บทที่ 2

ทฤษฎี เทคโนโลยี และงานวิจัยที่เกี่ยวข้อง

2.1 การจัดการของระบบจัดการความรู้

การจัดการกับการตัดสินใจ (ศรีไพร และเจษฎาพร, 2549)

การจัดการ (Management) หมายถึง การบริหารอย่างเป็นระบบ ประกอบด้วยกิจกรรมของกลุ่มบุคคลที่ร่วมมือกันดำเนินงานเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้โดยใช้กระบวนการและทรัพยากรอย่างเหมาะสมและเกิดประโยชน์สูงสุด การจัดการเป็นศาสตร์และศิลปะ ซึ่งกระบวนการจัดการประกอบด้วยการวางแผน (Planning) การจัดองค์การ (Organizing) การสั่งการหรืออำนวยการ (leading/Directing) และการควบคุม (Controlling) โดยการจัดการที่มีประสิทธิภาพนั้น ผู้บริหารจะต้องสามารถนำเอาความรู้ ความเข้าใจในศาสตร์ด้านการบริหารมาประยุกต์ใช้ให้เหมาะสมกับการทำงาน สถานการณ์ และสิ่งแวดล้อมโดยเฉพาะในสภาพแวดล้อมทางธุรกิจที่มีการแข่งขันกันสูง ผู้บริหารจะต้องรู้จักเลือกและวิเคราะห์ข้อมูลเพื่อให้ได้สารสนเทศในรูปแบบที่ง่ายต่อความเข้าใจและเป็นประโยชน์ต่อการบริหารและการตัดสินใจ ตลอดจนมองหาโอกาสและวางกลยุทธ์ได้อย่างชาญฉลาด รวดเร็วและเหนือคู่แข่งขันจึงจะสามารถนำพาองค์การให้เจริญก้าวหน้าต่อไปได้

ความจำเป็นในการพัฒนาระบบสารสนเทศ (ศรีไพร และเจษฎาพร, 2549)

การพัฒนาระบบเป็นการสร้างระบบงานใหม่หรือปรับปรุงระบบงานเดิมที่มีอยู่ให้ดีกว่าเดิมเพื่อแก้ปัญหาในการดำเนินงานบางอย่าง เช่น ผู้ใช้อาจไม่ได้รับข้อมูลที่ต้องการเนื่องจากมีความต้องการเพิ่มเติมหรือสิ่งแวดล้อมในการทำงานเปลี่ยนไป เทคโนโลยีที่ใช้กับระบบปัจจุบันล้าสมัยและมีค่าใช้จ่ายในการบำรุงรักษาสูง หรือผู้บริหารต้องการสร้างโอกาสในการแข่งขันในการดำเนินธุรกิจ ซึ่งสามารถสรุปความจำเป็นในการพัฒนาระบบได้ดังนี้

- **การเปลี่ยนแปลงกระบวนการบริหารและการปฏิบัติงาน**

ระบบเดิมไม่สามารถให้ข้อมูลหรือทำงานได้ตามต้องการ มีการดำเนินงานหลายขั้นตอนยุ่งยากในการรวบรวมข้อมูลเพื่อนำมาจัดทำข้อมูลสรุปสำหรับการติดตามการปฏิบัติงานโดยรวมขององค์การ และไม่สามารถสนับสนุนข้อมูลให้กับผู้บริหารได้เป็นอย่างดี จึงจำเป็นต้องพัฒนาหรือปรับปรุงระบบสารสนเทศที่สามารถช่วยให้ขั้นตอนการปฏิบัติงานภายในและกระบวนการบริหารมีประสิทธิภาพมากขึ้น

- **การเปลี่ยนแปลงด้านเทคโนโลยี**

เทคโนโลยีมีราคาถูกลง เทคโนโลยีที่ใช้อยู่ในระบบสารสนเทศปัจจุบันล้าสมัย ค่าใช้จ่ายในการบำรุงรักษาระบบมีราคาสูง เมื่อมีอุปกรณ์หรือชิ้นส่วนบางอย่างเสียไม่สามารถซ่อมหรือหาอุปกรณ์ทดแทนได้กอรปกับความต้องการที่จะลดต้นทุนและการปรับปรุงคุณภาพการบริการลูกค้า จึงต้องรับเอาเทคโนโลยีใหม่ ๆ มาประยุกต์ใช้ซึ่งทำให้มีการเปลี่ยนแปลงระบบการทำงานที่มีอยู่เดิม

- **การปรับองค์การและสร้างความได้เปรียบในการแข่งขัน**

ระบบที่ใช้งานอยู่ในปัจจุบันมีขั้นตอนการทำงานที่ยุ่งยากซับซ้อน ขาดเอกสารอ้างอิงหรือเอกสารที่มีอยู่ไม่ได้มาตรฐาน ทำให้การปรับปรุงหรือแก้ไขทำได้ยากหรือมีความจำเป็นต้องปรับปรุงระบบการควบคุมกอรปกับความต้องการปรับองค์การให้เหมาะสมเพื่อสามารถตอบสนองต่อการเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจได้อย่างรวดเร็วและสร้างความได้เปรียบในการแข่งขัน ซึ่งระบบปัจจุบันไม่สามารถรองรับการเปลี่ยนแปลงในอนาคตได้ องค์การจึงมองหาวิธีการหรือแนวทางใหม่ ๆ เพื่อรักษาส่วนแบ่งตลาดเอาไว้ หรือเพื่อขยายตลาดเพิ่มขึ้น

ปัจจัยที่มีผลต่อการพัฒนาระบบสารสนเทศให้ประสบความสำเร็จ

การพัฒนาระบบสารสนเทศให้ประสบความสำเร็จจำเป็นต้องอาศัยปัจจัยสนับสนุนหลายด้าน ได้แก่

1. การสนับสนุนจากฝ่ายบริหาร ในการพัฒนาระบบสารสนเทศใด ๆ ก็ตาม ย่อมต้องการทรัพยากรทั้งด้านงบประมาณ บุคลากร และเวลา หากผู้บริหารไม่สนับสนุนหรือไม่ให้ความสนใจในการพัฒนาระบบ เช่น ไม่อนุมัติงบประมาณจัดซื้อฮาร์ดแวร์และซอฟต์แวร์ให้ ก็ยากที่จะพัฒนาระบบให้สำเร็จ นอกจากการสนับสนุนจากผู้บริหารที่เกี่ยวข้องกับระบบแล้ว ผู้พัฒนาระบบยังต้องการความมั่นใจ (Commitment) จากผู้บริหารว่าจะดำเนินการตามที่ตกลงไว้ เช่น เปลี่ยนแปลงขั้นตอนการทำงานใหม่ หรืออาจเปลี่ยนแปลงหน้าที่ของบุคลากรตามที่กำหนดไว้ ซึ่งหากผู้บริหารไม่ดำเนินการตามที่ตกลงไว้อย่างจริงจังจะเป็นสาเหตุให้การพัฒนาระบบไม่ประสบความสำเร็จด้วย

2. การกำหนดขอบเขตและวัตถุประสงค์ที่ชัดเจน ทีมงานพัฒนาระบบจะต้องร่วมกันกำหนดวัตถุประสงค์ ขอบเขต และหน้าที่ของการพัฒนาระบบให้ชัดเจนเพื่อให้เกิดความเข้าใจตรงกันในทีมงานและสามารถพัฒนาระบบได้ตรงตามความต้องการขององค์การ

3. ความรู้ ความสามารถและประสบการณ์ของทีมพัฒนาระบบ สมาชิกของทีมงานควรได้รับการคัดเลือกจากผู้ที่มีความรู้และประสบการณ์ในการพัฒนาระบบ มีมนุษยสัมพันธ์ที่ดี มีความรับผิดชอบในการทำงานและมีความสามารถในการสื่อสารให้เข้าใจซึ่งกันและกัน ทีมงานจะต้องสามารถรวบรวมปัญหาและความต้องการได้อย่างถูกต้อง รู้ความต้องการใช้งานระบบเป็นอย่างดีจึงจะ

สามารถพัฒนาระบบเพื่อแก้ปัญหาหรือเพิ่มโอกาสและศักยภาพในการแข่งขันให้กับองค์การได้ตามวัตถุประสงค์

4. การเลือกใช้เทคโนโลยีสารสนเทศที่เหมาะสม เทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว มีเครื่องมือซอฟต์แวร์จำนวนมากที่ผู้พัฒนาระบบสามารถนำมาใช้สนับสนุนการพัฒนาระบบงาน ควรพิจารณาเลือกใช้เทคโนโลยีที่เหมาะสมกับลักษณะและการใช้งานของระบบ ความคุ้นเคยหรือความสามารถของทีมงานพัฒนาระบบในการใช้ซอฟต์แวร์นั้น ๆ รวมถึงการทำงานร่วมกันได้ของซอฟต์แวร์ ฮาร์ดแวร์ โครงสร้างระบบและฐานข้อมูล โดยต้องคำนึงถึงค่าใช้จ่ายและความง่ายต่อการใช้งานประกอบด้วย ดังนั้นจึงไม่ควรมุ่งเน้นไปที่เทคโนโลยีราคาแพงหรือมีความทันสมัยมาก ๆ แต่ควรพิจารณาด้านความเหมาะสมและความคุ้มค่าที่จะได้รับ

5. การบริหารโครงการพัฒนาระบบสารสนเทศอย่างมีประสิทธิภาพ การพัฒนาระบบสารสนเทศให้เสร็จตามกำหนดเวลา ภายใต้กรอบของงบประมาณและได้ระบบตรงกับความต้องการจำเป็นต้องอาศัยการบริหารโครงการที่ดี โดยทั่วไปทีมงานพัฒนาระบบจะประกอบด้วยบุคลากรที่มีความรู้และประสบการณ์เกี่ยวกับระบบหลากหลายแตกต่างกัน อาทิ นักวิเคราะห์ระบบ โปรแกรมเมอร์ ผู้ใช้ ผู้สนับสนุน และผู้เชี่ยวชาญ จึงต้องอาศัยการบริหารจัดการที่ดีเพื่อช่วยให้บุคลากรเหล่านี้ทำงานประสานร่วมกันและแก้ไขปัญหาอุปสรรคต่าง ๆ ที่อาจเกิดขึ้นในช่วงของการทำงาน การบริหารโครงการพัฒนาระบบจะต้องมีการวางแผน การกำหนดขอบเขต วัตถุประสงค์ การจัดสรรและควบคุมการใช้ทรัพยากร การดำเนินตามแผน การตรวจสอบและประเมินผล ซึ่งบางองค์การจะกำหนดกลุ่มบุคคลจากหน่วยงานต่าง ๆ ในองค์การซึ่งอาจอยู่ในรูปคณะกรรมการ คณะทำงาน ฯลฯ เพื่อทำหน้าที่และมีความรับผิดชอบในการบริหารโครงการพัฒนาระบบ

