ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

โดย

นางสาวศิริรัตน์ ศรีสว่าง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาระบบสารสนเทศเพื่อการจัดการ
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

โดย

นางสาวศิริรัตน์ ศรีสว่าง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาระบบสารสนเทศเพื่อการจัดการ
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

FACTORS AFFECTING COMPUTER CRIME PROTECTION BEHAVIOR

BY

MISS SIRIRAT SRISAWANG

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF SCIENCE

MANAGEMENT INFORMATION SYSTEMS

FACULTY OF COMMERCE AND ACCOUNTANCY

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2015

มหาวิทยาลัยธรรมศาสตร์
คณะพาณิชยศาสตร์และการบัญชี

วิทยานิพนธ์

ของ

นางสาวศิริรัตน์ ศรีสว่าง

เรื่อง

ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

เมื่อ วันที่ 11 เม.ย. 2559

ประธานกรรมการสอบวิทยานิพนธ์ .....
(รองศาสตราจารย์ ดร.สุพีชา พาณิชย์ปฐม)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก .....
(ผู้ช่วยศาสตราจารย์ ดร.มฑุปายาส ทองมาก)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม .....
(รองศาสตราจารย์ ดร.อัจฉราวรรณ งามญาณ)

กรรมการสอบวิทยานิพนธ์ .....
(ดร.อมฤต เหล่ารักพงษ์)

คณบดี .....
(ศาสตราจารย์ ดร.ศิริลักษณ์ โรจนกิจอำนวย)

หัวข้อวิทยานิพนธ์	ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์
ชื่อผู้เขียน	นางสาวศิริรัตน์ ศรีสว่าง
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	สาขาวิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.มฑุปายาส ทองมาก
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	รองศาสตราจารย์ ดร.อัจฉราวรรณ งามญาณ
ปีการศึกษา	2558

บทคัดย่อ

การวิจัยครั้งนี้เป็นการศึกษาความสัมพันธ์เชิงสาเหตุ โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ เพื่อตรวจสอบความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ และเพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ ข้อมูลที่ใช้ในการวิจัยเป็นข้อมูลที่รวบรวมผ่านแบบสอบถามจากผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลทั้งที่ใช้งานที่บ้านและที่ทำงานในประเทศไทยจำนวน 600 คน เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถาม

ผลการวิจัยสรุปว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ได้รับอิทธิพลจากปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน โดยส่งผ่านการรับรู้ต่อสภาวะคุกคาม การรับรู้ความสามารถในการจัดการกับภัยคุกคาม และ แรงจูงใจในการป้องกัน โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีความไม่แปรเปลี่ยนของรูปแบบโมเดลและค่าพารามิเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ

คำสำคัญ: ทฤษฎีแรงจูงใจเพื่อป้องกัน อาชญากรรมคอมพิวเตอร์ พฤติกรรมการป้องกัน

Thesis Title	FACTORS AFFECTING COMPUTER CRIME PROTECTION BEHAVIOR
Author	Miss Sirirat Srisawang
Degree	Master of science
Department/Faculty/University	Management Information Systems Faculty of Commerce and Accountancy Thammasat University
Thesis Advisor	Asst.Prof.Dr.Mathupayas Thongmak
Thesis Co-Advisor	Assoc.Prof.Dr.Atcharawan Ngarmyarn
Academic Years	2015

ABSTRACT

This research aimed to investigate factors that affect computer crime protection behavior, based on the protection motivation theory. Personal factors were considered, including: conscientious personality, perceived value of data, and prior experience. In addition, Environmental factors were evaluated, including: subjective norm, security knowledge, and safeguard costs. These factors are mediated by threat appraisal and coping appraisal. The data were collected from 600 personal computer users by use of a questionnaire. Data were analyzed using structural equation modeling. Findings showed that all factors had significant effects on the computer crime protection behavior. In addition, the results showed that security knowledge, one of the environmental factors, had the strongest effects on coping appraisal which subsequently had the strongest impact on protection behavior.

Keywords: Protection Motivation Theory (PMT), Computer crime, Protection behavior

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จลุล่วงเป็นอย่างดี โดยได้รับความกรุณาอย่างสูงจากผู้ช่วยศาสตราจารย์ ดร.มฑุปายาส ทองมาก และ รองศาสตราจารย์ ดร.อัจฉราวรรณ งามญาณ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่ได้ให้แนวคิด คำปรึกษา คำแนะนำ แก้ไขข้อบกพร่อง และผลักดันให้ผู้วิจัยทำวิทยานิพนธ์สำเร็จ ผู้วิจัยซาบซึ้งและขอกราบขอบพระคุณอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณ รองศาสตราจารย์ ดร.สุพีชา พาณิชย์ปฐม และ ดร.อมฤต เหล่ารักพงษ์ ที่ให้ความกรุณาเป็นประธานและกรรมการสอบวิทยานิพนธ์ และให้คำชี้แนะที่มีคุณค่าต่อการปรับปรุงแก้ไขวิทยานิพนธ์ฉบับนี้ให้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบพระคุณคณาจารย์โครงการปริญญาโทสาขาวิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์ และอาจารย์จากภายนอกทุกท่าน ที่ได้ให้ความรู้ รวมถึงเจ้าหน้าที่โครงการที่คอยติดต่อประสานงานและให้ความช่วยเหลือเป็นอย่างดี

ขอขอบคุณผู้ที่ให้ความร่วมมือในการตอบแบบสอบถาม และให้ข้อเสนอแนะที่เป็นประโยชน์ต่องานวิจัยนี้

สุดท้ายนี้ ขอขอบคุณบุคคลในครอบครัวทุกท่านที่ให้ความช่วยเหลือ และให้การสนับสนุนมาโดยตลอด ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยนี้จะเป็นประโยชน์ให้ผู้สนใจต่อไป

นางสาวศิริรัตน์ ศรีสว่าง

สารบัญ

สารบัญตาราง

สารบัญภาพ

รายการสัญลักษณ์และคำย่อ

สัญลักษณ์/คำย่อ	คำเต็ม/คำจำกัดความ
$\bar{x}$	ค่ามัชฌิมเลขคณิต หรือ ค่าเฉลี่ย (mean)
SD	ส่วนเบี่ยงเบนมาตรฐาน (standard deviation)
SE	ความคาดเคลื่อนมาตรฐาน (standard error)
MAX	คะแนนสูงสุด (maximum)
MIN	คะแนนต่ำสุด (minimum)
SK	ค่าความเบ้ (skewness)
KU	ค่าความโด่ง (kurtosis)
CV	สัมประสิทธิ์การกระจาย (coefficient of variation)
χ^2	ดัชนีตรวจสอบความกลมกลืนประเภทค่าสถิติไค-สแควร์
df	ค่าองศาอิสระ (degree of freedom)
Γ	เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง
β	เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง
R^2	ค่าสัมประสิทธิ์การทำนาย (coefficient of determination)
R	ค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ
GFI	ดัชนีวัดระดับความกลมกลืน (goodness of fit index)
AGFI	ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (adjusted goodness of fit index)
NFI	ดัชนีระดับความเป็นปกติ (normed fit index)
RFI	ดัชนีระดับความสัมพัทธ์ (relative fit index)
RMR	ดัชนีรากของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ (root mean squared residual)
P	ระดับนัยสำคัญทางสถิติ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์ในหลากหลายด้าน เช่น การติดต่อสื่อสาร การแลกเปลี่ยนข้อมูลข่าวสาร การซื้อขายแลกเปลี่ยนสินค้าและบริการ เป็นต้น อีกทั้งการนำระบบคอมพิวเตอร์เข้ามาเป็นส่วนสำคัญในการประกอบกิจการของสถานประกอบการต่างๆ ทำให้ข้อมูลส่วนใหญ่ทั้งที่เป็นข้อมูลส่วนตัวและข้อมูลขององค์กรถูกประมวลผลและจัดเก็บไว้บนระบบคอมพิวเตอร์ หรือถูกส่งผ่านระบบเครือข่ายไปยังคอมพิวเตอร์เครื่องอื่น (Ng, Kankanhalli, & Xu, 2009) เมื่อคอมพิวเตอร์มีบทบาทและมีความสำคัญมากขึ้น ผลเสียของการใช้เทคโนโลยีคอมพิวเตอร์ คือก่อให้เกิดปัญหาการขยายตัวของอาชญากรรมข้ามชาติและก่อให้เกิดรูปแบบอาชญากรรมใหม่ๆ ที่มีความยุ่งยากซับซ้อนมากขึ้น เช่นอาชญากรรมทางเศรษฐกิจ โดยเฉพาะอย่างยิ่งอาชญากรรมคอมพิวเตอร์

Parker (2007) ได้ให้ความหมายของอาชญากรรมคอมพิวเตอร์ไว้ว่าเป็นการล่วงละเมิดหรือใช้คอมพิวเตอร์ไปในทางที่ผิดเกี่ยวกับระบบข้อมูลและระบบเครือข่าย ที่ส่งผลให้ผู้ตกเป็นเหยื่อได้รับความเสียหายต่อชีวิตและทรัพย์สิน ซึ่งอาจกล่าวได้ว่าอาชญากรรมคอมพิวเตอร์ก่อให้เกิดความเสียหายอย่างรุนแรงต่อความสงบสุข ศีลธรรมอันดีของประชาชน ความปลอดภัยทางด้านเศรษฐกิจ สังคม และความมั่นคงของประเทศ จากรายงานสถิติการก่ออาชญากรรมทางคอมพิวเตอร์ประจำปีของหน่วยงาน Computer Security Institute (CSI) ประเทศสหรัฐอเมริกา (CSI, 2011) ซึ่งได้ทำการสำรวจสถิติการก่ออาชญากรรมทางคอมพิวเตอร์ทั้งในหน่วยงานภาครัฐและเอกชน โดยการตอบแบบสอบถามของผู้เชี่ยวชาญด้านการรักษาความปลอดภัยคอมพิวเตอร์ประมาณ 500 คน พบว่ามีอัตราสูงถึงร้อยละ 41.1 โดยภัยจากอาชญากรรมคอมพิวเตอร์ที่มีสถิติการละเมิดสูงสุดได้แก่ ภัยจากโปรแกรมมุ่งประสงค์ร้าย (Malware injection) มีอัตราร้อยละ 67.1 ของจำนวนผู้ถูกละเมิดทั้งหมด รองลงมาคือภัยจากกับดักหลอกลวง (Phishing) การโจรกรรมเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์เคลื่อนที่ (Laptop/Mobile device theft) และการโจมตีเครื่องคอมพิวเตอร์ผ่านเครือข่าย (Bots on Network) มีอัตราร้อยละ 38.9 33.5 และ 28.9 ตามลำดับ นอกจากนี้ยังพบว่าอาชญากรรมคอมพิวเตอร์มีอัตราเพิ่มสูงขึ้นจากปี 2009 ส่งผลให้มูลค่าความเสียหายจากการก่ออาชญากรรมคอมพิวเตอร์เพิ่มสูงขึ้นตามไปด้วย

ความเสียหายอันเนื่องมาจากอาชญากรรมคอมพิวเตอร์ เป็นแรงจูงใจให้องค์กรนำมาตรการต่างๆ มาใช้เพื่อป้องกันและลดความความเสี่ยงจากภัยคุกคามที่มีโอกาสเกิดขึ้น (Ng et al., 2009) วิธีการที่ถูกนำมาใช้อย่างแพร่หลาย คือการกำหนดนโยบายหรือระเบียบการใช้งานคอมพิวเตอร์ให้พนักงานยึดถือปฏิบัติตาม เพื่อเป็นการป้องกันข้อมูลและระบบคอมพิวเตอร์จากภัยคุกคามต่างๆ แต่จากงานวิจัยในอดีต พบว่าพนักงานส่วนใหญ่ไม่ปฏิบัติตามนโยบายที่องค์กรกำหนด (Gordon, Loeb, Lucyshyn, & Richardson, 2006; Warkentin & Willison, 2009) อีกทั้งการควบคุมด้วยวิธีการดังกล่าวไม่มีประสิทธิภาพในการป้องกันการใช้งานคอมพิวเตอร์ผิดประเภท เช่น การเปิดเผยบัญชีเข้าใช้งานระบบแก่บุคคลอื่น หรือการเข้าถึงเครือข่ายอินเทอร์เน็ตด้วยระบบเครือข่ายไร้สายที่ให้บริการแบบไม่คิดค่าใช้จ่ายโดยปราศจากการเข้ารหัสลับข้อมูล เป็นต้น (Cronan, Foltz, & Jones, 2006) การส่งเสริมให้พนักงานมีความตระหนักและมีพฤติกรรมด้านความปลอดภัยเพิ่มมากขึ้น จึงเป็นประเด็นที่หลายๆ องค์กรให้ความสำคัญ (Anderson & Agarwal, 2010) เนื่องจากการแสดงพฤติกรรมเกี่ยวกับรักษาความปลอดภัยคอมพิวเตอร์นั้น เป็นเรื่องเฉพาะของแต่ละบุคคล (Ng et al., 2009) ซึ่งหากมีแรงจูงใจหรือมีความตั้งใจในการป้องกันก็จะสามารถปกป้องระบบคอมพิวเตอร์และระบบข้อมูลได้ (Anderson & Agarwal, 2010)

งานวิจัยในอดีตได้มีการศึกษาปัจจัยที่มีอิทธิพลต่อพฤติกรรมของบุคคลในการป้องกันภัยโดยนำทฤษฎีต่างๆ มาเป็นกรอบแนวคิดในการทำนายพฤติกรรม ผลการวิจัยพบว่าพฤติกรรมการป้องกันเป็นผลมาจากปัจจัยต่างๆ ทั้งปัจจัยด้านตัวบุคคล เช่น การรับรู้คุณค่าของข้อมูล ประสบการณ์ในอดีต รวมทั้งบุคลิกภาพ หรือนิสัย เป็นต้น และปัจจัยด้านสภาพแวดล้อม เช่นการให้รางวัล การให้ความรู้เกี่ยวกับความปลอดภัย และแรงผลักดันจากสังคม เป็นต้น (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Pahnila, Siponen, & Mahmood, 2007) แต่ยังไม่พบงานวิจัยที่มุ่งเน้นเปรียบเทียบความสำคัญระหว่างปัจจัยด้านตัวบุคคลและด้านสภาพแวดล้อม รวมทั้งเปรียบเทียบพฤติกรรมการป้องกันภัยระหว่างกลุ่มคนที่มีความแตกต่างกัน เช่นกลุ่มคนที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT people) และกลุ่มคนที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT people) เป็นต้น

จากเหตุผลและความสำคัญดังที่ได้กล่าวมาข้างต้น จึงเป็นที่มาของงานวิจัยนี้ ซึ่งใช้กรอบแนวคิดของทฤษฎีแรงจูงใจเพื่อป้องกัน (Protection motivation theory) เป็นพื้นฐาน และนำปัจจัยที่มีความสำคัญต่อแรงจูงใจในการป้องกันภัยจากงานวิจัยในอดีตมาขยายขอบเขตในการศึกษา โดยมีคำถามวิจัยดังนี้

(1) ปัจจัยใดบ้างที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน

(2) โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีความสอดคล้องกับข้อมูลเชิงประจักษ์หรือไม่

(3) โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ มีความแปรเปลี่ยนหรือไม่เมื่อกลุ่มตัวอย่างมีทักษะด้านเทคโนโลยีสารสนเทศแตกต่างกัน

1.2 วัตถุประสงค์งานวิจัย

(1) เพื่อศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของบุคคลที่ใช้งานคอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน

(2) เพื่อตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีความสอดคล้องกับข้อมูลเชิงประจักษ์

(3) เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ระหว่างกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ

1.3 ขอบเขตงานวิจัย

ขอบเขตการศึกษาของงานวิจัยนี้ คือการศึกษาปัจจัยด้านตัวบุคคลและด้านสภาพแวดล้อมที่ส่งผลต่อการแสดงพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ อันได้แก่เครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desktop computer) และเครื่องคอมพิวเตอร์แบบพกพา (Notebook/Laptop computer) ที่มีการใช้งานทั้งที่บ้านและที่ทำงานทั่วประเทศไทยเท่านั้น ไม่รวมถึงเครื่องคอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet computer) และสมาร์ทโฟน (Smart phone) โดยมุ่งเน้นศึกษาเฉพาะพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ที่แต่ละบุคคลสามารถปฏิบัติได้ด้วยตนเอง

1.4 คำจำกัดความที่ใช้ในการวิจัย

เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) หมายถึงเครื่องคอมพิวเตอร์ขนาดเล็กที่ทำขึ้นไว้ใช้เป็นการเฉพาะหรือส่วนบุคคล หมายรวมถึงคอมพิวเตอร์ตั้งโต๊ะ (Desktop computer) คอมพิวเตอร์แบบพกพา (Laptop computer) และคอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet computer) ซึ่งประกอบด้วย 3 ส่วนหลัก ได้แก่ ฮาร์ดแวร์ (Hardware)

ซอฟต์แวร์ (Software) และอุปกรณ์รับ-แสดงผลข้อมูล เช่น แป้นพิมพ์ และจอภาพ เป็นต้น (สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2551)

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

ผลการวิจัยสามารถนำไปประยุกต์ใช้ได้จริงในทางปฏิบัติในการควบคุมปัจจัยต่างๆ ที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ทั้งนี้จะเป็นประโยชน์ดังนี้

(1) เพื่อเป็นแนวทางให้องค์กรสามารถกำหนดนโยบายและจัดหลักสูตรฝึกอบรมด้านความมั่นคงปลอดภัยที่มีประสิทธิผลในการป้องกันอาชญากรรมคอมพิวเตอร์แก่พนักงานภายในองค์กร

(2) เพื่อเป็นแนวทางในการส่งเสริมและสนับสนุนให้บุคคลทั่วไปสามารถดำเนินการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ด้วยตนเองได้

บทที่ 2
วรรณกรรมและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาแนวคิดและทฤษฎีจากเอกสารงานวิจัยต่างๆ เพื่อนำมากำหนดเป็นกรอบแนวคิดในการวิจัย เรื่องปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ ผู้วิจัยขอนำเสนอผลการศึกษาค้นคว้า ดังนี้

2.1 อาชญากรรมคอมพิวเตอร์ (Computer Crime)

2.2 ทฤษฎีแรงจูงใจเพื่อป้องกัน (Protection Motivation Theory)

2.3 งานวิจัยที่เกี่ยวข้องกับพฤติกรรมหรือการปฏิบัติตามมาตรการป้องกันภัย

2.4 กรอบแนวคิดในการวิจัย

2.5 สมมติฐานงานวิจัย

2.1 อาชญากรรมคอมพิวเตอร์ (Computer Crime)

อาชญากรรมคอมพิวเตอร์หมายถึงการกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ทำให้ผู้ใช้คอมพิวเตอร์นั้นได้รับความเสียหาย เช่น การลักทรัพย์อุปกรณ์คอมพิวเตอร์ เป็นต้น นอกจากนี้ยังหมายรวมถึงการกระทำใดๆ ที่เป็นความผิดทางอาญา ซึ่งจะต้องใช้ความรู้เกี่ยวกับคอมพิวเตอร์ในการกระทำความผิดนั้น เช่น การบิดเบือนข้อมูล (Extortion) การเผยแพร่รูปอนาจารผู้เยาว์ (Child pornography) การฟอกเงิน (Money Laundering) ฉ้อโกง (Fraud) การถอดรหัสโปรแกรมคอมพิวเตอร์ โดยไม่รับอนุญาต แล้วเผยแพร่ให้ผู้อื่นดาวน์โหลดได้ บางครั้งเรียกว่า การโจรกรรมโปรแกรม (Software Pirating) และการขโมยข้อมูลความลับทางการค้าของบริษัท (Corporate Espionage) เป็นต้น (Shelly & Vermaat, 2010)

อาชญากรรมคอมพิวเตอร์เป็นความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มของปัจเจกบุคคลด้วยเหตุจูงใจทางอาญา ที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ ทั้งทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต (ห้องแช็ต อีเมล กระดานประกาศ และกลุ่มข่าว) และโทรศัพท์เคลื่อนที่ (เอสเอ็มเอส/เอ็มเอ็มเอส) (Halder, Jaishankar, & Jaishankar, 2012) ปัจจุบันอาชญากรรมทางคอมพิวเตอร์ถือเป็นอาชญากรรมทางเศรษฐกิจ หรือ อาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ เนื่องจากได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล

อาชญากรรมคอมพิวเตอร์ สามารถแบ่งออกเป็น 5 ประเภท ได้แก่ การโจมตีจากโปรแกรมที่มุ่งร้ายต่อระบบคอมพิวเตอร์ การโจมตีเครื่องคอมพิวเตอร์ผ่านเครือข่าย การลักลอบเข้าใช้งานโดยไม่ได้รับอนุญาต การขโมยและทำลายฮาร์ดแวร์ และการขโมยข้อมูล รายละเอียดตามภาคผนวก ก โดยอาชญากรรมคอมพิวเตอร์แต่ละประเภทมีวิธีการป้องกัน แสดงดังตารางที่ 2.1

ตารางที่ 2.1

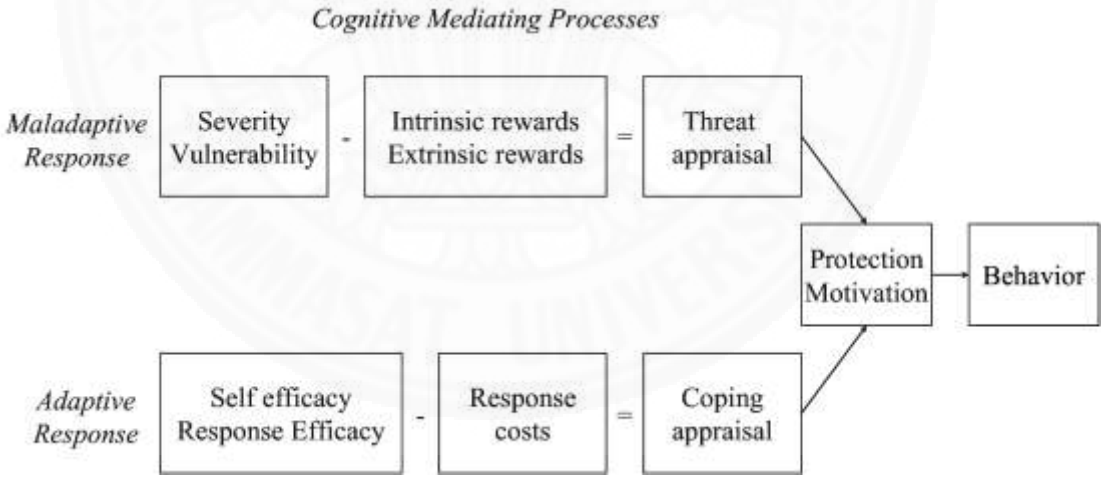
ประเภทของอาชญากรรมคอมพิวเตอร์และวิธีการป้องกัน

ประเภท	วิธีการป้องกัน
การโจมตีจากโปรแกรมที่มุ่งร้ายต่อระบบคอมพิวเตอร์	- ติดตั้งโปรแกรมป้องกันไวรัส (antivirus software) - ติดตั้งโปรแกรมซ่อมแซมหรือปรับปรุงระบบ (software patch) และมีการอัพเดทโปรแกรมอย่างสม่ำเสมอ สำรองข้อมูลและโปรแกรมบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ และไม่เก็บข้อมูลสำรองไว้ในสถานที่เดียวกัน
การโจมตีเครื่องคอมพิวเตอร์ผ่านเครือข่าย	- ติดตั้งโปรแกรมไฟร์วอลล์ (firewall) บนเครื่องคอมพิวเตอร์
การลักลอบเข้าใช้งานโดยไม่ได้รับอนุญาต	- ใช้การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ก่อนเข้าเครื่องคอมพิวเตอร์และระบบต่างๆ - ใช้รหัสผ่านที่ยากต่อการเดาและเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - ไม่เปิดเผยรหัสผ่านต่อบุคคลอื่น รวมทั้งไม่จดบันทึกรหัสผ่านไว้บนโต๊ะหรือบนพื้นที่ที่สามารถมองเห็นได้โดยง่าย
การขโมยและทำลายฮาร์ดแวร์	- วางเครื่องคอมพิวเตอร์ไว้ในที่ปลอดภัยและใช้สายเคเบิลรักษาความปลอดภัยคล้องเครื่องคอมพิวเตอร์เข้ากับวัตถุที่เคลื่อนที่ไม่ได้ - ติดตั้งระบบความปลอดภัยหรือระบบติดตามเครื่องคอมพิวเตอร์ - สำรองข้อมูลและโปรแกรมบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ และไม่เก็บข้อมูลสำรองไว้ในสถานที่เดียวกัน
การขโมยข้อมูล	- ใช้เทคนิคการเข้ารหัส (Encryption) ข้อมูลและโปรแกรมบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

หมายเหตุ. จาก *Discovering Computers 2011: Complete* (น. 555-591) โดย G. Shelly และ M. Vermaat, 2010

2.2 ทฤษฎีแรงจูงใจเพื่อป้องกัน (Protection Motivation Theory)

ทฤษฎีแรงจูงใจเพื่อป้องกัน (Protection motivation theory) ได้รับการพัฒนาขึ้นโดย Rogers ในปี ค.ศ.1975 (Ronald W. Rogers, 1975) ทฤษฎีนี้มีส่วนประกอบร่วมกันระหว่างแบบแผนความเชื่อด้านสุขภาพ (Health Belief Model) และทฤษฎีความคาดหวังในความสามารถตนเอง (Self-Efficacy Theory) ทฤษฎีแรงจูงใจเพื่อป้องกันได้รับการพัฒนาขึ้นเพื่อช่วยสร้างความเข้าใจเกี่ยวกับความกลัวของบุคคล โดยกำหนดตัวแปรที่ทำให้บุคคลเกิดความกลัว 3 ตัวแปรคือ การรับรู้ความรุนแรงของภัย (Perceived Severity) การรับรู้โอกาสเสี่ยงต่อการถูกคุกคาม (Perceived Vulnerability) และความคาดหวังในประสิทธิภาพของการตอบสนอง (Response Efficacy) ซึ่งต่อมาได้รวมตัวแปรความคาดหวังในความสามารถของตนเอง (Self-Efficacy) เพิ่มขึ้น (R. W. Rogers, 1983) กระบวนการที่ทำให้เกิดการรับรู้ในภาพรวมของบุคคลประกอบไปด้วยกระบวนการรับรู้ต่อสภาวะคุกคาม (Threat appraisal) และกระบวนการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (Coping appraisal) จะเป็นตัวเชื่อมโยงไปสู่การเปลี่ยนแปลงความตั้งใจและพฤติกรรมต่อไป แสดงดังภาพที่ 2.1



ภาพที่ 2.1 กระบวนการรับรู้ตามทฤษฎีแรงจูงใจเพื่อป้องกัน จาก *A schematic representation of the cognitive mediating processes of PMT*, โดย R. W. Rogers, 1983

ทฤษฎีแรงจูงใจในการป้องกันเป็นหนึ่งในทฤษฎีที่ถูกนำมาใช้ในการทำนายพฤติกรรมด้านความปลอดภัยของแต่ละบุคคล (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Pahnila et al., 2007; Woon, Tan, & Low, 2005) และพฤติกรรมในการนำเทคโนโลยีมาใช้

ป้องกันภัย (Chenoweth, Minch, & Gattiker, 2009) งานวิจัยในอดีตแสดงให้เห็นว่าการประเมินภัยคุกคามและการประเมินความสามารถในการจัดการกับภัยคุกคามเป็นปัจจัยที่มีอิทธิพลต่อการแสดงพฤติกรรมการรักษาความปลอดภัยในสถานที่ทำงาน (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Workman, Bommer, & Straub, 2008) และที่บ้าน (LaRose, Rifon, & Enbody, 2008; Woon et al., 2005)

2.3 งานวิจัยที่เกี่ยวข้องกับพฤติกรรมหรือการปฏิบัติตามมาตรการป้องกันภัย

จากการศึกษางานวิจัยในอดีตที่นำทฤษฎีแรงจูงใจเพื่อป้องกันมาเป็นกรอบแนวคิดในการวิจัยแล้ว นอกจากนี้ยังมีงานวิจัยที่นำทฤษฎีอื่นๆ มาใช้ในการศึกษาปัจจัยที่ส่งผลต่อการแสดงพฤติกรรมการป้องกันหรือปฏิบัติตามคำแนะนำด้านความปลอดภัย ซึ่งสามารถแยกเป็น 2 ประเภท คือ ปัจจัยส่วนบุคคลและปัจจัยด้านสภาพแวดล้อม ดังนี้

2.3.1 ปัจจัยส่วนบุคคล (Personal Factors)

2.3.1.1 บุคลิกภาพ (Personality)

บุคลิกภาพ (Personality) หมายถึง ลักษณะเฉพาะของบุคคลซึ่งเป็นสิ่งบ่งชี้ความเป็นปัจเจกบุคคล และเป็นสิ่งกำหนดลักษณะการมีปฏิสัมพันธ์กับสิ่งแวดล้อมหรือสถานการณ์ของบุคคลนั้นๆ หนึ่งในทฤษฎีเกี่ยวกับบุคลิกภาพที่ยอมรับกันอย่างแพร่หลายมากที่สุดคือ Big Five Personality Theories โดย Costa และ McCrae (Robert R. McCrae & Paul T. Costa, 1987) ได้จำแนกลักษณะของบุคลิกภาพออกเป็น 5 ประเภทใหญ่ ภายใต้เงื่อนไขว่าคนทุกคนล้วนมีบุคลิกทั้ง 5 แบบในระดับที่ต่างกัน บุคลิกภาพทั้ง 5 แบบคือ บุคลิกภาพแบบเปิดเผย (Extraversion) บุคลิกภาพแบบหวั่นไหว (Neuroticism) บุคลิกภาพแบบประนีประนอม (Agreeableness) บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) และบุคคลิกภาพแบบเปิดรับประสบการณ์ (Openness) รายละเอียดแสดงดังตารางที่ 2.2

ตารางที่ 2.2

คำอธิบายลักษณะบุคลิกภาพ

ประเภท	ลักษณะบุคลิกภาพ
บุคลิกภาพแบบเปิดเผย (Extraversion)	ลักษณะของบุคคลที่ถูกปลุกปั่นได้ง่าย มีความเป็นกันเอง ชอบติดต่อสื่อสารกับผู้อื่น เป็นคนช่างพูดช่างเจรจา กล้าแสดงออกในความคิดของตนเอง และแสดงออกทางอารมณ์ความรู้สึกสูง
บุคลิกภาพแบบประนีประนอม (Agreeableness)	ลักษณะของบุคคลที่มีความสุภาพ เอื้อเฟื้อเผื่อแผ่ ซื่อสัตย์สุจริต มีไหวพริบ เข้าใจและเห็นใจผู้อื่น
บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness)	ลักษณะของบุคคลที่มีความตั้งใจในการทำกิจกรรมต่างๆ เป็นผู้ที่มีระเบียบวินัย มีความแม่นยำ มีความรับผิดชอบ สามารถทำตามคำสั่งให้สำเร็จไปได้ด้วยดี
บุคลิกภาพแบบหวั่นไหว (Neuroticism)	บุคลิกภาพแบบหวั่นไหว คือ องค์ประกอบของบุคลิกภาพด้านอารมณ์ในการตอบสนองต่อสิ่งเร้าต่างๆ
บุคคลิกภาพแบบเปิดรับประสบการณ์ (Openness)	ลักษณะของบุคคลที่มีความรอบรู้ มีสติปัญญาในการปฏิบัติงาน มีจินตนาการ มีความคิดสร้างสรรค์ ยอมรับความคิดของคนอื่น ยึดหลักความจริง ชอบศึกษาหาความรู้ใหม่ๆ มีความสนใจในเรื่องของสังคมและวัฒนธรรม

หมายเหตุ. จาก *Validation of the five-factor model of personality across instruments and observers* โดย McCrae และ Costa, 1987

งานวิจัยในอดีตได้มีการนำทฤษฎี Big Five Personality มาใช้เพื่อหาความสัมพันธ์ระหว่างบุคลิกภาพกับพฤติกรรมการปฏิบัติตามแนวทางการรักษาความปลอดภัยในโลกไซเบอร์ต่อมาได้มีการนำมาใช้ในการหาความสัมพันธ์กับพฤติกรรมการป้องกันภัย งานวิจัยของ Shropshire และคณะ (2006) พบว่าบุคคลที่มีบุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) และแบบประนีประนอม (Agreeableness) จะมีโอกาสถูกคุกคามน้อยกว่าบุคคลที่มีบุคลิกภาพแบบหวั่นไหว (Neuroticism) บุคลิกภาพจึงเป็นจุดเริ่มต้นที่ทำให้เกิดแรงจูงใจที่แตกต่างกันของแต่ละบุคคลในการแสดงพฤติกรรมหรือไม่แสดงพฤติกรรมการป้องกันภัย (Shropshire et al., 2006) สอดคล้องกับงานวิจัยของ Warkentin และคณะ (2011) ซึ่งกล่าวว่าลักษณะบุคลิกภาพที่แตกต่างกัน

จะส่งผลต่อการรับรู้ที่แตกต่างกันด้วย ดังนั้นรูปแบบการให้ความรู้ของกลุ่มคนแต่ละประเภทจึงต้องเหมาะสมกับลักษณะของคนประเภทนั้น

2.3.1.2 การรับรู้คุณค่าของข้อมูล (Perceived Value of data)

