที่จะรอดปลอดภัยในสถานการณ์ฉุกเฉินร้ายแรง **Slide 13**

แต่เดิมในประเทศไทยไม่ค่อยมีเหตุการณ์ฉุกเฉินร้ายแรงเท่าใดนัก ในปัจจุบันสภาพการณ์ส่อเค้าไปในทางที่จะมีความรุนแรงค่อนข้างสูงเป็นครั้งคราว จึงจำเป็นอยู่เองที่องค์กรต้องคำนึงถึงประเด็นการกู้คืนข้อมูลและระบบในสภาวการณ์ฉุกเฉินขั้นร้ายแรง ดังที่เห็นในรูป ลักษณะนี้คือการจัดสร้าง DRC หรือ Disaster Recovery Center เป็นลักษณะของศูนย์เพื่อกู้คืนในสภาพการณ์ภัยพิบัติร้ายแรงหรืออาจพิจารณาได้ว่าเป็นศูนย์สำรองหรือ Backup Site ลักษณะของศูนย์สำรองนี้ถือเป็นหลักประกันสำหรับองค์กรในกรณีเกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติร้ายแรง อย่างธนาคารกสิกรไทยได้จัดทำศูนย์ประมวลผลไว้ถึงสามแห่งด้วยกัน ให้อยู่ในระยะห่างเพียงพอที่สภาพการณ์ร้ายแรงอย่างไฟไหม้ใหญ่หรือจลาจลจะไม่มีผลกระทบครอบคลุมศูนย์ทั้งหมด สิ่งนี้ถือเป็นประเด็นทาง Business Continuation หรือการที่ธุรกิจหรือธุรกรรมขององค์กรจะต้องดำเนินต่อไปได้โดยไม่สะดุดชะงักเนื่องจากความเสียหายต่อข้อมูล

การบริหารจัดการระบบข้อมูลที่ดีอีกประเด็นหนึ่งคือเรื่องของการจัดวางข้อมูลหรือ Data Placement คือการที่องค์กรจะจัดวางข้อมูลไว้ในองค์กรให้สอดคล้องกับลักษณะขององค์กรหรือการใช้งาน
ที่มาของประเด็นนี้อาจแสดงให้เห็นได้จากตัวอย่าง ปกติเมื่ออาจารย์จะเข้าสอนในชั้นเรียนต้องขอใบเซ็นชื่อมาจากสำนักทะเบียน และเมื่อมีนักศึกษาเพิ่มหรือลดวิชา ใบเซ็นชื่อที่มีอยู่ในมือของอาจารย์จะล้าสมัยไป **Slide 14** หรือใบขับขี่ตลอดชีพนั้นมีข้อมูลที่เก่าแก่มหาศาล ล้าสมัยไปหลายต่อหลายปีแล้ว เพราะเป็นข้อมูลเก่านับสิบๆ ปี ข้อมูลที่มีอยู่ในใบขับขี่นั้นก็ต้องถือว่าเป็นสำเนาหนึ่งของข้อมูลของบุคคลเช่นกัน เพียงแต่ไม่ตรงกับข้อมูลที่มีเก็บไว้ในระบบทะเบียนราษฎร์ของกระทรวงมหาดไทย หรือข้อมูลที่ให้ไว้กับธนาคารในตอนที่เปิดบัญชีเงินฝาก

ตัวอย่างอีกอย่างหนึ่งคือระบบโทรศัพท์ซึ่งแต่เดิมมีเลขเพียงเจ็ดตัว แต่แล้วก็มีโทรศัพท์เคลื่อนที่หรือระบบมือถือ ทำให้ต้องเพิ่มเลขขึ้นไปอีกเป็น 01 แต่ต่อมาไม่เพียงพอจึงต้องใช้ 08 นำหน้าอีกทีหนึ่ง ดังนั้นสมุดโทรศัพท์และรายชื่อคนที่ติดต่อด้วยในเครื่องโทรศัพท์มือถือทั่วประเทศจะต้องถูกปรับแก้ใหม่กันหมด เกิดโกลาหลกันอยู่พักใหญ่
หรือฝ่ายวิจัยของมหาวิทยาลัยต้องการข้อมูลการตีพิมพ์ผลงานวิจัยของคณาจารย์ในรูปของบทความวิจัยที่ไปลงในวารสารวิชาการต่างๆ แต่ข้อมูลนี้ฝ่ายวิชาการของมหาวิทยาลัยก็ต้องการเพื่อไปสนับสนุนการวางแผนการบริหารจัดการของมหาวิทยาลัยเช่นการจัดลำดับสถาบันอุดมศึกษา ส่วนฝ่าย

