การวิเคราะห์ปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในองค์กรของประเทศไทย

ธนาวรรณ จันทรัตนไพบูลย์[1] และ อัจกิต อุฒาธรรม[2]*

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อต้องการศึกษาหาปัจจัยที่ทำให้เกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ และสร้างโมเดลเพื่อใช้ทำนายความเสี่ยงของภัยคุกคาม โดยใช้วิธีการออกแบบสอบถาม ซึ่งจะแบ่งเป็น 2 ส่วนคือ 1) แบบสอบถามสำรวจหาปัจจัย โดยมีกลุ่มตัวอย่างเป็นบุคลากรในองค์กรที่เกี่ยวข้องในด้านระบบสารสนเทศจำนวน 117 คน 2) แบบสอบถามเชิงลึก โดยใช้ข้อมูลจากแบบสอบถามส่วนแรกมาเป็นข้อมูลในการออกแบบสอบถามเพื่อใช้ในการวิเคราะห์ โดยมีกลุ่มตัวอย่างเป็นหัวหน้าหรือตัวแทนแผนกที่เกี่ยวข้องกับระบบสารสนเทศ จำนวน 298 ชุด เพื่อนำไปวิเคราะห์สร้างโมเดล โดยใช้ Multinomial Regression และใช้ s-2Log Likelihood และ Wald Statistics ในการหาค่าความเชื่อมั่นของโมเดลและสัมประสิทธิ์ตามลำดับ และพัฒนาเป็นโปรแกรมเพื่อช่วยทำนาย ผลวิจัยพบว่าจากการศึกษาและสำรวจปัจจัยได้ปัจจัยทั้งหมด 24 ปัจจัย และจากการวิเคราะห์ได้โมเดลที่สามารถทำนายการเกิดภัยคุกคาม 7 ประเภทด้วยกัน ซึ่งได้แก่ 1) ความผิดพลาดที่มาจากมนุษย์ 2) การบุกรุก 3) การกรรโชกข้อมูล 4) การทำลายระบบหรือข้อมูล 5) การโจรกรรม 6) การโจมตีจากซอฟต์แวร์และ 7) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ โดยมีนัยสำคัญเป็น 0.05 ผลการทดสอบพบว่าโมเดลมีความสอดคล้องกับปัจจัยที่กล่าวมาข้างต้นร้อยละ 50.00, 79.17, 66.67, 43.75, 83.33, 91.67 และ 93.75 ตามลำดับ

คำสำคัญ: ภัยคุกคามความปลอดภัย การทำนายความเสี่ยง ปัจจัยภัยคุกคาม

[1] ผู้ช่วยศาสตราจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

[2] นิสิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 0-2908-9661 อีเมล: ajagit_ag@hotmail.com

รับเมื่อ 7 กุมภาพันธ์ 2556 ตอบรับเมื่อ 25 มีนาคม 2556

The Factor Analysis and Modeling for Risk Prediction of Information Security Threats in Organization of Thailand

Thanawan Chantaratanapibul[1] and Ajagit Utatham[2]*

Abstract

The purposes of this study are to find factors causing information security threats and to design a model forcasing risks of the cyber threats, using a questionnaire survey consisting of 2 parts. Part I asks about the potential threat factors from 117 staff members for relevant information system organizations as samples searches for factors of the threats. Part 2 includes a set of in-depth additional questions, asking 298 supervisors/ employees from information system departments for further analysis and generating a forecasting model. Multinomial Regression, s-2Log likelihood and Wald Statistics are used for assessing the model reliability and variables' coefficients and develop the model into a predicting program. This study reveals 24 factors, of the threats and the model can significantly predict 7 factors ($p<.05$), including 1) Human mistakes 2) Intrusion 3) Threats for information 4) System or information destruction 5) Stealing 6) Attacking software and 7) Hardware technical errors. The agreement results between the model and the mentioned factors are 50.00%, 79.17%, 66.67%, 43.75%, 83.33%, 91.67% and 93.75% respectively.

Keywords: Security Threats, Risk Prediction, Threat Factors

1 Assistant Professor, Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University.

2 Students, Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University.

* Corresponding Author, Tel. 0-2908-9661, E-mail: ajagit_ag@hotmail.com

Received 7 February 2013; Accepted 25 March 2013

1. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานและการจัดการภายในองค์กรทั้งภาครัฐและเอกชน ทั้งนี้ก็เพื่อเพิ่มประสิทธิภาพการดำเนินงานและการเสริมสร้างภาพลักษณ์ที่ดีขององค์กรนั้น แต่อย่างไรก็ตามการนำเอาเทคโนโลยีสารสนเทศมาใช้ในองค์กรย่อมมีผลกระทบในด้านต่างๆ เช่น การรักษาความปลอดภัยของข้อมูล การเพิ่มระดับของการพึ่งพาต่อระบบสารสนเทศและการควบคุมภายในมีความสลับซับซ้อนมากขึ้น นอกจากนี้ยังมีผลกระทบทางด้านภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศ ซึ่งหากมีข้อผิดพลาดเกิดขึ้นอาจส่งผลกระทบที่รุนแรง และรวดเร็วขึ้นต่อการบริหารจัดการและการดำเนินงานภายในองค์กรนั้น