งานวิจัยในอดีตได้ให้คำนิยามข้อมูลที่มีคุณค่าว่าเป็นข้อมูลที่มีความสำคัญในการดำเนินธุรกิจที่สามารถส่งผลต่อความสำเร็จหรือล้มเหลวขององค์กรได้ เช่น ข้อมูลในด้านการลงทุน ข้อมูลลับทางการค้า เป็นต้น ซึ่งมีลักษณะเป็นข้อมูลที่ล้าสมัยเร็ว และคุณค่าลดลงตามเวลา (Moody & Walsh, 1999) คุณค่าของข้อมูลที่บุคคลรับรู้นั้นเป็นไปได้ทั้งคุณค่าทางด้านตัวเงินและคุณค่าทางด้านความรู้สึก (Malimage & Warkentin, 2011) งานวิจัยในอดีตได้ทำการศึกษาอิทธิพลของการรับรู้คุณค่าของข้อมูลของบุคคลต่อพฤติกรรมการป้องกันเมื่อเครื่องคอมพิวเตอร์ถูกคุกคาม งานวิจัยของ Chai และคณะ (2009) พบว่าการรับรู้ถึงคุณค่าและความสำคัญของข้อมูลที่เป็นข้อมูลส่วนตัวเป็นแรงจูงใจในการดำเนินการเพื่อป้องกันข้อมูลเหล่านั้น เช่นเดียวกับ Malimage และ Warkentin (2011) ที่กล่าวว่าการรับรู้คุณค่าของข้อมูลมีอิทธิพลต่อความเชื่อของบุคคลที่ว่าการใช้เทคโนโลยีป้องกันเช่น โปรแกรมแอนตีไวรัส เป็นต้น สามารถหยุดยั้งผลกระทบจากการโจมตีของไวรัสคอมพิวเตอร์ได้

2.3.1.3 ประสบการณ์ในอดีต (Prior experience)

ทฤษฎีพฤติกรรมนิยม (Behavioral View of Motivation) ให้ความสำคัญกับประสบการณ์ในอดีตว่ามีผลต่อแรงจูงใจของบุคคลเป็นอย่างมาก ส่วนใหญ่พฤติกรรมของมนุษย์จะได้รับอิทธิพลที่เป็นแรงจูงใจมาจากประสบการณ์ในอดีต โดยประสบการณ์ด้านบวกจะกลายเป็นแรงจูงใจทางบวกที่ส่งผลเร้าให้มนุษย์มีความต้องการแสดงพฤติกรรมในทิศทางนั้นมากยิ่งขึ้น ในขณะที่ประสบการณ์ด้านลบในอดีตจะกลายเป็นแรงจูงใจทางบวกที่ส่งผลเร้าให้มนุษย์มีความต้องการแสดงพฤติกรรมในทิศทางตรงกันข้ามมากยิ่งขึ้นเช่นกัน ประสบการณ์ในอดีตจึงมีผลกระทบต่อการตัดสินใจแสดงพฤติกรรมใดๆ ในปัจจุบัน ซึ่งสอดคล้องกับงานวิจัยของ Chai และคณะ (2009) กล่าวว่าประสบการณ์ในอดีตเช่นการที่เครื่องคอมพิวเตอร์โดนไวรัสหรือถูกขโมยข้อมูลส่วนตัว เป็นปัจจัยที่มีอิทธิพลต่อแรงจูงใจในการป้องกันภัยมากขึ้นเพราะมีความกังวลและไม่ต้องการถูกคุกคามอีกในอนาคต

2.3.2 ปัจจัยด้านสภาพแวดล้อม (Environmental Factors)

2.3.2.1 การคล้อยตามกลุ่มอ้างอิง (Subjective Norm)

การคล้อยตามกลุ่มอ้างอิงหรือบุคคลรอบข้าง เป็นเสมือนแรงกดดันหรือแรงกระตุ้นทางสังคม (Bulgurcu, Cavusoglu, & Benbasat, 2010) การแสดงพฤติกรรมของกลุ่มอ้างอิงจะมีอิทธิพลหรือกระตุ้นให้บุคคลคล้อยตามและแสดงพฤติกรรมเช่นเดียวกันนั้นออกมา (Johnston & Warkentin, 2010) ซึ่งส่วนใหญ่เกิดจากการชักชวนด้วยวาจา (Pahnila et al., 2007)

การให้คำปรึกษาหรือสังเกตจากพฤติกรรมของบุคคลอื่น (M. T. Siponen, Pahnila, & Mahmood, 2010) โดยกลุ่มอ้างอิงอาจเป็นคนใกล้ตัว เช่น เพื่อนร่วมงาน ผู้บังคับบัญชา เพื่อนสนิท หรือคนในครอบครัว เป็นต้น กลุ่มอ้างอิงจะมีอิทธิพลต่อการกระทำพฤติกรรมมากหรือน้อยขึ้นอยู่กับความสำคัญของบุคคลนั้นๆ (Ajzen, 1991)

2.3.2.2 ความรู้เกี่ยวกับการรักษาความปลอดภัย (Security Knowledge)

ปัญหาสำคัญที่ทำให้เกิดภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ในประเทศกำลังพัฒนา คือการขาดความรู้ ขาดทักษะในการรักษาความปลอดภัย และขาดความชำนาญในการใช้ภาษาอังกฤษ เนื่องจากคำแนะนำ คู่มือการใช้งานและเนื้อหาอื่นๆ สำหรับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศส่วนใหญ่เป็นภาษาอังกฤษ ทำให้เกิดการละเลยและปฏิเสธที่จะเรียนรู้แนวทางการป้องกันภัยนั้นด้วยตนเอง (Kshetri, 2010) การให้ความรู้และความเข้าใจถึงภัยจากอาชญากรรมคอมพิวเตอร์และมาตรการป้องกันที่มีประสิทธิภาพ โดยเน้นให้เห็นโอกาสเสี่ยงของการเกิดภัยคุกคามและความรุนแรงของการสูญเสียที่เกิดจากภัยคุกคาม (D'Arcy, Hovav, & Galletta, 2009; H. Liang & Y. Xue, 2010) เป็นปัจจัยสำคัญในการสร้างแรงจูงใจในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ซึ่งจะทำให้การจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ (Bulgurcu, Cavusoglu, & Benbasat, 2009) วิธีการให้ความรู้นั้นไม่ใช่เพียงการฝึกอบรมเท่านั้น แต่ยังรวมถึงการรณรงค์ การโฆษณา การพูดคุยอย่างเป็นทางการหรือไม่เป็นทางการ และการให้ความรู้ผ่านสื่อต่างๆ (M. Siponen, Pahnila, & Mahmood, 2006) นอกจากนี้การรายงานเหตุละเมิดจากภัยคุกคามที่เกิดขึ้นก็เป็นอีกวิธีที่ได้ผล (M. T. Siponen et al., 2010) เช่นเดียวกับที่ Boon-Yuen และคณะ (2009) ได้กล่าวไว้ว่า หลักสูตรการฝึกอบรม การให้ความรู้ผ่านสื่อหรือคำแนะนำจากผู้เชี่ยวชาญเป็นสิ่งกระตุ้นให้เกิดแรงจูงใจและแสดงพฤติกรรมการรักษาความปลอดภัยคอมพิวเตอร์

องค์กรต้องมีกลยุทธ์ในการฝึกอบรมและให้ความรู้ที่เหมาะสมกับพนักงานแต่ละกลุ่มไม่ว่าจะเป็นกลุ่มผู้บริหารระดับสูง กลุ่มผู้บริหารระดับกลาง และพนักงาน สำหรับพนักงานยังสามารถแบ่งได้เป็นพนักงานที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) กับพนักงานที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) กลยุทธ์ในการจัดโปรแกรมฝึกอบรมแก่พนักงานแต่ละกลุ่มต้องแตกต่างกัน (M. T. Siponen et al., 2010) เนื่องจากจะมีพื้นฐานความรู้และความเชี่ยวชาญด้านคอมพิวเตอร์ที่แตกต่างกัน การฝึกอบรมนั้นไม่เพียงสอนให้ผู้ใช้คอมพิวเตอร์มีความเข้าใจถึงวิธีการใช้งานและวิธีป้องกันที่ถูกต้องเท่านั้น แต่ยังต้องเน้นในเรื่องของการสร้างจิตสำนึกและการตระหนักในการป้องกันภัยจากการใช้งานคอมพิวเตอร์ด้วย จึงจะสามารถจูงใจให้ผู้ใช้คอมพิวเตอร์แสดงพฤติกรรมการป้องกันได้ (Lu & Jen, 2010)

2.3.2.3 ค่าใช้จ่ายในการป้องกัน (Safeguard cost)

ความพยายามหรือค่าใช้จ่ายที่ต้องเสียไปเป็นข้อจำกัดต่อการแสดงพฤติกรรมและลดแรงจูงใจในการแสดงพฤติกรรม เนื่องจากโดยปกติบุคคลจะเปรียบเทียบค่าใช้จ่ายที่ต้องเสียไปกับผลประโยชน์ที่ได้รับก่อนที่จะตัดสินใจกระทำหรือไม่กระทำพฤติกรรมใด (H. Liang & Y. Xue, 2010) ถ้าประเมินแล้วว่าค่าใช้จ่ายที่ต้องเสียเพื่อดำเนินการป้องกันสูงเกินไปบุคคลนั้นก็เลือกที่จะยอมรับความเสี่ยง และไม่กระทำการป้องกันใดๆ ในทำนองเดียวกันถ้าค่าใช้จ่ายไม่สูงเกินไปแต่การป้องกันนั้นมีประสิทธิภาพ บุคคลนั้นก็จะตัดสินใจดำเนินการป้องกัน (LaRose, Rifon, Liu, & Lee, 2005; Woon et al., 2005)

2.3.3 การรับรู้ต่อสภาวะคุกคาม (Threat appraisal)

กระบวนการรับรู้ต่อสภาวะคุกคามเกิดจากการ 2 องค์ประกอบสำคัญคือการรับรู้โอกาสเสี่ยงของการถูกคุกคาม (Perceived Vulnerability) และการรับรู้ความรุนแรงของภัยคุกคาม (Perceived Severity) ซึ่งการรับรู้ความรุนแรงของภัย (Perceived Severity) (R. W. Rogers, 1983) นั้นหมายถึงความเชื่อมั่นของบุคคลต่อความรุนแรงจากการที่ไม่มีการป้องกันความเสียหายที่จะเกิดขึ้น โดยเฉพาะอย่างยิ่งความเสียหายที่เกิดขึ้นกับข้อมูลเช่น การสูญเสียข้อมูลอันเป็นความลับ ข้อมูลขาดความสมบูรณ์และไม่พร้อมใช้งาน เป็นต้น ซึ่งส่งผลกระทบต่อองค์กรและพนักงานให้ไม่สามารถปฏิบัติงานได้อย่างต่อเนื่อง งานวิจัยของ Boon-Yuen และคณะ (2009) ได้ทำการศึกษาปัจจัยที่ส่งผลให้พนักงานแสดงพฤติกรรมการป้องกันภัย พบว่าพนักงานมีการรับรู้ความรุนแรงและความเสียหายที่จะเกิดจากการถูกคุกคามในระดับที่แตกต่างกัน ถ้ารับรู้ความรุนแรงมากก็จะรู้สึกกลัวและวิตกกังวลต่อความเสียหายที่จะเกิดขึ้นซึ่งเป็นเหตุให้บุคคลนั้นแสดงพฤติกรรมการป้องกันภัยมากยิ่งขึ้น ส่วนการรับรู้โอกาสเสี่ยงของการถูกคุกคามมาจากแบบแผนความเชื่อด้านสุขภาพ (Health Belief Model) หมายถึงความเชื่อของบุคคลที่มีผลโดยตรงต่อคำแนะนำในการป้องกันภัย บุคคลจะมีการรับรู้โอกาสเสี่ยงของการถูกคุกคามที่แตกต่างกันแม้ว่าจะได้รับข้อมูลที่เหมือนกันก็ตาม ซึ่งจะส่งผลต่อพฤติกรรมการป้องกันภัยที่แตกต่างกันตามไปด้วย (Ng et al., 2009) สามารถสรุปได้ว่าการให้ข้อมูลเกี่ยวกับความน่าจะเป็นของการถูกคุกคามส่งผลให้บางคนรับรู้ว่ามีความเสี่ยงสูงที่จะถูกคุกคามในขณะที่บางคนรับรู้ว่าโอกาสเสี่ยงนั้นจะไม่มีทางเกิดขึ้น บุคคลจะประเมินความเป็นไปได้ที่ตนเองจะถูกคุกคามประกอบกับประเมินว่าภัยนั้นมีความรุนแรงมากน้อยเพียงใดรวมทั้งคาดคะเนโอกาสที่จะเกิดซ้ำ ดังนั้นแต่ละบุคคลจะมีความเชื่อมั่นต่อภาวะการเกิดภัยคุกคามในระดับที่แตกต่างกัน

2.3.4 การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (Coping appraisal)

กระบวนการรับรู้ความสามารถในการจัดการกับภัยคุกคามประกอบไปด้วยประสิทธิภาพในการตอบสนอง (Response Efficacy) และ การรับรู้ความสามารถของตนเอง (Self-Efficacy) (R. W. Rogers, 1983) การรับรู้ความสามารถในการจัดการกับภัยคุกคามเกิดขึ้นเมื่อบุคคล

นั้นได้ประเมินประสิทธิภาพในการตอบสนองซึ่งเป็นความเชื่อมั่นของบุคคลต่อประสิทธิภาพของวิธีการหรือมาตรการในการป้องกันภัยที่ได้รับการแนะนำรวมกับการประเมินความความสามารถของตนเองที่จะกระทำตามมาตรการนั้น เช่น การติดตั้งโปรแกรม Antivirus หรือการปิดการใช้งาน cookie บนเว็บบราวเซอร์ เป็นต้น เมื่อรับรู้ความสามารถในการจัดการกับภัยคุกคามแล้ว ก็จะส่งผลต่อการแสดงพฤติกรรมการป้องกัน งานวิจัยหลายงานในอดีตได้ทำการพิสูจน์แล้วว่า บุคคลจะมีแรงจูงใจในการดำเนินการป้องกันภัยเพิ่มมากขึ้นถ้าระดับความเชื่อมั่นต่อประสิทธิภาพในการตอบสนองและความเชื่อมั่นในตนเองเพิ่มสูงขึ้น (H. Liang & Y. Xue, 2010; Ng et al., 2009; Woon et al., 2005; Workman et al., 2008)

2.3.5 แรงจูงในในการป้องกัน (Protection Motivation)

ทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory) กล่าวว่าแรงจูงใจเกิดจากการเรียนรู้ทางสังคมและเป็นปัจจัยสำคัญในการทำนายการแสดงพฤติกรรมของบุคคล (Ajzen, 1991) แรงจูงใจเป็นตัวพยากรณ์ที่ดีในการทำนายพฤติกรรมที่จะแสดงออกมาจริงๆของบุคคล (M. Siponen et al., 2006) กล่าวคือเมื่อมีปัจจัยที่มีอิทธิพลให้บุคคลเกิดแรงจูงใจในการป้องกันภัยเพิ่มมากขึ้น พฤติกรรมการป้องกันภัยที่แสดงออกมาก็จะเพิ่มมากขึ้นเช่นเดียวกัน (Bulgurcu et al., 2009; H. Liang & Y. Xue, 2010; Ng et al., 2009)

2.3.6 พฤติกรรมการป้องกันภัย (Protection Behavior)

งานวิจัยของ Siponen และคณะ (2006) พบว่าการที่บุคคลจะแสดงพฤติกรรมการป้องกันภัยนั้น ต้องได้นั้นเกิดจากปัจจัยต่างๆ ทั้งส่วนบุคคลเองเช่น ทัศนคติ ทัศนวิสัย และปัจจัยจากภายนอกที่ส่งเสริมให้บุคคลนั้นเกิดกระบวนการเรียนรู้และวิเคราะห์ว่าจะแสดงพฤติกรรมใดออกมา เช่น แรงกระตุ้นจากหัวหน้างาน การให้การอบรม หรือคู่มือเกี่ยวกับการรักษาความปลอดภัย เป็นต้น

จากการศึกษาทฤษฎี เอกสาร และงานวิจัยที่เกี่ยวข้องกับปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันหรือปฏิบัติตามคำแนะนำด้านความปลอดภัย ผู้วิจัยได้สรุปปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ มีรายละเอียดแสดงดังตารางที่ 2.3

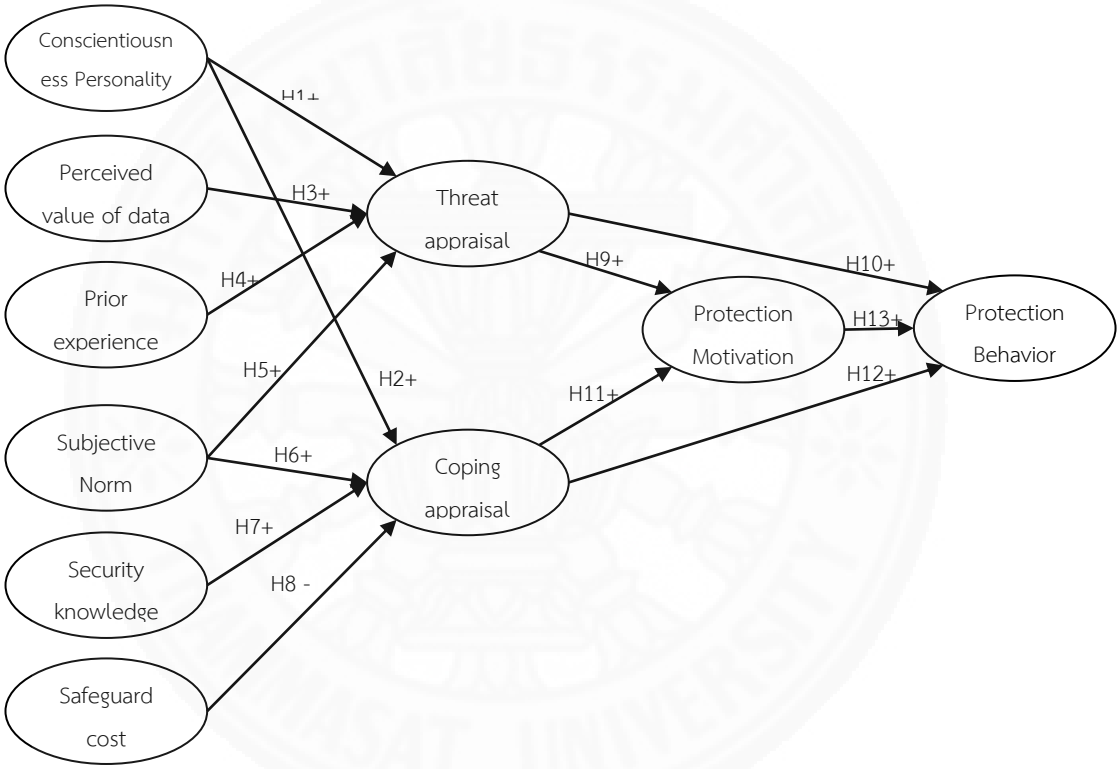
ตารางที่ 2.3

ผลงานวิจัยที่เกี่ยวข้องกับตัวแปรที่อยู่ในกรอบแนวคิดการวิจัย

	(Anderson & Agarwal, 2010)	(Bulgurcu et al., 2009)	(Bulgurcu et al., 2010)	(Chai, Bagchi-Sen, et al., 2009)	(Chenoweth et al., 2009)	(D'Arcy et al., 2009)	(Herath & Rao, 2009)	(Ifinedo, 2012)	(Johnston & Warkentin, 2010)	(Kirsch & Boss, 2007)	(LaRose et al., 2008)	(LaRose et al., 2005)	(Li & Siponen, 2011)	(H. Liang & Y. Xue, 2010)	(Lu & Jen, 2010)	(Malimage & Warkentin, 2011)	(Ng et al., 2009)	(Pahnila et al., 2007)	(H.-S. Rhee, C.-T. Kim, & Y. U. Ryu, 2009)	(Shropshire et al., 2006)	(M. Siponen et al., 2006)	(M. T. Siponen et al., 2010)	(Vance, Siponen, & Pahnila, 2009)	(Warkentin et al., 2011)	(Woon et al., 2005)	(Workman et al., 2008)
Conscientiousness Personality																				✓				✓	✓		
perceived value of data				✓												✓	✓										
Prior experience				✓																							
Safeguard cost			✓		✓	✓	✓	✓			✓	✓	✓	✓	✓	✓			✓							✓	✓
Security knowledge		✓	✓			✓		✓			✓		✓		✓		✓					✓				✓	✓
Subjective Norm	✓		✓					✓	✓	✓	✓		✓					✓				✓	✓			✓	✓
Threat appraisal	✓		✓		✓			✓	✓	✓	✓			✓		✓		✓				✓		✓		✓	✓
Coping appraisal	✓				✓			✓	✓	✓	✓			✓		✓		✓				✓		✓		✓	✓
Protection Motivation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protection Behavior	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

2.4 กรอบแนวคิดในการวิจัย

จากการทบทวนวรรณกรรม รวมถึงศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง ทำให้สามารถพัฒนากรอบแนวคิดของปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกัน ซึ่งเป็นการบูรณาการกรอบแนวคิดมาจากงานวิจัยในอดีต โดยพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ซึ่งเป็นตัวแปรตามได้รับผลมาจากตัวแปรอิสระซึ่งประกอบด้วยปัจจัยด้านบุคคลและปัจจัยด้านสภาพแวดล้อม แสดงดังภาพที่ 2.2 และมีรายละเอียดคำนิยามของตัวแปร แสดงดังตารางที่ 2.4



ภาพที่ 2.2 กรอบแนวคิดของงานวิจัย (Conceptual Model)

ตารางที่ 2.4

คำนิยามตัวแปร

ตัวแปร	คำนิยาม	อ้างอิง
บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness Personality)	บุคลิกภาพแบบมีจิตสำนึก หมายถึงบุคคลที่มีความตั้งใจในการทำกิจกรรมต่างๆ เป็นผู้ที่มีระเบียบวินัย มีความแม่นยำ มีความรับผิดชอบ สามารถทำตามคำสั่งให้สำเร็จไปได้ด้วยดี	(Shropshire et al., 2006)
การรับรู้คุณค่าของข้อมูล (Perceived Value of data)	การรับรู้คุณค่า หมายถึงการให้ความสำคัญต่อข้อมูลหรือทรัพย์สิน ทั้งในรูปแบบของคุณค่าที่เป็นตัวเงินและความรู้สึก ซึ่งแต่ละคนจะให้ระดับความสำคัญต่อข้อมูลที่แตกต่างกัน	(Chai, Bagchi-Sen, et al., 2009)
ประสบการณ์ในอดีต (Prior experience)	ประสบการณ์ในอดีต หมายถึงการที่บุคคลเคยพบเจอเหตุการณ์ถูกละเมิดหรือถูกคุกคามมาก่อน	(Chai, Bagchi-Sen, et al., 2009)
การคล้อยตามกลุ่มอ้างอิง (Subjective norm)	การคล้อยตามกลุ่มอ้างอิง หมายถึงการรับรู้เกี่ยวกับความกดดันทางสังคมที่มีต่อการดึงดูดความสนใจของบุคคล ให้กระทำหรือไม่กระทำพฤติกรรมหนึ่งๆ	(Anderson & Agarwal, 2010)
ความรู้ด้านความปลอดภัย (Security Knowledge)	ความรู้ด้านความปลอดภัย หมายถึงความรู้ ความเข้าใจเกี่ยวกับภัยจากอาชญากรรมคอมพิวเตอร์และมาตรการป้องกัน ซึ่งอาจเกิดจากการได้รับการฝึกอบรม การสื่อสารจากแหล่งต่างๆ เป็นต้น	(M. Siponen et al., 2006)
ค่าใช้จ่ายในการป้องกัน (Safeguard cost)	ค่าใช้จ่ายในการตอบสนอง หมายถึงค่าใช้จ่ายที่รับรู้ได้ของแต่ละบุคคลในการปฏิบัติตามคำแนะนำหรือใช้มาตรการเพื่อป้องกันอาชญากรรมคอมพิวเตอร์ อาจเป็นค่าใช้จ่ายที่เป็นตัวเงิน ความไม่สะดวก ความยากลำบาก หรือผลข้างเคียงจากการใช้มาตรการป้องกัน	(H. Liang & Y. Xue, 2010; Woon et al., 2005)

ตารางที่ 2.4

คำนิยามตัวแปร (ต่อ)

ตัวแปร	คำนิยาม	อ้างอิง
การรับรู้ต่อสภาวะคุกคาม (Threat appraisal)	การรับรู้ต่อสภาวะคุกคามเกิดจากการประเมินระดับความเป็นไปได้ที่ตนเองจะถูกคุกคามและประเมินระดับความรุนแรงและความเสียหายที่จะเกิดขึ้นหากเกิดภัยคุกคามขึ้น	(Ng et al., 2009)
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (Coping appraisal)	การรับรู้ความสามารถในการจัดการกับภัยคุกคามเกิดจากการประเมินระดับความเชื่อมั่นในประสิทธิภาพของมาตรการที่นำมาใช้ในการตอบสนองต่อภัยคุกคามนั้นและความเชื่อมั่นในทักษะ ความรู้ และความสามารถของตนเองในการแสดงพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ให้ประสบความสำเร็จได้	(Ng et al., 2009)
แรงจูงใจในการป้องกัน (Protection Motivation)	แรงจูงใจในการป้องกัน หมายถึงเมื่อมีสิ่งที่มากระตุ้นหรือโน้มน้าวใจแล้วเกิดความพยายามที่จะป้องกันอาชญากรรมคอมพิวเตอร์ โดยสิ่งกระตุ้นนั้นเป็นสิ่งผลักดันจากส่วนบุคคลซึ่งอาจจะเป็นเจตคติ ความคิด ความสนใจ ความตั้งใจ การมองเห็นคุณค่า ความพอใจ ความต้องการฯลฯ หรือเป็นสิ่งผลักดันภายนอกตัวบุคคลที่มากระตุ้นให้เกิดพฤติกรรมอาจจะเป็นการได้รับรางวัล เกียรติยศชื่อเสียง คำชม หรือยกย่อง	(H. Liang & Y. L. Xue, 2010)
พฤติกรรมการป้องกัน (Protection Behavior)	พฤติกรรมการป้องกัน หมายถึงอาการที่แสดงออกถึงการปฏิบัติหรือกระทำการเพื่อป้องกันอาชญากรรมคอมพิวเตอร์ที่คาดว่าจะเกิดขึ้นเพื่อตอบสนองต่อสิ่งเร้า	(H. Liang & Y. Xue, 2010)

2.5 สมมติฐานงานวิจัย

ความสัมพันธ์ระหว่างบุคลิกภาพแบบมีจิตสำนึกกับการรับรู้ต่อสภาวะคุกคามและการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ตามทฤษฎีแรงจูงใจเพื่อป้องกัน การที่บุคคลจะแสดงพฤติกรรมใดๆ นั้นมีจุดเริ่มต้นที่ทำให้เกิดกระบวนการรับรู้ที่นำไปสู่การตัดสินใจซึ่งก็คือบุคลิกภาพ บุคลิกภาพที่แตกต่างกันทำให้เกิดการตัดสินใจที่แตกต่างกัน ดังนั้นแต่ละบุคคลจึงมีการแสดงพฤติกรรมที่แตกต่างกันออกไป จากทฤษฎีบุคลิกภาพ 5 องค์ประกอบ หรือ Big Five Personality Theories โดย Costa และ McCrae (2004) ได้ระบุอุปนิสัยอย่างหนึ่งของบุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) ไว้ว่าสามารถเผชิญปัญหาและเหตุการณ์ที่อยู่ในภาวะกดดันได้ (Jones, Meijen, McCarthy, & Sheffield, 2009) จากผลการศึกษาของ Vance และคณะ (2009) พบว่า บุคลิกภาพแบบมีจิตสำนึกเป็นบุคคลิกภาพที่ส่งเสริมให้เกิดกระบวนการการรับรู้ต่อสภาวะคุกคามและการรับรู้ความสามารถในการจัดการกับภัยคุกคาม ซึ่งเป็นแรงจูงใจที่นำไปสู่การแสดงพฤติกรรมการป้องกัน เช่นเดียวกับ Shropshire และคณะ (2006) ที่พบว่าบุคลิกภาพแบบมีจิตสำนึกมีความสัมพันธ์อย่างยิ่งกับการที่พนักงานภายในองค์กรรับรู้ว่าตนเองสามารถที่จะจัดการกับภัยคุกคามได้โดยการนำเทคโนโลยีมาใช้ป้องกันอาชญากรรมคอมพิวเตอร์ตามนโยบายขององค์กร นอกจากนี้ผลการวิจัย Warkentin และ Willison (2009) ยังพบว่าบุคคลที่มีลักษณะเช่นนี้จะทำการประเมินโอกาสเสี่ยงและความเสียหายที่อาจจะเกิดจากภัยคุกคามบนอินเทอร์เนต และทำการประเมินความสามารถของตนเองว่าสามารถที่ดำเนินการลดหรือกำจัดภัยคุกคามนั้นได้อย่างไร สำหรับงานวิจัยจึงมุ่งเน้นที่บุคลิกภาพแบบมีจิตสำนึกเพียงลักษณะเดียว ดังนั้นบุคคลที่มีบุคลิกภาพแบบมีจิตสำนึกจะประเมินสภาวะการถูกคุกคามและความสามารถในการจัดการกับภัยคุกคาม (Devaraj, Easley, & J. Michael Crant, 2007; M. Siponen et al., 2006a; Vance, Suponen, & Pahnila, 2009) สามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 1: บุคลิกภาพแบบมีจิตสำนึกส่งผลเชิงบวกต่อการรับรู้ต่อสภาวะคุกคาม

สมมติฐานที่ 2: บุคลิกภาพแบบมีจิตสำนึกส่งผลเชิงบวกต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ความสัมพันธ์ระหว่างการรับรู้คุณค่าของข้อมูลกับการรับรู้ต่อสภาวะคุกคาม

ผลจากงานวิจัยในอดีตพบว่าการรับรู้และให้ความสำคัญกับข้อมูลจะส่งผลต่อการเพิ่มแรงจูงใจในการแสดงพฤติกรรมเพื่อดำเนินกิจกรรมที่เกี่ยวข้องกับการปกป้องข้อมูลนั้น (Chai, Bagchi-Sen, et al., 2009; Warkentin & Willison, 2009) นอกจากนี้ยังพบว่าผู้ใช้คอมพิวเตอร์ที่

ให้ความสำคัญกับข้อมูลที่มีความเป็นส่วนตัวสูงมีแนวโน้มที่จะปกป้องข้อมูลส่วนบุคคลนั้น มากกว่าผู้ที่ให้ความสำคัญกับข้อมูลต่ำกว่า (Chai, Bagchi-Sen, et al., 2009) และการรับรู้คุณค่าของข้อมูลมีอิทธิพลโดยตรงต่อพฤติกรรมการติดตั้งและใช้งานโปรแกรมป้องกันไวรัส (Warkentin & Malimage, 2010) ถ้าบุคคลรับรู้ว่าข้อมูลที่จัดเก็บอยู่ในเครื่องคอมพิวเตอร์นั้นมีคุณค่าสูง ก็มีแนวโน้มที่จะรับรู้ถึงผลกระทบและความรุนแรงของภัยคุกคามจากไวรัสคอมพิวเตอร์มากขึ้น และจะหาวิธีการที่จำเป็นเพื่อยับยั้งการคุกคามที่จะเกิดขึ้น จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 3: การรับรู้คุณค่าของข้อมูลส่งผลเชิงบวกต่อการรับรู้ต่อสภาวะคุกคาม

ความสัมพันธ์ระหว่างประสบการณ์ในอดีตกับการรับรู้ต่อสภาวะคุกคาม

ประสบการณ์ที่ไม่ดีในอดีตที่เกิดขึ้นโดยตรงกับตนเองเช่นเครื่องคอมพิวเตอร์ที่ใช้งานถูกคุกคามจากไวรัสคอมพิวเตอร์จนได้รับความเสียหายเป็นต้น จะส่งผลให้บุคคลนั้นรับรู้ว่าตนเองมีโอกาสเสี่ยงที่จะถูกคุกคามและรับรู้ว่าการถูกคุกคามนั้นมีความรุนแรงเพียงใด ซึ่งจะส่งผลให้บุคคลนั้นแสดงพฤติกรรมเพื่อป้องกันไม่ให้เกิดภัยคุกคามอีก (Chai, Sharmistha, Claudia, R., & J., 2009; H.-S. Rhee, C. Kim, & Y. U. Ryu, 2009) งานวิจัยในอดีตจำนวนไม่มากนักที่นำประสบการณ์ในอดีตมาหาความสัมพันธ์กับแรงจูงใจในการป้องกัน ดังนั้นการศึกษาในครั้งนี้จึงมุ่งพิสูจน์ว่าถ้าบุคคลเคยได้รับความเสียหายโดยตรงจากการประสบภัยคุกคามในอดีต จะมีอิทธิพลต่อการรับรู้ต่อสภาวะคุกคามด้านความปลอดภัยมากกว่าคนที่ไม่เคยถูกคุกคามมาก่อน จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 4: ประสบการณ์ในอดีตส่งผลเชิงบวกต่อการรับรู้ต่อสภาวะคุกคาม