การจัดการความรู้ (ศรีไพร และเจษฎาพร, 2549)

การจัดการความรู้เป็นวิธีที่เป็นระบบเพื่อให้สารสนเทศและความรู้เกิดและกระจายไปสู่ผู้ที่ต้องการในเวลาที่เหมาะสมเพื่อสร้างคุณค่า การจัดการความรู้เป็นศิลปะของการสร้างคุณค่าจากทรัพย์สินที่เป็นนามธรรม (Intangible Assets)

การจัดการความรู้เป็นการรวบรวมองค์ความรู้ที่มีอยู่ในส่วนราชการซึ่งกระจัดกระจายอยู่ในตัวบุคคลหรือเอกสาร มาพัฒนาให้เป็นระบบเพื่อให้ทุกคนในองค์การสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพ อันจะส่งผลให้องค์การมีความสามารถในเชิงแข่งขันสูงสุด (สำนักงานพัฒนาระบบราชการ (ก.พ.ร.),

โดยสรุป การจัดการความรู้ หมายถึง กระบวนการอย่างเป็นระบบในการสรรหา การเลือก การรวบรวมการจัดระบบ การสร้างและจัดเก็บความรู้ในลักษณะที่เป็นแหล่งความรู้ที่ทุกคนในองค์การสามารถเข้าถึงได้ง่ายและแบ่งปันความรู้กันได้อย่างเหมาะสม เพื่อที่จะพัฒนาตนเองและมี

ความสามารถที่นำความรู้ไปประยุกต์ใช้อันจะเกิดประโยชน์ต่อการปฏิบัติงานของตน ซึ่งจะส่งผลต่อการเพิ่มความสามารถในการแข่งขันขององค์การ

การจัดการความรู้ที่ดีช่วยให้องค์การได้รับประโยชน์ เช่น

1. ช่วยเก็บรักษาความรู้ให้ควบคู่กับองค์การตลอดไป
2. ช่วยลดระยะเวลาการพัฒนาผลิตภัณฑ์ การให้บริการ หรือการเรียนรู้งานใหม่
3. ปรับปรุงประสิทธิภาพ และช่วยเพิ่มผลผลิตให้กับทุกส่วนขององค์การ
4. เสริมสร้างนวัตกรรมใหม่ทั้งทางด้านผลิตภัณฑ์และการบริการ
5. ส่งเสริมให้มีการเรียนรู้ แสดงความคิดเห็น และแลกเปลี่ยนความรู้ ซึ่งจะส่งผลให้บุคลากรมีคุณภาพเพิ่มขึ้นและสามารถประยุกต์ใช้ความรู้ในการปฏิบัติงานอันก่อให้เกิดประโยชน์ต่อองค์การ
6. ช่วยให้องค์การมีความพร้อมในการปรับตัวให้เหมาะสมกับการเปลี่ยนแปลงของสิ่งแวดล้อมในการดำเนินธุรกิจเพื่อความอยู่รอดและได้เปรียบทางการแข่งขัน

ความรู้เป็นการผสมผสานของกรอบประสบการณ์ คุณค่า สารสนเทศและการหยั่งเห็น ซึ่งเป็นการผสมผสานที่ให้กรอบสำหรับการประเมินและการนำประสบการณ์และสารสนเทศใหม่มาผสมรวมกัน (Davenport & Prusak, 1995 อ้างถึงใน Tiwana, 2002 : 37)

ความรู้ (Knowledge) ตามความหมายพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542 คือ สิ่งทีสั่งสมมาจากการศึกษาเล่าเรียน การค้นคว้า หรือประสบการณ์ รวมทั้งความสามารถเชิงปฏิบัติและทักษะความเข้าใจ หรือสารสนเทศที่ได้รับมาจากประสบการณ์ สิ่งที่ได้รับมาจากการได้ยิน ได้ฟัง การคิดหรือการปฏิบัติ องค์วิชาในแต่ละสาขา

จากคำจำกัดความที่มีผู้กล่าวไว้ในเบื้องต้น สามารถสรุปได้ว่า ความรู้เป็นการผสมผสานของประสบการณ์ สารสนเทศ ความเข้าใจ ทักษะและความเชี่ยวชาญ รวมถึงสิ่งที่ได้รับการสั่งสมมาจากการศึกษาเล่าเรียน ค้นคว้าและถ่ายทอด ที่นำไปสู่การกำหนดกรอบความคิดสำหรับการประเมินความเข้าใจ และการนำสารสนเทศและประสบการณ์ใหม่มาผสมรวมกัน

ศาสตราจารย์โนนากะและทาเคอูชิ ได้แบ่งความรู้เป็น 2 ประเภทคือ

1. ความรู้โดยนัย (Tacit Knowledge) เป็นความรู้ที่ซ่อนอยู่ในตัวบุคคล ยากที่จะถ่ายทอดออกมาเป็นตัวอักษร เช่น ความรู้ที่ได้จากประสบการณ์ พรสวรรค์ ความรู้สึกนึกคิด ทักษะในการทำงาน งานฝีมือ หรือการคิดเชิงวิเคราะห์ ความรู้ประเภทนี้สามารถพัฒนาและแบ่งปันได้ และเป็นความรู้ที่สร้างความได้เปรียบในการแข่งขัน

2. ความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่เป็นเหตุและผล สามารถเขียนบรรยายหรือถ่ายทอดมาเป็นตัวอักษร ข้อความ กฎเกณฑ์ สูตร นิยาม หรือลักษณะตัวแบบทางคณิตศาสตร์ได้ เช่น หนังสือ เอกสาร และคู่มือต่าง ๆ

จริยธรรมในสังคมสารสนเทศ (ทิพวรรณ, 2545)

ยังระบุไว้ว่า จริยธรรม หมายถึง “หลักของความถูกและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ” โดยสรุปแล้ว จริยธรรมจะมีความหมายไปในแนวเดียวกันคือ เป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม ในทางปฏิบัติแล้ว การระบุว่าการกระทำสิ่งใดผิดจริยธรรมนั้นอาจกล่าวได้ไม่ชัดเจนมากนัก ทั้งนี้ย่อมขึ้นอยู่กับวัฒนธรรมของสังคมในแต่ละประเทศด้วย อาทิเช่น กรณีที่เจ้าของบริษัทใช้กล้องในการตรวจจับหรือเฝ้าดูการทำงานของพนักงาน เป็นต้น สำหรับตัวอย่างของการกระทำที่ยอมรับกันโดยทั่วไปว่าเป็นการกระทำที่ผิดจริยธรรม เช่น

1. การใช้คอมพิวเตอร์ทำร้ายผู้อื่นให้เกิดความเสียหายหรือก่อความรำคาญ เช่น การนำภาพหรือข้อมูลส่วนตัวของบุคคลไปลงบนอินเทอร์เน็ตโดยไม่ได้รับอนุญาต
2. การใช้คอมพิวเตอร์ในการขโมยข้อมูล
3. การเข้าถึงข้อมูลหรือคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาต
4. การละเมิดลิขสิทธิ์ซอฟต์แวร์

2.2 การรักษาความปลอดภัยของระบบสารสนเทศ (ศรีไพร และเจษฎาพร, 2549)

2.2.1 การพิสูจน์ตัวตน (Authentication) ของผู้เข้าใช้ระบบสารสนเทศ

โดยทั่วไปวิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์จากบุคคลที่ไม่ได้รับอนุญาตจะแตกต่างกันออกไป ในที่นี้จะแนะนำ 4 วิธีคือ (Shelly, 2006)

1. การใช้ Username หรือ User ID และรหัสผ่าน (Password) บางระบบจะกำหนดชื่อผู้ใช้และรหัสผ่านมาให้เพื่อความสะดวก ในขณะที่บางระบบจะให้ผู้ใช้กำหนดเอง หากระบบใดมีการกำหนดรหัสผ่านมาให้ ผู้ใช้ควรเปลี่ยนแปลงด้วยตนเองในภายหลัง และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นวันเกิด หรือรหัสอื่น ๆ ที่แฮกเกอร์สามารถเดาได้

2. การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ ได้แก่ บัตร หรือกุญแจ ตัวอย่างเช่น การใช้บัตร ATM เพื่อทำธุรกรรมเกี่ยวกับบัญชีธนาคาร ซึ่งโดยปกติจะใช้บัตรควบคู่กับ PIN (Personal Identification Number) ประกอบด้วยตัวเลข 4 หลัก และ PIN ก็เป็นรหัสผ่านที่เจ้าของควรให้ความสำคัญ เช่น ไม่ควรใช้ปีเกิดหรือจดลงในบัตร

3. การใช้อุปกรณ์ทางชีวภาพ (Biometric Devices) เป็นการใช้อุปกรณ์ที่ตรวจสอบลักษณะส่วนบุคคลเพื่อการอนุญาตใช้โปรแกรม ระบบ หรือการเข้าใช้ห้องคอมพิวเตอร์ เช่น การตรวจสอบเสียง ลายนิ้วมือ ฝ่ามือ ลายเซ็น ม่านตา และรูปหน้า เป็นต้น โดยอุปกรณ์จะทำการแปลงลักษณะส่วนบุคคลให้อยู่ในรูปดิจิทัลแล้วเปรียบเทียบกับข้อมูลที่จัดเก็บในคอมพิวเตอร์ ถ้าข้อมูลไม่ตรงกันคอมพิวเตอร์ก็จะปฏิเสธการเข้าสู่ระบบ

4. ระบบเรียกกลับ (Callback System) เป็นระบบที่ผู้ใช้ระบุชื่อและรหัสผ่านเพื่อขอเข้าใช้ระบบปลายทาง หากข้อมูลถูกต้อง คอมพิวเตอร์ก็จะเรียกกลับให้เข้าใช้งานเอง ระบบในลักษณะนี้เป็นการเพิ่มความปลอดภัยให้คอมพิวเตอร์อีกระดับหนึ่ง คือคอมพิวเตอร์จะตรวจสอบหมายเลขโทรศัพท์ของผู้ใช้เมื่อเรียกกลับ อย่างไรก็ตามการใช้งานลักษณะนี้จะมีประสิทธิภาพมากขึ้นถ้าผู้ขอใช้ระบบใช้เครื่องคอมพิวเตอร์จากตำแหน่งเดิม คือ จากบ้าน หรือที่ทำงาน (หมายเลขโทรศัพท์เดิม) ในขณะที่การใช้คอมพิวเตอร์แบบพกพา อาจต้องเปลี่ยนหมายเลขโทรศัพท์ ทำให้เกิดความเสี่ยงมากกว่า

ความปลอดภัยของเครือข่ายคอมพิวเตอร์ส่วนบุคคลและเว็บไซต์ (อภิชัย, 2548)