ภัยคุกคามความปลอดภัยของระบบสารสนเทศนั้นอาจจะเกิดได้หลายปัจจัย ทั้งภายในองค์กรและภายนอกองค์กร ปัจจัยหลักเกิดจากบางองค์กรให้ความสำคัญต่อความปลอดภัยของระบบสารสนเทศไม่ถูกที่ [1] ส่งผลทำให้มีภัยคุกคามเกิดขึ้นในระบบสารสนเทศนั้น ซึ่งจากการศึกษางานวิจัยพบว่าอัตราการเกิดภัยคุกคามนั้นมีอัตราร้อยละ 47.6 [2]

ฉะนั้นในบทความนี้จึงต้องการนำเสนอวิธีการหาปัจจัยและวิเคราะห์ภัยคุกคามทั้ง 12 ประเภท [2], [3] ได้แก่ 1) ความผิดพลาดที่มาจากบุคคลากรอาจจะเกิดจากอุบัติเหตหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา 2) การละเมิดทรัพย์สินทางปัญญาหรือการละเมิดลิขสิทธิ์ทางซอฟต์แวร์ 3) การบุกรุก 4) การกรรโชกข้อมูล 5) การทำลายระบบหรือข้อมูล 6) การโจรกรรม 7) การโจมตีจากซอฟต์แวร์ 8) ภัยธรรมชาติ 9) คุณภาพของผู้ให้บริการ 10) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ 11) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ 12) เทคโนโลยีล้าสมัย เพื่อสร้างโมเดลใช้ทำนายหรือพยากรณ์ความเสี่ยงของการเกิดภัยคุกคามที่จะเกิดขึ้นกับองค์กรในประเทศไทยได้เพื่อที่สามารถเตรียมรับมือกับภัยคุกคามที่จะเกิดขึ้น

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 การวิเคราะห์องค์ประกอบ (Factor Analysis)

การวิเคราะห์องค์ประกอบ เป็นเทคนิคการวิเคราะห์ทางสถิติของการวิจัย ที่มุ่งลดจำนวนตัวแปรที่มีอยู่มากทั้งนี้ก็ด้วยเหตุผลตัวแปรบางตัวอาจมีคุณสมบัติในการอธิบายลักษณะของข้อมูลเหมือนกัน ตัวแปรในลักษณะนี้อาจจะต้องตัดทิ้งไป หรือตัวแปรบางตัวมีลักษณะความสัมพันธ์ใกล้เคียงกันจะถูกรวมเข้ากลุ่มกันเป็นตัวแปรใหม่เรียกว่า ปัจจัย (Factor) การรวมกลุ่มของตัวแปรจะจัดเป็นกลุ่มหรือกี่ปัจจัย การวิเคราะห์จะดูที่ค่าความสัมพันธ์กัน ซึ่งอาจจะสัมพันธ์กันในทางบวกหรือทางลบก็ได้ [1] จำนวนองค์ประกอบที่ได้จะพิจารณาจากค่าของไอเกน (Eigen Value) ซึ่งค่าไอเกนจะมีค่าเท่ากับจำนวนตัวแปรในองค์ประกอบนั่นสามารถคำนวณได้จาก Eigen Value = $\sum(w)^2$ โดยที่ w คือน้ำหนักของตัวแปรในองค์ประกอบนั้นและองค์ประกอบใหม่ที่ได้จะนำค่า Factor Score ไปใช้ซึ่งคำนวณได้จาก

$$Fik = W_{i1}Z_{1k} + W_{i2}Z_{2k} + \ldots + W_{ip}Z_{pk} \quad (1)$$

โดยที่

K คือ 1, 2,…., n และ i คือ 1, 2,…, m

Z_{jk} คือค่าปัจจัยที่ j ของ Case ที่ k

n คือจำนวนข้อมูล

m คือจำนวน Factor

W_{ik} คือค่าสัมประสิทธิ์ หรือ Loading Factor ของตัวแปรที่ k ใน Factor ที่ i

F_{ik} คือ Factor Score ของ Factor ที่ i ของ Case ที่ k

2.2 การวิเคราะห์การถดถอยโลจิสติกแบบหลายกลุ่ม

การวิเคราะห์การถดถอยโลจิสติกเป็นการนำตัวแปรอิสระซึ่งเป็นตัวแปรที่ทำหน้าที่เป็นเหตุทำให้เกิดผลอย่างใดอย่างหนึ่งจำนวนหลายตัวแปรมาวิเคราะห์ความสัมพันธ์พร้อมกันกับตัวแปรตาม ซึ่งเป็นตัวแปรที่เป็นผลและเป็นตัวแปรเชิงกลุ่ม [4], [5] โดยมีสมการเชิงเส้นเป็น

$$Z = e^{\beta_0+\beta_1 x_1+\ldots+\beta_n x_n} \quad (2)$$

และมีสมการความน่าจะเป็น คือ

$$\text{Prob(event)} = \frac{e^{\beta_0+\beta_1 x_1+\ldots+\beta_n x_n}}{1+e^{\beta_0+\beta_1 x_1+\ldots+\beta_n x_n}} \quad (3)$$