ประชาสัมพันธ์ก็ต้องการข้อมูลเดียวกันนี้เพื่อจะนำไปลงในวารสารข่าวประชาสัมพันธ์ของมหาวิทยาลัยเพื่อแจกจ่ายออกไปในวงกว้าง

เหล่านี้เป็นธรรมชาติของข้อมูลที่แม้จะมีเพียงชุดเดียวในองค์กรแต่มีแนวโน้มที่จะไปปรากฏหรือกระจายไปอยู่ตามที่ต่างๆ เนื่องจากความจำเป็นในการใช้งานขององค์กร ดังนั้นองค์กรจึงจำต้องคำนึงถึงการจัดวางหรือ Placement ของข้อมูลเป็นประเด็นสำคัญ ไม่เช่นนั้นอาจเกิดความคลาดเคลื่อนหรือลักลั่นระหว่างสำเนาทั้งหลายของข้อมูลเหล่านั้น ไม่ว่าจะด้วยเจตนาหรือไม่ก็ตาม (แต่โดยปกติจะไม่เจตนาให้สำเนาเหล่านั้นคลาดเคลื่อนกัน)

องค์กรมีทางเลือกอยู่สองแบบคือให้ข้อมูลรวมกันไว้ที่เดียวกัน เป็นลักษณะการจัดวางแบบรวมศูนย์หรือ Centralized Data Placement หรือให้ข้อมูลสามารถกระจายไปอยู่ตามที่ต่างๆ เป็นการจัดวางแบบกระจายหรือ Distributed Data Placement ไม่ว่าจะเป็นแบบแยกส่วนกันไปหรือเป็นแบบมีสำเนากระจายไปในหลายๆ สถานที่ก็ตาม

การจัดวางข้อมูลแบบรวมศูนย์นั้น มุ่งเน้นให้ข้อมูลทุกอย่างขององค์กรรวมไว้ในที่เดียวกันเชิงกายภาพ อาจเป็นเครื่องเดียวหรือหลายเครื่องแต่อยู่ในห้องเซิร์ฟเวอร์เดียวกันหรืออยู่ภายใต้การควบคุมดูแลของหน่วยงานกลางหน่วยเดียวขององค์กร

Slide 15

การจัดวางข้อมูลแบบรวมศูนย์หรือ Centralized Data Placement นั้นมีข้อดีคือควบคุมดูแลได้สะดวก สามารถกำหนดและสร้างมาตรฐานในระดับองค์กรและสามารถควบคุมตรวจสอบการทำระบบข้อมูลให้เป็นไปตามมาตรฐานที่กำหนดขึ้นได้โดยง่าย ระบบรวมศูนย์ยังเป็นระบบที่ไม่ซับซ้อน ดูแลรักษาปรับปรุงได้สะดวก มีความมั่นคงปลอดภัยสูง การพัฒนาระบบงานและการวิเคราะห์สถานภาพรวมขององค์กรสามารถทำได้โดยสะดวก และเนื่องจากเป็นความรับผิดชอบของหน่วยงานกลางจึงเป็นการไม่ยากที่จะได้รับงบประมาณเป็นกอบเป็นกำจากองค์กร

นอกจากนั้นหน่วยงานกลางที่รับผิดชอบข้อมูลที่รวมศูนย์นี้ยังมีลักษณะเป็นหน่วยงานใหญ่ มีความเข้มแข็งในด้านระบบอุปกรณ์ งบประมาณ ความรู้ความสามารถของบุคลากร ความชำนาญ และความเข้าใจในภาพรวมขององค์กร ซึ่งจะช่วยให้ระบบสารสนเทศขององค์กรมีเสถียรภาพไปด้วย

