การวิเคราะห์ปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงาน

Factor Analyzing for Security in Providing Computer Network Services for Organizations

นพดล สายคติกรณ์* และ เพียงฤทัย หนูสวัสดิ์
Noppadol Saikatikorn* and Paingruthai Nusawat
สาขาวิชาเทคโนโลยีสารสนเทศทางธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตวังไกลกังวล
Faculty of Business Administration, Department of Business Information Technology, RMUTR, Thailand
***Corresponding author; E-mail:** noppadol.sai@rmutr.ac.th

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงานโดยใช้แบบจำลองสมการเชิงโครงสร้าง ผู้วิจัยได้รวบรวมตัวชี้วัดจากการศึกษาวรรณกรรมอ้างอิง เก็บข้อมูลจากกลุ่มตัวอย่าง ทำการวิเคราะห์และสามารถสกัดปัจจัยได้ 6 ปัจจัย ทำการหาความสัมพันธ์ของปัจจัยต่าง ๆ ด้วยการวิเคราะห์สมการโครงสร้าง ผลของการวิจัยพบว่าปัจจัยด้านการควบคุมการเข้าถึงข้อมูลในระบบเครือข่าย (F2) และปัจจัยด้านการใช้งานข้อมูล การใช้งานอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูลในระบบเครือข่าย (F4) มีความสัมพันธ์กันในทางบวกแบบสองทิศทาง ค่าที่ได้จากแบบจำลองสอดคล้องกับข้อมูลโดยมีค่าพี (P-value) เท่ากับ 0.151 ค่าเอจีเอฟไอ (AGFI) เท่ากับ 0.957 ค่าจีเอฟไอ (GFI) เท่ากับ 0.988 ค่าอาร์เอ็มเอสอีเอ (RMSEA) เท่ากับ 0.048 และค่าความแม่นยำ (MMRE) เท่ากับ 10.144% ตามลำดับ โดยหน่วยงานที่ให้บริการระบบเครือข่ายควรให้ความสำคัญในประเด็นสำคัญ ดังนี้ 1) มีวิธีควบคุมและตรวจสอบการใช้งานของ user account 2) มีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกและเมื่อถูก reset password 3) มีการบังคับให้ผู้ใช้งานตั้งรหัสผ่านให้ยากแก่การคาดเดา เช่น ใช้ตัวอักษรผสมกับตัวเลข ห้ามใช้ชื่อหรือนามสกุล 4) มีการแจ้งเตือนเมื่อเข้าสู่เว็บไซต์ที่ไม่พึงประสงค์ 5) หากระบบตรวจพบไวรัส หรือสปายแวร์บนอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูล ระบบจะไม่อนุญาตให้ใช้งานได้

คำสำคัญ : แบบจำลองสมการเชิงโครงสร้าง ระบบความปลอดภัยข้อมูล ระบบเครือข่ายคอมพิวเตอร์

Abstract

This research aims to develop a prototype for security factor analysis in order to provide computer network services for agencies. By using the structural equation model, we collected the indicators from kinds of literature. Thirty-nine indicators were collected from the samples. Six factors can be extracted and analyzed. The relationship was determined by structural equation analysis. The results showed that the factors influencing the safety of using computer network services are factors controlling data access in the network (F2) and data usage factor, the use of devices and media for recording data in the network (F4). Both factors have a positive bi-directional relationship. The value obtained from the model corresponds to the data with a P-value of 0.151. The AGFI value is 0.957. The GFI is 0.988. The EMS (RMSEA) is 0.048 and the accuracy (MMRE) is 10.144%, respectively. The network service provider should pay attention to the important issues as follows. 1) There is the method to control and monitor user account usage. 2) Forcing the users to immediately change the password after first login and when resetting the password. 3) Forcing users to set their passwords which are hard to predict, such as using letters mixed with numbers, not using names or surnames. 4) There is a notification when entering unwanted websites. 5) In case of the system detects virus or spyware on various devices and media for recording data, the system will not allow using.

Keywords : Structural Equation Model, Information Security System, Computer Network System

บทนำ

การนำคอมพิวเตอร์มาใช้งานในการเชื่อมต่อถึงกันทั้งระบบเครือข่ายภายในและการเชื่อมต่อเข้าสู่โลกอินเทอร์เน็ตเพื่อการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลในรูปแบบต่าง ๆ เช่น ตัวอักษร ภาพและเสียง สามารถค้นหาข้อมูลจากที่ต่าง ๆ มีการรับส่งข้อมูลที่ทันสมัยได้ตลอดเวลาและสามารถใช้บริการในรูปแบบต่าง ๆ ได้ เช่น การรับส่งไปรษณีย์อิเล็กทรอนิกส์ (E-mail) การสืบค้นข้อมูลในอินเทอร์เน็ต การโอนย้ายข้อมูล (file transfer) และการดาวน์โหลดข้อมูล ฯลฯ จากความนิยมอย่างแพร่หลายของการใช้งานระบบเครือข่ายอินเทอร์เน็ตในด้านต่าง ๆ ส่งผลทำให้เกิดความเสี่ยงในด้านการจัดการระบบการรักษาความปลอดภัยของข้อมูลเป็นอย่างมาก

การรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ในหน่วยงานเป็นสิ่งจำเป็นและต้องกำหนดแบบแผนการดำเนินการตั้งแต่การออกแบบเครือข่าย เนื่องด้วยโลกธุรกิจในปัจจุบันข่าวสารที่สำคัญทางธุรกิจเป็นสิ่งที่ต้องปกป้องดูแล หากเครือข่ายไม่ได้ป้องกันให้ดีพอแล้วบุคคลภายนอกก็สามารถเข้ามาขโมยความลับทางธุรกิจผ่านเครือข่ายได้หรือแม้กระทั่งคนภายในองค์กรเอง ซึ่งอาจนำความลับขององค์กรไปได้เช่นกัน [1]

การที่ในหน่วยงานมีบุคลากรจำนวนมาก มีความหลากหลายในความต้องการเพื่อเข้าถึงระบบเครือข่ายคอมพิวเตอร์ขององค์กร อีกทั้งความต้องการ

ของบุคคลภายนอก เช่น ลูกค้า หรือ ผู้มีส่วนได้เสีย สำหรับการเข้าถึงซึ่งข้อมูลในส่วนที่ตนเองสามารถมีสิทธิ์ในการเข้าถึงได้นั้น และหลายหน่วยงานได้มีการนำเอาเทคโนโลยีสารสนเทศมาใช้เพื่ออำนวยความสะดวก

ผู้ดูแลระบบรักษาความปลอดภัยบนเครือข่าย สำหรับองค์กรจะคำนึงถึงระบบการรักษาความปลอดภัยเมื่อมีการต่อเชื่อมระบบเครือข่ายท้องถิ่นเข้าเครือข่ายอินเทอร์เน็ต โดยจะต้องมีการวางแผนและออกแบบระบบเครือข่าย เพื่อกำหนดรูปแบบในการป้องกันภัยจากบุคคลภายนอกหรือผู้ไม่ประสงค์ดีที่จะเข้ามาในระบบเครือข่าย และเพื่อไม่ให้สามารถเข้าใช้ข้อมูลได้ [2]

การวิเคราะห์ปัจจัย (Factor analysis) [3] หรือการวิเคราะห์ตัวประกอบเป็นเทคนิคที่จะจับกลุ่มหรือรวมตัวแปรที่มีความสัมพันธ์ไว้ในกลุ่มหรือปัจจัยเดียวกัน ตัวแปรที่อยู่ในปัจจัยเดียวกันจะมีความสัมพันธ์กันมาก โดยความสัมพันธ์นั้นอาจจะเป็นในทิศทางบวก (ไปในทางเดียวกัน) หรือทิศทางลบ (ไปในทางตรงกันข้าม) ก็ได้ ส่วนตัวแปรที่อยู่คนละปัจจัยจะไม่มีความสัมพันธ์กัน หรือมีความสัมพันธ์กันน้อยมาก

1. วัตถุประสงค์ของเทคนิค Factor analysis

1.1 การลดจำนวนตัวแปรหลายตัวให้เป็นปัจจัยเพียงไม่กี่ปัจจัย ซึ่งได้จากการศึกษาโครงสร้างความสัมพันธ์ระหว่างตัวแปร โดยที่จำนวนปัจจัยจะน้อยกว่าจำนวนตัวแปรโดยการนำตัวแปรที่มีความสัมพันธ์กันไว้ในปัจจัยเดียวกัน

1.2 เพื่อต้องการทดสอบสมมติฐานเกี่ยวกับโครงสร้างของปัจจัยและตัวแปรแต่ละตัวควรมีน้ำหนักหรืออัตราความสัมพันธ์กับปัจจัยมากน้อยเพียงใดตรงกับที่คาดคะเนไว้หรือไม่ หรือสรุปได้ว่าเพื่อต้องการทดสอบว่าปัจจัยนี้ตรงกับแบบจำลองหรือตรงกับบททฤษฎีที่มีอยู่หรือไม่ แบบจำลองนี้เรียกว่า Confirmatory Factor Analysis Model

2. ขั้นตอนการวิเคราะห์ของเทคนิค Factor analysis มีขั้นตอนต่าง ๆ ที่สำคัญ 4 ขั้นตอนดังนี้

2.1 เก็บรวบรวมข้อมูลและตรวจสอบว่าตัวแปรต่าง ๆ มีความสัมพันธ์กันหรือไม่ การวิเคราะห์ปัจจัยใช้หลักการการรวบรวมตัวแปรอิสระที่มีค่าความสัมพันธ์ต่อกันสูง การวิเคราะห์ภาพรวมของความสัมพันธ์ที่ตัวแปรอิสระทุก ๆ ตัวมีต่อกันว่าสูงพอต่อการนำไปจัดสร้างเป็นปัจจัยหรือไม่ จะพิจารณาจากค่า KMO (Kaiser-Meyer-Olkin Measure of Sampling Adequacy) ซึ่งเป็นค่าที่ได้จากการเปรียบเทียบขนาดของผลรวมของค่าสัมประสิทธิ์สหสัมพันธ์ที่ได้จากข้อมูลกับค่าผลรวมของค่าสัมประสิทธิ์สหสัมพันธ์เชิงส่วน หากค่า KMO มากกว่า 0.5 ขึ้นไปถือว่าอยู่ในเกณฑ์ที่สูงพอต่อการวิเคราะห์ปัจจัย ดังสมการที่ 1

