วิสัยทัศน์และการสร้างองค์กรแห่งความมั่นคงปลอดภัยด้านข้อมูล

ดร. ครรชิต มาลัยวงศ์ ราชบัณฑิต

ที่ปรึกษา บจม. ไอ.ซี.ซี. อินเตอร์เนชั่นแนล

เนื้อหาคำบรรยาย

- องค์กรที่ประสบปัญหาวิกฤติ
- ความหมายของความมั่นคง และ ความปลอดภัย
- องค์กรที่มีความมั่นคงปลอดภัย
- วิสัยทัศน์ และ กลยุทธ์
- สรุป

องค์กรเป็นเหมือนทศกัณฐ์

- องค์กรทุกวันนี้มีลักษณะเหมือนทศกัณฐ์มากขึ้น
- ในวรรณกรรมเรื่องรามเกียรติ ทศกัณฐ์ ถอดดวงใจใส่กล่องไปฝากไว้กับพระฤาษี ทำให้ไม่มีใครฆ่าทศกัณฐ์ได้ ทำให้พระรามต้องส่งหนุมานไปหลอกเอากล่องดวงใจมานั่นแหละจึงฆ่าได้
- องค์กรจัดเก็บข้อมูลที่สำคัญต่อองค์กรเป็นจำนวนมากเอาไว้ในฐานข้อมูลซึ่งอยู่ในกล่องฮาร์ดดิสก์ หากใครเอาฮาร์ดดิสก์นี้ไปได้ก็สามารถฆ่าองค์กรได้

องค์กรประสบปัญหาข้อมูลเป็นประจำ

- พนักงานธนาคารแห่งหนึ่งทำข้อมูลลูกค้ากลุ่มหนึ่งในฐานข้อมูลหายไปในวันเงินเดือนออก สร้างความปั่นป่วนไปทั่ว
- พนักงานธนาคารอีกแห่งหนึ่ง แก้ไขโปรแกรมที่กำลังใช้งานอยู่ ทำให้เกิดช่องว่างให้คนมาถอนเงินไปโดยไม่มีเงินในบัญชีรวมแล้วนับสิบล้าน
- พนักงานธนาคารในไต้หวัน พิมพ์ข้อมูลเงินเดือนผิด แทนที่จะจ่ายเงินเดือนให้คนละ 15,000 NT กลับจ่ายไปคนละ 15,000,000 NT คนงานหลายคนเบิกเงินแล้วหายตัวไป

ปัญหาใหม่มาจากนอกองค์กร

- ธนาคารซิตีแบงก์ในลอนดอนตรวจพบว่า พนักงานได้โอนเงินไปยังบัญชีแห่งหนึ่งในอเมริกาใต้ตามคำสั่งของลูกค้า แต่คำสั่งนั้นมาโดยวิธีการที่ไม่ถูกต้อง และมีการสั่งโอนเงินที่ไม่มีตัวตนมาเป็นทอด ๆ จากอินโดนีเซีย ในที่สุดก็ตรวจพบว่าตัวการอยู่ในเซนต์ปีเตอร์สเบิรก ในรัสเซีย และต้องใช้ความพยายามมากทีเดียวที่จะนำตัวการมาลงโทษที่อังกฤษ

ปัญหาจากอินเทอร์เน็ต

- คอมพิวเตอร์ที่ต่อเชื่อมกับอินเทอร์เน็ตทุกเครื่องมีความเสี่ยง
  - จากไวรัสคอมพิวเตอร์
  - จากหนอนคอมพิวเตอร์
  - จากคุกกี้
  - จากสปายแวร์
  - จากสแปมเมล
  - จากแฮคเกอร์ที่จ้องเล่นงานอย่างลับ ๆ
  - จากพนักงานที่ไม่พอใจและต้องการแก้แค้น