เมื่อ

β_0 คือค่าคงที่

$\beta_1,\ldots,\beta_n$ คือค่าสัมประสิทธิ์ของตัวแปรต่าง ๆ มีทั้งหมด n ตัว

$x_1, x_2, \ldots, x_n$ คือตัวแปรอิสระมีทั้งหมด n ตัว

e คือเป็นค่าคงที่ทางคณิตศาสตร์มีค่าประมาณ 2.718

ทั้งนี้ หลักเกณฑ์ในการเลือกแบบจำลองที่เหมาะสมต้องพิจารณาโดยใช้ -2Log Likelihood และ Wald Statistics ในการในการหาค่าความเชื่อมั่นของโมเดลและค่าสัมประสิทธิ์ตามลำดับ

3. วิธีการดำเนินการวิจัย

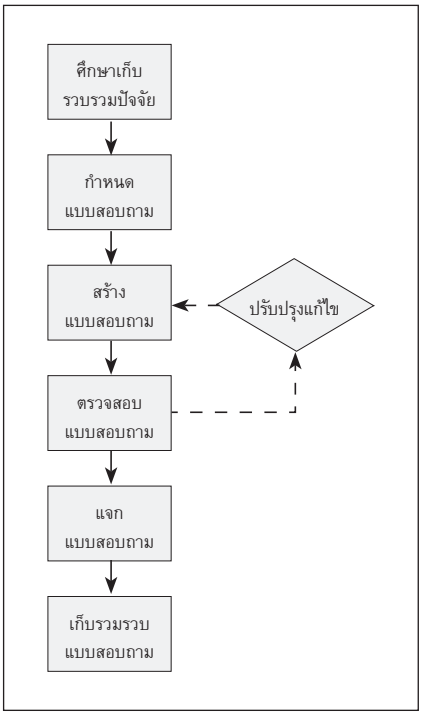
งานวิจัยนี้เป็นการเก็บรวบรวมข้อมูลเพื่อใช้สำหรับสร้างโมเดลทำนายความเสี่ยงของภัยคุกคาม ซึ่งมีวิธีการดำเนินการวิจัยแบ่งออกเป็น 3 ระยะ

3.1 ขั้นตอนสร้างแบบสอบถามเพื่อเก็บรวบรวมข้อมูล

จากรูปที่ 1 เป็นขั้นตอนสร้างแบบสอบถาม ซึ่งต้องมีการศึกษาข้อมูลที่จะใช้สร้างแบบสอบถามจากนั้นจะเป็นการกำหนดประเภทคำถามและข้อมูลของคำตอบซึ่งจะใช้ในการวิเคราะห์จากนั้นจะสร้างแบบสอบถามและจะถูกพิจารณาจากอาจารย์ที่ปรึกษาเพื่อปรับปรุงและแก้ไขก่อนทำการแจก โดยงานวิจัยนี้จะแบ่งเป็น 2 ส่วนคือ

3.1.1 ส่วนที่ 1 แบบสอบถามสำรวจความคิดเห็นของปัจจัยความเสี่ยงด้านความปลอดภัย

แบบสอบถามนี้จะลักษณะปลายปิด คือให้ผู้ตอบได้เลือกตอบในสิ่งที่คิดว่าเป็นปัจจัยของการเกิดภัยคุกคาม

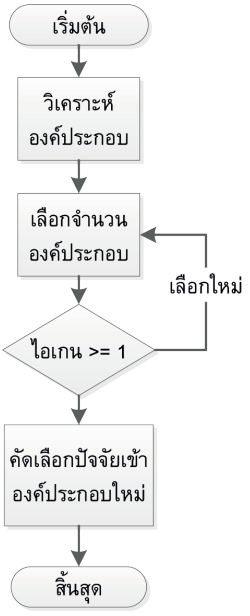


รูปที่ 1 แสดงขั้นตอนการสร้างแบบสอบถาม

กลุ่มตัวอย่างจากบุคลากรที่ทำงานเกี่ยวข้องในด้านคอมพิวเตอร์มาจำนวน 117 คน ในการตอบแบบสอบถามโดยวิธีการสำรวจจะเป็นการแจกแบบสอบถามโดยตรง ให้แก่บุคลากรของแต่ละองค์กรเพื่อสำรวจความคิดเห็นและหาปัจจัยของการเกิดความเสี่ยงทางด้านความปลอดภัยของระบบสารสนเทศ