$$KMO = \frac{\sum r_i^2}{\sum r_i^2 + \sum (\text{partial correlation})^2}$$

KMO คือค่าที่ได้จากการเปรียบเทียบขนาดของผลรวมของค่าสัมประสิทธิ์สหสัมพันธ์ที่ได้จากข้อมูลกับค่าผลรวมของค่าสัมประสิทธิ์สหสัมพันธ์เชิงส่วน (Kaiser -Meyer Olkin Measure of Sampling Adequacy)

Σ (partial correlation)^2 คือผลรวมของค่ายกกำลังสองของความสัมพันธ์บางส่วนของตัวแปร

2.2 การสกัดองค์ประกอบหรือการสกัดปัจจัย (Factor extraction) คือการหาจำนวนปัจจัยที่สามารถใช้แทนตัวแปรทั้งหมดทุกตัวได้ หรือเป็นการดึงรายละเอียดจากตัวแปรมาไว้ในปัจจัย วิธีการสกัดปัจจัยแบ่งออกเป็น 2 วิธีใหญ่ๆ คือ วิธีองค์ประกอบหลัก (Principal Component Analysis: PCA) และวิธีองค์ประกอบร่วม (Common Factor Analysis: CFA)

2.3 การหมุนแกนปัจจัย (Factor rotation) เป็นขั้นตอนที่จะดำเนินการแยกตัวแปรให้เห็นเด่นชัดว่าตัวแปรหนึ่ง ๆ ควรจะจัดอยู่ในกลุ่มหรือในปัจจัยใด เนื่องจากในการสกัดปัจจัยจะได้หนึ่งหรือหลายปัจจัย ซึ่งแต่ละปัจจัยจะเกิดการรวมของตัวแปรแบบเชิงเส้นตรง แต่ปัญหาที่เกิดขึ้นคือตัวแปรหนึ่ง ๆ อาจจะเป็นสมาชิกในหลายปัจจัยซึ่งยากต่อการให้ความหมายของปัจจัยและการกำหนดชื่อปัจจัยหรืออาจได้ความหมายของแต่ละปัจจัยไม่ชัดเจนการหมุนแกนจะเป็นวิธีการที่จะทำให้สมาชิกของแต่ละตัวแปรในปัจจัยหนึ่ง ๆ ชัดเจนขึ้น

2.4 การหาค่าคะแนนของปัจจัย (Factor score) เมื่อสามารถจัดตัวแปรที่มีอยู่จำนวนมากเหลือเป็นกลุ่มตัวแปรไม่กี่กลุ่ม สามารถคำนวณ หาค่า Factor score ของแต่ละกรณี (case) ได้ เช่น ถ้ามี 2 ปัจจัยก็สามารถคำนวณหาค่า Factor score ของทั้ง 2 ปัจจัยได้และถือว่าทั้ง 2 เป็นตัวแปรใหม่ที่นำไปวิเคราะห์ต่อไปได้

จากปัญหาหรือผลกระทบที่หลายหน่วยงานประสบเกี่ยวกับด้านการรักษาความปลอดภัยของข้อมูลในระบบเครือข่ายขององค์กรหรือในหน่วยงานนั้น ผู้วิจัยมีแนวคิดที่จะทำการศึกษาและวิเคราะห์ปัจจัยเชิงสาเหตุที่มีผลต่อความปลอดภัยในการใช้บริการระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน โดยใช้แบบจำลองสมการเชิงโครงสร้าง เพื่อนำระบบรักษาความปลอดภัยมาใช้งานให้เกิดประโยชน์สูงสุดต่อหน่วยงาน โดยนำการประเมินของผู้ใช้งานที่มีต่อระบบ รวมถึงการนำผลที่วิเคราะห์ได้ไปปรับปรุงระบบรักษาความปลอดภัยของเครือข่ายให้เกิดประโยชน์และเกิดประสิทธิภาพมากยิ่งขึ้น

วัตถุประสงค์การวิจัย

เพื่อวิเคราะห์ปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงานโดยใช้แบบจำลองสมการเชิงโครงสร้าง

วิธีการวิจัย

ในการดำเนินการวิจัยเพื่อทำการสร้างต้นแบบสำหรับวิเคราะห์ความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์ในหน่วยงานนั้น ผู้วิจัยได้ดำเนินงานโดยมีขั้นตอนการดำเนินงานดังนี้

1. ศึกษารวบรวมตัวชี้วัด (Manifest variable) ที่มีการอ้างอิงต่อความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จากงานวิจัย โดยสามารถจำแนกได้ ดังนี้

