การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในประเทศไทย

นายอัจกิต อุฒาธรรม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

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

Mr. Ajagit Utatham

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Enigneering

Faculty of Engineering

Chulalongkorn University

Academic Year 2012

หัวข้อวิทยานิพนธ์	การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในประเทศไทย
โดย	นาย อัจกิต อุฒาธรรม
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ธนาวรรณ จันทรัตนไพบูลย์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

…….. คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร. บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

…… ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. สืบสกุล พิภพมงคล)

…….. อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ธนาวรรณ จันทรัตนไพบูลย์)

…… กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ธนารัตน์ ชลิดาพงศ์)

…… กรรมการภายนอกมหาวิทยาลัย
(ดร. นล เปรมัษเสียร)

อัจกิต อุฒมาธรรม: การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในประเทศไทย (THE FACTOR ANALYSIS AND MODELING FOR RISK PREDICTION OF INFORMATION SECURITY THREATS IN THAILAND) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ธนาวรรณ จันทรัตนไพบูลย์, 109 หน้า.

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อต้องการศึกษาหาปัจจัยที่ทำให้เกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ และสร้างโมเดลเพื่อใช้ทำนายความเสี่ยงของภัยคุกคาม โดยใช้วิธีการออกแบบสอบถาม ซึ่งจะแบ่งเป็น 2 ส่วนคือ 1) แบบสอบถามสำรวจหาปัจจัยโดยมีกลุ่มตัวอย่างเป็นบุคลากรในองค์กรที่เกี่ยวข้อง ในด้านระบบสารสนเทศจำนวน 117 คน 2) แบบสอบถามเชิงลึก โดยใช้ข้อมูลจากแบบสอบถามส่วนแรกมาเป็นข้อมูลในการออกแบบสอบถามเพื่อใช้ใน การวิเคราะห์ โดยมีกลุ่มตัวอย่างเป็นหัวหน้าหรือตัวแทนแผนกที่เกี่ยวข้องกับระบบสารสนเทศ จำนวน 298 ชุด เพื่อนำไปวิเคราะห์สร้างโมเดล โดยใช้ Multinomial Regression และใช้ s-2Log likelihood และ Wald Statistics ในการหาค่าความเชื่อมั่นของโมเดลและสัมประสิทธิ์ตามลำดับและพัฒนาเป็น โปรแกรมเพื่อช่วยทำนาย ผลวิจัยพบว่าจากการศึกษาและสำรวจปัจจัยได้ปัจจัยทั้งหมด 24 ปัจจัยและ จากการวิเคราะห์ได้โมเดลที่สามารถทำนายการเกิดภัยคุกคาม 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

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2555

##5271471121: MAJOR COMPUTER SCIENCE
KEYWORD: SECURITY THREATS, RISK PREDICTION

AJAGIT UTATHAM: THE FACTOR ANALYSIS AND MODELING FOR RISK PREDICTION OF INFORMATION SECURITY THREATS IN THAILAND. ADVISOR: ASST. PROF. THANAWAN CHANTARATANAPIBUL, 109 pp.

The purposes of this study are to find factors causing information security threat and to build a model to predict risks of the threats by using questionnaires which consist of 2 parts: 1) the questionnaire which has 117 officers from information system organizations as samples searches for factors of the threats 2) In-depth questionnaire which has 298 samples of leaders or representations from information system departments uses information from the first questionnaire to be designed to analysis and build a model. Multinomial Regression, s-2Log likelihood and Wald Statistics are used to find out the model's reliability and the variables' coefficients and develop the model into a predicting program. This study shows that there are 24 factors of the threats and the model can predict 7 factors which are 1) Human mistakes 2) Intrusion 3) Threats for information.4) System or information destruction 5) Stealing 6) Attacking software 7) Hardware technical errors. With reliability as 0.05, the results from relation experiment between the model and the mentioned factors are 50.00%, 79.17%, 66.67%, 43.75%, 83.33%, 91.67% and 93.75%, respectively.

Department : Computer Engineering Student's Signature .....
Field of Study : Computer Science Advisor's Signature .....
Academic Year : 2012

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ ผศ.ธนาวรรณ จันทรัตนไพบูลย์ อาจารย์ที่ปรึกษา ที่คอยให้คำแนะนำและคำปรึกษาตลอดจนแก้ไขข้อบกพร่องในการทำวิทยานิพนธ์

ขอกราบขอบพระคุณ ผศ.ดร. แสงหล้า ชัยมงคล ภาควิชาคณิตศาสตร์และสถิติ มหาวิทยาลัยธรรมศาสตร์ ที่ช่วยเหลือให้คำแนะนำในเรื่องสถิติ

ท้ายที่สุดนี้ผู้วิจัยขอกราบขอบพระคุณ นางดวงเดือน ภิรมย์ทอง มารดาของข้าพเจ้าซึ่งคอยให้กำลังใจตลอดมา

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง ..... ญ

สารบัญรูป ..... ฏ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาของปัญหา 1

1.2 วัตถุประสงค์ 4

1.3 ขอบเขตการดำเนินงาน 4

1.4 ขั้นตอนดำเนินการ 5

1.5 ประโยชน์ที่คาดว่าจะได้รับ 5

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 6

2.1 ส่วนที่ 1 ข้อมูลและทฤษฎีที่เกี่ยวข้องกับภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์ 6

2.2 ส่วนที่ 2 ทฤษฎีที่ใช้ในการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงของภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์ 10

บทที่ 3 การเก็บรวบรวมข้อมูล 16

3.1 ส่วนที่ 1 การออกแบบสอบถามสำรวจความคิดเห็นของปัจจัยความเสี่ยงคอมพิวเตอร์ด้านความปลอดภัย 17

หน้า

3.2 ส่วนที่ 2 การออกแบบสอบถามเชิงลึก 18
บทที่ 4 การวิเคราะห์ข้อมูล 20
4.1 การวิเคราะห์องค์ประกอบ 20
4.2 การวิเคราะห์เพื่อสร้างโมเดล 24
บทที่ 5 การพัฒนาระบบ 55
5.1 การวิเคราะห์ระบบ 55
5.2 การออกแบบระบบทำนายความเสี่ยง 55
5.3 การออกแบบกระบวนการทำงานของระบบ 58
5.4 การออกแบบโครงสร้างส่วนประสาน 59
5.5 การออกแบบไดอะแกรม 60
5.6 การออกแบบการนำทาง 66
5.7 การออกแบบการจัดเก็บฐานข้อมูลและโครงสร้างของข้อมูล 69
5.8 การพัฒนาระบบ 74
บทที่ 6 ผลการทดสอบ 76
6.1 ข้อมูลการทดสอบ 76
6.2 สภาพแวดล้อมในการทดสอบระบบ 76
6.3 สรุปผลการทดสอบระบบ 76
บทที่ 7 สรุปผลการวิจัยและข้อเสนอแนะ 80
7.1 สรุปผลการวิจัย 80
7.2 ปัญหาและอุปสรรคในการวิจัย 81

หน้า

7.3 ข้อเสนอแนะ 82
รายการอ้างอิง 83
ภาคผนวก 84
ภาคผนวก ก แบบสอบถาม 85
ภาคผนวก ข ผลสรุปการตอบแบบสอบถาม 94
ภาคผนวก ค ผลการวิเคราะห์ข้อมูล 99
ภาคผนวก ง หน้าจอผู้ใช้งานระบบ 102
ประวัติผู้เขียนวิทยานิพนธ์ 109

สารบัญตาราง

หน้า

ตารางที่ 1.1 จำนวนช่วงของการเกิดภัยคุกคามต่อเดือนโดยคิดเป็นร้อยละ..... 2
ตารางที่ 1.2 อัตราการเกิดภัยคุกคามต่อเดือนโดยคิดเป็นร้อยละ..... 2
ตารางที่ 3.1 ระดับอัตราการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์..... 18
ตารางที่ 3.2 ข้อมูลผู้ตอบแบบสอบถาม..... 19
ตารางที่ 4.1 ค่าไอเกนจากปัจจัยทั้ง 24 ปัจจัย..... 21
ตารางที่ 4.2 Factor loading ที่ได้จากการวิเคราะห์ Factor..... 22
ตารางที่ 4.3 การแยกปัจจัยกับองค์ประกอบใหม่ที่ได้..... 23
ตารางที่ 4.4 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดจากการกระทำของมนุษย์..... 49
ตารางที่ 4.5 ผลวิเคราะห์ภัยคุกคามประเภทการละเมิดทรัพย์สินทางปัญญาหรือการละเมิด
ลิขสิทธิ์ทางซอฟต์แวร์..... 50
ตารางที่ 4.6 ผลวิเคราะห์ภัยคุกคามประเภทการบุกรุก..... 50
ตารางที่ 4.7 ผลวิเคราะห์ภัยคุกคามประเภทการกรรโชกข้อมูล..... 50
ตารางที่ 4.8 ผลวิเคราะห์ภัยคุกคามประเภทการทำลายระบบหรือข้อมูล..... 51
ตารางที่ 4.9 ผลวิเคราะห์ภัยคุกคามประเภทการโจรกรรม..... 51
ตารางที่ 4.10 ผลวิเคราะห์ภัยคุกคามประเภทการโจมตีจากซอฟต์แวร์..... 52
ตารางที่ 4.11 ผลวิเคราะห์ภัยคุกคามประเภทภัยธรรมชาติ..... 52
ตารางที่ 4.12 ผลวิเคราะห์ภัยคุกคามประเภทคุณภาพของผู้ให้บริการ..... 52
ตารางที่ 4.13 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์..... 53
ตารางที่ 4.14 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดทางเทคนิคของซอฟต์แวร์..... 53
ตารางที่ 4.15 ผลวิเคราะห์ภัยคุกคามประเภทเทคโนโลยีล้าสมัย..... 54
ตารางที่ 5.1 สรุปฟังก์ชันของระบบทำนายความเสี่ยง..... 55
ตารางที่ 5.2 อธิบายยูสเคส ระบุปัจจัยที่กำหนด..... 56

หน้า

ตารางที่ 5.3 อธิบายยูสเคส ทำนายความเสี่ยง 57
ตารางที่ 5.4 อธิบายยูสเคส แสดงรายงาน..... 57
ตารางที่ 5.5 อธิบายยูสเคส กราฟรายงาน..... 58
ตารางที่ 5.6 ข้อมูลตาราง predict..... 72
ตารางที่ 5.7 ข้อมูลตาราง titles..... 72
ตารางที่ 5.8 ข้อมูลตาราง results 72
ตารางที่ 5.9 ข้อมูลตาราง users 72
ตารางที่ 5.10 ข้อมูลตาราง factor_result 73
ตารางที่ 5.11 ข้อมูลตาราง factors 74
ตารางที่ 5.12 ข้อมูลตาราง choice 74
ตารางที่ 5.13 เครื่องมือที่ใช้ในการพัฒนา 75
ตารางที่ 5.14 สภาพแวดล้อมในการพัฒนา 75
ตารางที่ 6.1 สภาพแวดล้อมในการพัฒนา 76
ตารางที่ 6.2 เปรียบเทียบผลการทดสอบโมเดลจากข้อมูล 1 ชุด..... 77
ตารางที่ 6.2 ผลการทดสอบโมเดลทำนายความเสี่ยง..... 78
ตารางที่ ข.1 แสดงผลสรุปที่ได้จากการสำรวจปัจจัยการเกิดความเสี่ยงของ
ภัยคุกคามด้านความปลอดภัยระบบคอมพิวเตอร์ 94
ตารางที่ ข.2 ข้อมูลปัจจัยที่ใช้ทดสอบทั้งหมด 48 ข้อมูล..... 95
ตารางที่ ข.3 ข้อมูลการเกิดภัยคุกคามที่ใช้ทดสอบทั้งหมด 48 ข้อมูล..... 97
ตารางที่ ค.1 ผลการวิเคราะห์ Polychoric Correlation 99
ตารางที่ ค.2 ผลการวิเคราะห์ Factor Loading 101

สารบัญรูป

หน้า

รูปที่ 3.1 ขั้นตอนการเก็บรวบรวมข้อมูลการสำรวจหาปัจจัย 16
รูปที่ 4.1 การแยกปัจจัยกับองค์ประกอบใหม่ที่ได้ 24
รูปที่ 4.2 Case Processing Summary 25
รูปที่ 4.3 Model Fitting Information 26
รูปที่ 4.4 Likelihood Ratio Tests 26
รูปที่ 4.5 Parameter Estimate 27
รูปที่ 4.6 Classification 27
รูปที่ 4.7 Case Processing Summary 28
รูปที่ 4.8 Model Fitting Information 28
รูปที่ 4.9 Case Processing Summary 29
รูปที่ 4.10 Model Fitting Information 29
รูปที่ 4.11 Likelihood Ratio Tests 29
รูปที่ 4.12 Parameter Estimate 30
รูปที่ 4.13 Classification 31
รูปที่ 4.14 Case Processing Summary 32
รูปที่ 4.15 Model Fitting Information 32
รูปที่ 4.16 Likelihood Ratio Tests 32
รูปที่ 4.17 Parameter Estimate 33
รูปที่ 4.18 Classification 34
รูปที่ 4.19 Case Processing Summary 34
รูปที่ 4.20 Model Fitting Information 35
รูปที่ 4.21 Likelihood Ratio Tests 35
รูปที่ 4.22 Parameter Estimate 36
รูปที่ 4.23 Classification 37

หน้า

รูปที่ 4.24 Case Processing Summary 37
รูปที่ 4.25 Model Fitting Information 38
รูปที่ 4.26 Likelihood Ratio Tests 38
รูปที่ 4.27 Parameter Estimate 39
รูปที่ 4.28 Classification 39
รูปที่ 4.29 Case Processing Summary 40
รูปที่ 4.30 Model Fitting Information 40
รูปที่ 4.31 Likelihood Ratio Tests 41
รูปที่ 4.32 Parameter Estimate 41
รูปที่ 4.33 Classification 42
รูปที่ 4.34 Case Processing Summary 43
รูปที่ 4.35 Model Fitting Information 43
รูปที่ 4.36 Case Processing Summary 44
รูปที่ 4.37 Model Fitting Information 44
รูปที่ 4.38 Likelihood Ratio Tests 44
รูปที่ 4.39 Case Processing Summary 45
รูปที่ 4.40 Model Fitting Information 45
รูปที่ 4.41 Likelihood Ratio Tests 46
รูปที่ 4.42 Parameter Estimate 46
รูปที่ 4.43 Classification 47
รูปที่ 4.44 Case Processing Summary 47
รูปที่ 4.45 Model Fitting Information 48
รูปที่ 4.46 Case Processing Summary 48
รูปที่ 4.47 Model Fitting Information 48

หน้า

รูปที่ 5.1 แผนภาพยูสเคสระบบทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศ 56
รูปที่ 5.2 แผนภาพการทำงานของระบบ 59
รูปที่ 5.3 แผนภาพส่วนต่อประสานงานผู้ใช้ 60
รูปที่ 5.4 Class Diagram ระบบทำนายความเสี่ยงภัยคุกคามระบบสารสนเทศ 61
รูปที่ 5.5 Sequence Diagram ของการทำนายความเสี่ยงภัยคุกคามระบบสารสนเทศ 62
รูปที่ 5.6 Sequence Diagram การแสดงประวัติการทำนาย 63
รูปที่ 5.7 Sequence Diagram การแสดงกราฟรายงานผลการทำนาย 63
รูปที่ 5.8 หน้าจอทำนายความเสี่ยง 66
รูปที่ 5.9 หน้าจอทำนายความเสี่ยง 67
รูปที่ 5.10 หน้าจอทำนายความเสี่ยง 68
รูปที่ 5.11 หน้าจอทำนายความเสี่ยง 68
รูปที่ 5.12 หน้าจอทำนายความเสี่ยง 59
รูปที่ 5.13 หน้าจอทำนายความเสี่ยง 69
รูปที่ 5.14 โครงสร้างและความสัมพันธ์ของตารางในฐานข้อมูล 71
รูปที่ 5.15 โครงสร้างและความสัมพันธ์ของตารางในฐานข้อมูล 71
รูปที่ 6.1 ตัวอย่างของการทดสอบความแม่นยำของโมเดล 77
รูปที่ ง.1 หน้าจอเข้าสู่ระบบ 102
รูปที่ ง.2 หน้าจอผู้ใช้งานในส่วนของหน้าแรก 103
รูปที่ ง.3 หน้าจอระบุปัจจัยความเสี่ยง 104
รูปที่ ง.4 หน้าจอแสดงผลการทำนาย 105
รูปที่ ง.5 หน้าจอรายการใช้งานย้อนหลังการทำนายความเสี่ยง 106
รูปที่ ง.6 หน้าจอแสดงผลการใช้งานย้อนหลังการทำนายความเสี่ยง 107
รูปที่ ง.7 หน้าจอแสดงรายงานในรูปแบบของกราฟเพื่อใช้เปรียบเทียบ 108

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานและการจัดการภายในองค์กรทั้งภาครัฐและเอกชน ทั้งนี้ก็เพื่อเพิ่มประสิทธิภาพการดำเนินงานและการเสริมสร้างภาพลักษณ์ที่ดีขององค์กรนั้น แต่อย่างไรก็ตามการนำเอาเทคโนโลยีสารสนเทศมาใช้ในองค์กรย่อมมีผลกระทบในด้านต่างๆ เช่น การรักษาความปลอดภัยของข้อมูล การเพิ่มระดับของการพึ่งพาต่อระบบสารสนเทศและการควบคุมภายในมีความสลับซับซ้อนมากขึ้น นอกจากนี้ยังมีผลกระทบทางด้านภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศ ซึ่งหากมีข้อผิดพลาดเกิดขึ้น อาจส่งผลกระทบที่รุนแรง และรวดเร็วขึ้นต่อการบริหารจัดการและการดำเนินงานภายในองค์กรนั้น

ภัยคุกคามความปลอดภัยของระบบสารสนเทศนั้น อาจเกิดขึ้นได้ทั้งภายในองค์กรและภายนอกองค์กร ผู้บริหารบางองค์กรไม่ให้ความสำคัญต่อความปลอดภัยของระบบสารสนเทศที่ใช้ภายในองค์กรเท่าที่ควร จึงทำให้เกิดความเสี่ยงที่จะเกิดภัยคุกคามแก่องค์กรเพิ่มมากขึ้น ด้วยเหตุที่มีความปลอดภัยน้อยลงจึงเป็นผลให้เกิดภัยคุกคามบ่อยขึ้นและโดนโจมตีมากขึ้น ภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศนั้นสามารถเกิดได้กับทุกองค์กรทุกหน่วยงาน ไม่ว่าองค์กรหรือหน่วยงานนั้นจะมีขนาดเล็กหรือขนาดใหญ่ ผลกำไรมากหรือผลกำไรน้อยก็ตาม ปัญหาภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศนั้นจึงเป็นปัญหาสำหรับทุกองค์กรที่มีการนำระบบสารสนเทศเข้าไปใช้ภายในองค์กร จากการศึกษารายงานเรื่อง Human factors in information security: The insider[1] นั้นจะเน้นการป้องกันภัยคุกคามความปลอดภัยจากภายนอก เช่น การป้องกันการเจาะระบบ การดักข้อมูล เป็นต้น ซึ่งไม่สามารถป้องกันภัยคุกคามนี้ได้ทั้งหมด โดยร้อยละ 70 เกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศจากบุคคลภายใน เช่น บุคลากรไม่ทำตามนโยบายความปลอดภัยขององค์กร เนื่องมาจากองค์กรนั้นไม่มีบทลงโทษอย่างจริงจัง เป็นต้น และ ร้อยละ 90 ทำการป้องกันความปลอดภัยที่เกิดจากภายนอก เช่น การสแกนอีเมลล์ที่ได้รับเข้ามา การใช้งานไฟวอลล์ รายงานนี้แสดงให้เห็นว่าการป้องกันภัยคุกคามจากภายนอกอย่างเดียวนั้นไม่เพียงพอที่จะจัดการความปลอดภัยของระบบสารสนเทศในองค์กรนั้นได้ จำเป็นต้องมีการจัดการป้องกันภัยคุกคามทั้งภายนอกและภายในองค์กร

ผู้วิจัยได้ศึกษางานวิจัยและผลสำรวจของอัตราการเกิดภัยคุกคามความปลอดภัยด้านระบบสารสนเทศทั้งในประเทศและต่างประเทศ พบว่างานวิจัยภายในประเทศได้มีการศึกษา

ข้อมูลของภัยคุกคามความปลอดภัยของคอมพิวเตอร์เฉพาะภัยคุกคามประเภทการขโมยข้อมูล (Deliberate acts of theft)[2] และทำการศึกษางานวิจัยเรื่อง In defense of the realm: understanding the threats to information security[3] ซึ่งเป็นงานวิจัยในประเทศสหรัฐอเมริกา ใช้วิธีเก็บข้อมูลจากการตอบแบบสอบถามของผู้บริหารฝ่ายระบบสารสนเทศขององค์กร พบว่า อัตราการเกิดภัยคุกคามความปลอดภัยด้านระบบสารสนเทศนั้น มีอัตราการเกิดที่สูงโดยอัตราการเกิดภัยคุกคามนั้นคิดเป็นร้อยละ (Yes%) 47.6 ส่วนอัตราที่ไม่ได้เกิดนั้นคิดเป็นร้อยละ(No%) 50.9 และส่วนที่เหลือ (No answer%) 1.5 คือไม่ได้ตอบแบบสอบถาม จากงานวิจัยนี้แสดงให้เห็นว่ามีอัตราการเกิดภัยคุกคามและไม่เกิดภัยคุกคาม ที่ใกล้เคียงกัน ดังแสดงในตาราง ที่ 1.1

ตารางที่ 1.1 จำนวนช่วงของการเกิดภัยคุกคามต่อเดือนโดยคิดเป็นร้อยละ

Number of attacks per month	None (%)	< 10 (%)	10–50 (%)	51–100 (%)	> 100 (%)	No answer (%)
1. Act of human error or failure	24.0	41.7	14.6	2.1	5.2	12.5
2. Compromises to intellectual property	61.5	25.0	3.1	2.1	1.0	7.3
3. Deliberate acts of espionage or trespass	68.8	20.8	3.1	3.1	4.2	
4. Deliberate acts of information extortion	90.6	8.3	1.0			
5. Deliberate acts of sabotage or vandalism	64.6	31.3	3.1		1.0	
6. Deliberate acts of theft	54.2	38.5	7.3			
7. Deliberate software attacks	16.7	47.9	14.6	9.4	11.5	
8. Forces of nature	62.5	34.4	2.1		1.0	
9. Quality of service deviations from service providers	46.9	43.8	8.3	1.0		
10. Technical hardware failures or errors	34.4	51.0	11.5	3.1		
11. Technical software failures or errors	30.2	45.8	18.8	5.2		
12. Technological obsolescence	60.4	21.9	15.6	1.0		1.0
Average responses	50.9	35.4	8.3	2.1	1.8	1.5

เพื่อการเปรียบเทียบให้เห็นถึงภาพรวมทั้งหมดของอัตราการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศที่แสดงดังตารางข้างต้นในแต่ละประเภท ผู้วิจัยจึงได้นำข้อมูลจากตารางที่ 1.1 มาจัดเรียงใหม่ดังแสดงในตารางที่ 1.2

ตารางที่ 1.2 อัตราการเกิดภัยคุกคามต่อเดือนโดยคิดเป็นร้อยละ

Percentage of attacks per month	No(%)	Yes(%)	No Answer(%)
1. Act of human error or failure	24.0%	63.6%	12.5%
2. Compromises to intellectual property	61.5%	31.2%	7.3%
3. Deliberate acts of espionage or trespass	68.8%	31.2%	
4. Deliberate acts of information extortion	90.6%	9.4%	
5. Deliberate acts of sabotage or vandalism	64.6%	35.4%	

ตารางที่ 1.2 อัตราการเกิดภัยคุกคามต่อเดือนโดยคิดเป็นร้อยละ (ต่อ)

6. Deliberate acts of theft	54.2%	45.8%	
7. Deliberate software attacks	16.7%	83.3%	
8. Forces of nature	62.5%	37.5%	
9. Quality of service deviations from service providers	46.9%	53.1%	
10. Technical hardware failures or errors	34.4%	65.6%	
11. Technical software failures or errors	30.2%	69.8%	
12. Technological obsolescence	60.4%	38.6%	1.0%
Average responses	50.9%	47.6%	1.5%

(No %) หมายถึง อัตราที่ไม่มีการเกิดภัยคุกคามโดยคิดเป็นร้อยละจากผลสำรวจทั้งหมด
(Yes %) หมายถึง อัตราการเกิดภัยคุกคามโดยคิดเป็นร้อยละจากผลสำรวจทั้งหมด
(No answer %) หมายถึง อัตราที่ไม่ตอบแบบสอบถามโดยคิดเป็นร้อยละจากผลสำรวจทั้งหมด

จากตัวเลขเฉลี่ยในตารางที่ 1.2 นี้แสดงให้เห็นว่าเกือบร้อยละ 50 ของแบบสอบถามมีองค์กรที่ประสบกับปัญหาภัยคุกคามความปลอดภัยของระบบสารสนเทศในรูปแบบต่างๆ และจากการศึกษาผลการสำรวจของ CSI Computer Crime & Security Survey ซึ่งเป็นการศึกษาเกี่ยวกับอาชญากรรมความปลอดภัยคอมพิวเตอร์ซึ่งเป็นภัยคุกคามอย่างหนึ่ง พบว่าองค์กรที่มีการเกิดอาชญากรรมความปลอดภัยคอมพิวเตอร์มากที่สุดคือ องค์กรที่เกี่ยวข้องกับการเงิน[4] ซึ่งปัจจุบันการจัดการความเสี่ยงที่ใช้กันอยู่นั้นจะใช้รูปแบบของตารางการวิเคราะห์ โดยมีโอกาสที่จะเกิดภัยคุกคามและระดับความรุนแรงมาเป็นตัวประเมินความเสี่ยงซึ่งต้องใช้ข้อมูลสถิติของการเกิดภัยคุกคามก่อนหน้านี้ ผู้วิจัยได้ศึกษาหาข้อมูลจากทางอินเทอร์เน็ตและเว็บไซต์ที่เกี่ยวกับภัยคุกคามของความปลอดภัยของระบบสารสนเทศในประเทศไทย พบว่าปัจจุบันประเทศไทยยังไม่มีสิ่งที่สามารถทำนายความเสี่ยงของภัยคุกคามได้ จากข้อมูลเหล่านี้ได้นำผู้วิจัยไปสู่การพิจารณาและตั้งสมมติฐาน ว่าการเกิดภัยคุกคามความปลอดภัยของคอมพิวเตอร์นั้น มีปัจจัยที่สามารถนำไปสู่การทำนายความเสี่ยงของการเกิดภัยคุกคามได้ โดยจะนำข้อมูลของภัยคุกคามความปลอดภัยของระบบสารสนเทศที่ผู้วิจัยได้ศึกษาค้นคว้ามาทั้งต่างประเทศและในประเทศ มาทำการออกแบบสอบถามเพื่อสร้างเป็นโมเดลทำนายความเสี่ยง โดยที่ผลลัพธ์ของโมเดลทำนายความเสี่ยงนี้ เป็นระดับของโอกาสการเกิดภัยคุกคามอีกทั้งองค์กรสามารถนำไปประยุกต์เพื่อทราบถึงภัยคุกคามที่จะเกิดขึ้นกับภายในองค์กรได้

1.2 วัตถุประสงค์

งานวิจัยนี้จัดทำขึ้นเพื่อศึกษาปัจจัยและสร้างโมเดลเพื่อทำนายความเสี่ยงของภัยคุกคามความปลอดภัยของระบบสารสนเทศและใช้หน่วยงานที่เกี่ยวข้องกับการเงินเป็นกรณีศึกษา โดยมีวัตถุประสงค์ดังนี้

1) สำรวจความคิดเห็นเพื่อหาปัจจัยของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ

2) วิเคราะห์หาตัวทำนายของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ

3) สร้างโมเดลเพื่อใช้ทำนายผลของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ

1.3 ขอบเขตการดำเนินงาน

1) สำรวจความคิดเห็นเพื่อหาปัจจัยของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ โดยใช้วิธีการออกแบบสอบถาม เป็น 2 ส่วนคือ

ส่วนที่ 1 การออกแบบสอบถามเพื่อหาปัจจัยของการเกิดภัยคุกคาม โดยใช้กลุ่มตัวอย่าง ที่เป็นบุคลากรทางด้านคอมพิวเตอร์ไม่ต่ำกว่า 100 คน

ส่วนที่ 2 การออกแบบสอบถามเชิงลึก โดยนำข้อมูลที่ได้จากแบบสอบถามส่วนที่ 1 มาคัดเลือกเพื่อใช้ในการวิเคราะห์และออกแบบสอบถามในเชิงลึก โดยใช้กลุ่มตัวอย่างที่เป็นองค์กรที่เกี่ยวข้องกับการเงิน เช่น ธนาคาร สินเชื่อ เป็นกรณีศึกษา จำนวนไม่น้อยกว่า 30 องค์กร หรือไม่ต่ำกว่า 200 ชุด จากนั้นแบ่งสอบถามในส่วนนี้ออกเป็น 2 ชุด คือ training set สำหรับการสร้างโมเดล (80%) และ test set (20%) สำหรับการทดสอบโมเดล

2) นำข้อมูล training set มาวิเคราะห์หาตัวแปรที่เป็นตัวทำนายของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศโดยใช้เครื่องมือทางสถิติ เช่น การวิเคราะห์แบบการถดถอยพหุคูณโลจิสติค (Multinomial Logistic Regression Analysis) เป็นต้น เข้ามาเพื่อช่วยในการวิเคราะห์และสร้างโมเดล

3) ทดสอบโมเดลโดยใช้ข้อมูล test set เป็นตัวทดสอบโมเดล

4) ออกแบบและพัฒนาระบบโมเดลทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศโดยใช้ภาษา UML ในการออกแบบและพัฒนาระบบเป็น Web Application โดยใช้ภาษา PHP

1.4 ขั้นตอนดำเนินการ

1) ศึกษาข้อมูลเพื่อใช้ในการทำงานวิจัย ซึ่งมีหัวข้อดังนี้
   - ข้อมูลเกี่ยวกับความเสี่ยงของภัยคุกคามทางคอมพิวเตอร์
   - วิธีการประเมินความเสี่ยงในองค์กร
   - ผลการสำรวจอาชญากรรมคอมพิวเตอร์
   - เครื่องมือที่ใช้ในการวิเคราะห์
2) ออกแบบสอบถามโดยแบ่งเป็น 2 ส่วนได้แก่
   - แบบสอบถามเพื่อหาปัจจัยของภัยคุกคามระบบสารสนเทศ
   - แบบสอบถามเชิงลึกเพื่อใช้ในการวิเคราะห์
3) วิเคราะห์ข้อมูลเพื่อสร้างโมเดลทำนายความเสี่ยงของภัยคุกคามระบบสารสนเทศ
4) ทดสอบโมเดลที่ได้จากการวิเคราะห์
5) ออกแบบและพัฒนาระบบทำนายความเสี่ยงด้วยโมเดลที่ได้จากการวิเคราะห์
6) สรุปผลและเรียบเรียงวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) องค์กรสามารถนำโมเดลต้นแบบจากงานวิจัยนี้ไปประยุกต์ใช้ในการประเมินความเสี่ยงภายในองค์กรได้

2) องค์กรสามารถหาวิธีป้องกันหรือรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ หากสามารถทราบตัวทำนายที่ทำให้เกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศขององค์กร

3) องค์กรสามารถนำงานวิจัยนี้ไปต่อยอดเพื่อหาโมเดลของการทำนายความเสี่ยงที่ดีขึ้น

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการวิจัยครั้งนี้ ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง โดยแบ่งออกเป็น 2 ส่วน ดังนี้ ส่วนที่ 1 ข้อมูลและทฤษฎีที่เกี่ยวข้องกับภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์ ส่วนที่ 2 ทฤษฎีที่ใช้ในการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงของภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์ โดยมีรายละเอียดดังนี้

2.1 ส่วนที่ 1 ข้อมูลและทฤษฎีที่เกี่ยวข้องกับภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์

ภัยคุกคามความปลอดภัยของระบบสารสนเทศ คือ การกระทำหรือเกิดเหตุการณ์ที่มีผลต่อความปลอดภัยของระบบสารสนเทศ ทำให้ไม่สามารถดำเนินงานตามวัตถุประสงค์หรือเป้าหมายได้ ในแต่ละองค์กรอาจมีภัยคุกคามที่แตกต่างกันไป

2.1.1 การแบ่งกลุ่มของภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์ Dr. Michael E. Whiteman และHerbert J. Mattord [8] ได้มีการจัดกลุ่มของประเภทภัยคุกคามความปลอดภัยของระบบสารสนเทศไว้ 12 ประเภทดังนี้

1) ข้อผิดพลาดจากการกระทำของมนุษย์ (Acts of human error or failure) เกิดจากการผิดพลาดหรืออุบัติเหตุจากการกระทำบางอย่างของมนุษย์

2) การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property) เช่น การละเมิดหรือการลักลอบใช้ซอฟต์แวร์ เป็นต้น

3) การบุกรุก (Deliberate Acts of Trespass) เช่น การลักลอบเข้าระบบ เป็นต้น

4) การกรรโชกข้อมูลสารสนเทศ (Deliberate Acts of Information Extortion) เช่น การขู่เอาข้อมูลเพื่อแลกบางสิ่ง หรือ การบีบบังคับเพื่อให้ได้ข้อมูลมา เป็นต้น

5) การก่อวินาศกรรมหรือการทำลาย (Deliberate Acts of Sabotage or Vandalism) เกิดจากการทำลายระบบหรือข้อมูลของสารสนเทศ เช่น Denial of service (DoS)

6) การโจรกรรม (Deliberate Acts of Theft) เช่น การลักลอบขโมย อุปกรณ์คอมพิวเตอร์หรือข้อมูลสารสนเทศ เป็นต้น

7) การโจมตีซอฟต์แวร์ (Deliberate Software Attacks) เช่น การโจมตีที่มาจากซอฟต์แวร์ เช่น ไวรัส โทรจัน ซอมบี้ เป็นต้น