3.1.2 ส่วนที่ 2 แบบสอบถามเชิงลึก

การออกแบบสอบถามจะใช้ข้อมูลในสอบถามส่วนที่ 1 เพื่อใช้เป็นข้อมูลในสร้างแบบสอบถามเชิงลึกเพื่อใช้ในการวิเคราะห์ โดยออกแบบให้มีการประเมินการเกิดภัยคุกคามเป็น 5 ระดับดังแสดงในตารางที่ 1 โดยมีกลุ่มตัวอย่างเป็นองค์กรที่มีแผนกเกี่ยวข้องกับระบบสารสนเทศจำนวน 298 ชุด โดยผู้ตอบแบบสอบถามจะเป็นผู้ที่เกี่ยวข้องหรือมีความรู้ด้านสารสนเทศโดยวิธีการสอบถามจะทำการแจกแบบสอบถามโดยตรงไปรษณีย์และทางอินเทอร์เน็ต



รูปที่ 2 ขั้นตอนการวิเคราะห์องค์ประกอบ

ตารางที่ 1 ระดับอัตราการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์

ระดับ	โอกาสเกิด	จำนวนครั้ง/เดือน
1	น้อยที่สุด	0 - 4
2	น้อย	ระหว่าง 5 - 11
3	ปานกลาง	ระหว่าง 12 - 18
4	เกิดมาก	ระหว่าง 19 - 25
5	มากที่สุด	มากกว่า 26

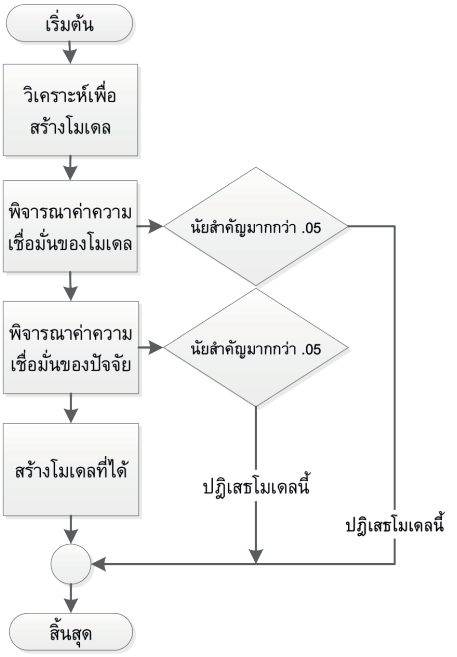
3.2 การวิเคราะห์เพื่อสร้างโมเดล

จากข้อมูลที่ได้จากแบบสอบถามส่วนที่ 2 แบ่งออกเป็น 2 ส่วน คือ ส่วนแรกแบ่งสำหรับการสร้างโมเดล 80% และส่วนที่สองแบ่งสำหรับการทดสอบ 20% จากนั้นจะนำส่วนแรกไปทำการวิเคราะห์เพื่อสร้างโมเดล โดยขั้นตอนการวิเคราะห์จะแบ่งออกเป็น 2 ขั้นตอน คือ

3.2.1 วิเคราะห์องค์ประกอบ

การวิเคราะห์องค์ประกอบนี้เนื่องจากข้อมูลที่ใช้ในการวิเคราะห์นี้เป็นข้อมูลเชิงกลุ่ม (Categorical Data) จึงเลือกใช้วิธีการวิเคราะห์ Polychoric Correlation [6], [7] โดยใช้โปรแกรม R เป็นเครื่องมือช่วยในการวิเคราะห์ ขั้นตอนการวิเคราะห์องค์ประกอบ จะแสดงดังรูปที่ 2

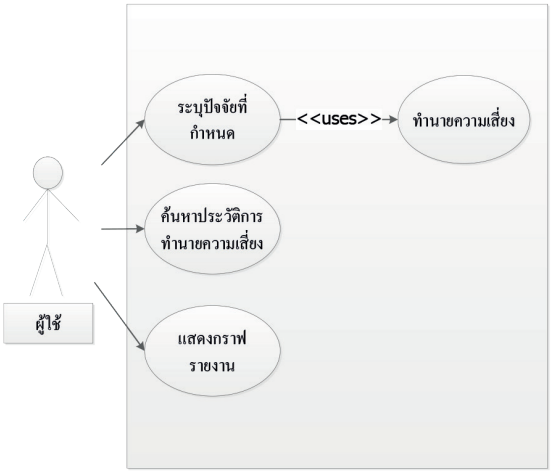
เมื่อเข้าสู่กระบวนการวิเคราะห์องค์ประกอบแล้ว จะทำการหาค่าไอเกนเพื่อเลือกจำนวนองค์ประกอบ โดยองค์ประกอบที่เลือกจะต้องมีค่าไอเกนที่มากกว่าหรือเท่ากับ 1 เมื่อเลือกจำนวนองค์ประกอบที่ได้แล้ว จะทำการคัดเลือกปัจจัยเข้าสู่องค์ประกอบใหม่ ทั้งนี้จะพิจารณาจากค่าน้ำหนักของปัจจัยที่ลู่เข้าสู่ 1 หรือ -1 ซึ่งจากการวิเคราะห์สามารถสร้างองค์ประกอบใหม่โดยองค์ประกอบใหม่ที่ได้จะนำไปใช้ในการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงต่อไป