หมวดที่ 1 ด้านความปลอดภัยทางกายภาพและสิ่งแวดล้อม

Zs1_1. มีประตูทางเข้า-ออกที่มีการควบคุมเพื่อป้องกันการเข้าถึงอุปกรณ์ต่าง ๆ อย่างเคร่งครัด เช่น มีการใช้ proxy card หรือการตรวจสอบทางกายภาพของผู้เข้า-ออกบริเวณที่สำหรับให้บริการระบบเครือข่ายทุกครั้ง

Zs1_2. มีการอนุญาตให้ผ่านเข้า-ออกบริเวณห้องสำหรับให้บริการระบบเครือข่ายเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

Zs1_3. มีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อตรวจสอบความเคลื่อนไหวของบุคคลภายในบริเวณที่ให้บริการระบบเครือข่าย

Zs1_4. มีการป้องกันภัยคุกคามจากสิ่งแวดล้อมภายนอก ได้แก่ ไฟไหม้ น้ำท่วม ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

Zs1_5. มีการจัดวางและการป้องกันอุปกรณ์เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

Zs1_6. มีการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาตการทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

Zs1_7. มีระบบสำรองไฟฟ้ากรณีฉุกเฉินที่สามารถใช้งานได้ทันที

Zs1_8. มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

Zs1_9. มีการห้ามนำทรัพย์สินของหน่วยงานออกนอกพื้นที่ ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

หมวดที่ 2 ด้านการบริหาร การจัดการด้านการสื่อสารและการดำเนินงาน

Zs2_1. มีเจ้าหน้าที่คอยอำนวยความสะดวกเมื่อเกิดปัญหาเกี่ยวกับระบบเครือข่ายเพียงพอกับความต้องการ

Zs2_2. มีการจัดทำคู่มือการใช้งานระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานเผยแพร่แก่บุคลากร

Zs2_3. มีการจัดทำคู่มือการบริหารจัดการระบบความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานเผยแพร่แก่บุคลากร

Zs2_4. มีนโยบายและระเบียบปฏิบัติครอบคลุมเรื่องการควบคุมการใช้ข้อมูลและระบบคอมพิวเตอร์ของผู้ใช้งาน

Zs2_5. มีนโยบายและระเบียบปฏิบัติครอบคลุมเรื่องการรักษาความปลอดภัยเครือข่าย เช่น การป้องกันไวรัส เป็นต้น

Zs2_6. มีเอกสาร/คู่มือ การแนะนำการติดตั้งหรือการใช้งานระบบเครือข่ายอำนวยความสะดวกให้แก่ท่านอย่างเหมาะสม

Zs2_7. มีการจัดอบรมเพิ่มพูนความรู้ทางด้านระบบความปลอดภัยของเครือข่ายตรงกับความต้องการของบุคลากร

Zs2_8. มีการแนะนำวิธีการป้องกัน แก้ไขไวรัส สปายแวร์ หรืออื่น ๆ ที่เกี่ยวข้องอย่างสม่ำเสมอ

Zs2_9. เมื่อเกิดปัญหาจาก ไวรัส สปายแวร์ หรืออื่นๆ ที่เกี่ยวข้อง ที่เกิดจากการใช้งานระบบเครือข่าย ระบบจะมีการแจ้งเตือน กำจัด เป็นอย่างดี

Zs2_10. มีการเผยแพร่ประชาสัมพันธ์เกี่ยวกับบริการที่มีอยู่แล้ว หรือมีใหม่รวมถึงประโยชน์ต่าง ๆ ที่ผู้ใช้งานจะได้รับ

หมวดที่ 3 ด้านการควบคุมการเข้าถึงข้อมูลในระบบเครือข่าย

Zs3_1. มีการลงทะเบียนเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

Zs3_2. มีการบริหารจัดการสิทธิการใช้งานระบบ และจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

Zs3_3. มีวิธีควบคุมและตรวจสอบการใช้งาน user account

Zs3_4. มีการตรวจสอบสิทธิการเข้าใช้งานระบบเครือข่ายทุกครั้ง

Zs3_5. ระบบมีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกและเมื่อถูก reset password

Zs3_6. ระบบมีการบังคับให้ผู้ใช้งานตั้งรหัสผ่านให้ยากแก่การคาดเดา เช่น ใช้ตัวอักษรผสมกับตัวเลข ห้ามใช้ชื่อหรือนามสกุล

Zs3_7. ระบบมีการบังคับไม่ให้ใช้รหัสผ่านซ้ำกับของเดิม

Zs3_8. ระบบมีการห้ามการใช้งานโดยอัตโนมัติในกรณีที่ผู้ใช้งานป้อนรหัสผ่านผิดตามจำนวนครั้งที่กำหนด

Zs3_9. ระบบมีการห้ามการใช้งานโดยอัตโนมัติ ในกรณีที่ไม่ได้มีการใช้งานที่หน้าจอตามระยะเวลาที่กำหนด

Zs3_10. ระบบมีการบังคับไม่ให้ใช้บัญชีผู้ใช้งานเดียวกันเข้าระบบพร้อมกัน

หมวดที่ 4 ด้านการใช้งานข้อมูล การใช้งานอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูลในระบบเครือข่าย

