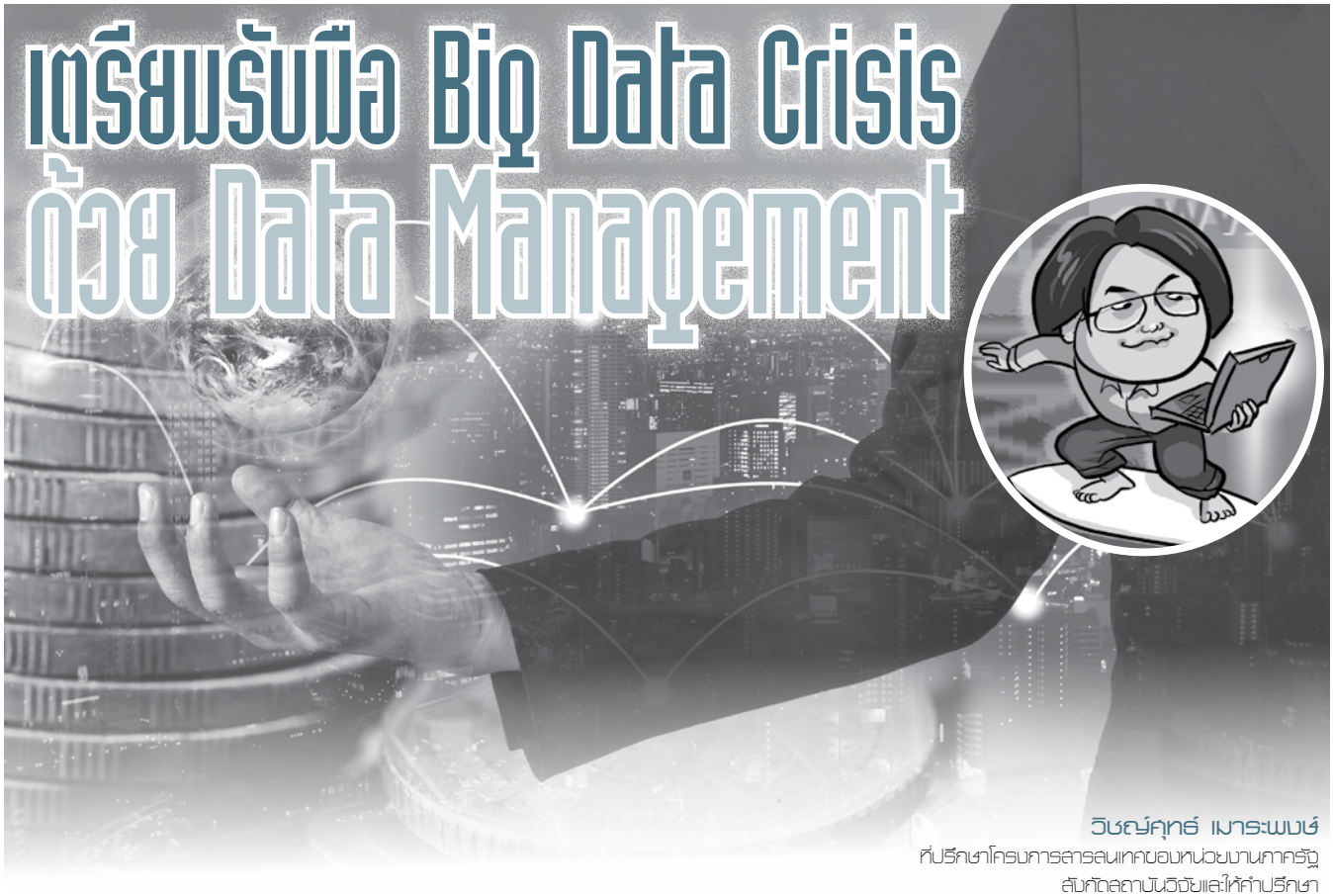
เตรียมรับมือ Big Data Crisis ด้วย Data Management



วิชญ์คุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ขั้นตอนที่ 3 การจัดทำ Information Security Policy ที่สามารถนำมาใช้งานจริงได้

ขั้นตอนนี้เป็นขั้นตอนที่ให้ความสำคัญกับการจัดทำ Information Security Policy ที่ต้องสามารถนำมาใช้งานจริงได้ สำหรับการกำหนดนโยบายต่างๆ จะมีการกำหนดขอบเขตของการควบคุมไว้เป็นหลายชั้น ดังนี้