ความสัมพันธ์ระหว่างการคล้อยตามกลุ่มอ้างอิงกับการรับรู้ต่อสภาวะคุกคามและการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ตามทฤษฎีการกระทำตามแผน (Theory of Planned behavior) การคล้อยตามกลุ่มอ้างอิงเป็นปัจจัยหนึ่งที่สามารถทำนายพฤติกรรมของบุคคลได้ (Ajzen, 1991) เป็นไปตามงานวิจัยของ Bulgurcu และคณะ (2010) Tejaswini Herath และ H. Raghav Rao (2009) ที่พบว่าการคล้อยตามกลุ่มอ้างอิงมีอิทธิพลต่อความตั้งใจของบุคคลในการที่จะปฏิบัติตนให้สอดคล้องกับนโยบายด้านความปลอดภัย กลุ่มอ้างอิงเป็นเสมือนแรงจูงใจให้เกิดกระบวนการเรียนรู้และรับรู้สภาวะคุกคาม กล่าวคือการที่บุคคลเห็นพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของคนรอบข้างไม่ว่าจะเป็นคนในครอบครัว เพื่อน หัวหน้างาน หรือเพื่อนร่วมงาน จะทำให้เกิดกระบวนการรับรู้ว่าภัยนั้นมีความรุนแรงและมีโอกาสเกิดขึ้นกับตนด้วย รวมทั้งการแสดงพฤติกรรมการป้องกันอาชญากรรม

คอมพิวเตอร์ของกลุ่มอ้างอิงก็เป็นแรงกดดันหรือแรงกระตุ้นให้บุคคลเกิดการเรียนรู้และลอกเลียนพฤติกรรมนั้น (LaRose et al., 2008; Pahnila et al., 2007; Zhang, Reithel, & Li, 2009) การที่บุคคลรับรู้แรงกดดันจากบุคคลรอบข้างมากเท่าไรก็จะส่งผลต่อการรับรู้ความสามารถในการจัดการภัยคุกคามมากขึ้นเท่านั้น (Li & Siponen, 2011; Pahnila et al., 2007) จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 5: การคล้อยตามกลุ่มอ้างอิงส่งผลเชิงบวกต่อการรับรู้ต่อสภาวะคุกคาม

สมมติฐานที่ 6: การคล้อยตามกลุ่มอ้างอิงส่งผลเชิงบวกต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ความสัมพันธ์ระหว่างความรู้ด้านความปลอดภัยกับการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

การให้ความรู้เกี่ยวกับภัยคุกคามเป็นปัจจัยที่กระตุ้นให้เกิดกระบวนการเรียนรู้ซึ่งนำไปสู่แรงจูงใจในการแสดงพฤติกรรมการป้องกันภัย (M. Siponen et al., 2006) ซึ่งกระบวนการเรียนรู้ดังกล่าวเกิดจากการที่บุคคลได้รับความรู้เกี่ยวกับภัยคุกคามความปลอดภัยข้อมูลและความรู้เกี่ยวกับวิธีการที่จะต้องดำเนินการเพื่อป้องกันภัย แล้วนำความรู้นั้นมาประเมินความสามารถในการจัดการภัยของตนเอง (Bulgurcu et al., 2009, 2010) องค์กรสามารถจัดทำแนวทางการรักษาความปลอดภัยที่เน้นการให้ความรู้เกี่ยวกับวิธีหรือมาตรการในการป้องกันภัยที่มีประสิทธิภาพเพื่อส่งเสริมพฤติกรรมการป้องกันภัยของพนักงานได้ (Gordon et al., 2006) เช่นเดียวกับ Boon-Yuen และคณะ (2009) ที่พบว่าการจัดหลักสูตรอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยคอมพิวเตอร์และให้ความรู้เกี่ยวกับวิธีในการป้องกันภัยเป็นการส่งเสริมให้พนักงานเกิดความตั้งใจในการที่จะปฏิบัติตาม นอกจากนี้หลักสูตรอบรมทั้งที่เป็นการให้ความรู้เกี่ยวกับการใช้งานคอมพิวเตอร์อย่างปลอดภัยและการสร้างจิตสำนึกและความตระหนักด้านความปลอดภัยมีอิทธิพลทำให้ผู้ใช้คอมพิวเตอร์เกิดการรับรู้ความสามารถในการจัดการกับภัยคุกคามนั้นเพิ่มมากขึ้นซึ่งจะนำมาซึ่งแรงจูงใจในการเปลี่ยนแปลงพฤติกรรมการป้องกันภัยมากขึ้นด้วย (Lu & Jen, 2010) แต่สำหรับผู้ใช้งานที่บ้านจะไม่ได้รับการฝึกอบรมด้านความปลอดภัยอย่างเป็นทางการ ต้องใช้การเรียนรู้ด้วยตัวเองผ่านสื่อต่างๆ เช่น หนังสือพิมพ์ วิทยุ โทรทัศน์หรือเว็บไซต์เป็นต้น (Li & Siponen, 2011) การศึกษาในครั้งนี้จึงเป็นการทดสอบว่าการที่บุคคลได้รับการอบรมด้านความปลอดภัยไม่ว่าจะแบบทางการหรือไม่ทางการมากขึ้นส่งผลให้การรับรู้ความสามารถในการจัดการกับภัยคุกคามเพิ่มมากขึ้นตามไปด้วย จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 7: ความรู้ด้านความปลอดภัยส่งผลเชิงบวกต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ความสัมพันธ์ระหว่างค่าใช้จ่ายในการป้องกันกับการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ค่าใช้จ่ายในการป้องกันเป็นค่าใช้จ่ายที่บุคคลนั้นรับรู้ได้ว่าจะเกิดขึ้นหากปฏิบัติตามมาตรการในการป้องกันภัยที่ได้รับการแนะนำ เช่นการติดตั้งซอฟต์แวร์ป้องกันสปายแวร์ เป็นต้น ซึ่งไม่ใช่เพียงค่าใช้จ่ายที่เป็นตัวเงินเท่านั้น ยังรวมถึงค่าใช้จ่ายอื่นๆ เช่น เวลา แรงงาน หรือความไม่สะดวกสบายภายหลังการติดตั้งเป็นต้น (Chenoweth et al., 2009) การประเมินความเหมาะสมของค่าใช้จ่ายขึ้นอยู่กับการรับรู้คุณค่าของบุคคลต่อข้อมูลหรือทรัพย์สินที่ต้องการป้องกัน (Workman et al., 2008) ค่าใช้จ่ายที่ต้องสูญเสียไปจะส่งผลต่อการเพิ่มหรือลดความสามารถในการจัดการภัยคุกคาม บุคคลจะรับรู้ความสามารถในการป้องกันภัยเพิ่มมากขึ้นถ้าค่าใช้จ่ายในการป้องกันภัยไม่แพงเกินไป (H. Liang & Y. Xue, 2010) งานวิจัยของ LaRose และคณะ (LaRose et al., 2008; LaRose et al., 2005) พบว่าค่าใช้จ่ายมีผลต่อการตัดสินใจเลือกมาตรการในการป้องกันภัยกล่าวคือบุคคลจะเลือกมาตรการป้องกันที่มีค่าใช้จ่ายต่ำแต่ประสิทธิภาพในการป้องกันมากกว่ามาตรการที่มีค่าใช้จ่ายสูง นอกจากนี้ Woon และคณะ (Woon et al., 2005) ได้แสดงให้เห็นว่าค่าใช้จ่ายในการตอบสนองมีความสัมพันธ์กับความตั้งใจที่จะป้องกันภัยคือถ้าประเมินค่าใช้จ่ายในการตอบสนองต่ำก็จะมีความมุ่งมั่นที่จะดำเนินการป้องกันภัย สำหรับในงานวิจัยนี้จะเน้นศึกษาค่าใช้จ่ายในการตอบสนองที่เป็นตัวเงินและความไม่สะดวกสบายในการนำมาตรการเพื่อป้องกันภัยจากอาชญากรรมคอมพิวเตอร์มาติดตั้งที่เครื่องคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ ถ้าบุคคลประเมินค่าใช้จ่ายในการป้องกันแล้วพบว่ามีราคาสูงเกินไปหรือการใช้งานยุ่งยากซับซ้อนมากเกินไป ก็จะเกิดการรับรู้ว่าตนเองไม่มีความสามารถในการนำมาตรการมาติดตั้งลดลง จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 8: ค่าใช้จ่ายในการตอบสนองส่งผลเชิงลบต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

ความสัมพันธ์ระหว่างการรับรู้ต่อสภาวะคุกคามกับแรงจูงใจในการป้องกันและพฤติกรรมการป้องกัน

หลักสำคัญของทฤษฎีแรงจูงใจเพื่อป้องกันคือระดับความกังวลที่แต่ละบุคคลรับรู้เกี่ยวกับภัยคุกคามที่อาจเกิดขึ้น ซึ่งเกิดจากกระบวนการรับรู้โอกาสเสี่ยงของการถูกคุกคามและความรุนแรงจากการถูกคุกคาม (Ronald W. Rogers, 1975) การรับรู้สภาวะคุกคามมีความสัมพันธ์ต่อ

ทัศนคติหรือแรงจูงใจที่จะปฏิบัติตามนโยบายด้านความปลอดภัย (Pahnila et al., 2007) และการแสดงพฤติกรรมด้านความปลอดภัย (Lee & Larsen, 2009; Woon et al., 2005; Workman et al., 2008) โดยแต่ละบุคคลนั้นจะรับรู้ต่อสภาวะคุกคามในระดับที่แตกต่างกัน (Ng et al., 2009) การที่แต่ละบุคคลรับรู้ต่อสภาวะคุกคามมากขึ้นเท่าไร ก็ยิ่งส่งผลต่อแรงจูงใจในการดำเนินการป้องกันภัยมากขึ้นเท่านั้น (Lee & Larsen, 2009; H. Liang & Y. Xue, 2010; Pahnila et al., 2007; Woon et al., 2005) รวมทั้งระดับการรับรู้ต่อสภาวะคุกคามนั้นยังสามารถส่งผลโดยตรงต่อการแสดงพฤติกรรมการป้องกันภัยที่มากขึ้นอีกด้วย (Anderson & Agarwal, 2010; Workman et al., 2008) สร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 9: การรับรู้ต่อสภาวะคุกคามส่งผลเชิงบวกต่อแรงจูงใจในการป้องกัน

สมมติฐานที่ 10: การรับรู้ต่อสภาวะคุกคามส่งผลเชิงบวกต่อพฤติกรรมการป้องกัน

ความสัมพันธ์ระหว่างการการรับรู้ความสามารถในการจัดการกับภัยกับแรงจูงใจในการป้องกันและพฤติกรรมการป้องกัน

การรับรู้ความสามารถในการจัดการกับภัยคุกคามเกิดจากการประเมินประสิทธิภาพของมาตรการหรือวิธีการที่จะนำมาใช้ในการตอบสนองและความสามารถของตนเองในการที่จะดำเนินการจัดการกับภัย (Rogers, 1975) การรับรู้ความสามารถในการจัดการกับภัยคุกคามเป็นปัจจัยสำคัญที่สามารถนำมาอธิบายแรงจูงใจและความตั้งใจในการปฏิบัติตามนโยบายด้านการรักษาความปลอดภัย (Anderson & Agarwal, 2010; Pahnila et al., 2007) จากการศึกษาในอดีตพบว่าการที่บุคคลรับรู้ความสามารถในการจัดการกับภัยคุกคามในระดับที่สูงขึ้น จะยิ่งมีโอกาสน้อยลงที่จะละเว้นไม่แสดงพฤติกรรมการป้องกันภัยไม่ว่าเป็นในที่ทำงาน (Bulgurcu et al., 2010; Lee & Larsen, 2009; Workman et al., 2008) และที่บ้าน (Woon et al., 2005) บุคคลรับรู้ว่าตนเองมีความสามารถในการจัดการกับภัยคุกคามอย่างมีประสิทธิภาพ ก็จะเป็นแรงจูงใจให้บุคคลนำมาตรการการนั้นมาใช้งานเพิ่มมากขึ้น หรือสามารถส่งผลโดยตรงต่อการแสดงพฤติกรรมการป้องกันภัยที่มากขึ้นอีกด้วย (Anderson & Agarwal, 2010; Workman et al., 2008) สร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 11: การรับรู้ความสามารถในการจัดการกับภัยคุกคามส่งผลเชิงบวกต่อแรงจูงใจในการป้องกัน

สมมติฐานที่ 12: การรับรู้ความสามารถในการจัดการกับภัยคุกคามส่งผลเชิงบวกต่อพฤติกรรมการป้องกัน

ความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันกับพฤติกรรมการป้องกัน

แรงจูงใจหรือความตั้งใจแสดงพฤติกรรมการป้องกัน สามารถทำนายพฤติกรรมที่บุคคลจะปฏิบัติอย่างนั้นจริงได้อย่างแม่นยำ (Ajzen, 1991) ซึ่งเป็นไปตามผลการวิจัยในอดีต (Herath & Rao, 2009; H. Liang & Y. Xue, 2010; Malimage & Warkentin, 2011; M. Siponen et al., 2006) ดังนั้นบุคคลที่มีแรงจูงใจในการป้องกันภัยมีอิทธิพลอย่างยิ่งต่อการแสดงพฤติกรรมการป้องกัน จึงสามารถสร้างสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 13: แรงจูงใจในการป้องกันส่งผลเชิงบวกต่อพฤติกรรมการป้องกัน

บทที่ 3
วิธีการวิจัย

การวิจัยครั้งนี้เป็นการศึกษาความสัมพันธ์เชิงสาเหตุพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของบุคคลที่ใช้งานคอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน โดยมีวิธีดำเนินการวิจัย ดังนี้

3.1 ประชากร

ประชากรที่ใช้ในการศึกษาครั้งนี้ คือผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ได้แก่เครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desktop computer) และเครื่องคอมพิวเตอร์แบบพกพา (Notebook/Laptop computer) ที่มีการใช้งานทั้งที่บ้านและที่ทำงานทั่วประเทศไทย ซึ่งในการศึกษาครั้งนี้จะไม่รวมถึงแท็บเล็ตคอมพิวเตอร์ (tablet computer) และสมาร์ทโฟน (smart phone/mobile) เนื่องจากไม่สามารถระบุจำนวนประชากรที่ชัดเจนได้ ทราบเพียงในภาพรวมของปี 2553 มีบุคลากรที่ใช้คอมพิวเตอร์ในการปฏิบัติงานเป็นประจำอยู่ประมาณ 2.1 ล้านคน (สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2554b) และจำนวนประชากรที่มีอายุตั้งแต่ 6 ปีขึ้นไปที่มีการใช้คอมพิวเตอร์ในครัวเรือนประมาณ 19.1 ล้านคน (สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2554a)

3.2 กลุ่มตัวอย่าง

กลุ่มตัวอย่างของงานวิจัยนี้ คือผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลทั่วประเทศไทย แต่เนื่องจากจำนวนประชากรมีขนาดใหญ่ จึงได้ทำการคำนวณขนาดตัวอย่างโดยใช้สูตรการกำหนดขนาดตัวอย่างจากการประมาณค่าเฉลี่ยประชากร สำหรับกรณีที่ประชากรมีขนาดใหญ่ โดยกำหนดระดับความเชื่อมั่นที่ร้อยละ 95 และค่าความคลาดเคลื่อนที่ยอมรับได้ไม่เกินร้อยละ 5 สามารถคำนวณขนาดตัวอย่างได้ตามสูตรดังนี้ (กัลยา วินิชย์บัญชา, 2546)

สูตร $$n = \frac{Z^2\sigma^2}{e^2}$$

เมื่อ

n = ขนาดตัวอย่าง

Z = ค่าปกติมาตรฐานที่ได้จากตารางการแจกแจงแบบปกติมาตรฐานที่ระดับนัยสำคัญ 0.05 (ระดับความเชื่อมั่น 95%) มีค่าเท่ากับ 1.96

σ= ค่าเบี่ยงเบนมาตรฐานของประชากร ซึ่งในกรณีที่ไม่ทราบค่าเบี่ยงเบนมาตรฐานของประชากร สามารถใช้ค่าเบี่ยงเบนมาตรฐานของตัวอย่าง (S) แทนได้ (กัลยา วินิชย์บัญชา, 2546) ผู้วิจัยจึงใช้ค่าเบี่ยงเบนมาตรฐานของตัวอย่างที่ได้จากงานวิจัยในอดีต ซึ่งใช้วิธีการเก็บข้อมูลเป็นแบบ 5-point Likert Scale เช่นเดียวกันงานวิจัยนี้ มีค่าเท่ากับ 1.25 (Workman et al., 2008)

e = ค่าความคลาดเคลื่อนจากการสุ่มตัวอย่าง ซึ่งจะเท่ากับผลคูณของ ขอบเขตความผิดพลาดที่ยอมรับได้ (Acceptable Margin of Error) กับ ค่าเฉลี่ย (Mean) โดยผู้วิจัยกำหนดให้ขอบเขตความผิดพลาดที่ยอมรับได้เท่ากับ 5% และใช้วิธีการเก็บข้อมูลเป็นแบบ 5-point Likert Scale ค่าเฉลี่ยเท่ากับ 2.5 ดังนั้น e = 0.05 x 2.5 มีค่าเท่ากับ 0.125

แทนค่าตามสูตรได้ดังนี้

$$n = \frac{(1.96)^2(1.25)^2}{(0.125)^2}$$

n = 384.16

จากการคำนวณพบว่า กลุ่มตัวอย่างที่ได้มีขนาดเท่ากับ 384 ตัวอย่าง เพื่อลดความคลาดเคลื่อนและสร้างความเชื่อมั่นในการเก็บข้อมูลของงานวิจัยนี้ จึงใช้ขนาดตัวอย่างไม่ต่ำกว่า 500 ตัวอย่าง

3.3 การเลือกตัวอย่าง

การเลือกตัวอย่างในงานวิจัยนี้ใช้การสุ่มตัวอย่างแบบไม่ใช้ความน่าจะเป็น ซึ่งผู้วิจัยจะเก็บข้อมูลจากกลุ่มประชากรที่มีความสะดวกในการให้ข้อมูลซึ่งเป็นบุคคลที่ใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและพกพาทั้งที่ใช้งานที่บ้านและที่ทำงานในประเทศไทย โดยใช้การกระจายแบบสอบถามไปยังประชาสัมพันธ์หรือ Contact Point ขององค์กรต่างๆ และผ่านทางเครือข่ายสังคมออนไลน์

3.4 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยนี้ คือแบบสอบถาม ที่ผู้วิจัยพัฒนาขึ้นจากการทบทวนวรรณกรรมต่างๆ เพื่อให้ครอบคลุมตามวัตถุประสงค์ที่ได้ตั้งไว้ ซึ่งลักษณะโครงสร้างของแบบสอบถามเป็นคำถามปลายปิดและคำถามปลายเปิด ทั้งนี้แบบสอบถามที่ใช้ในการจัดเก็บข้อมูลสำหรับงานวิจัยได้แบ่งคำถามทั้งหมดออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 เป็นคำถามเกี่ยวกับการใช้คอมพิวเตอร์และความปลอดภัยคอมพิวเตอร์

ส่วนที่ 2 เป็นคำถามเกี่ยวกับข้อมูลภูมิหลัง และข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศอายุ ระดับการศึกษา ตำแหน่งงาน สาขาวิชาที่ศึกษา

ส่วนที่ 3 เป็นคำถามเกี่ยวกับการวัดค่าปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นข้อมูลของผู้ใช้คอมพิวเตอร์ว่ามีความคิดเห็นต่อปัจจัยต่างๆ มากน้อยเพียงใด จำนวน 39 ข้อ ข้อคำถามเป็นแบบมาตรประมาณค่า (rating scale) 5 ระดับ ซึ่งเกณฑ์การให้คะแนน แสดงดังตารางที่ 3.1

ตารางที่ 3.1

เกณฑ์การให้คะแนนข้อคำถาม

ระดับความคิดเห็น	**เกณฑ์การให้คะแนน**	
	คำถามเชิงนิมาน	**คำถามเชิงนิเสธ**
เห็นด้วยอย่างยิ่ง	5	1
เห็นด้วย	4	2
เห็นด้วยปานกลาง	3	3
ไม่เห็นด้วย	2	4
ไม่เห็นด้วยอย่างยิ่ง	1	5

3.5 การสร้างและการตรวจสอบคุณภาพเครื่องมือ

(1) ศึกษาแนวคิดทฤษฎี เอกสารและงานวิจัย เพื่อกำหนดกรอบแนวคิด โครงสร้างของตัวแปรที่ต้องการวัดและรูปแบบของการสร้างคำถาม

(2) สร้างแบบสอบถามโดยพิจารณาจากการศึกษาค้นคว้า แล้วนำให้อาจารย์ที่ปรึกษาพิจารณาตรวจสอบ จากนั้นนำมาปรับปรุงแก้ไข

(3) นำแบบสอบถามที่ได้ในเบื้องต้นไปปรึกษากับผู้เชี่ยวชาญในการทำงานวิจัยเพื่อตรวจสอบในเรื่องเนื้อหา และความชัดเจนของคำถามต่างๆ ในแบบสอบถาม

(4) ปรับปรุงแก้ไขแบบสอบถามตามข้อเสนอแนะที่ได้จากผู้เชี่ยวชาญทดสอบแบบสอบถามกับผู้ใช้คอมพิวเตอร์ส่วนบุคคลจำนวน 52 คน เพื่อหาคุณภาพของเครื่องมือ โดยทดสอบความเที่ยง (Reliability) ของแบบสอบถามด้วยวิธีสัมประสิทธิ์แอลฟาของครอนบัค (Cronbach's alpha coefficient) โดยเลือกเฉพาะข้อคำถามที่มีค่าความเที่ยงไม่ต่ำกว่า 0.70 (Reynaldo & Santos, 1999)

จากการตรวจสอบความเที่ยงของแบบสอบถาม พบว่า ข้อคำถามของปัจจัยแต่ละด้านมีค่าสัมประสิทธิ์ความเที่ยงอยู่ระหว่าง 0.792 ถึง 0.900 แสดงว่าแบบสอบถามที่ผู้วิจัยได้พัฒนาขึ้นมีคุณภาพเหมาะสมที่จะนำไปใช้ในการเก็บข้อมูล โดยรายละเอียดค่าความเที่ยงของข้อคำถามเกี่ยวกับปัจจัยแต่ละด้าน แสดงดังตารางที่ 3.2

(5) นำผลการวิเคราะห์มาเป็นข้อมูลในการปรับปรุงแก้ไขและจัดทำแบบสอบถามฉบับสมบูรณ์โดยมีโครงสร้างของเนื้อหาและจำนวนข้อของแบบสอบถาม แสดงดังตารางที่ 3.3

ตารางที่ 3.2

ค่าสัมประสิทธิ์ความเที่ยงของตัวแปร

ปัจจัย	จำนวนข้อ	ค่าความเที่ยง
บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness Personality)	4	0.792
การรับรู้คุณค่าของข้อมูล (Perceived Value of data)	4	0.805
ประสบการณ์ในอดีต (Prior experience)	4	0.900
การคล้อยตามกลุ่มอ้างอิง (Subjective norm)	4	0.874
ความรู้ด้านความปลอดภัย (Security Knowledge)	4	0.797
ค่าใช้จ่ายในการป้องกัน (Safeguard cost)	4	0.804
การรับรู้ต่อสภาวะคุกคาม (Threat appraisal)	4	0.876
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (Coping appraisal)	4	0.808
แรงจูงใจในการป้องกัน (Protection Motivation)	4	0.879
พฤติกรรมการป้องกัน (Protection Behavior)	3	0.834

ตารางที่ 3.3

ความสัมพันธ์ระหว่างปัจจัยและคำถามในแบบสอบถาม

ปัจจัย	ตัวแปร	คำถาม	อ้างอิง
บุคลิกภาพแบบมีจิตสำนึก (CP)	CP1	(1) คุณสามารถทำงานที่ได้รับมอบหมายอย่างมีประสิทธิภาพ	(R. R. McCrae & P. T. Costa, 1987)
	CP2	(2) คุณเป็นคนมีระเบียบวินัย	(R. R. McCrae & P. T. Costa, 1987)
	CP3	(3) คุณเป็นคนที่ชอบความสมบูรณ์แบบ	(R. R. McCrae & P. T. Costa, 1987)
	CP4	(4) คุณคิดอย่างรอบคอบก่อนที่จะพูดหรือลงมือทำใดๆ	(R. R. McCrae & P. T. Costa, 1987)
การรับรู้คุณค่าของข้อมูล (PV)	PV1	(5) คุณคิดว่าข้อมูลของคุณควรได้รับปกป้องจากอาชญากรรมคอมพิวเตอร์ เช่น ไวรัสคอมพิวเตอร์ หรือการขโมยข้อมูลเป็นต้น	(Chai, Sharmistha, et al., 2009)
	PV2	(6) คุณรู้สึกกังวลว่าข้อมูลในเครื่องคอมพิวเตอร์ของคุณไม่ปลอดภัย	(Chai, Sharmistha, et al., 2009)
	PV3	(7) คุณคิดว่าข้อมูลต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ของคุณมีความสำคัญ	(Chai, Sharmistha, et al., 2009)
	PV4	(8) คุณจะได้รับความเสียหาย ถ้าข้อมูลในเครื่องคอมพิวเตอร์ของคุณถูกขโมย	(Chai, Sharmistha, et al., 2009)
ประสบการณ์ในอดีต (PE)	PE1	(9) ครอบครัว เพื่อน หรือบุคคลใกล้ชิดของคุณเคยประสบปัญหาจากอาชญากรรมคอมพิวเตอร์ เช่น ถูกขโมยข้อมูล ขโมยเครื่องคอมพิวเตอร์ หรือถูกไวรัส เป็นต้น	(Chai, Sharmistha, et al., 2009)
	PE2	(10) คุณเคยประสบปัญหาจากอาชญากรรมคอมพิวเตอร์	(Chai, Sharmistha, et al., 2009)
	PE3	(11) คุณเคยได้รับความเสียหายจากอาชญากรรมคอมพิวเตอร์ เช่น เครื่องคอมพิวเตอร์ ถูกไวรัสจนข้อมูลสูญหาย หรือ ถูกขโมยข้อมูลสำคัญและนำไปเผยแพร่ เป็นต้น	(Chai, Sharmistha, et al., 2009)

ตารางที่ 3.3

ความสัมพันธ์ระหว่างปัจจัยและคำถามในแบบสอบถาม (ต่อ)

ปัจจัย	ตัวแปร	คำถาม	อ้างอิง
ประสบการณ์ในอดีต (PE)	PE4	(12) คุณสงสัยว่าเครื่องคอมพิวเตอร์ของคุณเคยถูกคุกคามจากอาชญากรรมคอมพิวเตอร์	(Chai, Sharmistha, et al., 2009)
การคล้อยตามกลุ่มอ้างอิง (SN)	SN1	(13) หน่วยงานด้านความปลอดภัยกระตุ้นให้คุณดำเนินการด้านความปลอดภัยคอมพิวเตอร์	(Anderson & Agarwal, 2010)
	SN2	(14) เพื่อนกระตุ้นหรือชักชวนให้คุณดำเนินการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์	(Ifinedo, 2011)
	SN3	(15) ครอบครัวของคุณสนับสนุนให้คุณป้องกันภัยจากอาชญากรรมคอมพิวเตอร์	(Anderson & Agarwal, 2010)
	SN4	(16) หัวหน้างานหรือบุคคลที่น่าเชื่อถือกระตุ้นให้คุณดำเนินการด้านความปลอดภัย	(Anderson & Agarwal, 2010)
ความรู้ด้านความปลอดภัย (SK)	SK1	(17) คุณได้รับการอบรมหรือได้รับความรู้เกี่ยวกับการใช้งานคอมพิวเตอร์อย่างปลอดภัย	(D'Arcy et al., 2009)
	SK2	(18) คุณอ่านข่าวสารหรือข้อมูลด้านความปลอดภัยคอมพิวเตอร์จากสื่อต่างๆ	(D'Arcy et al., 2009)
	SK3	(19) คุณให้ความสนใจและติดตามข้อมูลเกี่ยวกับการรักษาความปลอดภัยคอมพิวเตอร์	(D'Arcy et al., 2009)
	SK4	(20) คุณคิดว่าคู่มือหรือคำแนะนำด้านความปลอดภัยที่ดีจะช่วยปกป้องหรือลดโอกาสเกิดอาชญากรรมคอมพิวเตอร์ได้	(D'Arcy et al., 2009)
ค่าใช้จ่ายในการป้องกัน (SC)	SC1	(21) คุณคิดว่าการติดตั้งและการใช้ซอฟต์แวร์ด้านความปลอดภัยจะทำให้โปรแกรมอื่นๆ บนเครื่องคอมพิวเตอร์เกิดปัญหาหรือเกิดความไม่สะดวกในการใช้งาน	(H. Liang & Y. L. Xue, 2010)

ตารางที่ 3.3

ความสัมพันธ์ระหว่างปัจจัยและคำถามในแบบสอบถาม (ต่อ)

ปัจจัย	ตัวแปร	คำถาม	อ้างอิง
ค่าใช้จ่ายในการป้องกัน (SC)	SC2	(22) คุณคิดว่าการติดตั้งและใช้ซอฟต์แวร์ป้องกันภัยบนเครื่องคอมพิวเตอร์เป็นภาระ	(H. Liang & Y. L. Xue, 2010)
	SC3	(23) คุณคิดว่าการติดตั้งและใช้ซอฟต์แวร์ป้องกันภัยบนเครื่องคอมพิวเตอร์นั้นเสียเวลา	(H. Liang & Y. L. Xue, 2010)
	SC4	(24) คุณคิดว่าเครื่องมือหรือซอฟต์แวร์ที่นำมาใช้ป้องกันภัยมีราคาแพงเกินไป	-
การรับรู้ต่อสภาวะคุกคาม (TA)	TA1	(25) คุณคิดว่าทุกคนมีโอกาสถูกคุกคามจากอาชญากรรมคอมพิวเตอร์	-
	TA2	(26) คุณคิดว่าทุกคนมีความเสี่ยงที่จะถูกคุกคามจากอาชญากรรมคอมพิวเตอร์	(H. Liang & Y. L. Xue, 2010)
	TA3	(27) อาชญากรรมคอมพิวเตอร์ทำให้เกิดความเสียหายต่อคอมพิวเตอร์และข้อมูลของคุณ	(H. Liang & Y. L. Xue, 2010)
	TA4	(28) คุณคิดว่าในปัจจุบันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์มีอัตราเพิ่มขึ้น	(Johnston & Warkentin, 2010)
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	CA1	(29) คุณเชื่อมั่นว่าคุณมีทักษะเพียงพอในการดำเนินการป้องกันภัยคอมพิวเตอร์	(H. Liang & Y. L. Xue, 2010)
	CA2	(30) คุณเชื่อมั่นว่าภัยคุกคามจากอาชญากรรมคอมพิวเตอร์นั้นสามารถป้องกันได้	-
	CA3	(31) คุณสามารถดำเนินการป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ด้วยตัวเอง	-
	CA4	(32) ถ้าคอมพิวเตอร์ถูกคุกคามจากอาชญากรรมคอมพิวเตอร์คุณรู้วิธีจัดการกับปัญหานี้	(Liang & Xue, 2010)
แรงจูงใจในการป้องกัน (PM)	PM1	(33) คุณตั้งใจนำเครื่องมือต่างมาใช้เพื่อหลีกเลี่ยงภัยคุกคามจากอาชญากรรมคอมพิวเตอร์	(Liang & Xue, 2010)
	PM2	(34) เมื่อคุณได้รับข้อมูลหรือข่าวสารเกี่ยวกับอาชญากรรมคอมพิวเตอร์ คุณจะหาวิธีการป้องกันไม่ให้คอมพิวเตอร์ของคุณถูกคุกคาม	(Liang & Xue, 2010)

ตารางที่ 3.3

ความสัมพันธ์ระหว่างปัจจัยและคำถามในแบบสอบถาม (ต่อ)

ปัจจัย	ตัวแปร	คำถาม	อ้างอิง
แรงจูงใจในการป้องกัน (PM)	PM3	(35) คุณมุ่งมั่นที่จะปฏิบัติหรือดำเนินการตามคำแนะนำเพื่อป้องกันภัย	(Liang & Xue, 2010)
	PM4	(36) คุณพยายามหาวิธีการต่างๆ มาใช้เพื่อป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ถึงแม้คุณจะไม่เคยถูกคุกคามมาก่อน	-
พฤติกรรมการป้องกัน (PB)	PB1	(37) คุณทำการปกป้องคอมพิวเตอร์และข้อมูลของคุณเพื่อไม่ให้ถูกคุกคาม	(H. Liang & Y. L. Xue, 2010)
	PB2	(38) คุณปฏิบัติตามคำแนะนำต่างๆ ที่ได้รับคำแนะนำเพื่อไม่ให้ถูกคุกคาม	-
	PB3	(39) คุณใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัยเพื่อป้องกันการถูกคุกคาม	(H. Liang & Y. L. Xue, 2010)

3.6 การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลโดยมีขั้นตอน ดังนี้

(1) ส่งแบบสอบถามไปยังกลุ่มตัวอย่าง ผ่านผ่านทางเครือข่ายสังคมออนไลน์ และขอความอนุเคราะห์หน่วยงานต่างๆ ในการประชาสัมพันธ์และกระจายแบบสอบถามไปยังผู้ใช้คอมพิวเตอร์ในองค์กร

(2) เมื่อได้รับแบบสอบถามคืนแล้ว ผู้วิจัยตรวจสอบความถูกต้องสมบูรณ์ของแบบสอบถาม และคัดเลือกเฉพาะแบบสอบถามที่มีความถูกต้องสมบูรณ์มาทำการตรวจให้คะแนนตามเกณฑ์ที่กำหนดไว้