8) ภัยธรรมชาติ (Forces of Nature) เป็นภัยธรรมชาติที่ไม่สามารถควบคุมได้ เช่น น้ำท่วม ฟ้าฝ่า ไฟไหม้ เป็นต้น

9) คุณภาพของผู้ให้บริการ (Deviations in Quality of Service) ปัญหาที่มาจากผู้ให้บริการเรา เช่น delay ของ internet packet lose เป็นต้น

10) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors) ฮาร์ดแวร์นั้นทำงานผิดปกติ เช่น ฮาร์ดดิสเกิด Bad Sector เป็นต้น

11) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors) ซอฟต์แวร์นั้นทำงานผิดพลาด เช่น การเกิด bug หรือ เกิดจากโค้ดที่ผิดพลาด เป็นต้น

12) เทคโนโลยีล้าสมัย (Technological Obsolescence) เทคโนโลยีที่ไม่ทันสมัย เช่น ฮาร์ดแวร์รุ่นเก่า หรือ ระบบที่เก่า เป็นต้น

จากภัยคุกคามดังกล่าว ในแต่ละองกรค์จะมีความเสี่ยงในการเกิดภัยคุกคามแต่ละกลุ่มไม่เหมือนกัน ดังนั้นเพื่อที่จะป้องกันระบบสารสนเทศหรือระบบคอมพิวเตอร์สามารถดำเนินงานตามวัตถุประสงค์หรือเป้าหมายได้ จึงควรมีกระบวนการเตรียมความพร้อมที่จะรับมือกับความเสี่ยงของการเกิดภัยคุกคาม นั่นก็คือกระบวนการจัดการความเสี่ยง

2.1.2 การจัดการความเสี่ยง

การจัดการความเสี่ยงในระบบสารสนเทศ เป็นกระบวนการที่สามารถควบคุมความเสี่ยงที่จะเกิดภัยคุกคามในองค์กรนั้นได้ ซึ่งเป็นการระบุปัจจัยของความเสี่ยงและประเมินความเสี่ยง[8] โดยนำมาใช้เพื่อหาระดับความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยที่จะเกิดขึ้นในองค์กร โดยมีขั้นตอน [4] การทำงานดังนี้

2.1.2.1 การประเมินความเสี่ยง (Risk assessment) เป็นกระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิดเหตุการณ์และผลกระทบของภัยคุกคามซึ่งประกอบด้วยกระบวนการวิเคราะห์ความเสี่ยงและ การประเมินค่าความเสี่ยง

การวิเคราะห์ความเสี่ยง (Risk analysis) ประกอบด้วย 4 ขั้นตอนดังนี้

1) การชี้ระบุความเสี่ยง (Risk identification) เป็นขั้นตอนการชี้ความเสี่ยงที่จะเกิดขึ้นในองค์กร

2) ลักษณะรายละเอียดของความเสี่ยง (Risk description) เป็นการบรรยายรายละเอียดของความเสี่ยงนั้น เช่น ชื่อความเสี่ยง ผู้ที่ได้รับผลกระทบ เป็นต้น

3) การประมาณความเสี่ยง (Risk estimation) เป็นการประมาณค่าความเสี่ยงที่ระบุมาว่ามากน้อยเพียงใด

4) ประเมินค่าความเสี่ยง (Risk evaluation) เป็นหลักเกณฑ์ที่ยอมรับว่าจะยอมรับได้มากน้อยเพียงใดจากการประมาณค่าความเสี่ยงข้างบน

2.1.2.2 การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) รายงานผลความเสี่ยงที่วิเคราะห์ได้

2.1.2.3 การควบคุมความเสี่ยง (Risk control) กำหนดวิธีควบคุมจากรายงานความเสี่ยงที่เกิดขึ้นซึ่งแต่ละองค์กรมีวิธีการควบคุมที่แตกต่างกันไป มีแนวทางดังนี้

1) การหลีกเลี่ยง (Avoidance) คือการหลีกเลี่ยงความเสี่ยงที่จะเกิดขึ้น

2) การโยกย้าย (Transfer) เป็นการโยกย้ายความเสี่ยงที่จะเกิดขึ้นภายในองค์กรไปยังนอกองค์กร

3) การแบ่งเบา (Mitigation) คือการลดความรุนแรงที่จะเกิดขึ้นนั้นลง

4) การยอมรับ (Acceptance) การยอมรับและเข้าใจความเสี่ยงที่จะเกิดโดยไม่ต้องทำอะไร

2.1.2.4 การเฝ้าสังเกต (Monitoring) เป็นกระบวนการเฝ้าสังเกตความเหมาะสมของการจัดการความเสี่ยง

จากขั้นตอนการทำงานดังกล่าว จะเห็นได้ว่าขั้นตอนการวิเคราะห์ความเสี่ยงเป็นขั้นตอนของการจัดการความเสี่ยงที่สำคัญขั้นตอนหนึ่ง เพราะถ้าหากองค์กรมีการวิเคราะห์ความเสี่ยงผิดพลาดก็จะทำให้ขั้นตอนอื่นผิดพลาดตามไปด้วย เช่น หากองค์กรกำลังจะเกิดปัญหาของภัยคุกคามที่มาจากมนุษย์แต่กลับสนใจแต่ภัยคุกคามที่เกิดจากการโจมตีของซอฟต์แวร์ก็จะทำให้องค์กรนั้นแก้ไขไม่ตรงจุด เป็นต้น ดังนั้นถ้าหากมีการสร้างโมเดลทางคณิตศาสตร์ ที่สามารถทำนายความเสี่ยงของการเกิดภัยคุกคามระบบสารสนเทศในองค์กรได้ ก็จะทำให้องค์กรนั้นจัดการภัยคุกคามที่ตรงจุดได้

2.1.3 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องเกี่ยวกับข้อมูลของภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศของต่างประเทศมีดังนี้

2.1.3.1 งานวิจัยของ Michael E.Whitman [9] ได้ศึกษาข้อมูลของภัยคุกคามความปลอดภัยระบบสารสนเทศ โดยได้ศึกษาและทดสอบเพิ่มเติมจาก Loch et al. (1992) งานวิจัยนี้ได้กำหนดวัตถุประสงค์ของงานวิจัยไว้ 4 ข้อ

1) หาภัยคุกคามความปลอดภัยระบบสารสนเทศ

2) จัดอันดับภัยคุกคามที่อันตรายมาก

3) หาความถี่ของภัยคุกคามที่เกิดขึ้น

4) จัดอันดับภัยคุกคามที่มีค่าใช้จ่ายในการป้องกันสูง

จากผลงานวิจัย ซึ่งเป็นประโยชน์กับผู้วิจัยในด้านของการศึกษาข้อมูลประเภทภัยคุกคามความปลอดภัยของระบบสารสนเทศประเภทต่างๆ

2.1.3.2 งานวิจัยของ Mary Sumner [13] ได้ทำการศึกษาข้อมูลของโอกาสและผลกระทบของภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศและวิเคราะห์นำมาเปรียบเทียบระหว่าง ผลกระทบ(impact) โอกาสการเกิด(probability) และการรับมือ(preparedness) ของภัยคุกคามที่เกิดขึ้นซึ่งใช้ข้อมูลจากการตอบแบบสอบถามทางอินเทอร์เน็ต โดยแบบสอบถามนี้จะแบ่งสเกลทั้งหมด 7 สเกล โดยผลการวิเคราะห์นั้นพบว่ามีภัยคุกคาม ที่เกิดจากการผิดพลาดของมนุษย์ (Human Error) จากภัยธรรมชาติ (Force of Nature) จากคุณภาพของผู้ให้บริการต่างๆ (Quality of Service Deviations) และเทคโนโลยีที่ล้าสมัย (Technological Obsolescence) อยู่ในกลุ่มของ High-Impact/High-Probability Risk มีระดับการรับมือที่ต่ำ และงานวิจัยนี้ได้เสนอให้องค์กรนั้นควรมีการประเมินความเสี่ยงอย่างต่อเนื่อง และ มีการจัดการบรรเทาความเสี่ยงนั้นด้วย ซึ่งเป็นประโยชน์กับผู้วิจัยในเรื่องของการให้แนวคิดของการเก็บแบบสอบถามและการวิเคราะห์แบบสอบถาม

2.1.3.3 งานวิจัยของ Chaoju Hu and Chunmei Lv [7] ได้ทำการศึกษาการประเมินความเสี่ยง โดยนำหลักการของ Back Propagation (BP) Neural Network และ Fuzzy Neural Network มาใช้ ซึ่งวิธีนี้เป็นการตัดสินใจที่เหมาะกับค่าที่ไม่เป็นเชิงเส้น โดยมีการทำงาน 3 ขั้นตอน คือ

ขั้นที่ 1 จำแนกกำหนดความเสี่ยงโดยนำมาจากระดับของการป้องกันซึ่งมีด้วยกันอยู่ 5 ระดับ

ขั้นที่ 2 หาปัจจัยที่เกิดจากความเสี่ยงที่ได้มาแล้วนำปัจจัยนั้นไปวิเคราะห์โดย Fuzzy Theory

ขั้นที่ 3 นำผลที่ได้จากขั้นที่ 2 นำมาใส่ใน BP Neural Network

ผลการทดลองสรุปได้ว่า การใช้วิธีนี้สามารถที่จะลดปัญหาของผลกระทบที่มนุษย์สร้างขึ้นได้และมีประสิทธิภาพให้การเรียนรู้การตัดสินใจได้และการคำนวณมีความแม่นยำสูง ซึ่งงานวิจัยนี้ให้แนวคิดของการสร้างโมเดลทำนายความเสี่ยงแก่ผู้วิจัย

2.1.3.4 งานวิจัยของ Carl Colwill Human factors in information security: The insider threat e Who can you trust these days?(2010) ศึกษาและอธิบายถึงภัยคุกคามของระบบสารสนเทศที่เกิดขึ้นจากภายในองค์กรที่เกี่ยวข้องกับปัจจัยของสภาพสังคม เศรษฐกิจและวัฒนธรรม ปัญหาความภัยคุกคามของระบบสารสนเทศที่เกิดขึ้นนั้นส่วนใหญ่แล้วจะมาจากภายในองค์กรเองมากกว่าการมาจากภายนอก ซึ่งแนะนำว่าองค์กรควรที่จะจัดการความเสี่ยงในเชิงรุก ไม่ใช่เชิงรับและยอมรับสภาพปัญหาและผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม

2.2 ส่วนที่ 2 ทฤษฎีที่ใช้ในการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงของภัยคุกคามทางด้านความปลอดภัยของคอมพิวเตอร์

งานวิจัยนี้ได้ทำการศึกษาและหาปัจจัยของการเกิดภัยคุกคามความปลอดภัยของคอมพิวเตอร์ เพื่อที่จะมาสร้างโมเดลเพื่อทำนายความเสี่ยงดังนั้น จำเป็นต้องใช้การวิเคราะห์ข้อมูลเข้ามาช่วยในการสร้างโมเดล เทคนิคการวิเคราะห์นั้น มีหลายประเภทซึ่งผู้วิจัยเสนอ คือ การวิเคราะห์การถดถอยโลจิสติคแบบหลายกลุ่ม (Multinomial Logistic Regression Analysis)

2.2.1 ประเภทของข้อมูล

ประเภทของข้อมูล เป็นสิ่งที่สำคัญอย่างยิ่งในการวิเคราะห์ข้อมูล ทั้งนี้เนื่องจากประเภทของข้อมูล และวัตถุประสงค์จะเป็นสิ่งที่กำหนดในการเลือกเทคนิคการวิเคราะห์ข้อมูลที่ถูกต้องเหมาะสม ประเภทของข้อมูลสามารถจำแนกได้ ดังนี้ [1]

2.2.1.1 จำแนกตามแหล่งที่มาของข้อมูล จะสามารถจำแนกข้อมูลตามแหล่งที่มาของข้อมูลนั้นได้ 2 ประเภท

1) ข้อมูลปฐมภูมิ (Primary Data) เป็นข้อมูลที่ผู้ใช้หรือหน่วยงานที่จะใช้ข้อมูลเป็นผู้เก็บรวบรวมเอง ซึ่งอาจจะเก็บโดยการสัมภาษณ์ หรือทดลอง หรือสังเกตการณ์ ข้อมูลปฐมภูมิจะเป็นข้อมูลที่มีรายละเอียดตรงกับที่ผู้ใช้ต้องการ แต่จะต้องเสียเวลาและค่าใช้จ่ายมาก และข้อมูลที่ได้จะเป็นข้อมูลดิบ (Raw Data) ซึ่งยังเป็นข้อมูลที่ไม่ได้วิเคราะห์

2) ข้อมูลทุติยภูมิ (Secondary Data) เป็นข้อมูลที่ผู้ใช้ไม่ได้เก็บรวบรวมเอง แต่มีหน่วยงานหรือผู้อื่นทำการเก็บรวบรวมไว้แล้ว และมักจะเป็นข้อมูลที่ได้ทำการวิเคราะห์เบื้องต้นมาแล้ว ผู้ใช้นำมาใช้ได้เลยจึงประหยัดทั้งเวลาและค่าใช้จ่ายบางครั้งข้อมูลทุติยภูมิจะไม่ตรงกับ

ความต้องการหรือไม่มีรายละเอียดเพียงพอนอกจากนั้นผู้ใช้มักจะไม่ทราบถึงข้อผิดพลาดของข้อมูล ซึ่งอาจทำให้ผู้อื่นที่นำมาใช้สรุปผลการวิจัยผิดพลาดไปด้วย ผู้ที่นำข้อมูลทุติยภูมิมาใช้ควรระมัดระวังอย่างยิ่ง

2.2.1.2 จำแนกตามลักษณะของข้อมูล ถ้าจำแนกตามลักษณะของข้อมูลจะสามารถจำแนกได้เป็น 2 ประเภทดังนี้

1) ข้อมูลเชิงคุณภาพ (Qualitative Data) เป็นข้อมูลที่อยู่ในรูปข้อความ เพื่อแสดงความแตกต่างของลักษณะต่างๆ เช่น การแบ่งเพศ ชายและหญิง เป็นต้น

2) ข้อมูลเชิงปริมาณ (Quantitative Data) เป็นข้อมูลที่อยู่ในรูปของตัวเลขที่มีความหมาย หรือสามารถวัดค่าได้ว่า มากกว่า หรือน้อยกว่า เช่น ปริมาณวัตถุดิบ ยอดขาย น้ำหนัก เป็นต้น

2.2.1.3 แบ่งตามชนิดสเกลของข้อมูล การเลือกเทคนิคการวิเคราะห์ข้อมูลให้เหมาะสมกับชนิดหรือสเกลของข้อมูล เป็นสิ่งที่สำคัญและจำเป็นอย่างมาก เพื่อที่จะสามารถนำข้อมูลที่มีมาใช้การการวิเคราะห์ได้อย่างเหมาะสม โดยทั่วไปสเกลของข้อมูลแบ่งออกเป็น 4 ชนิด

1) สเกลนามกำหนดหรือสเกลแบ่งกลุ่ม (Nominal Scales) เป็นการแบ่งกลุ่มของข้อมูลออกเป็นกลุ่มย่อย เช่น แบ่งตามเพศ อาชีพ ศาสนา พรรคการเมืองที่ชอบ เป็นต้น ไม่สามารถระบุได้ว่ากลุ่มใดดีกว่าหรือมากกว่า หรือสำคัญกว่ากลุ่มอื่นๆ

2) สเกลอันดับ (Ordinal Scale) เป็น สเกลที่ใช้แบ่งกลุ่ม เช่นเดียวกับสเกลแบ่งกลุ่ม แต่จะให้รายละเอียดมากกว่า คือสามารถแสดงความแตกต่างระหว่างกลุ่มอื่นได้ๆ โดยสามารถระบุหรือจัดอันดับได้ว่ากลุ่มใดดีกว่า มากกว่า เห็นด้วยมากกว่า พอใจมากกว่ากลุ่มอื่นๆ เช่น ตัวแปรอายุที่แบ่งเป็นช่วง ระดับการศึกษา รายได้ที่แบ่งเป็นช่วงหรือลำดับที่

3) สเกลอันตรภาคหรือสเกลแบบช่วง (Interval Scale) เป็นสเกลที่มีรายละเอียดมากว่าสเกลแบบกลุ่มและสเกลอันดับ เป็นสเกลที่วัดความแตกต่างได้ สามารถระบุได้ว่าดีกว่า มากกว่า หรือน้อยกว่าเท่าใด นิยมใช้กันมากในงานวิจัยด้านสังคมศาสตร์ เช่น คะแนนแสดงความคิดเห็น หรือทัศนคติ คะแนนความพึงพอใจ คะแนนสอบ โดยการกำหนดคะแนนอาจแตกต่างกัน และเป็นสเกลที่สามารถระบุระยะห่างด้วยช่วงที่เท่าๆ กันได้

4) สเกลอัตราส่วน (Ratio Scale) เป็นสเกลที่สมบูรณ์ที่สุด คือเป็นข้อมูลที่ระบุขนาดได้ทำให้สามารเทียบได้ ระบุความแตกต่างได้ และจุดเริ่มต้นเป็นค่าที่มีความหมายด้วย

2.2.2 การวิเคราะห์องค์ประกอบ (Factor Analysis)

การวิเคราะห์องค์ประกอบ เป็นเทคนิคการวิเคราะห์ทางสถิติของการวิจัย ที่มุ่งลดจำนวนตัวแปรที่มีอยู่มาก ทั้งนี้ก็ด้วยเหตุผลตัวแปรบางตัวอาจมีคุณสมบัติในการอธิบายลักษณะของข้อมูลเหมือนๆ กันตัวแปรในลักษณะนี้อาจจะต้องตัดทิ้งไป หรือตัวแปรบางตัวมีลักษณะความสัมพันธ์ใกล้เคียงกัน จะถูกรวมเข้ากลุ่มกันเป็นตัวแปรใหม่ เรียกว่าปัจจัย (Factor) การรวมกลุ่มของตัวแปร จะจัดเป็นกลุ่มของปัจจัย การวิเคราะห์จะดูที่ค่าความสัมพันธ์กัน ซึ่งอาจจะสัมพันธ์กันในทางบวก หรือทางลบก็ได้ ความหมายของคำต่างๆ ในการวิเคราะห์องค์ประกอบ มีดังนี้ [1]

2.2.2.1. องค์ประกอบร่วมกัน (Common Factor) หมายถึง องค์ประกอบที่ประกอบด้วยตัวแปร 2 ตัวขึ้นไปมารวมกันอยู่ในองค์ประกอบเดียวกัน โดยองค์ประกอบร่วมจะอาศัยจากค่าสัมประสิทธิ์สหสัมพันธ์ หรือค่า r องค์ประกอบที่ประกอบด้วยตัวแปรที่มีค่าความสัมพันธ์กันมาก จะเป็นองค์ประกอบที่มีความหมายในการวิเคราะห์องค์ประกอบ

2.2.2.2. องค์ประกอบเฉพาะ (Specific Factor) ได้แก่ องค์ประกอบที่มีตัวแปรเพียงตัวเดียว

2.2.2.3. ความร่วมกัน (Communalities) หมายถึง ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรหนึ่งกับตัวแปรอื่นๆ ที่เหลือทั้งหมด มีค่าอยู่ระหว่าง 0 กับ 1 ถ้าตัวแปรใดมีค่านี้ต่ำตัวแปรนั้นจะถูกตัดออก ค่านี้ดูได้จาก Initial Statistic หรือค่าทแยงมุมของ Reproduced Correlation Matrix

2.2.2.4. น้ำหนักองค์ประกอบ (Factor Loading) เป็นค่าความสัมพันธ์ระหว่างตัวแปรกับองค์ประกอบ ซึ่งควรมีค่ามากกว่า 0.5 [1] ตัวแปรใดมีน้ำหนักในองค์ประกอบใดมาก ควรจัดตัวแปรนั้นอยู่ในองค์ประกอบนั้น ในโปรแกรม SPSS น้ำหนักองค์ประกอบของแต่ละองค์ประกอบดูได้จากตาราง Component Matrix ก่อนการหมุนแกนองค์ประกอบ หรือดูได้จากเส้นทแยงมุมของแมทริกซ์ของค่าไอเกน (Eigen Value)

2.2.2.5. คะแนนองค์ประกอบ (Factor Score) เป็นคะแนนที่ได้จากน้ำหนักองค์ประกอบและค่าของตัวแปร เพื่อใช้เป็นค่าของตัวแปรใหม่ ที่เรียกว่า องค์ประกอบ หรือ ปัจจัย (Factor) สำหรับการคำนวณหา Factor Score มีดังนี้

$$F_{ik} = W_{i1}Z_{1k} + W_{i2}Z_{2k} + \ldots + W_{ip}Z_{pk}$$

$$k = 1, 2, \ldots, n$$

i = 1, 2,..., m

โดยที่

Z_{jk} = เป็นค่าปัจจัยที่ j ของ case ที่ k

n = จำนวนข้อมูล

m = จำนวน Factor

W_{ik} = ค่าสัมประสิทธิ์ หรือ loading factor ของตัวแปรที่ k ใน Factor ที่ i

F_{ik} = Factor score ของ Factor ที่ i ของ case ที่ k

2.2.2.6. ค่าไอเกน (Eigen Value) เป็นค่าความผันแปรของตัวแปรทั้งหมดในแต่ละองค์ประกอบ ในการวิเคราะห์องค์ประกอบ องค์ประกอบร่วม (Common Factor) ที่ได้องค์ประกอบแรก จะเป็นองค์ประกอบที่แยกความผันแปรของตัวแปรออกมาจากองค์ประกอบอื่นได้มากที่สุด จึงมีตัวแปรร่วมอยู่มากที่สุดค่าของไอเกนจะเท่ากับจำนวนตัวแปรในองค์ประกอบนั้น ดังนั้นในแต่ละองค์ประกอบจึงมีค่าไอเกนที่มากกว่า 1 โดยค่า ไอเกนสามารถคำนวณได้จาก Eigen Value = $\sum(w)^2$ โดยที่ w คือน้ำหนักของตัวแปรในองค์ประกอบนั้น

2.2.3 การวิเคราะห์แบบการถดถอยพหุคูณโลจิสติค (Multinomial Logistic Regression)

การวิเคราะห์การถดถอยโลจิสติค เป็นการนำตัวแปรอิสระซึ่งเป็นตัวแปรที่ทำหน้าที่เป็นเหตุทำให้เกิดผลอย่างใดอย่างหนึ่ง จำนวนหลายตัวแปรมาวิเคราะห์ความสัมพันธ์พร้อมๆ กันกับตัวแปรตาม ซึ่งเป็นตัวแปรที่เป็นผลและเป็นตัวแปรเชิงกลุ่ม (Categorical data) การวิเคราะห์ประเภทนี้สามารถบอกได้ว่าตัวแปรอิสระหรือปัจจัยใดที่ทำให้เกิดเหตุการณ์ที่คาดหวัง หรือเป็นการวิเคราะห์ถึงโอกาสในการเกิดเหตุการณ์ที่สนใจ ในการวิเคราะห์โลจิสติคจะต้องกำหนดโมเดลโลจิสติค เรียกว่า Logit Model ในสมการที่ 3 ซึ่งเป็นแบบจำลองที่นำมาใช้วิเคราะห์ข้อมูลว่าตัวแปรอิสระ (X) ส่งผลต่อโอกาสการเกิดเหตุการณ์ที่สนใจ (Y) หรือไม่ ซึ่งความน่าจะเป็นของการเกิดเหตุการณ์จะมีค่าในช่วง 0 ถึง 1 โดยมีรูปแบบสมการดังนี้

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

Prob(no event) = 1 - Prob(event)

$$= \frac{1}{1+e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

เมื่อ

β_0	คือ	ค่าคงที่
$\beta_1,\ldots, \beta_n$	คือ	ค่าสัมประสิทธิ์ของตัวแปรต่างๆ มีทั้งหมด n ตัว
$x_1, x_2, \ldots, x_n$	คือ	ตัวแปรอิสระมีทั้งหมด n ตัว
e	คือ	เป็นค่าคงที่ทางคณิตศาสตร์มีค่าประมาณ 2.718

เนื่องจากสมการ (1) เป็นความสัมพันธ์ระหว่างตัวแปรอิสระและตัวแปรตามที่ไม่เป็นเชิงเส้น จึงมีการปรับให้อยู่ในรูปแบบของเชิงเส้น โดยโมเดลโลจิสติค สามารถเขียนให้อยู่ในรูปของ odd ของการเกิดเหตุการณ์ได้ odd หมายถึงอัตราส่วนระหว่างโอกาสการเกิดเหตุการณ์กับโอกาสไม่เกิดเหตุการณ์
จากสมการที่ (1) และ (2) จะได้

$$\left(\frac{prob\ event}{prob\ no\ event}\right) = \frac{e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}}{1+e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}} \Big/ \frac{1}{1+e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}}$$

$$= e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}$$

ดังนั้น

$$\text{odds} = \left(\frac{prob\ event}{prob\ no\ event}\right) = e^{\beta_0+\beta_1 x_1+\cdots+\beta_n x_n}$$

และเมื่อปรับให้อยู่ในรูปแบบของเชิงเส้นจะได้

$$\ln(\text{odds}) = \ln\left(\frac{prob\ event}{prob\ no\ event}\right)$$

$$= \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n \quad \text{..... (3)}$$

การประมาณค่าสัมประสิทธิ์ β_0- β_n จะใช้หลักการของความน่าจะเป็นสูงสุด (Maximum Likelihood) หรือการประมาณค่า β_0- β_n ที่ทำให้ ln L จากสมการ

$$\ln L = \sum_{i=1}^{n} y_i \left\{\frac{e^z}{1+e^z}\right\} + \sum_{i=1}^{n} 1 - y_i \left\{\frac{1}{1+e^z}\right\}$$

มีค่ามากที่สุด โดยการหาอนุพันธ์ลำดับที่ 1 ของสมการ

$$L = \prod_{i=1}^{n} \left\{\frac{e^z}{1+e^z}\right\}^{y_i} \left\{\frac{1}{1+e^z}\right\}^{1-y_i}$$

เทียบกับ β_0- β_n แล้วให้เท่ากับศูนย์ อย่างไรก็ตามไม่สามารถหาค่า β_0- β_n ได้โดยตรง เนื่องจากสมการไม่ได้อยู่ในรูปเชิงเส้น จึงใช้เทคนิคการทำซ้ำ (Iteration) ดังนั้นส่วนใหญ่จึงมักใช้โปรแกรมสำเร็จรูปทางสถิติ เช่น SAS, SPSS, JMP เป็นต้น

เมื่อ z คือ $\beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n$

y_i คือ เหตุการณ์ที่สนใจ

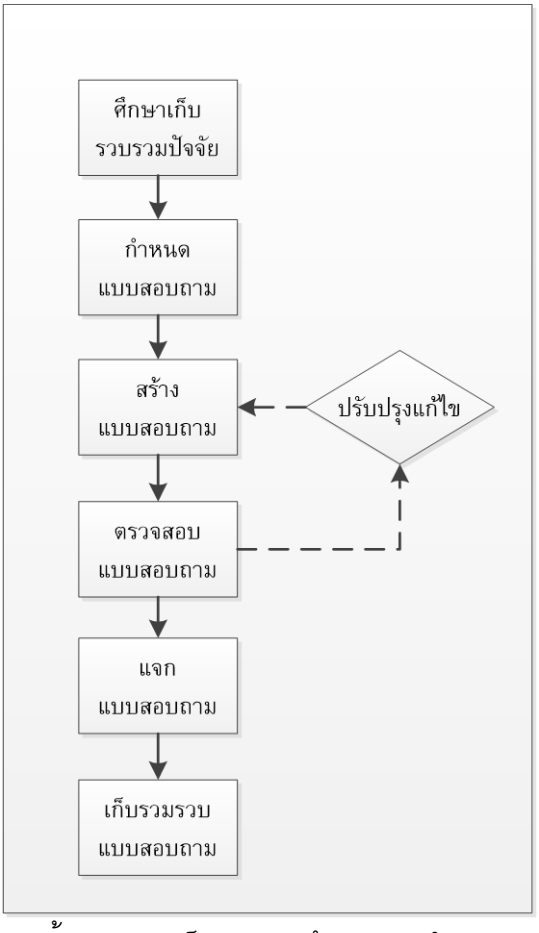
ทั้งนี้หลักเกณฑ์ในการเลือกแบบจำลองที่เหมาะสมต้องพิจารณาจากค่า Sig. ของ -2 Log Likelihood Ratio Test และ Walds Statistic เพื่อใช้ในการพิจารณาโมเดลและปัจจัยที่เหมาะสม

หมายเหตุ ในโปรแกรม SPSS เทคนิค Multinomail Logistic Regression จะให้ Category สุดท้ายเป็น Reference Category ซึ่ง Category นั้นจะมีสมการ z = 0 [1]

บทที่ 3
การเก็บรวบรวมข้อมูล

งานวิจัยนี้เป็นการเก็บรวบรวมข้อมูล เพื่อสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ โดยใช้การวิเคราะห์แบบ Multinomial Logistic Regression ซึ่งเป็นวิธีการหาความสัมพันธ์ระหว่างปัจจัยกับระดับการเกิดภัยคุกคาม เพื่อจะสร้างเป็นโมเดลที่ใช้ทำนายความเสี่ยง โดยมีวัตถุประสงค์คือ 1) วิเคราะห์หาตัวทำนายของการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์ 2) สร้างโมเดลเพื่อใช้ทำนายผลของการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์

สำหรับบทนี้จะเป็นการอธิบายเกี่ยวกับขั้นตอนการเก็บรวบรวมข้อมูลที่จะใช้ในการวิเคราะห์เพื่อทำนายความเสี่ยง แสดงภาพรวมดัง รูปที่ 3.1



รูปที่ 3.1 ขั้นตอนการเก็บรวบรวมข้อมูลการสำรวจหาปัจจัย

โดยในขั้นตอนนี้เป็นการเก็บรวบรวมข้อมูล โดยจะใช้วิธีการออกแบบสอบถามเพื่อนำข้อมูลไปใช้ในการวิเคราะห์ ซึ่งจะแบ่งแบบสอบถามเป็น 2 ส่วนดังนี้

3.1 ส่วนที่ 1 การออกแบบสอบถามสำรวจความคิดเห็นของปัจจัยความเสี่ยงคอมพิวเตอร์ด้านความปลอดภัย

ในการออกแบบสอบถามนี้เพื่อใช้สำรวจหาปัจจัยที่ทำให้เกิดภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศในปัจจุบัน ผู้วิจัยเลือกใช้กลุ่มตัวอย่างจากบุคลากรที่ทำงานเกี่ยวข้องในด้านระบบสารสนเทศมาจำนวน 117 คนในการตอบแบบสอบถามซึ่งลักษณะแบบสอบถามจะเป็นคำถามปลายปิดและคำถามปลายเปิด โดยวิธีการสำรวจจะเป็นการแจกแบบสอบถามให้แก่บุคลากรของแต่ละองกรค์โดยตรง เพื่อสำรวจความคิดเห็นเกี่ยวกับปัจจัยของการเกิดความเสี่ยงทางด้านความปลอดภัยของระบบคอมพิวเตอร์ (แบบสอบถามสำรวจหาปัจจัยจะแสดงภาคผนวก ก.1) ซึ่งสำหรับการเก็บรวบรวมข้อมูลในส่วนนี้จะมีขั้นตอนดังนี้

3.1.1 การสร้างแบบสอบถามสำรวจความคิดเห็นของปัจจัย

1) ศึกษาเพื่อเก็บรวบรวมปัจจัยที่มีผลทำให้เกิดภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศ จากหนังสือ อินเทอร์เน็ต และงานวิจัยที่เกี่ยวข้อง

2) วางแผนการกำหนดแบบสอบถาม

3) สร้างแบบสอบถามโดยจะใช้ปัจจัยที่ศึกษามาจากข้างต้นเป็นแนวทางสำหรับผู้ตอบแบบสอบถามและให้ผู้ตอบแบบสอบถามแสดงความคิดเห็นปัจจัยเพิ่มเติ่มที่นอกเหนือจากปัจจัยที่มี

4) ตรวจสอบแบบสอบถาม โดยเอาแบบสอบถามฉบับร่างนำเสนอต่ออาจารย์ที่ปรึกษาเพื่อตรวจสอบความตรงเชิงเนื้อหา (content validity) และปรับปรุงตามคำแนะนำของอาจารย์ที่ปรึกษา

3.1.2 การแจกแบบสอบถามและเก็บรวบรวมข้อมูลการสำรวจปัจจัยจากแบบสอบถาม

1) นำแบบสอบถามที่สร้างเรียบร้อยแล้วแจกโดยองค์กรต่างๆ ที่มีแผนกสารสนเทศในองค์กร

2) เก็บรวมรวบแบบสอบถามและเรียบเรียงข้อมูลปัจจัยที่ได้จากการสำรวจปัจจัยโดยจะคัดเลือกปัจจัยที่ไม่มีผู้ตอบแบบสอบถามเลือกออกและยุบรวมปัจจัยที่ซ้ำซ้อนเพื่อนำข้อมูลส่วนนี้ไปออกแบบสอบถามเชิงลึกต่อไป (ผลสรุปแบบสอบแสดงในภาคผนวก ข.1)

3.2 ส่วนที่ 2 การออกแบบสอบถามเชิงลึก

การสร้างแบบสอบถามจะใช้ข้อมูลในการออกแบบสอบถามในข้อ 3.1 เพื่อใช้เป็นข้อมูลของปัจจัยที่ทำให้เกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ โดยออกแบบให้มีการประเมินการเกิดภัยคุกคามแบบ 5 ระดับดังตารางที่ 3.1 (แบบสอบถามสำรวจหาปัจจัยแสดงในภาคผนวก ก.2)

ตารางที่ 3.1 ระดับอัตราการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์

ระดับ	โอกาสเกิดความเสี่ยงจากภัยคุกคาม	จำนวนครั้ง/เดือน
1	โอกาสเกิดน้อยที่สุด	0 - 4 ครั้ง
2	โอกาสเกิดน้อย	ระหว่าง 5 - 11 ครั้ง
3	โอกาสเกิดปานกลาง	ระหว่าง 12 - 18 ครั้ง
4	โอกาสเกิดมาก	ระหว่าง 19 - 25 ครั้ง
5	โอกาสเกิดมากที่สุด	มากกว่า 26 ครั้ง