■ Administrative Level (ควบคุมในระดับผู้ดูแลระบบ) ประกอบด้วย

- การกำหนดโครงสร้างการบริหารจัดการ
- การกำหนดนโยบายต่างๆ
- การกำหนดมาตรฐานต่างๆ
- การกำหนดแนวทางปฏิบัติ (Guideline) ต่างๆ
- กระบวนการบริหารจัดการ
- การตรวจสอบระบบ
- การวางแผนการใช้งานทรัพยากรระบบ
- การควบคุมในระดับบุคคล
- การฝึกอบรมเพื่อตระหนักรู้ด้านการรักษาความปลอดภัยระบบ
- การทดสอบระบบ

■ Physical Level (ควบคุมในระดับกายภาพ)

- นโยบายเรื่องการใช้งานอาคาร และสิ่งก่อสร้างต่างๆ
- นโยบายเรื่องการใช้พื้นที่ปฏิบัติงานต่างๆ
- นโยบายเรื่องการรักษาความปลอดภัยพื้นที่ต่างๆ (พื้นที่ควบคุม)
- นโยบายเรื่องการปิดกั้นพื้นที่ต่างๆ (พื้นที่หวงห้าม)

■ Technical Level (ควบคุมในระดับเทคนิค)

- การควบคุมระบบคอมพิวเตอร์
- การควบคุม Network Zone ต่างๆ
- การตรวจจับผู้บุกรุก
- สถาปัตยกรรมเครือข่าย
- การเข้าถึงระบบเครือข่าย และระบบคอมพิวเตอร์ต่างๆ
- การสำรองข้อมูล
- การตรวจสอบระบบ
- โพรโตคอลต่างๆ

■ Data Level (ควบคุมในระดับข้อมูล)

- การเข้ารหัสข้อมูลที่สำคัญ
- การกำหนดกระบวนการในการเข้าถึงข้อมูลต่างๆ
- การกำหนดสิทธิในข้อมูลสำหรับผู้ใช้งานระบบต่างๆ

Security Policy ที่เป็นมาตรฐานสากล และมีการใช้งานอย่างแพร่หลาย อาทิ

1. BS ISO/IEC 17799 เป็นมาตรฐานที่ใช้อ้างอิงในการเขียนนโยบายด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ซึ่งเน้นไปที่รูปแบบการทำงาน และภาพรวมของระบบโดยไม่ได้ลงในรายละเอียดแนวทางการปฏิบัติ

2. CobiT (Control Objective for Information and Related Technology) เป็นนโยบายที่เน้นการตรวจ สอบโดยผู้ตรวจสอบด้าน Information System โดยตรง ซึ่งธนาคารหรือสถาบันการเงินนำมาใช้งาน

3. CBK (Common Body of Knowledge) เป็นข้อมูลพื้นฐานหรือองค์ความรู้สำคัญที่จำเป็นในการกำหนดนโยบายด้านการรักษาความปลอดภัยระบบข้อมูลคอมพิวเตอร์

4. SANS / FBI Top20 Vulnerability เป็นข้อมูลเกี่ยวกับช่องโหว่และการสำคัญสำหรับผู้ดูแลระบบในการนำไปใช้กับระบบที่ตนดูแล

Security Policy Plan

- Policy หมายถึง นโยบายในภาพรวมที่กระชับ และได้ใจความเรียกว่า “Goal” หรือเป้าหมายที่องค์การต้องการไปถึง
- Standard หมายถึง มาตรฐานที่ต้องบังคับใช้ในการปฏิบัติจริง เช่น มาตรฐานเกี่ยวกับการตั้งรหัสผ่าน เป็นต้น
- Guideline หมายถึง แนวทางในการปฏิบัติที่ไม่ได้บังคับแต่แนะนำเพื่อให้ผู้ปฏิบัติสามารถบรรลุเป้าหมายได้ง่ายยิ่งขึ้น
- Procedure หมายถึง รายละเอียดปลีกย่อยเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่ง Standard ที่ได้วางไว้