Zs4_1. การโอนสิทธิ์การใช้งานทรัพยากรที่ตนเองได้รับสิทธิ์ให้ใช้แก่บุคคลอื่นยกเว้นได้รับอนุญาตจากหน่วยงาน

Zs4_2. มีการเผยแพร่ข้อมูลหรือสารสนเทศที่เป็นเท็จ หรือดำเนินการใด ๆ ที่จะส่งผลต่อความเสียหายแก่ผู้อื่นหรือหน่วยงาน

Zs4_3. มีการกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่นหรือหน่วยงาน

Zs4_4. ระบบมีการป้องกันการทำลาย หรือพยายามทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

Zs4_5. ระบบมีการแจ้งเตือนเมื่อเข้าสู่เว็บไซต์ที่ไม่พึงประสงค์

Zs4_6. ระบบมีการแจ้งเตือนเมื่อมีการดาวน์โหลดไฟล์ที่อาจจะก่อให้เกิดความเสียหายต่อระบบเครือข่ายได้

Zs4_7. ระบบมีการแจ้งเตือนเมื่อมีการติดตั้งโปรแกรมที่ไม่เหมาะสม อาจจะก่อให้เกิดความเสียหายต่อระบบเครือข่ายได้

Zs4_8. มีระบบการป้องกันและตรวจจับไวรัสครอบคลุมทุกเครื่องลูกข่ายที่สำคัญ

Zs4_9. มีการกำหนดให้ตรวจสอบไวรัสก่อนการใช้งานอุปกรณ์ และสื่อสำหรับการบันทึกข้อมูลต่าง ๆ บนระบบเครือข่าย ทุกครั้งก่อนการใช้งานหากระบบตรวจพบไวรัสหรือสปายแวร์บนอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูล ระบบจะไม่อนุญาตให้ใช้งานได้

2. จัดสร้างแบบสอบถามและเก็บรวบรวมข้อมูล โดยในการสร้างเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล มีขั้นตอนดังนี้

2.1 ติดต่อผู้เชี่ยวชาญที่มีประสบการณ์ด้านระบบเครือข่ายคอมพิวเตอร์ หรือด้านความปลอดภัยทางคอมพิวเตอร์จำนวน 5 ท่าน ในการสร้างแบบสอบถามจะใช้ค่าดัชนีความสอดคล้อง (IOC) จากผู้เชี่ยวชาญเพื่อหาข้อสรุปในการจัดสร้างแบบสอบถามสำหรับกลุ่มตัวอย่าง

2.2 จัดสร้างแบบสอบถามเพื่อใช้ในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง

3. การหาคุณภาพของแบบสอบถาม ผู้วิจัยได้นำแบบสอบถามฉบับร่างทดลองใช้กับกลุ่มตัวอย่างจำนวน 30 ชุด นำมาหาค่าความเชื่อมั่นของแบบสอบถามได้เท่ากับ 0.5329 สรุปได้ว่าแบบสอบถามชุดนี้สามารถใช้งานนำไปใช้เก็บข้อมูลจากกลุ่มตัวอย่างได้

4. การวิเคราะห์ปัจจัยการตรวจสอบข้อกำหนดเพื่อให้การวิเคราะห์ปัจจัยดำเนินไปด้วยความถูกต้อง จึงต้องทำการตรวจสอบต้องกำหนด ต่าง ๆ ดังนี้ [4]

4.1 การกำหนดจำนวนตัวอย่าง การคำนวณแบบ Maximum likelihood estimation (MLE) [9] ต้องใช้กลุ่มตัวอย่างจำนวนมากเพื่อใช้ในการคำนวณ ผู้วิจัยได้รวบรวมแบบสอบถามทั้งสิ้น 350 ชุด ซึ่งเกินจากข้อกำหนดขั้นต่ำที่กำหนดไว้ 200 ชุด

4.2 การกำหนดให้เป็นค่ามาตรฐาน (Standardized) เนื่องจากตัวแปรแต่ละหน่วยมีขนาดหน่วยที่ไม่เท่ากัน เช่น บางตัวแปรเป็นข้อมูลเชิงปริมาณ บางตัวแปรเป็นข้อมูลเชิงคุณภาพ อาจจะก่อให้เกิดอิทธิพลต่อตัวแปร ทำให้เกิดความผิดพลาดในการสร้างแบบจำลองได้ [5]

4.3 ผู้วิจัยได้นำแบบสอบถามที่ได้เก็บข้อมูลจากกลุ่มตัวอย่างมาทำการวิเคราะห์ปัจจัยโดยการสกัดปัจจัยแบบ PCA และทำการหมุนแกนแบบตั้งฉาก พบว่าค่า KMO = 0.914 โดยที่ค่าที่เหมาะสมควรมากกว่า 0.6 และการสกัดปัจจัยสามารถอธิบายความผันแปรของ

ทุกตัวแปรสะสม (Cumulative sum of squared loading variance explained) = 65.720 % นั่นคือการสกัดปัจจัยมีความเหมาะสม มีจำนวนตัวอย่างมากพอสำหรับการวิเคราะห์ปัจจัยและมีค่านัยสำคัญทางสถิติและได้ค่าจากการสกัดปัจจัยดังแสดงใน Table 1

Table 1. Factor and indicators

Factor	Indicators
F1	Zs2_1, Zs2_2, Zs2_3, Zs2_4, Zs2_5, Zs2_6, Zs2_7, Zs2_8, Zs2_9, Zs2_10
F2	Zs3_3, Zs3_4, Zs3_5, Zs3_6, Zs3_7, Zs3_8, Zs3_9, Zs3_10,
F3	Zs1_1, Zs1_2, Zs1_3, Zs1_4, Zs1_5, Zs1_6, Zs1_7, Zs1_8, Zs1_9

Table 1. Factor and indicators (Cont.)