โดยมีวัตถุประสงค์ในการออกแบบสอบถามนี้เพื่อใช้ข้อมูลที่ได้จากการตอบแบบสอบถามไปใช้ในการวิเคราะห์สร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์ โดยใช้ข้อมูลจากแบบแบบสอบถามจำนวน 298 ชุด จาก 302 ชุด โดยผู้ตอบแบบสอบถามจะเป็นผู้ที่เกี่ยวข้องหรือมีความรู้ด้านสารสนเทศโดยวิธีการสอบถามจะทำการแจกแบบสอบถามไปยังองค์กรต่างๆ โดยตรงและใช้วิธีการแจกแบบสอบถามทางอินเทอร์เน็ต

3.2.1 การสร้างแบบสอบถามเชิงลึก

1) ศึกษาการออกแบบสอบถามที่เกี่ยวข้องเพื่อใช้เป็นแนวทางในการออกแบบสอบถาม

2) วางแผนกำหนดประเภทข้อมูลของการออกแบบสอบถามและการกำหนดแบบสอบถาม

3) ศึกษาข้อมูลของการเกิดภัยคุกคามของคอมพิวเตอร์ด้านความปลอดภัยโดยศึกษาจากหนังสือ เอกสาร และอินเทอร์เน็ต

4) เก็บรวบรวมและคัดเลือกผลสำรวจที่ได้จากการตอบสอบถามในส่วนแรก

5) สร้างแบบสอบถามเชิงลึกโดยใช้ข้อมูลที่คัดเลือกมาจากแบบสอบถาม

6) ตรวจสอบแบบสอบถาม โดยเอาแบบสอบถามฉบับร่างนำเสนอต่ออาจารย์ที่ปรึกษาและผู้ที่มีความรู้ทางด้านนี้ตรวจสอบความตรงเชิงเนื้อหา (content validity) และปรับปรุงตามคำแนะนำ

3.1.2 การเก็บรวบรวมข้อมูล

1) นำแบบสอบถามที่สร้างเรียบร้อยแล้วแจกโดยองค์กรต่างๆ ที่มีแผนกสารสนเทศในองค์กรและทางอินเทอร์เน็ต

2) เก็บรวบรวมแบบสอบถามเรียบเรียงและบันทึกข้อมูลเพื่อเตรียมใช้ในการวิเคราะห์โดยสรุปข้อมูลทั่วไปของกลุ่มผู้ตอบแบบดังตารางที่ 3.2

ตารางที่ 3.2 ข้อมูลผู้ตอบแบบสอบถาม

ตำแหน่งงาน	จำนวน	ร้อยละ
Programmer	91	30.54
Systems Analyst	17	5.70
Information Officer	28	9.40
Security Officer	8	2.68
Network Administrator	32	10.74
Database Administrator	-	-
Help Desk Support	7	2.35
Technician	13	4.36
Trainer & Teacher	-	-
Web Designer & Developer	67	22.49
IT Manager	14	4.70
อื่นๆ	21	7.05
รวม	298	100.00

บทที่ 4
การวิเคราะห์ข้อมูล

ในบทนี้เป็นการอธิบายถึงขั้นตอนการวิเคราะห์ข้อมูล เพื่อใช้ในการสร้างโมเดลทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัย โดยจะนำข้อมูลที่รวบรวมได้จากการเก็บแบบสอบถามเชิงลึกในบทที่ 3 มาแบ่งออกเป็น 2 ส่วน ส่วนแรกจะแบ่งเป็น 80% เพื่อการวิเคราะห์หาความสัมพันธ์ระหว่างปัจจัยและระดับการเกิดภัยคุกคามเพื่อที่จะสร้างเป็นโมเดลทำนายความเสี่ยง โดยการวิเคราะห์แบบการถดถอยพหุคูณโลจิสติค (Multinomial Logistic Regression) และส่วนสอง จะแบ่ง 20% เพื่อนำมาทดสอบโมเดลที่สร้างขึ้นมาเพื่อตรวจสอบความเหมาะสมของโมเดล โดยขั้นตอนการวิเคราะห์มีดังนี้

4.1 การวิเคราะห์องค์ประกอบ

เนื่องจากจำนวนปัจจัยที่มากและต้องการกำจัดปัจจัยที่มีความสัมพันธ์กันออก เพื่อที่จะสามารถนำไปเข้ากระบวนการวิเคราะห์ต่อไป จะต้องมีกระบวนการที่ใช้วิเคราะห์ปัญหาเหล่านี้ โดยในที่นี้จะใช้วิธีการวิเคราะห์องค์ประกอบมาเพื่อกำจัดปัญหาดังกล่าวโดยจะใช้ข้อมูลที่แบ่งจากแบบสอบถามจำนวน 250 ชุด

4.1.1 เครื่องมือที่ใช้

เนื่องจากข้อมูลที่ได้จากแบบสอบถามเป็นข้อมูลประเภท Ordinal Data และ Categories Data ผู้วิจัยจึงเลือกใช้วิธีการหาค่าความสัมพันธ์ (Correlation) โดยใช้วิธี Polychoric Correlation ซึ่งเป็นวิธีการที่เหมาะกับข้อมูลประเภท Ordinal Data และ Categories Data (ผลการวิเคราะห์หาความสัมพันธ์ของปัจจัยแสดงในภาคผนวก ค.1) แล้วนำข้อมูลใช้ในการวิเคราะห์องค์ประกอบโดยใช้โปรแกรม R เป็นเครื่องมือช่วยในการวิเคราะห์

4.1.2 ผลการวิเคราะห์

ในการวิเคราะห์องค์ประกอบของโปรแกรม R จะต้องหาองค์ประกอบที่เหมาะสมก่อน ซึ่งจะพิจารณาที่ค่าไอเกน (Eigen) ซึ่งค่าไอเกนขององค์จำนวนประกอบจะต้องมีค่าไม่ต่ำกว่า 1 ซึ่งค่าไอเกนของปัจจัยแสดงดังตารางที่ 4.1

ตารางที่ 4.1 ค่าไอเกนจากปัจจัยทั้ง 24 ปัจจัย

องค์ประกอบใหม่	**ค่าไอเกน**
F1	8.93
F2	3.73
F3	1.72
F4	1.41
F5	1.06
F6	0.91
F7	0.88
F8	0.78
F9	0.68
F10	0.66
F11	0.59
F12	0.48
F13	0.47
F14	0.37
F15	0.29
F16	0.26
F17	0.26
F18	0.14
F19	0.12
F20	0.08
F21	0.05
F22	0.02
F23	0.02
F24	0.01

โดยที่ F1-F24 จะเป็นองค์ประกอบใหม่ที่ได้จากการวิเคราะห์ จากนั้นจะเลือกองค์ประกอบที่มี

ค่าไอเกนมากกว่าหรือเท่ากับ 1 ซึ่งดังตารางที่ 4.1 จะได้จำนวนองค์ประกอบ 5 องค์ประกอบ จากนั้นจะทำการวิเคราะห์องค์ประกอบโดยมีจำนวนองค์ประกอบเท่ากับ 5 ซึ่งผลการวิเคราะห์องค์ประกอบจะได้ค่า Factor loading ดังตารางที่ 4.2

ตารางที่ 4.2 Factor loading ที่ได้จากการวิเคราะห์ Factor

	องค์ประกอบ				
	F1	F2	F3	F4	F5
การป้องกันในระบบเครือข่าย (V1)	-0.74	0.55	0.22	0.18	0.05
การอัพเดทระบบป้องกัน (V2)	0.18	0.72	-0.04	-0.17	-0.05
อายุการใช้งานฮาร์ดแวร์ (V3)	0.31	-0.51	-0.31	-0.15	-0.06
สภาพแวดล้อมของฮาร์ดแวร์ (V4)	0.94	0.23	0.13	-0.04	-0.09
จำนวนเครื่องเซิร์ฟเวอร์(V5)	-0.88	-0.19	-0.20	0.06	0.13
การป้องกันไฟล์ข้อมูล (V6)	0.78	0.06	0.12	0.28	-0.08
การแบ็คอัพข้อมูล (V7)	-0.03	0.09	0.63	-0.15	-0.10
ความขัดแย้งภายในองค์กร (V8)	-0.76	-0.2	0.13	0.07	0
ความใส่ใจความปลอดภัย (V9)	-0.42	0.42	0.02	0.51	0.02
ขาดผู้เชี่ยวชาญ (V10)	0.02	0.42	0.18	-0.66	-0.09
การตั้งรหัสคอมพิวเตอร์ (V11)	0.01	-0.05	-0.01	-0.15	0.77
การใช้คอมพิวเตอร์ร่วมกัน (V12)	-0.70	0.08	0.39	-0.04	0.04
มีการเปิดเผยรหัสผ่าน (V13)	0.07	-0.05	0.33	-0.04	-0.67
เก็บรักษารหัสไม่ดีพอ (V14)	-0.82	-0.05	0.13	0.24	0.25
สั่งงานผ่านอีเมลล์ส่วนตัว (V15)	0.89	-0.14	-0.01	-0.04	0.07
การอบรมความปลอดภัย (V16)	0.81	0.24	0.23	0.35	0.08
อายุขององค์กร (V17)	-0.19	-0.09	-0.72	-0.07	0.22
นโยบายความปลอดภัย (V18)	0.74	0.10	0.39	0.34	0.10
บทลงโทษ (V19)	0.80	0.42	0.27	0.09	-0.01
การแบ่งหน้าที่การทำงาน (V20)	0.14	0.60	0.42	-0.03	0.18
งบประมาณ (V21)	0.24	0.77	-0.14	-0.13	-0.01

	องค์ประกอบ				
	F1	F2	F3	F4	F5
ขาดการสนับสนุน (V22)	-0.12	0.04	0.01	-0.49	0.22
การใช้เอาท์ซอส (V23)	0.34	0.79	0.32	0.05	-0.13
ระบบที่ใช้บริการไม่มีคุณภาพ เช่น ไฟฟ้า อินเทอร์เน็ต (V24)	-0.90	-0.11	-0.06	0.09	-0.05

จากตารางที่ 4.2 เป็นปัจจัยใหม่ที่ถูกสร้างขึ้นจากการวิเคราะห์องประกอบโดยจะแสดงค่าน้ำหนักปัจจัย (Factor Loading) โดยค่านี้จะเป็นตัวชี้ว่าตัวแปรใดควรจะอยู่กับปัจจัยไหน ซึ่งหากค่าน้ำหนักของปัจจัยใดมีค่ามาก (เข้าใกล้ +1 หรือ -1) ปัจจัยนั้นก็จะอยู่ในองค์ประกอบนั้น จากตารางข้างต้น ได้สรุปผลการวิเคราะห์องค์ประกอบโดยการจำแนกกลุ่มปัจจัย ซึ่งปัจจัยใหม่ที่ได้จะแบ่งออกเป็น 5 กลุ่ม แสดงดังตารางที่ 4.3 และ รูปที่ 4.1

ตารางที่ 4.3 การแยกปัจจัยกับองค์ประกอบใหม่ที่ได้

ปัจจัยใหม่	ตัวแปร
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

จากการวิเคราะห์องค์ประกอบ จะสามารถหาค่าองค์ประกอบใหม่ดังที่กล่าวไว้ในบทที่ 2 โดยจะมีสมการที่ได้ดังนี้

F1 = (0.74) V1+ (0.94) V4+ (-0.88) V5+ (0.78) V6+ (-0.76) V8+ (-0.70) V12+ (-0.82) V14+ (0.89) V15+ (0.81) V16+ (0.74) V18+ (0.80) V19+ (-0.90) V24

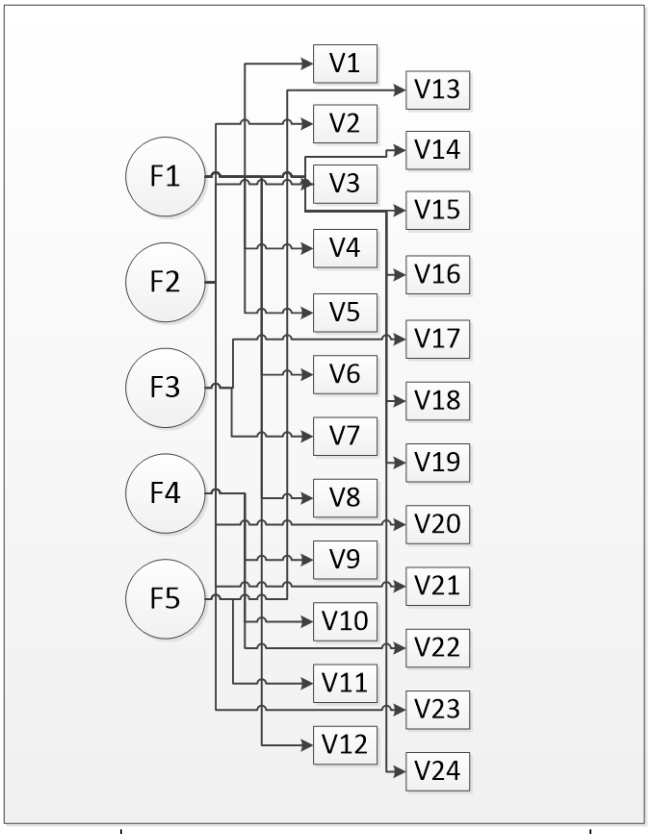
F2 = (0.72) V2+ (-0.51) V3+ (0.60) V20+ (0.77) V21+ (0.79) V23

F3 = (0.63) V7+ (-0.72) V17

F4 = (0.52) V9+ (-0.66) V10

F5 = (0.77) V11+ (-0.67) V13

เมื่อ V_k แทน ค่าปัจจัยของเคสที่ k โดยที่ k = 1, 2, 3,……., 24



รูปที่ 4.1 การแยกปัจจัยกับองค์ประกอบใหม่ที่ได้

จากรูปที่ 4.1 เป็นการแสดงองค์ประกอบใหม่ที่ได้ ซึ่งแต่ละปัจจัยจะมีองค์ประกอบที่แตกต่างกันไป จากองค์ประกอบใหม่ดังกล่าว จะนำค่าองค์ประกอบใหม่ที่ได้ไปใช้ในการคำนวณกับโมเดลความเสี่ยงต่อไป

4.2 การวิเคราะห์เพื่อสร้างโมเดล

จะนำข้อมูลที่ได้จากตารางน้ำหนักของปัจจัยมาเป็นข้อมูลในการวิเคราะห์ เพื่อหาความสัมพันธ์ระหว่างปัจจัยกับการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ ในการสร้างโมเดลทำนายความเสี่ยง

4.2.1 เครื่องมือที่ใช้

ผู้วิจัยเลือกใช้การวิเคราะห์การถดถอยพหุคูณโลจิสติค (Multinomial Logistic Regression) เป็นเครื่องมือสถิติในการช่วยวิเคราะห์ เพื่อจะพยากรณ์เหตุการณ์ที่สนใจซึ่งเหมาะกับข้อมูลที่เป็น Category Data โดยใช้ระดับนัยสำคัญที่ 0.05 ซึ่งเป็นระดับนัยสำคัญที่ยอมรับค่าความเชื่อถือได้ในทางสถิติและใช้โปรแกรม SPSS เป็นเครื่องมือที่ช่วยในการวิเคราะห์ ซึ่งผลการวิเคราะห์จะใช้ ตาราง Model Fitting Information เพื่อใช้ในการทดสอบโมเดล โดยพิจารณาจากค่า Sig. ที่น้อยกว่าระดับนัยสำคัญที่ตั้งไว้ และใช้ตาราง Likelihood Ratio Tests กับ ตาราง Parameter Estimate ในการพิจารณาหาความเหมาะสมของปัจจัยโดยพิจารณาจากค่า Sig. ที่น้อยกว่าระดับนัยสำคัญเช่นกัน

4.2.2 ผลการวิเคราะห์

ส่วนนี้จะเป็นผลการวิเคราะห์ โดยจะใช้ข้อมูลที่ได้จากการวิเคราะห์องค์ประกอบมาทำการวิเคราะห์เพื่อสร้างโมเดลโดยผลที่ได้จะแบ่งออกเป็นตามประเภทของภัยคุกคามมี 12 ประเภทดังนี้ (ซึ่งกล่าวไว้ในบทที่ 2 ในหัวข้อที่ 2.1)

1) ความผิดพลาดที่มาจากบุคลากรอาจจะเกิดจากอุบัติเหตุหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา (Act of human error or failure)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	38	15.2%
	โอกาสเกิดน้อย	36	14.4%
	โอกาสเกิดปานกลาง	59	23.6%
	โอกาสเกิดมาก	34	13.6%
	โอกาสเกิดมากที่สุด	83	33.2%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.2 Case Processing Summary

จากรูปที่ 4.2 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 38 ข้อมูล โอกาสเกิดน้อย จำนวน 36 ข้อมูล โอกาสเกิดปานกลาง จำนวน 59 ข้อมูล โอกาสเกิดมาก จำนวน 34 ข้อมูล และเลือกโอกาสเกิดมากที่สุด จำนวน 83 ข้อมูล หรือคิดเป็นร้อยละ 15.2,14.4, 23.6,13.6 และ 33.2 ตามลำดับ จากข้อมูลที่ใช้ในการวิเคราห์ 250 ข้อมูล โดยมีประชากรย่อยที่ใช้ในการวิเคราะห์เพื่อสร้างโมเดลจำนวน 118 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	644.331			
Final	367.938	276.393	20	.000

รูปที่ 4.3 Model Fitting Information

จากรูปที่ 4.3 จากค่า Chi-Square = 276.39 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ .05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	395.449	27.512	4	.000
Factor1	417.799	49.861	4	.000
Factor2	394.715	26.777	4	.000
Factor3	397.930	29.992	4	.000
Factor4	380.492	12.554	4	.014
Factor5	377.157	9.220	4	.056

รูปที่ 4.4 Likelihood Ratio Tests

จากรูปที่ 4.4 จากค่า Chi-Square ของ Factor1 = 49.86 Sig. = 0.00, Factor2 = 26.78 Sig. = 0.00, Factor3 = 30.00 Sig. = 0.00, Factor4 = 12.55 Sig. = 0.01 และ Factor5 = 9.220 Sig. = 0.06 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2, Factor3 และ Factor4

ระดับความเสี่ยงี้		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	13.608	3.370	16.307	1	.000			
	PC1	-.361	.104	12.096	1	.001	.697	.568	.854
	PC2	-1.375	.489	7.896	1	.005	.253	.097	.660
	PC3	-.264	.451	.343	1	.558	.768	.317	1.859
	PC4	-.644	.631	1.042	1	.307	.525	.152	1.809
	PC5	-1.564	1.185	1.742	1	.187	.209	.021	2.136
โอกาสเกิดน้อย	Intercept	6.421	3.402	3.563	1	.059			
	PC1	-.556	.106	27.651	1	.000	.574	.466	.706
	PC2	-1.466	.471	9.697	1	.002	.231	.092	.581
	PC3	1.046	.474	4.862	1	.027	2.846	1.123	7.209
	PC4	-.086	.589	.021	1	.884	.917	.289	2.913
	PC5	.852	1.180	.521	1	.470	2.344	.232	23.703
โอกาสเกิดปานกลาง	Intercept	6.467	2.960	4.773	1	.029			
	PC1	-.248	.070	12.645	1	.000	.781	.681	.895
	PC2	-.805	.449	3.206	1	.073	.447	.185	1.079
	PC3	.326	.384	.721	1	.396	1.385	.653	2.938
	PC4	-.109	.523	.043	1	.835	.897	.322	2.499
	PC5	-.109	.966	.013	1	.910	.896	.135	5.950
โอกาสเกิดมาก	Intercept	9.948	3.140	10.040	1	.002			
	PC1	-.289	.075	14.776	1	.000	.749	.647	.868
	PC2	-.734	.471	2.430	1	.119	.480	.191	1.208
	PC3	-.387	.434	.795	1	.373	.679	.290	1.589
	PC4	.700	.526	1.772	1	.183	2.013	.719	5.641
	PC5	-1.223	1.041	1.379	1	.240	.294	.038	2.266

a. The reference category is: โอกาสเกิดมากที่สุด.

รูปที่ 4.5 Parameter Estimate

จากรูปที่ 4.5 จะสามารถสร้างสมการโมเดลจากบทที่ 2 ในหัวข้อการวิเคราะห์แบบการถดถอยพหุคูณโลจิสติค ได้ดังนี้

Z1 = 13.60 + (-0.36) F1 + (-1.37) F2 + (-0.26) F3 สมการที่ 1

Z2 = 6.42 + (-0.55) F1 + (-1.46) F2+ (1.04) F3 สมการที่ 2

Z3 = 6.46 + (-0.24) F1 + (-0.80) F2+ (0.32) F3 สมการที่ 3

Z4 = 0. 9.94 + (-0.28) F1 + (-0.73) F2+ (-0.38) F3 สมการที่ 4

Z5 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 5

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$P(\text{ระดับ } 1) = \frac{e^{z1}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 2) = \frac{e^{z2}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 3) = \frac{e^{z3}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P\ (\text{ระดับ } 4) = \frac{e^{z4}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P\ (\text{ระดับ } 5) = \frac{1}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

	Predicted					
Observed	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	โอกาสเกิดมาก	โอกาสเกิดมากที่สุด	Percent Correct
โอกาสเกิดน้อยที่สุด	28	4	2	2	2	73.7%
โอกาสเกิดน้อย	2	25	7	2	0	69.4%
โอกาสเกิดปานกลาง	2	8	11	3	35	18.6%
โอกาสเกิดมาก	4	5	2	8	15	23.5%
โอกาสเกิดมากที่สุด	1	0	1	2	79	95.2%
Overall Percentage	14.8%	16.8%	9.2%	6.8%	52.4%	60.4%

รูปที่ 4.6 Classification

จากรูปที่ 4.6 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 38 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 28 ข้อมูล หรือ 73.7% มีโอกาสเกิดความเสี่ยงน้อย จาก 36 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 25 ข้อมูล หรือ 69.4% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 59 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 11 ข้อมูล หรือ 18.6% มีโอกาสเกิดความเสี่ยงมาก จาก 34 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 8 ข้อมูล หรือ 23.5% มีโอกาสเกิดความเสี่ยงมากที่สุด จาก 83 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 79 ข้อมูล หรือ 95.2% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 60.4%

2) การละเมิดทรัพย์สินทางปัญญาหรือการละเมิดลิขสิทธิ์ทางซอฟต์แวร์

(Compromises to intellectual property)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	232	92.8%
	โอกาสเกิดน้อย	18	7.2%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.7 Case Processing Summary

จากรูปภาพที่ 4.7 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 232 ข้อมูล และ โอกาสเกิดน้อย จำนวน 18 ข้อมูล หรือคิดเป็นร้อยละ 92.8 และ 7.2 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	94.350			
Final	90.911	3.439	5	.633

รูปที่ 4.8 Model Fitting Information

จากรูปที่ 4.8 จากค่า Chi-Square = 3.439 ที่ Sig. = 0.633 ซึ่งมากกว่านัยสำคัญที่กำหนดไว้คือ .05 แสดงว่าโอกาสเกิดภัยคุกคามนี้ไม่ได้ขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

3) การบุกรุก (Deliberate acts of espionage or trespass)

		N	Marginal Percentage
ระดับความเสี่ยง	**โอกาสเกิดน้อยมาก**	120	48.0%
	โอกาสเกิดน้อย	58	23.2%
	โอกาสเกิดปานกลาง	37	14.8%
	โอกาสเกิดมาก	15	6.0%
	โอกาสเกิดมากที่สุด	20	8.0%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.9 Case Processing Summary

จากรูปที่ 4.9 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 120 ข้อมูล โอกาสเกิดน้อย จำนวน 58 ข้อมูล โอกาสเกิดปานกลาง จำนวน 37 ข้อมูล โอกาสเกิดมาก จำนวน 15 ข้อมูล และเลือกโอกาสเกิดมากที่สุด จำนวน 20 ข้อมูล หรือคิดเป็นร้อยละ 48.0, 23.2, 14.8, 6.0 และ 8.0 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	562.981			
Final	258.808	304.174	20	.000

รูปที่ 4.10 Model Fitting Information

จากรูปที่ 4.10 จากค่า Chi-Square = 304.17 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	299.411	40.604	4	.000
Factor1	329.900	71.093	4	.000
Factor2	300.878	42.071	4	.000
Factor3	260.783	1.975	4	.740
Factor4	377.856	119.049	4	.000
Factor5	273.488	14.680	4	.005

รูปที่ 4.11 Likelihood Ratio Tests

จากรูปที่ 4.11 จากค่า Chi-Square ของ Factor1 = 71.09 Sig. = 0.00, Factor2 = 42.07 Sig. = 0.00, Factor3 = 1.98 Sig. = 0.74, Factor4 = 119.05 Sig. = 0.00 และ Factor5 = 14.68 Sig. = 0.01 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2, Factor4 และ Factor5

ระดับความเสี่ยงa		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยมาก	Intercept	34.107	9.454	13.016	1	.000			
	PC1	.341	.158	4.644	1	.031	1.406	1.031	1.918
	PC2	-3.576	.914	15.307	1	.000	.028	.005	.168
	PC3	-.218	1.032	.045	1	.833	.804	.106	6.078
	PC4	-11.141	2.193	25.801	1	.000	1.451E-05	1.971E-07	.001
	PC5	3.747	2.636	2.020	1	.155	42.392	.242	7432.438
โอกาสเกิดน้อย	Intercept	36.006	9.451	14.514	1	.000			
	PC1	.262	.160	2.693	1	.101	1.299	.950	1.777
	PC2	-3.515	.914	14.800	1	.000	.030	.005	.178
	PC3	-.392	1.031	.145	1	.704	.676	.089	5.101
	PC4	-10.130	2.183	21.529	1	.000	3.988E-05	5.527E-07	.003
	PC5	1.247	2.631	.225	1	.636	3.480	.020	604.079
โอกาสเกิดปานกลาง	Intercept	30.816	9.464	10.603	1	.001			
	PC1	-.083	.163	.258	1	.612	.921	.669	1.266
	PC2	-3.177	.907	12.273	1	.000	.042	.007	.247
	PC3	.066	1.048	.004	1	.950	1.068	.137	8.330
	PC4	-8.766	2.188	16.048	1	.000	.000	2.138E-06	.011
	PC5	1.711	2.737	.391	1	.532	5.532	.026	1181.985
โอกาสเกิดมาก	Intercept	4.384	8.422	.271	1	.603			
	PC1	-.564	.265	4.522	1	.033	.569	.338	.957
	PC2	-.439	.686	.409	1	.523	.645	.168	2.476
	PC3	-.076	1.257	.004	1	.952	.927	.079	10.891
	PC4	.305	1.222	.062	1	.803	1.356	.124	14.891
	PC5	-.319	3.016	.011	1	.916	.727	.002	268.080

a. The reference category is: โอกาสเกิดมากที่สุด.

รูปที่ 4.12 Parameter Estimate

จากรูปที่ 4.12 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 34.10 + (0.34) F1 + (-3.57) F2+ (-11.14) F4 สมการที่ 1

Z2 = 36.00 + (.26) F1 + (-3.51) F2+ (-10.13) F4 สมการที่ 2

Z3 = 30.81 + (-0.08) F1 + (-3.17) F2+ (-8.76) F4 สมการที่ 3

Z4 = 4.38 + (-0.56) F1 + (-0.43) F2+ (0.30) F4 สมการที่ 4

Z5 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 5

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$P(\text{ระดับ } 1) = \frac{e^{z1}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 2) = \frac{e^{z2}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 3) = \frac{e^{z3}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 4) = \frac{e^{z4}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$P(\text{ระดับ } 5) = \frac{1}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

Observed	Predicted					
	โอกาสเกิดน้อยมาก	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	โอกาสเกิดมาก	โอกาสเกิดมากที่สุด	Percent Correct
โอกาสเกิดน้อยมาก	105	7	8	0	0	87.5%
โอกาสเกิดน้อย	44	8	6	0	0	13.8%
โอกาสเกิดปานกลาง	6	1	29	1	0	78.4%
โอกาสเกิดมาก	0	0	2	13	0	86.7%
โอกาสเกิดมากที่สุด	0	0	0	2	18	90.0%
Overall Percentage	62.0%	6.4%	18.0%	6.4%	7.2%	69.2%

รูปที่ 4.13 Classification

จากรูปที่ 4.13 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 120 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 105 ข้อมูล หรือ 87.5% มีโอกาสเกิดความเสี่ยงน้อย จาก 58 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 8 ข้อมูล หรือ 13.8% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 37 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 29 ข้อมูล หรือ 78.4% มีโอกาสเกิดความเสี่ยงมาก จาก 15 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 13 ข้อมูล หรือ 86.7% มีโอกาสเกิดความเสี่ยงมากที่สุด จาก 20 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 18 ข้อมูล หรือ 90.0% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 69.2%

4) การกรรโชกข้อมูล (Deliberate acts of information extortion)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	137	54.8%
	โอกาสเกิดน้อย	86	34.4%
	โอกาสเกิดปานกลาง	27	10.8%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.14 Case Processing Summary

จากรูปที่ 4.14 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 137 ข้อมูล โอกาสเกิดน้อย จำนวน 86 ข้อมูล และโอกาสเกิดปานกลาง จำนวน 27 ข้อมูล หรือคิดเป็นร้อยละ 54.8, 34.4 และ 10.8 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	355.642			
Final	247.621	108.021	10	.000

รูปที่ 4.15 Model Fitting Information

จากรูปที่ 4.15 จากค่า Chi-Square = 108.02 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ .05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	302.258	54.637	2	.000
PC1	264.731	17.109	2	.000
PC2	301.863	54.242	2	.000
PC3	290.531	42.909	2	.000
PC4	287.742	40.121	2	.000
PC5	261.670	14.049	2	.001

รูปที่ 4.16 Likelihood Ratio Tests

จากรูปที่ 4.16 จากค่า Chi-Square ของ Factor1 = 17.11 Sig. = 0.00, Factor2 = 54.24 Sig. = 0.00, Factor3 = 42.91 Sig. = 0.00, Factor4 = 40.121 Sig. = 0.00 และ Factor5 = 14.049 Sig. = 0.00 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2, Factor4 และ Factor5

ระดับความเสี่ยง		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	33.937	6.147	30.484	1	.000			
	PC1	-.004	.092	.002	1	.966	.996	.832	1.192
	PC2	-6.692	1.234	29.424	1	.000	.001	.000	.014
	PC3	3.927	.775	25.665	1	.000	50.734	11.106	231.767
	PC4	6.010	1.272	22.314	1	.000	407.442	33.660	4931.876
	PC5	7.137	2.213	10.404	1	.001	1257.952	16.451	96188.892
โอกาสเกิดน้อย	Intercept	32.936	6.144	28.733	1	.000			
	PC1	.137	.094	2.149	1	.143	1.147	.955	1.378
	PC2	-6.727	1.234	29.730	1	.000	.001	.000	.013
	PC3	4.011	.780	26.471	1	.000	55.213	11.979	254.486
	PC4	6.043	1.273	22.532	1	.000	421.345	34.748	5109.168
	PC5	6.909	2.230	9.596	1	.002	1001.591	12.650	79303.726

รูปที่ 4.17 Parameter Estimate

จากรูปที่ 4.17 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 33.93 + (-6.69) F2 + (3.92) F3+ (6.01) F4+ (7.13) F5 สมการที่ 1

Z2 = 32.93 + (-6.72) F2 + (4.01) F3+ (6.04) F4+ (6.90) F5 สมการที่ 2

Z3 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 3

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$P(\text{ระดับ } 1) = \frac{e^{z1}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ } 2) = \frac{e^{z2}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ } 3) = \frac{1}{e^{z1}+e^{z2}+1}$$

	Predicted			
Observed	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	Percent Correct
โอกาสเกิดน้อยที่สุด	91	43	3	66.4%
โอกาสเกิดน้อย	26	57	3	66.3%
โอกาสเกิดปานกลาง	2	9	16	59.3%
Overall Percentage	47.6%	43.6%	8.8%	65.6%

รูปที่ 4.18 Classification

จากรูปที่ 4.18 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 137 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 91 ข้อมูล หรือ 66.4% มีโอกาสเกิดความเสี่ยงน้อย จาก 86 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 57 ข้อมูล หรือ 66.3% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 27 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 16 ข้อมูล หรือ 59.3% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 65.6%

5) การทำลายระบบหรือข้อมูล (Deliberate acts of sabotage or vandalism)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	52	20.8%
	โอกาสเกิดน้อย	87	34.8%
	โอกาสเกิดปานกลาง	12	4.8%
	โอกาสเกิดมาก	28	11.2%
	โอกาสเกิดมากที่สุด	71	28.4%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.19 Case Processing Summary

จากรูปที่ 4.19 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 52 ข้อมูล โอกาสเกิดน้อย จำนวน 87 ข้อมูล โอกาสเกิดปานกลาง จำนวน 12 ข้อมูล โอกาสเกิดมาก จำนวน 28 ข้อมูล และเลือกโอกาสเกิดมากที่สุด จำนวน 71 ข้อมูล หรือคิดเป็นร้อยละ 20.8, 34.8, 4.8, 11.2 และ 28.4 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	641.108			
Final	323.065	318.043	20	.000

รูปที่ 4.20 Model Fitting Information

จากรูปที่ 4.20 จากค่า Chi-Square = 318.04 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	374.260	51.195	4	.000
PC1	343.069	20.005	4	.000
PC2	354.136	31.071	4	.000
PC3	486.139	163.074	4	.000
PC4	350.920	27.855	4	.000
PC5	328.598	5.533	4	.237

รูปที่ 4.21 Likelihood Ratio Tests

จากรูปที่ 4.21 จากค่า Chi-Square ของ Factor1 = 20.00 Sig. = 0.00, Factor2 = 31.07 Sig. = 0.00, Factor3 = 163.07 Sig. = 0.00, Factor4 = 27.86 Sig. = 0.00 และ Factor5 = 5.53 Sig. = 0.24 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2, Factor3 และ Factor4

ระดับความเสี่ยง[a]		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	16.613	3.009	30.489	1	.000			
	PC1	.273	.087	9.883	1	.002	1.314	1.108	1.559
	PC2	1.093	.307	12.639	1	.000	2.982	1.633	5.447
	PC3	-5.109	.708	52.031	1	.000	.006	.002	.024
	PC4	2.667	.659	16.364	1	.000	14.394	3.954	52.402
	PC5	1.277	1.390	.845	1	.358	3.587	.235	54.696
โอกาสเกิดน้อย	Intercept	13.028	2.806	21.558	1	.000			
	PC1	.258	.070	13.768	1	.000	1.295	1.130	1.484
	PC2	1.396	.300	21.583	1	.000	4.038	2.241	7.275
	PC3	-4.362	.624	48.788	1	.000	.013	.004	.043
	PC4	2.566	.572	20.131	1	.000	13.011	4.242	39.908
	PC5	-.482	1.202	.161	1	.689	.618	.059	6.515
โอกาสเกิดปานกลาง	Intercept	.470	4.763	.010	1	.921			
	PC1	.111	.095	1.375	1	.241	1.118	.928	1.346
	PC2	1.330	.664	4.013	1	.045	3.782	1.029	13.899
	PC3	-2.390	.791	9.117	1	.003	.092	.019	.432
	PC4	1.561	.885	3.115	1	.078	4.766	.842	26.987
	PC5	.950	1.927	.243	1	.622	2.585	.059	112.994
โอกาสเกิดมาก	Intercept	4.019	2.021	3.955	1	.047			
	PC1	-.001	.060	.000	1	.992	.999	.888	1.124
	PC2	.250	.203	1.511	1	.219	1.284	.862	1.912
	PC3	-1.028	.380	7.329	1	.007	.358	.170	.753
	PC4	.573	.405	2.001	1	.157	1.774	.802	3.924
	PC5	-.939	1.129	.692	1	.406	.391	.043	3.572

a. The reference category is: โอกาสเกิดมากที่สุด.