การมีคอมพิวเตอร์ใช้จึงเป็นความเสี่ยง

- การประยุกต์คอมพิวเตอร์ในทางธุรกิจปัจจุบันมีความเสี่ยงสูง
- หากโปรแกรมประยุกต์ทำงานผิดพลาด บริษัทอาจเสียหาย ขายหน้า และอาจจะเกิดปัญหาทางกฎหมายได้
- หากเครือข่ายขัดข้อง บริษัทอาจแข่งขันกับคู่แข่งไม่ได้
- หากเกิดอุบัติภัยกับระบบคอมพิวเตอร์ บริษัทอาจไม่สามารถทำธุรกิจต่อไปได้
- การกำหนดนโยบายเพื่อรับมือกับปัญหาความเสี่ยงจึงเป็นสำคัญ

ความมั่นคง

- หน่วยงานที่ secure หรือมีความมั่นคง หมายถึงหน่วยงานที่มีความสามารถที่จะดำเนินงานต่อไปได้ แม้จะประสบปัญหาจากภัยพิบัติที่ไม่คาดฝันทั้งจากน้ำมือคนหรือธรรมชาติ ทนทานต่อการกลั่นแกล้งจากผู้ไม่หวังดี และ การก่อการร้าย อีกทั้งมีวิธีการที่สามารถป้องกัน ต่อต้าน และ ตรวจจับ การบุกรุก การโจรกรรม การจารกรรม หรือการหลอกลวงที่จะทำให้หน่วยงานเสียหายได้

ความปลอดภัย

- หน่วยงานที่มีความปลอดภัย หรือ safety หมายถึงหน่วยงานที่สามารถคุ้มครองชีวิตและทรัพย์สินของลูกค้า พันธมิตร และพนักงาน ไม่ให้สูญหาย เสียหาย หรือถูกนำไปใช้โดยไม่ได้รับการยินยอมจากเจ้าของและผู้เกี่ยวข้อง
- อินเทอร์เน็ตที่ปลอดภัย หมายถึง ระบบที่ป้องกันไม่ให้ผู้ใช้โดยเฉพาะเด็กในครอบครัวได้รับข่าวสารที่เป็นพิษเป็นภัย สามารถป้องกันไม่ให้เข้าถึงเว็บลามกอนาจารได้

คนไทยนิยมใช้คู่กัน

- คนไทยทั่วไปนิยมใช้ทั้งสองคำ คือ ความมั่นคงปลอดภัย แต่ในทางวิชาการแล้ว แม้ทั้งสองจะเกี่ยวกัน แต่ก็ต่างกัน
- ในทางมาตรฐานเราใช้คำว่า **Information Security** หรือ ความมั่นคงของสารสนเทศ ไม่ได้ใช้คำว่า ความมั่นคงของข้อมูล
- ที่สำคัญคือ เราสนใจพัฒนามาตรฐานและวิธีปฏิบัติทางด้านการจัดการความมั่นคงของสารสนเทศ (**Information Security Management**) มากขึ้น

Information Security

- ความมั่นคงปลอดภัยของสารสนเทศ เน้นที่การปกป้องสารสนเทศจากปัญหาคุกคามต่าง ๆ เพื่อให้แน่ใจว่า หน่วยงาน
  - สามารถดำเนินงานต่อไปได้
  - เกิดความสูญเสียทางธุรกิจน้อยที่สุดเมื่อเกิดปัญหาขึ้น
  - ได้รับผลตอบแทนจากการลงทุนป้องกันปัญหามากที่สุด
  - ได้รับความเชื่อถือจากตลาดหลักทรัพย์ พันธมิตร ลูกค้า และหน่วยงานที่กำกับดูแล