Factor	Indicators
F4	Zs4_4, Zs4_5, Zs4_6, Zs4_7, Zs4_8, Zs4_9, Zs4_10
F5	Zs4_1, Zs4_2, Zs4_3
F6	Zs3_1, Zs3_2

การสร้างแบบจำลองสมการเชิงโครงสร้าง

จากการวิเคราะห์ปัจจัยผลที่ได้จะนำมาสร้างเป็นแบบจำลองโครงสร้างตั้งต้นโดยวิธีการ Maximum likelihood estimation ดังแสดงใน Figure 1

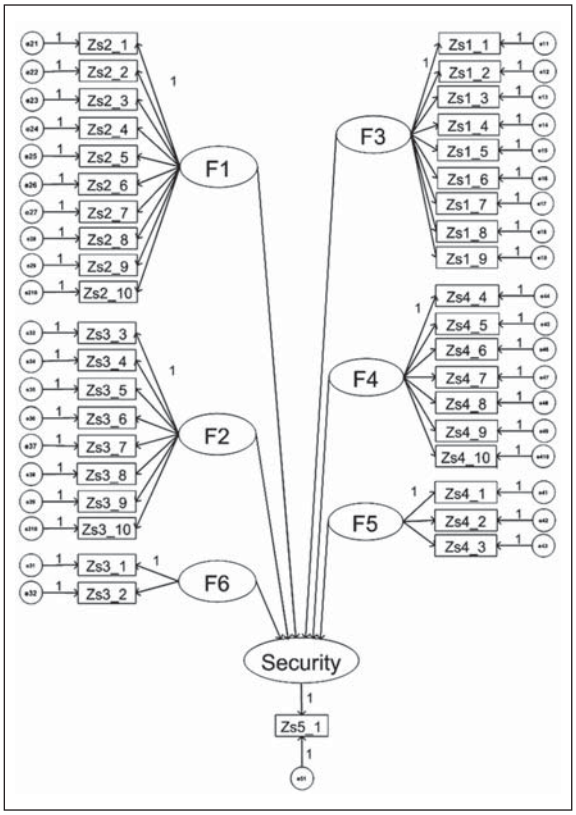

Figure 1. First Structural Equation Model

การประเมินความเหมาะสมของแบบจำลอง [6] การเริ่มต้นประเมินความเหมาะสมของแบบจำลองระบุแฟ้มข้อมูลที่ใช้เป็น Data set ในการคำนวณ ซึ่งเป็นข้อมูลที่ได้มาจากการเก็บตัวอย่างแล้วนำมาหาค่าทางสถิติ ระบุวิธีการวิเคราะห์สมการแบบจำลอง ในงานวิจัยนี้ใช้วิธีการวิเคราะห์สมการแบบจำลองโครงสร้าง โดยใช้วิธีแบบ MLE เนื่องจากข้อมูลที่นำมาคำนวณนั้นมากพอจึงสามารถเลือกใช้วิธีการนี้ได้

ค่าประมาณการของค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรต่าง ๆ ทั้งหมดในแบบจำลอง หากไม่มีความสำคัญทางสถิติแบบมีนัยสำคัญต่อกัน (P>0.05) สมควรที่จะต้องตัดออกจากแบบจำลอง เมื่อดำเนินการตัดออกต้องทำการวิเคราะห์ใหม่ เมื่อประมวลผลข้างต้นทำการตรวจสอบค่า Model Fit Summary เพื่อหาว่า

แบบจำลองมีความเหมาะสมหรือไม่ โดยการตรวจสอบค่าไค-สแคว (χ^2) ว่ามีค่า significance หรือไม่ ในงานวิจัยนี้พบว่าค่า ไค-สแคว (χ^2) significance คือค่า P=0.151 นั่นคือแบบจำลองเข้ากันได้กับ Data set ดังแสดงผลใน Table 2

Table 2. Statistics modeling structural equation

Statistics	Criterion	Value	interpretation
Chi-Square	> 0.05	0.151	qualified
GFI	> 0.9	0.988	qualified
AGFI	> 0.9	0.957	qualified
RMSEA	< 0.05	0.048	qualified
HOELTER	< 75	333	qualified