รูปที่ 4.22 Parameter Estimate

จากรูปที่ 4.22 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 16.61+ (0.27) F1+ (1.09) F2+ (-5.10) F3+ (2.66) F4 สมการที่ 1

Z2 = 13.02+ (0.25) F1+ (1.39) F2+ (-4.36) F3+ (2.56) F4 สมการที่ 2

Z3 = .47+ (0.11) F1+ (1.33) F2+ (-2.39) F3+ (1.56) F4 สมการที่ 3

Z4 = 4.01+ (-0.00) F1+ (0.25) F2+ (-1.02) F3+ (0.57) F4 สมการที่ 4

Z5 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 5

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$\text{P (ระดับ 1)} = \frac{e^{z1}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 2)} = \frac{e^{z2}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 3)} = \frac{e^{z3}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 4)} = \frac{e^{z4}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 5)} = \frac{1}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

	Predicted					
Observed	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	โอกาสเกิดมาก	โอกาสเกิดมากที่สุด	Percent Correct
โอกาสเกิดน้อยที่สุด	38	13	0	0	1	73.1%
โอกาสเกิดน้อย	5	79	0	0	3	90.8%
โอกาสเกิดปานกลาง	0	9	0	0	3	.0%
โอกาสเกิดมาก	0	10	0	2	16	7.1%
โอกาสเกิดมากที่สุด	2	5	0	1	63	88.7%
Overall Percentage	18.0%	46.4%	.0%	1.2%	34.4%	72.8%

รูปที่ 4.23 Classification

จากรูปที่ 4.23 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 52 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 38 ข้อมูล หรือ 73.1% มีโอกาสเกิดความเสี่ยงน้อย จาก 87 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 79 ข้อมูล หรือ 90.8% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 12 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 0 ข้อมูล หรือ 0% มีโอกาสเกิดความเสี่ยงมาก จาก 28 ข้อมูลสามารถพยากรณ์ได้ถูกต้อง 2 ข้อมูล หรือ 7.1% มีโอกาสเกิดความเสี่ยงมาก

ที่สุด จาก 71 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 63 ข้อมูล หรือ 88.7% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 72.8

6) การโจรกรรม (Deliberate acts of theft)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	109	43.6%
	โอกาสเกิดน้อย	121	48.4%
	โอกาสเกิดปานกลาง	20	8.0%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.24 Case Processing Summary

จากรูปที่ 4.24 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 109 ข้อมูล โอกาสเกิดน้อย จำนวน 121 ข้อมูล โอกาสเกิดปานกลาง จำนวน 20 ข้อมูล หรือคิดเป็นร้อยละ 43.6, 48.4 และ 8.0 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	439.980			
Final	115.960	324.020	10	.000

รูปที่ 4.25 Model Fitting Information

จากรูปที่ 4.25 จากค่า Chi-Square = 324.02 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	117.275	1.314	2	.518
PC1	253.149	137.188	2	.000
PC2	118.052	2.091	2	.351
PC3	118.985	3.025	2	.220
PC4	141.103	25.142	2	.000
PC5	116.064	.104	2	.950

รูปที่ 4.26 Likelihood Ratio Tests

จากรูปที่ 4.26 จากค่า Chi-Square ของ Factor1 = 137.188 Sig. = 0.00, Factor2 = 2.09 Sig. = 0.351, Factor3 = 3.025 Sig. = 0.22, Factor4 = 25.14 Sig. = 0.00 และ Factor5 = 0.104 Sig. = 0.95 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1 และ Factor4

ระดับความเสี่ยงี้		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	4.732	4.311	1.205	1	.272			
	PC1	-.580	.133	18.989	1	.000	.560	.431	.727
	PC2	.425	.357	1.414	1	.234	1.529	.759	3.081
	PC3	-.959	.641	2.237	1	.135	.383	.109	1.347
	PC4	-2.816	.813	11.999	1	.001	.060	.012	.294
	PC5	.342	1.759	.038	1	.846	1.408	.045	44.192
โอกาสเกิดน้อย	Intercept	1.374	3.202	.184	1	.668			
	PC1	.172	.127	1.825	1	.177	1.188	.925	1.524
	PC2	.396	.341	1.353	1	.245	1.486	.762	2.898
	PC3	-.653	.458	2.036	1	.154	.520	.212	1.276
	PC4	-1.249	.549	5.175	1	.023	.287	.098	.841
	PC5	-.143	1.069	.018	1	.893	.866	.107	7.038

a. The reference category is: โอกาสเกิดปานกลาง.

รูปที่ 4.27 Parameter Estimate

จากรูปที่ 4.27 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 4.73 + (-0.58) F1 + (-2.81) F4 สมการที่ 1

Z2 = 1.37 + (0.17) F1 + (-1.24) F4 สมการที่ 2

Z3 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 3

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$P(\text{ระดับ 1}) = \frac{e^{z1}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ 2}) = \frac{e^{z2}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ 3}) = \frac{1}{e^{z1}+e^{z2}+1}$$

Observed	Predicted			
	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	Percent Correct
โอกาสเกิดน้อยที่สุด	106	3	0	97.2%
โอกาสเกิดน้อย	1	120	0	99.2%
โอกาสเกิดปานกลาง	3	11	6	30.0%
Overall Percentage	44.0%	53.6%	2.4%	92.8%

รูปที่ 4.28 Classification

จากรูปที่ 4.28 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 109 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 106 ข้อมูล หรือ 97.2% มีโอกาสเกิดความเสี่ยงน้อย จาก 121 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 120 ข้อมูล หรือ 99.2% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 20 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 11 ข้อมูล หรือ 30.0% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 92.8%

7) การโจมตีจากซอฟต์แวร์ (Deliberate software attacks)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	77	30.8%
	โอกาสเกิดน้อย	88	35.2%
	โอกาสเกิดปานกลาง	40	16.0%
	โอกาสเกิดมาก	18	7.2%
	โอกาสเกิดมากที่สุด	27	10.8%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.29 Case Processing Summary

จากรูปที่ 4.29 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 77 ข้อมูล โอกาสเกิดน้อย จำนวน 88 ข้อมูล โอกาสเกิดปานกลาง จำนวน 40 ข้อมูล โอกาสเกิดมาก จำนวน 18 ข้อมูล และเลือกโอกาสเกิดมากที่สุด จำนวน 27 ข้อมูล หรือคิดเป็นร้อยละ 30.8, 35.2, 16.0, 7.2 และ 10.8 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	600.098			
Final	263.013	337.085	20	.000

รูปที่ 4.30 Model Fitting Information

จากรูปที่ 4.30 จากค่า Chi-Square = 337.09 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	306.862	43.849	4	.000
PC1	406.123	143.110	4	.000
PC2	354.110	91.096	4	.000
PC3	280.984	17.971	4	.001
PC4	388.411	125.398	4	.000
PC5	283.149	20.136	4	.000

รูปที่ 4.31 Likelihood Ratio Tests

จากรูปที่ 4.31 จากค่า Chi-Square ของ Factor1 = 143.11 Sig. = 0.00, Factor2 = 91.10 Sig. = 0.00, Factor3 = 17.97 Sig. = 0.00, Factor4 = 125.40 Sig. = 0.00 และ Factor5 = 20.136 Sig. = 0.00 แสดงว่าโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2, Factor3, Factor4 และ Factor5

ระดับความเสี่ยงใ		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	36.910	9.207	16.071	1	.000			
	PC1	.932	.211	19.564	1	.000	2.540	1.681	3.839
	PC2	-6.435	1.573	16.727	1	.000	.002	7.346E-05	.035
	PC3	2.642	1.128	5.481	1	.019	14.041	1.538	128.212
	PC4	-11.623	2.038	32.513	1	.000	8.959E-06	1.649E-07	.000
	PC5	7.299	2.898	6.345	1	.012	1479.016	5.052	433030.917
โอกาสเกิดน้อย	Intercept	37.581	9.213	16.641	1	.000			
	PC1	1.016	.218	21.643	1	.000	2.763	1.800	4.239
	PC2	-6.692	1.577	18.015	1	.000	.001	5.645E-05	.027
	PC3	2.781	1.128	6.074	1	.014	16.139	1.767	147.381
	PC4	-11.737	2.040	33.111	1	.000	7.993E-06	1.467E-07	.000
	PC5	7.595	2.899	6.864	1	.009	1987.294	6.773	583079.468
โอกาสเกิดปานกลาง	Intercept	34.391	9.084	14.331	1	.000			
	PC1	.298	.186	2.567	1	.109	1.347	.936	1.938
	PC2	-5.250	1.533	11.726	1	.001	.005	.000	.106
	PC3	1.975	1.070	3.404	1	.065	7.205	.884	58.707
	PC4	-8.473	1.957	18.756	1	.000	.000	4.515E-06	.010
	PC5	5.022	2.770	3.287	1	.070	151.657	.666	34543.178
โอกาสเกิดมาก	Intercept	20.267	7.497	7.307	1	.007			
	PC1	-.430	.178	5.811	1	.016	.651	.459	.923
	PC2	-1.376	1.038	1.755	1	.185	.253	.033	1.934
	PC3	-.633	.963	.431	1	.511	.531	.080	3.508
	PC4	-1.707	.998	2.922	1	.087	.181	.026	1.284
	PC5	-4.835	2.914	2.752	1	.097	.008	2.628E-05	2.405

a. The reference category is: โอกาสเกิดมากที่สุด.

รูปที่ 4.32 Parameter Estimate

จากรูปที่ 4.32 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 36.91 + (0.93) F1 + (-6.43) F2 + (2.64) F3 + (-11.62) F4 + (7.29) F5 สมการที่ 1

Z2 = 37.58 + (1.01) F1 + (-6.69) F2 + (2.78) F3 + (-11.73) F4 + (7.59) F5 สมการที่ 2

Z3 = 34.39 + (0.29) F1 + (-5.25) F2 + (1.97) F3 + (-8.47) F4 + (5.02) F5 สมการที่ 3

Z4 = 20.26 + (-0.43) F1 + (-1.37) F2 + (-0.63) F3 + (-1.70) F4 + (-4.83) F5 สมการที่ 4

Z5 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 5

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$\text{P (ระดับ 1)} = \frac{e^{z1}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 2)} = \frac{e^{z2}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 3)} = \frac{e^{z3}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 4)} = \frac{e^{z4}}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

$$\text{P (ระดับ 5)} = \frac{1}{e^{z1}+e^{z2}+e^{z3}+e^{z4}+1}$$

Observed	Predicted					
	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	โอกาสเกิดมาก	โอกาสเกิดมากที่สุด	Percent Correct
โอกาสเกิดน้อยที่สุด	19	56	2	0	0	24.7%
โอกาสเกิดน้อย	16	70	2	0	0	79.5%
โอกาสเกิดปานกลาง	3	4	27	6	0	67.5%
โอกาสเกิดมาก	0	0	9	4	5	22.2%
โอกาสเกิดมากที่สุด	0	0	0	3	24	88.9%
Overall Percentage	15.2%	52.0%	16.0%	5.2%	11.6%	57.6%

รูปที่ 4.33 Classification

จากรูปที่ 4.33 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 77 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 19 ข้อมูล หรือ 24.7% มีโอกาสเกิดความเสี่ยงน้อย จาก 88 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 70 ข้อมูล หรือ 79.5% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 40 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 27 ข้อมูล หรือ 67,5 % มีโอกาสเกิดความเสี่ยงมาก จาก 18 ข้อมูลสามารถพยากรณ์ได้ถูกต้อง 4 ข้อมูล หรือ 22.2% มีโอกาสเกิดความเสี่ยงมากที่สุด จาก 5 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 27 ข้อมูล หรือ 88.9% และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 57.6%

8) ภัยธรรมชาติ (Forces of nature)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	233	93.2%
	โอกาสเกิดน้อย	17	6.8%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.34 Case Processing Summary

จากรูปที่ 4.34 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 233 ข้อมูล โอกาสเกิดน้อย จำนวน 17 ข้อมูล หรือคิดเป็นร้อยละ 93.2 และ 6.8 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	89.614			
Final	83.311	6.303	5	.278

รูปที่ 4.35 Model Fitting Information

จากรูปที่ 4.35 จากค่า Chi-Square = 6.30 ที่ Sig. = 0.29 ซึ่งมากกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นไม่ขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์หรือปัจจัยที่ใช้ในการวิเคราะห์ไม่เหมาะสมกับโมเดลนี้

9) คุณภาพของผู้ให้บริการ (Deviations in Quality of Service)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	107	42.8%
	โอกาสเกิดน้อย	36	14.4%
	โอกาสเกิดปานกลาง	21	8.4%
	โอกาสเกิดมาก	25	10.0%
	โอกาสเกิดมากที่สุด	61	24.4%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.36 Case Processing Summary

จากรูปที่ 4.36 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 107 ข้อมูล โอกาสเกิดน้อย จำนวน 36 ข้อมูล โอกาสเกิดปานกลาง จำนวน 21 ข้อมูล โอกาสเกิดมาก จำนวน 25 ข้อมูล และเลือกโอกาสเกิดมากที่สุด จำนวน 61 ข้อมูล หรือคิดเป็นร้อยละ 42.8, 14.4, 8.4, 10.0 และ 24.4 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	517.843			
Final	483.213	34.629	20	.022

รูปที่ 4.37 Model Fitting Information

จากรูปที่ 4.37 จากค่า Chi-Square = 34.63 ที่ Sig. = 0.022 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	491.958	8.745	4	.068
PC1	487.088	3.875	4	.423
PC2	486.967	3.754	4	.440
PC3	491.484	8.271	4	.082
PC4	490.374	7.161	4	.128
PC5	485.642	2.429	4	.657

รูปที่ 4.38 Likelihood Ratio Tests

จากรูปที่ 4.38 จะเห็นได้ว่าค่า Sig. = 0.00 ของแต่ละปัจจัยที่มาใช้วิเคราะห์นั้นมีค่านัยสำคัญเกินกว่าที่กำหนด ดังนั้นจึงสรุปได้ว่า โมเดลนี้ไม่เหมาะสมที่จะใช้ทำนายโอกาสการเกิดภัยคุกคามความปลอดภัย เนื่องจากการพิจารณาโมเดลในแต่ละครั้ง การเลือกใช้ตัวทดสอบโมเดลอย่างใดอย่างหนึ่งไม่ได้ เพราะมันอาจจะไม่เพียงพอต่อการเลือกโมเดลนั้น

10) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical hardware failures or errors)

		N	Marginal Percentage
ระดับความเสี่ยง	**โอกาสเกิดน้อยที่สุด**	113	45.2%
	โอกาสเกิดน้อย	94	37.6%
	โอกาสเกิดปานกลาง	43	17.2%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.39 Case Processing Summary

จากรูปที่ 4.39 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 113 ข้อมูล โอกาสเกิดน้อย จำนวน 94 ข้อมูล โอกาสเกิดปานกลาง จำนวน 43 ข้อมูล หรือคิดเป็นร้อยละ 45.2, 37.6 และ 17.2 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	450.926			
Final	130.259	320.666	10	.000

รูปที่ 4.40 Model Fitting Information

จากรูปที่ 4.40 จากค่า Chi-Square = 320.67 ที่ Sig. = 0.00 ซึ่งน้อยกว่านัยสำคัญที่กำหนดไว้คือ 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	df	Sig.
Intercept	134.128	3.869	2	.145
PC1	242.864	112.604	2	.000
PC2	137.411	7.152	2	.028
PC3	132.128	1.868	2	.393
PC4	132.610	2.351	2	.309
PC5	138.830	8.571	2	.014

รูปที่ 4.41 Likelihood Ratio Tests

จากรูปที่ 4.41 เห็นได้ว่ามีเพียงปัจจัย Factor1, Factor2 และ Factor4 เท่านั้นที่มีค่า Sig. น้อยกว่า 0.05 ดังนั้นโอกาสเกิดภัยคุกคามประเภทนี้ขึ้นอยู่กับปัจจัย Factor1, Factor2 และ Factor4

ระดับความเสี่ยงa		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B)	
								Lower Bound	Upper Bound
โอกาสเกิดน้อยที่สุด	Intercept	4.425	4.185	1.118	1	.290			
	PC1	-.791	.217	13.289	1	.000	.453	.296	.694
	PC2	-1.025	.870	1.388	1	.239	.359	.065	1.974
	PC3	.813	.727	1.252	1	.263	2.256	.543	9.374
	PC4	-.561	.959	.342	1	.559	.571	.087	3.739
	PC5	5.575	2.155	6.691	1	.010	263.667	3.861	18007.492
โอกาสเกิดน้อย	Intercept	-.018	3.599	.000	1	.996			
	PC1	-.162	.197	.674	1	.412	.851	.578	1.252
	PC2	-.170	.802	.045	1	.832	.844	.175	4.063
	PC3	.343	.625	.301	1	.583	1.409	.414	4.793
	PC4	-1.064	.789	1.821	1	.177	.345	.074	1.618
	PC5	4.000	1.859	4.628	1	.031	54.590	1.427	2088.433

a. The reference category is: โอกาสเกิดปานกลาง.

รูปที่ 4.42 Parameter Estimate

จากรูปที่ 4.42 จะสามารถสร้างสมการโมเดลได้ดังนี้

Z1 = 4.42 + (-0.79) F1 + (5.57) F5 สมการที่ 1

Z2 = -0.01 + (-0.16) F1 + (4.00) F5 สมการที่ 2

Z3 = 0 เนื่องจากเป็นฐานของการเปรียบเทียบ สมการที่ 3

จากสมการถดถอยเชิงเส้นข้างต้น จะได้สมการความน่าจะเป็นดังนี้

$$P(\text{ระดับ } 1) = \frac{e^{z1}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ } 2) = \frac{e^{z2}}{e^{z1}+e^{z2}+1}$$

$$P(\text{ระดับ } 3) = \frac{1}{e^{z1}+e^{z2}+1}$$

Observed	Predicted			
	โอกาสเกิดน้อยที่สุด	โอกาสเกิดน้อย	โอกาสเกิดปานกลาง	Percent Correct
โอกาสเกิดน้อยที่สุด	112	1	0	99.1%
โอกาสเกิดน้อย	5	81	8	86.2%
โอกาสเกิดปานกลาง	0	28	15	34.9%
Overall Percentage	46.8%	44.0%	9.2%	83.2%

รูปที่ 4.43 Classification

จากรูปที่ 4.43 แสดงความแม่นยำของการทำนายจะเห็นได้ว่า จากข้อมูลทั้งหมด 113 ข้อมูล มีโอกาสเกิดความเสี่ยงน้อยที่สุด พยากรณ์ได้ถูกต้อง 112 ข้อมูล หรือ 99.1% มีโอกาสเกิดความเสี่ยงน้อย จาก 94 ข้อมูล สามารถ พยากรณ์ได้ถูกต้อง 81 ข้อมูล หรือ 86.2% มีโอกาสเกิดความเสี่ยงปานกลาง จาก 43 ข้อมูล สามารถพยากรณ์ได้ถูกต้อง 15 ข้อมูล หรือ 34.9 % และมีโอกาสพยากรณ์ได้ถูกต้องทั้งหมด 83.2%

11) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical software failures or errors)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อย	104	41.6%
	โอกาสเกิดปานกลาง	127	50.8%
	โอกาสเกิดสูง	19	7.6%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.44 Case Processing Summary

จากรูปที่ 4.44 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 104 ข้อมูล โอกาสเกิดน้อย จำนวน 127 ข้อมูล โอกาสเกิดปานกลาง จำนวน 19 ข้อมูล หรือคิดเป็นร้อยละ 41.6, 50.8 และ 7.6 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	335.788			
Final	318.696	17.093	10	.072

รูปที่ 4.45 Model Fitting Information

จากรูปที่ 4.45 จากค่า Sig. = 0.072 ซึ่งมากกว่า 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นไม่ขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

12) เทคโนโลยีล้าสมัย (Technological obsolescence)

		N	Marginal Percentage
ระดับความเสี่ยง	โอกาสเกิดน้อยที่สุด	232	92.8%
	โอกาสเกิดน้อย	18	7.2%
Valid		250	100.0%
Missing		0	
Total		250	
Subpopulation		118	

รูปที่ 4.46 Case Processing Summary

จากรูปที่ 4.46 จากผลการวิเคราะห์จะเห็นได้ว่า ภัยคุกคามที่มีโอกาสเกิดน้อยที่สุด จำนวน 232 ข้อมูล โอกาสเกิดน้อย จำนวน 18 ข้อมูล หรือคิดเป็นร้อยละ 92.8 และ 7.2 ตามลำดับ จากข้อมูลทั้งหมด 250 ข้อมูล

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	94.350			
Final	90.911	3.439	5	.633

รูปที่ 4.47 Model Fitting Information

จากรูปที่ 4.47 จากค่า Sig. = 0.633 ซึ่งมากกว่า 0.05 แสดงว่าโอกาสเกิดภัยคุกคามนั้นไม่ขึ้นอยู่กับปัจจัยที่ใช้ในการวิเคราะห์

จากผลการวิเคราะห์ภัยคุกคามทั้ง 12 ประเภท สามารถสรุปผลการวิเคราะห์แสดงดังตารางที่ 4.4 – 4.18

ตารางที่ 4.4 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดจากการกระทำของมนุษย์

ชื่อตาราง	**ปัจจัย**	**มีความสัมพันธ์**	**ไม่มีความสัมพันธ์**
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5		✓
Parameter Estimate	F1	✓	
	F2	✓	
	F3	✓	
	F4		✓
	F5		✓

ตารางที่ 4.5 ผลวิเคราะห์ภัยคุกคามประเภทการละเมิดทรัพย์สินทางปัญญาหรือการละเมิดลิขสิทธิ์ทางซอฟต์แวร์

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-		✓

ตารางที่ 4.6 ผลวิเคราะห์ภัยคุกคามประเภทการบุกรุก

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3		✓
	F4	✓	
	F5	✓	
Parameter Estimate	F1	✓	
	F2	✓	
	F3		✓
	F4	✓	
	F5		✓

ตารางที่ 4.7 ผลวิเคราะห์ภัยคุกคามประเภทการกรรโชกข้อมูล

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5	✓	
Parameter Estimate	F1		✓
	F2	✓	

ตารางที่ 4.7 ผลวิเคราะห์ภัยคุกคามประเภทการกรรโชกข้อมูล (ต่อ)

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
	F3	✓	
	F4	✓	
	F5	✓	

ตารางที่ 4.8 ผลวิเคราะห์ภัยคุกคามประเภทการทำลายระบบหรือข้อมูล

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5		✓
Parameter Estimate	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5		✓

ตารางที่ 4.9 ผลวิเคราะห์ภัยคุกคามประเภทการโจรกรรม

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2		✓
	F3		✓
	F4	✓	
	F5		✓
Parameter Estimate	F1	✓	

ตารางที่ 4.9 ผลวิเคราะห์ภัยคุกคามประเภทการโจรกรรม (ต่อ)

	F2		✓
	F3		✓
	F4	✓	
	F5		✓

ตารางที่ 4.10 ผลวิเคราะห์ภัยคุกคามประเภทการโจมตีจากซอฟต์แวร์

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5	✓	
Parameter Estimate	F1	✓	
	F2	✓	
	F3	✓	
	F4	✓	
	F5	✓	

ตารางที่ 4.11 ผลวิเคราะห์ภัยคุกคามประเภทภัยธรรมชาติ

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-		✓

ตารางที่ 4.12 ผลวิเคราะห์ภัยคุกคามประเภทคุณภาพของผู้ให้บริการ

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1		✓
	F2		✓

ตารางที่ 4.12 ผลวิเคราะห์ภัยคุกคามประเภทคุณภาพของผู้ให้บริการ (ต่อ)

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
	F3		✓
	F4		✓
	F5		✓
Parameter Estimate	F1		✓
	F2		✓
	F3		✓
	F4		✓
	F5		✓

ตารางที่ 4.13 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-	✓	
Likelihood Ratio Tests	F1	✓	
	F2	✓	
	F3		✓
	F4		✓
	F5	✓	
Parameter Estimate	F1	✓	
	F2		✓
	F3		✓
	F4		✓
	F5	✓	

ตารางที่ 4.14 ผลวิเคราะห์ภัยคุกคามประเภทข้อผิดพลาดทางเทคนิคของซอฟต์แวร์

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-		✓

ตารางที่ 4.15 ผลวิเคราะห์ภัยคุกคามประเภทเทคโนโลยีล้าสมัย

ชื่อตาราง	ปัจจัย	มีความสัมพันธ์	ไม่มีความสัมพันธ์
Model Fitting Information	-		✓

จากตารางสรุปดังกล่าว เป็นตารางที่สรุปความความสัมพันธ์ของโมเดลและปัจจัยที่มีผลทำให้เกิดภัยคุกคาม การพิจารณาความสัมพันธ์ของโมเดลซึ่งพิจารณาได้จากตาราง Model Fitting Information หากพิจารณาแล้วพบว่าโมเดลนี้ไม่มีความสัมพันธ์ต่อการเกิดภัยคุกคามก็จะสรุปได้ว่าโมเดลนี้ไม่เหมาะสมที่จะนำมาใช้ในการทำนายและหากพิจารณาพบว่าโมเดลมีความสัมพันธ์จะต้องพิจารณาถึงปัจจัยในแต่ละตัวจากตาราง Likelihood Ratio Tests และ Parameter Estimate จากตารางที่ 4.48 – 4.59 จะเห็นได้ว่ามีโมเดลที่มีความสัมพันธ์กับการเกิดภัยคุกคามทั้งหมด 7 ประเภท ซึ่งสามารถนำใช้เพื่อทำนายความเสี่ยงของการเกิดภัยคุกคามได้ซึ่งได้แก่

1. ข้อผิดพลาดจากการกระทำของมนุษย์
2. การบุกรุก
3. การกรรโชกข้อมูล
4. การทำลายระบบหรือข้อมูล
5. การโจรกรรม
6. การโจมตีจากซอฟต์แวร์
7. ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์

จากโมเดลที่ได้ทั้ง 7 โมเดลจะนำไปสู่กระบวนการพัฒนาระบบทำนายความเสี่ยงการเกิดภัยคุกคามต่อไป

บทที่ 5
การพัฒนาระบบ

ในบทนี้จะอธิบายถึงการพัฒนาระบบทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของสารสนเทศ ซึ่งหลังจากที่ได้โมเดลที่ใช้ทำนายความเสี่ยงแล้ว จะนำโมเดลที่ได้มาเพื่อพัฒนาระบบเพื่อให้สะดวกต่อการคำนวณ การทดสอบ และให้มีประสิทธิผลมากขึ้น โดยขั้นตอนการสร้างระบบทำนายความเสี่ยงของภัยคุกคามมีดังนี้

5.1 การวิเคราะห์ระบบ

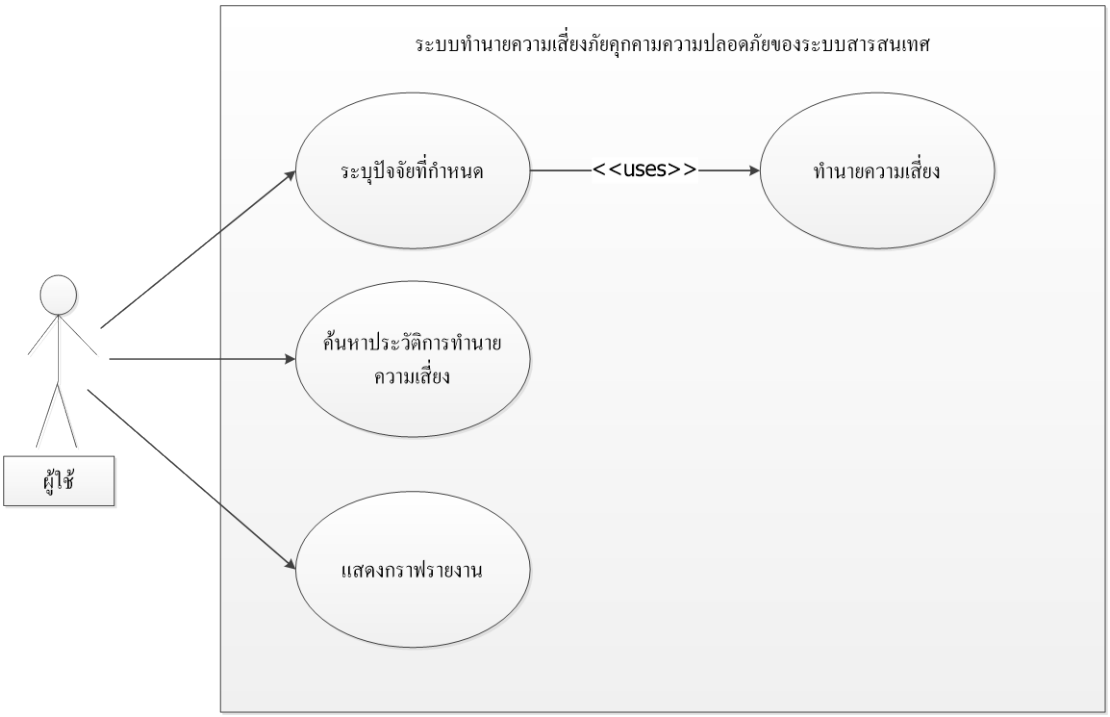
จากโมเดลและปัจจัยที่ใช้ในการทำนายความเสี่ยงผู้วิจัยสามาถสรุปข้อมูลออกมาได้เป็นความต้องการเชิงฟังก์ชันดังตารางที่ 5.1

ตารางที่ 5.1 สรุปฟังก์ชันของระบบทำนายความเสี่ยง

ลำดับ	ความต้องการเชิงฟังก์ชัน	รายละเอียด
1	การทำนายความเสี่ยง	ระบบสามารถทำนายความเสี่ยงได้จาก ปัจจัยที่ผู้ใช้ได้ระบุและจะแสดงผลการทำนายของภัยคุกคามทั้ง 7 ประเภท
2	ประวัติการทำนายย้อนหลัง	ระบบต้องสามารถดูผลการทำนายย้อนหลังได้
3	รายงานรูปแบบกราฟ	ระบบสามารถแสดงรายงานการทำนายในแต่ละครั้งได้โดยรายงานจะอยู่ในรูปของกราฟแท่ง ซึ่งจะเป็นการเปรียบเทียบระดับการเกิดภัยคุกคามของแต่ละครั้งในประเภทภัยคุกคามเดียวกัน และกราฟวงกลมจะเป็นการเปรียบเทียบภาพรวมของระดับการเกิดภัยคุกคามทั้งหมด

5.2 การออกแบบระบบทำนายความเสี่ยง

ในที่นี้จะขอเรียกผู้ที่ใช้ระบบทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศว่า ผู้ใช้ (User) ระบบจะให้ผู้ใช้งานได้กรอกข้อมูลปัจจัยตามที่กำหนดไว้ จากนั้นจะนำข้อมูลปัจจัยไปคำนวณเพื่อหาโอกาสเกิดความเสี่ยงของในแต่ละระดับของภัยคุกคาม ซึ่งมีทั้งหมด 5 ระดับ ระบบจะมียูสเคสดังรูปที่ 5.1



รูปที่ 5.1 แผนภาพยูสเคสระบบทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศ

1) ระบุปัจจัยที่กำหนด เป็นส่วนที่ให้ผู้ใช้ระบุปัจจัยจากคำถามที่ตั้งเอาไว้ เพื่อระบบจะนำข้อมูลไปใช้ในการประมวลผลต่อไป

ตารางที่ 5.2 อธิบายยูสเคส ระบุปัจจัยที่กำหนด

ชื่อยูสเคส :	ระบุปัจจัยที่กำหนด
รายละเอียด :	ผู้ใช้งานจะต้องระบุปัจจัยที่ระบบได้ทำการตั้งเอาไว้ เมื่อกรอกข้อมูลครบจะสามารถดูผลของการทำนายได้
เงื่อนไขในการทำงาน :	1. ผู้ใช้งานจะต้องล็อคอินเข้าสู่ระบบก่อน

ขั้นตอนการทำงาน :	1. ยูสเคสนี้จะเริ่มเมื่อผู้ใช้งานเลือกรายการ “ทำนายความเสี่ยง” 2. ผู้ใช้งานต้องระบุปัจจัยที่ระบบได้ตั้งไว้ตามความเป็นจริง 3. ผู้ใช้งานกดปุ่มตกลง เพื่อส่งข้อมูลให้ระบบคำนวณความเสี่ยง 4. ยูสเคสนี้จะไปเรียก ยูสเคสทำนายความเสี่ยง เพื่อส่งข้อมูลไปคำนวณผล
ผู้ใช้งาน :	ผู้มีสิทธิในการเข้าใช้งานระบบ