ปัญหาต่าง ๆ ของการล่วงละเมิดนั้นมักมาจากความประมาทของผู้ใช้งานคอมพิวเตอร์ทั้งสิ้น ตลอดจนความรู้ไม่เท่าทันกับการพัฒนาของภัยต่าง ๆ ที่เข้ามาแวะเวียนคุกคาม ดังนั้นเราจำเป็นที่จะต้องรู้จักวิธีที่เราจะสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์ของตัวเอง ซึ่งจะทำให้ระบบคอมพิวเตอร์ขององค์กรมีความปลอดภัยมากขึ้นไปด้วย

ความปลอดภัยของคอมพิวเตอร์นั้น เป็นเพียงกระบวนการที่ใช้ยืนยันความถูกต้องของผู้ใช้งานว่าได้รับอนุญาตหรือไม่ ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ที่ต่อเข้าระบบเครือข่าย หรือจะเป็นผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์ ต่างต้องแสดงความเป็นเจ้าของหรือตัวตนของตนเอง เพื่อที่จะทำให้เกิดความปลอดภัย ยกตัวอย่างเช่น ผู้ใช้เครื่องคอมพิวเตอร์เข้าใช้เครื่องจำเป็นที่จะต้องทำการ Login เข้าระบบโดยกรอกชื่อ (User Name) และรหัสผ่าน (Password) เพื่อเป็นการยืนยันว่าเป็นผู้ที่ได้รับอนุญาตในการเข้าใช้ระบบ ถ้าใช่ก็สามารถเข้าระบบได้ แต่ไม่ก็ไม่สามารถเข้าใช้ระบบได้นี้ระบบรักษาความปลอดภัยขั้นพื้นฐานที่จำเป็นต้องมี ซึ่งเป็นการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าใช้เครื่องคอมพิวเตอร์ของเรา ส่วนระบบเครือข่ายก็เช่นเดียวกัน

2.2.2 การเข้าใช้งานหรือการโจมตีของผู้บุกรุก

การตรวจสอบหรือพิสูจน์ตัวตน (Authentication) ของผู้เข้าใช้ด้วยการตรวจสอบบัตรประชาชน

การตรวจสอบรหัสบัตรประชาชน (first, 2552) เวลาจะตรวจสอบว่าข้อมูลตัวเลขในบัตรประชาชนที่กรอกลงในส่วนต่าง ๆ ของเว็บไซต์ถูกต้องหรือไม่ มีวิธีการคือการคำนวณ Check Digit จากเลขหลักอื่น ๆ เพื่อเปรียบเทียบกับ Check Digit ที่กรอกมาว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าข้อมูลถูกต้องไม่ผิด แต่ถ้าไม่ตรงกันก็แปลว่าข้อมูลที่กรอกมามีข้อมูลอาจจะ 1 หลัก หรือ 2 หลักที่ผิดระบบ ก็สามารถเตือนให้ผู้ใช้ทราบและกรอกใหม่อีกครั้งได้

ความหมายของ Check Digit

Check Digit เป็นตัวเลข 1 หลัก ที่เกิดจากการนำเลขหลักอื่น ๆ มา บวก ลบ คูณ หาร กัน และ Check Digit จะช่วยให้ตรวจสอบในเบื้องต้นได้ว่า ข้อมูลที่กรอกมาถูกต้องรึเปล่า

รหัสประจำตัวจะอยู่ในรูป x-xxxx-xxxxx-xx-x (เลข 13 หลัก) แต่รหัสประจำตัวจริง ๆ แล้วมีแค่ 12 หลักเท่านั้น (12 หลักแรก) แต่เลขตัวสุดท้าย เป็น Check Digit

ตัวอย่างรหัสประชาชน

1-2015-41462-23-4 **Check Digit** ของรหัสประชาชนนี้คือเลข 4 (เลขตัวสุดท้าย)

ขั้นตอนที่ 1 นำเลข 12 หลักมา เขียนแยกหลักกันก่อน (หลักที่ 13 ไม่ต้องนำมา)
จะได้ 120154146223

ขั้นตอนที่ 2 นำเลข 12 หลักนั้นมา คูณเข้ากับเลขประจำหลัก
รหัสบัตร 1 2 0 1 5 4 1 4 6 2 2 3 ตัวคูณ 13 12 11 10 9 8 7 6 5 4 3 2
จะได้ (1*13)+(2*12)+(0*11)+(1*10)+(5*9)+(4*8)+(1*7)+(4*6)+(6*5)+(2*4)+(2*3)+(3*2)
ผลคูณ 13+24+0+10+45+32+7+24+30+8+6+6

ขั้นตอนที่ 3 นำผลคูณทั้ง 12 ตัวมาบวกกันทั้งหมด จะได้
13+24+0+10+45+32+7+24+30+8+6+6=205

ขั้นตอนที่ 4 นำเลขที่ได้จากขั้นตอนที่ 3 มา mod 11 (หารเอาเศษ) จะได้ 205 mod 11 = 7

ขั้นตอนที่ 5 นำ 11 ตั้ง ลบออกด้วย เลขที่ได้จากขั้นตอนที่ 4 จะได้ 11-7 = 4
(จะได้ 4 เป็นเลขในหลัก Check Digit)

ถ้าลบแล้วได้ออกมาเป็นเลข 2 หลัก ให้ใช้เลขในหลักหน่วยมาเป็น Check Digit (เช่น 11 ให้ใช้ 1 มาเป็นตัวเช็ค, 10 ให้ใช้ 0 มาเป็นตัวเช็ค เป็นต้น)

ก่อนที่จะกล่าวถึง เรื่องราวการบุกรุกเครื่องส่วนบุคคลนั้น ขอกล่าวถึงผู้บุกรุกเสียก่อน จากหัวข้อขอใช้คำว่า “แฮกเกอร์ (Hacker)” แต่ยังมีอีกหนึ่งคำที่คิดว่าน่าจะเหมาะสมกว่า แต่หลาย ๆ ท่านอาจจะไม่คุ้นนั้นคือ “แคร็กเกอร์ (Cracker)”

แฮกเกอร์ (Hacker) นั้นหมายถึง บุคคลที่มีความชำนาญ หลงไหล ฝักใฝ่ในการเรียนรู้เกี่ยวกับคอมพิวเตอร์ นับได้ว่าแฮกเกอร์เป็นผู้ที่มีความรู้ความสามารถสูงมาก โดยการทำงานของแฮกเกอร์นั้นจะทำงานด้วยความจริงใจ ต้องการที่จะค้นหา ปกป้อง แก้ไขข้อผิดพลาดของระบบ โดยไม่คิดที่จะขโมย หรือทำลายข้อมูล

แคร็กเกอร์ (Cracker) นั้นหมายถึง บุคคลที่มีความชำนาญทางคอมพิวเตอร์ แต่จุดประสงค์ของการทำงานนั้น เพื่อขโมย ทำลายระบบหรือข้อมูล คนกลุ่มนี้อาจเป็นแฮกเกอร์ที่ฝักใฝ่ทางฝ่ายอธรรม ทำเพื่อเงินมากกว่าความสนใจที่จะต้องการแก้ไขปัญหาของระบบ นับได้ว่าผู้ที่ก่อกวนในระบบเครือข่ายนั้นมักจะเป็นแคร็กเกอร์ (Cracker) แต่ส่วนใหญ่ก็มักจะใช้คำว่าแฮกเกอร์ไป ในที่นี้จึงขอใช้คำว่า “แฮกเกอร์ (Hacker) เป็นคำเรียกการกระทำที่ไม่ดีหรือก่อให้เกิดความเสียหาย แม้มันจะเป็นการกระทำของแคร็กเกอร์ก็ตาม

ภัยร้ายบนอินเทอร์เน็ต ภัยคุกคามต่าง ๆ มีดังต่อไปนี้

1. Malware เป็นกลุ่มหลักในการก่อกวน ซึ่งประกอบไปด้วยสมาชิกดังต่อไปนี้คือ ไวรัส หนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (trojan Horse)

2. Adware และ Spyware เป็นโปรแกรมสายลับมาขโมยข้อมูล ตลอดจนการส่งโฆษณามายังเครื่องคอมพิวเตอร์ ก่อให้เกิดความรำคาญอย่างยิ่ง

3. Spam Mail หรืออีเมลขยะ อันนี้ก่อให้เกิดความรำคาญ

4. Phishing การหลอกลวงให้หลงเชื่อ

5. PC Zombie แฮกเกอร์จะทำให้เครื่องคอมพิวเตอร์เรา ทำให้เครื่องคนอื่นใช้งานไม่ได้

6. การขโมยข้อมูล ทั้งที่เป็นข้อมูลส่วนตัวและเป็นข้อมูลทางธุรกิจ

ภัยทางอินเทอร์เน็ตสำหรับผู้ใช้งานทั่วไป

1. Hard Drive Crashing เป็นปัญหาที่ทำให้ระบบเกิดการทำงานผิดปกติ ไม่ว่าจะเป็นไฟล์งาน ซอฟต์แวร์ ไปจนถึงระบบปฏิบัติการ ต่างทำงานรวมกันหมด เหตุก็ไม่ใช่ใครก็เป็นพวก Malware อันได้แก่ ไวรัส (Virus), หนอนอินเทอร์เน็ต (Worm), โทรจัน (Trojan Horse) เป็นต้น

2. Identity Theft เป็นการเข้ามาขโมยข้อมูลส่วนตัวนำไปใช้งานในทางที่ไม่ดี ไม่ว่าจะเป็นการสมัครบัตรเครดิต ซึ่งเจ้าตัวไม่ทราบ จะมาทราบอีกทีก็มีสลิปเก็บเงินมาที่บ้านแล้ว

3. Credit Theft เป็นการขโมยหมายเลขบัตรเครดิตในเครื่องคอมพิวเตอร์ แล้วนำไปใช้โดยมักจะส่งไปยังที่อยู่ชั่วคราว เพื่อปกปิดตัวเอง

4. Tunneling สำหรับคนที่มักจะรีโมตเครื่องของตัวเองจากที่บ้านเข้าไปยังระบบของบริษัท อาจถูกวางยามีมือดีแอบส่งโทรจันเข้ามาไว้ และก็แฝงตัวเข้าระบบบริษัทของผู้ใช้งานโดยไม่รู้ตัว ซึ่งอาจสร้างความเสียหายอย่างมากมายได้

5. Extortion เป็นการเจาะระบบเพื่อทำให้เกิดความไม่สบายใจ เช่น นำหมายเลขบัตรเครดิตไปโพสต์ไว้ที่เว็บบอร์ด เป็นต้น ความเสียหายอาจเกิดตามมาถ้ามีใครนำหมายเลขบัตรเครดิตของคุณไปใช้ต่อ