แต่ขณะเดียวกันการจัดวางข้อมูลแบบรวมศูนย์ก็มีข้อเสียด้วยเช่นกัน **Slide 16** กล่าวคือองค์กรที่ใช้ระบบข้อมูลแบบรวมศูนย์จำต้องมีระบบเครือข่ายที่ดีมากเพื่อให้การเข้าถึงข้อมูลสามารถกระทำได้โดยสะดวกรวดเร็ว ลองนึกถึงข้อมูลในใบขับขี่ตลอดชีพที่ล้าสมัยมากเพราะไม่อาจเข้าถึงข้อมูลของทางราชการได้เนื่องจากอยู่ในรูปของกระดาษและอยู่ในกระเป๋าของผู้ขับขี่ขวยยานแต่หากเป็นใบขับขี่อิเล็กทรอนิกส์หรือเป็นแบบ Smart Card จะสามารถติดต่อสื่อสารกับกรมการขนส่งทางบกหรือระบบทะเบียนราษฎร์เพื่อปรับปรุงข้อมูลต่างๆ เช่นที่อยู่ ให้เป็นปัจจุบันได้ตลอดเวลา

ตัวอย่างคือการขอรายชื่อนักศึกษาเพื่อใช้เป็นใบเซ็นชื่อเข้าชั้นเรียนเมื่อขอไปทางสำนักทะเบียนของมหาวิทยาลัย ได้คำตอบกลับมาว่าให้ทำเรื่องเป็นบันทึกข้อความไป เซ็นโดยอาจารย์หัวหน้าวิชา

หัวหน้าภาควิชา และคณบดี เช่นนี้ก็ย่อมต้องยาวนานมากและจะส่งผลให้อาจารย์หาทางสร้างฐานข้อมูลนักศึกษาในวิชาที่ตนสอนขึ้นมาเอง เพราะไม่อาจใช้ประโยชน์ ใช้บริการ หรือหวังพึ่งข้อมูลที่รวมศูนย์อยู่ที่ส่วนกลางได้

อีกประการหนึ่งที่ทำให้ระบบข้อมูลแบบรวมศูนย์เสียเปรียบคือการที่เครื่องและอุปกรณ์คอมพิวเตอร์มีราคาถูกลงมีประสิทธิภาพสูงขึ้นอย่างรวดเร็วตามกฎของคุณมัวร์ ซึ่งทำให้มีโอกาสที่ข้อมูลจะเกิดขึ้นและถูกสะสมดูแลไว้ที่จุดที่เกิดขึ้นของข้อมูลนั้น เกิดสภาพการกระจายตัวของข้อมูลขององค์กรอยู่เอง เช่นการทำเว็บไซต์ของคณะ เว็บไซต์ของอาจารย์ การทำการวิจัย การทำวิทยานิพนธ์ ฝ่ายวิเคราะห์ของคณะ ของภาควิชา และของมหาวิทยาลัย เหล่านี้เป็นความสะดวกในการสร้างและดูแลรักษาข้อมูลเหล่านั้นเอง กระจายข้อมูลออกไปตามลักษณะการกระจายตัวของงานและความรับผิดชอบภายในองค์กร

การรวมศูนย์ของข้อมูลนั้นทำให้หน่วยงานกลางที่รับผิดชอบมีสภาพเป็นหน่วยใหญ่ที่เข้มแข็ง แต่ในทางกลับกันก็ทำให้เกิดการทำตัวเป็นเจ้าของข้อมูลขององค์กรไปด้วย ทำให้เกิดการ "หวงของ" และหย่อนเรื่องการให้บริการข้อมูลแก่หน่วยงานต่างๆ ขององค์กร ตัวอย่างที่เห็นได้ชัดคือหน่วยงานต่างๆ ของรัฐที่ต้องแบ่งปันข้อมูลกันใช้ แต่มักไม่เกิดความร่วมมือเหล่านี้ หน่วยงานต่างๆ ต่างก็พยายามขวนขวายหาข้อมูลด้วยตัวเองทั้งที่มีความซ้ำซ้อนกับข้อมูลของหน่วยงานอื่นเพราะไม่อาจขอใช้ข้อมูลจากหน่วยงานต่างๆ ได้

ข้อเสียที่สำคัญสุดท้ายของระบบข้อมูลแบบรวมศูนย์คือการที่ระบบข้อมูลขององค์กรเกิดความล่อแหลมที่จะเสียหายได้หากเกิดภัยพิบัติร้ายแรงเนื่องจากรวมอยู่ในที่เดียวกัน หากไม่มีการป้องกันที่เหมาะสมจะสร้างความเสียหายแก่องค์กรได้มากทีเดียว