2) ทำนายความเสี่ยง เป็นยูสเคสที่ใช้คำนวณความเสี่ยงและแสดงผล

ตารางที่ 5.3 อธิบายยูสเคส ทำนายความเสี่ยง

ชื่อยูสเคส :	ทำนายความเสี่ยง
รายละเอียด :	ยูสเคสนี้จะนำข้อมูลที่ได้จากการระบุปัจจัยของผู้ใช้ มาคำนวณความเสี่ยงจากโมเดลที่สร้างขึ้น จากนั้นจะแสดงผลการทำนาย
เงื่อนไขในการทำงาน :	1. ผู้ใช้งานจะต้องล็อคอินเข้าสู่ระบบก่อน 2. ผู้ใช้งานต้องกรอกข้อมูลปัจจัยจากยูสเคส ระบุปัจจัยที่กำหนดให้ครบ
ขั้นตอนการทำงาน :	1. ผู้ใช้งานได้กดปุ่มตกลงจากยูสเคส ระบุปัจจัยที่กำหนด 2. ยูสเคสนี้จะนำข้อมูลปัจจัยที่ผู้ใช้ระบุทำการคำนวณผล 3. ยูสเคสแสดงผลการทำนายความเสี่ยงพร้อมกับบันทึกผลลงฐานข้อมูล
ผู้ใช้งาน :	ผู้มีสิทธิในการเข้าใช้งานระบบ

3) ประวัติการทำนายความเสี่ยง ส่วนนี้จะแสดงประวัติที่มีการเก็บบันทึกทั้งหมด

ตารางที่ 5.4 อธิบายยูสเคส แสดงรายงาน

ชื่อยูสเคส :	ค้นหาประวัติการทำนายความเสี่ยง
รายละเอียด :	จะแสดงประวัติการทำนายความเสี่ยงทั้งหมดที่ระบบมีการทำนายในแต่ละครั้ง
เงื่อนไขในการ	1. ผู้ใช้งานจะต้องล็อคอินเข้าสู่ระบบก่อน

ทำงาน :	
ขั้นตอนการทำงาน :	1. ยูสเคสนี้จะเริ่มเมื่อผู้ใช้งานเลือกเมนู ดูประวัติย้อนหลัง 2. ระบบจะแสดงรายการ การทำนายความเสี่ยงในแต่ละครั้ง 3. ผู้ใช้งานต้องเลือกรายการที่ต้องการจะดูย้อนหลัง 4. ระบบจะแสดงผลการทำนายย้อนหลัง
ผู้ใช้งาน :	-

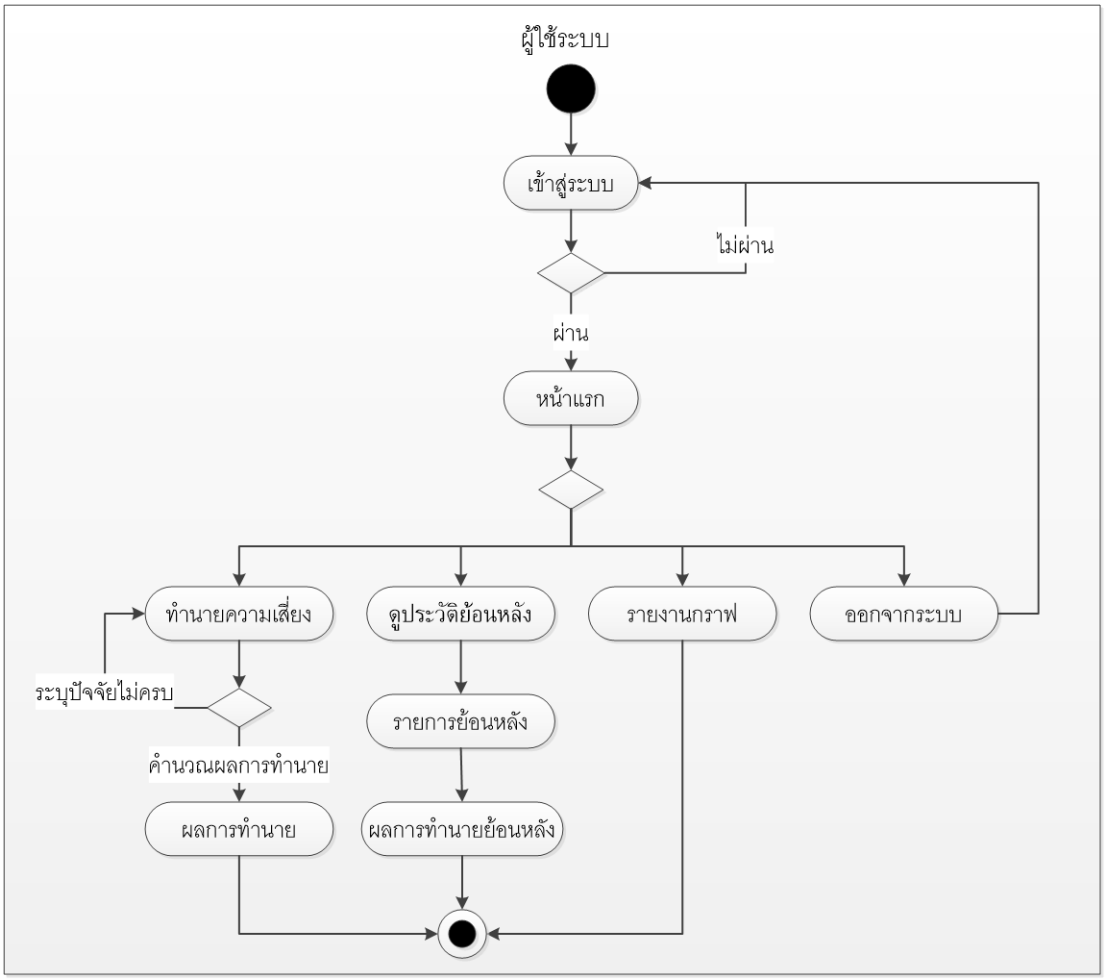
4) กราฟรายงาน ส่วนนี้จะแสดงรายงานของการเกิดภัยคุกคามในรูปแบบกราฟ

ตารางที่ 5.5 อธิบายยูสเคส กราฟรายงาน

ชื่อยูสเคส :	แสดงกราฟรายงาน
รายละเอียด :	จะแสดงรายงานเปรียบเทียบการเกิดภัยคุกคามในแต่ละครั้งและการเปรียบเทียบภาพรวมของภัยคุกคามทั้งหมด
เงื่อนไขในการทำงาน :	1. ผู้ใช้งานจะต้องล็อคอินเข้าสู่ระบบก่อน
ขั้นตอนการทำงาน :	1. ยูสเคสนี้จะเริ่มเมื่อผู้ใช้งานเลือกรายการ “รายงานแบบกราฟ” 2. ระบบจะแสดงผลการสรุปออกมาในรูปแบบกราฟ ผู้ใช้งานสามารถดูเพื่อเปรียบเทียบการเกิดภัยคุกคามในแต่ละครั้ง และเปรียบเทียบการเกิดภัยคุกคามในแต่ละประเภท
ผู้ใช้งาน :	-

5.3 การออกแบบกระบวนการทำงานของระบบ

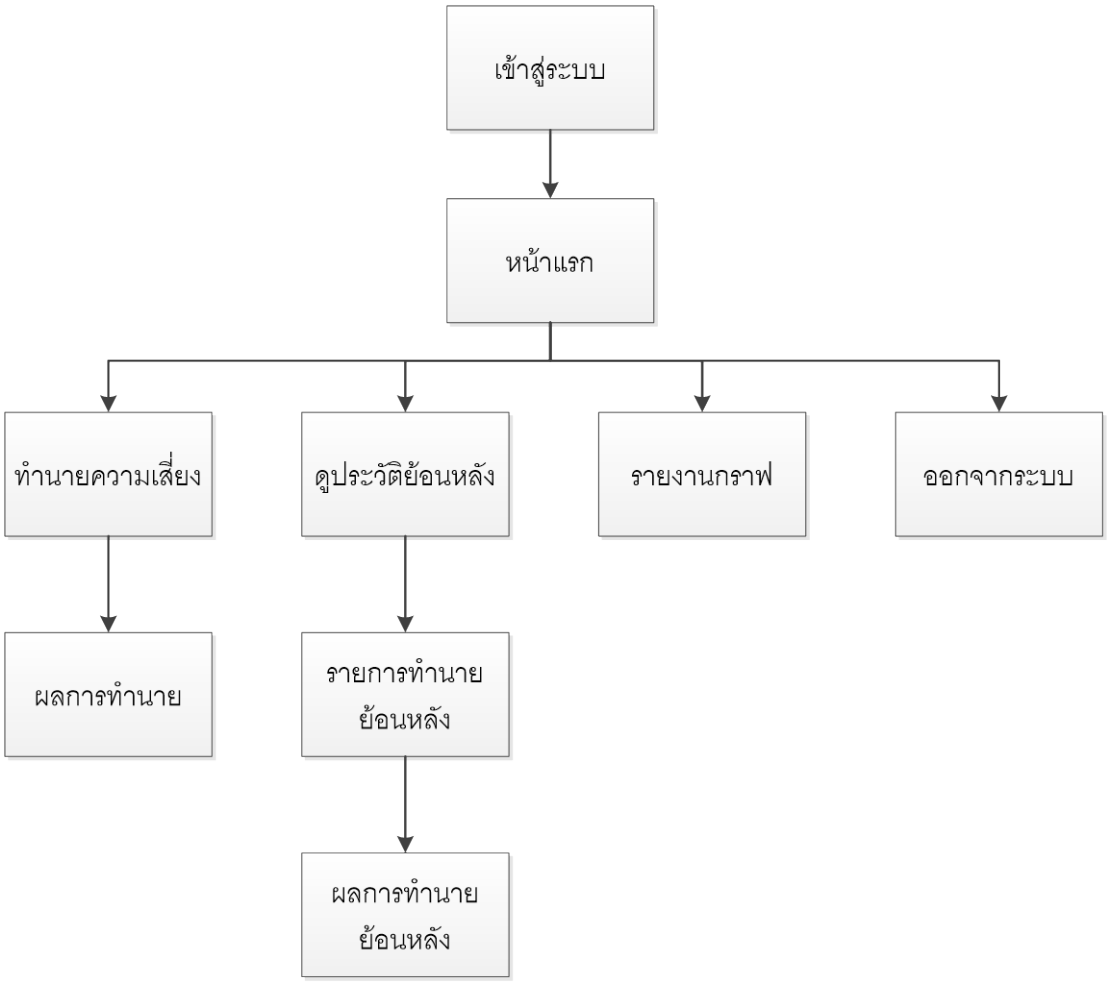
ผู้วิจัยได้ออกแบบการทำงานของระบบเพื่อให้ผู้ใช้ได้เห็นภาพการทำงานโดยรวมของระบบทำนายความเสี่ยงการเกิดภัยคุกคาม โดยแสดงดังรูปที่ 5.2



รูปที่ 5.2 แผนภาพการทำงานของระบบ

5.4 การออกแบบโครงสร้างส่วนต่อประสาน

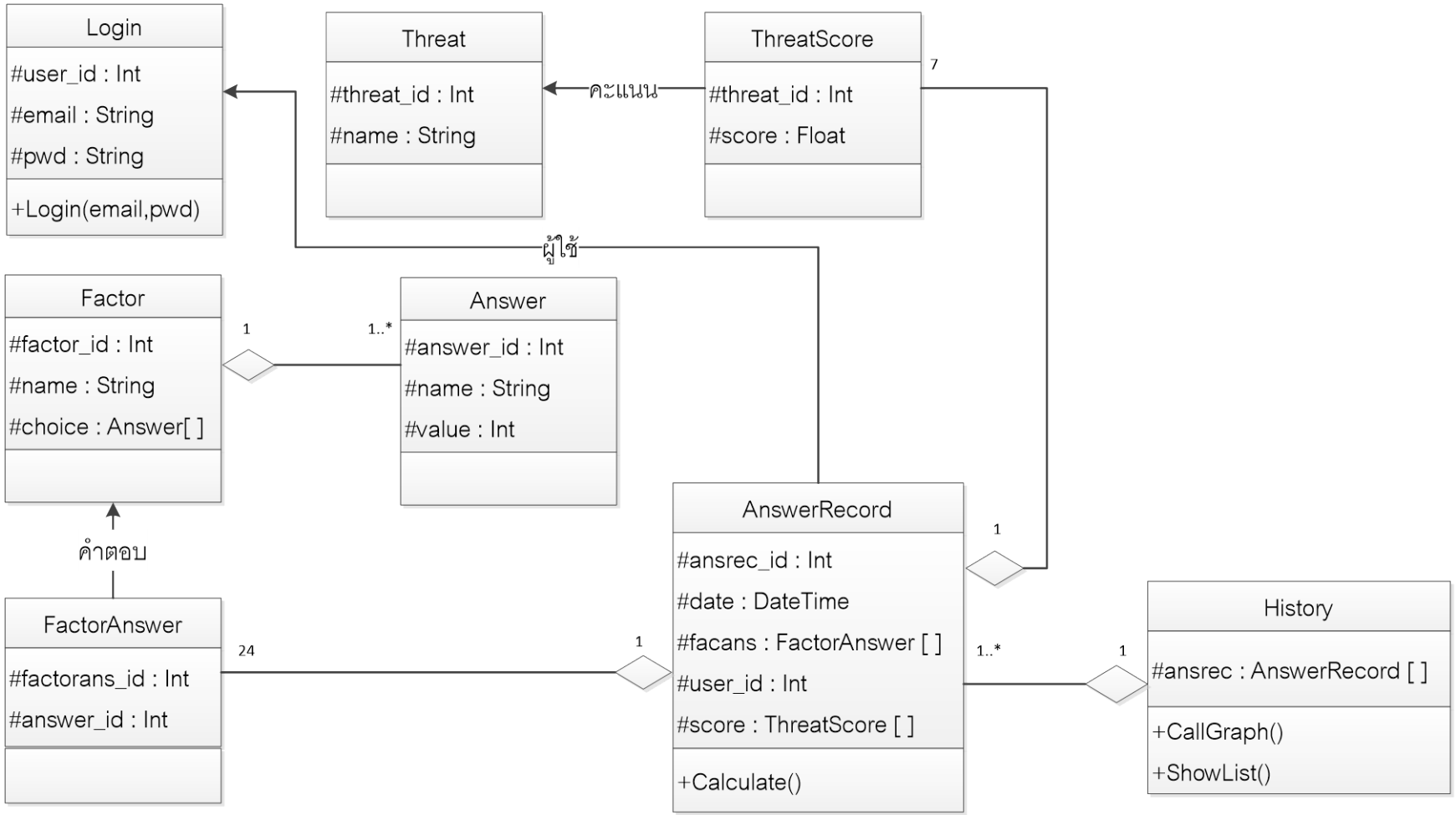
เมื่อผู้ใช้งานเข้าสู่ระบบ ระบบจะแสดงรายการเมนูให้เลือกใช้ทำงาน โดยรายการเมนูหลักจะแสดงผลอยู่ในทุกๆ หน้าของการใช้งานระบบ ทำให้ผู้ใช้งานสามารถเลือกเข้าใช้งานในแต่ละฟังก์ชันได้โดยสะดวก โครงสร้างของเมนูแสดงในรูปที่ 5.3



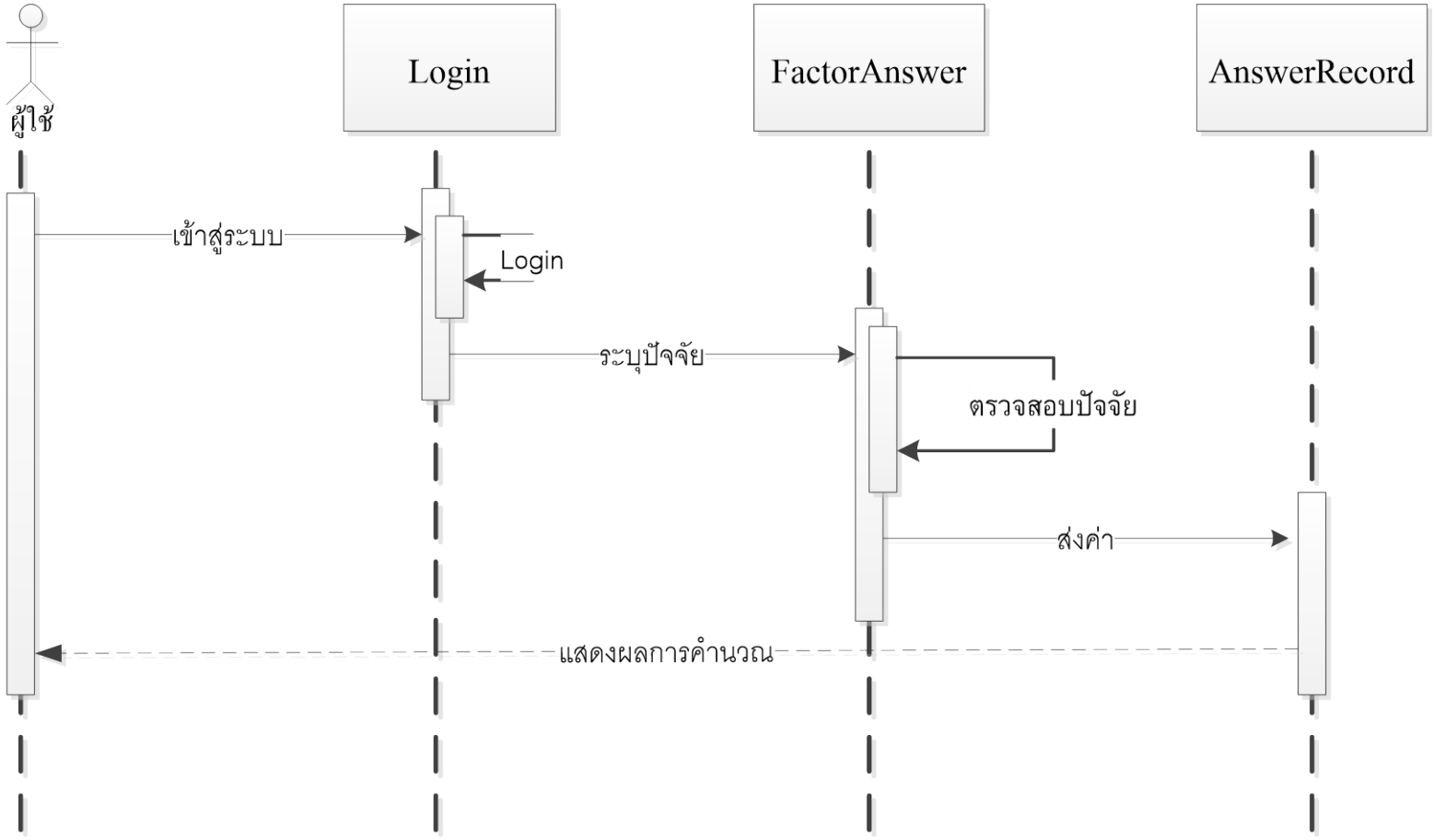
รูปที่ 5.3 แผนภาพส่วนต่อประสานงานผู้ใช้

5.5 การออกแบบไดอะแกรม

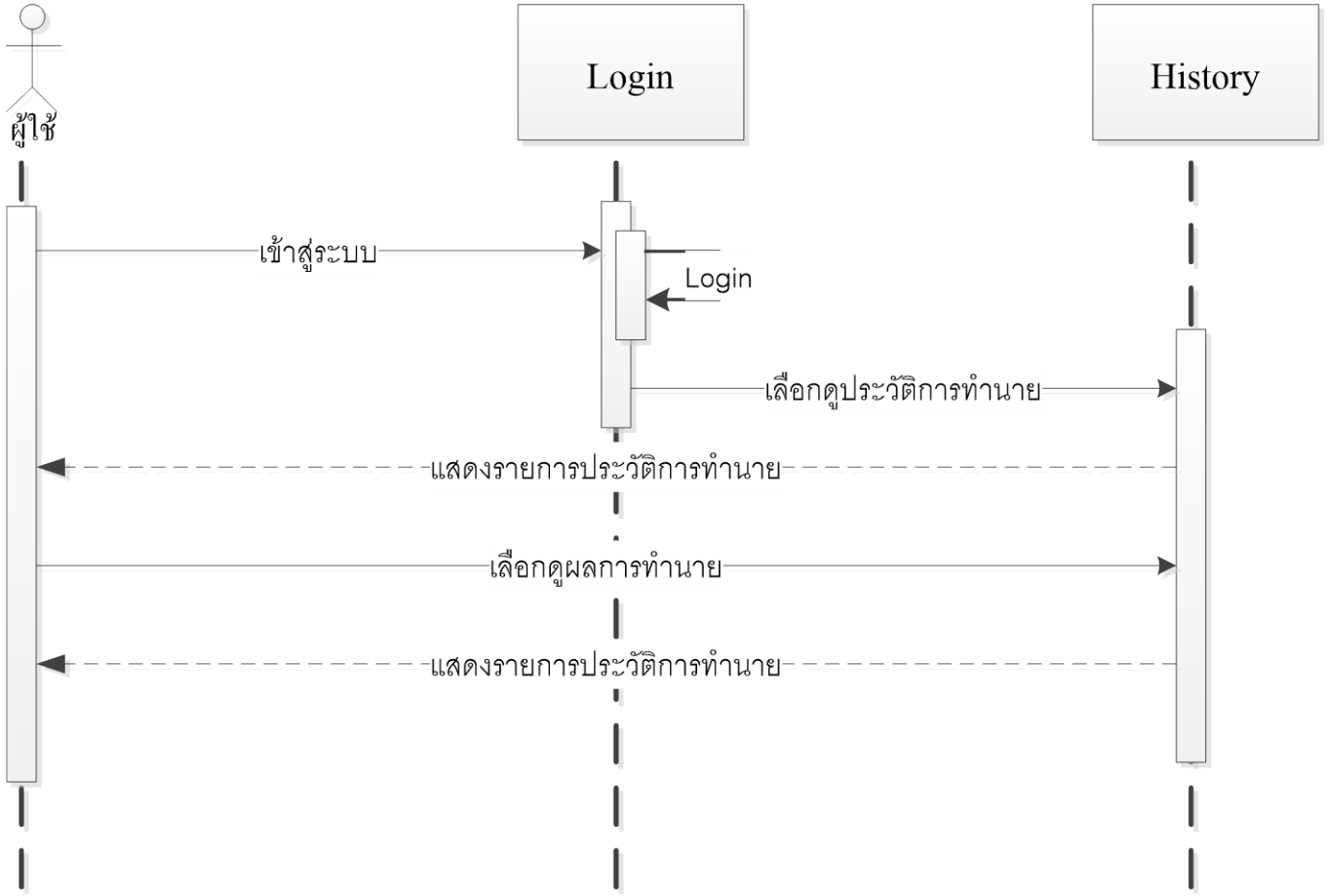
ในส่วนหัวข้อนี้จะแสดงการออกแบบไดอะแกรม ซึ่งผู้วิจัยได้มีการออกแบบไดอะแกรม 2 แบบคือ Class Diagram และ Sequence Diagram ซึ่งแสดงดังนี้



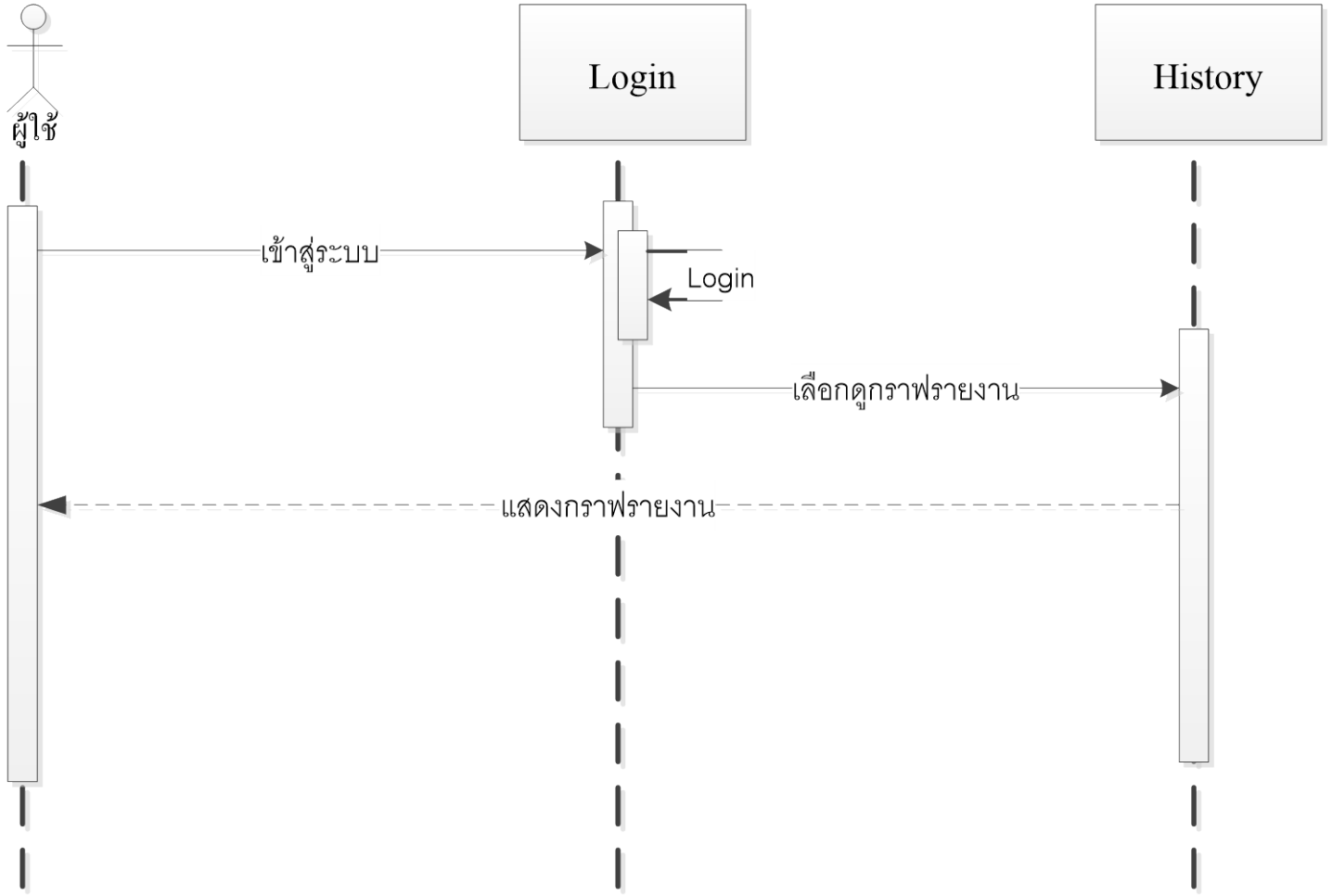
รูปที่ 5.4 Class Diagram ระบบทำนายความเสี่ยงภัยคุกคามระบบสารสนเทศ



รูปที่ 5.5 Sequence Diagram ของการทำนายความเสี่ยงภัยคุกคามระบบสารสนเทศ



รูปที่ 5.6 Sequence Diagram การแสดงประวัติการทำนาย



รูปที่ 5.7 Sequence Diagram การแสดงกราฟรายงานผลการทำนาย

จากรูปที่ 5.4 สามารถอธิบายแผนภาพ Class Diagram ได้ดังนี้

1) Login เป็นคลาสของล็อคอินเข้าสู่ระบบ

Attribute

user_id	รหัสอ้างอิงชื่อผู้ใช้
email	อีเมลล์ใช้ในการล็อคอินเข้าสู่ระบบเพื่อยืนยัน
pwd	รหัสผ่านที่ใช้ในการล็อคอิน

Operation

Login(email,pwd)	ใช้ตรวจสอบการล็อคอินเพื่อเข้าสู่ระบบ

2) Answer เป็นคลาสของตัวเลือกในปัจจัย

Attribute

answer_id	รหัสอ้างอิงตัวเลือก
name	ชื่อของตัวเลือก
value	ค่าของตัวเลือก

3) Factor เป็นคลาสของปัจจัยของการทำนายความเสี่ยง

Attribute

factor_id	รหัสอ้างอิงปัจจัย
name	ชื่อของปัจจัย
choice	ตัวเลือกของปัจจัยซึ่งเป็นประเภท Answer

4) FactorAnswer เป็นคลาสคำตอบของปัจจัย

Attribute

factorans_id	รหัสอ้างอิง
answer_id	รหัสอ้างอิงตัวเลือก

5) AnswerRecord เป็นคลาสบันทึกปัจจัย

Attribute

ansrec_id	รหัสอ้างอิง

date	วันและเวลาที่ทำการบันทึก
facans	ปัจจัยทั้ง 24 ตัวซึ่งมีประเภทเป็น FactorAnswer
user_id	รหัสอ้างอิงชื่อผู้ใช้
score	คะแนนผลการทำนายภัยคุกคามในแต่ละประเภทซึ่งมีประเภทเป็น ThreatScore

Operation

Calculate()	คำนวณผลการทำนาย

6) ThreatScore เป็นคลาสของคะแนนผลการทำนาย

Attribute

threat_id	รหัสอ้างอิงประเภทภัยคุกคาม
score	คะแนนผลการทำนาย

7) Threat เป็นคลาสของภัยคุกคาม

Attribute

threat_id	รหัสอ้างอิงประเภทภัยคุกคาม
name	ชื่อของภัยคุกคาม

8) History เป็นคลาสของประวัติในการทำนาย

Attribute

ansrec	เป็นผลการตอบปัจจัยที่ซึ่งมีประเภทเป็น AnswerRecord

Operation

CallGraph()	แสดงกราฟรายงานเปรียบเทียบ
ShowList()	แสดงรายการประวัติการทำนาย

5.6 การออกแบบการนำทาง

ผู้วิจัยได้ออกแบบหน้าจอ (หน้าจอผู้ใช้ทั้งหมดจะแสดงในภาค ผนวก ง) เพื่อให้ผู้ใช้งานได้สามารถเข้าถึงข้อมูลของระบบได้ง่าย โดยจะแสดงดังรูปที่ 5.8

จากรูปที่ 5.8 จะอธิบายหมายเลขต่างๆ ดังนี้

1) เมนูของระบบซึ่งผู้ใช้งานสามารถเข้าถึงข้อมูลต่างๆ ของระบบได้จากเมนูทางด้านซ้ายมือ

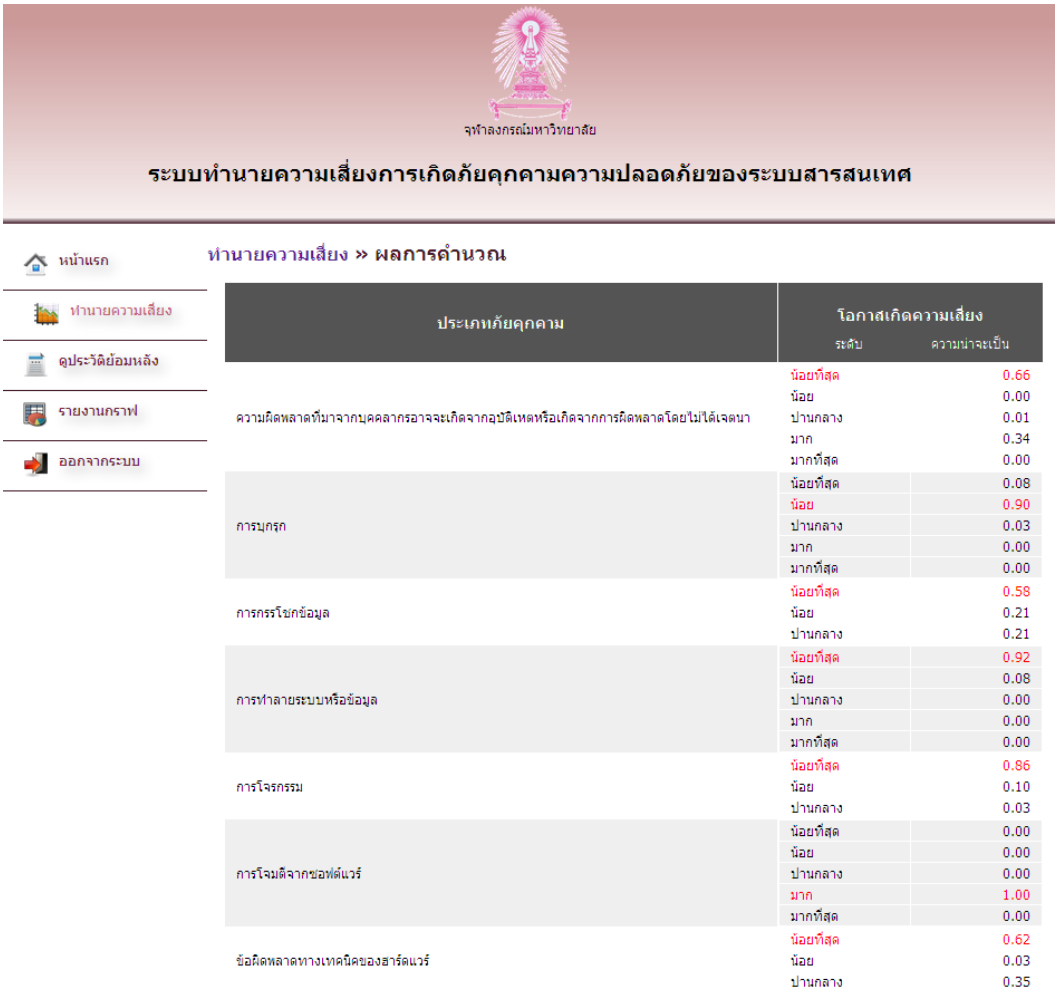
2) ส่วนแสดงหัวข้อตามเมนูหลัก ในส่วนนี้จะแสดงชื่อเมนูหลักที่กำลังใช้งานอยู่