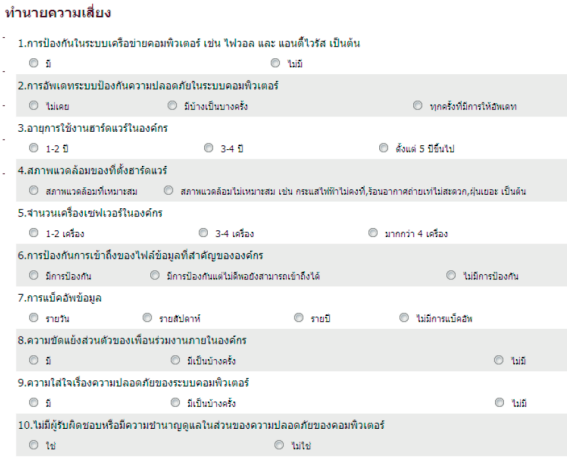
รูปที่ 3 ขั้นตอนการวิเคราะห์เพื่อสร้างโมเดล

3. 2. 2 วิเคราะห์เพื่อสร้างโมเดล

นำข้อมูลองค์ประกอบใหม่ที่ได้มาทำการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามทั้ง 12 ประเภท ขั้นตอนการวิเคราะห์จะได้ดังรูปที่ 3



รูปที่ 4 Use Case Diagram ของระบบ



รูปที่ 5 หน้าจอระบุปัจจัยเพื่อทำนายความเสี่ยง

โดยจะใช้การวิเคราะห์แบบการถดถอยโลจิสติกแบบหลายกลุ่ม (Multinomial Logistic Regression) เพื่อสร้างโมเดลทำนายความเสี่ยงโดยใช้โปรแกรม SPSS เป็นเครื่องมือช่วยในการวิเคราะห์ และมีนัยสำคัญอยู่ที่ 0.05 โดยโมเดลที่ได้จะถูกพิจารณา 2 ส่วน คือ ส่วนที่ 1 พิจารณาในส่วนของโมเดล โดยพิจารณาจากค่านัยสำคัญของโมเดลที่ได้จาก Likelihood Ratio Test ส่วนที่ 2 พิจารณาในส่วนของปัจจัยในแต่ละตัวโดยพิจารณาจากค่านัยสำคัญที่ได้จาก Walds Statistic ซึ่งหากมีค่านัยสำคัญเกินกว่าที่กำหนดจะปฏิเสธโมเดลหรือปัจจัยในโดยจะสรุปได้ว่าโมเดลหรือปัจจัยที่ถูกปฏิเสธนั้นไม่มีความสอดคล้องทำให้เกิดภัยคุกคาม

3.3 สร้างระบบเพื่อช่วยในการทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของสารสนเทศ

จากการศึกษาและวิเคราะห์ข้อมูลทำให้ทราบถึงขั้นตอนการทำงานของระบบ ข้อมูลที่จะนำเข้าระบบ บุคคลที่เกี่ยวข้องกับระบบ จึงได้ใช้แผนภาพ UML (Unified Modeling Language) แสดงให้เห็นภาพขั้นตอนการทำงานของระบบจะแสดงดังรูปที่ 4

จากรูปที่ 4 จะแบ่งการทำงานออกเป็น 3 ฟังก์ชัน คือ

1) การคำนวณเพื่อการทำนายความเสี่ยง โดยนำค่าจากปัจจัยที่ระบุจากผู้ใช้ คำนวณกับโมเดลที่ได้และแสดงระดับโอกาสเกิดความเสี่ยงของภัยคุกคามนั่น

2) แสดงรายงานประวัติการใช้การคำนวณความเสี่ยงย้อนหลังของแต่ละครั้ง

3) แสดงรายงานเปรียบเทียบในรูปแบบของกราฟ

ในการพัฒนาระบบช่วยคำนวณการทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้จะพัฒนาเป็น Web Application ซึ่งมีข้อมูลเครื่องมือในการพัฒนาระบบดังแสดงในตารางที่ 2

ตารางที่ 2 ข้อมูลเครื่องมือในการพัฒนาระบบ

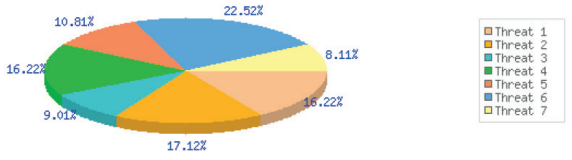
ระบบ OS	Window XP
ภาษา	PHP 5.2.6
เซิร์ฟเวอร์	Apache 2.2.8
ฐานข้อมูล	MySQL 5.0.51b

ในการใช้งานระบบทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้ ได้มีการออกแบบหน้าจอการใช้งานของระบบ ซึ่งจะขอนำเสนอเป็นเพียงบางส่วนโดยตัวอย่างหน้าจอการใช้งานของระบบ จะแสดงดังรูปที่ 5-7