6. Zombies หลาย ๆ คนคิดว่าตนเองไม่ได้มีข้อมูลอะไรสำคัญ บัตรเครดิตก็ไม่มีจะกลัวอะไร แต่ที่มีก็คือ ทรัพยากรที่เป็นเครื่องคอมพิวเตอร์ของเรา แฮกเกอร์อาจเจาะเข้ามาแล้วฝากโปรแกรมที่เข้าเอาไว้ควบคุมเครื่องคอมพิวเตอร์ของเรา เพื่อให้ไปทำลายเครื่องคอมพิวเตอร์เครื่องอื่น ๆ จึงเรียกคอมพิวเตอร์ที่ถูกควบคุมนี้ว่า Zombies หรือผีดิบ

7. Compromise of Private Information เป็นการนำข้อมูลส่วนตัวของเราไปแจกจ่ายให้คนอื่น ๆ

บัญญัติ 10 ประการ สำหรับความปลอดภัยของผู้ใช้ตามบ้าน (Computer Home Use)

1. ทำการติดตั้งโปรแกรมป้องกันไวรัสและทำการอัปเดตอย่างสม่ำเสมอ

2. อย่าเปิดอีเมลที่ได้รับจากคนที่ไม่รู้จัก

3. มีการใช้รหัสผ่านที่เดาได้ยาก การตั้งรหัสผ่านนั้นถือว่าเป็นศาสตร์อย่างหนึ่ง เพราะถ้าตั้งยากมากก็ลืมอีก ถ้าตั้งง่าย ๆ ก็ทำให้ไม่ปลอดภัย การตั้งรหัสผ่านนั้นอย่างน้อยควรใช้ตัวอักษร 8 ตัว โดยใช้ทั้งตัวพิมพ์ใหญ่ และพิมพ์เล็ก ตัวเลข ไปจนถึงสัญลักษณ์ต่าง ๆ (&$!) ผสมกัน โดยการสร้างรหัสผ่านนั้นจะว่างอยู่บนหลักการดังนี้

- ยากต่อการเดา ไม่ใช้รหัสผ่านที่มีอยู่ในดิกชันนารี เพราะโปรแกรมแกะรหัสผ่านสามารถเดาได้ หรือการตั้งชื่อลูก ภรรยา สุนัข เจ้านายเป็นรหัสผ่านก็ทำให้ผู้ไม่หวังดีเดาได้เช่นกัน

- อย่าใช้รหัสผ่านเหมือนเดิมในทุก ๆ ระบบ เช่น การใช้งานคอมพิวเตอร์และระบบอื่น ๆ เหมือนกันหมด จำง่ายแค่จำรหัสเดียว ใช้หมดทุกอย่าง เป็น Master Password อันนี้ถ้าเขารู้ว่ารหัสผ่านเป็นอะไรก็สามารถเข้าระบบทุก ๆ อย่างได้หมด

- การที่ให้เราจำได้ง่าย ไม่ต้องไปจดไว้ที่ใด ๆ เพราะส่วนใหญ่ทำให้เดายาก และจำยากเลยต้องเขียนไว้และแปะไว้ที่หน้าจอคอมพิวเตอร์นั่นแหล่ะ เพราะมันจำยากจริง ๆ เลยทำให้คนที่ต้องการรหัสไม่ต้องไปเดายาก ลอกจากกระดาษมาเลย

- ควรเปลี่ยนรหัสผ่านอย่างน้อยเดือนละหนึ่งครั้ง แต่จริง ๆ ถ้าใช้งานกับคนหมู่มากควรเปลี่ยนทุก ๆ สองสัปดาห์ก็จะเป็นการดี

4. ใช้ไฟล์วอลล์เพื่อป้องกันการบุกรุกของแฮกเกอร์ ไฟล์วอลล์เป็นระบบตรวจสอบการเข้าออกของข้อมูลในเครื่องคอมพิวเตอร์ของบเรา ทำหน้าที่คล้ายกับเจ้าหน้าที่ รปภ. ที่คอยตรวจสอบคนที่เข้าออกในองค์การหรือสนามบิน เพื่อป้องกันไม่ให้มีผู้ร้ายที่พกอาวุธเข้ามาในสถานที่นั้น ๆ หรือพูดง่าย ๆ ว่ายอมให้เฉพาะคนที่ทางสถานที่นั้น ๆ อนุญาตให้เข้าได้เท่านั้น เช่นเดียวกันไฟล์วอลล์ก็จะตรวจสอบข้อมูลที่วิ่งเข้าออกเครื่องคอมพิวเตอร์ของเรา และจะอนุญาตเฉพาะข้อมูลที่เราต้องการให้เข้าออกเครื่องคอมพิวเตอร์ของเราเท่านั้น หรือเราสามารถที่จะควบคุมข้อมูลต่าง ๆ ที่วิ่งเข้าออกเครื่องคอมพิวเตอร์ของเราได้นั่นเอง

5. ป้องกันไม่ให้คนที่ไม่รู้จักเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเรา การที่เราอนุญาตให้ใครก็ไม่รู้มาใช้งานเครื่องคอมพิวเตอร์ของเรา นับว่าเป็นการเพิ่มความเสี่ยงให้กับเครื่องคอมพิวเตอร์ของเราเป็นอย่างมาก เพราะเราไม่สามารถรู้เลยว่าเขาได้ทำการสำเนาไฟล์งานของคุณไปด้วยหรือไม่ หรือนำโปรแกรมโทรจันมาใส่ไว้ให้คุณหรือไม่ หรือนำไวรัสมาติดเครื่องของคุณ

การป้องกันที่ดีควรที่จะให้เฉพาะบุคคลที่เรารู้จักเป็นอย่างดีเท่านั้นมาใช้งาน

2.2.3 การพิสูจน์สิทธิของผู้เข้าใช้เว็บไซต์

ความปลอดภัยของเว็บ (ธวัชชัย, 2553) ในเว็บไซต์ระบบสมาชิกนั้น หลังจากที่ผู้ใช้ล็อกอินเข้าสู่ระบบได้สำเร็จ เว็บไซต์จะสร้าง Session ID ขึ้นมาเพื่อใช้เป็นตัวอ้างอิงถึงผู้ใช้คนนั้น Session ID จะเป็นค่า String ยาว ๆ ที่มักจะถูกสร้างขึ้นโดยใช้เทคนิคการสุ่มตัวอักษรผสมกับตัวเลข และทุกครั้งที่ผู้ใช้มีการส่ง HTTP Request ไปยังเว็บเซิร์ฟเวอร์เพื่อขอหน้าเว็บเพจ (เช่น การคลิกลิงค์ Inbox ของ Gmail เพื่อเช็คอีเมล์) ใน HTTP Request จะมี Cookie และข้อมูลใน Cookie จะมี Session ID อยู่ภายใน เมื่อเว็บไซต์ปลายทางได้รับ HTTP Request ก็จะทราบว่าผู้ใช้คนใดเป็นร้องขอ โดยเว็บไซต์จะตรวจสอบจาก Session ID ที่อยู่ภายใน Cookie จากนั้นก็จะประมวลผลและตอบกลับด้วย HTTP Response ซึ่งมีข้อมูลที่ผู้ใช้คนนั้นต้องการ (เช่น Gmail ตอบกลับด้วยข้อมูลใน Mail Box ของผู้ใช้คนนั้น)

การโจมตีเว็บไซต์โดยวิธี Session Hijacking คือการปล้นเอา Session ID ของเหยื่อ โดย Session ID นั้น มักจะถูกบรรจุไว้ภายใน Cookie ดังนั้นหากผู้โจมตีดักจับหรือขโมยเอา Cookie ของเหยื่อมาได้ ผู้โจมตีก็สามารถนำเอา Session ID ที่อยู่ภายใน Cookie ไปใช้เพื่อเข้าสู่เว็บไซต์ด้วยสิทธิ์ของเจ้าของ Cookie นั้นได้ การขโมยเอา Cookie เพื่อมาทำ Session Hijacking จำเป็นต้องมีการขโมยค่า Cookie ซึ่งสามารถทำได้ด้วยเทคนิคต่าง ๆ มากมาย ผู้โจมตีที่อยู่เน็ตเวิร์กเดียวกันกับเหยื่อมักจะขโมย Cookie โดยการดักจับข้อมูลในระบบ LAN แต่ถ้าหากผู้โจมตีอยู่ต่างเน็ตเวิร์กกับเหยื่อ เช่น อยู่คนละซีกโลก ก็ยังสามารถขโมย Cookie ได้โดยใช้เทคนิคอื่นเพิ่มเติม เช่น XSS : Cross Site Seripting หรืออาจจะใช้ Spyware เป็นต้น

การส่ง Session ID จากบราวเซอร์ไปยังเว็บไซต์ นอกจากส่งโดยใช้ Cookie แล้ว ยังสามารถส่งทางอื่นได้อีก เช่น ส่งทางฟิลด์ที่ซ่อน (Hidden Field) หรือส่ง Session ID ทาง URL ก็มี การส่ง Session ID ทาง Hidden Field นั้น ผู้โจมตีสามารถเปลี่ยนค่าในฟิลด์ซ่อนได้โดยตรง ส่วนการส่ง Session ID ทาง URL ผู้โจมตีก็สามารถแก้ไขค่าบน Address Bar ได้โดยตรง เนื่องจากสามารถถูกโจมตีได้ง่ายทั้งสองวิธีที่กล่าวมา จึงไม่ค่อยเป็นที่นิยม ในทางตรงกันข้ามจะเห็นได้ว่าเว็บไซต์ฟรีอีเมล์ยอดนิยมอย่าง Hotmail, Gmail และ Yahoo Mail ก็ใช้การส่ง Session ID ทาง Cookie

การป้องกัน Session Hijacking

จากที่แฮกเกอร์ใช้จะพบว่าในการดักจับ Session ID ในระบบ LAN นั้น แฮกเกอร์จำเป็นที่จะต้องมีการทำ ARP Spoof เพื่อให้ข้อมูลของเหยื่อวิ่งผ่านเครื่องของแฮกเกอร์ และใช้โปรแกรมประเภท Sniffer ดักจับข้อมูล ดังนั้นการป้องกันจึงสามารถทำได้โดยวิธีการต่าง ๆ ดังต่อไปนี้

- การป้องกัน ARP Spoof
- ป้องกันการดักจับข้อมูล
- ป้องกันการนำ Cookie/Session ID ที่ดักจับได้ไปใช้งาน

หน้าจอเว็บล็อกอินที่ให้ผู้ใช้ป้อนทางบราวเซอร์เพื่อเข้าสู่ระบบ เป็นช่องทางหนึ่งที่ทำให้แฮกเกอร์สามารถที่จะข้ามผ่านการตรวจสอบสิทธิ์แล้วเข้าสู่ระบบด้วยสิทธิ์ของผู้ดูแลระบบได้ หรือในบางครั้งแฮกเกอร์อาจจะเข้ายึดครองและควบคุมเครื่องเซิร์ฟเวอร์นั้นได้ ตัวอย่างหน้าจอล็อกอินดังกล่าว เช่น ล็อกอินเพื่อเช็คอีเมล์, ล็อกอินเพื่อเข้าสู่เว็บบอร์ด (ที่ต้องลงทะเบียนเป็นสมาชิกเท่านั้นจึงใช้งานได้) หรือหน้าจอล็อกอินอื่น ๆ ที่มีการตรวจสอบสิทธิ์ของผู้ใช้จากฐานข้อมูลเชิงสัมพันธ์ (Relational Database)