(3) นำคะแนนที่ได้ไปวิเคราะห์ข้อมูลทางสถิติ เพื่อทดสอบสมมติฐาน สรุปผล และรายงานผลการวิจัยต่อไป

3.7 การวิเคราะห์ข้อมูล

(1) วิเคราะห์ค่าสถิติพื้นฐานของกลุ่มตัวอย่าง เพื่อให้ทราบลักษณะการแจกแจงของกลุ่มตัวอย่างด้วยสถิติเชิงบรรยาย ได้แก่ ความถี่ ร้อยละ และวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่ใช้ในการพัฒนาโมเดล ประกอบด้วย ตัวแปรสังเกตได้ 39 ตัวแปร เพื่อให้ทราบลักษณะการแจกแจง และการกระจายของตัวแปรสังเกตได้ที่ใช้ในการศึกษาในโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ด้วยสถิติเชิงพรรณา ได้แก่ ค่าเฉลี่ย (mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard deviation) สัมประสิทธิ์การกระจาย (Coefficient of variation) ความเบ้ (Skewness) และความโด่ง (Kurtosis) โดยใช้โปรแกรมสำเร็จรูป SPSS for Windows

(2) วิเคราะห์ความสัมพันธ์ระหว่างตัวแปร ด้วยการวิเคราะห์หาค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson’s product-moment correlation coefficient) ระหว่างตัวแปร เพื่อให้เห็นความสัมพันธ์ระหว่างตัวแปรต่าง ๆ ว่าเป็นความสัมพันธ์เชิงเส้นตรงหรือไม่ (Linear relationship) ทิศทาง (Direction) ของความสัมพันธ์เป็นบวกและลบ ขนาด (Strength) ของความสัมพันธ์มีค่าอยู่ในระดับใด เพื่อใช้เป็นข้อมูลพื้นฐานในการวิเคราะห์โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ โดยใช้โปรแกรมสำเร็จรูป SPSS for Windows

(3) วิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory factor analysis) ของตัวแปรสาเหตุเพื่อศึกษาความตรงเชิงโครงสร้างของตัวแปร โดยใช้โปรแกรม LISREL for Windows version 8.72

(4) ตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ ที่สร้างขึ้นจากทฤษฎีและงานวิจัยที่เกี่ยวข้องกับข้อมูลเชิงประจักษ์ด้วยโปรแกรม LISREL for Windows version 8.72

(5) ทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศแตกต่างกัน ด้วยการวิเคราะห์กลุ่มพหุด้วยโปรแกรม LISREL for Windows version 8.72

โดยค่าดัชนีสำคัญที่ใช้ตรวจสอบความสอดคล้องกลมกลืนของโมเดลตามสมมติฐานกับข้อมูลเชิงประจักษ์ แสดงดังตารางที่ 3.4

ตารางที่ 3.4

ดัชนีที่ใช้ตรวจสอบความกลมกลืนของโมเดลตามสมมติฐานกับข้อมูลเชิงประจักษ์

ดัชนีที่ใช้ตรวจสอบความกลมกลืนของโมเดล	**เกณฑ์การพิจารณา**	**อ้างอิง**
Likelihood Ratio Chi-Square Statistic (χ^2)	> 0.050	(Diamantopoulos & Siguaw, 2000)
Relative χ^2 (χ^2)/df)	< 2.00	(Diamantopoulos & Siguaw, 2000)
Goodness of Fit Index (GFI)	> 0.900	(Diamantopoulos & Siguaw, 2000)
Adjusted Goodness of Fit Index (AGFI)	> 0.900	(Diamantopoulos & Siguaw, 2000)
Root Mean Squared Residuals (RMR)	< 0.050	(Diamantopoulos & Siguaw, 2000)
Root Mean Squared Error of Approximation (RMSEA)	< 0.050	(Diamantopoulos & Siguaw, 2000)
Critical N (CN)	> 200	(Diamantopoulos & Siguaw, 2000)

ในกรณีที่ผลการตรวจสอบพบว่าโมเดลไม่สอดคล้องกับข้อมูลเชิงประจักษ์ กล่าวคือ ค่าสถิติที่คำนวณได้ไม่เป็นไปตามเกณฑ์ที่กำหนด ผู้วิจัยจะทำการปรับโมเดล (Model adjustment) โดยอาศัยเหตุผลเชิงทฤษฎีและค่าดัชนีปรับแต่งโมเดล (Model modification indices) ซึ่งเป็นค่าสถิติเฉพาะของพารามิเตอร์แต่ละตัวทำการปรับโมเดลจนได้โมเดลที่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์และมีค่าสถิติตามเกณฑ์ที่กำหนด

บทที่ 4
ผลการวิจัยและอภิปรายผล

ผู้วิจัยจะนำเสนอผลการวิเคราะห์ข้อมูลแบ่งออกเป็น 4 ตอน ดังนี้

4.1 การวิเคราะห์ค่าสถิติพื้นฐานและและความสัมพันธ์ระหว่างตัวแปรสังเกตได้

4.2 การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory factor analysis)

4.3 การวิเคราะห์เพื่อตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ที่สร้างขึ้นกับข้อมูลเชิงประจักษ์

4.4 การวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน

เพื่อให้การนำเสนอผลการวิจัยเป็นไปอย่างกระชับ ในการกล่าวถึง “กลุ่มตัวอย่างทั้งหมด” จะหมายถึง กลุ่มตัวอย่างทั้งหมดที่นำมาศึกษาในครั้งนี้ แต่ถ้ากล่าวถึง “กลุ่มตัวอย่าง IT People” จะหมายถึง กลุ่มตัวอย่างเฉพาะผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ และถ้ากล่าวถึง “กลุ่มตัวอย่าง Non-IT People” จะหมายถึง กลุ่มตัวอย่างเฉพาะผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ

4.1 การวิเคราะห์ค่าสถิติพื้นฐานและความสัมพันธ์ระหว่างตัวแปรสังเกตได้

การวิเคราะห์ข้อมูลในตอนนี้ แบ่งการนำเสนอเป็น 3 ส่วน คือ

4.1.1 การวิเคราะห์ค่าสถิติพื้นฐานของผู้ตอบแบบสอบถาม เป็นการนำเสนอผลการวิเคราะห์ค่าสถิติพื้นฐานของผู้ตอบแบบสอบถาม เพื่อศึกษาลักษณะการกระจายของผู้ตอบแบบสอบถาม โดยค่าสถิติที่นำเสนอคือการแจกแจงความถี่ และร้อยละ

4.1.2 การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ เป็นการนำเสนอผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ เพื่อศึกษาลักษณะการแจกแจง การกระจายและทดสอบสมมติฐานลักษณะความเบ้และความโด่งของตัวแปรสังเกตได้ว่าแตกต่างจากศูนย์หรือไม่ ค่าสถิติที่นำเสนอคือ ค่าเฉลี่ย ($\bar{x}$) ส่วนเบี่ยงเบนมาตรฐาน (SD) สัมประสิทธิ์การกระจาย (CV) ค่าความเบ้ (SK) และความโด่ง (KU)

4.1.3 เป็นการนำเสนอผลการวิเคราะห์ความสัมพันธ์ของตัวแปรสังเกตได้ เพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรสังเกตได้ และพิจารณาตรวจสอบความเหมาะสมของเมทริกซ์สหสัมพันธ์

ระหว่างตัวแปรสังเกตได้ ค่าสถิติที่นำเสนอคือ ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน ค่าสถิติ Bartlett's test of sphericity และค่าดัชนี Kaiser- Mayer-Olkin

4.1.1 การวิเคราะห์ค่าสถิติพื้นฐานของผู้ตอบแบบสอบถาม

การวิเคราะห์ข้อมูลในส่วนนี้เป็นการวิเคราะห์ข้อมูลพื้นฐานของกลุ่มตัวอย่างที่ตอบแบบสอบถามจำนวน 600 คน นำมาจำแนกเป็นกลุ่มคนที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT people) กับคนที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT people) ได้จำนวนกลุ่มละ 300 คน โดยเกณฑ์ที่ใช้ในการจำแนกกลุ่มตัวอย่างคือ ตำแหน่งงานและสาขาวิชาที่กำลังศึกษา รายละเอียดแสดงดังภาคผนวก ค

ผลการวิคราะห์ค่าสถิติพื้นฐาน สภาพโดยทั่วไปของกลุ่มตัวอย่างที่ตอบแบบสอบถามจำแนกตามเพศ อายุ ระดับการศึกษาสูงสุด และประสบการณ์การทำงาน พบว่ากลุ่มตัวอย่างทั้งหมดเป็นเพศหญิงมากกว่าเพศชาย โดยเพศหญิงร้อยละ 53.50 และเพศชายร้อยละ 46.50 ส่วนใหญ่มีอายุระหว่าง 25 ถึง 34 ปี คิดเป็นร้อยละ 64 และระดับการศึกษาสูงสุดคือระดับปริญญาตรี คิดเป็นร้อยละ 51 โดยมีประสบการณ์ทำงาน 5 ถึง 10 ปี มากที่สุด คิดเป็นร้อยละ 53.83 นอกจากนี้ ผลการวิเคราะห์โดยแยกเป็นกลุ่มคนที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT people) กับคนที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT people) พบว่าทั้ง 2 กลุ่มตัวอย่างมีลักษณะใกล้เคียงกันทั้งเพศ อายุ ระดับการศึกษาสูงสุด และประสบการณ์การทำงาน มีรายละเอียดแสดงดังตารางที่ 4.1

สำหรับลักษณะการใช้งานคอมพิวเตอร์ของกลุ่มตัวอย่าง พบว่ากลุ่มตัวอย่างมีการใช้เครื่องคอมพิวเตอร์แบบพกพาได้แก่โน๊ตบุ๊ค หรือแล็บท็อปมากกว่าคอมพิวเตอร์พีซี คิดเป็นร้อยละ 52.67 และ 47.33 ตามลำดับ โดยมีวัตถุประสงค์เพื่อใช้ในเรื่องที่เกี่ยวข้องกับการทำงานมากกว่าการทำธุรกรรมส่วนตัวคิดเป็น 54 และ 46 ตามลำดับ เมื่อพิจารณาประสบการณ์ใช้งานคอมพิวเตอร์ส่วนใหญ่อยู่ระหว่าง 11 ถึง 20 ปี คิดเป็นร้อยละ 46.83 นอกจากนี้ยังพบว่ากลุ่มตัวอย่างส่วนใหญ่จะมีสิทธิ์ติดตั้งโปรแกรมต่างๆ ลงบนเครื่องคอมพิวเตอร์ได้ด้วยตนเอง ร้อยละ 55.33 และส่วนใหญ่เก็บข้อมูลสำคัญและข้อมูลที่เป็นความลับไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เป็นประจำ ร้อยละ 79.50 ส่วนช่องทางการรับรู้ข้อมูลข่าวสารด้านคอมพิวเตอร์จะผ่านทางอินเทอร์เน็ตเป็นส่วนใหญ่ รองลงมาคือโทรทัศน์ และวารสาร/หนังสือ คิดเป็นร้อยละ 52.14 22.45 และ 18.53 ตามลำดับ ซึ่งเมื่อพิจารณาโดยแยกกลุ่มตัวอย่างออกเป็นกลุ่มคนที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT people) กับคนที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT people) พบว่าทั้ง 2 กลุ่มตัวอย่างมีลักษณะการใช้งานคอมพิวเตอร์ใกล้เคียงกัน มีรายละเอียดแสดงดังตารางที่ 4.2

ตารางที่ 4.1

ผลการวิเคราะห์จำนวนและร้อยละของผู้ตอบแบบสอบถามจำแนกตามเพศ อายุ ระดับการศึกษาสูงสุด และประสบการณ์การทำงาน

รายการ	IT People		Non-IT People		รวม	
	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ
เพศ						
ชาย	138	46.00	141	47.00	279	46.50
หญิง	162	54.00	159	53.00	321	53.50
อายุ						
18–24 ปี	34	11.33	62	2.53	96	16.00
25–34 ปี	211	7.33	173	57.53	384	64.00
35–44 ปี	37	12.33	28	9.20	65	1.83
45–55 ปี	10	3.33	20	6.87	30	5.00
มากกว่า 55 ปี	8	2.67	17	5.87	25	4.17
ระดับการศึกษาสูงสุด						
ต่ำกว่าปริญญาตรี	18	6.00	30	1.00	48	8.00
ปริญญาตรี	152	5.67	154	51.33	306	51.00
สูงกว่าปริญญาตรี	130	43.33	116	38.67	246	41.00
ประสบการณ์การทำงาน						
ยังไม่ได้ทำงาน	39	13.00	48	16.00	87	14.50
ต่ำกว่า 1 ปี	19	6.33	17	5.67	36	6.00
1-5 ปี	63	21.00	66	22.00	129	21.50
5-10 ปี	168	56.00	155	51.67	323	53.83
มากกว่า 10 ปี	11	3.67	14	4.67	25	4.17

ตารางที่ 4.2

ข้อมูลลักษณะการใช้งานคอมพิวเตอร์ของกลุ่มตัวอย่าง

รายการ	IT People		Non-IT People		รวม	
	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ
วัตถุประสงค์ในการใช้คอมพิวเตอร์						
เกี่ยวกับการทำงาน	162	54.00	162	54.00	324	54.00
ธุรกรรมส่วนตัว	138	46.00	138	46.00	276	46.00
ประสบการณ์ใช้งานคอมพิวเตร์						
1-5 ปี	11	3.67	20	6.67	31	5.17
6-10 ปี	116	38.67	122	4.67	238	39.67
11-20 ปี	153	51.00	128	42.67	281	46.83
มากกว่า 20 ปี	20	6.67	30	1.00	50	8.33
ประเภทคอมพิวเตอร์						
พีซี	140	46.67	144	48.00	284	47.33
โน๊ตบุ๊ค/ แล็บท็อป	160	53.33	156	52.00	316	52.67
สิทธิ์การติดตั้งซอฟท์แวร์ลงบนเครื่องคอมพิวเตอร์						
ได้	182	6.67	150	5.00	332	55.33
ไม่ได้	106	35.33	120	4.00	226	37.67
ไม่แน่ใจ	12	4.00	30	1.00	42	7.00
เก็บข้อมูลสำคัญและเป็นความลับบนเครื่องคอมพิวเตอร์						
ใช่	249	83.00	228	76.00	477	79.50
ไม่ใช่	37	12.33	40	13.33	77	12.83
ไม่แน่ใจ	14	4.67	32	1.67	46	7.67
ช่องทางการรับรู้ข้อมูลข่าวสารด้านคอมพิวเตอร์						
อินเทอร์เน็ต	245	52.69	194	51.46	439	52.14
วารสารหรือหนังสือ	92	19.78	64	16.98	156	18.53
โทรทัศน์	108	23.23	81	21.49	189	22.45
อื่นๆ	20	4.30	38	1.08	58	6.89

4.1.2 การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้

ในส่วนนี้เป็นการนำเสนอค่าสถิติพื้นฐานของตัวแปรสังเกตได้จำนวน 39 ตัวแปร ได้แก่ ปัจจัยบุคลิกภาพแบบมีจิตสำนึก (CP1-CP4) การรับรู้คุณค่าของข้อมูล (PV1-PV4) ประสบการณ์ในอดีต (PE1-PE4) การคล้อยตามกลุ่มอ้างอิง (SN1-SN4) ความรู้ด้านความปลอดภัย (SK1-SK4) ค่าใช้จ่ายในการป้องกัน (SC1-SC4) การรับรู้ต่อสภาวะคุกคาม (TA1-TA4) การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA1-CA4) และแรงจูงใจในการป้องกัน (PM1-PM4) ซึ่งมีตัววัดปัจจัยละ 4 ข้อ และพฤติกรรมการป้องกันมีตัววัด 3 ข้อ (PB1-PB3) โดยผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้แยกพิจารณาตามกลุ่มตัวอย่าง ได้แก่ กลุ่มตัวอย่างทั้งหมด กลุ่มตัวอย่าง IT People และ กลุ่มตัวอย่าง Non-IT People โดยมีรายละเอียดดังนี้

4.1.2.1 การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด

การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง จำนวน 600 คน และตัวแปรสังเกตได้จำนวน 39 ตัวแปร รายละเอียดแสดงดังตารางที่ 4.3

ตารางที่ 4.3

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด

ตัวแปรสังเกตได้	$\bar{X}$	**SD**	**CV(%)**	**SK**	**KU**	**MIN**	**MAX**
CP1	3.962	0.754	19.031	-0.242	-0.481	2.00	5.00
CP2	3.898	0.720	18.471	-0.195	-0.285	2.00	5.00
CP3	3.927	0.723	18.411	-0.262	-0.191	2.00	5.00
CP4	3.945	0.761	19.290	-0.545	0.474	1.00	5.00
PV1	4.160	0.639	15.361	-0.346	0.185	2.00	5.00
PV2	4.157	0.627	15.083	-0.333	0.325	2.00	5.00
PV3	4.100	0.679	16.561	-0.447	0.311	2.00	5.00
PV4	4.160	0.713	17.139	-0.493	-0.087	2.00	5.00
PE1	3.692	0.969	26.246	-0.479	-0.308	1.00	5.00
PE2	3.702	0.961	25.959	-0.504	-0.245	1.00	5.00
PE3	3.695	0.922	24.953	-0.526	0.204	1.00	5.00
PE4	3.707	0.945	25.492	-0.494	-0.214	1.00	5.00
SN1	4.155	0.745	17.930	-0.744	0.818	1.00	5.00
SN2	4.202	0.752	17.896	-0.823	0.868	1.00	5.00
SN3	4.215	0.759	18.007	-0.795	0.632	1.00	5.00
SN4	4.210	0.777	18.456	-0.769	0.392	1.00	5.00

ตารางที่ 4.3

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด (ต่อ)

ตัวแปรสังเกตได้	$\bar{X}$	SD	CV(%)	SK	KU	MIN	MAX
SK1	3.988	0.810	2.311	-0.698	0.647	1.00	5.00
SK2	3.940	0.915	23.223	-0.523	-0.210	1.00	5.00
SK3	3.952	0.889	22.495	-0.749	0.253	1.00	5.00
SK4	3.995	0.915	22.904	-0.713	0.115	1.00	5.00
SC1	1.982	0.887	44.753	0.569	-0.080	1.00	5.00
SC2	2.200	0.871	39.591	0.484	0.083	1.00	5.00
SC3	2.095	0.878	41.909	0.453	-0.151	1.00	5.00
SC4	2.132	0.914	42.871	0.500	-0.053	1.00	5.00
TA1	4.447	0.763	17.158	-1.315	1.300	1.00	5.00
TA2	4.482	0.786	17.537	-1.638	2.931	1.00	5.00
TA3	4.540	0.725	15.969	-1.602	2.129	2.00	5.00
TA4	4.295	0.858	19.977	-1.227	1.469	1.00	5.00
CA1	3.893	0.774	19.882	-0.355	-0.204	2.00	5.00
CA2	3.973	0.835	21.017	-0.692	0.880	1.00	5.00
CA3	3.972	0.828	2.846	-0.514	0.020	1.00	5.00
CA4	3.945	0.951	24.106	-0.733	0.147	1.00	5.00
PM1	3.745	0.809	21.602	-0.130	-0.536	2.00	5.00
PM2	3.755	0.721	19.201	0.082	-0.545	2.00	5.00
PM3	3.792	0.765	2.174	0.171	-0.900	2.00	5.00
PM4	3.627	0.869	23.959	0.051	-0.686	1.00	5.00
PB1	3.950	0.938	23.747	-0.730	0.111	1.00	5.00
PB2	3.962	0.937	23.650	-0.742	0.234	1.00	5.00
PB3	3.975	0.918	23.094	-0.847	0.682	1.00	5.00

เมื่อพิจารณาสัมประสิทธิ์การกระจาย (CV) พบว่า ตัวแปรสังเกตได้ SC1 มีการกระจายของข้อมูลมากที่สุดคือ ร้อยละ 44.753 รองลงมาคือ SC4 และ SC3 ร้อยละ 42.871 และ 41.909 ตามลำดับ ส่วนตัวแปรสังเกตได้ PV2 มีการกระจายตัวน้อยที่สุดคือร้อยละ 15.083 ส่วนตัวแปรอื่น ๆ มีการกระจายอยู่ระหว่าง 15.361 – 39.591

นอกจากนี้เมื่อพิจารณาความเบ้พบว่าตัวแปรสังเกตได้ส่วนใหญ่มีการแจกแจงในลักษณะเบ้ซ้าย (ค่าความเบ้เป็นลบ) แสดงว่าข้อมูลของตัวแปรสังเกตได้เหล่านี้มีคะแนนส่วนใหญ่สูงกว่าค่าเฉลี่ย ยกเว้นตัวแปร (PM2-PM4) และ (SC1-SC4) ที่มีการแจกแจงในลักษณะเบ้ขวา (ค่าความเบ้เป็นบวก) แสดงว่าข้อมูลเหล่านี้มีคะแนนส่วนใหญ่ต่ำกว่าค่าเฉลี่ย สำหรับการพิจารณาค่าความโด่ง ตัวแปรที่มีลักษณะเตี้ยแบนกว่าโค้งปกติ (ค่าความโด่งเป็นลบ) แสดงว่ามีความการจายของ

ข้อมูลสูง ส่วนตัวแปรที่มีลักษณะการแจกแจงสูงกว่าโค้งปกติ (ค่าความโด่งเป็นบวก) แสดงว่ามีความการจายของข้อมูลต่ำ ผลการวิเคราะห์แสดงว่าทุกตัวแปรสังเกตได้มีความเบ้และความโด่งอยู่ในเกณฑ์ที่ยอมรับได้ เนื่องจากค่าความเบ้ (Skewness) อยู่ในช่วง –2.0 ถึง 2.0 และความโด่ง (Kurtosis) อยู่ในช่วง -3.0 ถึง +3.0 แสดงว่าลักษณะการแจกแจงข้อมูลแบบปกติ

4.1.2.1 การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง IT People

การนำเสนอจะเสนอในภาพรวมของกลุ่มตัวอย่าง IT People จำนวน 300 คน และตัวแปรสังเกตได้จำนวน 39 ตัวแปร รายละเอียดแสดงดังตารางที่ 4.4

ตารางที่ 4.4

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง IT People

ตัวแปรสังเกตได้	$\bar{X}$	SD	CV (%)	SK	SU	MIN	MAX
CP1	4.023	0.751	18.677	-0.324	-0.416	2.00	5.00
CP2	3.973	0.717	18.050	-0.235	-0.314	2.00	5.00
CP3	3.970	0.715	18.003	-0.288	-0.148	2.00	5.00
CP4	4.013	0.731	18.224	-0.382	-0.095	2.00	5.00
PV1	4.170	0.650	15.588	-0.330	-0.065	2.00	5.00
PV2	4.167	0.643	15.435	-0.319	0.001	2.00	5.00
PV3	4.093	0.702	17.152	-0.482	0.238	2.00	5.00
PV4	4.163	0.696	16.726	-0.412	-0.236	2.00	5.00
PE1	3.690	0.968	26.233	-0.414	-0.487	1.00	5.00
PE2	3.707	0.958	25.835	-0.510	-0.157	1.00	5.00
PE3	3.723	0.911	24.462	-0.574	0.425	1.00	5.00
PE4	3.693	0.946	25.624	-0.473	-0.238	1.00	5.00
SN1	4.223	0.736	17.431	-0.632	-0.071	2.00	5.00
SN2	4.290	0.745	17.356	-0.771	0.021	2.00	5.00
SN3	4.343	0.717	16.504	-0.835	0.196	2.00	5.00
SN4	4.367	0.722	16.524	-0.896	0.239	2.00	5.00
SK1	3.987	0.771	19.351	-0.373	-0.303	2.00	5.00
SK2	3.927	0.911	23.212	-0.441	-0.435	1.00	5.00
SK3	3.957	0.851	21.503	-0.573	-0.189	2.00	5.00
SK4	3.973	0.903	22.726	-0.606	-0.131	1.00	5.00
SC1	2.017	0.905	44.879	0.485	-0.297	1.00	5.00
SC2	2.273	0.895	39.376	0.392	-0.151	1.00	5.00
SC3	2.127	0.898	42.232	0.445	-0.166	1.00	5.00
SC4	2.213	0.954	43.120	0.491	-0.041	1.00	5.00

ตารางที่ 4.4

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง IT People (ต่อ)

ตัวแปรสังเกตได้	$\bar{x}$	SD	CV (%)	SK	SU	MIN	MAX
TA1	4.523	0.733	16.214	-1.592	2.473	1.00	5.00
TA2	4.533	0.760	16.763	-1.702	2.906	1.00	5.00
TA3	4.593	0.695	15.129	-1.783	2.845	2.00	5.00
TA4	4.293	0.862	2.078	-1.078	0.824	1.00	5.00
CA1	3.860	.0797	2.658	-0.301	-0.362	2.00	5.00
CA2	3.950	0.831	21.026	-0.647	0.770	1.00	5.00
CA3	3.997	0.824	2.616	-0.463	-0.203	1.00	5.00
CA4	3.933	0.937	23.829	-0.676	0.086	1.00	5.00
PM1	3.767	0.801	21.256	-0.223	-0.400	2.00	5.00
PM2	3.730	0.716	19.186	0.174	-0.599	2.00	5.00
PM3	3.813	0.757	19.863	0.140	-0.882	2.00	5.00
PM4	3.637	0.884	24.295	-0.011	-0.635	1.00	5.00
PB1	3.970	0.905	22.789	-0.623	-0.223	1.00	5.00
PB2	3.940	0.931	23.618	-0.682	0.133	1.00	5.00
PB3	3.987	0.911	22.842	-0.910	0.944	1.00	5.00

จากตารางที่ 4.4 ในการนำเสนอค่าเฉลี่ยของตัวแปรสังเกตได้ พบว่าค่าเฉลี่ยของตัวแปรมีค่าอยู่ระหว่าง 2.017 – 4.593 ซึ่งอยู่ในระดับปานกลางถึงสูง โดยตัวแปร TA3 มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$= 4.593 และ SD = 0.695) และ SC1 มีค่าเฉลี่ยต่ำที่สุด ($\bar{x}$ = 2.017 และ SD = 0.905) สำหรับค่าส่วนเบี่ยงเบนมาตรฐานของตัวแปรสังเกตได้มีค่าใกล้เคียงกัน ส่วนมากอยู่ในเกณฑ์ที่เหมาะสม โดยมีค่าน้อยกว่า 1 แสดงว่าความแตกต่างของคะแนนที่ประเมินมานั้นมีความแตกต่างกันไม่มาก ตัวแปรสังเกตได้ที่มีค่าส่วนเบี่ยงเบนมาตรฐานสูงสุดคือ PE1 มีส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.968 ส่วนตัวแปรสังเกตได้ PV2 มีค่าส่วนเบี่ยงเบนมาตรฐานน้อยที่สุดเท่ากับ 0.643

เมื่อพิจารณาสัมประสิทธิ์การกระจาย (CV) พบว่า ตัวแปรสังเกตได้ SC1 มีการกระจายของข้อมูลมากที่สุดคือ ร้อยละ 44.879 รองลงมาคือ SC4 และ SC3 ร้อยละ 43.12 และ 42.232 ตามลำดับ ส่วนตัวแปรสังเกตได้ TA3 มีการกระจายตัวน้อยที่สุดคือร้อยละ 15.129 ส่วนตัวแปรอื่น ๆ มีการกระจายอยู่ระหว่าง 15.435 – 39.376

นอกจากนี้เมื่อพิจารณาความเบ้พบว่าตัวแปรสังเกตได้ส่วนใหญ่มีการแจกแจงในลักษณะเบ้ซ้าย (ค่าความเบ้เป็นลบ) แสดงว่าข้อมูลของตัวแปรสังเกตได้เหล่านี้มีคะแนนส่วนใหญ่สูงกว่าค่าเฉลี่ย ยกเว้นตัวแปร (PM3-PM4) และ (SC1-SC4) ที่มีการแจกแจงในลักษณะเบ้ขวา (ค่าความเบ้เป็นบวก) แสดงว่าข้อมูลเหล่านี้มีคะแนนส่วนใหญ่ต่ำกว่าค่าเฉลี่ย สำหรับการพิจารณาค่า

ความโด่ง ตัวแปรที่มีลักษณะเตี้ยแบนกว่าโค้งปกติ (ค่าความโด่งเป็นลบ) แสดงว่ามีความการจายของข้อมูลสูง ส่วนตัวแปรที่มีลักษณะการแจกแจงสูงกว่าโค้งปกติ (ค่าความโด่งเป็นบวก) แสดงว่ามีความการจายของข้อมูลต่ำ ผลการวิเคราะห์แสดงว่าทุกตัวแปรสังเกตได้มีความเบ้และความโด่งอยู่ในเกณฑ์ที่ยอมรับได้ เนื่องจากค่าความเบ้ (Skewness) อยู่ในช่วง –2.0 ถึง 2.0 และความโด่ง (Kurtosis) อยู่ในช่วง -3.0 ถึง +3.0 แสดงว่าลักษณะการแจกแจงข้อมูลแบบปกติ

4.1.2.2 การวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง Non-IT People

การนำเสนอจะเสนอในภาพรวมของกลุ่มตัวอย่าง Non-IT People จำนวน 300 คน และตัวแปรสังเกตได้จำนวน 39 ตัวแปร รายละเอียดแสดงดังตารางที่ 4.5

ตารางที่ 4.5

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง Non-IT People

ตัวแปรสังเกตได้	$\bar{x}$	SD	CV (%)	SK	KU	MIN	MAX
CP1	3.900	0.752	19.277	-0.166	-0.494	2.00	5.00
CP2	3.823	0.717	18.749	-0.164	-0.222	2.00	5.00
CP3	3.883	0.729	18.774	-0.234	-0.211	2.00	5.00
CP4	3.877	0.785	2.259	-0.655	0.787	1.00	5.00
PV1	4.150	0.629	15.154	-0.369	0.487	2.00	5.00
PV2	4.147	0.611	14.730	-0.355	0.735	2.00	5.00
PV3	4.107	0.656	15.969	-0.400	0.392	2.00	5.00
PV4	4.157	0.731	17.579	-0.563	0.036	2.00	5.00
PE1	3.693	0.971	26.285	-0.545	-0.116	1.00	5.00
PE2	3.697	0.967	26.149	-0.501	-0.314	1.00	5.00
PE3	3.667	0.934	25.464	-0.481	0.030	1.00	5.00
PE4	3.720	0.944	25.378	-0.519	-0.171	1.00	5.00
SN1	4.087	0.749	18.328	-0.864	1.608	1.00	5.00
SN2	4.113	0.750	18.231	-0.907	1.701	1.00	5.00
SN3	4.087	0.780	19.078	-0.749	0.926	1.00	5.00
SN4	4.053	0.800	19.726	-0.650	0.525	1.00	5.00
SK1	3.990	0.848	21.251	-0.942	1.274	1.00	5.00
SK2	3.953	0.921	23.284	-0.607	0.033	1.00	5.00
SK3	3.947	0.927	23.497	-0.882	0.536	1.00	5.00
SK4	4.017	0.927	23.078	-0.819	0.378	1.00	5.00
SC1	1.947	0.868	44.576	0.660	0.204	1.00	5.00
SC2	2.127	0.840	39.518	0.574	0.419	1.00	5.00
SC3	2.063	0.857	41.554	0.455	-0.137	1.00	5.00
SC4	2.050	0.866	42.245	0.463	-0.193	1.00	5.00

ตารางที่ 4.5

ค่าสถิติพื้นฐานของตัวแปรสังเกตได้ของกลุ่มตัวอย่าง Non-IT People

ตัวแปรสังเกตได้	$\bar{x}$	SD	CV (%)	SK	KU	MIN	MAX
TA1	4.423	0.766	17.307	-1.248	1.028	2.00	5.00
TA2	4.430	0.809	18.254	-1.586	2.972	1.00	5.00
TA3	4.487	0.752	16.754	-1.453	1.627	2.00	5.00
TA4	4.127	1.049	25.426	-1.252	1.170	1.00	5.00
CA1	3.927	0.750	19.111	-0.405	0.000	2.00	5.00
CA2	3.997	0.840	21.018	-0.743	1.035	1.00	5.00
CA3	3.947	0.832	21.090	-0.565	0.239	1.00	5.00
CA4	3.957	0.965	24.389	-0.790	0.225	1.00	5.00
PM1	3.723	0.818	21.968	-0.041	-0.636	2.00	5.00
PM2	3.780	0.726	19.199	-0.008	-0.462	2.00	5.00
PM3	3.770	0.774	2.531	0.205	-0.907	2.00	5.00
PM4	3.617	0.856	23.659	0.116	-0.734	2.00	5.00
PB1	3.930	0.970	24.691	-0.810	0.330	1.00	5.00
PB2	3.983	0.945	23.720	-0.805	0.366	1.00	5.00
PB3	3.963	0.926	23.374	-0.791	0.470	1.00	5.00

จากตารางที่ 4.5 ในการนำเสนอค่าเฉลี่ยของตัวแปรสังเกตได้ พบว่าค่าเฉลี่ยของตัวแปรมีค่าอยู่ระหว่าง 1.947 – 4.487 ซึ่งอยู่ในระดับปานกลางถึงสูง โดยตัวแปร TA3 มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$= 4.487 และ SD = 0.752) และ SC1 มีค่าเฉลี่ยต่ำที่สุด ($\bar{x}$ = 1.947 และ SD = 0.868) สำหรับค่าส่วนเบี่ยงเบนมาตรฐานของตัวแปรสังเกตได้มีค่าใกล้เคียงกัน ส่วนมากอยู่ในเกณฑ์ที่เหมาะสม โดยมีค่าน้อยกว่า 1 แสดงว่าความแตกต่างของคะแนนที่ประเมินมานั้นมีความแตกต่างกันไม่มาก ยกเว้น TA4 ที่มีค่าส่วนเบี่ยงเบนมาตรฐานมากกว่า 1 คือมีค่า 1.049