จากค่าที่ได้ใน Table 2 จะเห็นได้ว่าค่าสถิติต่าง ๆ ได้ผ่านข้อกำหนดขั้นต่ำมีความเข้ากันได้กับแบบจำลองของข้อมูลตัวอย่างที่ทำการวิเคราะห์แบบจำลองได้ [8] หลังจากที่ได้สมการแล้วในการประมาณค่าความปลอดภัยของการใช้บริการระบบเครือข่าย เพื่อคำนวณหาค่า MRE ของแบบสอบถามตัวอย่าง จนครบ 30 ตัวอย่าง แล้วทำการหาค่าเฉลี่ย MMRE (Average absolute MRE*100%) ได้ค่าเป็นร้อยละของความคลาดเคลื่อนเฉลี่ยของการประมาณการของแบบจำลอง

ผลการวิจัย

การวิจัยเรื่องการวิเคราะห์ปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงาน โดยใช้แบบจำลองสมการเชิงโครงสร้างนั้น

ผลของการวิจัยพบว่า ปัจจัยด้านการควบคุมการเข้าถึงข้อมูลในระบบเครือข่าย (F2) และปัจจัยด้านการใช้งานข้อมูล การใช้งานอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูลในระบบเครือข่าย (F4) มีความสัมพันธ์กันในทางบวกแบบสองทิศทาง ค่าที่ได้จากแบบจำลองสอดคล้องกับข้อมูลโดยมีค่าพี (P-Value) อยู่ที่ 0.151 ค่าเอจีเอฟไอ (AGFI) อยู่ที่ 0.957 ค่าจีเอฟไอ (GFI) อยู่ที่ 0.988 ค่าอาร์เอ็มเอสอีเอ (RMSEA) อยู่ที่ 0.048 และค่าความแม่นยำ (MMRE) อยู่ที่ 10.144% ตามลำดับ ผลดัง Figure 2

จากแบบจำลองสมการโครงสร้างปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงาน โดยการประเมินผลของผู้ใช้งานนั้น

สมการที่ได้จากแบบจำลองสามารถแสดงได้ดังนี้

Zs5_1 (ค่าคะแนนมาตรฐานความปลอดภัยจากการพยากรณ์) = 0.9 * Security (2)

Security = (0.52 * F2) + (0.65 * F4) (3)

F2=(0.82*Zs3_6)+(0.82*Zs3_5)+(0.80*Zs3_3) (4)

F4 = (0.72* Zs4_5)+(0.67*Zs4_10) (5)

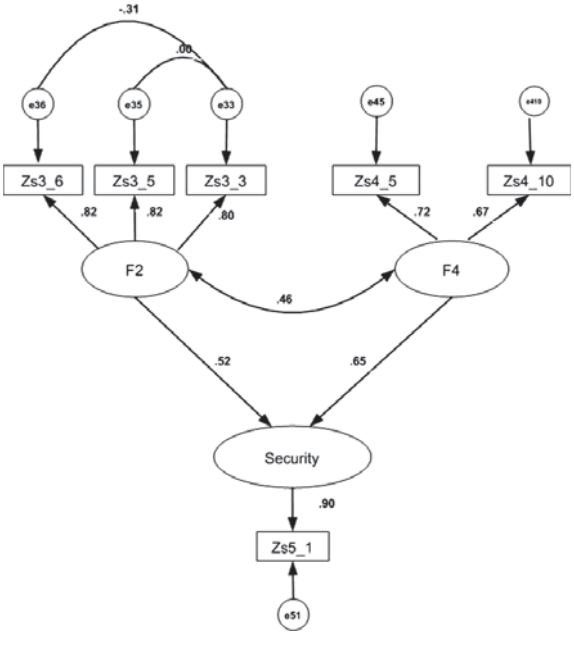

Figure 2. Structural equation model from data analysis

ความหมายของตัวบ่งชี้มาตรฐาน มีความหมายดังต่อไปนี้

Zs3_3 คือ ค่าคะแนนมาตรฐานมีวิธีควบคุมและตรวจสอบการใช้งาน user account

Zs3_5 คือ ค่าคะแนนมาตรฐานระบบมีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกและเมื่อถูก reset password

Zs3_6 คือ ค่าคะแนนมาตรฐานระบบมีการบังคับให้ผู้ใช้งานตั้งรหัสผ่านให้ยากแก่การคาดเดา เช่น ใช้ตัวอักษรผสมกับตัวเลขห้ามใช้ชื่อหรือนามสกุล

Zs4_5 คือ ค่าคะแนนมาตรฐานระบบมีการแจ้งเตือนเมื่อเข้าสู่เว็บไซต์ที่ไม่พึงประสงค์

Zs4_10 คือ ค่าคะแนนมาตรฐานหากระบบตรวจพบไวรัส หรือสปายแวร์บนอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูล ระบบจะไม่อนุญาตให้ใช้งานได้

อภิปรายผล

ปัจจัยด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์นั้น หน่วยงานต่าง ๆ ควรให้ความสำคัญเป็นอันดับแรก คือ ปัจจัยด้านการควบคุมการเข้าถึงข้อมูลในระบบเครือข่าย (F2) และรองลงมาคือ ปัจจัยด้านการใช้งานข้อมูล การใช้งานอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูลในระบบเครือข่าย (F4) โดยทั้งสองปัจจัยมีความสัมพันธ์กันในทางบวกแบบสองทิศทาง ซึ่งรายละเอียดของตัวบ่งชี้ด้านความปลอดภัยในการให้บริการระบบเครือข่ายคอมพิวเตอร์สำหรับหน่วยงาน ประกอบด้วย