ในระบบสมาชิกต่าง ๆ นั้น ผู้ดูแลระบบมักจะเก็บข้อมูลของสมาชิกไว้ในฐานข้อมูล เช่น Oracle, SQL, Server, MySQL และ MS Access เป็นต้น และเมื่อสมาชิกที่ประสงค์จะเข้าสู่ระบบก็ต้องพบกับหน้าจอตรวจสอบสิทธิ์ ซึ่งสมาชิกจำเป็นต้องป้อนชื่อผู้ใช้และรหัสผ่านให้ถูกต้อง

ฟอร์มล็อกอินนี้จะรับค่า username และ password และมีปุ่มให้กดเพื่อล็อกอิน หลังจากที่ผู้ใช้กดปุ่มล็อกอินดังกล่าวแล้ว ฟอร์มนี้จะส่งข้อมูล username และ password ไปให้ระบบตรวจสอบสิทธิ์โดยการส่งไปยังโปรแกรมในฝั่งเซิร์ฟเวอร์ ซึ่งอาจจะเป็น ASP, CGI/Perl หรือ PHP เป็นต้น ซึ่งโดยส่วนมากแล้วเว็บโปรแกรมเมอร์มักจะเขียนโปรแกรมง่าย ๆ เพื่อที่จะนำ username และ password เข้ามาเป็นส่วนหนึ่งของคำสั่ง SQL แล้วส่งไปให้ Database Server สืบค้นข้อมูล

โปรแกรมเมอร์จะเขียนคำสั่ง SQL login บางส่วนไว้ในโค้ดโปรแกรม และเมื่อนำค่าตัวแปร username และ password ที่ผู้ใช้ป้อนผ่านฟอร์ม นำมาประกอบเข้าด้วยกัน (นำมาเรียงต่อกัน) ก็จะเป็นคำสั่ง SQL login ที่สมบูรณ์ ซึ่งความหมายของคำสั่ง SQL login ดังกล่าวคือ ให้สืบค้นข้อมูลของผู้ใช้จากตารางชื่อ tbl_Users ที่ค่าในฟิลด์ Username ตรงกันกับค่าในตัวแปร strUsername และค่าในฟิลด์ Password ตรงกันกับค่าในตัวแปร strPassword หลังจากที่พบข้อมูลแล้ว ตัวแปร strAuthCheck จะรับค่าข้อมูลของผู้ใช้คนนั้น แต่ถ้าค้นหาไม่พบ (ซึ่งอาจจะเกิดจากไม่มีผู้ใช้ตามที่ระบุ หรือป้อนค่ารหัสผ่านผิด) ค่าในตัวแปร strAuthCheck จะได้รับค่าว่างเปล่า ซึ่งจะทำให้โปรแกรมทราบว่าการตรวจสอบสิทธิ์ผ่านหรือไม่ จะเกิดอะไรขึ้นถ้าตัวแปรสำหรับ username และ password ที่ถูกส่งเข้ามานั้นไม่ใช่ชื่อผู้ใช้และรหัสผ่าน แต่กลับกลายเป็นส่วนหนึ่งของคำสั่ง SQL ที่สามารถทำให้ความหมายของคำสั่งเปลี่ยนไป

ยังมีวิธีป้องกันคือ การป้องกันการข้ามผ่านการตรวจสอบสิทธิ์ด้วย SQL Injection โดยใช้การป้อนอักขระพิเศษผ่านทางฟอร์มอินพุต การจำกัดความยาวของฟอร์มอินพุต การย้าย script ป้องกันฝั่ง clent ไปยังฝั่ง server การป้องกัน remote file inclusion การป้องกันการโจมตีด้วย XSS และการป้องกัน login cracking

เนื่องจากงานวิจัยถือเป็นทรัพย์สินทางปัญญา กลุ่มงานวิจัยเมื่อนำมาอยู่บนเว็บไซต์ นักวิจัยซึ่งเป็นผู้ที่นำงานวิจัยออกสู่สาธารณชนจะได้ตระหนักถึงเรื่องความถูกต้องของข้อมูล ดังนี้

ความถูกต้องของข้อมูล (Accuracy)

ในการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูลนั้น คุณลักษณะที่สำคัญประการหนึ่งคือ ความน่าเชื่อถือได้ของข้อมูล ทั้งนี้ข้อมูลจะมีความน่าเชื่อถือมากน้อยเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูลด้วย ประเด็นด้านจริยธรรมที่เกี่ยวข้องกับความถูกต้องของข้อมูล โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่ เช่น ในกรณีที่องค์การให้ลูกค้าลงทะเบียนด้วยตนเอง หรือกรณีของข้อมูลที่เผยแพร่ผ่านทางเว็บไซต์ อีกประเด็นหนึ่งคือ จะทราบได้อย่างไรว่าข้อผิดพลาดที่เกิดขึ้นนั้นไม่ได้เกิดจากความจงใจและผู้ใดจะเป็นผู้รับผิดชอบหากเกิดข้อผิดพลาด ดังนั้นในการจัดทำข้อมูลและสารสนเทศให้มีความถูกต้อง น่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ นอกจากนี้ควรให้สิทธิแก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลของตนเองได้

การตรวจสอบหรือเช็คคำหยาบโดยใช้ฐานข้อมูล (ศรีนนท์, 2552)

ในการตรวจสอบคำหยาบมีตัวอย่างโปรแกรมที่ต้องทำมีดังนี้

```
//การ import ฐานข้อมูล
CREATE TABLE `tb_word` (`id` int(11) NOT NULL auto_increment,`word` varchar(200)
NOT NULL,PRIMARY KEY (`id`)) ENGINE=MyISAM DEFAULT CHARSET=tis620
AUTO_INCREMENT=16 ;

//กำหนดการเพิ่มคำหยาบลงในฐานข้อมูล
INSERT INTO `tb_ban` VALUES ('คำหยาบ');
INSERT INTO `tb_ban` VALUES ('คำหยาบ');
INSERT INTO `tb_ban` VALUES ('คำหยาบ');
INSERT INTO `tb_ban` VALUES ('คำหยาบ');
INSERT INTO `tb_ban` VALUES ('คำหยาบ');
INSERT INTO `tb_ban` VALUES ('คำหยาบ');

//ตัวอย่างการเรียกใช้งาน หน้า รับ ข้อมูล
$detail=$_POST[detail];
$name_ans=$_POST[name_ans];
```

```
//ประกาศตัวแปรสำหรับตรวจสอบคำไม่สุภาพ
$unaccept_detail_ans = "N";
$unaccept_name_ans =  "N";

//วนลูปเพื่อตรวจสอบคำไม่สุภาพ
$sql="select word from tb_word"; // เรียกใช้งานตาราง word
$result=mysql_db_query($dbname,$sql);
while($row=mysql_fetch_array($result))
{ $word=$row[word];
if(strstr($detail,$row["word"]))
{ $unaccept_detail_ans = "Y"; }
if(strstr($name,$row["word"]))
{ $unaccept_name_ans = "Y"; } }

//แสดงข้อความเตือนเมื่อตรวจพบคำไม่สุภาพ
if($unaccept_detail_ans == "Y")
{ echo "<script language='javascript'>" ;
echo "alert('มีคำหยาบอยู่ในช่อง รายละเอียดกระทู้ กรุณากลับไปกรอกข้อมูลให้ถูกต้องด้วยคำที่
สุภาพ ')" ;
echo "</script>" ;
echo "<script language='javascript'>javascript:history.back()</script>";
exit(); }
else if($unaccept_name_ans == "Y")
{ "<script language='javascript'>" ;
echo "alert('มีคำหยาบอยู่ในช่อง ชื่อผู้ตั้งกระทู้ กรุณากลับไปกรอกข้อมูลให้ถูกต้องด้วยคำที่
สุภาพ')" ;
echo "</script>" ;
echo "<script language='javascript'>javascript:history.back()</script>";
exit(); }
```

ในตัวอย่างข้างต้น นั้นมีการตรวจสอบอยู่ 2 ตัว คือ $detail หรือรายละเอียดของผู้ตั้งกระทู้ และอีก 1 ตัว คือ $name ชื่อผู้ตั้ง กระทู้ เมื่อผู้ที่ตั้งกระทู้ ส่งค่ามาจาก from ระบบก็จะตรวจสอบว่ามีคำที่ตรงกับคำที่อยู่ในฐานข้อมูลใหม่ ถ้ามีระบบก็จะหยุดการทำงานแล้วใช้ Javascript เช็คให้

ย้อนกลับไปกรอกข้อมูลด้วยคำที่สุภาพใหม่ จะพบว่า ระบบจะตรวจเจอคำที่มีอยู่ในฐานข้อมูล ผู้ที่โพสจะไม่สามารถโพสคำถามหรือคำตอบนั้นได้

การเข้าถึงข้อมูล (Data Accessibility)

ปัจจุบันการเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์หรือเว็บไซต์ มักจะมีการกำหนดสิทธิตามระดับของผู้ใช้งาน ทั้งนี้เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิในการใช้งานระบบ เช่น การบันทึก การแก้ไข/ปรับปรุง และการลบ เป็นต้น ดังนั้นในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงของผู้ใช้ และการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้นก็ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนตัว

ในการใช้งานคอมพิวเตอร์และเครือข่ายร่วมกันให้เป็นระเบียบ หากผู้ใช้ร่วมใจกันปฏิบัติตามระเบียบและข้อบังคับของแต่ละหน่วยงานอย่างเคร่งครัดแล้ว การผิดจริยธรรมก็คงจะไม่เกิดขึ้น

ข้อควรระวังก่อนเข้าไปในโลกไซเบอร์

Haag ได้เสนอกฎไว้ 2 ข้อ (ธวัชชัย, 2553) คือ ถ้าคอมพิวเตอร์มีโอกาสถูกขโมย ให้ป้องกันโดยการล็อคมัน และถ้าไฟล์มีโอกาสที่จะถูกทำลายให้ป้องกันด้วยการสำรอง (Backup) เช่น ในการใช้คอมพิวเตอร์พกพาหรือโน้ตบุ๊ก ให้ใช้สายเคเบิลและกุญแจล็อค เพื่อให้ยากแก่การขโมย ส่วนในเรื่องของไฟล์ให้ทำสำเนาลงในสื่อต่าง ๆ ซึ่งการสำเนาไฟล์มีความจำเป็นอย่างมาก ในบางครั้งข้อมูลหรือไฟล์มีค่ามากกว่าฮาร์ดแวร์เสียอีก

