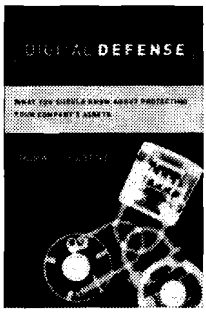
Book Review

นิพนธ์ เบญจกุล



Parenty, T.J., 2003.

Digital Defense :

What You Should Know About

Protecting Your Company's Assets.

Harvard Business School Publishing Corporation, New York.

หนังสือการป้องกันในระบบดิจิตอลที่ให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศที่เน้นที่ภาคธุรกิจ กล่าวถึงเรื่องราวใหม่ของไวรัส นักเจาะระบบคอมพิวเตอร์ และการประกันความผิดมารยาทของสื่อมวลชน ในครึ่งแรกของปี ค.ศ. 2000 มีไวรัสใหม่ 23,279 ตัว ทีกระจายอยู่ในคอมพิวเตอร์ การจัดการด้านความปลอดภัยในคอมพิวเตอร์กระทำผิดพลาดอย่างมาก เพื่อความมั่นคงในระบบคอมพิวเตอร์มีประเทศมากกว่า 40 ประเทศที่ตัดสินใจปรับปรุงระบบการป้องกันความปลอดภัยเพื่อให้ลูกค้าใช้ดำเนิน การทางการเงิน

ทำไมจึงต้องมีการจัดการปัญหาความปลอดภัย

คำตอบก็คือการจัดการความเสี่ยง การโจมตีบนคอมพิวเตอร์ และการขโมยหรือการใช้คอมพิวเตอร์ในทางที่ไม่เหมาะสม เป็นการเสี่ยงต่อการกำหนดสารสนเทศร่วมกัน เพื่อตอบสนองธุรกิจที่ต้องการทั้งการประเมินราคาและจัดการ ผู้ดูแลระบบปลอดภัยจะต้องประพฤติตนเสมือนผู้รับผิดชอบทางการเงินเหมือนกับการปกป้องทรัพย์สินของบริษัท นั่นคือเหตุผลว่าทำไม

ธุรกิจควรจะใช้เวลามาดูความปลอดภัยสารสนเทศ

หนังสือนี้ตอบสนองความต้องการของนักธุรกิจที่เห็นความสำคัญของการป้องกันวิกฤตของบริษัทที่อาจเกิดขึ้นจากการใช้สารสนเทศเป็นเครื่องมือที่ช่วยให้ผู้บริหารมีความเข้าใจระหว่างความสัมพันธ์แข็งแกร่งระหว่างระบบความปลอดภัยและกลยุทธ์ในองค์การ การเข้าใจผลกระทบของรูปแบบและนโยบายสูงสุดของความปลอดภัย

หนังสือนี้ได้แนะนำวิธีการในการพัฒนาและการปฏิบัติในกระบวนการจัดการความปลอดภัย ซึ่งวิธีการเข้าสู่ระบบความปลอดภัยของสารสนเทศ

หนังสือนี้สะท้อนถึงกระบวนการประเมินเอกสารและวิธีการความปลอดภัยสารสนเทศของบริษัทให้เหมาะสมการแก้ปัญหา

บทที่ 1 การระบุคุณสมบัติสารสนเทศ

เริ่มต้นด้วยการเกริ่นนำว่าทำไมระบบสารสนเทศในปัจจุบันจึงไม่มีความปลอดภัย รูปแบบการใช้สารสนเทศมี 3 รูปแบบคือ (1) ใช้แทนเอกสารที่เป็นกระดาษ (2) ใช้ควบคุมการคำนวณ (3) ไม่ได้อยู่ในการควบคุมจากบริษัท และมีนำเสนอตารางคุณสมบัติสารสนเทศ ประกอบด้วย 2 ตาราง คือ ตารางที่ 1 ตารางคุณสมบัติสารสนเทศที่การกำหนดขอบเขตของสารสนเทศ ตารางที่ 2 ตารางคุณสมบัติสารสนเทศที่การกำหนดชื่อคุณสมบัติ การประเมินค่า สถานการณ์เป็นเจ้าของ และได้บอกถึงประโยชน์ของการใช้ตารางคุณสมบัติสารสนเทศ