1) มีวิธีควบคุมและตรวจสอบการใช้งาน user account

2) มีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกและเมื่อถูก reset password

3) มีการบังคับให้ผู้ใช้งานตั้งรหัสผ่านให้ยากแก่การคาดเดา เช่น ใช้ตัวอักษรผสมกับตัวเลขห้ามใช้ชื่อหรือนามสกุล

4) มีการแจ้งเตือนเมื่อเข้าสู่เว็บไซต์ที่ไม่พึงประสงค์

5) หากระบบตรวจพบไวรัส หรือสปายแวร์บนอุปกรณ์ต่าง ๆ และสื่อสำหรับการบันทึกข้อมูล ระบบจะไม่อนุญาตให้ใช้งานได้

ซึ่งสอดคล้องกับงานวิจัยของ วิเศษ ศักดิ์ศิริ [2] ที่กล่าวถึง บรรทัดฐานความปลอดภัยในระบบสารสนเทศขององค์กร จำเป็นต้องมีการควบคุมการเข้าถึงข้อมูลของบุคคลเพื่อและการให้สิทธิ์การเข้าถึงข้อมูลในแต่ละระดับชั้นของหน่วยงาน เพื่อความปลอดภัยทั้งของข้อมูลและความปลอดภัยของหน่วยงานเพื่อลดความเสี่ยงของการถูกโจรกรรมข้อมูลได้ อีกทั้งสอดคล้องกับงานวิจัยของ ศิริพร อ่วมมีเพียร และวลัยนุช สกุลนุ้ย [7] การเข้ารหัสก่อนส่งข้อมูลในระบบเครือข่ายแบบไร้สายและเมื่อเกิดปัญหาจากไวรัส สปายแวร์หรืออื่นๆ ที่เกี่ยวข้องที่เกิดจากการใช้ระบบเครือข่าย ระบบจะมีการแจ้งเตือนเป็นปัจจัยสำคัญเพื่อให้ผู้ดูแลระบบเครือข่ายทราบในการบริหารจัดการระบบให้มีความปลอดภัยอย่างเกิดประสิทธิภาพ ทั้งนี้รัชดา เจริญศรี [8] รายงานว่าการให้บริการเครือข่ายคอมพิวเตอร์สำหรับหน่วยงาน การมีวิธีควบคุมและตรวจสอบการใช้งาน user account และมีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกและเมื่อถูก reset password เป็นปัจจัยพื้นฐานในการเข้าใช้งานระบบเครือข่ายขององค์กร เช่นกัน

เอกสารอ้างอิง

1. จตุชัย แพงจันทร์. 2540. มาสเตอร์ อิน ซีเคียวริตี้ ความปลอดภัยของข้อมูล. นนทบุรี: ไอดีซีฯ.
2. วิเศษ ศักดิ์ศิริ. 2548. บรรทัดฐานความปลอดภัยในระบบสารสนเทศ. วารสารเทคโนโลยีสารสนเทศ. 20-25.
3. วัชราพร วงศ์สมิง. 2552. การพัฒนาแบบจำลองการประมาณค่าใช้จ่ายในการพัฒนาซอฟต์แวร์ประยุกต์เชิงโครงข่าย ประเภทการประมวลผลรายการกระทบยอดด้วยการวิเคราะห์สมการถดถอยและการวิเคราะห์ปัจจัย. ปริญญาวิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
4. สมชาย ปราการเจริญ. 2550. การวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการประมาณค่าใช้จ่ายในการพัฒนาซอฟต์แวร์ประยุกต์เชิงโครงข่ายโดยวิธีแบบจำลองสมการโครงสร้าง. บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
5. ยุทธ ไกยวรรณ์. 2556. การวิเคราะห์โมเดลสมการโครงสร้างด้วย AMOS. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.
6. พูลพงศ์ สุขสว่าง. 2557. หลักการวิเคราะห์โมเดลสมการโครงสร้าง. วารสารมหาวิทยาลัยนราธิวาสราชนครินทร์. ปีที่ 6: 136-145.
7. ศิริพร อ่วมมีเพียร และ วลัยนุช สกุลนุ้ย. 2552. ความพึงพอใจในการใช้บริการเครือข่ายคอมพิวเตอร์ วิทยาลัยราชพฤกษ์. สาขาวิชาคอมพิวเตอร์ธุรกิจ มหาวิทยาลัยราชพฤกษ์.
8. รัชดา เจริญศรี. 2550. การวิเคราะห์ปัจจัยเชิงสาเหตุที่มีผลต่อความพึงพอใจในการใช้บริการเครือข่ายคอมพิวเตอร์ของนักศึกษา โดยใช้แบบจำลองสมการโครงสร้าง กรณีศึกษา มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ. ปริญญาวิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
9. Schumacker, R. E. and Lomax, R. G. 2010. A beginner's guide to structural equation modeling. (3rd Edition), New Jersey: Lawrence Erlbaum Associates.