ข้อควรระวังในการเข้าไปยังโลกไซเบอร์

ถ้าท่านซื้อสินค้าและบริการผ่านอินเทอร์เน็ต ให้พิจารณาข้อพึงระวังต่อไปนี้

1) บัตรเครดิตและการแอบอ้าง

- ให้หมายเลยบัตรเครดิตเฉพาะบริษัทที่ท่านไว้วางใจได้เท่านั้น
- ใช้เฉพาะเว็บไซต์ที่มีระบบรักษาความปลอดภัย เช่น https://
- ใช้รหัสผ่านอย่างน้อย 10 ตัวอักขระ (ควรผสมกันระหว่างตัวอักษรและตัวเลข)
- ใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบหรือเว็บไซต์

2) การป้องกันข้อมูลส่วนบุคคล

- พิจารณาอย่างรอบคอบก่อนการให้ข้อมูลส่วนตัว และให้ข้อมูลในส่วนที่จำเป็นเฉพาะบุคคลนั้น ๆ เท่านั้น

3) การป้องกันการติดตามการท่องเว็บไซต์

- ใช้โปรแกรม เช่น SurfSecret เพื่อป้องกันการติดตามการท่องเว็บไซต์ โปรแกรมจะทำงานคล้ายกับโปรแกรมป้องกันไวรัส และลบข่าวสาร/โฆษณาที่เกิดขึ้นเมื่อผู้ใช้ทางเว็บไซต์

4) การหลีกเลี่ยงสแปมเมล

- สแปมเมลอาจก่อความรำคาญแก่ผู้ใช้อินเตอร์เน็ตได้อย่างมาก เนื่องจากมันจะทวีจำนวนขึ้นเรื่อย ๆ ถ้าผู้ใช้ให้ที่อยู่อีเมลแก่บริษัทที่ทำธุรกิจออนไลน์ ดังนั้นจึงต้องระมัดระวังการลงทะเบียนเพื่อรับข่าวสารกลับมายังอีเมลของท่าน

5) การป้องกันระบบคอมพิวเตอร์และเครือข่าย

- ใช้ไฟร์วอลล์ (Firewall) ที่เป็นฮาร์ดแวร์หรือซอฟต์แวร์เพื่อทำหน้าที่เป็นยามประตูตรวจสอบการเข้าระบบ และถ้าท่านใช้งานคอมพิวเตอร์เพียงเครื่องเดียว โปรแกรมไฟร์วอลล์ก็เพียงพอที่จะใช้ป้องกันระบบ เช่น McAfee Personal Firewall (www.mcafee.com), Norton Internet Security (www.symantec.com), Sygate Personal Firewall (www.sygate.com) และ ZoneAlarm (www.zonelabs.com) สำหรับเวอร์ชันธรรมดาดาวน์โหลดฟรี แต่ถ้าเป็นเวอร์ชัน Pro และ Plus จะต้องเสียค่าใช้จ่าย

6) การป้องกันไวรัสคอมพิวเตอร์

- ปฏิบัติตามเคล็ดลับง่าย ๆ 5 ข้อ ด้วยตัวอักษรย่อ **EMAIL** ดังนี้ (http://www.technofocusweb.com/intrend/160946.html)

E ย่อมาจาก Exempt from unknown คือ ไม่เปิดอีเมลจากคนแปลกหน้า เพราะมีโอกาสเสี่ยงสูงที่จะติดไว้รัสหรือเป็นอีเมลขยะ

M ย่อมาจาก Mind the subject คือ หมั่นสังเกตหัวข้อของจดหมายก่อนที่จะเปิดอ่าน โดยเฉพาะอีเมลที่มีหัวข้อเป็นภาษาอังกฤษ ที่มีใจความดึงดูดให้รีบเปิดอ่าน หรือมีการหลอกล่อด้วยวิธีการต่าง ๆ เช่น มีคำว่า “RE.....” อยู่หน้าหัวข้อ ทำให้ผู้รับอีเมลคิดว่าเป็นการตอบจดหมายกลับมา

A ย่อมาจากประโยค Antivirus must be installed หมายความว่า ควรติดตั้งโปรแกรมป้องกันไวรัส เช่น Norton Antivirus (www.symantec.com), PC-cillin (www.pc-cillin.com), Dr.Solomon Anti-Virus และหมั่นอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ

I ย่อมาจาก Interest on virus news หมายความว่า ควรให้ความสนใจกับข่าวเกี่ยวกับไวรัส ติดตามข่าวสารจากสื่อต่างๆ

L ย่อมาจาก Learn to be cautious หมายความว่า ให้ระวังให้มาก อย่าเปิดอีเมลแบบไม่ยั้งคิด เพราะจากการสำรวจพบว่า ร้อยละ 70-80 ของอีเมลทั้งหมดคือไวรัสและอีเมลขยะ

- ติดตามข่าวสารเกี่ยวกับการป้องกันการก่อกวนและทำลายข้อมูลได้ที่ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (http://thaicert.nectec.or.th/)

ตัวอย่างของไวรัสคอมพิวเตอร์ที่มีผลต่อองค์กร (หนังสือพิมพ์ M2F, 8 มิ.ย.2555)

ไวรัสคอมพิวเตอร์นับว่าเป็นเชื้อโรคทางไอที ที่ยากจะหาทางรักษาหรือกำจัดให้พ้นได้ แม้ว่าจะมีบริษัทหลายแห่งออกมาสร้างโปรแกรมด้านไวรัสเพื่อให้ข้อมูลในคอมพิวเตอร์อยู่รอดปลอดภัย แต่มิวายที่บรรดาผู้ผลิตไวรัสจะคิดค้นเชื้อตัวใหม่ให้ป่วนระบบคอมพิวเตอร์ขึ้นอีกครั้ง ซึ่งก่อให้เกิดภาวะสงครามไซเบอร์ที่กำลังจะอุบัติขึ้นไปทั่วโลก

“เฟลม” (Worm Win32 Flame) คือไวรัสที่รัฐบาลของสหรัฐอเมริกาและหน่วยงานความมั่นคงทั่วโลกกำลังจับตามอง เพราะศักยภาพของไวรัสตัวนี้สามารถโจมตีระบบออนไลน์และโจรกรรมข้อมูลข้ามชาติ สิ่งที่ ”เฟลม”ฉกชิงไปนั้นไม่ใช่แค่เพียงข้อมูลความลับขององค์กรเท่านั้น แต่ล้วงข้อมูลทางด้านการธนาคาร ลุกลามไปถึงประเด็นการเมือง การทหาร เศรษฐกิจ สังคม วัฒนธรรม และการพัฒนาอาวุธนิวเคลียร์ อันจะนำไปสู่ความบานปลายแห่งสงครามที่ต่อสู้กันไม่รู้จบ

จากการตรวจสอบของเซดริก เล่ห์ตัน อดีตเจ้าหน้าที่กองทัพอากาศแห่งสหรัฐเผยว่า ไวรัส “เฟลม” ถูกเขียนขึ้นโดยใช้ภาษา Lua เป็นภาษาเดียวกับเกมยอดฮิตอย่าง “แองกรี้เบิร์ด” เกมยอดนิยมแห่งโลกออนไลน์ สาเหตุที่ใช้ภาษา Lua นั้นสืบเนื่องมาจากเป็นภาษาที่เหล่าโปรแกรมเมอร์ที่มีความสามารถที่จะเข้าใจ อีกทั้งยังเป็นรหัสลับที่จดจำและใช้งานได้ง่าย ด้วยเหตุนี้ผู้ปล่อยเชื้อไวรัส “เฟลม” จึงสามารถสร้างเครือข่ายและระบบป้องกันที่แข็งแกร่ง เพื่อให้แพร่กระจายมากและรวดเร็วที่สุด โดยเป้าหมายที่ “เฟลม” จะมุ่งโจมตีนั่นก็คือประเทศที่ไม่ทันระวังตัวในภัยพิบัติด้านเทคโนโลยี

ผู้เชี่ยวชาญด้านคอมพิวเตอร์เผยว่า รหัสลับของ “เฟลม” นี้อาจสร้างมาจากผู้ผลิตหนอนคอมพิวเตอร์ “สตักซ์เน็ต” นั้นทำได้แค่เพียงการเล่นงานให้อิหร่านเกิดความปั่นป่วนเท่านั้น แต่เทคโนโลยีที่ได้พัฒนาอย่างต่อเนื่องนั้นทำให้ “เฟลม” มีประสิทธิภาพการทำงานที่ยอดเยี่ยมกว่า “สตักซ์เน็ต” มากถึง 20 เท่า หรือก็คือ “เฟลม” จะสามารถโจรกรรมข้อมูลได้ทุกรูปแบบโดยที่เหยื่อไม่รู้ตัวเลยแม้แต่น้อย วิธีการที่ง่ายและแยบยลมากที่สุดที่ “เฟลม” จะชิงข้อมูลนั้นมาจากการใช้แฮนดี้ไดรฟ์ที่ห้อยอยู่ที่คอนั่นเอง จากนั้นแฮนดี้ไดรฟ์จะบันทึกข้อมูลจากเครื่องหนึ่งไปสู่อีกเครื่องหนึ่ง ทำให้ไวรัส “เฟลม” สามารถแพร่กระจายไปโดยเร็วที่สุด นอกจากนี้”เฟลม” ยังมีรูปแบบอื่นอีก เช่น การขโมยข้อมูลระหว่างที่เหยื่อเชื่อมต่ออินเทอร์เน็ตทางเว็บแคม ไมโครโฟน และบลูทูธ เพื่อที่จะสังเกต บันทึก และอัดเสียง ซึ่งไม่มีทางป้องกันหรือระวังตัวได้เลยแม้แต่วินาทีเดียว

สหภาพการสื่อสารโทรคมนาคม (ไอทียู) และบริษัทแคสเปอร์สกีแล็ป บริษัทผู้ผลิตซอฟต์แวร์สัญชาติรัสเซียได้ออกคำเตือนให้ทั่วโลกเฝ้าระวังไวรัสนี้ เนื่องจากเป็นเครื่องมือโจรกรรมข้อมูลที่อันตรายอย่างยิ่งยวด ด้วยความที่ไวรัส “เฟลม” ได้พบในแถบตะวันออกกลางอย่างอิหร่าน เลบานอน และซีเรีย ทำให้หลายฝ่ายคาดการณ์ว่าต้นตอของผู้ผลิตนั้นอาจจะมาจากชาติตะวันตกหรืออิสราเอลก็เป็นได้ เนื่องจากทั้งอิหร่านและอิสราเอลเป็นประเทศปรปักษ์กันมาตลอด จึงไม่น่าจะเป็นเรื่องแปลกที่สองประเทศนี้กำลังจะสร้างสงครามเย็นลูกใหม่ที่มีการใช้อาวุธไซเบอร์เข้าโจมตีกัน อย่างไรก็ตาม