3) ส่วนของเมนูในหน้าหลัก

รูปที่ 5.8 หน้าจอทำนายความเสี่ยง

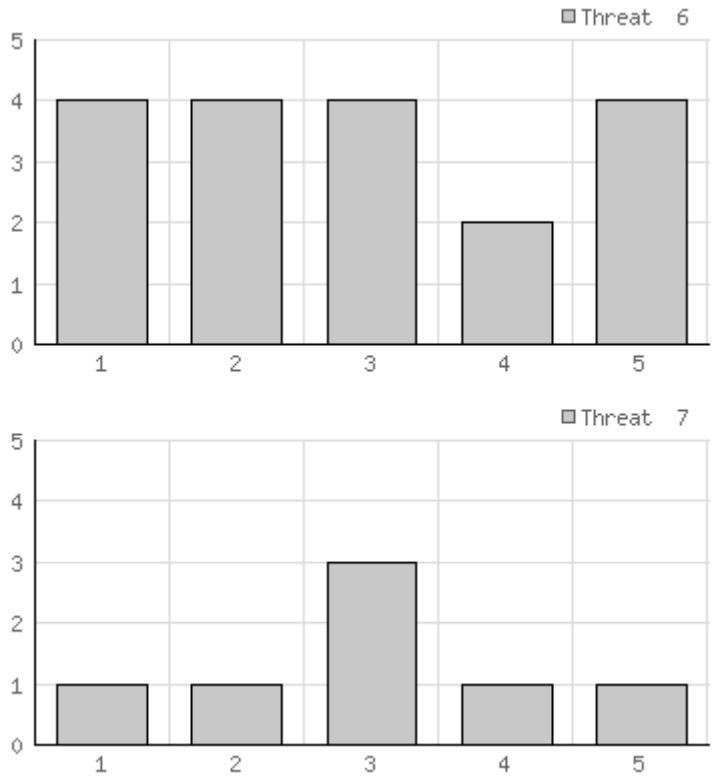
รูปที่ 5.9 หน้าจอทำนายความเสี่ยง

จากรูปที่ 5.9 เป็นรูปหน้าจอระบุปัจจัยเพื่อใช้ในการทำนายความเสี่ยง โดยจะมีตัวเลือกแบบ เลือก 1 ตัวเลือก ซึ่งผู้ใช้จะต้องระบุปัจจัยครบทุกข้อและรูปที่ 5.10 หน้าจอแสดงผลการทำนายความเสี่ยงซึ่งสีแดง หมายถึงมีโอกาสที่จะเกิดในระดับนั้นมากสุด รูปที่ 5.11 หน้าจอแสดงรายการย้อนหลังการใช้ทำนายความเสี่ยงโดยจะมีคอลัมน์วัน เวลา และผู้ใช้งานแสดง รูปที่ 5.12 กราฟแท่ง แสดงข้อมูลเปรียบเทียบการทำนายในแต่ละครั้งของภัยคุกคามแต่ละประเภท และรูปที่ 5.13 กราฟวงกลมแสดงการเปรียบเทียบภาพรวมของภัยคุกคามแต่ละประเภท

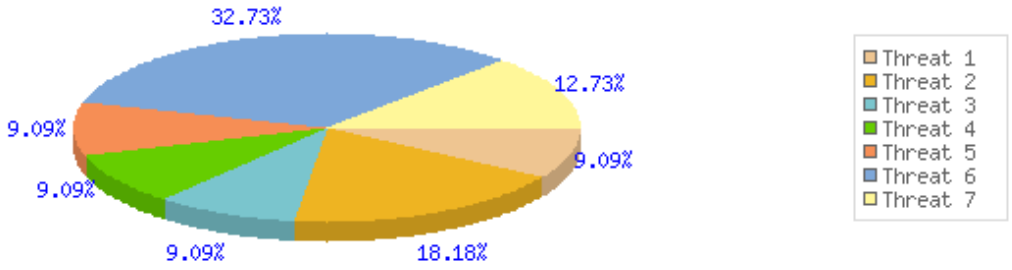


รูปที่ 5.10 หน้าจอทำนายความเสี่ยง

รูปที่ 5.11 หน้าจอทำนายความเสี่ยง



รูปที่ 5.12 หน้าจอทำนายความเสี่ยง

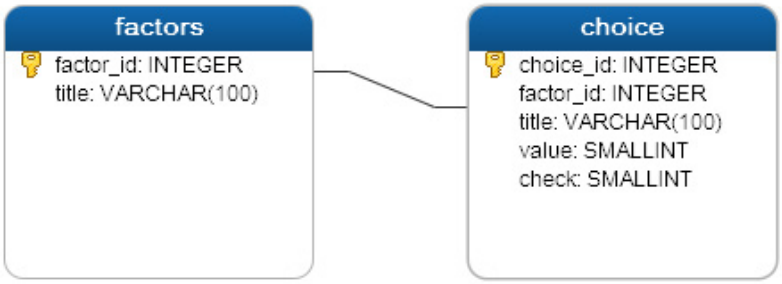


รูปที่ 5.13 หน้าจอทำนายความเสี่ยง

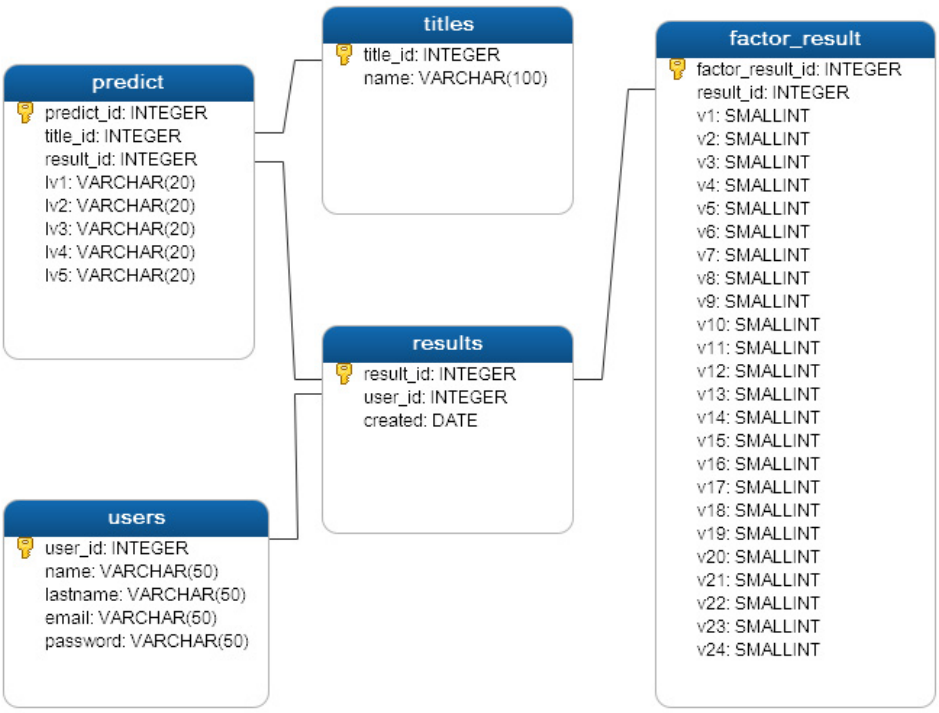
5.7 การออกแบบการจัดเก็บฐานข้อมูลและโครงสร้างของข้อมูล

ในการพัฒนาระบบจะเลือกใช้ระบบฐานข้อมูลของ MySQL ซึ่งเป็นโปรแกรมที่ใช้งานง่ายและติดตั้งสะดวกเหมาะสำหรับข้อมูลที่มีขนาดไม่ใหญ่มากและสามารถใช้งานได้กับระบบปฏิบัติการทุกระบบ อีกทั้งมีการใช้งานกันอย่างแพร่หลาย

ระบบทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้มีตาราง (Table) ที่ใช้เก็บข้อมูลซึ่งจะแสดงโครงสร้างข้อฐานข้อมูลดังรูปที่ 5.14 และ 5.15



รูปที่ 5.14 โครงสร้างและความสัมพันธ์ของตารางในฐานข้อมูล



รูปที่ 5.15 โครงสร้างและความสัมพันธ์ของตารางในฐานข้อมูล

ตารางที่ 5.6 ข้อมูลตาราง predict

ชื่อตาราง: predict (ตารางเก็บรายละเอียดผลการทำนายความเสี่ยงในแต่ละระดับ)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
id(PK)	INT	ลำดับที่ของการทำนาย
title_id(FK)	INT	ใช้อ้างอิงกับตาราง titles
result_id(FK)	INT	ใช้อ้างอิงกับตาราง results
lv1	VARCHAR(20)	ระดับภัยคุกคามที่ 1
lv2	VARCHAR(20)	ระดับภัยคุกคามที่ 2
lv3	VARCHAR(20)	ระดับภัยคุกคามที่ 3
lv4	VARCHAR(20)	ระดับภัยคุกคามที่ 4
lv5	VARCHAR(20)	ระดับภัยคุกคามที่ 5

ตารางที่ 5.7 ข้อมูลตาราง titles

ชื่อตาราง: titles (ตารางเก็บประเภทของภัยคุกคามในแต่ละประเภท)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
id(PK)	INT	ลำดับที่ของภัยคุกคาม
name	VARCHAR(100)	ชื่อประเภทภัยคุกคาม

ตารางที่ 5.8 ข้อมูลตาราง results

ชื่อตาราง: results (ตารางเก็บรายการของการทำนายในแต่ละครั้ง)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
id(PK)	INT	ลำดับที่ของการทำนายในแต่ละครั้ง
user_id(FK)	INT	ใช้อ้างอิงกับตาราง users
created	DATETIME	ชื่อประเภทภัยคุกคาม

ตารางที่ 5.9 ข้อมูลตาราง users

ชื่อตาราง: users (ตารางเก็บข้อมูลของผู้มีสิทธิใช้งานระบบ)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
id(PK)	INT	ลำดับที่ของผู้ใช้งาน

ตารางที่ 5.9 ข้อมูลตาราง users (ต่อ)

ชื่อตาราง: users (ตารางเก็บข้อมูลของผู้มีสิทธิใช้งานระบบ)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
name	VARCHAR(50)	ชื่อผู้ใช้งาน
lastname	VARCHAR(50)	นามสกุลผู้ใช้งาน
email	VARCHAR(50)	อีเมลล์ใช้ในการล็อคอิน
password	VARCHAR(50)	รหัสของในการล็อคอิน

ตารางที่ 5.10 ข้อมูลตาราง factor_result

ชื่อตาราง: factor_result (ตารางเก็บข้อมูลค่าปัจจัยที่เคยใช้งาน)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
id	INT	ลำดับที่
result_id	INT	ใช้อ้างอิงกับตาราง results
V1	SMALLINT	ค่าของปัจจัยที่ 1
V2	SMALLINT	ค่าของปัจจัยที่ 2
V3	SMALLINT	ค่าของปัจจัยที่ 3
V4	SMALLINT	ค่าของปัจจัยที่ 4
V5	SMALLINT	ค่าของปัจจัยที่ 5
V6	SMALLINT	ค่าของปัจจัยที่ 6
V7	SMALLINT	ค่าของปัจจัยที่ 7
V8	SMALLINT	ค่าของปัจจัยที่ 8
V9	SMALLINT	ค่าของปัจจัยที่ 9
V10	SMALLINT	ค่าของปัจจัยที่ 10
V11	SMALLINT	ค่าของปัจจัยที่ 11
V12	SMALLINT	ค่าของปัจจัยที่ 12
V13	SMALLINT	ค่าของปัจจัยที่ 13
V14	SMALLINT	ค่าของปัจจัยที่ 14
V15	SMALLINT	ค่าของปัจจัยที่ 15
V16	SMALLINT	ค่าของปัจจัยที่ 16

ตารางที่ 5.10 ข้อมูลตาราง factor_result (ต่อ)

ชื่อตาราง: factor_result (ตารางเก็บข้อมูลค่าปัจจัยที่เคยใช้งาน)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
V17	SMALLINT	ค่าของปัจจัยที่ 17
V18	SMALLINT	ค่าของปัจจัยที่ 18
V19	SMALLINT	ค่าของปัจจัยที่ 19
V20	SMALLINT	ค่าของปัจจัยที่ 20
V21	SMALLINT	ค่าของปัจจัยที่ 21
V22	SMALLINT	ค่าของปัจจัยที่ 22
V23	SMALLINT	ค่าของปัจจัยที่ 23
V24	SMALLINT	ค่าของปัจจัยที่ 24

ตารางที่ 5.11 ข้อมูลตาราง factors

ชื่อตาราง: factors (ตารางเก็บข้อมูลของ factor ทั้งหมดเพื่อใช้ในการทำนายในระบบ)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
Id(PK)	INT	ลำดับที่
title	VARCHAR(100)	ชื่อของปัจจัย

ตารางที่ 5.12 ข้อมูลตาราง choice

ชื่อตาราง: choice (ตารางเก็บข้อมูลของตัวเลือกของปัจจัยต่าง ๆ)		
ชื่อ ฟิลด์	**ชนิดข้อมูล**	**รายละเอียด**
Id(PK)	INT	ลำดับที่ของตัวเลือก
factor_id(FK)	INT	ใช้อ้างอิงกับตาราง factors
title	VARCHAR(100)	ชื่อของตัวเลือก
value	SMALLINT	ค่าของตัวเลือก
check	SMALLINT	ใช้ระบุในการเลือก

5.8 การพัฒนาระบบ

ในการพัฒนาระบบทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้ใช้เทคโนโลยีในลักษณะเว็บ (Web Application) เพื่อให้รองรับการทำงานผ่านระบบเครือข่ายได้และผู้ใช้งานสามารถใช้งานได้สะดวกและสามารถเรียกใช้งานผ่านเว็บบราวเซอร์ โดยไม่จำเป็นต้องติดตั้งระบบ

5.8.1 เครื่องมือที่ใช้ในการพัฒนา

เครื่องมือที่ใช้จะพัฒนาระบบนี้ผู้วิจัยจะใช้ Labtop ในการพัฒนาะระบบทำนายความเสี่ยงและติดตั้งระบบจำลองเซิร์ฟเวอร์ภายในเครื่อง โดยมีการเรียกใช้งานผ่านบราวเซอร์ รายละเอียดจะประกอบไปด้วยดังตารางที่ 5.13

ตารางที่ 5.13 เครื่องมือที่ใช้ในการพัฒนา

รายการ	**รายละเอียด**
เครื่องมือช่วยในการพัฒนา	NetBeans เวอชั่น 6.9.1
ภาษา	PHP 5.2.6
เซิ ร์ ฟเวอร์	Apache 2.2.8
ฐานข้อมูล	MySQL 5.0.51b
บราวเซอร์	Mozilla Fire Fox 18.0.2

5.8.2 สภาพแวดล้อมในการพัฒนา

ในการพัฒนาระบบผู้วิจัยได้พัฒนาระบบโดยใช้ Laptop รุ่น Satellite 160 ซึ่งมีสภาพแวดล้อมของเครื่องที่ใช้ในการพัฒนาดังตารางที่ 5.14

ตารางที่ 5.14 สภาพแวดล้อมในการพัฒนา

รายการ	**รายละเอียด**
ประเภทหน่วยประมวลผล	Intel(R) Core(Tm)2 Duo CPU T6600
ความเร็วหน่วยประมวลผล	2.20 GHz
ระบบปฏิบัติการ	Microsoft Window XP 2009
หน่วยความจำ	4.0 GB

บทที่ 6
ผลการทดสอบ

การนำเสนอในบทนี้เป็นการกล่าวถึงการทดสอบโมเดลทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศเพื่อตรวจสอบความแม่นยำในการทำนายของโมเดลที่ได้ โดยผู้วิจัยได้ทำการทดสอบโมเดลที่ได้จากการวิเคราะห์ซึ่งมีรายละเอียดดังต่อไปนี้

6.1 ข้อมูลการทดสอบ

ในการทดสอบโมเดลทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศผู้วิจัยได้ใช้ข้อมูลที่ได้แบ่งจากการตอบแบบสอบถามเชิงลึกในช่วงต้นมาใช้ในการทดสอบโมเดล ซึ่งมีจำนวน 48 ข้อมูล (ข้อมูลที่ใช้ทดสอบจะแสดงในภาคผนวก ข) โดยผู้วิจัยจะใช้ข้อมูลทั้งหมดนี้ทดสอบโมเดลทำนายความเสี่ยงทั้ง 7 โมเดล

6.2 สภาพแวดล้อมในการทดสอบ

การทดสอบโมเดลทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ ผู้วิจัยได้ใช้สภาพแวดล้อมเดียวกับการพัฒนาระบบโดยมีรายละเอียด ดังตารางที่ 6.1

ตารางที่ 6.1 สภาพแวดล้อมในการพัฒนา

รายการ	รายละเอียด
ประเภทหน่วยประมวลผล	Intel(R) Core(Tm)2 Duo CPU T6600
ความเร็วหน่วยประมวลผล	2.20 GHz
ระบบปฏิบัติการ	Microsoft Window XP 2009
หน่วยความจำ	4.0 GB

6.3 สรุปผลการทดสอบ

การทดสอบโมเดลทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศทำขึ้นเพื่อตรวจสอบความถูกต้องและความแม่นยำของการทำนายโมเดลทั้ง 7 โดยใช้ข้อมูลจำนวน 48 ข้อมูล ในการทดสอบของการทำนายความแม่นยำโดยใช้ระบบที่ผู้วิจัยได้พัฒนาขึ้น ซึ่งผลการทดสอบในแต่ละข้อมูลจะแสดงตัวอย่างดังรูปที่ 6.1

ประเภทภัยคุกคาม	โอกาสเกิดความเสี่ยง	
	ระดับ	ความน่าจะเป็น
ความผิดพลาดที่มาจากบุคคลากรอาจจะเกิดจากอุบัติเหตหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา	น้อยที่สุด	0.66
	น้อย	0.00
	ปานกลาง	0.02
	มาก	0.32
	มากที่สุด	0.00
การบุกรุก	น้อยที่สุด	0.08
	น้อย	0.89
	ปานกลาง	0.03
	มาก	0.00
	มากที่สุด	0.00
การกรรโชกข้อมูล	น้อยที่สุด	0.75
	น้อย	0.25
	ปานกลาง	0.00
การทำลายระบบหรือข้อมูล	น้อยที่สุด	0.80
	น้อย	0.20
	ปานกลาง	0.00
	มาก	0.00
	มากที่สุด	0.00
การโจรกรรม	น้อยที่สุด	0.92
	น้อย	0.06
	ปานกลาง	0.02
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 6.1 ตัวอย่างของการทดสอบความแม่นยำของโมเดล

จากรูปที่ 6.1 เป็นตัวอย่างผลการทดสอบโมเดลกับข้อมูลที่ใช้ในการทดสอบแต่ละข้อมูล โดยที่ตัวหนังสือสีแดงในช่องโอกาสเกิดความเสี่ยง จะเป็นตัวที่บอกถึงระดับการเกิดภัยคุกคามนั้นที่ได้จากการทำนายของโมเดล ซึ่งจากผลการทำนายนี้จะนำมาเปรียบเทียบกับระดับการเกิดภัยคุกคามที่ได้จากข้อมูลทดสอบ หากมีระดับการเกิดภัยคุกคามที่ตรงกันหรือมีค่าใกล้เคียงกันถือว่าผ่าน โดยตัวอย่างผลการเปรียบเทียบจะแสดงดังตารางที่ 6.2

ตารางที่ 6.เปรียบเทียบผลการทดสอบโมเดลจากข้อมูล 1 ชุด

ประเภทโมเดล	**ระดับภัยคุกคามจากข้อมูลทดสอบ**	**ระดับภัยคุกคามจากผลการทำนาย**	**ผ่าน**	**ไม่ผ่าน**
ข้อผิดพลาดจากการกระทำของมนุษย์	น้อย	น้อยที่สุด	✓	
การบุกรุก	น้อย	น้อย	✓	

ตารางที่ 6.2 เปรียบเทียบผลการทดสอบโมเดลจากข้อมูล 1 ชุด (ต่อ)

ประเภทโมเดล	ระดับภัยคุกคามจากข้อมูลทดสอบ	ระดับภัยคุกคามจากผลการทำนาย	ผ่าน	ไม่ผ่าน
การกรรโชกข้อมูล	น้อยที่สุด	น้อยที่สุด	✓	
การทำลายระบบหรือข้อมูล	น้อยที่สุด	น้อยที่สุด	✓	
การโจรกรรม	มาก	น้อยที่สุด		✓
การโจมตีจากซอฟต์แวร์	ปานกลาง	มากที่สุด		✓
ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์	น้อยที่สุด	น้อยที่สุด	✓	

จากผลการทดสอบโมเดลกับข้อมูลทั้งหมด 48 ข้อมูลซึ่งผู้วิจัยได้สรุปผลการสอบทดสอบโดยจะแสดงดังตารางที่ 6.3

ตารางที่ 6.3 ผลการทดสอบโมเดลทำนายความเสี่ยง

ประเภทภัยคุกคาม	ผ่าน	ไม่ผ่าน	ความสอดคล้อง(%)
ข้อผิดพลาดจากการกระทำของมนุษย์(T_1)	24	24	50.00
การบุกรุก (T_2)	38	10	79.17
การกรรโชกข้อมูล (T_3)	32	16	66.67
การทำลายระบบ (T_4)	21	27	43.75
การโจรกรรม (T_5)	40	8	83.33
การโจมตีจากซอฟต์แวร์ (T_6)	44	4	91.67
ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (T_7)	45	3	93.75

ผ่าน หมายถึง ระดับของการภัยคุกคามที่ได้จากการทำนายกับข้อมูลจริงตรงกัน

ไม่ผ่าน หมายถึง ระดับของการภัยคุกคามที่ได้จากการทำนายกับข้อมูลจริงไม่ตรงกัน

ความสอดคล้อง หมายถึง ความถูกต้องในโมเดลที่ใช้ทดสอบกับชุดข้อมูลทดสอบโดยคิดเป็นร้อยละของข้อมูล 48 ข้อมูล

จากตารางที่ 6.3 ผลการทดสอบของโมเดลที่ได้ พบว่าจากข้อมูลทั้งหมด 48 ข้อมูล โมเดลของภัยคุกคามประเภทข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ มีความสอดคล้องมากที่สุด โดยคิดเป็นร้อยละ 93.75 ประเภทการโจมตีจากซอฟต์แวร์ มีความสอดคล้องร้อยละ 91.67 ประเภทการโจรกรรม มีความสอดคล้องร้อยละ 83.33 ประเภทการบุกรุก มีความสอดคล้องร้อยละ 79.17 ประเภทการกรรโชกข้อมูล มีความสอดคล้องร้อยละ 66.67 ประเภทข้อผิดพลาดจากการกระทำของมนุษย์ มีความสอดคล้องร้อยละ 50.00 และประเภทการทำลายระบบ มีความสอดคล้องน้อยสุดร้อยละ 43.75 ตามลำดับ

บทที่ 7
สรุปผลการวิจัยและข้อเสนอแนะ

7.1 สรุปผลการวิจัย

งานวิจัยนี้เป็นการหาปัจจัยและสร้างโมเดลสำหรับทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยทั้ง 12 ประเภท มีการเก็บข้อมูลโดยใช้แบบสอบถาม ซึ่งแบบสอบถามจะแบ่งออกเป็น 2 ส่วน คือ แบบสอบถามสำหรับสำรวจปัจจัยของการเกิดภัยคุกคามและแบบสอบถามเชิงลึกสำหรับใช้วิเคราะห์เพื่อสร้างโมเดล จากนั้นจะนำข้อมูลที่ได้จากแบบสอบถามเชิงลึกเข้าสู่กระบวนการวิเคราะห์ ซึ่งกระบวนการวิเคราะห์จะแบ่งเป็น 2 ส่วน คือ การวิเคราะห์องค์ประกอบและการวิเคราะห์เพื่อสร้างโมเดลที่ใช้ทำนายความเสี่ยง โดยจะแบ่งขั้นตอนการทำงานออกเป็น 3 ส่วน คือ

ส่วนที่ 1 การออกแบบสอบถามเพื่อเก็บรวบรวมข้อมูลใช้แบบสอบถาม 2 ชุด

ชุดแรก เป็นแบบสอบถามที่ใช้ในการสำรวจหาปัจจัย มีกลุ่มตัวอย่างเป็นบุคลากรที่มีความรู้ด้านคอมพิวเตอร์จำนวน 117 คน โดยแบบสอบถามจะเป็นลักษณะปลายปิดและปลายเปิด คือจะมีสามารถเลือกได้ว่า ปัจจัยที่ระบุในแบบสอบถามนี้เป็นสาเหตุของการเกิดภัยคุกคามหรือไม่ โดยปัจจัยที่ระบุในแบบสอบถามจะได้มาจาก หนังสือและงานวิจัยต่างๆ และสามารถเขียนแสดงความคิดเห็นปัจจัยอื่นๆ เพิ่มเติมได้นอกเหนือจากปัจจัยที่กำหนด

ชุดสอง แบบสอบถามเชิงลึกจะใช้ข้อมูลจากแบบสอบถามชุดแรก เพื่อวิเคราะห์และสร้างโมเดลโดยใช้กลุ่มตัวอย่างเป็นบุคลากรที่มีความรู้ด้านคอมพิวเตอร์จำนวน 298 คน และผู้วิจัยได้แบ่งระดับการเกิดภัยคุกคามออกเป็น 5 ระดับ คือ น้อยที่สุด น้อย ปานกลาง มาก และมากที่สุด ข้อมูลในส่วนนี้จะแบ่งออกเป็น 2 ส่วน ส่วนแรก ไว้สำหรับวิเคราะห์ 80% ส่วนสอง ไว้สำหรับทดสอบโมเดลที่ได้ 20%

ส่วนที่ 2 การวิเคราะห์ข้อมูลเพื่อสร้างโมเดลทำนายความเสี่ยง ในการวิเคราะห์จะแบ่งเป็น 2 ขั้นตอน คือ

ขั้นตอนที่ 1 การวิเคราะห์องค์กอบเพื่อลดจำนวนปัจจัย โดยใช้ Factor Analysis ซึ่งต้องใช้วิธี Polychoric Correlation ในการหาความสัมพันธ์ของปัจจัยแต่ะตัวโดยใช้ โปรแกรม R เป็นเครื่องมือช่วยในการวิเคราะห์โดยจำนวนปัจจัยที่ใช้ในการวิเคราะห์องค์ประกอบมีทั้งหมด 24

ปัจจัย และจากปัจจัยดังกล่าวเมื่อนำไปวิเคราะห์องค์ประกอบจะได้องค์ประกอบใหม่ทั้งหมด 5 องค์ประกอบ ซึ่งกล่าวไว้ในบทที่ 3

ขั้นตอนที่ 2 การวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงซึ่งจะใช้ Multinomial Logistic Regression ในการวิเคราะห์และใช้โปรแกรม SPSS ในเป็นเครื่องมือในการช่วยวิเคราะห์ จากผลการวิเคราะห์จะได้โมเดลที่เหมาะสมทั้งหมด 7 โมเดล และผลการทดสอบโมเดลกับชุดข้อมูลที่ใช้ทดสอบ มีความถูกต้องของการทดสอบโดยคิดเป็นร้อยละดังนี้

ความผิดพลาดที่มาจากบุคลากร	50.00
การบุกรุก	79.17
การกรรโชกข้อมูล	66.67
การทำลายระบบ	43.75
การโจรกรรม	83.33
การโจมตีจากซอฟต์แวร์	91.67
ข้อผิดพลาดทางฮาร์ดแวร์	93.75

ส่วนที่ 3 การสร้างระบบทำนายความเสี่ยง

ระบบทำนายความเสี่ยงจะเป็นการนำเอาโมเดลที่ได้จากการวิเคราะห์ในเบื้องต้นมาพัฒนาเป็นระบบทำนายความเสี่ยง เพื่อให้สะดวกต่อการใช้งานซึ่งระบบจะถูกพัฒนาโดยภาษา PHP ซึ่งจะเป็น Web Application สามารถเปิดทำงานได้ด้วย บราวเซอร์ เพื่อง่ายต่อการใช้งานโดยไม่ต้องติดตั้งระบบ ฟังก์ชันการทำงานหลักของระบบมีดังนี้

1) ฟังก์ชันการทำนายความเสี่ยง
2) ฟังก์ชันการแสดงประวัติการทำนาย
3) ฟังก์ชันแสดงรายงานในรูปแบบกราฟ

7.2 ปัญหาและอุปสรรคในการวิจัย

เนื่องจากงานวิจัยนี้มีข้อมูลเป็นประเภทตัวแปรกลุ่มจึงไม่สามารถใช้การวิเคราะห์ Factor Analysis แบบปกติบน SPSS ได้เนื่องจากการใช้ Factor Analysis บน SPSS จะใช้การหาความสัมพันธ์ของปัจจัยโดยวิธี Principal Component ซึ่งไม่เหมาะสมกับข้อมูลในงานวิจัยนี้ ผู้วิจัยจึงเปลี่ยนวิธีการหาความสัมพันธ์โดยใช้ Polychoric Correlation บน โปรแกรม R แทน และจำนวนปัจจัยที่มากจึงต้องใช้ข้อมูลที่มีจำนวนมากตาม ทำให้ต้องเก็บรวบรวมข้อมูลและใช้เวลา

เก็บข้อมูลมากขึ้น อีกทั้งในงานวิจัยนี้มีการวิเคราะห์ภัยคุกคามทั้ง 12 ประเภท ซึ่งอาจจะทำให้การหาปัจจัยของภัยคุกคามในแต่ละประเภทไม่ครอบคลุม รวมถึงภัยคุกคามบางประเภทมีปัจจัยที่เกิดจากภายนอกองค์กรที่ไม่สามารถควบคุมได้ [5]

7.3 **ข้อเสนอแนะ**

งานวิจัยนี้เป็นการศึกษาหาปัจจัยและสร้างโมเดลเพื่อใช้ทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ ทั้งหมด 12 ประเภท จากการวิจัยจะเห็นว่าการวิเคราะห์สร้างโมเดลนั้นสามารถสร้างโมเดลได้เพียง 7 โมเดล ซึ่งอาจมีหลายสาเหตุด้วยกันดังนี้

1) จำนวนปัจจัยที่ไม่ครอบคลุม

2) ข้อมูลที่ไม่มีจำกัด

3) ภัยคุกคามบ้างประเภทอาจจะมีปัจจัยที่มาจากภายนอกซึ่งไม่สามารถควบคุมได้

ผู้วิจัยจึงเสนอให้เลือกภัยคุกคามที่สำคัญหรือสนใจขึ้นมาประเภทหนึ่งจากทั้งหมด 12 ประเภท เพื่อที่จะได้ศึกษาและวิเคราะห์ภัยคุกคามนั้นอย่างละเอียดและอาจจะเปลี่ยนจากการทำนายระดับการเกิดภัยคุกคามเป็นความเสียหายขององค์กร

รายการอ้างอิง

[1] กัลยา วานิชย์บัญชา. การใช้ SPSS for Windows ในการวิเคราะห์ข้อมูล. กรุงเทพฯ: บริษัทธรรมสาร, 2548

[2] ธวัชชัย วรพงศธร. เทคนิคของวิธีวิเคราะห์การถดถอยพหุแบบโลจิสติกส์. วารสารวิจัยวิทยาศาสตร์การแพทย์, 2533

[3] ยุทธ ไกยวรรณ์. วิเคราะห์ข้อมูลวิจัย step by step SPSS 4. ศูนย์สื่อเสริมกรุงเทพ, 2552

[4] เศรษฐพงศ์ มะลิสุวรรณ. การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ. [ออนไลน์]. 2552. แหล่งที่มา: our-teacher.com/our-teacher/article/1article/index.htm

[5] สังสิทธิ์ เดชน้อย. ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อแผ่นซีดีละเมิดลิขสิทธิ์ของผู้บริโภคในเขตกรุงเทพมหานคร. [ออนไลน์].
แหล่งที่มา: nenfe.nfe.go.th/elearning/courses/89/section4.pdf

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

[7] Chaoju Hu and Chunmei Lv. Method of Risk Assessment Based on Classified Security Protection and Fuzzy Neural Network, IEEE Xplore, 2010

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

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

[10] Professor Andy Field. Factor Analysis for Likert/Ordinal/Non-normal Data. [Online]. Available from: methodspace.com/profiles/blogs/ factor-analysis-for-likert-ordinal-non-normal-data

[11] Richardson R. CSI Computer Crime & Security Survey. [Online]. Available from: http://gocsi.com, 2008

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

[13] Mary S. Information Security Threats: A Comparative Analysis of Impact, Probability and Preparedness. Taylor & Francis, 2009

ภาคผนวก

ภาคผนวก ก

แบบสอบถาม

ก.1 แบบสอบถามสำรวจหาปัจจัยของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ

หลักสูตรวิทยาศาสตรมหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะ วิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

แบบสอบถาม ข้อมูลเกี่ยวกับปัจจัยที่มีผลกระทบทำให้เกิดภัยคุกคามความด้านปลอดภัยของระบบคอมพิวเตอร์

วัตถุประสงค์ **เพื่อเก็บรวบรวมข้อมูลที่เป็นปัจจัย ของการเกิดภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์และนำไปวิเคราะห์เพื่อพัฒนาระบบทำนายความเสี่ยงของภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์**

คำชี้แจง กรุณาใส่เครื่องหมาย ✓ หน้าข้อความที่ตรงกับข้อเท็จจริงหรือความคิดเห็นของท่านมากที่สุด

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. ตำแหน่งงานปัจจุบัน

❒ Programmer ❒ Systems Analyst ❒ Information Officer

❒ Security Officer ❒ Network Administrator ❒ Database Administrator

❒ Help Desk Support ❒ Technician ❒ Trainer & Teacher

❒ Web Designer & Developer ❒ อื่นๆ.....

2. วุฒิการศึกษาสูงสุด

❒ ต่ำกว่าปริญญาตรี ❒ ปริญญาตรี ❒ สูงกว่าปริญญาตรี

3. อายุการทำงานที่เกี่ยวข้องกับอาชีพสายคอมพิวเตอร์

❒ ต่ำกว่า 1 ปี ❒ 1 – 5 ปี

❒ 6 – 10 ปี ❒ 11 – 20 ปี

❒ มากกว่า 20 ปี

4. ท่านเคยประสบปัญหากับเหตุการณ์ภัยคุกคามด้านความปลอดภัยคอมพิวเตอร์

❒ เคย ❒ ไม่เคย

5. ท่านเคยติดตามข่าวสารเกี่ยวกับความปลอดภัยคอมพิวเตอร์บ้างหรือไม่ ถ้าท่านติดตาม ติดตามจากสื่อใด (ตอบได้มากกว่า 1 ข้อ)

❒ หนังสือพิมพ์ ❒ นิตยสาร ❒ วิทยุ

❒ โทรทัศน์ ❒ อินเทอร์เน็ต ❒ อื่นๆ.....