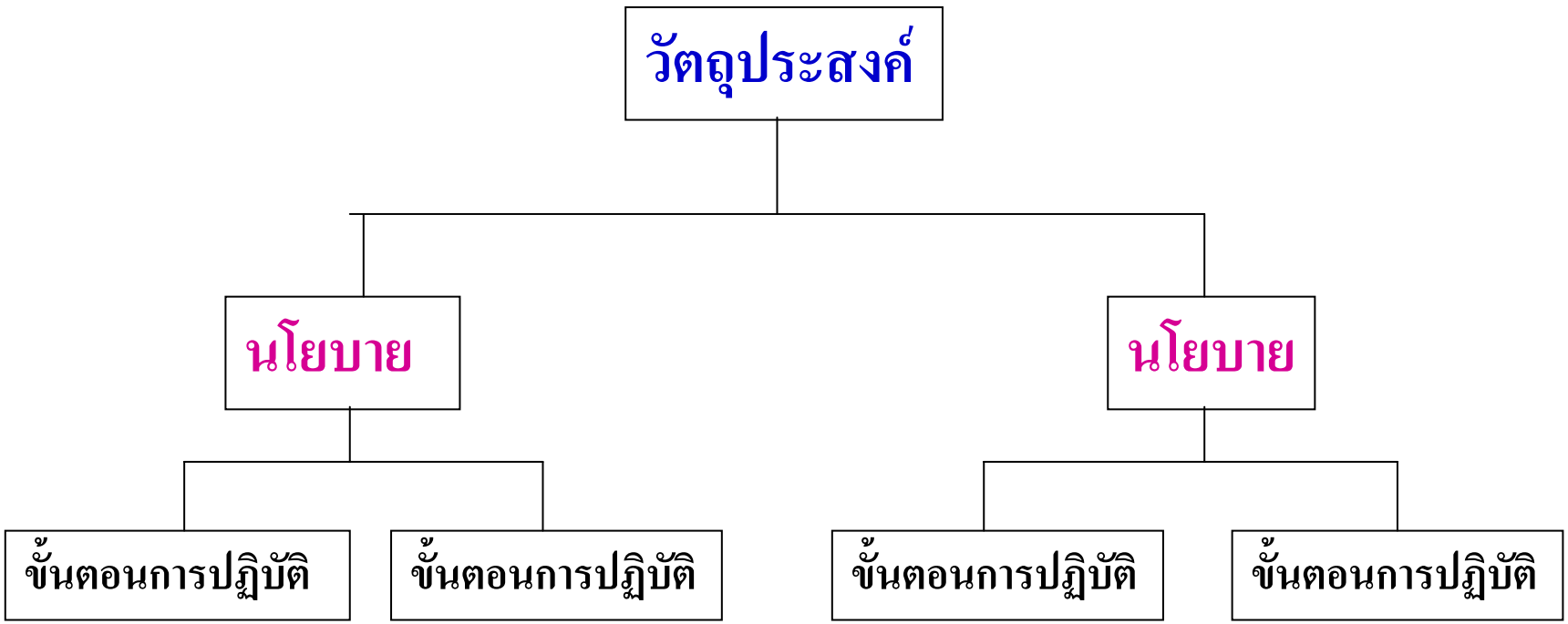
Information Security เกี่ยวกับ 3 ประเด็นหลัก

- **Confidentiality ความมั่นคงของสารสนเทศช่วยให้แน่ใจว่าข้อมูลและสารสนเทศที่เก็บไว้นั้น จะเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น**
- **Integrity ช่วยป้องกันรักษาให้ข้อมูลและสารสนเทศ ตลอดจนวิธีการประมวลผล มีความแม่นยำและสมบูรณ์**
- **Availability ช่วยให้แน่ใจว่าผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูลและสารสนเทศนั้น สามารถเข้าถึงข้อมูลและสารสนเทศที่ต้องการได้จริง**

การบริหารงาน Information Security

- โดยปกติเราไม่ใช้คำว่า Vision กับงานด้านนี้ เพราะ Vision มักจะใช้กับความคิดเชิงธุรกิจ เมื่อมีวิสัยทัศน์แล้วจึงกำหนดวัตถุประสงค์ให้สอดคล้องกับวิสัยทัศน์
- ไม่ว่าวิสัยทัศน์เป็นอย่างไร ต้องกำหนดวัตถุประสงค์ในการจัดการความมั่นคงของสารสนเทศให้ชัดเจน
- จากนั้นจึงกำหนดนโยบาย (Policies) และ ขั้นตอนการปฏิบัติ (Procedures)