ตารางผลการทำนาย

ประเภทภัยคุกคาม	โอกาสเกิดความเสี่ยง ระดับ	ความน่าจะเป็น
ความผิดพลาดที่มาจากบุคคลากรอาจจะเกิดจากอุบัติเหตหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา	น้อยที่สุด	0.32
	น้อย	0.00
	ปานกลาง	0.02
	มาก	0.66
	มากที่สุด	0.00
การบุกรุก	น้อยที่สุด	0.00
	น้อย	0.89
	ปานกลาง	0.03
	มาก	0.00
	มากที่สุด	0.08
การกรรโชกข้อมูล	น้อยที่สุด	0.00
	น้อย	0.25
	ปานกลาง	0.75
การทำลายระบบหรือข้อมูล	น้อยที่สุด	0.00
	น้อย	0.20
	ปานกลาง	0.00
	มาก	0.00
	มากที่สุด	0.80
การโจรกรรม	น้อยที่สุด	0.02
	น้อย	0.06
	ปานกลาง	0.92
การโจมตีจากซอฟต์แวร์	น้อยที่สุด	0.03
	น้อย	0.02
	ปานกลาง	0.32
	มาก	0.62
	มากที่สุด	0.00
ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์	น้อยที่สุด	0.98
	น้อย	0.01
	ปานกลาง	0.01

รูปที่ 6 หน้าจอแสดงผลการทำนายความเสี่ยง



รูปที่ 7 ตัวอย่างกราฟเปรียบเทียบผลการทำนาย

จากรูปที่ 5 เป็นตัวอย่างหน้าจอที่ผู้ใช้ต้องทำการระบุปัจจัยที่ระบบกำหนดให้ครบซึ่งมีทั้งหมด 24 ปัจจัย

รูปที่ 6 หน้าจอแสดงผลการทำนายความเสี่ยงซึ่งจะบอกเป็นระดับการเกิดของภัยคุกคามแต่ละประเภทโดยจะพิจารณากับเฉพาะระดับที่มีโอกาสเกิดมากสุด

รูปที่ 7 กราฟรายงานเปรียบเทียบการเกิดภัยคุกคามทั้งหมดในแต่ละประเภทโดยแต่ละสีจะเป็นตัวบอกถึงประเภทของภัยคุกคาม

4. ผลการทดลอง

ส่วนนี้จะเป็นการแสดงถึงผลการทดลองของงานวิจัยซึ่งแบ่งได้ดังนี้

4.1 ผลการสำรวจปัจจัย

ผลการสำรวจปัจจัยที่ได้จากการศึกษาและตอบแบบสอบถามนั้นมีจำนวนปัจจัยทั้งหมด 24 ปัจจัยดังนี้

1. การป้องกันในระบบเครือข่าย (V1)
2. การอัพเดทระบบป้องกัน (V2)
3. อายุการใช้งานฮาร์ดแวร์ (V3)
4. สภาพแวดล้อมของฮาร์ดแวร์ (V4)
5. จำนวนเครื่องเซฟเวอร์ (V5)
6. การป้องกันการเข้าถึงไฟล์ข้อมูล (V6)
7. การแบ็คอัพข้อมูล (V7)
8. ความขัดแย้งภายในองค์กร (V8)
9. ความใส่ใจความปลอดภัย (V9)
10. ขาดผู้เชี่ยวชาญ (V10)
11. การตั้งรหัสคอมพิวเตอร์ (V11)
12. การใช้คอมพิวเตอร์ร่วมกัน (V12)
13. มีการเปิดเผยรหัสผ่าน (V13)
14. เก็บรักษารหัสไม่ดีพอ (V14)
15. สั่งงานผ่านอีเมลล์ส่วนตัว (V15)
16. การอบรมความปลอดภัย (V16)
17. อายุขององค์กร (V17)
18. นโยบายความปลอดภัย (V18)
19. บทลงโทษ (V19)
20. การแบ่งหน้าที่การทำงาน (V20)
21. งบประมาณ (V21)
22. ขาดการสนุบสนุน (V22)
23. การใช้เอาท์ซอส (V23)
24. ระบบที่ใช้บริการไม่มีคุณภาพ เช่น ไฟฟ้า อินเทอร์เน็ต (V24)

จากปัจจัยทั้ง 24 ปัจจัย จะนำเข้าสู่กระบวนการวิเคราะห์องค์ประกอบเพื่อนำไปใช้ในการวิเคราะห์ เพื่อสร้างโมเดลทำนายความเสี่ยงต่อไป

4.2 ผลการวิเคราะห์องค์ประกอบ

จากการพิจารณาจากค่าไอเกนที่ได้สามารถสร้างองค์ประกอบใหม่ได้ 5 องค์ประกอบ และผลการพิจารณาค่าน้ำหนักของปัจจัยแต่ละตัว ซึ่งจะสรุปผลการรวมปัจจัยแสดงดังตารางที่ 3