เมื่อพิจารณาสัมประสิทธิ์การกระจาย (CV) พบว่า ตัวแปรสังเกตได้ SC1 มีการกระจายของข้อมูลมากที่สุดคือ ร้อยละ 44.576 รองลงมาคือ SC4 และ SC3 ร้อยละ 42.245 และ 41.554 ตามลำดับ ส่วนตัวแปรสังเกตได้ TA3 มีการกระจายตัวน้อยที่สุดคือร้อยละ 14.73 ส่วนตัวแปรอื่น ๆ มีการกระจายอยู่ระหว่าง 15.154 – 39.518

นอกจากนี้เมื่อพิจารณาความเบ้พบว่าตัวแปรสังเกตได้ส่วนใหญ่มีการแจกแจงในลักษณะเบ้ซ้าย (ค่าความเบ้เป็นลบ) แสดงว่าข้อมูลของตัวแปรสังเกตได้เหล่านี้มีคะแนนส่วนใหญ่สูงกว่าค่าเฉลี่ย ยกเว้นตัวแปร (PM2-PM4) และ (SC1-SC4) ที่มีการแจกแจงในลักษณะเบ้ขวา (ค่าความเบ้เป็นบวก) แสดงว่าข้อมูลเหล่านี้มีคะแนนส่วนใหญ่ต่ำกว่าค่าเฉลี่ย สำหรับการพิจารณาค่าความโด่ง ตัวแปรที่มีลักษณะเตี้ยแบนกว่าโค้งปกติ (ค่าความโด่งเป็นลบ) แสดงว่ามีความการจายของ

ข้อมูลสูง ส่วนตัวแปรที่มีลักษณะการแจกแจงสูงกว่าโค้งปกติ (ค่าความโด่งเป็นบวก) แสดงว่ามีความการจายของข้อมูลต่ำ ผลการวิเคราะห์แสดงว่าทุกตัวแปรสังเกตได้มีความเบ้และความโด่งอยู่ในเกณฑ์ที่ยอมรับได้ เนื่องจากค่าความเบ้ (Skewness) อยู่ในช่วง –2.0 ถึง 2.0 และความโด่ง (Kurtosis) อยู่ในช่วง -3.0 ถึง +3.0 แสดงว่าลักษณะการแจกแจงข้อมูลแบบปกติ

4.1.3 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกตได้

การวิเคราะห์ในตอนนี้มีวัตถุประสงค์เพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรสังเกตได้ทุกตัวว่ามีความสัมพันธ์หรือไม่ มีทิศทางและขนาดของความสัมพันธ์เป็นอย่างไร โดยใช้สถิติความสัมพันธ์แบบเพียร์สัน (Pearson’s product moment correlation) ซึ่งแบ่งการวิเคราะห์ออกเป็นการวิเคราะห์ความสัมพันธ์ของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด และจำแนกตามกลุ่มตัวอย่าง ได้แก่ กลุ่มตัวอย่างทั้งหมด กลุ่มตัวอย่าง IT People และ กลุ่มตัวอย่าง Non-IT People รวมทั้งการทดสอบว่าเมทริกซ์สหสัมพันธ์นั้นเป็นเมทริกซ์เอกลักษณ์หรือไม่ โดยมีรายละเอียดดังต่อไปนี้

4.1.3.1 การวิเคราะห์ความสัมพันธ์ของกลุ่มตัวอย่างทั้งหมด

ผลการวิเคราะห์ความสัมพันธ์ของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด มีรายละเอียดดังตารางที่ 4.6 พบว่า ค่าสถิติ Bartlett’s Test of Sphericity ซึ่งเป็นค่าสถิติทดสอบสมมติฐานว่าเมทริกซ์สหสัมพันธ์นั้นเป็นเมทริกซ์เอกลักษณ์ (identity metrix) หรือไม่ มีค่าสถิติเท่ากับ 19984.24 ($p < 0.01$) แสดงว่าเมทริกซ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ทั้งหมดของกลุ่มตัวอย่างแตกต่างกันจากเมทริกซ์เอกลักษณ์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 สอดคล้องกับผลการวิเคราะห์ค่าดัชนีไกเซอร์-ไมเยอร์-ออลคิน (Kaiser-Meyer-Olkin หรือ KMO) มีค่าเท่ากับ 0.901 ซึ่งเป็นค่าที่เข้าใกล้ 1 แสดงว่าตัวแปรสังเกตได้ของข้อมูลชุดนี้มีความสัมพันธ์ภายในต่อกันเหมาะสมที่จะนำไปใช้ในการวิเคราะห์โมเดลลิสเรลต่อไป

ผลการวิเคาะห์ค่าความสัมพันธ์ระหว่างตัวแปรสังเกตได้ จำนวน 39 ตัวแปร พบว่า ส่วนใหญ่มีความสัมพันธ์กันในทิศทางบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และ 0.01 โดยมีค่าสัมประสิทธิ์สหสัมพันธ์อยู่ระหว่าง 0.096 ถึง 0.919 ยกเว้นตัวแปรสังเกตได้ที่เป็นองค์ประกอบของตัวแปรแฝงค่าใช้จ่ายในการป้องกัน (SC1-SC4) ที่มีความความสัมพันธ์กับตัวแปรสังเกตได้ที่เป็นองค์ประกอบของตัวแปรอื่นๆ ในทิศทางลบ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์อยู่ระหว่าง -0.097 ถึง -0.355

เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ที่เป็นองค์ประกอบของตัวแปรแฝงเดียวกัน พบว่ามีความสัมพันธ์กันในทิศทางบวกอย่างมีนัยสำคัญที่ระดับ 0.01 โดยค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงบุคลิกภาพแบบมีจิตสำนึก (CP1-CP4) มีค่าอยู่

ระหว่าง 0.507 ถึง 0.700 ซึ่งถือว่ามีความสัมพันธ์กันในระดับปานกลาง (0.300<r<0.700) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงการรับรู้คุณค่าของข้อมูล (PV1-PV4) มีค่าอยู่ระหว่าง 0.170 ถึง 0.881 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงปานกลาง (0.300<r<0.700) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงประสบการณ์ในอดีต (PE1-PE4) มีค่าอยู่ระหว่าง 0.153 ถึง 0.801 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงการคล้อยตามกลุ่มอ้างอิง (SN1-SN4) มีค่าอยู่ระหว่าง 0.238 ถึง 0.919 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงความรู้ด้านความปลอดภัย (SK1-SK4) มีค่าอยู่ระหว่าง 0.157 ถึง 0.779 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงค่าใช้จ่ายในการป้องกัน (SC1-SC4) มีค่าอยู่ระหว่าง 0.272 ถึง 0.858 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงการรับรู้ต่อสภาวะคุกคาม (TA1-TA4) มีค่าอยู่ระหว่าง 0.149 ถึง 0.870 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA1-CA4) มีค่าอยู่ระหว่าง 0.266 ถึง 0.777 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงสูง (0.700<r<0.900) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงแรงจูงใจในการป้องกัน (PM1-PM4) มีค่าอยู่ระหว่าง 0.276 ถึง 0.650 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงปานกลาง (0.300<r<0.700) ค่าสัมประสิทธิ์สหสัมพันธ์ภายในตัวแปรแฝงพฤติกรรมการป้องกัน (PB1-PB3) มีค่าอยู่ระหว่าง 0.333 ถึง 0.680 ซึ่งถือว่ามีความสัมพันธ์กันในระดับปานกลาง (0.300<r<0.700)

4.1.3.2 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกตได้ของกลุ่ม IT People

จากตารางที่ 4.7 พบว่าค่าสถิติ Bartlett's Test of Sphericity ซึ่งเป็นค่าสถิติทดสอบสมมติฐานว่าเมทริกซ์สหสัมพันธ์นั้นเป็นเมทริกซ์เอกลักษณ์ (identity metrix) หรือไม่ มีค่าสถิติเท่ากับ 9954.42 ($p < 0.01$) แสดงว่าเมทริกซ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ทั้งหมดของกลุ่มตัวอย่างแตกต่างกันจากเมทริกซ์เอกลักษณ์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 สอดคล้องกับผลการวิเคราะห์ค่าดัชนีไกเซอร์-ไมเยอร์-ออลคิน (Kaiser-Meyer-Olkin หรือ KMO) มีค่าเท่ากับ 0.884 ซึ่งเป็นค่าที่เข้าใกล้ 1 แสดงว่าตัวแปรสังเกตได้ของข้อมูลชุดนี้มีความสัมพันธ์ภายในต่อกันเหมาะสมที่จะนำไปใช้ในการวิเคราะห์โมเดลลิสเรลต่อไป

ผลการวิเคาะห์ค่าความสัมพันธ์ระหว่างตัวแปรสังเกตได้ จำนวน 39 ตัวแปร พบว่า ส่วนใหญ่มีความสัมพันธ์กันในทิศทางบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และ

0.01 ยกเว้นตัวแปรสังเกตได้ที่เป็นองค์ประกอบของตัวแปรแฝงค่าใช้จ่ายในการป้องกัน (SC1-SC4) โดยมีค่าสัมประสิทธิ์สหสัมพันธ์อยู่ระหว่าง 0.116 ถึง 0.900 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงถึงสูง (0.700<r<0.900)

4.1.3.3 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกตได้ของกลุ่ม Non-IT People

จากตารางที่ 4.8 พบว่าค่าสถิติ Bartlett's Test of Sphericity ซึ่งเป็นค่าสถิติทดสอบสมมติฐานว่าเมทริกซ์สหสัมพันธ์นั้นเป็นเมทริกซ์เอกลักษณ์ (identity metrix) หรือไม่ มีค่าสถิติเท่ากับ 10477.91 ($p < 0.01$) แสดงว่าเมทริกซ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ทั้งหมดของกลุ่มตัวอย่างแตกต่างกันจากเมทริกซ์เอกลักษณ์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 สอดคล้องกับผลการวิเคราะห์ค่าดัชนีไกเซอร์-ไมเยอร์-ออลคิน (Kaiser-Meyer-Olkin หรือ KMO) มีค่าเท่ากับ 0.896 ซึ่งเป็นค่าที่เข้าใกล้ 1 แสดงว่าตัวแปรสังเกตได้ของข้อมูลชุดนี้มีความสัมพันธ์ภายในต่อกันเหมาะสมที่จะนำไปใช้ในการวิเคราะห์โมเดลลิสเรลต่อไป

ผลการวิเคาะห์ค่าความสัมพันธ์ระหว่างตัวแปรสังเกตได้ จำนวน 39 ตัวแปร พบว่า ส่วนใหญ่มีความสัมพันธ์กันในทิศทางบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และ 0.01 ยกเว้นตัวแปรสังเกตได้ที่เป็นองค์ประกอบของตัวแปรแฝงค่าใช้จ่ายในการป้องกัน (SC1-SC4) โดยมีค่าสัมประสิทธิ์สหสัมพันธ์อยู่ระหว่าง 0.113 ถึง 0.935 ซึ่งถือว่ามีความสัมพันธ์กันในระดับค่อนข้างต่ำ (r<0.300) ถึงถึงสูง (0.700<r<0.900)

ตารางที่ 4.6

ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด

ตัวแปร	CP1	CP2	CP3	CP4	PV1	PV2	PV3	PV4	PE1	PE2	PE3	PE4	SN1	SN2	SN3	SN4	SK1	SK2	SK3	SK4	SC1	SC2	SC3	SC4	TA1	TA2	TA3	TA4	CA1	CA2	CA3	CA4	PM1	PM2	PM3	PM4	PB1	PB2	PB3
CP1	1.000																																						
CP2	0.660**	1.000																																					
CP3	0.672**	0.685**	1.000																																				
CP4	0.538**	0.507**	0.700**	1.000																																			
PV1	0.183**	0.141**	0.188**	0.245**	1.000																																		
PV2	0.133**	0.124**	0.132**	0.183**	0.792**	1.000																																	
PV3	0.125**	0.116**	0.155**	0.192**	0.737**	0.881**	1.000																																
PV4	0.136**	0.188**	0.188**	0.170**	0.581**	0.721**	0.653**	1.000																															
PE1	0.354**	0.242**	0.330**	0.353**	0.193**	0.195**	0.184**	0.212**	1.000																														
PE2	0.339**	0.279**	0.336**	0.331**	0.162**	0.186**	0.115**	0.179**	0.735**	1.000																													
PE3	0.370**	0.247**	0.345**	0.349**	0.188**	0.175**	0.137**	0.153**	0.713**	0.801**	1.000																												
PE4	0.352**	0.255**	0.316**	0.349**	0.186**	0.188**	0.176**	0.211**	0.786**	0.679**	0.741**	1.000																											
SN1	0.308**	0.247**	0.300**	0.309**	0.400**	0.405**	0.392**	0.346**	0.235**	0.218**	0.210**	0.238**	1.000																										
SN2	0.314**	0.223**	0.288**	0.299**	0.391**	0.411**	0.395**	0.351**	0.260**	0.213**	0.214**	0.264**	0.919**	1.000																									
SN3	0.289**	0.205**	0.297**	0.289**	0.369**	0.399**	0.386**	0.377**	0.247**	0.228**	0.225**	0.270**	0.744**	0.804**	1.000																								
SN4	0.262**	0.164**	0.274**	0.274**	0.356**	0.399**	0.384**	0.367**	0.281**	0.238**	0.248**	0.273**	0.616**	0.688**	0.721**	1.000																							
SK1	0.377**	0.313**	0.355**	0.299**	0.187**	0.227**	0.215**	0.232**	0.336**	0.371**	0.398**	0.388**	0.269**	0.281**	0.257**	0.227**	1.000																						
SK2	0.372**	0.274**	0.359**	0.355**	0.233**	0.226**	0.233**	0.232**	0.326**	0.355**	0.439**	0.348**	0.202**	0.209**	0.220**	0.156**	0.618**	1.000																					
SK3	0.416**	0.370**	0.384**	0.349**	0.187**	0.193**	0.182**	0.202**	0.310**	0.331**	0.365**	0.345**	0.276**	0.284**	0.307**	0.220**	0.634**	0.710**	1.000																				
SK4	0.375**	0.291**	0.366**	0.342**	0.173**	0.202**	0.200**	0.224**	0.288**	0.325**	0.396**	0.360**	0.207**	0.227**	0.256**	0.157**	0.757**	0.779**	0.761**	1.000																			
SC1	-0.208**	-0.249**	-0.242**	-0.194**	-0.145**	-0.124**	-0.136**	-0.170**	-0.162**	-0.050	-0.054	-0.076	-0.112**	-0.107**	-0.083*	-0.028	-0.275**	-0.259**	-0.281**	-0.272**	1.000																		
SC2	-0.166**	-0.165**	-0.186**	-0.185**	-0.130**	-0.125**	-0.144**	-0.138**	-0.168**	-0.116**	-0.132**	-0.117**	-0.071	-0.049	-0.050	-0.008	-0.293**	-0.312**	-0.255**	-0.332**	0.757**	1.000																	
SC3	-0.199**	-0.201**	-0.205**	-0.212**	-0.149**	-0.155**	-0.170**	-0.171**	-0.180**	-0.073	-0.119**	-0.117**	-0.114**	-0.097*	-0.106**	-0.051	-0.332**	-0.325**	-0.306**	-0.355**	0.815**	0.858**	1.000																
SC4	-0.189**	-0.124**	-0.198**	-0.217**	-0.130**	-0.135**	-0.150**	-0.168**	-0.218**	-0.105**	-0.148**	-0.154**	-0.121**	-0.107**	-0.120**	-0.100*	-0.338**	-0.342**	-0.276**	-0.331**	0.666**	0.846**	0.833**	1.000															
TA1	0.347**	0.335**	0.384**	0.416**	0.268**	0.280**	0.255**	0.246**	0.363**	0.323**	0.320**	0.365**	0.363**	0.396**	0.324**	0.382**	0.327**	0.287**	0.305**	0.310**	-0.178**	-0.195**	-0.198**	-0.226**	1.000														
TA2	0.339**	0.382**	0.415**	0.402**	0.275**	0.274**	0.257**	0.276**	0.314**	0.299**	0.279**	0.274**	0.357**	0.372**	0.291**	0.343**	0.316**	0.363**	0.354**	0.324**	-0.143**	-0.126**	-0.154**	-0.149**	0.758**	1.000													
TA3	0.350**	0.351**	0.429**	0.399**	0.289**	0.302**	0.270**	0.278**	0.292**	0.270**	0.247**	0.288**	0.373**	0.403**	0.316**	0.370**	0.400**	0.321**	0.330**	0.349**	-0.236**	-0.190**	-0.214**	-0.216**	0.870**	0.744**	1.000												
TA4	0.333**	0.362**	0.377**	0.375**	0.279**	0.287**	0.259**	0.264**	0.333**	0.303**	0.285**	0.299**	0.351**	0.381**	0.302**	0.368**	0.308**	0.305**	0.338**	0.304**	-0.147**	-0.151**	-0.150**	-0.171**	0.842**	0.824**	0.779**	1.000											
CA1	0.205**	0.220**	0.284**	0.222**	0.105**	0.155**	0.170**	0.164**	0.274**	0.258**	0.251**	0.268**	0.188**	0.195**	0.158**	0.184**	0.403**	0.490**	0.431**	0.445**	-0.241**	-0.251**	-0.250**	-0.261**	0.324**	0.271**	0.323**	0.266**	1.000										
CA2	0.288**	0.304**	0.345**	0.336**	0.174**	0.187**	0.199**	0.231**	0.353**	0.260**	0.282**	0.371**	0.237**	0.259**	0.278**	0.215**	0.441**	0.500**	0.569**	0.472**	-0.258**	-0.257**	-0.261**	-0.282**	0.407**	0.312**	0.374**	0.361**	0.618**	1.000									
CA3	0.338**	0.396**	0.432**	0.413**	0.226**	0.240**	0.231**	0.271**	0.341**	0.291**	0.341**	0.378**	0.305**	0.334**	0.334**	0.290**	0.522**	0.551**	0.517**	0.516**	-0.333**	-0.321**	-0.327**	-0.306**	0.464**	0.393**	0.443**	0.423**	0.626**	0.777**	1.000								
CA4	0.295**	0.323**	0.373**	0.413**	0.201**	0.197**	0.205**	0.205**	0.337**	0.309**	0.339**	0.358**	0.302**	0.319**	0.306**	0.251**	0.437**	0.528**	0.499**	0.449**	-0.267**	-0.283**	-0.260**	-0.289**	0.393**	0.346**	0.365**	0.350**	0.543**	0.671**	0.753**	1.000							
PM1	0.302**	0.334**	0.308**	0.270**	0.086*	0.118**	0.071	0.143**	0.247**	0.293**	0.251**	0.214**	0.229**	0.227**	0.228**	0.157**	0.304**	0.302**	0.275**	0.323**	-0.270**	-0.271**	-0.290**	-0.273**	0.339**	0.225**	0.303**	0.275**	0.399**	0.368**	0.403**	0.412**	1.000						
PM2	0.216**	0.283**	0.286**	0.252**	0.111**	0.163**	0.139**	0.154**	0.219**	0.237**	0.229**	0.235**	0.226**	0.208**	0.194**	0.182**	0.358**	0.317**	0.258**	0.338**	-0.180**	-0.215**	-0.211**	-0.207**	0.382**	0.259**	0.330**	0.325**	0.447**	0.433**	0.467**	0.409**	0.637**	1.000					
PM3	0.206**	0.301**	0.277**	0.273**	0.123**	0.145**	0.114**	0.150**	0.262**	0.269**	0.272**	0.234**	0.150**	0.134**	0.140**	0.096*	0.292**	0.342**	0.275**	0.328**	-0.279**	-0.263**	-0.261**	-0.178**	0.366**	0.300**	0.359**	0.310**	0.286**	0.284**	0.365**	0.377**	0.588**	0.591**	1.000				
PM4	0.223**	0.297**	0.259**	0.231**	0.066	0.101*	0.083*	0.121**	0.248**	0.252**	0.214**	0.182**	0.138**	0.149**	0.155**	0.101*	0.174**	0.230**	0.296**	0.250**	-0.234**	-0.201**	-0.240**	-0.171**	0.358**	0.261**	0.286**	0.311**	0.412**	0.407**	0.329**	0.276**	0.650**	0.472**	0.518**	1.000			
PB1	0.281**	0.282**	0.300**	0.270**	0.175**	0.198**	0.202**	0.212**	0.262**	0.215**	0.231**	0.298**	0.276**	0.308**	0.334**	0.289**	0.349**	0.378**	0.342**	0.352**	-0.212**	-0.215**	-0.215**	-0.214**	0.398**	0.257**	0.366**	0.307**	0.476**	0.487**	0.581**	0.508**	0.412**	0.434**	0.323**	0.436**	1.000		
PB2	0.270**	0.276**	0.292**	0.259**	0.158**	0.204**	0.224**	0.199**	0.285**	0.228**	0.282**	0.319**	0.228**	0.260**	0.249**	0.231**	0.459**	0.480**	0.455**	0.424**	-0.196**	-0.248**	-0.249**	-0.294**	0.304**	0.261**	0.325**	0.278**	0.441**	0.605**	0.597**	0.520**	0.315**	0.384**	0.303**	0.333**	0.665**	1.000	
PB3	0.361**	0.398**	0.408**	0.373**	0.141**	0.169**	0.173**	0.220**	0.307**	0.262**	0.291**	0.334**	0.267**	0.283**	0.312**	0.277**	0.395**	0.384**	0.361**	0.394**	-0.202**	-0.255**	-0.244**	-0.259**	0.386**	0.311**	0.356**	0.349**	0.363**	0.463**	0.619**	0.559**	0.378**	0.395**	0.332**	0.340**	0.680**	0.649**	1.000

Bartlett's Test of Sphericity = 19984.24 df = 741 p = 0.000 Kaiser-Meyer-Olkin Measure of Sampling Adequacy = 0.901

หมายเหตุ ** หมายถึง p < 0.01, * หมายถึง P <0.05

ตารางที่ 4.7

ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรสังเกตได้ของกลุ่มตัวอย่าง IT People

ตัวแปร	CP1	CP2	CP3	CP4	PV1	PV2	PV3	PV4	PE1	PE2	PE3	PE4	SN1	SN2	SN3	SN4	SK1	SK2	SK3	SK4	SC1	SC2	SC3	SC4	TA1	TA2	TA3	TA4	CA1	CA2	CA3	CA4	PM1	PM2	PM3	PM4	PB1	PB2	PB3
CP1	1.000																																						
CP2	0.696**	1.000																																					
CP3	0.661**	0.671**	1.000																																				
CP4	0.596**	0.613**	0.743**	1.000																																			
PV1	0.156**	0.160**	0.198**	0.213**	1.000																																		
PV2	0.116*	0.147*	0.127*	0.159**	0.820**	1.000																																	
PV3	0.116*	0.125*	0.179**	0.199**	0.742**	0.869**	1.000																																
PV4	0.101	0.190**	0.171**	0.140*	0.603**	0.738**	0.646**	1.000																															
PE1	0.327**	0.267**	0.397**	0.422**	0.206**	0.132*	0.146*	0.135*	1.000																														
PE2	0.312**	0.300**	0.383**	0.383**	0.118*	0.080	0.031	0.082	0.721**	1.000																													
PE3	0.356**	0.291**	0.414**	0.402**	0.148*	0.096	0.088	0.082	0.680**	0.785**	1.000																												
PE4	0.306**	0.269**	0.357**	0.388**	0.199**	0.145*	0.149**	0.147*	0.765**	0.650**	0.708**	1.000																											
SN1	0.257**	0.227**	0.286**	0.255**	0.340**	0.352**	0.348**	0.281**	0.201**	0.202**	0.212**	0.204**	1.000																										
SN2	0.281**	0.215**	0.280**	0.269**	0.361**	0.381**	0.370**	0.282**	0.246**	0.199**	0.203**	0.255**	0.900**	1.000																									
SN3	0.240**	0.148*	0.275**	0.227**	0.377**	0.412**	0.415**	0.370**	0.207**	0.225**	0.243**	0.254**	0.716**	0.784**	1.000																								
SN4	0.268**	0.142*	0.294**	0.308**	0.401**	0.430**	0.427**	0.313**	0.240**	0.229**	0.246**	0.263**	0.582**	0.673**	0.732**	1.000																							
SK1	0.393**	0.290**	0.339**	0.297**	0.211**	0.200**	0.194**	0.222**	0.312**	0.343**	0.418**	0.402**	0.270**	0.269**	0.232**	0.195**	1.000																						
SK2	0.398**	0.294**	0.377**	0.378**	0.185**	0.169**	0.188**	0.193**	0.323**	0.339**	0.467**	0.400**	0.209**	0.199**	0.213**	0.168**	0.707**	1.000																					
SK3	0.436**	0.398**	0.388**	0.329**	0.122*	0.135*	0.113	0.170**	0.264**	0.300**	0.360**	0.307**	0.240**	0.226**	0.238**	0.200**	0.677**	0.682**	1.000																				
SK4	0.366**	0.293**	0.310**	0.294**	0.190**	0.198**	0.199**	0.214**	0.239**	0.269**	0.406**	0.358**	0.225**	0.235**	0.252**	0.179**	0.806**	0.778**	0.752**	1.000																			
SC1	-0.232**	-0.278**	-0.263**	-0.248**	-0.209**	-0.171**	-0.208**	-0.201**	-0.181**	-0.050	-0.071	-0.084	-0.131*	-0.100	-0.040	-0.020	-0.330**	-0.339**	-0.416**	-0.355**	1.000																		
SC2	-0.193**	-0.197**	-0.207**	-0.220**	-0.161**	-0.126*	-0.179**	-0.131*	-0.195**	-0.136*	-0.169**	-0.142*	-0.080	-0.030	-0.020	-0.020	-0.329**	-0.348**	-0.340**	-0.405**	0.737**	1.000																	
SC3	-0.213**	-0.234**	-0.213**	-0.211**	-0.186**	-0.147*	-0.199**	-0.151**	-0.166**	-0.050	-0.125*	-0.092	-0.070	-0.020	-0.020	0.011	-0.355**	-0.377**	-0.400**	-0.425**	0.816**	0.860**	1.000																
SC4	-0.231**	-0.158**	-0.221**	-0.229**	-0.177**	-0.145*	-0.190**	-0.163**	-0.247**	-0.136*	-0.201**	-0.183**	-0.116*	-0.080	-0.090	-0.100	-0.360**	-0.390**	-0.339**	-0.374**	0.650**	0.840**	0.811**	1.000															
TA1	0.330**	0.313**	0.375**	0.455**	0.248**	0.219**	0.210**	0.140*	0.338**	0.324**	0.328**	0.357**	0.285**	0.346**	0.287**	0.363**	0.243**	0.258**	0.251**	0.264**	-0.169**	-0.183**	-0.131*	-0.184**	1.000														
TA2	0.376**	0.407**	0.442**	0.493**	0.256**	0.235**	0.226**	0.195**	0.357**	0.321**	0.315**	0.335**	0.348**	0.382**	0.320**	0.368**	0.246**	0.351**	0.310**	0.299**	-0.149**	-0.122*	-0.109	-0.097	0.716**	1.000													
TA3	0.358**	0.347**	0.420**	0.412**	0.279**	0.272**	0.249**	0.228**	0.309**	0.272**	0.271**	0.323**	0.315**	0.377**	0.288**	0.358**	0.314**	0.285**	0.281**	0.292**	-0.255**	-0.202**	-0.185**	-0.176**	0.839**	0.748**	1.000												
TA4	0.294**	0.348**	0.318**	0.402**	0.251**	0.231**	0.198**	0.148*	0.334**	0.275**	0.274**	0.316**	0.255**	0.315**	0.264**	0.332**	0.147*	0.215**	0.236**	0.221**	-0.135*	-0.148*	-0.091	-0.109	0.793**	0.797**	0.697**	1.000											
CA1	0.229**	0.198**	0.304**	0.267**	0.111	0.098	0.119*	0.102	0.299**	0.275**	0.315**	0.280**	0.116*	0.119*	0.049	0.130*	0.383**	0.478**	0.449**	0.404**	-0.340**	-0.340**	-0.330**	-0.334**	0.280**	0.245**	0.283**	0.182**	1.000										
CA2	0.286**	0.301**	0.369**	0.342**	0.171**	0.103	0.123*	0.147*	0.334**	0.230**	0.282**	0.342**	0.139*	0.153**	0.147*	0.176**	0.443**	0.459**	0.574**	0.426**	-0.373**	-0.337**	-0.310**	-0.358**	0.312**	0.249**	0.330**	0.254**	0.611**	1.000									
CA3	0.346**	0.390**	0.420**	0.444**	0.282**	0.216**	0.197**	0.211**	0.326**	0.257**	0.364**	0.385**	0.293**	0.323**	0.268**	0.283**	0.516**	0.583**	0.544**	0.517**	-0.413**	-0.384**	-0.365**	-0.361**	0.440**	0.393**	0.442**	0.378**	0.620**	0.743**	1.000								
CA4	0.282**	0.306**	0.361**	0.377**	0.161**	0.091	0.101	0.094	0.338**	0.299**	0.370**	0.373**	0.220**	0.239**	0.188**	0.224**	0.410**	0.515**	0.454**	0.381**	-0.326**	-0.345**	-0.264**	-0.365**	0.348**	0.308**	0.343**	0.302**	0.507**	0.636**	0.727**	1.000							
PM1	0.293**	0.362**	0.327**	0.342**	0.070	0.063	0.021	0.075	0.234**	0.290**	0.274**	0.179**	0.123*	0.119*	0.076	0.044	0.287**	0.261**	0.270**	0.287**	-0.327**	-0.331**	-0.322**	-0.324**	0.283**	0.183**	0.280**	0.211**	0.399**	0.360**	0.420**	0.403**	1.000						
PM2	0.229**	0.247**	0.278**	0.282**	0.128*	0.113	0.090	0.082	0.231**	0.255**	0.270**	0.272**	0.172**	0.166**	0.097	0.134*	0.363**	0.318**	0.261**	0.341**	-0.205**	-0.255**	-0.228**	-0.239**	0.378**	0.241**	0.316**	0.281**	0.461**	0.439**	0.515**	0.422**	0.631**	1.000					
PM3	0.225**	0.329**	0.292**	0.294**	0.112	0.126*	0.083	0.109	0.199**	0.238**	0.259**	0.218**	0.099	0.079	0.057	0.009	0.276**	0.314**	0.294**	0.325**	-0.303**	-0.285**	-0.265**	-0.158**	0.321**	0.301**	0.357**	0.279**	0.289**	0.251**	0.379**	0.326**	0.579**	0.573**	1.000				
PM4	0.234**	0.338**	0.311**	0.344**	0.021	0.013	0.012	0.042	0.224**	0.218**	0.195**	0.142*	0.002	0.003	-0.050	-0.060	0.145*	0.174**	0.313**	0.210**	-0.327**	-0.276**	-0.287**	-0.221**	0.310**	0.225**	0.254**	0.259**	0.393**	0.390**	0.315**	0.213**	0.622**	0.405**	0.488**	1.000			
PB1	0.242**	0.220**	0.283**	0.289**	0.157**	0.135*	0.147*	0.146*	0.234**	0.156**	0.246**	0.278**	0.216**	0.281**	0.258**	0.268**	0.292**	0.358**	0.307**	0.322**	-0.224**	-0.242**	-0.213**	-0.252**	0.346**	0.218**	0.300**	0.251**	0.397**	0.430**	0.556**	0.471**	0.406**	0.385**	0.270**	0.413**	1.000		
PB2	0.251**	0.278**	0.314**	0.311**	0.177**	0.162**	0.193**	0.134*	0.250**	0.198**	0.276**	0.309**	0.220**	0.271**	0.216**	0.232**	0.432**	0.472**	0.449**	0.424**	-0.233**	-0.281**	-0.251**	-0.313**	0.242**	0.239**	0.319**	0.180**	0.394**	0.572**	0.593**	0.548**	0.331**	0.367**	0.278**	0.311**	0.681**	1.000	
PB3	0.338**	0.363**	0.380**	0.367**	0.145*	0.141*	0.159**	0.146*	0.291**	0.222**	0.294**	0.333**	0.274**	0.326**	0.309**	0.298**	0.328**	0.390**	0.340**	0.386**	-0.190**	-0.275**	-0.211**	-0.274**	0.391**	0.310**	0.361**	0.307**	0.283**	0.388**	0.570**	0.516**	0.376**	0.354**	0.307**	0.347**	0.682**	0.658**	1.000

Bartlett’s Test of Sphericity = 9954.42 df = 741 p = 0.000 Kaiser-Meyer-Olkin Measure of Sampling Adequacy = 0.884

หมายเหตุ ** หมายถึง p < 0.01, * หมายถึง P < 0.05

ตารางที่ 4.8

ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรสังเกตได้ของกลุ่มตัวอย่าง Non-IT People