รูปใน **Slide 17** แสดงให้เห็นถึงสภาพการณ์ร้ายแรงที่เกิดขึ้นกลางใจเมืองหลวงของไทยในเดือนพฤษภาคม พ.ศ. 2553 ที่ผ่านมา ความร้ายแรงนี้ทำให้บริษัทกิมเอ็งซึ่งเป็นบริษัทค้าหลักทรัพย์อันดับหนึ่งของไทยไม่อาจให้บริการลูกค้าได้แม้สำนักงานใหญ่จะไม่ถูกอัคคีภัยทำลายเสียหายก็ตามแต่สายใยแก้วที่เป็นช่องทางการสื่อสารเพื่อรับคำสั่งซื้อขายนั้นได้รับความเสียหายไหม้ไฟหมด ทำให้ไม่อาจให้บริการลูกค้าได้ แม้จะย้ายไปใช้ศูนย์สำรองที่อโศกแต่ก็ไม่อาจรับปริมาณการสั่งซื้อของลูกค้าได้ทำให้เกิดการชะงักงัน หยุดการให้บริการไป

หากหันมาพิจารณาทางเลือกของการจัดวางข้อมูลคือแบบกระจายหรือ Distributed Data Placement **Slide 18** จะเห็นว่าเป็นวิธีการที่สอดคล้องกับลักษณะธรรมชาติขององค์กรโดยทั่วไปที่ทุกส่วนและทุกฝ่ายขององค์กรย่อมต้องมีส่วนร่วมในการดำเนินงานขององค์กรอยู่เป็นธรรมดา นอกจากนั้นธุรกรรมต่างๆ ขององค์กรยังเกี่ยวเนื่องกับลูกค้าหรือผู้รับบริการรวมไปถึงองค์กรอื่นๆ ที่เกี่ยวเนื่องในธุรกิจหรือกิจการนั้น

นอกจากการมีส่วนร่วมโดยองค์ประกอบต่างๆ ทั้งในและนอกองค์กร ข้อมูลยังมีลักษณะที่กระจายเนื่องจากการที่ต้องสำรองข้อมูลเอาไว้เผื่อในกรณีข้อมูลเกิดเสียหายจากอุปกรณ์พังหรือจากภัยพิบัติร้ายแรงต่างๆ ดังนั้นเป็นธรรมชาติของข้อมูลอยู่แล้วที่ต้อง

กระจายตัวออกไปตามแหล่งที่เกิดและแหล่งที่ใช้งาน ไม่อาจอยู่รวมกันที่ศูนย์กลางได้
ปัญหาของการกระจายตัวของข้อมูลในลักษณะนี้คือความยากลำบากในการเข้าถึงและการใช้ข้อมูลร่วมกัน ซึ่งจะนำไปสู่การมีหลายสำเนาของข้อมูล เกิดความลักลั่นคลาดเคลื่อนระหว่างค่าของสำเนาเหล่านี้ ยากต่อการบังคับให้ค่าของสำเนาเหล่านี้ถูกต้องตรงกันหรือ Data Synchronization ซึ่งนำไปสู่ความด้อยประสิทธิภาพของระบบสารสนเทศขององค์กร

ประเด็นที่สำคัญอย่างหนึ่งของการจัดวางข้อมูลคือเกี่ยวกับ Multi-Centralized Database ซึ่งเป็นฐานข้อมูลที่ตั้งใจให้เป็นการรวมศูนย์ข้อมูล แต่เนื่องจากองค์กรนั้นซับซ้อนจึงมีโอกาสสูงที่จะเกิดฐานข้อมูลรวมศูนย์ในลักษณะนี้ขึ้นมาหลายฐาน เช่น ฐานข้อมูลการเงิน การผลิต การขาย ฐานข้อมูลบุคลากร เหล่านี้เป็นต้น **Slide 19**