ตารางที่ 3 ตารางสรุปการจัดองค์ประกอบใหม่

องค์ประกอบ	ปัจจัย
F1	V1, V4, V5, V6, V8, V12, V14, V15, V16, V18, V19, V24
F2	V2, V3, V20, V21, V23
F3	V7, V17
F4	V9, V10, V22
F5	V11, V13

จากหัวข้อ 2.1 สามารถนำค่าน้ำหนักของปัจจัยที่อยู่ในองค์ประกอบนั้นมาหาค่าขององค์ประกอบ ซึ่งจะมีสมการดังนี้

$$F1 = (.74)V1 + (.94)V4 + (-.88)V5 + (.78)V6 + (-.76)V8 + (-.70)V12 + (-.82)V14 + (.89)V15 + (.81)V16 + (.74)V18 + (.80)V19 + (-.90)V24 \quad (4)$$

$$F2 = (.72)V2 + (-.51)V3 + (.60)V20 + (.77)V21 + (.79)V23 \quad (5)$$

$$F3 = (.63)V7 + (-.72)V17 \quad (6)$$

$$F4 = (.52)V9 + (-.66)V10 + (-.49)V22 \quad (7)$$

$$F5 = (.77)V11 + (-.67)V13 \quad (8)$$

โดยที่ V1-V24 เป็นปัจจัยที่ได้จากการสำรวจและ F1-F5 เป็นองค์ประกอบใหม่ที่ได้จากการวิเคราะห์

4.3 ผลการวิเคราะห์เพื่อสร้างโมเดล

ผลการวิเคราะห์พบว่าจากภัยคุกคามทั้งหมด 12 ประเภท ที่นำมาวิเคราะห์กับข้อมูลปัจจัยทั้ง 24 ปัจจัย มีโมเดลที่สอดคล้องกับการเกิดภัยคุกคามทั้งหมด 7 ประเภท ได้แก่

1) ข้อผิดพลาดจากการกระทำของมนุษย์

$$Z1 = 13.60 + (-.36)F1 + (-1.37)F2 + (-.26)F3 \quad (9)$$

$$Z2 = 6.42 + (-.55)F1 + (-1.46)F2 + (1.04)F3 \quad (10)$$

$$Z3 = 6.46 + (-.24)F\ 1 + (-.80)F2 + (.32)F3 \quad (11)$$

$$Z4 = 9.94 + (-.28)F1 + (-.73) \quad (12)$$

$$Z5 = 0 \quad (13)$$

2) การบุกรุก

$$Z1 = 34.10 + (.34)F1 + (-3.57)F2 + (-11.14)F4 \quad (14)$$

$$Z2 = 36.00 + (.26)F1 + (-3.51)F2 + (-10.13)F4 \quad (15)$$

$$Z3 = 30.81 + (-.08)F1 + (-3.17)F2 + (-8.76)F4 \quad (16)$$

$$Z4 = 4.38 + (-.56)F1 + (-.43)F2 + (.30)F4 \quad (17)$$

$$Z5 = 0 \quad (18)$$

3) การกรรโชกข้อมูลสารสนเทศ

$$Z1 = 33.93 + (-6.69)F2 + (3.92)F3 + (6.01)F4 + (7.13)F5 \quad (19)$$

$$Z2 = 32.93 + (-6.72)F2 + (4.01)F3 + (6.04)F4 + (6.90)F5 \quad (20)$$

$$Z3 = 30.81 + (-.08)F1 + (-3.17)F2 + (-8.76)F4 \quad (21)$$

$$Z4 = 0 \quad (22)$$

4) การก่อวินาศกรรมหรือการทำลาย

$$Z1 = 16.61 + (.27)F1 + (1.09)F2 + (-5.10)F3 + (2.66)F4 \quad (23)$$

$$Z2 = 13.02 + (.25)F1 + (1.39)F2 + (-4.36)F3 + (2.56)F4 \quad (24)$$

$$Z3 = .47 + (.11)F1 + (1.33)F2 + (-2.39)F3 + (1.56)F4 \quad (25)$$

$$Z4 = 4.01 + (-.00)F1 + (.25)F2 + (-1.02)F3 + (.57)F4 \quad (26)$$

$$Z5 = 0 \quad (27)$$

5) การโจรกรรม

$$Z1 = 4.73 + (-.58)F1 + (-2.81)F4 \quad (28)$$

$$Z2 = 1.37 + (.17)F1 + (-1.24)F4 \quad (29)$$

$$Z3 = 0 \quad (30)$$

6) การโจมตีซอฟต์แวร์

$$Z1 = 36.91 + (.93)F1 + (-6.43)F2 + (2.64)F3 + (-11.62)F4 + (7.29)F5 \quad (31)$$

$$Z2 = 37.58 + (1.01)\ F1 + (-6.69)F2 + (2.78)F3 +$$

(-11.73)F4 + (7.59)F5 (32)