ตัวแปร	CP1	CP2	CP3	CP4	PV1	PV2	PV3	PV4	PE1	PE2	PE3	PE4	SN1	SN2	SN3	SN4	SK1	SK2	SK3	SK4	SC1	SC2	SC3	SC4	TA1	TA2	TA3	TA4	CA1	CA2	CA3	CA4	PM1	PM2	PM3	PM4	PB1	PB2	PB3
CP1	1.000																																						
CP2	0.619**	1.000																																					
CP3	0.680**	0.696**	1.000																																				
CP4	0.477**	0.401**	0.658**	1.000																																			
PV1	0.209**	0.118*	0.177**	0.275**	1.000																																		
PV2	0.149**	0.098	0.136*	0.205**	0.761**	1.000																																	
PV3	0.137*	0.111	0.131*	0.188**	0.731**	0.896**	1.000																																
PV4	0.169**	0.187**	0.204**	0.197**	0.560**	0.705**	0.663**	1.000																															
PE1	0.384**	0.220**	0.266**	0.292**	0.180**	0.262**	0.225**	0.285**	1.000																														
PE2	0.368**	0.260**	0.291**	0.285**	0.207**	0.297**	0.204**	0.271**	0.749**	1.000																													
PE3	0.381**	0.202**	0.277**	0.299**	0.228**	0.256**	0.189**	0.219**	0.747**	0.818**	1.000																												
PE4	0.403**	0.248**	0.278**	0.319**	0.172**	0.234**	0.205**	0.272**	0.807**	0.709**	0.774**	1.000																											
SN1	0.348**	0.253**	0.306**	0.348**	0.462**	0.462**	0.444**	0.409**	0.271**	0.235**	0.204**	0.276**	1.000																										
SN2	0.335**	0.212**	0.287**	0.313**	0.425**	0.446**	0.431**	0.419**	0.278**	0.228**	0.221**	0.281**	0.935**	1.000																									
SN3	0.317**	0.231**	0.306**	0.323**	0.369**	0.395**	0.374**	0.393**	0.292**	0.235**	0.205**	0.297**	0.766**	0.818**	1.000																								
SN4	0.237**	0.151**	0.246**	0.224**	0.323**	0.381**	0.365**	0.426**	0.331**	0.255**	0.248**	0.299**	0.640**	0.693**	0.695**	1.000																							
SK1	0.366**	0.338**	0.371**	0.304**	0.166**	0.255**	0.236**	0.240**	0.358**	0.396**	0.380**	0.377**	0.270**	0.296**	0.285**	0.262**	1.000																						
SK2	0.351**	0.261**	0.346**	0.339**	0.284**	0.286**	0.280**	0.269**	0.328**	0.371**	0.414**	0.297**	0.200**	0.226**	0.239**	0.158**	0.539**	1.000																					
SK3	0.400**	0.348**	0.382**	0.367**	0.249**	0.250**	0.251**	0.230**	0.353**	0.359**	0.370**	0.380**	0.310**	0.341**	0.372**	0.243**	0.599**	0.738**	1.000																				
SK4	0.391**	0.296**	0.424**	0.393**	0.156**	0.208**	0.201**	0.233**	0.336**	0.379**	0.389**	0.361**	0.195**	0.228**	0.276**	0.152**	0.715**	0.781**	0.771**	1.000																			
SC1	-0.193**	-0.230**	-0.227**	-0.152**	-0.077	-0.074	-0.055	-0.140*	-0.143*	-0.051	-0.039	-0.067	-0.101	-0.129*	-0.141*	-0.059	-0.223**	-0.175**	-0.153**	-0.186**	1.000																		
SC2	-0.155**	-0.151**	-0.178**	-0.169**	-0.099	-0.128*	-0.103	-0.147*	-0.141*	-0.097	-0.099	-0.090	-0.081	-0.092	-0.114*	-0.035	-0.261**	-0.273**	-0.176**	-0.256**	0.780**	1.000																	
SC3	-0.192**	-0.178**	-0.202**	-0.222**	-0.111	-0.165**	-0.137*	-0.192**	-0.194**	-0.094	-0.116*	-0.143*	-0.170**	-0.193**	-0.208**	-0.127*	-0.312**	-0.272**	-0.219**	-0.283**	0.814**	0.857**	1.000																
SC4	-0.162**	-0.110	-0.187**	-0.227**	-0.081	-0.128*	-0.104	-0.176**	-0.189**	-0.074	-0.099	-0.122*	-0.146*	-0.163**	-0.185**	-0.149**	-0.323**	-0.291**	-0.217**	-0.284**	0.684**	0.851**	0.861**	1.000															
TA1	0.335**	0.338**	0.388**	0.387**	0.298**	0.339**	0.296**	0.329**	0.342**	0.359**	0.324**	0.364**	0.455**	0.458**	0.375**	0.395**	0.424**	0.360**	0.390**	0.381**	-0.157**	-0.167**	-0.235**	-0.239**	1.000														
TA2	0.297**	0.351**	0.386**	0.315**	0.294**	0.312**	0.292**	0.350**	0.275**	0.279**	0.244**	0.220**	0.358**	0.355**	0.254**	0.311**	0.377**	0.378**	0.392**	0.352**	-0.144*	-0.144*	-0.203**	-0.217**	0.737**	1.000													
TA3	0.335**	0.346**	0.434**	0.380**	0.298**	0.332**	0.295**	0.323**	0.279**	0.268**	0.222**	0.259**	0.418**	0.418**	0.327**	0.368**	0.475**	0.357**	0.373**	0.406**	-0.227**	-0.193**	-0.250**	-0.274**	0.879**	0.738**	1.000												
TA4	0.300**	0.350**	0.356**	0.299**	0.245**	0.279**	0.238**	0.336**	0.340**	0.325**	0.313**	0.316**	0.403**	0.419**	0.322**	0.363**	0.317**	0.304**	0.364**	0.290**	-0.139*	-0.117*	-0.184**	-0.173**	0.837**	0.775**	0.693**	1.000											
CA1	0.189**	0.256**	0.272**	0.189**	0.101	0.221**	0.227**	0.228**	0.249**	0.241**	0.189**	0.254**	0.273**	0.288**	0.285**	0.263**	0.425**	0.503**	0.417**	0.487**	-0.129*	-0.144*	-0.159**	-0.169**	0.369**	0.306**	0.372**	0.313**	1.000										
CA2	0.296**	0.316**	0.327**	0.339**	0.178**	0.275**	0.280**	0.311**	0.372**	0.291**	0.284**	0.399**	0.341**	0.372**	0.414**	0.269**	0.441**	0.540**	0.566**	0.515**	-0.138*	-0.170**	-0.209**	-0.197**	0.481**	0.376**	0.421**	0.475**	0.626**	1.000									
CA3	0.328**	0.399**	0.442**	0.384**	0.169**	0.265**	0.268**	0.327**	0.356**	0.325**	0.317**	0.373**	0.313**	0.342**	0.394**	0.296**	0.530**	0.521**	0.495**	0.517**	-0.254**	-0.263**	-0.291**	-0.256**	0.482**	0.392**	0.443**	0.475**	0.636**	0.813**	1.000								
CA4	0.312**	0.347**	0.387**	0.452**	0.242**	0.306**	0.314**	0.308**	0.336**	0.319**	0.311**	0.343**	0.385**	0.404**	0.423**	0.289**	0.461**	0.540**	0.539**	0.513**	-0.206**	-0.220**	-0.255**	-0.210**	0.441**	0.384**	0.389**	0.395**	0.582**	0.705**	0.780**	1.000							
PM1	0.308**	0.304**	0.288**	0.202**	0.100	0.175**	0.124*	0.207**	0.259**	0.295**	0.229**	0.250**	0.329**	0.329**	0.363**	0.253**	0.319**	0.343**	0.280**	0.359**	-0.214**	-0.216**	-0.261**	-0.226**	0.401**	0.261**	0.323**	0.345**	0.403**	0.378**	0.386**	0.421**	1.000						
PM2	0.211**	0.330**	0.299**	0.234**	0.095	0.216**	0.190**	0.223**	0.208**	0.219**	0.192**	0.198**	0.287**	0.261**	0.300**	0.245**	0.355**	0.315**	0.256**	0.334**	-0.151**	-0.168**	-0.193**	-0.169**	0.433**	0.281**	0.350**	0.366**	0.431**	0.427**	0.423**	0.397**	0.646**	1.000					
PM3	0.184**	0.270**	0.260**	0.250**	0.133*	0.164**	0.147*	0.188**	0.324**	0.300**	0.282**	0.250**	0.196**	0.183**	0.210**	0.166**	0.307**	0.370**	0.258**	0.332**	-0.257**	-0.248**	-0.260**	-0.207**	0.413**	0.297**	0.360**	0.357**	0.288**	0.318**	0.349**	0.425**	0.596**	0.612**	1.000				
PM4	0.211**	0.255**	0.207**	0.124*	0.113*	0.198**	0.163**	0.198**	0.273**	0.288**	0.233**	0.223**	0.276**	0.297**	0.351**	0.255**	0.202**	0.287**	0.282**	0.291**	-0.136*	-0.123*	-0.190**	-0.118*	0.422**	0.297**	0.317**	0.386**	0.435**	0.426**	0.342**	0.340**	0.679**	0.542**	0.548**	1.000			
PB1	0.316**	0.338**	0.315**	0.252**	0.193**	0.260**	0.259**	0.270**	0.290**	0.270**	0.218**	0.318**	0.330**	0.333**	0.402**	0.311**	0.398**	0.397**	0.371**	0.381**	-0.203**	-0.194**	-0.220**	-0.183**	0.450**	0.290**	0.423**	0.318**	0.558**	0.541**	0.604**	0.543**	0.418**	0.481**	0.370**	0.459**	1.000		
PB2	0.294**	0.282**	0.274**	0.218**	0.139*	0.248**	0.257**	0.261**	0.319**	0.258**	0.289**	0.328**	0.243**	0.258**	0.293**	0.249**	0.484**	0.487**	0.461**	0.424**	-0.156**	-0.212**	-0.246**	-0.273**	0.357**	0.285**	0.336**	0.333**	0.489**	0.636**	0.603**	0.494**	0.301**	0.399**	0.329**	0.356**	0.652**	1.000	
PB3	0.384**	0.433**	0.434**	0.380**	0.136*	0.199**	0.188**	0.290**	0.322**	0.301**	0.287**	0.336**	0.260**	0.242**	0.319**	0.265**	0.455**	0.378**	0.379**	0.402**	-0.215**	-0.239**	-0.279**	-0.248**	0.390**	0.311**	0.352**	0.359**	0.448**	0.537**	0.665**	0.601**	0.379**	0.436**	0.357**	0.332**	0.678**	0.641**	1.000

Bartlett's Test of Sphericity = 10477.91 df = 741 p = 0.000 Kaiser-Meyer-Olkin Measure of Sampling Adequacy = 0.896

หมายเหตุ ** หมายถึง p < 0.01, * หมายถึง P <0.05

4.2 การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory factor analysis)

จุดมุ่งหมายในตอนนี้เพื่อตรวจสอบความตรงเชิงโครงสร้างของตัวแปรแฝง โดยใช้วิธีการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirm Factor Analysis) ผลการวิเคราะห์มีรายละเอียดแสดงดังตารางที่ 4.9

ตารางที่ 4.9

ผลการวิเคราะห์องค์ประกอบเชิงยืนยัน

ปัจจัย	ตัวแปร	น้ำหนักองค์ประกอบ	SE	t-Test	R^2	น้ำหนักองค์ประกอบมาตรฐาน
บุคลิกภาพแบบมีจิตสำนึก (CP)	CP1	0.64**	0.03	22.74	0.72	0.85
	CP2	0.54**	0.03	19.44	0.56	0.75
	CP3	0.57**	0.03	2.74	0.62	0.79
	CP4	0.55**	0.03	17.37	0.53	0.73
การรับรู้คุณค่าของข้อมูล (PV)	PV1	0.52**	0.05	23.98	0.66	0.81
	PV2	0.61**	0.02	32.31	0.95	0.97
	PV3	0.61**	0.02	28.34	0.82	0.90
	PV4	0.53**	0.03	2.81	0.54	0.74
ประสบการณ์ในอดีต (PE)	PE1	0.84**	0.03	25.96	0.76	0.87
	PE2	0.81**	0.03	23.89	0.72	0.85
	PE3	0.76**	0.03	24.03	0.68	0.83
	PE4	0.85**	0.03	27.29	0.81	0.90
การคล้อยตามกลุ่มอ้างอิง (SN)	SN1	0.61**	0.03	23.26	0.67	0.82
	SN2	0.67**	0.02	26.66	0.79	0.89
	SN3	0.69**	0.02	27.42	0.81	0.90
	SN4	0.62**	0.03	22.67	0.63	0.79
ความรู้ด้านความปลอดภัย (SK)	SK1	0.71**	0.03	24.81	0.76	0.87
	SK2	0.83**	0.03	26.32	0.82	0.90
	SK3	0.79**	0.03	25.30	0.78	0.88
	SK4	0.79**	0.03	25.50	0.74	0.86

ตารางที่ 4.9

ผลการวิเคราะห์องค์ประกอบเชิงยืนยัน (ต่อ)

ปัจจัย	ตัวแปร	น้ำหนักองค์ประกอบ	SE	t-Test	R^2	น้ำหนักองค์ประกอบมาตรฐาน
ค่าใช้จ่ายในการป้องกัน (SC)	SC1	0.75**	0.03	25.52	0.72	0.85
	SC2	0.78**	0.03	27.59	0.80	0.89
	SC3	0.84**	0.03	31.07	0.92	0.96
	SC4	0.79**	0.03	26.03	0.76	0.87
การรับรู้ต่อสภาวะคุกคาม (TA)	TA1	0.72**	0.02	3.44	0.91	0.96
	TA2	0.65**	0.03	23.33	0.68	0.83
	TA3	0.65**	0.02	27.54	0.81	0.90
	TA4	0.82**	0.03	25.08	0.73	0.85
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	CA1	0.54**	0.03	18.98	0.48	0.70
	CA2	0.70**	0.03	24.94	0.71	0.84
	CA3	0.76**	0.03	28.90	0.85	0.92
	CA4	0.77**	0.03	23.67	0.66	0.81
แรงจูงใจในการป้องกัน (PM)	PM1	0.66**	0.03	23.06	0.66	0.82
	PM2	0.58**	0.03	21.85	0.65	0.80
	PM3	0.55**	0.03	19.23	0.51	0.71
	PM4	0.67**	0.03	2.42	0.59	0.77
พฤติกรรมการป้องกัน (PB)	PB1	0.77**	0.03	23.52	0.68	0.82
	PB2	0.76**	0.03	22.77	0.65	0.81
	PB3	0.75**	0.03	23.14	0.66	0.82

Chi-square = 173.47, df = 642, χ^2/df =2.69, GFI = 0.871, AGFI = 0.843, RMR = 0.024, RMSEA=0.053

** = $p < 0.01$

จากตารางที่ 4.9 พบว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ พิจารณาจากค่าไค-สแควร์ (χ^2) ต่อองศาอิสระ (df) เท่ากับ 2.69 ดัชนีรากที่สองของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ (RMR) เท่ากับ 0.024 ดัชนีวัดความคลาดเคลื่อนในการประมาณค่าพารามิเตอร์ (RMSEA) มีค่า 0.053 ส่วนค่าดัชนีวัดระดับความกลมกลืน (GFI) มีค่าเป็น 0.871 และดัชนีวัดระดับ

ความกลมกลืนที่ปรับแก้แล้ว (AGFI) มีค่าเป็น 0.843 แม้ไม่ผ่านเกณฑ์ที่กำหนด แต่ก็มีค่าเข้าใกล้ 0.900 แสดงว่า มีความกลมกลืนระหว่างข้อมูลเชิงประจักษ์กับโมเดลโครงสร้าง

เมื่อพิจารณาในแต่ละองค์ประกอบย่อย พบว่า ตัวแปรในองค์ประกอบบุคลิกภาพแบบมีจิตสำนึก (CP) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.73 – 0.85 ตัวแปรในองค์ประกอบการรับรู้คุณค่าของข้อมูล (PV) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.74 – 0.97 ตัวแปรในองค์ประกอบประสบการณ์ในอดีต (PE) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.83 – 0.90 การคล้อยตามกลุ่มอ้างอิง (SN) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.79 – 0.90 ตัวแปรในองค์ประกอบความรู้ด้านความปลอดภัย (SK) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.86 – 0.90 ตัวแปรในองค์ประกอบค่าาใช้จ่ายในการป้องกัน (SC) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.85 – 0.96 ตัวแปรในองค์ประกอบการรับรู้ต่อสภาวะคุกคาม (TA) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.83 – 0.96 ตัวแปรในองค์ประกอบการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.70 – 0.92 ตัวแปรในองค์ประกอบแรงจูงใจในการป้องกัน (PM) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.871 – 0.82 และตัวแปรในองค์ประกอบพฤติกรรมการป้องกัน (PB) มีค่าน้ำหนักองค์ประกอบมาตรฐาน ระหว่าง 0.81 – 0.82

4.3 การวิเคราะห์ความสอดคล้องของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ที่สร้างขึ้นกับข้อมูลเชิงประจักษ์

การวิเคราะห์ข้อมูลในส่วนนี้เป็นการวิเคราะห์เพื่อตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ที่สร้างขึ้นกับข้อมูลเชิงประจักษ์ ผลการวิเคราะห์มีรายละเอียดดังต่อไปนี้

4.3.1 การตรวจสอบความกลมกลืนของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

การตรวจสอบความกลมกลืนของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ เป็นการตรวจสอบโมเดลความสัมพันธ์เชิงสาเหตุตามสมมติฐานกับข้อมูลเชิงประจักษ์ว่ามีความกลมกลืนกันหรือไม่ ผลการวิเคราะห์โมเดลในตอนแรก พบว่า โมเดลไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยจึงทำการปรับโมเดลโดยยอมให้ความคลาดเคลื่อนมีความสัมพันธ์กันได้ ซึ่งผู้วิจัยพิจารณาจากดัชนีดัดแปรโมเดล (modification indicies) และผลจาก

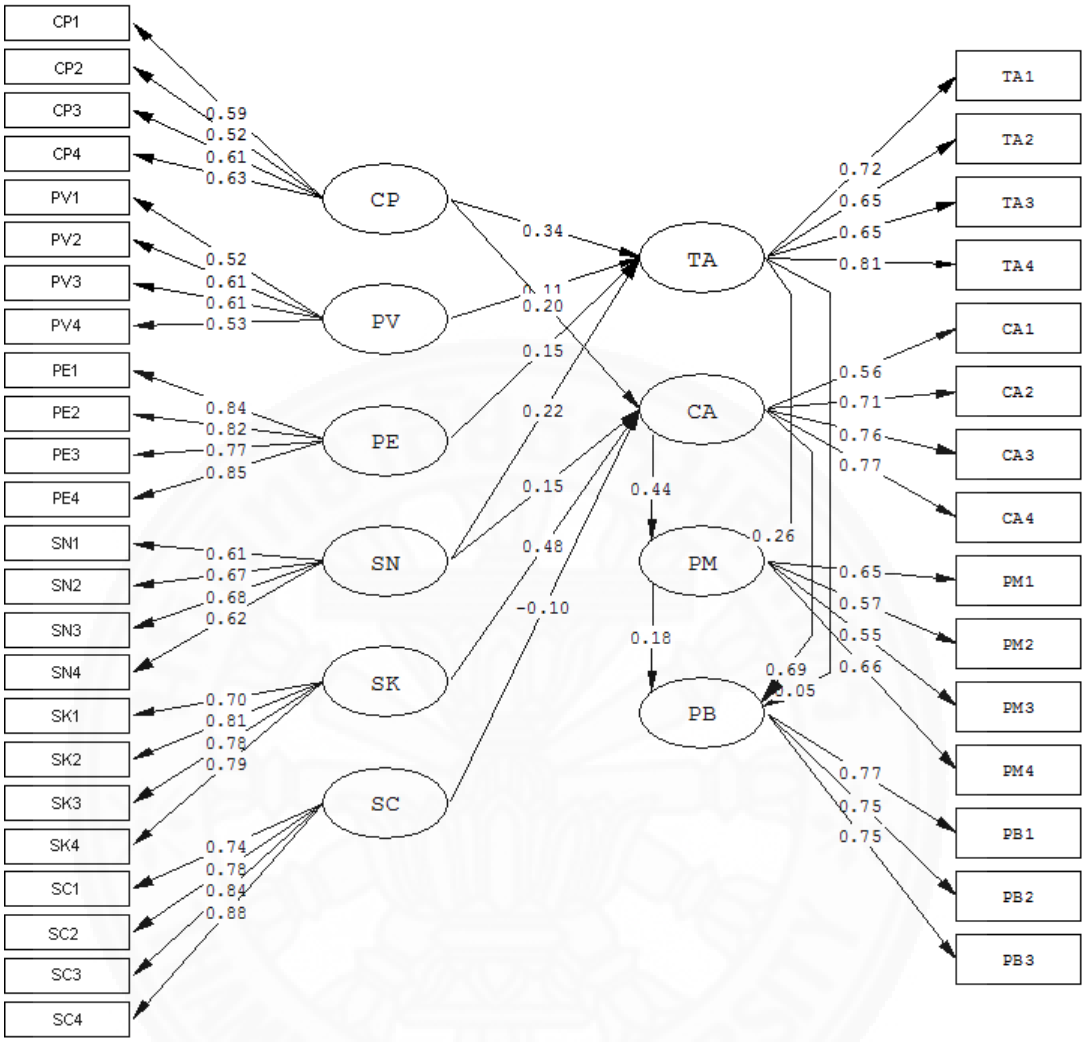
การปรับโมเดล ผู้วิจัยได้โมเดลเชิงสาเหตุของทักษะชีวิตที่สอดคล้องกับข้อมูลเชิงประจักษ์แสดงได้ดังภาพที่ 4.1 และมีรายละเอียดดังแสดงในตารางที่ 4.10

ตารางที่ 4.10

ค่าสถิติวิเคราะห์ความกลมกลืนของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ก่อนและหลังปรับโมเดล

ดัชนีที่ใช้ตรวจสอบความกลมกลืนของโมเดล	**เกณฑ์การพิจารณา**	**ค่าสถิติก่อนปรับโมเดล**	**ค่าสถิติหลังปรับโมเดล**
Likelihood Ratio Chi-Square Statistic (χ^2)	> 0.050	351.18 (p = 0.00)	241.338 (p = 0.00)
Relative χ^2 (χ^2/df)	2.000	0.488	0.976
Goodness of Fit Index (GFI)	> 0.900	0.832	0.904
Adjusted Goodness of Fit Index (AGFI)	> 0.900	0.806	0.881
Root Mean Squared Residuals (RMR)	< 0.050	0.035	0.030
Root Mean Squared Error of Approximation (RMSEA)	< 0.050	0.064	0.040
Critical N (CN)	> 200	187.137	323.189

จากตารางที่ 4.10 แสดงค่าสถิติวิเคราะห์ความกลมกลืนของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ ซึ่งพบว่า หลังจากทำการปรับโมเดลโมเดลความสัมพันธ์เชิงสาเหตุตามสมมติฐานมีความกลมกลืนกับข้อมูลเชิงประจักษ์ พิจารณาได้จากค่าสถิติวิเคราะห์ดังนี้คือ ค่าไค-สแควร์ (χ^2) ต่อองศาอิสระเท่ากับ 1.976 ผ่านเกณฑ์กำหนด เพราะน้อยกว่า 2.000 (ค่าไค-สแควร์เท่ากับ 1241.338 ที่องศาอิสระ 628) ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.904 ผ่านเกณฑ์กำหนดเพราะมากกว่า 0.900 ดัชนีรากที่สองของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ (RMR) เท่ากับ 0.030 ดัชนีวัดความคลาดเคลื่อนในการประมาณค่าพารามิเตอร์ (RMSEA) เท่ากับ 0.040 ผ่านเกณฑ์กำหนดเพราะน้อยกว่า 0.050 ค่าดัชนี CN เท่ากับ 323.189 ซึ่งผ่านเกณฑ์กำหนดเพราะมากกว่าหรือเท่ากับ 200 ส่วนดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) มีค่า 0.881 แม้ไม่ผ่านเกณฑ์ที่กำหนด คือมากกว่า 0.900 แต่ก็มีค่าใกล้เคียง



ภาพที่ 4.1 ค่าสถิติวิเคราะห์ความกลมกลืนของโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์หลังปรับโมเดล

4.3.2 การตรวจสอบความกลมกลืนของโมเดลการวัดในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

การตรวจสอบความกลมกลืนของโมเดลการวัดในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์เป็นการตรวจสอบภายหลังจากที่มีการปรับโมเดลความสัมพันธ์ให้มีความกลมกลืนกับข้อมูลเชิงประจักษ์แล้ว เพื่อประเมินความสามารถของตัวแปรสังเกตได้ที่ใช้วัดตัวแปรแฝงในโมเดล โดยการพิจารณาจากความมีนัยสำคัญของน้ำหนักองค์ประกอบประเมินค่าความแปรปรวนที่สกัดได้ และค่าความเชื่อมั่นของตัวแปรแฝงที่ศึกษา ผลการตรวจสอบความกลมกลืนของโมเดลการวัดดังกล่าว แสดงดังตารางที่ 4.11

ตารางที่ 4.11

การตรวจสอบความกลมกลืนของโมเดลการวัดในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

ปัจจัย	**ตัวแปรสังเกตได้**	**น้ำหนักองค์ประกอบมาตรฐาน**	**น้ำหนักองค์ประกอบ**	**SE**	**t-Test**	**R^2**	**CR**	**AVE**
บุคลิกภาพแบบมีจิตสำนึก (CP)	CP1	0.786	0.592	0.029	2.436	0.617	0.874	0.636
	CP2	0.723	0.521	0.034	15.540	0.523		
	CP3	0.850	0.614	0.026	23.626	0.772		
	CP4	0.824	0.627	0.028	22.036	0.680		
การรับรู้คุณค่าของข้อมูล (PV)	PV1	0.811	0.518	0.022	23.913	0.658	0.919	0.742
	PV2	0.976	0.612	0.019	32.430	0.953		
	PV3	0.903	0.613	0.022	28.418	0.815		
	PV4	0.736	0.525	0.025	2.816	0.542		
ประสบการณ์ในอดีต (PE)	PE1	0.868	0.841	0.032	26.007	0.753	0.922	0.747
	PE2	0.856	0.819	0.033	24.511	0.732		
	PE3	0.831	0.768	0.031	24.383	0.691		
	PE4	0.900	0.850	0.031	27.350	0.811		
การคล้อยตามกลุ่มอ้างอิง (SN)	SN1	0.816	0.608	0.026	23.284	0.666	0.913	0.724
	SN2	0.886	0.666	0.025	26.669	0.786		
	SN3	0.902	0.685	0.025	27.403	0.814		
	SN4	0.794	0.617	0.027	22.639	0.630		
ความรู้ด้านความปลอดภัย (SK)	SK1	0.868	0.701	0.028	24.872	0.753	0.929	0.765
	SK2	0.893	0.806	0.031	26.350	0.797		
	SK3	0.868	0.781	0.031	25.097	0.754		
	SK4	0.870	0.793	0.031	25.949	0.756		
ค่าใช้จ่ายในการป้องกัน (SC)	SC1	0.844	0.737	0.029	25.471	0.712	0.953	0.834
	SC2	0.896	0.785	0.028	27.836	0.802		
	SC3	0.960	0.842	0.027	31.098	0.921		
	SC4	0.950	0.878	0.030	29.380	0.902		

ตารางที่ 4.11

การตรวจสอบความกลมกลืนของโมเดลการวัดในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ (ต่อ)

ปัจจัย	ตัวแปรสังเกตได้	น้ำหนักองค์ประกอบมาตรฐาน	น้ำหนักองค์ประกอบ	SE	t-Test	R^2	CR	AVE
การรับรู้ต่อสภาวะคุกคาม (TA)	TA1	0.960	0.718	-	-	0.921	0.935	0.783
	TA2	0.830	0.654	0.024	27.103	0.688		
	TA3	0.900	0.652	0.019	34.296	0.810		
	TA4	0.844	0.807	0.028	28.895	0.712		
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	CA1	0.711	0.556	-	-	0.506	0.894	0.681
	CA2	0.848	0.712	0.035	2.066	0.720		
	CA3	0.918	0.761	0.035	21.800	0.842		
	CA4	0.810	0.772	0.039	19.566	0.656		
แรงจูงใจในการป้องกัน (PM)	PM1	0.808	0.647	-	-	0.652	0.856	0.598
	PM2	0.801	0.571	0.029	19.502	0.641		
	PM3	0.717	0.545	0.029	19.066	0.514		
	PM4	0.764	0.662	0.035	18.931	0.584		
พฤติกรรมการป้องกัน (PB)	PB1	0.826	0.771	-	-	0.682	0.855	0.663
	PB2	0.798	0.748	0.034	21.719	0.637		
	PB3	0.819	0.745	0.033	22.263	0.671		
	SN4	0.794	0.617	0.027	22.639	0.630		

จากตารางที่ 4.11 พบว่า ตัวแปรแฝงในโมเดลจำนวน 10 ตัวแปร ประกอบด้วยตัวแปรผล 1 ตัวแปรคือ พฤติกรรมการป้องกัน (PB) ตัวแปรคั่นกลาง 3 ตัวแปร คือ แรงจูงใจในการป้องกัน (PM) การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และการรับรู้ต่อสภาวะคุกคาม (TA) ซึ่งตัวแปรแฝงแต่ละตัวดังกล่าวมีตัวแปรสังเกตได้เป็นองค์ประกอบ ซึ่งรายละเอียดองค์ประกอบของตัวแปรแฝงแต่ละตัว และผลการประเมินความสามารถขององค์ประกอบหรือตัวแปรสังเกตได้ที่ใช้วัดตัวแปรแฝงในโมเดลสรุปได้ว่า ตัวแปรสังเกตได้ที่ใช้วัดตัวแปรแฝงในโมเดลแต่ละชุดตัวแปรนั้นโดยรวมมีค่าน้ำหนักองค์ประกอบมาตรฐานที่ดี คือมีค่ามากกว่า 0.50 โดยตัวแปรที่มีค่าน้ำหนักองค์ประกอบมาตรฐานมากที่สุดคือ PV2 มีค่า 0.976 รองลงมาคือ TA1 มีค่า 0.960 ส่วนตัวแปรที่มีค่าน้ำหนักองค์ประกอบมาตรฐานน้อยที่สุด คือ CA1 มีค่า 0.711 รองลงมาคือ PM3 มีค่า 0.717

นอกจากนี้ ทุกองค์ประกอบมีค่า Average Variance Extracted (AVE) มากกว่า 0.50 แสดงให้เห็นว่า โดยภาพรวม การวัดมีความตรงเชิงจำแนก (DiscriMINant Validity) กล่าวอีกนัยหนึ่งคือ ตัวแปรสังเกตได้ของแต่ละองค์ประกอบสามารถอธิบายองค์ประกอบนั้น ๆ ได้เป็นอย่างดี รวมถึง ค่า Composite Reliability มีค่ามากกว่า 0.80 แสดงว่ามีความเชื่อถือได้ของการวัดในแต่ละองค์ประกอบสูง

4.3.3 การวิเคราะห์ค่าสัมประสิทธิ์เส้นทาง (Path Coefficient) ในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

การวิเคราะห์ค่าสัมประสิทธิ์เส้นทาง (Path Coefficient) ในโมเดลความสัมพันธ์เชิงสาเหตุของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ เป็นการวิเคราะห์อิทธิพลทางตรง (Direct effect: DE) อิทธิพลทางอ้อม (Indirect effect: IE) และอิทธิพลรวม (Total effect: TE) เพื่อทราบอิทธิพลของตัวแปรเชิงสาเหตุที่มีต่อตัวแปรผลภายในโมเดลโครงสร้างความสัมพันธ์ ซึ่งในที่นี้ผู้วิจัยนำเสนอผลการวิเคราะห์อิทธิพลจำแนกเป็น 3 ส่วน ได้แก่ ผลของอิทธิพลทางตรง ผลของอิทธิพลทางอ้อม และผลของอิทธิพลรวม แสดงดังตารางที่ 4.12

ตารางที่ 4.12

อิทธิพลทางตรง อิทธิพลทางอ้อม และอิทธิพลรวมภายในโมเดลความสัมพันธ์เชิงสาเหตุของของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

ตัวแปรผล / **ตัวแปรสาเหตุ**	การรับรู้ต่อสภาวะคุกคาม (TA)			การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)			แรงจูงใจในการป้องกัน (PM)			พฤติกรรมการป้องกัน (PB)		
	TE	IE	DE	TE	IE	DE	TE	IE	DE	TE	IE	DE
บุคลิกภาพแบบมีจิตสำนึก (CP)	0.340**	-	0.340**	0.199**	-	0.199**	0.175**	0.175**	-	0.185**	0.185**	-
การรับรู้คุณค่าของข้อมูล (PV)	0.113**	-	0.113**	-	-	-	0.029*	0.029*	-	0.110*	0.110*	-
ประสบการณ์ในอดีต (PE)	0.149**	-	0.149**	-	-	-	0.036**	0.036**	-	0.014*	0.014*	-
การคล้อยตามกลุ่มอ้างอิง (SN)	0.215**	-	0.215**	0.148**	-	0.148**	0.121**	0.121**	-	0.134**	0.134**	-
ความรู้ด้านความปลอดภัย (SK)	-	-	-	0.483**	-	0.483**	0.214**	0.214**	-	0.372**	0.372**	-
ค่าใช้จ่ายในการป้องกัน (SC)	-	-	-	-0.105**	-	-0.105**	-0.046**	-0.046**	-	-0.080**	-0.080**	-
การรับรู้ต่อสภาวะคุกคาม (TA)	-	-	-	-	-	-	0.257**	-	0.257**	0.094**	0.046**	0.048**
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	-	-	-	-	-	-	0.443**	-	0.443**	0.769**	0.08**	0.689**
แรงจูงใจในการป้องกัน (PM)	-	-	-	-	-	-	-	-	-	0.18**	-	0.18**
R^2	0.370			0.524			0.343			0.672		