อิหร่านยังไม่ได้ระบุตัวผู้ลงมือปล่อยพิษร้ายทางเทคโนโลยีแต่อย่างใด เพียงแต่เผยว่าได้สร้างซอฟต์แวร์ต่อต้านไวรัสที่มีประสิทธิภาพในการตามล่าและจัดการ”เฟลม” ออกจากคอมพิวเตอร์ได้แล้ว หากยังมีการละเลยและไม่แก้ไขให้ทันเวลา เชื้อโรคไวรัส”เฟลม” ตัวนี้อาจจะก่อตัวกลายเป็นวิกฤตเลวร้ายในอนาคตก็เป็นได้

นอกจากข้อควรระวังแล้วยังมีข้อแนะนำบางประการเพื่อสร้างสังคมและรักษาสิ่งแวดล้อม ดังนี้

1) การป้องกันเด็กเข้าไปดูเว็บไซต์ที่ไม่เหมาะสม

การส่งเสริมให้เด็กใช้อินเตอร์เน็ตเพื่อการค้นคว้าเป็นสิ่งที่ดีมีประโยชน์ แต่ในขณะเดียวกันก็มีข้อควรพึงระวังด้วยเช่นกัน เนื่องจากสารสนเทศที่เผยแพร่ทางอินเทอร์เน็ตมีทั้งดีและไม่ดี ดังนั้นผู้ปกครองควรให้ความเอาใจใส่ให้เด็กใช้อินเทอร์เน็ตอย่างเหมาะสมด้วย โดยทั่วไปการป้องกันการเข้าไปในเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ภาพอนาจาร หรือเว็บไซต์การพนัน จะมีโปรแกรมสำหรับกลั่นกรอง (Web Filtering Software) โดยจะทำการเปรียบเทียบเว็บไซต์ที่เด็กจะเข้าไปกับฐานข้อมูลเว็บไซต์ที่รวบรวมไว้ว่าเป็นเว็บไซต์ที่ไม่เหมาะสม หากไม่พบก็จะไปตรวจสอบกับเนื้อหาในเว็บไซต์นั้น ถ้าพบคำที่ไม่เหมาะสมก็จะไม่อนุญาตให้เด็กเข้าไปยังเว็บไซต์นั้น ๆ

2) การวางแผนเพื่อจัดการกับเครื่องคอมพิวเตอร์ที่ไม่ใช้แล้ว

คอมพิวเตอร์ที่ซื้อในวันนี้จะล้าสมัยภายใน 2-3 ปี ในระหว่างการใช้งานผู้ใช้อาจมีความต้องการอัพเกรดอุปกรณ์ต่าง ๆ ส่งผลให้เกิดขยะอิเล็กทรอนิกส์ ซึ่งกำลังสร้างปัญหาอย่างมากในหลายประเทศ ไม่เพียงเฉพาะคอมพิวเตอร์ที่ล้าสมัย ไม่ใช้แล้วเท่านั้นที่ก่อปัญหาสิ่งแวดล้อม ยังรวมถึงคู่มือการใช้ซอฟต์แวร์โบรชัวร์ และบัตรลงทะเบียน ทุก ๆ ครั้งที่มีการปรับเปลี่ยนซอฟต์แวร์ ดิสเกตต์ หรือซีดีรอมของเดิมก็จะเปลี่ยนเป็นขยะไปในที่สุด ในบางบริษัทจัดการด้วยการบริจาคเครื่องคอมพิวเตอร์ที่ไม่ใช้แล้วให้กับโรงเรียน บางบริษัทที่จำหน่ายคอมพิวเตอร์ก็รับซื้อคืนเพื่อนำอุปกรณ์บางส่วนไปประกอบใหม่และขายในราคาถูก และในบางประเทศก็จะมีหน่วยงานที่ทำหน้าที่ดัดแปลงอุปกรณ์คอมพิวเตอร์มาใช้งานใหม่

3) การใช้พลังงาน

บริษัทที่ผลิตฮาร์ดแวร์และซอฟต์แวร์พยายามคิดค้นและผลิตสินค้าที่ใช้พลังงานให้น้อยที่สุด เครื่องคอมพิวเตอร์รุ่นใหม่ ๆ ผู้ใช้สามารถเลือกกำหนดเป็น Sleep Mode เพื่อหยุดการหมุนของฮาร์ดดิสก์และปิดการใช้งานจอภาพชั่วคราว ผู้ใช้ก็เป็นอีกผู้หนึ่งที่ช่วยลดมลพิษได้ด้วยการกำหนดระบบและเลือกใช้สินค้าที่ช่วยรักษาสภาพแวดล้อม

2.3 การดำเนินการจัดการความรู้ขององค์กรที่ปรากฏบนเว็บไซต์

การจัดการความรู้ในโรงพยาบาลศิริราช

คณะแพทยศาสตร์ศิริราชพยาบาล ได้เข้าร่วมเป็นหน่วยงานนำร่องในโครงการ “การจัดการองค์ความรู้ในองค์กร” ของสถาบันเพิ่มผลผลิตแห่งชาติ โดยผู้บริหารและคณะทำงานการจัดการความรู้ (คณะทำงาน KM) เข้ารับการอบรมและเลือกหัวข้อ “การทำ CQI (Continuous Quality Improvement) ทางคลินิก” มาบริหารจัดการตามรูปแบบการจัดการความรู้ข้างต้น

เหตุที่เลือก CQI คลินิกเพราะทางคณะฯ มีนโยบายการพัฒนากระบวนการดูแลผู้ป่วยเป็นหลัก และที่ผ่านมาทีมดูแลผู้ป่วยเกือบทุกทีมในโรงพยาบาลศิริราชต่างก็มีรูปแบบการพัฒนาเฉพาะกลุ่มเพื่อประโยชน์แก่ผู้ป่วย (http://www.si.mahidol.ac.th/km/document/document1.htm)

เป้าหมาย (Goal) ของการจัดการความรู้คือ มีระบบเครือข่ายในการถ่ายโอนความรู้ (ด้าน CQI ทางคลินิก) เพื่อให้มี Best Practices ในการดูแลผู้ป่วยของโรงพยาบาลศิริราช

ตัวอย่างของแผนและกิจกรรมของการจัดการความรู้ (ศรีไพร และเจษฎาพร, 2549)

ตารางที่ 1 กระบวนการจัดการความรู้ของคณะแพทยศาสตร์ศิริราชพยาบาล

กระบวนการ	ตัวอย่างของแผนและกิจกรรม
การเปลี่ยนแปลงและพฤติกรรม (Transition and Behavior Management)	● วิเคราะห์วัฒนธรรมองค์การเปรียบเทียบกับวัฒนธรรมการจัดการความรู้ ● วางแผนและจัดกิจกรรมเพื่อให้ผู้บริหารและผู้ที่เกี่ยวข้องให้การสนับสนุน โดยผู้บริหารจะทำหน้าที่เป็นตัวอย่างที่ดีในการเข้าร่วมกิจกรรมของโครงการ
การสื่อสาร (Communication)	มีการสื่อสารเกี่ยวกับการจัดการความรู้ในองค์การอย่างทั่วถึงและต่อเนื่องผ่านช่องทางการสื่อสารต่าง ๆ เช่น ● สารศิริราช ● เสียงตามสาย ● บอร์ดประชาสัมพันธ์ ● การประชุมและกิจกรรม ● เว็บไซต์ (KM Website) ● KM Call Center

กระบวนการ	ตัวอย่างของแผนและกิจกรรม
กระบวนการและเครื่องมือ (Process and Tools)	● มีฐานข้อมูล CQI และฐานข้อมูลผู้เชี่ยวชาญที่มีประสบการณ์ในการทำ CQI ● สร้างเครือข่ายการแลกเปลี่ยนความรู้ร่วมกัน (Community of Practice : CoP) ● มีระบบสารสนเทศที่เอื้ออำนวยต่อการจัดการความรู้ เช่น * SiNet เป็นสื่อกลาง และแลกเปลี่ยนความรู้อย่างเป็นระบบ * ปรับโปรแกรม Lotus Notes ที่มีอยู่เพื่อรองรับการดำเนินงาน
การเรียนรู้ (Learning)	จัดฝึกอบรมทักษะที่เกี่ยวข้องในการแลกเปลี่ยนความรู้ให้แก่บุคลากรทางคลินิกโดยผ่านทางสื่อต่าง ๆ เช่น ● วารสาร โปสเตอร์ บอร์ดนิทรรศการ ● เว็บไซต์ (KM Website)
การวัดผล (Measurements)	มีเครื่องมือชี้วัดในการดำเนินงาน เช่น ● จำนวนผู้เข้าชมเว็บไซต์ (KM Website) ● จำนวนสมาชิกที่เข้าเสวนาใน KM Web Board ● จำนวนสมาชิกที่ขอคำปรึกษาที่ KM Call Center ● จำนวนข้อมูลการทำ CQI ในเว็บไซต์
การยกย่องชมเชยและให้รางวัล (Recognition and Rewards)	มีระบบการให้รางวัลแก่บุคลากรที่มีการแลกเปลี่ยนความรู้และเข้าร่วมกิจกรรมเช่น ● ประกาศเกียรติคุณ ● ประกาศภาพถ่าย ชื่อ และผลงานผ่านสื่อ ● กำหนดให้ผลงาน CQI เป็นหัวข้อหนึ่งสำหรับการประเมินผลงาน

การจัดการความรู้ของบริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน)

บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) หรือที่รู้จักกันว่า “ทรู” เป็นผู้นำในการให้บริการสื่อสารครบวงจร และเป็นผู้ให้บริการด้านการสื่อสารรายใหญ่ที่สุดในกรุงเทพฯ และปริมณฑล ปัจจัยแห่งความสำเร็จอย่างหนึ่งของทรู คือ ความพึงพอใจของลูกค้า ดังนั้นการให้บริการที่ดีเลิศต่อลูกค้าจึงมีความสำคัญต่อทรูเป็นอย่างมาก ทรูจึงจัดทำโครงการจัดการความรู้ในส่วนสายงาน Customer Management เพื่อสร้างความพึงพอใจสูงสุดให้กับลูกค้าและพัฒนาการดำเนินงานรวมทั้งศักยภาพการแข่งขันขององค์การ โดยใช้รูปแบบการจัดการความรู้

เป้าหมาย (Goal) ของการจัดการความรู้ คือ “TRUE KM is aim to be a center of corporate information and establishing true knowledge sharing community”

ตัวอย่างกิจกรรมของกระบวนการจัดการความรู้ (ศรีไพร และเจษฎาพร, 2549)