Z3 = 34.39 + (.29)F1 + (-5.25)F2+ (1.97)F3 + (-8.47)F4 + (5.02)F5 (33)

Z4 = 20.26 + (-.43)F1 + (-1.37)F2+ (-.63)F3 + (-1.70)F4 + (-4.83)F5 (34)

Z5 = 0 (35)

7) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์

Z1 = 4.42 + (-.79)F1+ (5.57)F5 (36)

Z2 = -.01 + (-.16)F1+ (4.00)F5 (37)

Z3 = 0 (38)

จากโมเดลของภัยคุกคามในแต่ละประเภทจากหัวข้อที่ 2.2 สามารถนำไปคำนวณเพื่อหาระดับการเกิดของภัยคุกคามในแต่ละประเภทได้ ซึ่งผลการทดสอบระหว่างโมเดลทั้ง 7 กับข้อมูลทดสอบที่แบ่งไว้ในหัวข้อที่ 3.2 จำนวน 48 ข้อมูล พบว่าโมเดลมีความสอดคล้องกับการเกิดภัยคุกคาม โดยคิดเป็นร้อยละได้ดังแสดงในตารางที่ 4

ตารางที่ 4 ตารางแสดงผลการทดสอบโมเดล

โมเดลที่ใช้ทดสอบ	ความสอดคล้อง
ความผิดพลาดที่มาจากบุคคลากร (T1)	50.00
การบุกรุก (T2)	79.17
การกรรโชกข้อมูล (T3)	66.67
การทำลายระบบ (T4)	43.75
การโจรกรรม (T5)	83.33
การโจมตีจากซอฟต์แวร์ (T6)	91.67
ข้อผิดพลาดทางฮาร์ดแวร์ (T7)	93.75

จากตารางที่ 4 จะเห็นได้ว่าผลการทดสอบความสอดคล้องของข้อมูลกับโมเดลส่วนใหญ่มีความสอดคล้องมากกว่าร้อยละ 50 ซึ่งถือว่ามีความสอดคล้องที่ดีระดับหนึ่ง ซึ่งองค์กรสามารถนำโมเดลนี้ไปประยุกต์ใช้กับภายในองค์กรของตัวเองได้

5. สรุป

งานวิจัยนี้เป็นการหาปัจจัยและสร้างโมเดลสำหรับทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศ โดยใช้วิธีการเก็บข้อมูลจากแบบสอบถาม ซึ่งสามารถหาปัจจัยทั้งหมด 24 ปัจจัย แล้วมาทำการวิเคราะห์เพื่อจะรวมปัจจัยที่มีลักษณะซ้ำกันให้อยู่ในกลุ่มเดียวกันซึ่งจะใช้วิธีการวิเคราะห์องค์ประกอบจากนั้นจะนำองค์ประกอบใหม่ที่ได้มาทำการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงกับภัยคุกคามทั้ง 12 ประเภท ในการวิเคราะห์จะใช้วิธีการวิเคราะห์ถดถอยโลจิสติกแบบหลายกลุ่ม ซึ่งผลการวิจัยพบว่าสามารถสร้างโมเดลที่สอดคล้องกับการทำนายความเสี่ยงของการเกิดภัยคุกคามได้ทั้งหมด 7 ประเภท จากทั้งหมด 12 ประเภท ซึ่งผู้วิจัยได้สรุปสาเหตุของการได้โมเดลไม่ครบทั้ง 12 ประเภท โดยแบ่งเป็น 2 อย่าง คือ 1) ข้อมูลที่ใช้ทดสอบไม่เพียงพอในการใช้ทดสอบ 2) ปัจจัยที่มีไม่ครอบคลุม ทำให้โมเดลที่ได้มีประสิทธิภาพไม่เพียงพอ งานวิจัยนี้ต่อยอดได้โดยอาจจะเลือก วิเคราะห์ภัยคุกคามใดภัยคุกคามหนึ่ง เพื่อที่จะศึกษาภัยคุกคามนั้นอย่างครอบคลุม

เอกสารอ้างอิง

[1] C. Colwill, “Human factors in information security: The insider threat - Who can you trust these days?,” information security technical report, 2010.

[2] Michael E.Whitman, “In defense of the realm: understanding the threats to information security,” *International Journal of Information Management*, 2004.

[3] Michael E. Whiteman and Herbert J. Mattord, *Principles of Information Security*, Course Technology, 2003.

[4] Kanlaya Vanichbuncha, *Data Analysis By SPSS for Window*, Bangkok: Thammasan Company, 2548.

[5] Thavatchai Worrapongsaton, *Technique of Multiple Logistic Regression Analysis*, 2533.

[6] Andy Field, Factor Analysis for Likert/ Ordinal/ Non-normalData. [Online]. Available: http:// www.me thodspace.com/profiles/blogs/ factor-analysis-for-likert-ordinal-non-normal-data

[7] Ng. Serena, "CONSTRUCTING COMMON FACTORS FROM CONTINUOUS AND CATEGORICAL DATA," *Jel Classification Journals*, 2012.