หมายเหตุ DE หมายถึงอิทธิพลทางตรง, IE หมายถึงอิทธิพลทางอ้อม, TE หมายถึงอิทธิพลรวม, ** หมายถึง $p < 0.01$, * หมายถึง $p < 0.05$

จากตารางที่ 4.12 เมื่อพิจารณาค่าสัมประสิทธิ์การพยากรณ์ (R2) ของสมการโครงสร้างตัวแปรภายในแฝงในแฝงพบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ (PB) มีค่าเท่ากับ 0.672 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 67.2 ตัวแปรแรงจูงใจในการป้องกัน (PM) มีค่าสัมประสิทธิ์การพยากรณ์ (R2) เท่ากับ 0.343 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของแรงจูงใจในการป้องกันในการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 34.3 ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) มีค่าสัมประสิทธิ์การพยากรณ์ (R2) เท่ากับ 0.524 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 52.4 และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีค่าสัมประสิทธิ์การพยากรณ์ (R2) เท่ากับ 0.370 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้ความสามารถในการจัดการกับภัยคุกคามของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 37

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 จากตัวแปรแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลเท่ากับ 0.180 นอกจากนี้ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ยังมีอิทธิพลทางตรงต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) โดยมีขนาดอิทธิพลเท่ากับ 0.048 และ 0.689 ตามลำดับ สำหรับอิทธิพลทางอ้อมที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ยังมีอิทธิพลทางอ้อมต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) โดยตรงผ่านตัวแปรแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลเท่ากับ 0.046 และ 0.08 ตามลำดับ นอกจากนี้ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) ตัวแปรความรู้ด้านความปลอดภัย (SK) ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางอ้อมต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) โดยตรงผ่านตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรดังกล่าวมีอิทธิพลทางอ้อมอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ยกเว้นตัวแปรการรับรู้คุณค่าของข้อมูล (PV) และตัวแปรประสบการณ์ในอดีต (PE) ที่มีอิทธิพลทางอ้อมอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.185 0.11 0.014 0.134 0.372 และ -0.08 ตามลำดับ สำหรับอิทธิพลรวม พบว่าตัวแปรอิทธิพลรวมสูงสุดต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้

คอมพิวเตอร์ (PB) คือตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีขนาดอิทธิพลเท่ากับ 0.769 รองลงมาคือ ตัวแปรความรู้ด้านความปลอดภัย (SK) และ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) โดยมีขนาดอิทธิพลเท่ากับ 0.372 และ 0.185 ตามลำดับ

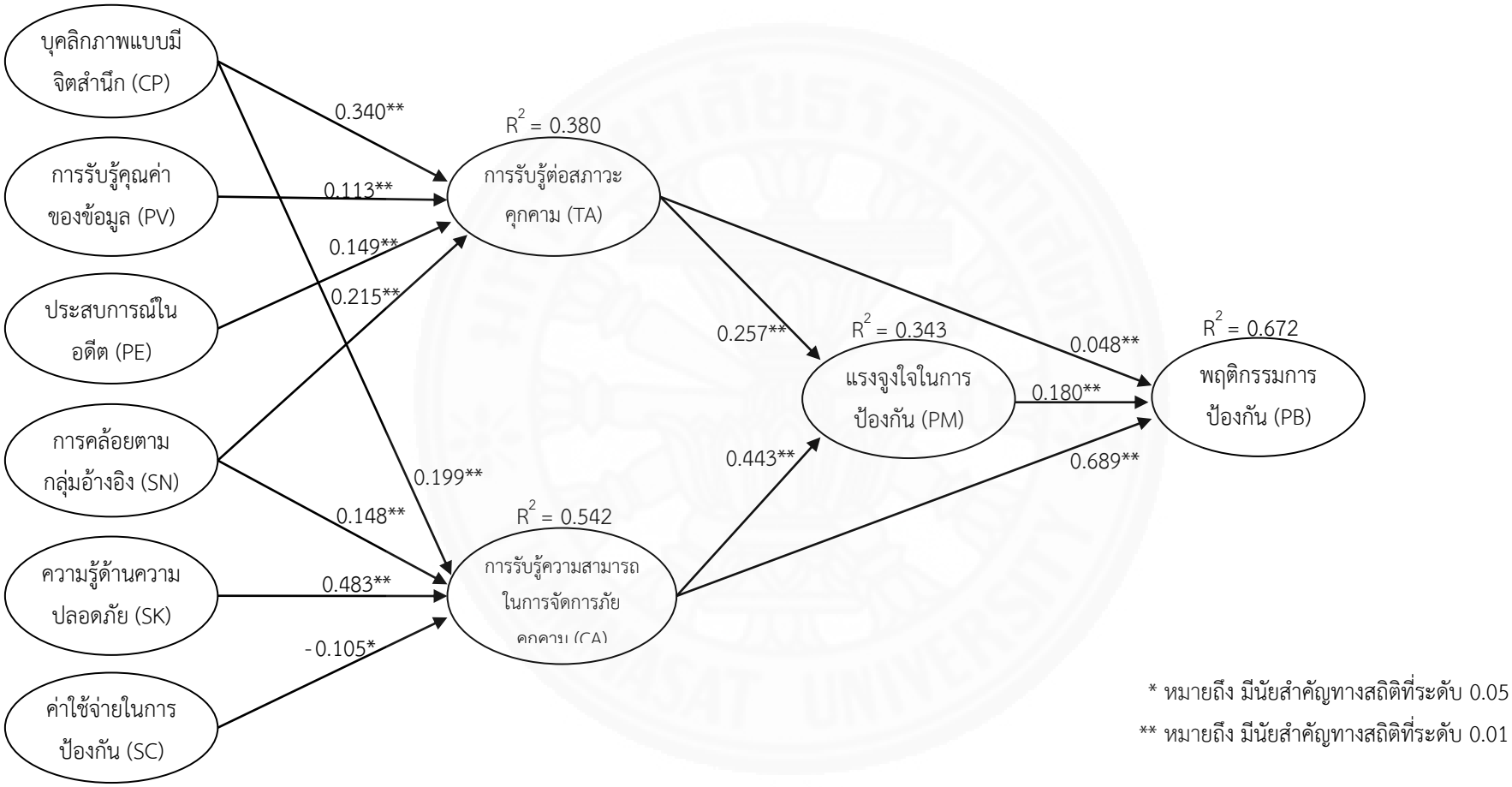
เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 จากตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) โดยมีขนาดอิทธิพลเท่ากับ 0.257 และ 0.443 สำหรับอิทธิพลทางอ้อมที่ส่งผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) ตัวแปรความรู้ด้านความปลอดภัย (SK) ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางอ้อมต่อแรงจูงใจในการป้องกัน (PM) โดยตรงผ่านตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรดังกล่าวมีอิทธิพลทางอ้อมอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ยกเว้นตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ที่มีอิทธิพลทางอ้อมอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีขนาดอิทธิพลเท่ากับ 0.175 0.029 0.036 0.121 0.214 และ -0.046 ตามลำดับ สำหรับอิทธิพลรวม พบว่าตัวแปรอิทธิพลรวมสูงสุดต่อแรงจูงใจในการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) คือตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีขนาดอิทธิพลเท่ากับ 0.443 รองลงมาคือ ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และ ตัวแปรความรู้ด้านความปลอดภัย (SK) โดยมีขนาดอิทธิพลเท่ากับ 0.257 และ 0.214 ตามลำดับ

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ต่อสภาวะคุกคาม (TA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 จากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) และตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) โดยมีขนาดอิทธิพลเท่ากับ 0.34 0.113 0.149 และ 0.215 ตามลำดับ แสดงว่าบุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล ประสบการณ์ในอดีต และการคล้อยตามกลุ่มอ้างอิง มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยบุคลิกภาพแบบมีจิตสำนึกมีอิทธิพลสูงกว่าการคล้อยตามกลุ่มอ้างอิง ประสบการณ์ในอดีต และการรับรู้คุณค่าของข้อมูลตามลำดับ สำหรับอิทธพลรวม พบว่า ตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) มีขนาดอิทธิพลเท่ากับ 0.34 รองลงมาคือ ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และ ตัวแปรประสบการณ์ในอดีต (PE) มีขนาดอิทธิพลเท่ากับ 0.215 และ 0.149 ตามลำดับ

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

จากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) ตัวแปรความรู้ด้านความปลอดภัย (SK) และตัวแปรค่าใช้จ่ายในการป้องกัน (SC) โดยมีขนาดอิทธิพลเท่ากับ 0.199 0.148 0.483 และ 0.105 ตามลำดับ แสดงว่าบุคลิกภาพแบบมีจิตสำนึก การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการการรับรู้ความสามารถในการจัดการกับภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยความรู้ด้านความปลอดภัยมีอิทธิพลสูงกว่าบุคลิกภาพแบบมีจิตสำนึก การคล้อยตามกลุ่มอ้างอิง และค่าใช้จ่ายในการป้องกันตามลำดับ สำหรับอิทธพลรวม พบว่า ตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรความรู้ด้านความปลอดภัย (SK) มีขนาดอิทธิพลเท่ากับ 0.483 รองลงมาคือ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) และตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) มีขนาดอิทธิพลเท่ากับ 0.199 และ 0.148 ตามลำดับ

จากข้อมูลที่กล่าวมาทั้งหมดข้างต้น สามารถแสดงค่าสถิติวิเคราะห์ต่างๆ ในโมเดล แสดงดังภาพที่ 4.2



ภาพที่ 4.2 ผลการวิเคราะห์โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์

4.4 การวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน

การวิเคราะห์ในตอนนี้มีจุดมุ่งหมายเพื่อทดสอบสมมติฐานเกี่ยวกับความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน โดยแบ่งเป็นกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ หรือ IT People และกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ หรือ Non-IT People เป็นการวิเคราะห์โดยใช้เทคนิคการวิเคราะห์กลุ่มพหุ (Multiple-Group analysis)

การตรวจสอบความไม่แปรเปลี่ยนของโมเดล มีสมมติฐานสำหรับการวิเคราะห์ความไม่แปรเปลี่ยนของโมเดล รวม 2 สมมติฐาน ดังนี้

(1) การทดสอบสมมติฐานความไม่แปรเปลี่ยนของรูปแบบโมเดล

(2) การทดสอบสมมติฐานความไม่แปรเปลี่ยนของพารามิเตอร์ของเมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β) และสมมติฐานข้อ 1

(3) การทดสอบสมมติฐานความไม่แปรเปลี่ยนของพารามิเตอร์ของเมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง (Γ) และสมมติฐานข้อ 2

ผลการวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน ตามสมมติฐานที่กล่าวไว้ข้างต้น มีรายละเอียดแสดงดังตารางที่ 4.13

ตารางที่ 4.13

ผลการทดสอบความไม่แปรปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน

สมมติฐาน	χ^2	df	χ^2/df	p	GFI	NFI	RFI	RMR
1. H_{form}	154.83	1298	1.660	0.000	0.845	0.957	0.951	0.039
2. H_{β}	159.58	1303	1.657	0.000	0.846	0.957	0.951	0.040
3. $H_{\beta\Gamma}$	167.14	1309	1.656	0.000	0.845	0.957	0.951	0.045
$\Delta\chi^2_{2-1}$ = 4.75 Δdf_{2-1} =5								
$\Delta\chi^2_{3-2}$ = 7.56 Δdf_{3-2} =6								

หมายเหตุ $\Delta\chi^2_{a-b}$ หมายถึง ผลต่างของค่าไค-แสควร์ที่ได้จากการวิเคราะห์โมเดลตามสมมติฐานที่ a และ b

Δdf_{a-b} หมายถึง ผลต่างของค่าองศาอิสระที่ได้จากการวิเคราะห์โมเดลตามสมมติฐานที่ a และ b

จากตารางที่ 4.13 เมื่อพิจารณาผลการวิเคราะห์สมการโครงสร้างกลุ่มพหุเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ในสมมติฐานแรก (H_{form}: รูปแบบไม่เปลี่ยน) ซึ่งเป็นการทดสอบความไม่แปรเปลี่ยนของรูปแบบโมเดลโดยไม่กำหนดให้ค่าพารามิเตอร์ระหว่างกลุ่มเท่ากัน ซึ่งก็คือการทดสอบความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ในแต่ละกลุ่มประชากร ผลการทดสอบพบว่า ไม่ปฏิเสธสมมติฐาน โดยพิจารณาจากค่า χ^2 = 2154.83 df=1298 GFI=0.845 NFI=0.957 RFI=0.951 RMR=0.039 และ χ^2/df =1.660 จากข้อมูลข้างต้น ค่า GFI NFI และRFI มีค่าเข้าใกล้ 1 RMR มีค่าน้อยกว่า 0.05 และค่าไค-สแควร์สัมพัทธ์มีค่าน้อยกว่า 2 โดยทุกค่าให้ผลที่สอดคล้องกัน จึงยอมรับสมมติฐานที่ว่าโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ตามสมมติฐานมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งเป็นหลักฐานยืนยันว่าโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศมีรูปแบบลักษณะโครงสร้างเป็นแบบเดียวกัน

ผลการทดสอบสมมติฐานข้อที่ 2 (H_{β}) ซึ่งเป็นการทดสอบสมมติฐานความไม่แปรเปลี่ยนของพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β) โดยการกำหนดให้เมทริกซ์พารามิเตอร์ดังกล่าวมีค่าเท่ากันทั้ง 2 กลุ่ม ผลการทดสอบพบว่า ไม่ปฏิเสธสมมติฐาน โดยพิจารณาจากค่า χ^2 = 2159.58 df=1303 GFI=0.846 NFI=0.957 RFI=0.951 RMR=0.040 และ χ^2/df

=1.657 จากข้อมูลข้างต้นจะเห็นได้ว่า ค่า GFI NFI และ RFI มีค่าเข้าใกล้ 1 ค่า RMR มีน้อยกว่า 0.05 และค่าไค-สแควร์สัมพัทธ์มีค่าน้อยกว่า 2 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ และผลการทดสอบความแตกต่างของค่าไค-แสควร์ระหว่างสมมติฐานที่ 2 และ 1 ($\Delta\chi^2_{2-1}$) มีค่าเท่ากับ 4.75 ที่ $\Delta df_{2-1} = 5$ พบว่าไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ผลการทดสอบนี้แสดงว่า การกำหนดเงื่อนไขบังคับให้เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β) ของกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) และกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) มีค่าเท่ากัน ไม่มีความแปรเปลี่ยนของค่าพารามิเตอร์

ผลการทดสอบสมมติฐานข้อที่ 3 ($H_{\beta\Gamma}$) ซึ่งเป็นการทดสอบสมมติฐานความไม่แปรเปลี่ยนของพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β) และพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง (Γ) โดยการกำหนดให้เมทริกซ์พารามิเตอร์ดังกล่าวมีค่าเท่ากันทั้ง 2 กลุ่ม ผลการทดสอบพบว่า ไม่ปฏิเสธสมมติฐาน โดยพิจารณาจากค่า χ^2 = 2167.14 df=1309 GFI=0.845 NFI=0.957 RFI=0.951 RMR=0.045 และ χ^2/df =1.656 จากข้อมูลข้างต้นจะเห็นได้ว่า ค่า GFI NFI และ RFI มีค่าเข้าใกล้ 1 ค่า RMR มีน้อยกว่า 0.05 และค่าไค-สแควร์สัมพัทธ์มีค่าน้อยกว่า 2 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ และผลการทดสอบความแตกต่างของค่าไค-แสควร์ระหว่างสมมติฐานที่ 2 และ 1 ($\Delta\chi^2_{3-2}$) มีค่าเท่ากับ 7.56 ที่ $\Delta df_{3-2} = 6$ พบว่าไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ผลการทดสอบนี้แสดงว่า การกำหนดเงื่อนไขบังคับให้เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง (Γ) และเมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β) ของกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) และกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) มีค่าเท่ากัน ไม่มีความแปรเปลี่ยนของค่าพารามิเตอร์

สรุปผลการทดสอบสมมติฐานความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของกลุ่มผู้ใช้คอมพิวเตอร์ระหว่าง 2 กลุ่ม คือ กลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) และกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) ตามที่ผู้วิจัยกำหนดไว้ สรุปได้ว่า โมเดลมีความไม่แปรเปลี่ยนในด้านรูปแบบโมเดล และค่าพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง (Γ) และค่าพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง (β)

ในการนำเสนอผลการวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลในกลุ่มทักษะด้านเทคโนโลยีสารสนเทศที่แตกต่างกัน ผู้วิจัยจะนำเสนอโมเดลที่มีความไม่แปรเปลี่ยนของรูปแบบโมเดล หรือโมเดลที่ไม่มีเงื่อนไขกำหนดให้ค่าพารามิเตอร์ของโมเดลมีค่าเท่ากัน แสดงได้ดังภาพที่ 4.3 และ 4.4 มีรายละเอียดแสดงดังตารางที่ 4.14

ตารางที่ 4.14

ผลการวิเคราะห์แยกค่าอิทธิพลของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศแตกต่างกัน

	กลุ่ม IT People											
ตัวแปรผล / **ตัวแปรสาเหตุ**	การรับรู้ต่อสภาวะคุกคาม (TA)			การรับรู้ความสามารถในการจัดการกับภัยคุกคาม(CA)			แรงจูงใจในการป้องกัน (PM)			พฤติกรรมการป้องกัน (PB)		
	TE	IE	DE	TE	IE	DE	TE	IE	DE	TE	IE	DE
บุคลิกภาพแบบมีจิตสำนึก (CP)	0.267**	-	0.267**	0.160**	-	0.160**	0.148**	0.148**	-	0.176**	0.176**	-
การรับรู้คุณค่าของข้อมูล (PV)	0.039	-	0.039	-		-	0.006	0.006	-	0.003	0.003	-
ประสบการณ์ในอดีต (PE)	0.092*	-	0.092*	-		-	0.014	0.014	-	0.007	0.007	-
การคล้อยตามกลุ่มอ้างอิง (SN)	0.150**	-	0.150**	0.026	-	0.026	0.040	0.040	-	0.037	0.037	-
ความรู้ด้านความปลอดภัย (SK)	-	-	-	0.229**	-	0.229**	0.153**	0.153**	-	0.222**	0.222**	-
ค่าใช้จ่ายในการป้องกัน (SC)	-	-	-	-0.092**	-	-0.092**	-0.062**	-0.062**	-	-0.090**	-0.090**	-
การรับรู้ต่อสภาวะคุกคาม (TA)	-	-	-	-	-	-	0.152**	-	0.152**	0.079	0.027	0.052
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	-	-	-	-	-	-	0.670**	-	0.670**	970**	0.119*	0.851**
แรงจูงใจในการป้องกัน (PM)	-	-	-	-	-	-	-	-	-	0.178*	-	0.178*
R^2	0.354			0.511			0.443			0.565		

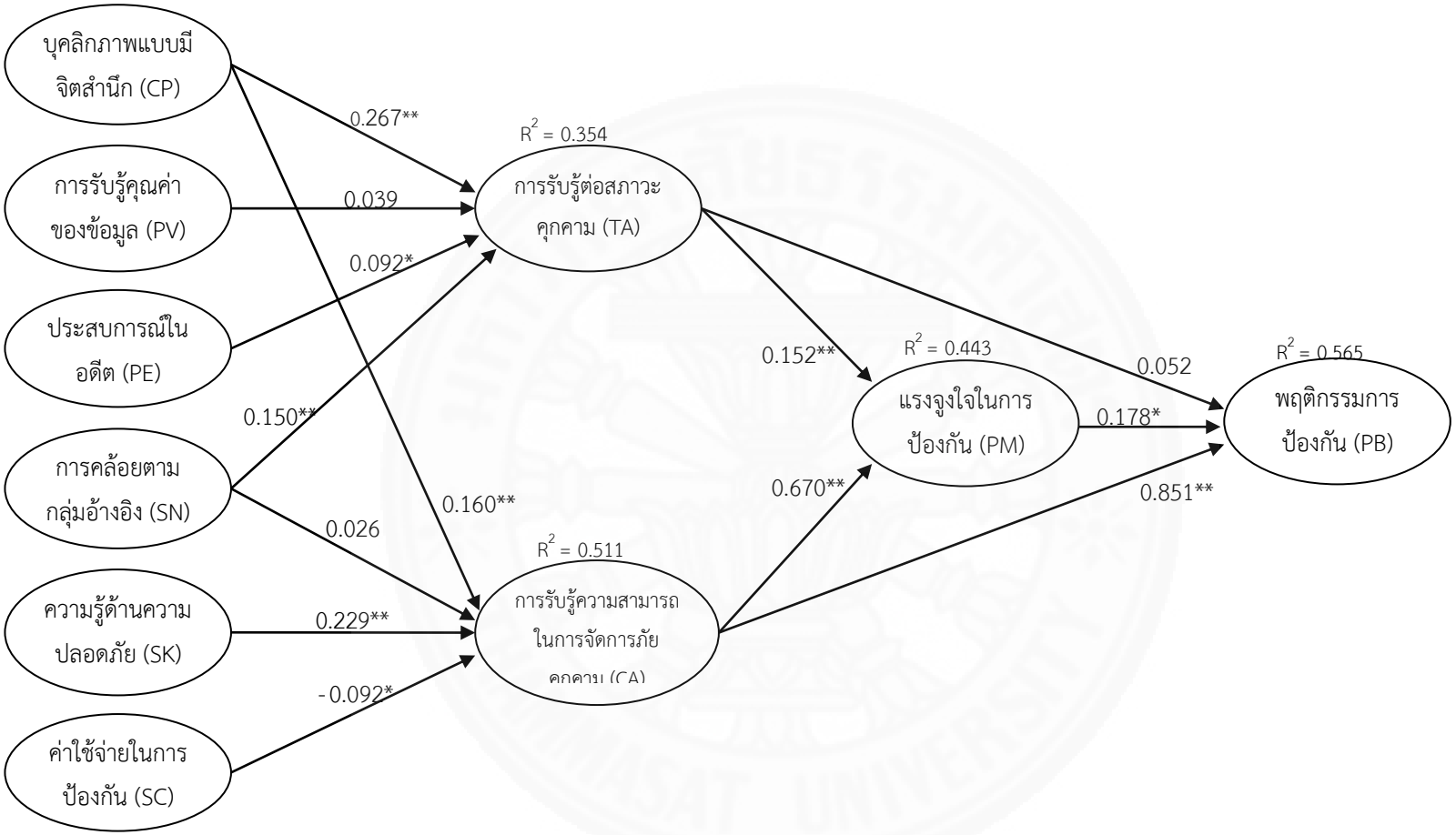
หมายเหตุ * หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.05 และ ** หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.01

ตารางที่ 4.14

ผลการวิเคราะห์แยกค่าอิทธิพลของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศแตกต่างกัน (ต่อ)

	กลุ่ม Non-IT People											
ตัวแปรผล / **ตัวแปรสาเหตุ**	การรับรู้ต่อสภาวะคุกคาม (TA)			การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)			แรงจูงใจในการป้องกัน (PM)			พฤติกรรมการป้องกัน (PB)		
	TE	IE	DE	TE	IE	DE	TE	IE	DE	TE	IE	DE
บุคลิกภาพแบบมีจิตสำนึก (CP)	0.240**	-	0.240**	0.086**	-	0.086**	0.107**	0.107**	-	0.118**	0.118**	-
การรับรู้คุณค่าของข้อมูล (PV)	0.105**	-	0.105**				0.027*	0.027*	-	0.008	0.008	-
ประสบการณ์ในอดีต (PE)	0.097*		0.097*				0.025*	0.025*	-	0.007	0.007	-
การคล้อยตามกลุ่มอ้างอิง (SN)	0.181**	-	0.181**	0.126**	-	0.126**	0.114**	0.114**	-	0.161**	0.161**	-
ความรู้ด้านความปลอดภัย (SK)	-	-	-	283**	-	283**	0.151**	0.151**	-	0.330**	0.330**	-
ค่าใช้จ่ายในการป้องกัน (SC)	-	-	-	0.022	-	0.022	-0.012	-0.012	-	-0.025	-0.025	-
การรับรู้ต่อสภาวะคุกคาม (TA)	-	-	-	-	-	-	0.257**	-	0.257**	0.075	0.059*	0.017
การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA)	-	-	-	-	-	-	0.535**	-	0.535**	10.166**	0.122**	10.044**
แรงจูงใจในการป้องกัน (PM)	-	-	-	-	-	-	-	-	-	0.229**	-	0.229**
R^2	0.380			0.561			0.393			0.697		

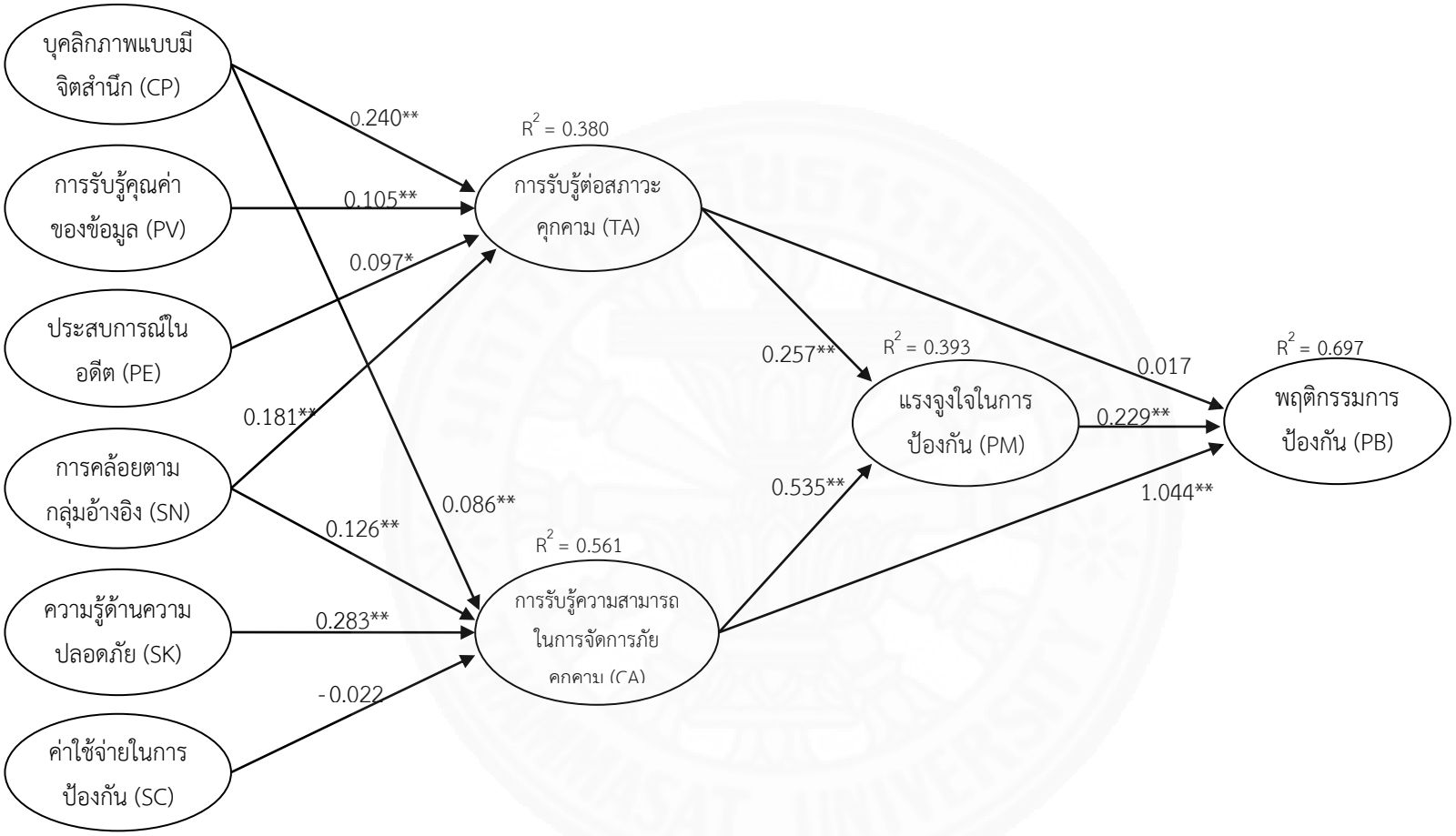
หมายเหตุ * หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.05 และ ** หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.01



หมายเหตุ * หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.05

** หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.01

ภาพที่ 4.3 โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People)



หมายเหตุ * หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.05

** หมายถึง มีนัยสำคัญทางสถิติที่ระดับ 0.01

ภาพที่ 4.4 โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People)

สำหรับการนำเสนอขนาดอิทธิพลของโมเดลสมการโครงสร้างกลุ่มพหุนี้ ผู้วิจัยได้นำเสนอขนาดอิทธิพลจำแนกตามทักษะด้านเทคโนโลยีสารสนเทศ คือผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ หรือ IT People และผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ หรือ Non-IT People ดังนี้

(1) ผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People)

เมื่อพิจารณาค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของสมการโครงสร้างตัวแปรภายในแฝงในแฝงพบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ (PB) มีค่าเท่ากับ 0.565 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 56.5 ตัวแปรแรงจูงใจในการป้องกัน (PM) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.443 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของแรงจูงใจในการป้องกันในการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 44.3 ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.354 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 35.4 และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.511 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้ความสามารถในการจัดการกับภัยคุกคามของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 51.1

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และตัวแปรแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.851 และ 0.178 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 ตามลำดับ

สำหรับอิทธิพลทางอ้อมที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ได้รับอิทธิพลทางอ้อมจากตัวแปรความรู้ด้านความปลอดภัย (SK) การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.222 0.119 และ 0.176 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 นอกจากนี้ ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางอ้อมพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) โดยมีขนาดอิทธิพลทางลบเท่ากับ 0.090 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

เมื่อพิจารณาอิทธิพลรวม พบว่า ตัวแปรที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) คือ ตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม

(CA) และตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.670 และ 0.152 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรความรู้ด้านความปลอดภัย (SK) ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.670 0.153 0.152 และ 0.148 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 นอกจากนี้ ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางตรงต่อแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลทางลบเท่ากับ 0.062 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

สำหรับอิทธิพลทางอ้อมที่มีผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ได้รับอิทธิพลทางอ้อมจากตัวแปรความรู้ด้านความปลอดภัย (SK) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.153 และ 0.148 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 นอกจากนี้ ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางอ้อมต่อแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลทางลบเท่ากับ 0.062 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

เมื่อพิจารณาอิทธิพลรวม พบว่า ตัวแปรที่มีผลต่อแรงจูงใจในการป้องกัน (PM) คือ ตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรความรู้ด้านความปลอดภัย (SK) ตัวแปรแรงจูงใจในการป้องกัน (PM) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.970 0.222 0.178 และ 0.176 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 นอกจากนี้ ตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ยังมีอิทธิพลทางตรงต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) โดยมีขนาดอิทธิพลทางลบเท่ากับ 0.090 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ต่อสภาวะคุกคาม (TA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และ ตัวแปรประสบการณ์ในอดีต (PE) โดยมีขนาดอิทธิพลเท่ากับ 0.267 0.150 และ 0.92 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 แสดงว่าบุคลิกภาพแบบมีจิตสำนึก ประสบการณ์ในอดีต และการคล้อยตามกลุ่มอ้างอิง มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยบุคลิกภาพแบบมีจิตสำนึกมีอิทธิพลสูงกว่าการคล้อยตามกลุ่มอ้างอิง และประสบการณ์ในอดีต ตามลำดับ สำหรับอิทธพลรวม พบว่าตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) มีขนาดอิทธิพลเท่ากับ 0.267 รองลงมาคือ ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และ ตัวแปรประสบการณ์ในอดีต (PE) มีขนาดอิทธิพลเท่ากับ 0.150 และ 0.92 ตามลำดับ

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรความรู้ด้านความปลอดภัย (SK) และตัวแปรค่าใช้จ่ายในการป้องกัน (SC) มีขนาดอิทธิพลเท่ากับ 0.160 0.229 และ 0.92 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยตัวแปรทุกตัวมีอิทธิพลทางบวกยกเว้นตัวแปรค่าใช้จ่ายในการป้องกัน (SC) ที่มีอิทธิพลทางลบต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) แสดงว่าบุคลิกภาพแบบมีจิตสำนึก ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการการรับรู้ความสามารถในการจัดการกับภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยความรู้ด้านความปลอดภัยมีอิทธิพลสูงกว่าบุคลิกภาพแบบมีจิตสำนึก และค่าใช้จ่ายในการป้องกันตามลำดับ สำหรับอิทธพลรวม พบว่า ตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรความรู้ด้านความปลอดภัย (SK) มีขนาดอิทธิพลเท่ากับ 0.229 รองลงมาคือ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) และตัวแปรค่าใช้จ่ายในการป้องกัน (SC) มีขนาดอิทธิพลเท่ากับ 0.160 และ 0.92 ตามลำดับ

(2) ผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People)

เมื่อพิจารณาค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของสมการโครงสร้างตัวแปรภายในแฝงในแฝงพบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ (PB) มีค่าเท่ากับ 0.697 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 69.7 ตัวแปรแรงจูงใจในการป้องกัน (PM) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.393 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของแรงจูงใจในการป้องกันในการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 39.3 ตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.380 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 38.0 และตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) มีค่าสัมประสิทธิ์การพยากรณ์ (R^2) เท่ากับ 0.561 แสดงว่าตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการรับรู้ความสามารถในการจัดการกับภัยคุกคามของผู้ใช้คอมพิวเตอร์ได้ร้อยละ 56.1