ฐานข้อมูลเหล่านี้หากไม่ติดต่อกัน ไม่สัมพันธ์กัน ไม่แลกเปลี่ยนใช้ข้อมูลร่วมกัน แต่ละฐานข้อมูลถือว่าเป็น Centralized Database ซึ่งจะทำให้ข้อมูลมีความซ้ำซ้อนกันบางส่วน และจะมีความต้องการในการใช้ข้อมูลข้ามฐานกันอยู่เสมอ เช่น ข้อมูลพนักงานจะเกี่ยวพันกับการขายและเกี่ยวพันกับฐานบุคลากรด้วย ในขณะที่ฝ่ายผลิตเองก็ต้องการข้อมูลบุคลากรและข้อมูลจากฝ่ายขายเพื่อใช้ประโยชน์ในการวางแผนการผลิต
ดังนั้นข้อมูลต้องรวมกันหรือสัมพันธ์กัน เกิดเป็นระบบข้อมูลที่เป็น Distributed Data แม้ว่าแต่ละฐานข้อมูลจะถูกออกแบบมาให้เป็น Centralized Database ก็ตาม

ดังนั้นในการวางแผน การจัดทำ และการบริหารจัดการระบบข้อมูลที่ดี จำต้องเข้าใจความแตกต่างระหว่าง Distributed Data คือข้อมูลที่มีลักษณะการเกิดและการใช้งานที่กระจายตัวออกไปในองค์กร ถูกจัดวางอยู่ในที่ต่างๆ แยกกันแต่มีลักษณะการใช้งานร่วมกันเป็นหนึ่งเดียว **Slide 20**

ปัญหาคือองค์กรเองตระหนักหรือไม่ว่าข้อมูลของตนนั้นมีการกระจายตัวอยู่ หากรู้ การสร้างฐานข้อมูลและระบบงานต่างๆ จะรองรับการกระจายตัวเหล่านั้น เกิดเป็น Distributed Database และ Application คือฐานข้อมูลในลักษณะกระจาย มีหลายฐานแต่ทำงานร่วมกันเป็นฐานเดียว และระบบงานที่เข้าใจถึงการกระจายของข้อมูลในฐานต่างๆ เหล่านี้
แต่ถ้าองค์กรไม่ตระหนักว่าข้อมูลนั้นมีการกระจายตัว ผลที่ได้คือระบบข้อมูลที่มีความซ้ำซ้อนสูง ลักลั่น ผิดพลาด ข้อมูลที่ซ้ำซ้อนกันนั้นไม่ตรงกัน ทางแก้ขององค์กรที่ไม่ตระหนักในธรรมชาติของการกระจายตัวของข้อมูลนี้จะเกิดเป็นความพยายามในการรวมศูนย์อย่างขนานใหญ่ ลงทุนสูง ใช้บุคลากรและเวลามาก อย่างเช่นระบบ SAP ที่ได้รับความนิยมอยู่ทั่วไปในวงการราชการ

แต่แม้องค์กรจะตระหนักว่าข้อมูลมีธรรมชาติของการกระจายตัวอยู่ ก็ต้องอาศัยมาตรฐานข้อมูลที่ดีขององค์กร ทั้งในส่วนของพจนานุกรมข้อมูล เพื่อให้พูดภาษาเดียวกันทั้งองค์กรในส่วนที่เกี่ยวข้องกับข้อมูลแต่ละตัว และทั้งในส่วนของแบบ

จำลองข้อมูล เพื่อให้เข้าใจรูปแบบของข้อมูลและความสัมพันธ์ระหว่างข้อมูลของทั้งองค์กร **Slide 21**

เมื่อมีมาตรฐานข้อมูลที่เหมาะสมแล้วแม้จะแยกข้อมูลกระจายกันออกไป แยกงานกันทำในแต่ละส่วนของข้อมูล แต่จะไม่มีความซ้ำซ้อนหรือมีแต่น้อย และไม่เกิดความแตกต่างระหว่างสำเนาทั้งหลายของข้อมูล เนื่องจากแต่ละฝ่ายแต่ละส่วนงานตระหนักจากพจนานุกรมข้อมูลและแบบจำลองข้อมูลว่าข้อมูลที่ระบบงานของตนต้องการนั้นอยู่ที่ฝ่ายใดและสามารถนำมาใช้ประโยชน์ได้ อย่างไร จึงทำให้เกิดการจัดหาหรือสะสมหรือเก็บงำข้อมูลเหล่านั้นในลักษณะที่ซ้ำซ้อนกับของฝ่ายอื่นน้อยลงไปอย่างมาก ความตระหนักในธรรมชาติการกระจายตัวของข้อมูลนี้จะนำไปสู่การลดซึ่งอัตตา หรือความรู้สึกเป็นเจ้าของข้อมูลลงได้เป็นอย่างมาก ทำให้เกิดการสมานฉันท์ในระหว่างหน่วยงานต่างๆ ขององค์กรที่จะร่วมมือกันทำระบบสารสนเทศและระบบข้อมูลที่เป็นประโยชน์ต่อลูกค้าและผู้ใช้บริการได้มากที่สุด