ความสัมพันธ์ระหว่างวัตถุประสงค์กับนโยบาย



การตรวจสอบ

- การกำหนดขั้นตอนสำหรับปฏิบัติเป็นเรื่องจำเป็นมาก แต่ยังไม่พอเพียงที่จะแน่ใจว่า หน่วยงานมีความมั่นคงด้านสารสนเทศ
- หน่วยงานต้องสร้างกระบวนการตรวจสอบ (Audit) ด้วย
- การตรวจสอบด้านความมั่นคงของสารสนเทศ เป็นการติดตามวัดผล และรายงานความเสี่ยงทางด้านสารสนเทศ พยายามลดความเสี่ยงด้วยการทำให้พนักงานของหน่วยงานตื่นตัวสนใจป้องกันปัญหา และ พยายามปรับปรุงวิธีการปฏิบัติด้วย

การควบคุมต้องได้ผล

- ตัวอย่างของนโยบาย
  - เมื่อคอมพิวเตอร์ของพนักงานคนใดรายงานว่าได้ตรวจพบไวรัสคอมพิวเตอร์แล้ว พนักงานผู้นั้นจะต้องแจ้งให้ศูนย์สารสนเทศทราบทันที แม้ว่าโปรแกรมที่ติดตั้งไว้จะได้ทำลายไวรัสนั้นไปแล้ว
- นโยบายเช่นนี้อาจดูหยุมหยิมจนพนักงานไม่สนใจปฏิบัติตาม เมื่อเป็นเช่นนั้นศูนย์สารสนเทศก็ไม่ได้รับทราบปัญหา และไม่ได้ติดตามไปหาสาเหตุที่ทำให้เกิดไวรัสนั้น
- ดังนั้นต้องมีวิธีการควบคุมให้พนักงานปฏิบัติตามนโยบายด้วย

การควบคุมจะได้ผลถ้า...

- มีการสร้างสิ่งแวดล้อมที่มั่นคงอย่างพอเพียง
  - มีการติดตั้งไฟร์วอลล์เพื่อป้องกันระบบ
  - มีการติดตั้งโปรแกรมในเมลเซิรฟเวอร์เพื่อตรวจสอบโปรแกรมร้ายที่ส่งมากับอีเมล
  - มีการติดตั้งโปรแกรมในดาต้าเบสเซิรฟเวอร์เพื่อตรวจสอบโปรแกรมร้าย และ รายงานการพยายามใช้งานของผู้ที่ไม่ได้รับอนุญาต
- มีการประชาสัมพันธ์และเผยแพร่ข่าวสารให้พนักงานเห็นความสำคัญของความมั่นคงของสารสนเทศ

การควบคุมจะได้ผลถ้า...

- ผู้บริหารเห็นความสำคัญและให้การสนับสนุน
- มีการแต่งตั้งผู้ทำหน้าที่เป็น CSO
- มีการจัดสรรทรัพยากรให้แก่ฝ่ายความมั่นคงด้านสารสนเทศอย่างพอเพียงที่จะดำเนินการ
- มีการกำหนดขั้นตอนการปฏิบัติอย่างละเอียด
- พนักงานทุกคนเห็นความสำคัญและปฏิบัติตาม

สรุปด้วยคำถาม

- นักศึกษาจะทำอย่างไรถ้าหากมาถึงห้องปฏิบัติการแล้วพบว่าคอมพิวเตอร์หายไปหนึ่งเครื่อง
- นักศึกษาจะทำอย่างไรถ้าหากคลิกเข้าไปอ่านเว็บของศรีปทุมแล้วพบว่ามีถูกแฮคและมีรูปอนาจารปรากฏแทน
- นักศึกษาให้เพื่อนยืมหมายเลขและรหัสผ่านไปใช้หรือไม่
- นักศึกษาจะทำอย่างไรถ้าหากเครื่องโน้ตบุ๊กของนักศึกษาที่วางไว้ในห้องเรียนหายไป และในนั้นมีรายงานที่จะต้องส่งอาจารย์ด้วย

คำถาม