ส่วนที่ 2 ให้ทำเครื่องหมาย ✓ หน้าข้อความที่ท่านเห็นว่าเป็นปัจจัยที่ทำให้เกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์

ใช่	ปัจจัย
	1. ไม่มีระบบป้องกัน Network เช่น Firewall Anti Virus เป็นต้น
	2. ไม่มีการ update โปรแกรมป้องกันความปลอดภัยอย่างสม่ำเสมอ
	3. อายุการใช้งาน Hardware มีอายุเกิน 5 ปี
	4. Hardware ตั้งในที่ที่มีผลทำให้เสียหายไวขึ้น
	5. จำนวนเครื่อง Server ในองค์กรที่มากเกินความจำเป็น
	6. ไม่มีการป้องกันการเข้าถึงของไฟล์ข้อมูลที่สำคัญขององค์กร
	7. ไม่มีการ back up ไฟล์ข้อมูล
	8. ความขัดแย้งส่วนตัวของเพื่อนร่วมงาน
	9. บุคลากรไม่ใส่ใจเรื่องความปลอดภัยของระบบคอมพิวเตอร์
	10. บุคลากรมีความรู้ด้านความปลอดภัยของคอมพิวเตอร์ไม่เพียงพอ

ใช่	ปัจจัย
	11. ไม่ตั้งรหัสผ่านให้กับคอมพิวเตอร์ที่ตนเองใช้ในองค์กร
	12. มีการใช้คอมพิวเตอร์ร่วมกันกับผู้อื่นในองค์กร
	13. เปิดเผยรหัสผ่านให้กับผู้อื่น
	14. มีการเก็บรหัสผ่านที่สำคัญที่คนอื่นสามาถเข้าถึงได้
	15. มีการสั่งงานโดยใช้ email
	16. องค์กรไม่มีการอบรมความรู้ด้านความปลอดภัยคอมพิวเตอร์ให้กับบุคคลากร
	17. อายุขององกรค์ที่น้อย
	18. ไม่มีการใช้มาตราฐาน ISO มาใช้ควบคุมความปลอดภัยของคอมพิวเตอร์ในองค์กร
	19. องค์กรไม่มีนโยบายเรื่องความปลอดภัยของระบบคอมพิวเตอร์
	20. องค์กรไม่ลงโทษผู้ที่ฝ่าฝืนนโยบายความปลอดภัยขององค์กร
	21. ไม่มีการแบ่งหน้าที่การทำงานกันชัดเจน
	22. งบประมาณด้านความปลอดภัยของคอมพิวเตอร์ไม่เพียงพอ
	23. ผู้บริหารหรือหัวหน้าไม่สนับสนุนเรื่องของภัยคุกคามของคอมพิวเตอร์
	24. มีการใช้ Outsource ในองค์กร

ส่วนที่ 3 หากท่านเห็นว่ามีปัจจัยอื่นที่ทำให้เป็นสาเหตุของการเกิดภัยคุกคามด้านความปลอดภัยระบบคอมพิวเตอร์โปรดระบุเพิ่มเติม

……

……

……

……

……

……

……

ขอกราบขอบพระคุณที่ท่านได้ให้ความอนุเคราะห์ในการตอบแบบสอบถามนี้

ก.2 แบบสอบถามเชิงลึกเพื่อใช้ในการวิเคราะห์การทำนายโอกาสการเกิดภัยคุกคามความปลอดภัยของระบบคอมพิวเตอร์

หลักสูตรวิทยาศาสตรมหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์

แบบสอบถาม ข้อมูลเกี่ยวกับการเกิดภัยคุกคามความด้านปลอดภัยของระบบคอมพิวเตอร์

วัตถุประสงค์ เพื่อเก็บรวบรวมข้อมูลการเกิดภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์และนำไปวิเคราะห์เพื่อพัฒนาระบบทำนายความเสี่ยงของภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์

คำชี้แจง กรุณาใส่เครื่องหมาย ✓ หน้าข้อความที่ตรงกับข้อเท็จจริงหรือความคิดเห็นของท่านมากที่สุด

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. ตำแหน่งงานปัจจุบัน

❒ Programmer ❒ Systems Analyst ❒ Information Officer
❒ Security Officer ❒ Network Administrator ❒ Database Administrator
❒ Help Desk Support ❒ Technician ❒ Trainer & Teacher
❒ Web Designer & Developer ❒ IT Manager ❒ อื่นๆ.....

2. วุฒิการศึกษาสูงสุด

❒ ต่ำกว่าปริญญาตรี ❒ ปริญญาตรี ❒ สูงกว่าปริญญาตรี

3. อายุการทำงานที่เกี่ยวข้องกับอาชีพสายคอมพิวเตอร์

❒ ต่ำกว่า 1 ปี ❒ 1 – 5 ปี ❒ 6 – 10 ปี
❒ 11 – 20 ปี ❒ มากกว่า 20 ปี

4. ท่านเคยประสบปัญหากับเหตุการณ์ภัยคุกคามด้านความปลอดภัยคอมพิวเตอร์

❒ เคย ❒ ไม่เคย

5. ท่านเคยติดตามข่าวสารเกี่ยวกับความปลอดภัยคอมพิวเตอร์บ้างหรือไม่ ถ้าท่านติดตาม ติดตามจากสื่อใด (ตอบได้มากกว่า 1 ข้อ)

❒ หนังสือพิมพ์ ❒ นิตยสาร ❒ วิทยุ

❒ โทรทัศน์ ❒ อินเทอร์เน็ต ❒ อื่นๆ

6. องค์กรที่ท่านทำงานอยู่ในปัจจุบันนี้เคยประสบปัญหากับเหตุการณ์ภัยคุกคามด้านความปลอดภัยคอมพิวเตอร์

❒ เคย ❒ ไม่เคย

7. ประเภทขององค์กร

.....

ส่วนที่ 2 ข้อมูลปัจจัยของภัยคุกคามด้านความปลอดภัยของคอมพิวเตอร์ภายในองค์กร

1. การป้องกันในระบบเครือข่ายคอมพิวเตอร์ เช่น ไฟร์วอลล์ และ แอนตี้ไวรัส เป็นต้น

❒ มี ❒ ไม่มี

2. การอัพเดทระบบป้องกันความปลอดภัยในระบบคอมพิวเตอร์

❒ ไม่เคย ❒ มีบ้างเป็นบางครั้ง ❒ ทุกครั้งที่มีการให้อัพเดท

3. อายุการใช้งานฮาร์ดแวร์ในองค์กร

❒ 1-2 ปี ❒ 3-4 ปี ❒ ตั้งแต่ 5 ปีขึ้นไป

4. สภาพแวดล้อมของที่ตั้งฮาร์ดแวร์

❒ สภาพแวดล้อมที่เหมาะสม ❒ สภาพแวดล้อมไม่เหมาะสม เช่น กระแสไฟฟ้าไม่คงที่, มีความชื้นสูง,ร้อนอากาศถ่ายเทไม่สะดวก,ฝุ่นเยอะ เป็นต้น

5. จำนวนเครื่องเซิร์ฟเวอร์ในองค์กร

❒ 1-2 เครื่อง ❒ 3-4 เครื่อง ❒ มากกว่า 4 เครื่อง

6. การป้องกันการเข้าถึงของไฟล์ข้อมูลที่สำคัญขององค์กร

❒ มีการป้องกัน ❒ มีการป้องกันแต่ไม่ดีพอยังสามารถเข้าถึงได้

❒ ไม่มีการป้องกัน

7. การแบ็คอัพข้อมูล

❒ รายวัน ❒ รายสัปดาห์ ❒ รายปี

❒ ไม่มีการแบ็คอัพ

8. ความขัดแย้งส่วนตัวของเพื่อนร่วมงานภายในองค์กร

❒ มี ❒ มีเป็นบ้างครั้ง ❒ ไม่มี

9. ความใส่ใจเรื่องความปลอดภัยของระบบคอมพิวเตอร์

❒ มี ❒ มีเป็นบ้างครั้ง ❒ ไม่มี

10. ไม่มีผู้รับผิดชอบหรือมีความชำนาญดูแลในส่วนของความปลอดภัยของคอมพิวเตอร์

❒ ใช่ ❒ ไม่ใช่

11. การตั้งรหัสคอมพิวเตอร์เครื่องที่ตัวเองใช้ในองค์กร

❒ มี ❒ ไม่มี

12. การใช้คอมพิวเตอร์ร่วมกันกับผู้อื่นในองค์กร

❒ ใช้ร่วมกันทุกครั้ง ❒ ใช้ร่วมกันบ้างเป็นบางครั้ง ❒ ใช้คนเดียว

13. มีการเปิดเผยรหัสผ่านให้กับผู้อื่นทั้งตั้งใจและไม่ตั้งใจ

❒ ใช่ ❒ ไม่ใช่

14. มีการเก็บรหัสผ่านที่สำคัญที่คนอื่นสามาถเข้าถึงได้

❒ ใช่ ❒ ไม่ใช่

15. มีการสั่งงานหรือคำสั่งต่างๆ โดยใช้อีเมลล์

❒ ทุกครั้ง ❒ เกือบทุกครั้ง

❒ เป็นบางครั้ง ❒ ไม่เคย

16. การอบรมความรู้ด้านความปลอดภัยคอมพิวเตอร์ให้กับบุคลากร

❒ มีการอบรมอย่างสม่ำเสมอ ❒ มีการอบรมบ้างเป็นบางครั้ง

❒ ไม่มีการอบรม

17. อายุขององค์กรท่าน

❒ 1-5 ปี ❒ 6-10 ปี ❒ มากกว่า10 ปี

18. นโยบายเรื่องความปลอดภัยของระบบคอมพิวเตอร์

❒ มีบังคับใช้อย่างจริงจัง ❒ มีแต่ไม่บังคับใช้อย่างจริงจัง ❒ ไม่มี

19. การลงโทษผู้ที่ฝ่าฝืนนโยบายความปลอดภัยขององค์กร

❒ มีการลงโทษอย่างเคร่งครัด ❒ มีการลงโทษบ้างเป็นบางครั้ง

❒ ไม่มีการลงโทษ

20. การแบ่งหน้าที่การทำงาน

❒ มีการแบ่งหน้าที่กันชัดเจน ❒ ไม่มีการแบ่งหน้าที่ที่ชัดเจน

21. งบประมาณด้านความปลอดภัยของคอมพิวเตอร์ไม่เพียงพอ

❒ ใช่ ❒ ไม่ใช่

22. ผู้บริหารหรือหัวหน้าไม่สนับสนุนเรื่องของภัยคุกคามของคอมพิวเตอร์

❒ ใช่ ❒ ไม่ใช่

23. การใช้เอาท์ซอสในองค์กร

❒ ใช่ ❒ ไม่ใช่

24. ระบบการสนับสนุนของระบบสารสนเทศอื่นๆ ไม่มีประสิทธิภาพ เช่น อินเทอร์เน็ต , ไฟฟ้า , การสื่อสาร เป็นต้น

❒ ใช่ ❒ ไม่ใช่

ส่วนที่ 3 ข้อมูลอัตราการเกิดภัยคุกคามด้านคอมปลอดภัยของคอมพิวเตอร์ภายในองค์กร

ภัยคุกคาม	จำนวนครั้งการเกิดภัยคุกคามต่อเดือน				
	0-4 ครั้ง	ระหว่าง 5 - 11 ครั้ง	ระหว่าง 12 - 18 ครั้ง	ระหว่าง 19 - 25 ครั้ง	มากกว่า 26 ครั้ง
1. **ความผิดพลาดที่มาจากบุคคลากรอาจจะเกิดจากอุบัติเหตหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา**					
ระบบเกิดการผิดพลาดหรือไม่สามารถดำเนินการต่อได้					
ข้อมูลสูญหายหรือไม่ถูกต้อง					
รหัสที่สำคัญถูกเปิดเผย					
อื่นๆ…… ……..					
2. **การละเมิดทรัพย์สินทางปัญญาหรือการละเมิดลิขสิทธิ์ทางซอฟต์แวร์**					
การถูกลักลอบใช้ซอฟแวร์ขององค์กรตนเองโดยไม่ได้รับอนุญาติหรือผิดกฎหมาย					
อื่นๆ……					
3. **การบุกรุก**					
โดนแอบลักลอบใช้คอมพิวเตอร์ของตนเองจากผู้อื่น					
อื่นๆ……					
4. **การกรรโชกข้อมูล**					
มีการข่มขู่กรรโชกข้อมูลสารสนเทศ					
อื่นๆ……					
5. **การทำลายระบบหรือข้อมูล**					
โดนทำลายระบบหรือข้อมูลจนไม่สามารถดำเนินงานต่อได้					

ภัยคุกคาม	จำนวนครั้งการเกิดภัยคุกคามต่อเดือน				
	0-4 ครั้ง	ระหว่าง 5 - 11 ครั้ง	ระหว่าง 12 - 18 ครั้ง	ระหว่าง 19 - 25 ครั้ง	มากกว่า 26 ครั้ง
โดนลบข้อมูลออกจากระบบจนไม่สามารถกู้คืนมาได้					
อื่นๆ.....					
6. **การโจรกรรม**					
ฮาร์ดแวร์ขององค์กรโดนขโมยทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์					
ข้อมูลที่สำคัญขององค์กรโดนขโมย					
โดนหลอกลวงเพื่อล้วงเอาความลับทางข้อมูล					
อื่นๆ.....					
7. **การโจมตีจากซอฟต์แวร์**					
มีไวรัสทำให้ระบบคอมพิวเตอร์ที่ใช้งานมีปัญหาหรือประสิทธิภาพความไวช้าลง					
ถูกขัดขวางจนไม่สามารถดำเนินการทำงานต่อได้					
อื่นๆ.....					
8. **ภัยธรรมชาติ**					
เครื่องคอมพิวเตอร์เสียหายเนื่องมากจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ฟ้าฝ่า					
อื่นๆ.....					
9. **คุณภาพของผู้ให้บริการ**					
ไฟฟ้าดับบ่อยจนทำให้ระบบคอมพิวเตอร์ไม่สามารถดำเนินการต่อได้					
อินเทอร์เน็ตล้มไม่สามารถใช้งานหรือเชื่อมต่อได้					
อื่นๆ.....					
10. **ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์**					
การเสื่อมการใช้งานของฮาร์ดแวร์					
ฮาร์ดแวร์เกิดความเสียหายทำให้ระบบไม่สามารถดำเนินการต่อไป					
อื่นๆ.....					
11. **ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์**					
ซอฟต์แวร์ที่ใช้มีปัญหาทำให้ต้องหยุดการทำงานหรือการทำงานล่าช้ากว่าปกติ					

ภัยคุกคาม	จำนวนครั้งการเกิดภัยคุกคามต่อเดือน				
	0-4 ครั้ง	ระหว่าง 5 - 11 ครั้ง	ระหว่าง 12 - 18 ครั้ง	ระหว่าง 19 - 25 ครั้ง	มากกว่า 26 ครั้ง
มีช่องโหว่จนสามารถทำให้เกิดภัยคุกคามได้					
อื่นๆ.....					
12. **เทคโนโลยีล้าสมัย**					
มีการทำงานช้าหรือผิดพลาดจนไม่สามารถบรรลุวัตถุประสงค์ได้					
เทคโนโลยีที่มีอยู่ไม่สามารถป้องกันภัยคุกคามที่จะเกิดขึ้นได้					
อื่นๆ.....					

ภาคผนวก ข.
ผลสรุปการตอบแบบสอบถาม

ตารางที่ ข.1 ผลสรุปที่ได้จากการสำรวจปัจจัยการเกิดความเสี่ยงของภัยคุกคามด้านความปลอดภัยระบบคอมพิวเตอร์

ปัจจัย	จำนวน	ร้อยละ
1. การป้องกันในระบบเครือข่ายคอมพิวเตอร์ เช่น ไฟร์วอลล์ และ แอนตี้ไวรัส เป็นต้น	92	78.63
2. การอัพเดทระบบป้องกันความปลอดภัยในระบบคอมพิวเตอร์	90	76.96
3. อายุการใช้งานฮาร์ดแวร์ในองค์กร	40	34.19
4. สภาพแวดล้อมของที่ตั้งฮาร์ดแวร์	28	23.93
5. จำนวนเครื่องเซิร์ฟเวอร์ในองค์กร	22	18.80
6. การป้องกันการเข้าถึงของไฟล์ข้อมูลที่สำคัญขององค์กร	79	67.52
7. การแบ็คอัพข้อมูล	72	61.54
8. ความขัดแย้งส่วนตัวของเพื่อนร่วมงานภายในองค์กร	40	34.19
9. ความใส่ใจเรื่องความปลอดภัยของระบบคอมพิวเตอร์	84	71.79
10. ไม่มีผู้รับผิดชอบหรือมีความชำนาญดูแลในส่วนของความปลอดภัยของคอมพิวเตอร์	75	64.10
11. การตั้งรหัสคอมพิวเตอร์เครื่องที่ตัวเองใช้ในองค์กร	35	29.91
12. การใช้คอมพิวเตอร์ร่วมกันกับผู้อื่นในองค์กร	64	54.70
13. มีการเปิดเผยรหัสผ่านให้กับผู้อื่นทั้งตั้งใจและไม่ตั้งใจ	62	52.99
14. มีการเก็บรหัสผ่านที่สำคัญที่คนอื่นสามาถเข้าถึงได้	67	57.26
15. มีการสั่งงานหรือคำสั่งต่างๆ โดยใช้อีเมลล์	35	29.91
16. การอบรมความรู้ด้านความปลอดภัยคอมพิวเตอร์ให้กับบุคคลากร	67	57.26
17. อายุขององค์กรท่าน	30	25.64
18. มีการนำมาตราฐาน ISO มาใช้ควบคุมความปลอดภัยของคอมพิวเตอร์ในองค์กร	85	72.65
19. นโยบายเรื่องความปลอดภัยของระบบคอมพิวเตอร์	72	61.54
20. บทลงโทษผู้ที่ฝ่าฝืนนโยบายความปลอดภัยขององค์กร	50	42.74
21. การแบ่งหน้าที่การทำงาน	43	36.75
22. งบประมาณด้านความปลอดภัยของคอมพิวเตอร์ไม่เพียงพอ	53	45.30
23. ผู้บริหารหรือหัวหน้าไม่สนับสนุนเรื่องของความปลอดภัยของคอมพิวเตอร์	58	49.57
24. การใช้เอาท์ซอสในองค์กร	32	27.35
25. ระบบการสนับสนุนของระบบสารสนเทศอื่นๆไม่มีประสิทธิภาพ เช่น อินเทอร์เน็ต, ไฟฟ้า, สื่อสาร เป็นต้น	43	36.75
26. การจำกัดพอตท์สำหรับการใช้งานอินเทอร์เน็ต	52	44.44

ตารางที่ ข.2 ข้อมูลปัจจัยที่ใช้ทดสอบทั้งหมด 48 ข้อมูล

	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12	v13	v14	v15	v16	v17	v18	v19	v20	v21	v22	v23	v24
1	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
2	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
3	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
4	2	3	2	1	3	1	2	3	3	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
5	2	3	2	1	3	1	4	3	2	2	1	3	2	2	1	2	1	2	2	2	2	2	2	2
6	2	3	2	1	3	1	2	3	2	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
7	2	3	2	1	3	1	2	3	2	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
8	2	3	2	1	3	1	4	3	2	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
9	1	3	3	2	1	2	1	1	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
10	1	3	3	2	1	2	1	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
11	2	3	2	1	3	1	1	3	3	2	1	3	1	2	1	2	2	2	2	2	2	2	2	2
12	2	3	2	1	3	1	1	3	2	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
13	2	3	2	1	3	1	4	1	2	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
14	1	3	1	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
15	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	1	3	3	1	2	2	2	1
16	1	3	1	2	2	2	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
17	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
18	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
19	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
20	1	3	1	2	2	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
21	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
22	2	3	2	1	3	1	4	3	3	2	1	3	2	2	1	2	2	2	2	2	2	2	2	2
23	1	3	3	2	1	2	2	2	3	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
24	1	3	3	2	1	2	4	2	3	2	1	2	2	1	3	3	1	3	3	1	2	2	2	1

ตารางที่ ข.2 ข้อมูลปัจจัยที่ใช้ทดสอบทั้งหมด 48 ข้อมูล (ต่อ)

	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12	v13	v14	v15	v16	v17	v18	v19	v20	v21	v22	v23	v24
25	1	3	1	2	1	2	3	2	3	2	1	2	2	1	3	3	2	3	3	1	2	1	2	1
26	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
27	1	3	3	2	1	3	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	1	2	1
28	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
29	1	3	3	2	1	2	3	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
30	1	3	3	2	1	3	2	1	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
31	1	3	1	2	1	2	4	2	1	2	1	2	1	1	3	3	1	3	3	2	2	2	2	1
32	1	3	3	2	2	2	2	2	3	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
33	1	3	1	2	1	2	4	1	3	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
34	1	3	3	2	2	3	2	2	3	2	1	2	2	1	3	3	2	3	3	1	2	2	2	1
35	1	3	3	2	1	2	4	2	3	2	1	2	2	1	3	3	2	3	3	1	2	2	2	1
36	1	3	3	2	1	3	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
37	1	3	3	2	1	3	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
38	1	3	3	2	1	3	4	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
39	1	3	3	2	1	3	4	2	1	2	1	2	2	1	3	3	1	3	3	2	2	1	2	1
40	1	3	1	2	1	2	4	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
41	1	3	3	2	2	2	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
42	1	3	3	2	1	2	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
43	1	3	1	2	1	2	3	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
44	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	1	3	3	1	2	2	2	1
45	1	3	3	2	2	2	2	2	1	2	1	2	2	1	3	3	2	3	3	2	2	2	2	1
46	1	3	1	2	1	2	2	1	1	2	1	2	2	1	3	3	1	3	3	2	2	2	2	1
47	1	3	3	2	1	2	4	2	1	2	1	2	2	1	3	3	2	3	3	2	2	1	2	1
48	1	3	1	2	1	2	2	2	1	2	1	1	2	1	3	3	2	3	3	2	2	2	2	1

ตารางที่ ข.3 ข้อมูลการเกิดภัยคุกคามที่ใช้ทดสอบทั้งหมด 48 ข้อมูล

	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12
1	1	1	1	2	3	2	1	1	1	3	2	1
2	3	3	1	2	3	2	2	3	3	3	1	1
3	5	5	1	2	5	2	1	5	3	3	2	1
4	4	4	4	1	1	1	5	4	1	2	1	1
5	3	3	3	2	5	1	4	3	1	2	2	1
6	3	3	3	1	2	1	4	3	2	1	1	2
7	3	3	3	1	2	1	4	3	2	2	2	3
8	3	3	3	2	5	1	3	3	1	1	1	1
9	3	3	2	3	1	2	1	3	3	3	3	3
10	5	5	2	2	1	2	1	5	3	3	1	2
11	4	4	4	1	1	1	5	4	1	1	2	1
12	3	3	3	1	1	1	3	3	1	1	2	1
13	1	1	3	3	5	1	3	1	1	1	1	4
14	3	3	2	1	5	2	1	3	3	3	1	1
15	1	1	1	1	2	2	1	1	3	3	3	5
16	5	5	2	1	2	2	1	5	4	3	3	1
17	5	5	1	2	5	2	2	5	4	3	3	1
18	5	5	2	2	2	2	1	5	3	3	1	1
19	5	5	2	1	2	2	2	5	4	3	2	2
20	3	3	1	2	5	2	2	3	4	3	2	1
21	5	5	1	1	2	2	1	5	3	3	2	1
22	4	4	4	1	5	1	5	4	1	1	2	1
23	5	5	5	1	2	2	5	5	3	2	1	2
24	4	4	5	1	5	2	5	4	1	2	1	1

ตารางที่ ข.3 ข้อมูลการเกิดภัยคุกคามที่ใช้ทดสอบทั้งหมด 48 ข้อมูล (ต่อ)

	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12
25	5	5	5	1	4	2	5	5	5	3	1	5
26	5	5	1	1	5	2	1	5	3	2	3	1
27	5	5	1	1	2	2	1	5	5	3	1	4
28	5	5	2	1	5	2	2	5	3	2	3	1
29	3	3	2	1	4	2	2	3	3	2	1	3
30	4	4	2	3	2	2	2	4	3	2	2	1
31	5	5	1	2	5	2	1	5	3	2	3	1
32	5	5	5	2	2	2	5	5	4	2	2	1
33	5	5	5	3	5	2	5	5	3	2	1	1
34	5	5	5	2	2	2	5	5	4	3	2	1
35	5	5	5	2	5	2	5	5	3	3	2	2
36	5	5	1	2	5	3	1	5	4	2	1	3
37	5	5	2	2	3	3	1	5	4	2	2	1
38	5	5	2	2	5	3	2	5	3	2	2	5
39	3	3	2	2	5	2	1	3	5	3	1	4
40	3	3	3	1	5	2	2	3	3	2	2	1
41	5	5	2	1	2	2	1	5	4	2	2	1
42	5	5	2	1	2	2	2	5	3	2	2	3
43	3	3	2	1	4	2	2	3	3	2	1	1
44	3	3	3	1	5	2	2	3	3	2	2	1
45	5	5	2	1	1	2	2	5	4	2	1	1
46	5	5	2	3	1	2	3	5	3	2	2	3
47	3	3	1	1	5	1	1	3	4	3	2	4
48	5	5	1	1	3	1	2	5	3	2	1	1

ภาคผนวก ค
ผลการวิเคราะห์ข้อมูล

ในภาคผนวก ค. นี้จะแสดงตารางผลการวิเคราะห์โดยจะแบ่ง 3 ส่วน ส่วนแรก Polychoric Correlation เป็นการวิเคราะห์หาค่าสัมประสิทธิ์ของตัวแปรอิสระทั้งหมด ส่วนที่สอง Factor Analysis เป็นการวิเคราะห์เพื่อสร้างองค์ประกอบหรือตัวแปรใหม่ขึ้นมาเพื่อลดจำนวนตัวแปรที่มีอยู่ และส่วนที่สาม Multinomial Logistic Regression

ส่วนแรก Polychoric Correlation

ตารางที่ ค.1 ผลการวิเคราะห์ Polychoric Correlation

	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10	v11	v12
v1	1	0.17	-0.52	-0.56	0.52	-0.49	0.15	0.49	0.59	0.11	-0.03	0.63
v2	0.17	1	-0.21	0.32	-0.28	0.18	0.08	-0.27	0.11	0.32	0.02	-0.07
v3	-0.52	-0.21	1	0.15	-0.12	0.08	-0.21	-0.15	-0.29	-0.13	0.04	-0.26
v4	-0.56	0.32	0.15	1	-0.91	0.74	0.08	-0.73	-0.28	0.18	-0.07	-0.55
v5	0.52	-0.28	-0.12	-0.91	1	-0.69	-0.11	0.68	0.29	-0.2	0.06	0.51
v6	-0.49	0.18	0.08	0.74	-0.69	1	0.07	-0.53	-0.21	-0.08	-0.06	-0.49
v7	0.15	0.08	-0.21	0.08	-0.11	0.07	1	0.05	0.12	0.17	-0.09	0.17
v8	0.49	-0.27	-0.15	-0.73	0.68	-0.53	0.05	1	0.23	-0.09	-0.03	0.53
v9	0.59	0.11	-0.29	-0.28	0.29	-0.21	0.12	0.23	1	-0.1	-0.04	0.34
v10	0.11	0.32	-0.13	0.18	-0.2	-0.08	0.17	-0.09	-0.1	1	0.01	0.18
v11	-0.03	0.02	0.04	-0.07	0.06	-0.06	-0.09	-0.03	-0.04	0.01	1	-0.03
v12	0.63	-0.07	-0.26	-0.55	0.51	-0.49	0.17	0.53	0.34	0.18	-0.03	1
v13	-0.03	0.01	-0.03	0.17	-0.17	0.14	0.15	-0.06	-0.09	0.03	-0.25	0.03
v14	0.68	-0.21	-0.28	-0.83	0.76	-0.58	-0.02	0.59	0.39	-0.13	0.08	0.64
v15	-0.76	0.04	0.34	0.82	-0.74	0.62	-0.04	-0.64	-0.37	0	-0.02	-0.57
v16	-0.34	0.22	0.01	0.82	-0.74	0.74	0.08	-0.6	-0.1	-0.07	-0.04	-0.48
v17	-0.06	-0.17	0.15	-0.29	0.39	-0.23	-0.33	0.07	-0.03	-0.14	0.12	-0.03
v18	-0.34	0.09	0.02	0.76	-0.69	0.69	0.11	-0.46	-0.11	-0.04	-0.04	-0.33
v19	-0.27	0.35	-0.03	0.89	-0.81	0.65	0.12	-0.61	-0.11	0.24	-0.12	-0.37
20	0.35	0.42	-0.36	0.3	-0.27	0.15	0.16	-0.17	0.06	0.22	0.04	0.13
v21	0.2	0.48	-0.24	0.39	-0.35	0.22	0.15	-0.3	0.14	0.36	0.02	-0.19
v22	0.07	0	-0.05	-0.1	0.16	-0.25	0.05	0.03	-0.09	0.11	0.02	0.04
v23	0.3	0.58	-0.31	0.57	-0.52	0.34	0.19	-0.38	0.21	0.37	-0.11	-0.08
v24	0.62	-0.34	-0.22	-0.9	0.82	-0.65	-0.02	0.68	0.34	-0.07	-0.05	0.55

ตารางที่ ค.1 ผลการวิเคราะห์ Polychoric Correlation (ต่อ)

	v13	v14	v15	v16	v17	v18	v19	20	v21	v22	v23	v24
v1	-0.03	0.68	-0.76	-0.34	-0.06	-0.34	-0.27	0.35	0.2	0.07	0.3	0.62
v2	0.01	-0.21	0.04	0.22	-0.17	0.09	0.35	0.42	0.48	0	0.58	-0.34
v3	-0.03	-0.28	0.34	0.01	0.15	0.02	-0.03	-0.36	-0.24	-0.05	-0.31	-0.22
v4	0.17	-0.83	0.82	0.82	-0.29	0.76	0.89	0.3	0.39	-0.1	0.57	-0.9
v5	-0.17	0.76	-0.74	-0.74	0.39	-0.69	-0.81	-0.27	-0.35	0.16	-0.52	0.82
v6	0.14	-0.58	0.62	0.74	-0.23	0.69	0.65	0.15	0.22	-0.25	0.34	-0.65
v7	0.15	-0.02	-0.04	0.08	-0.33	0.11	0.12	0.16	0.15	0.05	0.19	-0.02
v8	-0.06	0.59	-0.64	-0.6	0.07	-0.46	-0.61	-0.17	-0.3	0.03	-0.38	0.68
v9	-0.09	0.39	-0.37	-0.1	-0.03	-0.11	-0.11	0.06	0.14	-0.09	0.21	0.34
v10	0.03	-0.13	0	-0.07	-0.14	-0.04	0.24	0.22	0.36	0.11	0.37	-0.07
v11	-0.25	0.08	-0.02	-0.04	0.12	-0.04	-0.12	0.04	0.02	0.02	-0.11	-0.05
v12	0.03	0.64	-0.57	-0.48	-0.03	-0.33	-0.37	0.13	-0.19	0.04	-0.08	0.55
v13	1	-0.15	-0.03	0.09	-0.28	0.12	0.11	0.09	-0.04	-0.07	0.18	-0.06
v14	-0.15	1	-0.68	-0.48	0.14	-0.43	-0.6	-0.02	-0.32	0.05	-0.32	0.74
v15	-0.03	-0.68	1	0.63	-0.11	0.6	0.64	0.12	0.1	-0.1	0.14	-0.85
v16	0.09	-0.48	0.63	1	-0.28	0.92	0.88	0.3	0.34	-0.12	0.55	-0.7
v17	-0.28	0.14	-0.11	-0.28	1	-0.35	-0.32	-0.28	0.01	0.16	-0.41	0.21
v18	0.12	-0.43	0.6	0.92	-0.35	1	0.85	0.26	0.17	-0.11	0.46	-0.6
v19	0.11	-0.6	0.64	0.88	-0.32	0.85	1	0.43	0.47	-0.06	0.7	-0.76
20	0.09	-0.02	0.12	0.3	-0.28	0.26	0.43	1	0.37	0.03	0.62	-0.28
v21	-0.04	-0.32	0.1	0.34	0.01	0.17	0.47	0.37	1	0.05	0.55	-0.23
v22	-0.07	0.05	-0.1	-0.12	0.16	-0.11	-0.06	0.03	0.05	1	-0.04	0.1
v23	0.18	-0.32	0.14	0.55	-0.41	0.46	0.7	0.62	0.55	-0.04	1	-0.41
v24	-0.06	0.74	-0.85	-0.7	0.21	-0.6	-0.76	-0.28	-0.23	0.1	-0.41	1