สภาพการลดอัตตาในด้านข้อมูลนี้ทำให้เกิดสิ่งที่เรียกได้ว่า Data Custodian คือเป็นสภาวะที่หน่วยงานย่อยขององค์กรพิจารณาตัวเองว่าเป็นเพียงผู้ปกป้องหรือดูแลข้อมูลขององค์กรและของลูกค้าผู้ใช้บริการ หาใช่เจ้าของข้อมูลอย่างที่เชื่อกันมาแต่ก่อนแต่อย่างใดไม่ ดังนั้นจะเกิดความรู้สึกรับผิดชอบต่อข้อมูลขององค์กรมากขึ้นโดยเฉพาะในส่วนที่อยู่ภายใต้ความดูแลของหน่วยงานย่อยนั้นๆ

ธนาคาร **Slide 22** เป็นกรณีศึกษาของการจัดวางข้อมูลที่ดี เพราะธนาคารนั้นโดยธรรมชาติแล้วจะมีสาขากระจายอยู่ทั่วไป มีลูกค้าในละแวกหรือท้องถิ่นที่สาขาเป็นผู้ดูแล เพื่อให้การบริการฝากเงินและกู้เงินของธนาคารสามารถกระจายตัวไปได้ สร้างฐานลูกค้าได้กว้างไกล ดังนั้นแต่ละสาขาจึงมีข้อมูลของลูกค้าของตนสะสมไว้ในลักษณะของกระดาษ การฝากถอนหรือทำธุรกรรมใดๆ ของลูกค้าจึงไม่อาจทำข้ามหรือต่างสาขาได้

เมื่อยุคสมัยเปลี่ยนไป ลูกค้าของธนาคารมีการสัญจรไปมามากขึ้น ย่อมเกิดความไม่สะดวกในการใช้บริการเพราะต้องแล่นกลับไปที่สาขาดั้งเดิมของลูกค้าอยู่เสมอ ดังนั้นธนาคารจึงรวบรวมข้อมูลลูกค้าของทุกสาขามารวมศูนย์ไว้ที่สำนักงานใหญ่ สาขาสามารถเข้าใช้ข้อมูลของตนหรือของต่างสาขาได้โดยผ่านเครือข่ายของธนาคารเข้ามา

ปัญหาคือหากเครือข่ายล่ม สาขาจะให้บริการไม่ได้เลยแม้แต่ลูกค้าของตน ในยุคแรกเริ่มที่เครือข่ายยังมีเสถียรภาพต่ำ สาขาจะเก็บสำเนาของลูกค้าของตนเองเอาไว้ดังนั้นจึงสามารถให้บริการแก่ลูกค้าของตนได้แต่ให้บริการต่างสาขาไม่ได้ในกรณีที่เครือข่ายล่ม จะเห็นได้ว่าการจัดวางข้อมูลนั้นมีส่วนสำคัญต่อการให้บริการและการขายขององค์กรอย่างสูง ในระบบธนาคารที่กระจายข้อมูลออกไปยังสาขาต่างๆ เมื่อเครือข่ายล่มสาขาจะสามารถให้บริการลูกค้าของตนได้ แต่สาขาอื่นจะไม่อาจเข้าถึงข้อมูลของสาขานั้นได้แม้เครือข่ายในส่วนของตนไม่ล่มก็ตาม แต่หากรวมศูนย์ข้อมูลทุกสาขาไว้ที่สำนักงานใหญ่ หากเครือข่ายของสาขาหนึ่งล่มสาขาอื่นก็ยังสามารถให้บริการต่างสาขาสำหรับสาขาที่ล่มได้อยู่ เพราะข้อมูลอยู่ที่ส่วนกลาง แต่สาขาที่ล่มนั้นให้บริการแก่ลูกค้าไม่ได้เลยไม่ว่าจะเป็นต่างสาขาหรือของสาขาของตนเองก็ตาม แต่หากทำเป็นกึ่งกระจาย คือมีข้อมูลอยู่ทั้งที่