ขั้นตอนที่ 4 การป้องกันในระดับลึก และการนำเอาสูตรสำเร็จต่างๆ มาใช้

ในขั้นตอนนี้เป็นกระบวนการที่มีรายละเอียด ใช้กำลังคน งบประมาณ ระยะเวลาในการดำเนินการ และความรู้เชิงลึกในด้าน Information Security เพื่อทำให้ระบบขององค์การมีความปลอดภัยทั้งในปัจจุบัน และอนาคต โดยจะดำเนินการดังต่อไปนี้

- การจัดการแบบ “Layered Security” โดยจัดแบ่งระบบออกเป็นชั้นๆ แล้วทำการป้องกันระบบแต่ละชั้นโดยมีรายละเอียดในการป้องกันแตกต่างกันออกไปในแต่ละชั้น ในทางเทคนิคจะวิธีการดังกล่าวว่า “Compartmentalization” เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ เป็นต้น
- ออกแบบระบบเครือข่ายใหม่โดยเน้นความปลอดภัยในการใช้งานมากขึ้น
- ปรับแต่ง Configuration ต่างๆ ในระบบให้มีช่องโหว่น้อยที่สุด
- จัดทำแผนจัดการกับการเปลี่ยนแปลงต่างๆ ที่อาจเกิดขึ้นในระบบ
- สร้างระบบ Log Monitoring ขึ้นในระบบเพื่อการเฝ้าระวัง
- ดำเนินการเพื่อรักษาความปลอดภัยระบบย่อย
- วางแผนการกอบกู้ระบบในกรณีฉุกเฉิน (Recovery Plan) และแผนการจัดการกับความเสียหายเพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่องไม่หยุดชะงัก (Business Contingency Plan)

นอกจากนี้ยังมีแนวทางในการบริหารจัดการที่ง่าย และสามารถใช้งานได้ทันที นั่นคือการนำเอาสูตรสำเร็จใจการบริหารจัดการมาใช้งาน (Best Practice Implementation) โดยต้องพิจารณาถึงความเหมาะสม และสอดคล้องกับองค์การซึ่ง Best Practice โดยทั่วไปจะประกอบไปด้วยรายละเอียดทางด้านเทคนิคที่ผู้ดูแลระบบควรปฏิบัติ ตั้งแต่การติดตั้งระบบจนถึงการใช้งานรายวัน รายละเอียดการปิดช่องโหว่ต่างๆ

ขั้นตอนที่ 5 การสร้างความตระหนักเกี่ยวกับการรักษาความปลอดภัย และการฝึกอบรมความรู้ทางเทคนิคต่างๆ

ในขั้นตอนการฝึกอบรมเพื่อความตระหนักเกี่ยวกับการรักษาความปลอดภัยนั้น เป็นขั้นตอนที่มีความสำคัญเป็นอย่างมาก แต่เป็นขั้นตอนที่หลายๆ องค์การมองข้าม เนื่องจากส่วนใหญ่มองว่าควรจะเป็นการฝึกอบรมเฉพาะฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่เกี่ยวข้องด้านความปลอดภัยเท่านั้น แต่ในความเป็นจริงแล้วผู้บริหารตลอดจนบุคลากรที่ต้องใช้งานข้อมูลขององค์การมีความจำเป็นที่จะต้องได้รับการฝึกอบรมอย่างทั่วถึง

ในการฝึกอบรมต่างๆ ควรมีการแสดงกรณีตัวอย่างหรือ Case Study ให้ผู้เข้ารับการฝึกอบรมสามารถรับรู้ และเข้าใจได้อย่างเป็นรูปธรรม นำไปสู่การเกิดความตระหนักเรื่องความปลอดภัยในการใช้งานข้อมูล โดยจะมีฝ่ายเทคโนโลยีสารสนเทศคอยสนับสนุน และควบคุมการใช้งานในด้านเทคนิคประกอบกับระเบียบ และแนวปฏิบัติขององค์การที่เป็นกรอบในการทำงานซึ่งในการฝึกอบรมนั้นจะถูกแบ่งออกเป็นหลายระดับตามกลุ่มผู้ใช้งาน ได้แก่

- กลุ่มผู้บริหารระดับสูง
- กลุ่มผู้บริหารระดับกลาง
- กลุ่มผู้ดูแลระบบ (System Administrator)
- กลุ่มผู้ดูแลความปลอดภัยระบบคอมพิวเตอร์ (Security Administrator)
- กลุ่มผู้ตรวจสอบระบบสารสนเทศ (IT Auditor)
- กลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (User)

อ่านต่อฉบับหน้า