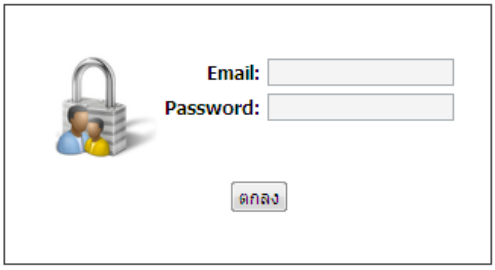
ส่วนที่สอง Factor Analysis

ตารางที่ ค.2 ผลการวิเคราะห์ Factor Loading

	1	2	3	4	5
1	-0.74	0.55	0.22	0.18	0.05
2	0.18	0.72	-0.04	-0.17	-0.05
3	0.31	-0.51	-0.31	-0.15	-0.06
4	0.94	0.23	0.13	-0.04	-0.09
5	-0.88	-0.19	-0.2	0.06	0.13
6	0.78	0.06	0.12	0.28	-0.08
7	-0.03	0.09	0.63	-0.15	-0.10
8	-0.76	-0.20	0.13	0.07	0
9	-0.42	0.42	0.02	0.51	0.02
10	0.02	0.42	0.18	-0.66	-0.09
11	0.01	-0.05	-0.01	-0.15	0.77
12	-0.70	0.08	0.39	-0.04	0.04
13	0.07	-0.05	0.33	-0.04	-0.67
14	-0.82	-0.05	0.13	0.24	0.25
15	0.89	-0.14	-0.01	-0.04	0.07
16	0.81	0.24	0.23	0.35	0.08
17	-0.19	-0.09	-0.72	-0.07	0.22
18	0.74	0.10	0.39	0.34	0.10
19	0.80	0.42	0.27	0.09	-0.01
20	0.14	0.60	0.42	-0.03	0.18
21	0.24	0.77	-0.14	-0.13	-0.01
22	-0.12	0.04	0.01	-0.49	0.22
23	0.34	0.79	0.32	0.05	-0.13
24	-0.90	-0.11	-0.06	0.09	-0.05

ภาคผนวก ง
หน้าจอผู้ใช้งานระบบ

ระบบทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ



รูปที่ ง.1 หน้าจอเข้าสู่ระบบ

รูปที่ ง.2 หน้าจอผู้ใช้งานในส่วนของหน้าแรก

รูปที่ ง.3 หน้าจอระบุปัจจัยความเสี่ยง

จุฬาลงกรณ์มหาวิทยาลัย

ระบบทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ

หน้าแรก
ทำนายความเสี่ยง
ดูประวัติย้อนหลัง
รายงานกราฟ
ออกจากระบบ

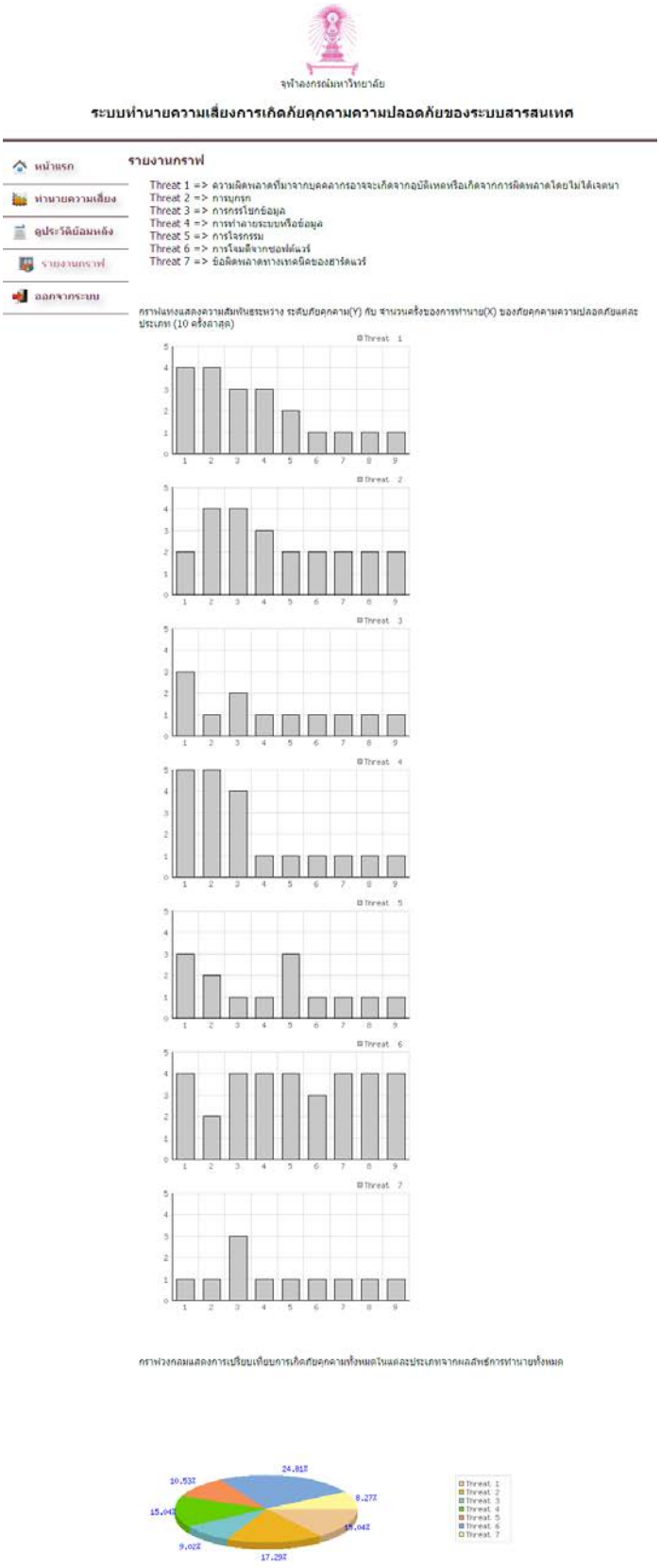
ทำนายความเสี่ยง » ผลการคำนวณ

ประเภทภัยคุกคาม	โอกาสเกิดความเสี่ยง	
	ระดับ	ความน่าจะเป็น
ความผิดพลาดที่มาจากบุคคลากรอาจจะเกิดจากอุบัติเหตหรือเกิดจากการผิดพลาดโดยไม่ได้เจตนา	น้อยที่สุด	0.65
	น้อย	0.00
	ปานกลาง	0.01
	มาก	0.34
	มากที่สุด	0.00
การบุกรุก	น้อยที่สุด	0.12
	น้อย	0.86
	ปานกลาง	0.02
	มาก	0.00
	มากที่สุด	0.00
การกรรโชกข้อมูล	น้อยที่สุด	0.62
	น้อย	0.18
	ปานกลาง	0.20
การทำลายระบบหรือข้อมูล	น้อยที่สุด	0.91
	น้อย	0.09
	ปานกลาง	0.00
	มาก	0.00
	มากที่สุด	0.00
การโจรกรรม	น้อยที่สุด	0.98
	น้อย	0.01
	ปานกลาง	0.00
การโจมตีจากซอฟต์แวร์	น้อยที่สุด	0.03
	น้อย	0.02
	ปานกลาง	0.23
	มาก	0.73
	มากที่สุด	0.00
ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์	น้อยที่สุด	0.99
	น้อย	0.01
	ปานกลาง	0.00

รูปที่ ง.4 หน้าจอแสดงผลการทำนาย

รูปที่ ง.5 หน้าจอรายการใช้งานย้อนหลังการทำนายความเสี่ยง

รูปที่ ง.6 หน้าจอแสดงผลการใช้งานย้อนหลังการทำนายความเสี่ยง



รูปที่ ง.7 หน้าจอแสดงรายงานในรูปแบบของกราฟเพื่อใช้เปรียบเทียบ

ประวัติผู้เขียนวิทยานิพนธ์

ชื่อ นามสกุล	:	นายอัจกิต อุฒาธรรม
วัน เดือน ปีเกิด	:	15 พฤษภาคม พ.ศ. 2529
วุฒิการศึกษา	:	วิทยาศาสตร์บัณฑิต สาขา คณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยธรรมศาสตร์ สำเร็จการศึกษาในปีการศึกษาที่ 2551

การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยง ของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศ ในประเทศไทย

by ajagit utatham

WORD COUNT	3690	TIME SUBMITTED	14-MAY-2013 12:13PM
CHARACTER COUNT	11671	PAPER ID	329890114

การวิเคราะห์ปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในองค์กรของประเทศไทย

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

อัจกิต อุฒาธรรม ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Ajagit Utatham Department of Computer Enigneering Faculty of Engineering Chulalongkorn University

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อต้องการศึกษาหาปัจจัยที่ทำให้เกิดภัย คุกคามความปลอดภัยของระบบสารสนเทศ และสร้างโมเดลเพื่อใช้ทำนายความเสี่ยงของภัยคุกคาม โดยใช้วิธีการออกแบบสอบถาม ซึ่งจะแบ่งเป็น 2 ส่วนคือ 1) แบบสอบถามสำรวจหาปัจจัยโดยมีกลุ่มตัวอย่างเป็นบุคลากรในองค์กรที่เกี่ยวข้อง ในด้านระบบสารสนเทศจำนวน 117 คน 2) แบบสอบถามเชิงลึก โดยใช้ข้อมูลจากแบบสอบถามส่วนแรกมาเป็นข้อมูลในการออกแบบสอบถามเพื่อใช้ใน การวิเคราะห์ โดยมีกลุ่มตัวอย่างเป็นหัวหน้าหรือตัวแทนแผนกที่เกี่ยวข้องกับระบบสารสนเทศ จำนวน 298 ชุด เพื่อนำไปวิเคราะห์สร้างโมเดล โดยใช้ Multinomial Regression และใช้ s-2Log likelihood และ Wald Statistics ในการหาค่าความเชื่อมั่นของโมเดลและสัมประสิทธิ์ตามลำดับ และพัฒนาเป็น โปรแกรมเพื่อช่วยทำนาย ผลวิจัยพบว่าจากการศึกษาและสำรวจปัจจัยได้ปัจจัยทั้งหมด 24 ปัจจัยและ จากการวิเคราะห์ได้โมเดลที่สามารถทำนายการเกิดภัยคุกคาม 7 ประเภทด้วยกัน ซึ่งได้แก่ 1) ความผิดพลาดที่มาจากมนุษย์ 3) การบุกรุก 4) การกรรโชกข้อมูล 5) การทำลายระบบหรือข้อมูล 6) การโจรกรรม 7) การโจมตีจากซอฟต์แวร์และ 10) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ โดยมีนัยสำคัญเป็น 0.05 ผลการทดลอบพบว่าโมเดลมีความสอดคล้องกับปัจจัยที่กล่าวมาข้างต้นร้อยละ 37.5, 52.08, 39.58, 43.75, 79.16, 52.08 และ 58.33 ตามลำดับ

คำสำคัญ: ภัยคุกคามความปลอดภัย, การทำนายความเสี่ยง, ปัจจัยภัยคุกคาม

Abstract

The purposes of this study are to find factors causing information security threat and to build a model to predict risks of the threats by using questionnaires which consist of 2 parts: 1) the questionnaire which has 117 officers from information system organizations as samples searches for factors of the threats 2) In-depth questionnaire which has 298 samples of leaders or representations from information system departments uses information from the first questionnaire to be designed to analysis and build a model. Multinomial Regression, s-2Log likelihood and Wald Statistics are used to find out the model's reliability and the variables' coefficients and develop the model into a predicting program. This study shows that there are 24 factors of the threats and the model can predict 7 factors which are 1) Human mistakes 3) Intrusion 4) Threats for information.5) System or information destruction 6) Stealing 7) Attacking software 10) Hardware technical errors. With reliability as 0.05, the results from relation experiment between the model and the mentioned factors are 37.5%, 52.08%, 39.58%, 43.75%, 79.16%, 52.08% and 58.33%, respectively.

Keyword: Security Threats, Risk Prediction, Threat Factors

1. คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานและการจัดการภายในองค์กรทั้งภาครัฐและเอกชน ทั้งนี้ก็เพื่อเพิ่มประสิทธิภาพการดำเนินงานและการเสริมสร้างภาพลักษณ์ที่ดีขององค์กร นั้นแต่อย่างไรก็ตามการนำเอาเทคโนโลยีสารสนเทศมาใช้ในองค์กรย่อมมีผลกระทบในด้านต่างๆ เช่น การรักษาความปลอดภัยของข้อมูล การเพิ่มระดับของการพึ่งพาต่อระบบสารสนเทศและการควบคุมภายในมีความสลับซับซ้อนมากขึ้น นอกจากนี้ยังมีผลกระทบทางด้านภัยคุกคามด้านความปลอดภัยของระบบสารสนเทศ ซึ่งหากมีข้อผิดพลาดเกิดขึ้น อาจส่งผลกระทบที่รุนแรง และรวดเร็วขึ้นต่อการบริหารจัดการและการดำเนินงานภายในองค์กรนั้น

ภัยคุกคามความปลอดภัยของระบบสารสนเทศนั้น อาจจะเกิดได้หลายปัจจัย 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. ทฤษฎีที่เกี่ยวข้อง

2.1 การวิเคราะห์องค์ประกอบ (Factor Analysis)

การวิเคราะห์องค์ประกอบ เป็นเทคนิคการวิเคราะห์ทางสถิติของการวิจัย ที่มุ่งลดจำนวนตัวแปรที่มีอยู่มากทั้งนี้ก็ด้วยเหตุผลตัวแปรบางตัวอาจมีคุณสมบัติในการอธิบายลักษณะของข้อมูลเหมือนกัน ตัวแปรในลักษณะนี้อาจจะต้องตัดทิ้งไป หรือตัวแปรบางตัวมีลักษณะความสัมพันธ์ใกล้เคียงกัน จะถูกรวมเข้ากลุ่มกันเป็นตัวแปรใหม่เรียกว่า ปัจจัย (Factor) การรวมกลุ่มของตัวแปรจะจัดเป็นกลุ่ม หรือกี่ปัจจัย การวิเคราะห์จะดูที่ค่าความสัมพันธ์กัน ซึ่งอาจจะสัมพันธ์กันในทางบวก หรือทางลบก็ได้ [1] จำนวนองค์ประกอบที่ได้จะพิจารณาจากค่าของไอเกน (Eigen Value) ซึ่งค่า ไอเกนจะมีค่าเท่ากับจำนวนตัวแปรในองค์ประกอบนั้นสามารถคำนวณได้จาก Eigen Value = $\sum(w)^2$ โดยที่ w คือ น้ำหนักของตัวแปรในองค์ประกอบนั้นและองค์ประกอบใหม่ที่ได้จะนำค่า Factor Score ไปใช้ซึ่งคำนวณได้จาก

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

โดยที่ k คือ 1, 2,...., n และ i คือ 1, 2,..., m

Z_{jk} คือ ค่าปัจจัยที่ j ของ case ที่ k

n คือ จำนวนข้อมูล

m คือ จำนวน Factor

W_{ik} คือ ค่าสัมประสิทธิ์ หรือ loading factor ของตัวแปรที่ k ใน Factor ที่ i

F_{ik} คือ Factor score ของ Factor ที่ i ของ case ที่ k

2.2 การวิเคราะห์การถดถอยโลจิสติคแบบหลายกลุ่ม

การวิเคราะห์การถดถอยโลจิสติค เป็นการนำตัวแปรอิสระซึ่งเป็นตัวแปรที่ทำหน้าที่เป็นเหตุทำให้เกิดผลอย่างใดอย่างหนึ่งจำนวนหลายตัวแปรมาวิเคราะห์ความสัมพันธ์พร้อมกันกับตัวแปรตาม ซึ่งเป็นตัวแปรที่เป็นผลและเป็น ตัวแปรเชิงกลุ่ม [4, 5] โดยมีสมการเชิงเส้นเป็น

$$Z = e^{\beta_0+\beta_1x_1+\cdots+\beta_nx_n} \quad (2)$$

และมีสมการความน่าจะเป็น คือ

$$\text{Prob(event)} = \frac{e^{\beta_0+\beta_1x_1+\cdots+\beta_nx_n}}{1+e^{\beta_0+\beta_1x_1+\cdots+\beta_nx_n}} \quad (3)$$

เมื่อ β_0 คือ ค่าคงที่

$\beta_1, \ldots, \beta_n$ คือ ค่าสัมประสิทธิ์ของตัวแปรต่างๆ มีทั้งหมด n ตัว

$X_1, X_2, \ldots, X_n$ คือ ตัวแปรอิสระมีทั้งหมด n ตัว

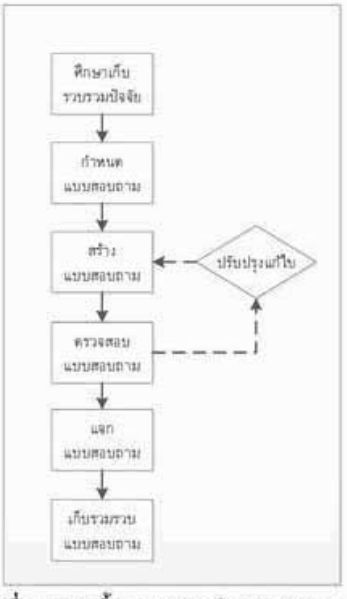
e คือ เป็นค่าคงที่ทางคณิตศาสตร์มีค่าประมาณ 2.718

ทั้งนี้ หลักเกณฑ์ในการเลือกแบบจำลองที่เหมาะสมต้องพิจารณาโดยใช้ -2Log likelihood และ Wald Statistics ในการในการหาค่าความเชื่อมั่นของ โมเดลและค่าสัมประสิทธิ์ตามลำดับ

3. วิธีการดำเนินการวิจัย

งานวิจัยนี้เป็นการเก็บรวบรวมข้อมูลเพื่อใช้สำหรับสร้างโมเดลทำนายความเสี่ยงของภัยคุกคามซึ่ง มีวิธีการดำเนินการวิจัยแบ่งออกเป็น 3 ระยะ

3.1 ขั้นตอนสร้างแบบสอบถามเพื่อเก็บรวบรวมข้อมูล



รูปที่ 1 แสดงขั้นตอนการสร้างแบบสอบถาม

จากรูปที่ 1 เป็นขั้นตอนสร้างแบบสอบถาม ซึ่งต้องมีการศึกษาข้อมูลที่จะใช้สร้างแบบสอบถามจากนั้นจะเป็นการกำหนดประเภทคำถามและข้อมูลของคำตอบซึ่งจะใช้ในการวิเคราะห์จากนั้นจะสร้างแบบสอบถามและจะถูกพิจารณาจากอาจารย์ที่ปรึกษาเพื่อปรับปรุงและแก้ไขก่อนทำการแจก โดยงานวิจัยนี้จะแบ่งเป็น 2 ส่วนคือ

3.1.1 ส่วนที่ 1 แบบสอบถามสำรวจความคิดเห็นของปัจจัยความเสี่ยงด้านความปลอดภัย

แบบสอบถามนี้จะลักษณะปลายปิด คือให้ผู้ตอบได้เลือกตอบในสิ่งที่คิดว่าเป็นปัจจัยของการเกิดภัยคุกคามกลุ่มตัวอย่างจากบุคลากรที่ทำงานเกี่ยวข้องในด้านคอมพิวเตอร์มาจำนวน 117 คน ในการตอบแบบสอบถาม โดยวิธีการสำรวจจะเป็นการแจกแบบสอบถามโดยตรง ให้แก่บุคลากรของแต่ละองค์กรเพื่อสำรวจความคิดเห็นและหาปัจจัยของการเกิดความเสี่ยงทางด้านความปลอดภัยของระบบสารสนเทศ

3.1.2 ส่วนที่ 2 แบบสอบถามเชิงลึก

การออกแบบสอบถามจะใช้ข้อมูลในสอบถามส่วนที่ 1 เพื่อใช้เป็นข้อมูลในสร้างแบบสอบถามเชิงลึกเพื่อใช้ในการวิเคราะห์ โดยออกแบบให้มีการประเมินการเกิดภัยคุกคามเป็น 5 ระดับดังตารางที่ 1 โดยมีกลุ่มตัวอย่างเป็นองค์กรที่มีแผนกเกี่ยวข้องกับระบบสารสนเทศจำนวน 298 ชุด โดยผู้ตอบแบบสอบถามจะเป็นผู้ที่เกี่ยวข้องหรือมีความรู้ด้านสารสนเทศโดยวิธีการสอบถามจะทำการแจกแบบสอบถามโดยตรง ไปรษณีย์และทางอินเตอร์เน็ต

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% จากนั้นจะนำส่วนแรกไปทำการวิเคราะห์เพื่อสร้าง

โมเดล โดยขั้นตอนการวิเคราะห์จะแบ่งออกเป็น 2 ขั้นตอน คือ

3.2.1 วิเคราะห์องค์ประกอบ

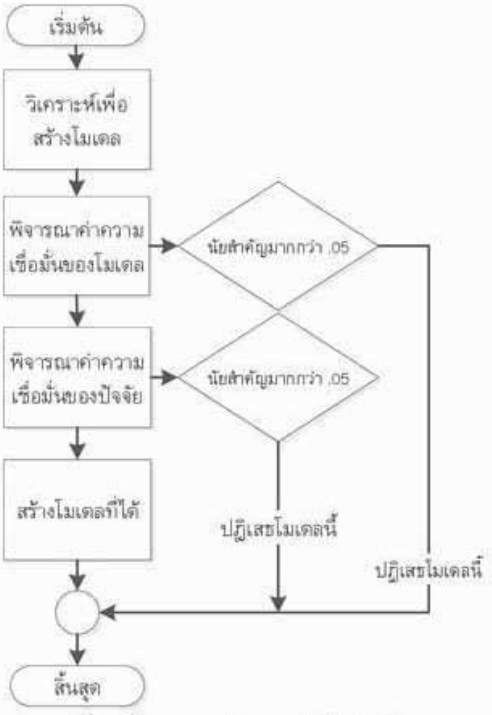
การวิเคราะห์องค์ประกอบนี้เนื่องจากข้อมูลที่ใช้ในการวิเคราะห์นี้เป็นข้อมูลเชิงกลุ่ม (Categorical Data) จึงเลือกใช้วิธีการวิเคราะห์ Polychoric Correlation [6, 7] โดยใช้โปรแกรม R เป็นเครื่องมือช่วยในการวิเคราะห์ ขั้นตอนการวิเคราะห์องค์ประกอบ จะแสดงดังรูปที่ 2

รูปที่ 2 ขั้นตอนการวิเคราะห์องค์ประกอบ

เมื่อเข้าสู่กระบวนการวิเคราะห์องค์ประกอบแล้ว จะทำการหาค่าไอเกนเพื่อเลือกจำนวนองค์ประกอบ โดยองค์ประกอบที่เลือกจะต้องมีค่าไอเกนที่มากกว่าหรือเท่ากับ 1 เมื่อเลือกจำนวนองค์ประกอบที่ได้แล้วจะทำการคัดเลือกปัจจัยเข้าสู่องค์ประกอบใหม่ ทั้งนี้จะพิจารณาจากค่าน้ำหนักของปัจจัยที่ลู่เข้าสู่ 1 หรือ -1 ซึ่งจากการวิเคราะห์สามารถสร้างองค์ประกอบใหม่โดยองค์ประกอบใหม่ที่ได้จะนำไปใช้ในการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงต่อไป

3. 2. 2 วิเคราะห์เพื่อสร้างโมเดล

นำข้อมูลองค์ประกอบใหม่ที่ได้มาทำการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยดุกคามทั้ง 12 ประเภท ขั้นตอนการวิเคราะห์จะได้ดังรูปที่ 3

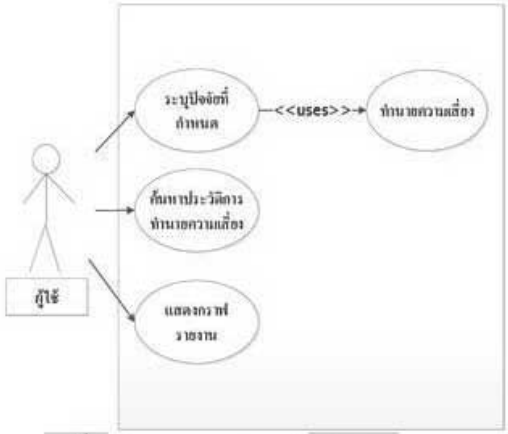


รูปที่ 3 ขั้นตอนการวิเคราะห์เพื่อสร้างโมเดล

โดยจะใช้การวิเคราะห์แบบ การถดถอยโลจิสติคแบบหลายกลุ่ม (Multinomial Logistic Regression) เพื่อสร้างโมเดลทำนายความเสี่ยงโดยใช้โปรแกรม SPSS เป็นเครื่องมือช่วยในการวิเคราะห์ [4, 8] และมีนัยสำคัญอยู่ที่ 0.05 โดยโมเดลที่ได้จะถูกพิจารณา 2 ส่วน คือ ส่วนที่1 พิจารณาในส่วนของโมเดล โดยพิจารณาจากค่านัยสำคัญของโมเดลที่ได้จาก Likelihood Ratio Test ส่วนที่ 2 พิจารณาในส่วนของปัจจัยในแต่ละตัวโดยพิจารณาจากค่านัยสำคัญที่ได้จาก Walds Statistic ซึ่งหากมีค่านัยสำคัญเกินกว่าที่กำหนดจะปฏิเสธโมเดลหรือปัจจัยในโดยจะสรุปได้ว่าโมเดลหรือปัจจัยที่ถูกปฏิเสธนั้นไม่มีความสอดคล้องทำให้เกิดภัยดุกคาม

3.3. สร้างระบบเพื่อช่วยในการทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของสารสนเทศ

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



รูปที่ 4 Use Case Diagram ของระบบ

จากรูปที่ 4 จะแบ่งการทำงานออกเป็น 3 ฟังชันก์ คือ

1) การคำนวณเพื่อการทำนายความเสี่ยง โดยนำค่าจากปัจจัยที่ระบุจากผู้ใช้ คำนวณกับโมเดลที่ได้และแสดงระดับโอกาสเกิดความเสี่ยงของภัยคุกคามนั้น

2) แสดงรายงานประวัติการใช้การคำนวณความเสี่ยงย้อนหลังของแต่ละครั้ง

3) แสดงรายงานเปรียบเทียบในรูปแบบของกราฟ

ในการพัฒนาระบบช่วยคำนวณการทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้ จะพัฒนาเป็น Web Application ซึ่งมีข้อมูลเครื่องมือในการพัฒนาระบบดังตารางที่ 2

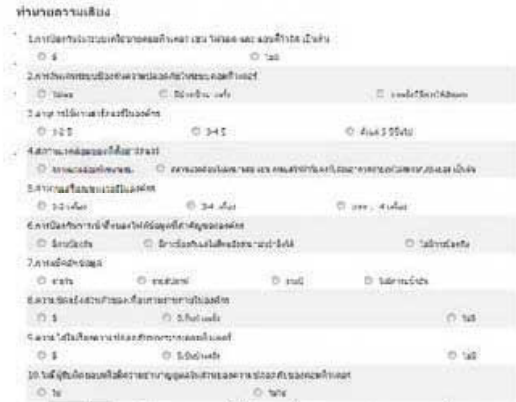
ตารางที่ 2 ข้อมูลเครื่องมือในการพัฒนาระบบ

ระบบ OS	Window XP
ภาษา	PHP 5.2.6
เซิร์ฟเวอร์	Apache 2.2.8

ตารางที่ 2 ข้อมูลเครื่องมือในการพัฒนาระบบ (ต่อ)

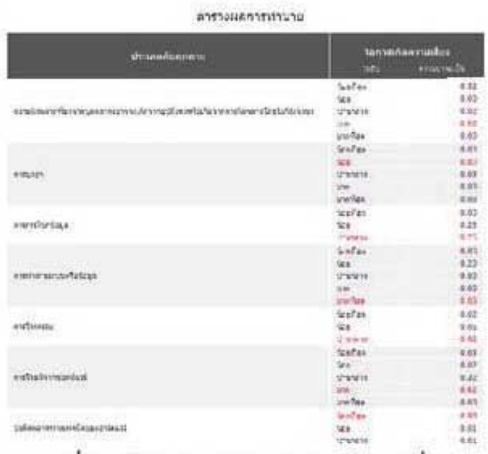
ฐานข้อมูล	MySQL 5.0.51b

ในการใช้งานระบบทำนายความเสี่ยงการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศนี้ ได้มีการออกแบบหน้าจอการใช้งานของระบบ ซึ่งจะขอนำเสนอเป็นเพียงส่วนโดยตัวอย่างหน้าจอการใช้งานของระบบ จะแสดงดังรูปที่ 5 - 7



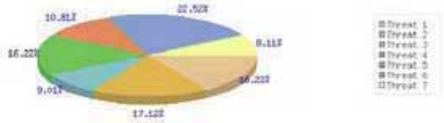
รูปที่ 5 หน้าจอระบุปัจจัยเพื่อทำนายความเสี่ยง

จากรูปที่ 5 เป็นตัวอย่างหน้าจอที่ผู้ใช้ต้องทำการระบุปัจจัยที่ระบบกำหนดให้ครบซึ่งมีทั้งหมด 24 ปัจจัย



รูปที่ 6 หน้าจอแสดงผลการทำนายความเสี่ยง

รูปที่ 6 หน้าจอแสดงผลการทำนายความเสี่ยงซึ่งจะบอกเป็นระดับการเกิดของภัยคุกคามแต่ละประเภทโดยจะพิจารณากับเฉพาะระดับที่มีโอกาสเกิดมากสุด



รูปที่ 7 ตัวอย่างกราฟเปรียบเทียบผลการทำนาย

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 อินเตอร์เน็ต (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 ประเภทได้แก่

1) ข้อผิดพลาดจากการกระทำของมนุษย์

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

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

Z3 = 6.46+ (-.24)F1+ (-.80)F2+ (.32)F3 (11)

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

Z5 = 0 (13)

2) การบุกรุก

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

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

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

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

Z5 = 0 (18)

3) การกรรโชกข้อมูลสารสนเทศ

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

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

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

Z4 = 0 (22)

4) การก่อวินาศกรรมหรือการทำลาย

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

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

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

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

Z5 = 0 (27)

5) การโจรกรรม

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

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

Z3 = 0 (30)

6) การโจมตีซอฟต์แวร์

Z1 = 36.91+ (.93)F1+ (-6.43)F2+ (2.64)F3+ (-11.62)F4+ (7.29)F5 (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 โดยคิดเป็นร้อยละได้ดัง ตารางที่ 4

ตารางที่ 4 ตารางแสดงผลการทดสอบโมเดล

โมเดลที่ใช้ทดสอบ	ความสอดคล้อง
ความผิดพลาดที่มาจากบุคคลากร (T1)	37. 50
การบุกรุก (T2)	52.08
การกรรโชกข้อมูล (T3)	39.58
การทำลายระบบ (T4)	43.75
การโจรกรรม (T5)	79.16
การโจมตีจากซอฟต์แวร์ (T6)	52.08
ข้อผิดพลาดทางฮาร์ดแวร์ (T7)	58.33

5. สรุปผลและข้อเสนอแนะ

งานวิจัยนี้เป็นการหาปัจจัยและสร้างโมเดลสำหรับทำนายความเสี่ยงภัยคุกคามความปลอดภัยของระบบสารสนเทศ โดยใช้วิธีการเก็บข้อมูลจากแบบสอบถามซึ่งสามารถหาปัจจัยทั้งหมด 24 ปัจจัย แล้วมาทำการวิเคราะห์เพื่อจะรวมปัจจัยที่มีลักษณะซ้ำกันให้อยู่ในกลุ่มเดียวกันซึ่งจะใช้วิธีการวิเคราะห์องค์ประกอบ จากนั้นจะนำองค์ประกอบใหม่ที่ได้มาทำการวิเคราะห์เพื่อสร้างโมเดลทำนายความเสี่ยงกับภัยคุกคามทั้ง 12 ประเภท ในการวิเคราะห์จะใช้วิธีการวิเคราะห์ถดถอยโลจิสติคแบบหลายกลุ่ม ซึ่งผลการวิจัยพบว่าสามารถสร้างโมเดลที่สอดคล้องกับการทำนายความเสี่ยงของการเกิดภัยคุกคาม 7 ประเภท จากทั้งหมด 12 ประเภท ซึ่งอาจมีสาเหตุมาจากข้อมูลปัจจัยของภัยคุกคามที่ไม่ครอบคลุมกับภัยคุกคามที่มีทำให้ไม่สามารถสร้างโมเดลได้ครบทั้งหมดและ จากผลการทดสอบความสอดคล้องของโมเดลกับ ข้อมูลที่ใช้ที่ทดลองจำนวน 48 ข้อมูล พบว่าโมเดลบางตัวมีความสอดคล้องกับข้อมูลค่อนข้างต่ำ ซึ่งผู้วิจัยได้สรุปสาเหตุได้ 2 อย่าง คือ 1) ข้อมูลที่ใช้ทดลองไม่เพียงพอในการใช้ทดลอง 2) ปัจจัยที่มีไม่ครอบคลุมทำให้โมเดลที่ได้มีประสิทธิภาพไม่เพียงพอ งานวิจัยนี้ต่อยอดได้โดยอาจจะเลือก วิเคราะห์ภัยคุกคามใดภัยคุกคามหนึ่ง เพื่อที่จะศึกษาภัยคุกคามนั้นอย่างครอบคลุม

เอกสารอ้างอิง

[1] Carl 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 24,pp. 43-57, 2004

[3] Dr.Michael E. Whiteman and Herbert J. Mattord, "Principles of Information Security", vol.3, pp. 9-15, 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] Professor Andy Field, "Factor Analysis for Likert/Ordinal/Non-normal Data". Available http: www.methodspace.com/profiles/blogs/factor-analysis-for-likert-ordinal-non-normal-data

[7] Serena Ng, "CONSTRUCTING COMMON FACTORS FROM CONTINUOUS AND CATEGORICAL DATA", Department of Economics Columbia University, 2012

[8] Yuth Kaiyavan, " Research data analysis step by step SPSS 4",Bangkok: SoonSueSerm Kungtep, vol. 189-205, 2552

การวิเคราะห์หาปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิด··

ORIGINALITY REPORT

5 %	4 %	1 %	1 %
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.saruthipong.com *Internet Source*	1%
2	C. Kern. "Parallel Performance of DES in ECB Mode", 2006 International Sy… *Publication*	1%
3	Submitted to Macquarie University *Student Paper*	1%
4	tum.mgt.psu.ac.th *Internet Source*	< 1%
5	Submitted to Chulalongkorn University *Student Paper*	< 1%
6	dmj.ac.th *Internet Source*	< 1%
7	sut2.sut.ac.th *Internet Source*	< 1%
8	www.sattc.net *Internet Source*	< 1%
9	fnatagro.csc.ku.ac.th *Internet Source*	< 1%
10	A. Schwarzenberg-Czerny. "Metallicity of clusters from RRab pulsators: res… *Publication*	< 1%
11	www.kmitl.ac.th *Internet Source*	< 1%
12	www.pteonline.org *Internet Source*	< 1%
13	www.dbpia.co.kr *Internet Source*	< 1%

EXCLUDE QUOTES OFF
EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY OFF