สาขาและสำเนาไปรวมศูนย์ไว้ที่สำนักงานใหญ่ แม้จะแก้ปัญหาเครือข่ายล่มได้มาก แต่จะทำให้เกิดปัญหาตามมาคือสำเนาข้อมูลของสาขาทั้งสองชุดนั้นอาจไม่ตรงกัน ต้องเสียโสหุ้ยมากขึ้นในการทำให้มีค่าสอดคล้องตรงกันไว้ตลอดเวลา โดยเฉพาะหลังจากการล่มของเครือข่ายและกู้คืนขึ้นมาได้แล้ว
ปัญหาที่สำคัญอย่างหนึ่งของการกระจายข้อมูลไปไว้ตามสาขาคือการที่สาขาจะต้องมีระบบเครื่องเซิร์ฟเวอร์ของตนเอง ทำให้ธนาคารต้องสิ้นเปลืองทรัพยากรในการจัดทำห้องเซิร์ฟเวอร์ขนาดเล็กกระจายตามสาขานับร้อยของตน รวมไปถึงการมีบุคลากรเพื่อคอยดูแลระบบที่กระจายตัวออกไปเช่นนั้นอีกจำนวนมาก

ดังนั้นทางออกที่ดีสำหรับการจัดวางข้อมูลคือเป็นแบบผสม **Slide 23** กล่าวคือทำการรวมศูนย์ข้อมูลในองค์กรให้มากที่สุด ให้เหลือฐานข้อมูลเพียงไม่กี่ตัวเท่าที่จำเป็น แต่ต้องเชื่อมโยงฐานข้อมูลเหล่านั้นเข้าด้วยกันในลักษณะของ Distributed Database เช่นนี้จะทำให้การดูแล ควบคุม บำรุงรักษาข้อมูล รวมไปถึงเรื่องเสถียรภาพและความมั่นคงปลอดภัยของข้อมูลกระทำได้โดยสะดวกและมีประสิทธิภาพ เสียค่าใช้จ่ายโดยรวมที่ต่ำ

แต่ขณะเดียวกันองค์กรต้องจัดสร้างเครือข่ายที่มีประสิทธิภาพสูง มีเสถียรภาพ น่าเชื่อถือ มีระบบและเส้นทางสำรองอย่างดี เพื่อให้ทุกภาคส่วนขององค์กรสามารถเข้าถึงข้อมูลได้สะดวก
และที่สำคัญคือองค์กรต้องจัดให้มีการประชุม สัมนา อบรม ให้ความรู้แก่บุคลากรเพื่อให้ลดอัตตา ความรู้สึกเป็นเจ้าข้าวเจ้าของของข้อมูล โดยเฉพาะหน่วยงานกลางที่ดูแลเรื่องการรวมศูนย์ข้อมูลต้องมีจิตใจการให้บริการเป็นที่ตั้ง ไม่ทำตัวเป็นจักรพรรดิ์แห่งข้อมูล ถ้าการบริการดีแล้ว พนักงานขององค์กรจะไม่มีการเก็บข้อมูลขององค์กรไว้ตามที่ต่างๆ โดยไม่จำเป็น ลดความซ้ำซ้อนและความผิดพลาดของข้อมูลลงไปได้อย่างมาก และอย่างเป็นระบบ
ตัวอย่างที่สำคัญของการมีข้อมูลรวมศูนย์และมีเครือข่ายและการให้บริการชั้นยอดคือบริษัท Google ที่บริการการค้นหา จะพบว่าแม้บริการจะอยู่ต่างประเทศหรือห่างไกลออกไป แต่ระดับการให้บริการนั้นน่าประทับใจมาก การสืบค้นข้อมูลแต่ละคราวจะใช้เวลาไม่ถึงวินาที และบริการของ Google นั้นมีเสถียรภาพมากกว่าเครือข่ายขององค์กรที่ต่อเข้าไปใช้บริการเสียอีก

ในคาบถัดไปจะเป็นกรณีศึกษาสำหรับวิชานี้เพื่อให้ผู้เรียนได้เห็นภาพรวมของระบบสารสนเทศที่ซับซ้อนได้ชัดเจนยิ่งขึ้น