บทที่ 2 ข้อกำหนดความไม่มั่นคงในปัจจุบัน

เมื่อมีการกำหนดคุณสมบัติสารสนเทศของบริษัทหนึ่ง ๆ ในขั้นต่อไปจะต้องกำหนดถึงความสามารถในการใช้งาน จะต้องมีการเปรียบเทียบระหว่างความสามารถการเข้าถึงคุณสมบัติจริง ๆ กับความสามารถที่ควรจะเข้าถึงคุณสมบัติ จำนวนสมาชิก รูปแบบสมาชิก ไม่ควรให้สารสนเทศของบริษัทมีเพียงหนึ่งมาตรวัดซึ่งจะเป็นการเสี่ยง และยังกล่าวถึงการเข้าถึงสารสนเทศอย่างถูกกฎหมายและการใช้ตารางคุณสมบัติสารสนเทศ เส้นทางของการเข้าทำลายระบบสารสนเทศ และการตรวจสอบความปลอดภัยสูงสุด

บทที่ 3 การป้องกันคอมพิวเตอร์

นี่เป็นจุดหนึ่งที่นักธุรกิจหลาย ๆ คน คิดถึงการทำงานที่มีระบบความปลอดภัยทางสารสนเทศ เขารู้ว่าอะไรคือคุณสมบัติสารสนเทศ เขามีและสามารถใช้มัน และเข้าติดตั้งและทำให้ระบบความปลอดภัยทันสมัยเพื่อขัดขวางนักเจาะระบบ หลายคนอาจใช้การป้องกัน

โปรแกรมไวรัสและการกรองโปรแกรมไวรัส(Firewall) เทคโนโลยีคล้ายกับโปรแกรมที่กรองและป้องกันไวรัสที่ใช้ป้องกันคอมพิวเตอร์ แต่มันไม่สามารถจัดหาได้อย่างเหมาะสมในการป้องกันคุณสมบัติสารสนเทศของบริษัท หรือการจัดการทางธุรกิจ มี 2 คำถามที่ควรรู้ คือ

1. คุณสมบัติสารสนเทศและกระบวนการทางธุรกิจของคุณต้องใช้เทคโนโลยีป้องกันความปลอดภัยด้วยอะไร

2. เทคโนโลยีความปลอดภัยอันไหนที่สอดคล้องกับคุณสมบัติสารสนเทศและกระบวนการธุรกิจแบบอัตโนมัติ

การกรองไวรัส (Firewall) เป็นวิธีป้องกันรอบนอก ที่ประกอบด้วยฮาร์ดแวร์และหรือซอฟแวร์ที่ทำหน้าที่ระหว่างคอมพิวเตอร์กับอินเทอร์เน็ต มีเป้าหมายคือ จำกัดการติดต่อระหว่างโลกภายนอกกับโลกภายในด้วยการเฝ้าดูที่ประตูเชื่อมต่อ การเข้าร่วมของคำว่า "ผนัง" ในไฟร์วอลล์ คือ การทำให้เหมือนกำแพงเมือง แต่ไฟร์วอลล์ในความจริงแล้วคือจำนวนประตูเชื่อมต่อ มันควบคุมสารสนเทศที่ผ่านระหว่างคอมพิวเตอร์ของบริษัทและอินเทอร์เน็ต มีสิ่งที่ไฟร์วอลล์ไม่สามารถทำได้คือไม่สามารถป้องกันการโจมตีจากผู้ต่อต้านระบบความปลอดภัย และไม่สามารถป้องกันบริษัทจากพนักงานในการให้บริการลูกค้า การทำงานของโปรแกรมป้องกันไวรัส การค้นหาผู้บุกรุกและการให้บริการจัดการความปลอดภัย