ตารางที่ 2 กระบวนการจัดการความรู้ของบริษัท ทรู

กระบวนการ	ตัวอย่างของแผนและกิจกรรม
การเปลี่ยนแปลงและพฤติกรรม (Transition and Behavior Management)	ปรับเปลี่ยนพฤติกรรมของคนในองค์การ ● คัดเลือกหน่วยงานที่เป็นผู้นำร่วมดำเนินโครงการเพื่อแลกเปลี่ยนความรู้ แนวคิด และเป็นตัวอย่างที่ดีในการดำเนินโครงการ ● จัดตั้งคณะทำงาน KM Community ● ประเมินผลของสถานการณ์จัดการความรู้ ● ปรับทัศนคติโดยเริ่มจากการสื่อสาร สัมมนาเชิงปฏิบัติการ ● กำหนดนิยามความรู้ในองค์การ ● กิจกรรมอื่น ๆ เพื่อก่อให้เกิดพฤติกรรมการเรียนรู้ เช่น การทำ Knowledge Sharing, การเปิด KM Web เป็นต้น
การสื่อสาร (Communication)	มีช่องทางการสื่อสารที่มีประสิทธิภาพ เช่น ● วารสารอิเล็กทรอนิกส์ ● E-mail ● E-Card ● โปสเตอร์ (Poster)
กระบวนการและเครื่องมือ (Process and Tools)	กำหนดขั้นตอนการจัดการความรู้อย่างเป็นระบบและสอดคล้องกับการปฏิบัติงานจริง รวมถึงจัดหาเครื่องมือและเทคโนโลยีที่ใช้ง่าย สะดวก มาสนับสนุนการแลกเปลี่ยนและถ่ายโอนความรู้ เช่น อินทราเน็ต (KM Web) เพื่อเป็นศูนย์กลางของความรู้ (Centralized Knowledge)
การอบรมและการเรียนรู้ (Training/Learning)	จัดฝึกงานให้แก่บุคลากร โดยกำหนดวัตถุประสงค์ที่ชัดเจน แต่ชี้ให้เห็นถึงประโยชน์ที่จะได้รับ เช่น การทำ ● E-book ● อินทราเน็ตของหน่วยงานและขององค์การ ● มุม KM (KM Corner) ● ส่งเสริมการเรียนรู้ด้วยตนเอง (Self-Learning) ● E-Learning

กระบวนการ	ตัวอย่างของแผนและกิจกรรม
การวัดผล (Measurements)	มีเครื่องมือชี้วัดที่เหมาะสมแยกตามประเภทต่าง ๆ เช่น ● ความง่ายในการใช้งานของระบบ ● ความพึงพอใจของพนักงาน ● คำแนะนำต่าง ๆ
การยกย่องชมเชยและให้รางวัล (Recognition and Rewards)	มีการส่งเสริมและให้รางวัลแก่พนักงานที่เข้าร่วมกิจกรรม เช่น ● ให้รางวัลเป็นเงินสด หนังสือ ของที่ระลึก ● ระบบสะสมแต้มแยกเป็นประเภทบุคคลและหน่วยงาน

ความรู้เป็นทรัพย์สินทางกลยุทธ์ขององค์การ การประยุกต์ใช้ความรู้ก่อให้เกิดนวัตกรรมซึ่งจะส่งผลต่อความสามารถในการแข่งขันขององค์การ

การจัดการความรู้ไม่ได้เป็นเทคโนโลยี แต่เทคโนโลยีสารสนเทศเป็นสิ่งที่ขาดไม่ได้ในการพัฒนาการจัดการความรู้อย่างมีประสิทธิภาพ องค์การควรมีกระบวนการในการจัดการความรู้อย่างเป็นระบบที่เหมาะสมกับบริบทขององค์การ เนื่องจากองค์การต่างก็มีลักษณะเฉพาะของตนเองที่ทำให้แตกต่างจากองค์การอื่น อย่างไรก็ตามการจัดการความรู้นอกจากจะต้องคำนึงถึงบุคลากรในองค์การแล้ว ยังต้องพิจารณาถึงปัจจัยอื่น ๆ ที่เอื้อต่อความสำเร็จในการจัดการด้วย อย่างเช่น วัฒนธรรมองค์การ การสนับสนุนจากผู้บริหาร การมีทิศทางและกลยุทธ์ที่ชัดเจนในการจัดการความรู้ มีการนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการจัดการความรู้ มีการวัดผลของการจัดการความรู้ และการมีโครงสร้างพื้นฐานที่รองรับหรือเอื้อให้เกิดการแลกเปลี่ยนความรู้ เป็นต้น

ระบบความปลอดภัยของ ME ของบมจ.ธนาคารทหารไทย

อาจารย์ปริญญา หอมอเนก ผู้ก่อตั้งและประธานบริษัท ACIS Professional Center บริษัทที่ปรึกษา และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (หนังสือพิมพ์ M2F, 8 มิ.ย.2555) กล่าวว่า ME by TMB คือ การธนาคารรูปแบบใหม่เพราะเป็นระบบการทำธุรกรรมแบบออนไลน์ กับการทำธุรกรรมผ่าน call center มาไว้ด้วยกัน ซึ่งถือเป็นการทำธุรกรรมแบบอิเล็กทรอนิกส์ครบวงจร เพราะเป็นการทำธุรกรรมโอนเงินต่างธนาคารผ่าน call center ในด้านความปลอดภัยที่มีการผูกบัญชีที่จะโอนเงินออกจาก ME ตั้งแต่ตอนลงทะเบียนแล้ว โดยเราต้องเลือกบัญชีออมทรัพย์ของธนาคารใดก็ได้ แต่ต้องเป็นชื่อเราเท่านั้น เพราะฉะนั้นมันเป็นไปไม่ได้เลยที่จะมีใครเอาเงินของเราจากบัญชี ME ไปโอนใส่บัญชีชื่อคนอื่น และหากเราหลงเข้าไปในพวกเว็บไซต์ปลอมที่ทำขึ้นมาหลอก เรียกว่าการโจมตีแบบ Phishing โดยเว็บของแฮคเกอร์จะหน้าตาเหมือนเว็บจริงแทบทุกอย่าง แม้แฮคเกอร์จะ

หลอกเอา User Name กับ Password ของเราไปก็ไม่มีปัญหาเพราะเงินก็โอนไปบัญชีอื่นที่ไม่ใช่ชื่อของเราไม่ได้

อีกส่วนหนึ่งของระบบความปลอดภัยคือ การใช้ OTP (One Time Password) หรือรหัสชั่วคราวสำหรับใช้ครั้งเดียว ที่จะส่งไปยังมือถือของเจ้าของบัญชีเท่านั้น ในกรณีที่มีการขอเปลี่ยนแปลงข้อมูลสำคัญ ๆ ทุกครั้ง รหัสนี้มีอายุใช้งานแค่ 3 นาที ถ้าขอแล้วไม่ใช้ในเวลา ต้องขอใหม่ตรงนี้สำคัญ เวลายิ่งน้อยยิ่งปลอดภัย ถ้าให้อายุใช้งานเป็นชั่วโมง แฮคเกอร์อาจเจาะเข้าบัญชีของเราได้เพราะมีเวลามากพอ

การทำธุรกรรมผ่าน call center ก็มีความปลอดภัยสูง ระบบมีชุดคำถามที่เราเท่านั้นที่รู้และต้องตอบให้ถูกต้องเพราะมันกรองพวกที่ปลอมแปลงมาได้ละเอียด จากที่ได้ทดสอบมีความมั่นใจเพราะต้องตอบคำถามหลาย ๆ ข้อที่ลึกมาก อีกทั้งการที่ต้องมาแสดงตัวที่ ME Place ถือเป็นเรื่องที่ดีมากในมุมของความปลอดภัยของลูกค้า เพราะทุกครั้งที่มีการเปลี่ยนข้อมูลสำคัญเช่น เปลี่ยนบัญชีที่ผูกไว้ ต้องมายืนยันความถูกต้องด้วยตัวเอง ต้องเอาสมุดบัญชีของธนาคารนั้น ๆ มาโชว์ เอาชื่อเอาหน้า และบัตรมาโชว์ ข้อมูลต้องตรงกันทั้งหมดทำแค่ครั้งเดียว

อาจารย์ปริญญากล่าวว่า ข้อมูลที่โดนแฮคก์จะโดนดักจับข้อมูลระหว่างที่มีการทำธุรกรรม โดยปกติข้อมูลที่ส่งผ่านเว็บเกี่ยวกับการเงินจะถูกเข้ารหัสเอาไว้อยู่แล้ว แต่การเข้ารหัสข้อมูลของ ME มีความละเอียดกว่าเว็บทั่วไปมาก เพราะกุญแจที่ใช้ในการเข้ารหัส SSL (Secured Socket Layer) นั้นมีความยาวถึง 256 bits ถ้าแฮคเกอร์เจาะเอาข้อมูลของเว็บสถาบันการเงินทั่วไปที่ใช้กุญแจในการเข้ารหัส SSL มีความยาว 128 bits จะใช้เวลาในการถอดรหัสน้อยกว่าของ ME ที่มีความยาวของกุญแจถึง 256 bits หมายความว่า ถ้าเจาะการเข้ารหัสของ ME ต้องใช้เวลากว่า 100 ปี ด้วยเทคโนโลยีในปัจจุบัน ซึ่งแทบจะเป็นไปไม่ได้เลยในทางปฏิบัติ

2.4 งานวิจัยที่เกี่ยวข้อง

งานวิจัยของ Wang Xueyuan, Yang Bo และ kuang Yin (2009) เรื่อง research on knowledge management system based on NXD เป็นดังนี้ This paper has introduced knowledge management and related concept, has analysed the characteristic of native xml database, aims at the bottleneck problem in the development of knowledge management system, Have put forward solution that establishment of knowledge management system based on native xml database, in the finally, have given a reference model of knowledge management system base on Tamino.

งานวิจัยของ An-Pin Chen และ Mu-Yen Chen (2005) ซึ่งเป็นการวัดประสิทธิภาพของระบบจัดการความรู้ เรื่อง A review of survey research in knowledge management performance measurement : 1995-2004 ได้ผลลัพธ์ดังนี้

Discussion is indicated the followings future development directions for KM performance evaluation: (1) KM performance evaluation is getting more important. (2) The quantitative analysis is the primary methodology in KM performance evaluation. (3) Firms are now highlighting the KM performance of competitors, through benchmarking or best practices, rather than internally auditing KM performance via balanced scorecard. (4) Firms may begin to focus more on project management measurement, than on the entire organization.

งานวิจัยของ Ployduangrat (2009) เรื่อง The development of knowledge management system for teacher in Basic Education School ได้ผลลัพธ์ดังนี้

A finding of this research was the effectiveness of developed knowledge management system was implemented in 20 teachers using by learned trough internet that everyone could manage their own knowledge by themselves in anywhere and anytime for the activities as long as their satisfaction. To collected the data from completed tasks of teacher activities on Web Blog. In addition the teachers suggested some problems and obstacles in knowledge management and learning and they had accepted the strengths and benefits of knowledge management on networking using by Web Blog.