บทที่ 4 การพัฒนากระบวนการความปลอดภัยบนพื้นฐานความไว้วางใจ

เป็นการดูเทคโนโลยีความปลอดภัยสารสนเทศใหม่ๆ มีการกำหนดว่าอะไรที่บริษัทต้องการความไว้วางใจในกิจกรรมทางธุรกิจด้วยกันและเลือกเทคโนโลยีด้านความปลอดภัยสารสนเทศอยู่บนพื้นฐานของความสามารถและการสร้างความไว้วางใจในโลกดิจิตอล สำหรับวัตถุประสงค์ 4 ประการที่สำคัญของความไว้วางใจ

1. ความลับ(Confidentiality)
2. การแสดงตัว (Identity)
3. การเข้าถึงข้อมูล (Access)
4. ลักษณะที่เชื่อถือได้ (Authenticity)

บทที่ 5 การเก็บสารสนเทศด้านความไว้วางใจ

วัตถุประสงค์ความไว้วางใจในลำดับแรกกำหนดปัญหาความต้องการไว้สำหรับสิ่งแวดล้อมส่วนตัวในสิ่งซึ่งชักนำธุรกิจและนำเข้าของการปกป้องเป็นความลับของสารสนเทศ

การนำข้อความมาเข้ารหัสสามารถจัดเตรียมบริษัทกับความลับและเป็นความลับเขาต้องการและอะไรคือการสร้างรหัสลับ ธุรกิจเดี่ยว ๆ มีการป้องกันโดยรหัสลับอย่างไร รหัสลับสามารถล้มเหลวได้อย่างไร และจะสร้างรหัสลับให้สู่จุดสูงสุดอย่างไร

บทที่ 6 การสร้างการระบุตัวตน

การไม่รู้จักกันของหุ้นส่วนบริษัท ผู้จำหน่าย หรือของลูกค้าที่ติดต่อทางธุรกิจที่แท้จริงไม่สามารถมองเห็นกันได้ทั้งหมด ในบทนี้ อธิบายว่าบริษัทสามารถสร้างและการระบุตัวตนในระบบดิจิตอลแบบอัตโนมัติเพื่อสร้างความไว้วางใจกับหุ้นส่วนทางการค้าขายแบบ online โดยได้บอกถึงการสร้างการแสดงตัวในระบบดิจิตอล ความน่าเชื่อถือของการแสดงตัวในระบบดิจิตอล การพิสูจน์ให้รู้จักบุคคล การพิสูจน์คุณสมบัติของบุคคล การพิสูจน์การวัดความมีชีวิต การใช้ระบบรับรองด้วยดิจิตอล เมื่อการแสดงตัวในระบบดิจิตอลเสียหาย การเลือกใช้เทคโนโลยีการแสดงตัวและลักษณะที่น่าเชื่อถือ และการสร้างการแสดงตัวและลักษณะที่น่าเชื่อถือให้ดีที่สุดได้อย่างไร

บทที่ 7 การเข้าถึงการควบคุมในโลกดิจิตอล

คุณค่าของเครื่องมือบริษัทคือสารสนเทศขึ้นอยู่กับความสามารถของบริษัทในการสร้างสารสนเทศให้กับคนที่มีสิทธิและป้องกันจากคนที่ไม่มีสิทธิเข้ามาสู่ระบบ ในบทนี้ยังครอบคลุมไปถึงทางเลือกความปลอดภัยสารสนเทศ เช่น การควบคุมการเข้าถึงโดยหน้าที่หรือบทบาทการทำงานและกล่าวถึงใครบ้างที่ควรจะเข้าสู่ระบบ การเข้าถึงพื้นฐานของงานในหน้าที่ การเข้าถึงพื้นฐานของบทบาทของลูกจ้าง การเข้าถึงพื้นฐานของกรอบของจริยธรรม การควบคุมที่ไม่สามารถควบคุมได้ หุ้นส่วนทางธุรกิจและการเสี่ยงร่วมกัน การค้นหาการเข้าถึงการควบคุมหน้าที่ และการควบคุมการเข้าถึงการบริหารให้สู่จุดสูงสุดได้อย่างไร

บทที่ 8 การรับรู้ว่าอะไรคือความจริงในโลกคอมพิวเตอร์

เขียนเอกสารและการลงลายมือชื่อจัดเตรียมกับบริษัทแบบดั้งเดิมกับการบันทึกธุรกิจน่าเชื่อถือ ในสิ่งแวดล้อมทางธุรกิจของโลกดิจิตอลไม่มีการบันทึกความเชื่อถือ บทนี้บอกถึงการจัดการกับปัญหาว่าบริษัทสามารถใช้เทคโนโลยีจัดการกับปัญหาได้อย่างไร เช่น การตรวจสอบและการสร้างรหัสเป็นการสร้างความเชื่อถือในการบันทึกทางอิเล็กทรอนิกส์ และบอกถึงว่าอะไรสารสนเทศที่สามารถทำให้คุณไว้วางใจ การสร้างความปลอดภัยในการดาวน์โหลด การบันทึกกิจกรรมทางด้านดิจิตอล และอะไรที่เป็นสิ่งที่น่าจะให้ความเชื่อถือที่สุด

บทที่ 9 ข้อแนะนำกระบวนการระบบความปลอดภัยไปสู่การปฏิบัติ

การป้องกันของบริษัทด้านสารสนเทศส่งผลถึงปัญหาองค์การเหมือนกับอุปสรรคของเทคโนโลยี รวมไปถึงผู้บริหารอาวุโส ที่จะซื้อด้วยการงบประมาณและการสร้างทีมงานด้านความปลอดภัยแล้ว บริษัทยังต้องการเกี่ยวกับความในการรวบความปลอดภัยสารสนเทศเข้ากับการตัดสินใจทางธุรกิจ และกล่าวถึงความพอใจของฝ่ายบริหาร การจำแนกทีมระบบความปลอดภัยออกเป็น 2 ทีมคือ ทีมหลัก กับทีมสนับสนุน งบประมาณและตารางทำงานและบทบาทของนโยบายและข้อตกลง

บทที่ 10 การปฏิรูปธุรกิจไปสู่ระบบความปลอดภัยทางสารสนเทศ

ครั้งหนึ่งบริษัทมีการจัดการปัญหาด้วยความต้องการความปลอดภัยสารสนเทศ ในปัจจุบันขั้นตอนต่อมาการค้นหาโอกาสธุรกิจทางใหม่ ๆ ว่าสามารถปฏิบัติและสนับสนุนตามกติกาด้านความปลอดภัยสารสนเทศ ในโลกเป็นเต็มด้วยตัวอย่างของกิจกรรมธุรกิจ จากการซื้อของทาง online ได้แพร่กระจายไปถึงการดูภาพยนต์ในโรงภาพยนต์ ความปลอดภัยสารสนเทศนั้นทำได้เค้าโครงความไว้วางใจสามารถช่วยบริษัทค้นหาโอกาสใหม่ของบริษัทเอง โดยในบทนี้จะกล่าวถึงระบบความปลอดภัยกระทบต่อธุรกิจอย่างไร การใช้เทคโนโลยีระบบความปลอดภัยเป็นนวตกรรมระบบความปลอดภัยเป็นมากกว่าความปลอดภัยในระบบอินเทอร์เน็ต ระบบความปลอดภัยไม่ใช่นวัตกรรมทางเทคโนโลยี และอนาคตจะใช้อะไรมาจัดการความปลอดภัยสารสนเทศ