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรแรงจูงใจในการป้องกัน (PM) ตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) การคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรความรู้ด้านความปลอดภัย (SK) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.229 1.166 0.118 161 และ 0.330 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 สำหรับอิทธิพลทางอ้อมที่มีผลต่อพฤติกรรมการป้องกัน

อาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) พบว่า ได้รับอิทธิพลทางอ้อมจาก การรับรู้ต่อสภาวะคุกคาม (TA) การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) การคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรความรู้ด้านความปลอดภัย (SK) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.059 0.122 0.118 0.161 และ 0.330 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 เมื่อพิจารณาอิทธิพลรวม พบว่า ตัวแปรที่มีผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ (PB) คือ การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และตัวแปรแรงจูงใจในการป้องกัน (PM) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 1.044 และ 0.229 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 ตามลำดับ

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่มีผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) ตัวแปรการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรความรู้ด้านความปลอดภัย (SK) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.257 0.535 0.107 0.027 0.025 0.114 และ 0.151 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 สำหรับอิทธิพลทางอ้อมที่มีผลต่อแรงจูงใจในการป้องกัน (PM) พบว่า ได้รับอิทธิพลทางอ้อมจากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรความรู้ด้านความปลอดภัย (SK) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 107 0.027 0.025 0.114 และ 0.151 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 เมื่อพิจารณาอิทธิพลรวม พบว่า ตัวแปรที่มีผลต่อแรงจูงใจในการป้องกัน (PM) คือ การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) และตัวแปรการรับรู้ต่อสภาวะคุกคาม (TA) โดยมีขนาดอิทธิพลทางบวกเท่ากับ 0.535 และ 0.257 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ต่อสภาวะคุกคาม (TA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการรับรู้คุณค่าของข้อมูล (PV) ตัวแปรประสบการณ์ในอดีต (PE) และตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) โดยมีขนาดอิทธิพลเท่ากับ 0.240 0.105 0.097 และ 0.181 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และ 0.05 แสดงว่าบุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล ประสบการณ์ในอดีต และการคล้อยตามกลุ่มอ้างอิง มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการรับรู้สภาวะคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยบุคลิกภาพแบบมีจิตสำนึกมีอิทธิพลสูงกว่าการคล้อยตามกลุ่มอ้างอิงและการรับรู้คุณค่าของข้อมูล ตามลำดับ สำหรับอิทธพลรวม พบว่าตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) มีขนาดอิทธิพลเท่ากับ 0.240

รองลงมาคือ ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรการรับรู้คุณค่าของข้อมูล (PV) มีขนาดอิทธิพลเท่ากับ 0.181 และ 0.105 ตามลำดับ

เมื่อพิจารณาอิทธิพลทางตรงที่ส่งผลต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคาม (CA) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) ตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรความรู้ด้านความปลอดภัย (SK) มีขนาดอิทธิพลเท่ากับ 0.086 0.126 และ 0.283 ตามลำดับ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 แสดงว่าบุคลิกภาพแบบมีจิตสำนึก การคล้อยตามกลุ่มอ้างอิง และความรู้ด้านความปลอดภัย มีอิทธิพลที่ทำให้ผู้ใช้คอมพิวเตอร์เกิดการการรับรู้ความสามารถในการจัดการกับภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ โดยความรู้ด้านความปลอดภัยมีอิทธิพลสูงกว่าการคล้อยตามกลุ่มอ้างอิง และบุคลิกภาพแบบมีจิตสำนึกตามลำดับ สำหรับอิทธพลรวม พบว่า ตัวแปรที่มีอิทธิพลรวมสูงสุดต่อรับรู้ต่อสภาวะคุกคามคือ ตัวแปรความรู้ด้านความปลอดภัย (SK) มีขนาดอิทธิพลเท่ากับ 0.283 รองลงมาคือตัวแปรการคล้อยตามกลุ่มอ้างอิง (SN) และตัวแปรบุคลิกภาพแบบมีจิตสำนึก (CP) มีขนาดอิทธิพลเท่ากับ 0.126 และ 0.086 ตามลำดับ

จากผลการวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) และไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) พบว่า ปัจจัยที่มีขนาดอิทธิพลรวมสูงสุดคือการรับรู้ความสามารถในการจัดการกับภัยคุกคาม ซึ่งมีผลสอดคล้องกับผลการวิเคราะห์ของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์โดยภาพรวม

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

การวิจัยในครั้งนี้เป็นการศึกษาความสัมพันธ์เชิงสาเหตุโดยมีวัตถุประสงค์ในการวิจัย 3 ประการ ได้แก่ 1) เพื่อศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของบุคคลที่ใช้งานคอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน 2) เพื่อตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีความสอดคล้องกับข้อมูลเชิงประจักษ์ และ 3) เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ระหว่างกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ

ประชากรที่ศึกษาคือ ผู้ใช้คอมพิวเตอร์ส่วนบุคคลทั่วประเทศไทยทั้งที่มีการใช้งานที่บ้านและที่ทำงาน ซึ่งใช้หลักการสุ่มแบบ จำนวนกลุ่มตัวอย่างทั้งหมด 600 คน แบ่งเป็น ผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศจำนวน 300 คน และผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศจำนวน 300 คน ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลโดยการส่งแบบสอบถามไปยังหน่วยงานประชาสัมพันธ์ขององค์กรต่างๆ และผ่านทางเครือข่ายสังคมออนไลน์ ได้รับแบบสอบถามคืนกลับมาจำนวน 615 ฉบับ และหลังจากที่ตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลพบว่าแบบสอบถามที่ข้อมูลมีความสมบูรณ์มีจำนวนทั้งสิ้น 600 ฉบับ คิดเป็นร้อยละ 97.56

ตัวแปรที่ใช้ในการวิจัยครั้งนี้ ประกอบด้วย ตัวแปรแฝง 10 ตัว และตัวแปรสังเกตได้ 39 ตัว ซึ่งจำแนกเป็นตัวแปรแฝงภายใน 4 ตัว ได้แก่ 1) การรับรู้ต่อสภาวะคุกคาม 2) การรับรู้ความสามารถในการจัดการกับภัยคุกคาม 3) แรงจูงใจในการป้องกัน ซึ่งตัวแปรแฝงภายในแต่ละตัววัดจากตัวแปรสังเกตได้ 4 ตัว และ 4) พฤติกรรมการป้องกันการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ซึ่งวัดจากตัวแปรสังเกตได้ 3 ตัว ตัวแปรแฝงภายนอก 6 ตัว ได้แก่ 1) บุคลิกภาพแบบมีจิตสำนึก 2) การรับรู้คุณค่าของข้อมูล 3) ประสบการณ์ในอดีต 4) การคล้อยตามกลุ่มอ้างอิง 5) ความรู้ด้านความปลอดภัย และ 6) ค่าใช้จ่ายในการป้องกัน ซึ่งตัวแปรแฝงภายนอกแต่ละตัววัดจากตัวแปรสังเกตได้ 4 ตัว

เครื่องมือที่ใช้ในการวิจัยนี้ คือแบบสอบถามจำนวน 1 ชุด โดยแบบสอบถามแบ่งเป็น 3 ส่วน คือ ส่วนที่ 1 เป็นคำถามเกี่ยวกับการใช้คอมพิวเตอร์และความปลอดภัยคอมพิวเตอร์ ส่วนที่ 2 เป็นคำถามเกี่ยวกับข้อมูลภูมิหลัง และข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศอายุ ระดับการศึกษา ตำแหน่งงาน สาขาวิชาที่ศึกษา และส่วนที่ 3 เป็นคำถามเกี่ยวกับปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์

การวิเคราะห์ข้อมูลใช้สถิติเชิงบรรยายเพื่ออธิบายการแจกแจงของตัวแปรสังเกตได้ วิเคราะห์ความสัมพันธ์เพื่อคำนวณค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรสังเกตได้เพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรสังเกตได้แต่ละคู่ โดยใช้โปรแกรม SPSS for Windows version 16.0 ในการตรวจสอบความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของบุคคลที่ใช้งานคอมพิวเตอร์ที่พัฒนาขึ้นกับข้อมูลเชิงประจักษ์ และการทดสอบความไม่แปรเปลี่ยนของโมเดลระหว่างกลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ ด้วยการวิเคราะห์โมเดลสมการโครงสร้างกลุ่มพหุ โดยใช้โปรแกรม LISREL for Windows version 8.72

5.1 สรุปผลการวิจัย

ผู้วิจัยสรุปผลการวิจัยโดยมีลำดับการนำเสนอ ดังนี้

(1) การวิเคราะห์ข้อมูลเบื้องต้นเกี่ยวกับลักษณะพื้นฐานของกลุ่มตัวอย่าง พบว่ากลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง มีอายุอยู่ในช่วง 25 ถึง 34 ปี มีการศึกษาในระดับปริญญาตรี และมีอายุการทำงาน 5 ถึง 10 ปี จำแนกเป็นผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศอย่างละเท่ากัน

ผลการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกตได้ พบว่า ตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด กลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ และกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ ส่วนใหญ่มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ขนาดของความสัมพันธ์ส่วนใหญ่อยู่ในระดับปานกลาง ($0.3<r<0.7$) ทิศทางของความสัมพันธ์ส่วนใหญ่มีทิศทางเดียวกัน เมื่อทดสอบสมมติฐานของเมทริกซ์สหสัมพันธ์ของตัวแปรสังเกตได้ของกลุ่มตัวอย่างทั้งหมด กลุ่มผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศ และกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศว่ามีความแตกต่างจากเมทริกซ์เอกลักษณ์หรือไม่ (Bartlett's Test of Sphericity) พบว่ามีความแตกต่างจากเมทริกซ์เอกลักษณ์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 และสอดคล้องกับผลการวิเคราะห์ค่าดัชนี Kaiser-Meyer-Olkin ซึ่งมีค่าเข้าใกล้ 1 นั้นคือ ตัวแปรสังเกตได้ทั้งหมดมีความสัมพันธ์กันและเหมาะสมที่จะนำไปใช้ในการพัฒนาโมเดลเชิงสาเหตุพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์และใช้ในการวิเคราะห์กลุ่มพหุต่อไป

(2) การตรวจสอบความตรงเชิงโครงสร้างของตัวแปรหลักในการวิจัย พบว่ามีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ พิจารณาจากค่าไค-สแควร์ มีค่าแตกต่างจากศูนย์อย่างไม่มี

นัยสำคัญทางสถิติ (Chi-square = 173.47, df = 642) โดยมีค่าดัชนีวัดระดับความกลมกลืน (GFI) มีค่าเป็น 0.871 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) มีค่าเป็น 0.843 และดัชนีรากของค่าเฉลี่ยกำลังสองของส่วนเหลือ (RMR) มีค่าเป็น 0.024 แสดงว่า มีความกลมกลืนระหว่างข้อมูลเชิงประจักษ์กับโมเดลโครงสร้าง

(3) ผลการวิเคราะห์ความสอดคล้องของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์โดยภาพรวมกับข้อมูลเชิงประจักษ์ พบว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยให้ค่าดัชนีความสอดคล้องระหว่างโมเดลตามกรอบแนวคิดกับข้อมูลเชิงประจักษ์ในรูปของค่าไค-สแควร์เท่ากับ 1241.338 ที่องศาอิสระ 628 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.904 และดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.881 ค่าดัชนีกำลังสองของเศษเหลือ (RMR) เท่ากับ 0.030 โดยที่ตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์โดยภาพรวมได้ร้อยละ 67.2

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ พบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้รับอิทธิพลทางตรงจากการรับรู้ความสามารถในการจัดการภัยคุกคามมากที่สุดอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยขนาดอิทธิพลมีค่าเท่ากับ 0.769 รองลงมาคือความรู้ด้านความปลอดภัย บุคลิกภาพแบบมีจิตสำนึก แรงจูงใจในการป้องกัน การคล้อยตามกลุ่มอ้างอิง การรับรู้คุณค่าของข้อมูล (PV) การรับรู้ต่อสภาวะคุกคามค่าใช้จ่ายในการป้องกันและได้รับอิทธิพลจากประสบการณ์ในอดีตน้อยที่สุด โดยมีขนาดอิทธิพลเท่ากับ 0.372 0.185 0.180 0.134 0.110 0.094 0.080 และ 0.014 ตามลำดับ

(4) ผลการวิเคราะห์เพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ พบว่า มีความไม่แปรเปลี่ยนของรูปแบบโมเดล และมีความไม่แปรเปลี่ยนของค่าพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายนอกแฝงไปตัวแปรภายในแฝง และค่าพารามิเตอร์เมทริกซ์อิทธิพลเชิงสาเหตุจากตัวแปรภายในแฝง สำหรับโมเดลที่ไม่มีเงื่อนไขกำหนดให้พารามิเตอร์ของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีค่าเท่ากันระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ ให้ค่าดัชนีความสอดคล้องระหว่างโมเดลตามกรอบแนวคิดกับข้อมูลเชิงประจักษ์ในรูปของค่าไค-สแควร์เท่ากับ 2154.83 ที่องศาอิสระ 1298 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.845 ค่าดัชนีกำลังสองของเศษเหลือ (RMR) เท่ากับ 0.039 โดยที่ตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของพฤติกรรมการป้องกันอาชญากรรม

คอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศได้ร้อยละ 56.5 และ 69.7 ตามลำดับ โดยพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ที่มีทักษะด้านเทคโนโลยีสารสนเทศและผู้ใช้คอมพิวเตอร์ที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศเป็นผลมาจากการรับรู้ความสามารถในการจัดการภัยคุกคามมากที่สุดเช่นเดียวกัน

5.2 การอภิปรายผล

จากสรุปผลการวิจัยที่นำเสนอข้างต้นแล้วนั้น จะเห็นได้ว่าโมเดลมีความสอดคล้องกับกรอบแนวคิดและสมมติฐานงานวิจัย โดยสามารถอภิปรายผลการวิจัยจำแนกเป็นรายข้อ ดังนี้

5.2.1 ความสัมพันธ์เชิงสาเหตุระหว่างตัวแปรในโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์โดยภาพรวม

จากผลการวิเคราะห์ความสัมพันธ์เชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์โดยภาพรวม พบว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้รับอิทธิพลทางตรงจากแรงจูงใจในการป้องกัน และได้รับอิทธิพลทั้งโดยทางตรงและทางอ้อมจากการรับรู้ต่อสภาวะคุกคามและการรับรู้ความสามารถในการจัดการกับภัยคุกคาม ซึ่งสอดคล้องกับสมมติฐานการวิจัย

พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ได้รับอิทธิพลทั้งโดยทางตรงและทางอ้อมเป็นบวกมากที่สุดจากปัจจัยการรับรู้ความสามารถในการจัดการกับภัยคุกคาม แสดงว่าการรับรู้ความสามารถในการจัดการกับภัยคุกคามเป็นปัจจัยที่มีความสำคัญต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ หากผู้ใช้คอมพิวเตอร์มีความเชื่อมั่นในประสิทธิภาพของมาตรการที่นำมาใช้ในการป้องกันอาชญากรรมคอมพิวเตอร์ มีความเชื่อมั่นในทักษะและความสามารถในการป้องกันอาชญากรรมคอมพิวเตอร์ของตนเองแล้ว ผู้ใช้คอมพิวเตอร์ก็จะแสดงพฤติกรรมในการป้องกันอาชญากรรมคอมพิวเตอร์ได้

โดยปัจจัยการรับรู้ความสามารถในการจัดการกับภัยคุกคามได้รับอิทธิพลทางตรงเชิงบวกสูงที่สุดจากปัจจัยความรู้ด้านความปลอดภัย แสดงว่า การได้รับความรู้ด้านความปลอดภัย ไม่ว่าจะเป็นการฝึกอบรม การสื่อสารผ่านสื่อต่างๆ เช่น หนังสือพิมพ์ อินเทอร์เน็ต โทรทัศน์ เป็นต้น หรือแม้แต่การพูดคุยกับบุคคลรอบตัวเกี่ยวกับวิธีการใช้งานคอมพิวเตอร์อย่างปลอดภัยและการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์มากขึ้น จะทำให้เกิดความเชื่อมั่นในตนเองและมาตรการหรือวิธีการที่จะนำมาใช้ในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์มากขึ้นตามไปด้วย ซึ่งสอดคล้อง

กับหลายงานวิจัยในอดีตที่พบว่า การให้ความรู้เกี่ยวกับการใช้งานคอมพิวเตอร์อย่างปลอดภัยมีอิทธิพลทำให้ผู้ใช้คอมพิวเตอร์เกิดการรับรู้ความสามารถในการจัดการกับภัยคุกคามนั้นเพิ่มมากขึ้น

ปัจจัยบุคลิกภาพแบบมีจิตสำนึก เป็นปัจจัยที่อิทธิพลทางตรงเชิงบวกต่อการรับรู้ความสามารถในการจัดการกับภัยคุกคามสูงเป็นอันดับที่สอง แสดงว่า ผู้ใช้คอมพิวเตอร์ที่มีบุคลิกภาพแบบมีจิตสำนึก จะรับรู้ความสามารถของตนเอง และมีความเชื่อมั่นต่อประสิทธิภาพในการป้องกันภัย ซึ่งสอดคล้องกับงานวิจัยในอดีตของ Shropshire และคณะ (2006) ที่พบว่าบุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) มีความสัมพันธ์อย่างยิ่งกับการที่พนักงานภายในองค์กรรับรู้ความสามารถที่จะจัดการกับภัยคุกคามโดยการนำเทคโนโลยีมาใช้ป้องกันภัยตามนโยบายขององค์กร

5.3 ข้อเสนอแนะ

การนำเสนอในตอนนี้ผู้วิจัยนำเสนอโดยแน่งเป็น 2 ส่วนคือ ส่วนแรก เป็นการนำเสนอข้อเสนอแนะในการนำผลการวิจัยไปใช้ และ ส่วนที่สอง เป็นข้อเสนอแนะในการทำวิจัยครั้งต่อไป โดยมีรายละเอียดดังนี้

5.3.1 ข้อเสนอแนะในการนำผลการวิจัยไปใช้

จากจากพัฒนาโมเดลเชิงสาเหตุพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของบุคคลที่ใช้งานคอมพิวเตอร์ พบว่า ตัวแปรปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน มีอิทธิพลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ โดยส่งผ่านการรับรู้ต่อสภาวะคุกคาม การรับรู้ความสามารถในการจัดการกับภัยคุกคาม และ แรงจูงใจในการป้องกัน อย่างมีนัยสำคัญทางสถิติทุกตัวแปร ผู้วิจัยจึงขอนำเสนอการนำผลการวิจัยไปใช้ในการพัฒนาหรือสร้างเสริมพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ โดยนำเสนอตามลำดับการใช้ประโยชน์ของบุลคล/หน่วยงาน ดังนี้

1. **ผู้ใช้คอมพิวเตอร์** จากข้อค้นพบของการพัฒนาโมลเดล บ่งชี้ว่า พฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ได้รับอิทธิพลจากปัจจัยส่วนบุคคลและปัจจัยด้านสภาพแวดล้อม โดยความรู้ด้านความปลอดภัยเกี่ยวกับการใช้งานคอมพิวเตอร์ เป็นปัจจัยที่ส่งอิทธิพลมากที่สุด ผู้ใช้คอมพิวเตอร์ควรหมั่นศึกษาและติดตามข้อมูลข่าวสารต่างๆ เกี่ยวกับการใช้งานคอมพิวเตอร์อย่างปลอดภัย รวมทั้งภัยคุกคามต่างๆ ที่เกิดขึ้นกับผู้ใช้คอมพิวเตอร์อย่างสม่ำเสมอ

เพื่อให้ผู้ใช้คอมพิวเตอร์เกิดการเรียนรู้ที่จะป้องกันตนเองจากการถูกคุกคาม และรับรู้ว่าอาชญากรรมคอมพิวเตอร์เป็นเรื่องใกล้ตัว ที่สามารถเกิดขึ้นได้กับทุกคน

2. **ผู้ปกครอง และเพื่อน** จากข้อค้นพบของการพัฒนาโมลเดล บ่งชี้ว่า การคล้อยตามกลุ่มอ้างอิง เป็นอีกหนึ่งปัจจัยที่มีความสำคัญต่อการการรับรู้สภาวะคุกคามและนำไปสู่การแสดงพฤติกรรมในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์เช่นเดียวกัน บุคคลใกล้ชิด ไม่ว่าจะเป็น พ่อแม่ ผู้ปกครอง คนในครอบครัว หรือเพื่อน ควรแสดงให้เห็นหรือให้คำแนะนำเกี่ยวกับวิธีการป้องกันอาชญากรรมพิวเตอร์ เพื่อให้บุคคลอื่นเกิดการตระหนักว่าอาชญากรรมคอมพิวเตอร์เป็นเรื่องใกล้ตัว และเกิดการเรียนรู้ที่จะปฏิบัติตาม

3. **หน่วยงานที่เกี่ยวข้อง** ควรนำข้อค้นพบไปเป็นแนวทางในการพัฒนาและส่งเสริมให้เกิดพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ โดยเน้นการให้ความรู้แก่ผู้ใช้คอมพิวเตอร์เกี่ยวกับการใช้คอมพิวเตอร์อย่างปลอดภัย รูปแบบของอาชญากรรมคอมพิวเตอร์และวิธีการป้องกัน รวมไปถึงสถิติการเกิดอาชญากรรมคอมพิวเตอร์ เผยแพร่ข้อมูลข่าวสารต่างๆ ที่แสดงให้เห็นถึงความเสียหายและความรุนแรงจากการถูกคุกคามจากอาชญากรรมคอมพิวเตอร์ ผ่านช่องทางต่างๆ ที่หลากหลาย เพื่อให้ผู้ใช้คอมพิวเตอร์สามารถเข้าถึงและรับรู้ได้โดยง่าย เพื่อให้ผู้ใช้คอมพิวเตอร์เกิดความตระหนักถึงความเสี่ยงและความเสียหายจากการถูกคุกคาม รวมทั้งรับรู้ความสามารถในการจัดการกับภัยคุกคามนั้น ซึ่งจะทำให้เกิดแรงจูงใจและนำไปสู่การแสดงพฤติกรรมในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์

5.3.2 ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. งานวิจัยนี้มุ่งเน้นที่จะศึกษาถึงปัจจัยที่จะส่งผลต่อพฤติกรรมในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ โดยเลือกปัจจัยที่มีความสำคัญจากงานวิจัยในอดีตและยังมีการศึกษาจำนวนไม่มาก ผู้วิจัยเห็นว่ายังมีปัจจัยบางอย่างที่ยังไม่ได้ศึกษาในงานวิจัยนี้ เช่น ผลตอบแทนหรือรางวัลที่จะได้รับ เป็นต้น

2. งานวิจัยนี้ ผู้วิจัยได้รวมผู้ใช้คอมพิวเตอร์ทั้งที่ใช้งานที่บ้านและที่ทำงานเป็นกลุ่มตัวอย่างเดียวกัน ซึ่งอาจจะมีความแตกต่างกันในเรื่องสภาพแวดล้อม การได้รับข้อมูลด้านเทคโนโลยีสรสนเทศ หรืออยู่ภายใต้กฎระบียบที่ไม่แหมือนกัน ซึ่งอาจส่งผลต่อการรับรู้และแสดงพฤติกรรมที่แตกต่างเช่นกัน ดังนั้นในอนาคต จึงอาจมีการจัดกลุ่มโดยให้สภาพแวดล้อมมีความใกล้เคียงกัน

3. งานวิจัยนี้ มุ่งเน้นเฉพาะผู้ใช้คอมพิวเตอร์ส่วนบุคคลที่เป็นแบบตั้งโต๊ะและพกพา แต่เนื่องจากในปัจจุบันมีการใช้งาน Tablet และ Smart phone กันเป็นจำนวนมากและมีแนวโน้มเพิ่มมากขึ้นอย่างต่อเนื่อง วัตถุประสงค์ของการใช้งานอาจแตกต่างจากการใช้คอมพิวเตอร์ส่วนบุคคล ซึ่งข้อมูลเกี่ยวกับการทำธุรกรรมทางการเงินหรือข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลหรือ

การทำธุรกรรมทางการเงิน อาจถูกจัดเก็บไว้บนอุปกรณ์เหล่านี้ เพื่อความสะดวกในการใช้งาน จึงมีความเสี่ยงที่จะถูกคุกคามจากอาชญากรรมคอมพิวเตอร์หรือที่เรียกว่า Cyber crime เช่นกัน ดังนั้น การศึกษาพฤติกรรมการป้องกันภัยที่จะเกิดกับการใช้งาน Tablet และ Smart phone จึงเป็นสิ่งที่ควรให้ความสำคัญในอนาคต

รายการอ้างอิง

หนังสือและบทความในหนังสือ

กัลยา วินิชย์บัญชา. (2546). การวิเคราะห์สถิติ: *สถิติสำหรับการบริหารและวิจัย.* กรุงเทพมหานครฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

บทความวารสาร

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักกำกับการใช้เทคโนโลยีสารสนเทศ (Cartographer). (2551). *คู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์*. Retrieved from www.mwit.ac.th/~cs/download/tech30102/handbook.pdf

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานสถิติแห่งชาติ. (2554a). สรุปผลที่สำคัญสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2553.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานสถิติแห่งชาติ. (2554b). สรุปผลที่สำคัญสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในสถานประกอบการ พ.ศ. 2553.

Books and Book Articles

Halder, Debarati, Jaishankar, Karuppannan, & Jaishankar, K. (2012). *Cyber crime and the victimization of women: laws, rights and regulations*: Information Science Reference.

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation*.

Shelly, G., & Vermaat, M. (2010). *Discovering Computers 2011: Complete*: Cengage Learning.

Articles

Ajzen, Icek. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi: 10.1016/0749-5978(91)90020-T

Anderson, Catherine L., & Agarwal, Ritu. (2010). *Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions*. *MIS Quarterly, 34*(3), 613-643.

Bulgurcu, Burcu, Cavusoglu, Hasan, & Benbasat, Izak. (2009). *Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance*. http://aisel.aisnet.org/amcis2009/419

Bulgurcu, Burcu, Cavusoglu, Hasan, & Benbasat, Izak. (2010). *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. *MIS Quarterly, 34*(3), 523-548.

Chai, Sangmi, Bagchi-Sen, Sharmistha, Morrell, Claudia, Rao, H Raghav, & Upadhyaya, Andshambhu J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *Professional Communication, IEEE Transactions on, 52*(2), 167-182.

Chai, Sangmi, Sharmistha, Bagchi-Sen, Claudia, Morrell, R., Rao H., & J., Upadhyaya Shambhu. (2009). Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182.

Chenoweth, Tim, Minch, Robert P., & Gattiker, Tom. (2009). *Application of Protection Motivation Theory to Adoption of Protective Technologies*. http://dx.doi.org/10.1109/HICSS.2009.74 http://doi.ieeecomputersociety.org/10.1109/HICSS.2009.587

Cronan, Timothy Paul, Foltz, C. Bryan, & Jones, Thomas W. (2006). *Piracy, computer crime, and IS misuse at the university*. *Communications of The ACM, 49*(6), 84-90. doi: 10.1145/1132472

CSI. (2011). *15th annual 2010/2011 Computer Crime and Security Survey*.

D'Arcy, John, Hovav, Anat, & Galletta, Dennis F. (2009). *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach*. *Information Systems Research, 20*(1), 79-98. doi: 10.1287/isre.1070.0160

Diamantopoulos, A, & Siguaw, JA. (2000). *Introducing LISREL: A Guide for the Uninitiated*: London: Sage Publication.

Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William, & Richardson, Robert. (2006). *2006 CSI/FBI computer crime and security survey*.

Halder, Debarati, Jaishankar, Karuppannan, & Jaishankar, K. (2012). *Cyber crime and the victimization of women: laws, rights and regulations*: Information Science Reference.

Herath, Tejaswini, & Rao, H. Raghav. (2009). *Protection motivation and deterrence: a framework for security policy compliance in organisations*. *EJIS, 18*(2), 106-125. doi: 10.1057/ejis.2009.6

Ifinedo, Princely. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers&Security, ScienceDirect, 31*(1), 83-95.

Ifinedo, Princely. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*. *Computers & Security, 31*(1), 83-95. doi: 10.1016/j.cose.2011.10.007

Johnston, Allen C., & Warkentin, Merrill. (2010). *Fear Appeals and Information Security Behaviors: An Empirical Study*. *MIS Quarterly, 34*(3), 549-566.

Kirsch, Laurie J., & Boss, Scott R. (2007). *The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines*. http://aisel.aisnet.org/icis2007/103

Kshetri, Nir. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Quarterly, 31*(7), 1057-1079. doi: 10.1080/01436597.2010.518752

LaRose, Robert, Rifon, Nora J., & Enbody, Richard J. (2008). *Promoting personal responsibility for internet safety*. *Communications of The ACM, 51*(3), 71-76. doi: 10.1145/1325555.1325569

LaRose, Robert, Rifon, Nora, Liu, Sunny, & Lee, Doohwang. (2005). Understanding online safety behavior: A multivariate model. *The 55th Annual Conference of the International Communication Association, New York City*.

Lee, Younghwa, & Larsen, Kai R. T. (2009). *Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software*. *EJIS, 18*(2), 177-187. doi: 10.1057/ejis.2009.11

Li, Ying, & Siponen, Mikko T. (2011). *A Call For Research On Home Users' Information Security Behaviour*. http://aisel.aisnet.org/pacis2011/112

Liang, Huigang, & Xue, Yajiong. (2010). *Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*. *J. AIS, 11*(7).

Liang, Huigang, & Xue, Yajiong (Lucky). (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7).

Lu, Chi-Chao, & Jen, Wen-Yuan. (2010). *A Historical Review of Computer User's Illegal Behavior Based on Containment Theory*. *JSW, 5*(6), 593-599. doi: 10.4304/jsw.5.6.593-599

Malimage, Kalana, & Warkentin, Merrill. (2011). *Influence of Perceived Value of Data on Anti-Virus Software Usage: An Empirical Study of Protection Motivation*. *IFIP Dewald Roode Workshop on Information Security*.

McCrae, R., & Costa, P. (2004). A contemplated revision of the NEO Five-Factor Inventory. *Personality and Individual Differences, 36*(3), 587-596. doi: citeulike-article-id:2485386

doi: 10.1016/s0191-8869(03)00118-1

McCrae, R. R., & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology, 52*(81-90).

McCrae, Robert R., & Costa, Paul T. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology, 52*(1), 81-90. doi: 10.1037//0022-3514.52.1.81

Moody, Daniel L., & Walsh, Peter. (1999). *Measuring the Value Of Information - An Asset Valuation Approach*. http://is2.lse.ac.uk/asp/aspecis/19990068.pdf

Ng, Boon-Yuen, Kankanhalli, Atreyi, & Xu, Yunjie Calvin. (2009). *Studying users' computer security behavior: A health belief perspective*. *Decision Support Systems, 46*(4), 815-825. doi: 10.1016/j.dss.2008.11.010

Pahnila, Seppo, Siponen, Mikko T., & Mahmood, M. Adam. (2007). *Employees' Behavior towards IS Security Policy Compliance*. http://dx.doi.org/10.1109/HICSS.2007.206 http://doi.ieeecomputersociety.org/10.1109/HICSS.2007.206

Parker, Donn B. (2007). *The Dark Side of Computing: SRI International and the Study of Computer Crime*. *IEEE Annals of the History of Computing, 29*(1), 3-15. doi: 10.1109/MAHC.2007.15

Reynaldo, J., & Santos, A. (1999). Cronbach's Alpha: A Tool for Assessing the Reliability of Scales. *Extension Information Technology, 37*(2). doi: citeulike-article-id:4432101

Rhee, Hyeun-Suk, Kim, Cheong-Tag, & Ryu, Young U. (2009). *Self-efficacy in information security: Its influence on end users' information security practice behavior*. *Computers & Security, 28*(8), 816-826. doi: 10.1016/j.cose.2009.05.008

Rhee, Hyeun-Suk, Kim, Cheongtag, & Ryu, Young U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, ScienceDirect, 28*(8), 816-826.

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation*.

Rogers, Ronald W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93-114. doi: 10.1080/00223980.1975.9915803

Shelly, G., & Vermaat, M. (2010). *Discovering Computers 2011: Complete*: Cengage Learning.

Shropshire, Jordan, Warkentin, Merrill, Johnston, Allen C., & Schmidt, Mark B. (2006). *Personality and IT security: An application of the five-factor model*. http://aisel.aisnet.org/amcis2006/415

Siponen, Mikko, Pahnila, Seppo, & Mahmood, Adam. (2006). *Factors Influencing Protection Motivation and IS Security Policy Compliance*. Paper presented at the International Conference on Innovations in Information Technology.

Siponen, Mikko T., Pahnila, Seppo, & Mahmood, M. Adam. (2010). *Compliance with Information Security Policies: An Empirical Investigation*. *IEEE Computer, 43*(2), 64-71. doi: 10.1109/MC.2010.35

Vance, A, Siponen, M, & Pahnila, S. (2009). How personality and habit affect protection motivation. *Workshop on Information Security and Privacy (WISP 2009)*, 14e21.

Warkentin, Merrill, Carter, Lemuria, & McBride, M. (2011). Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies. *The 2011 Dewald Roode Workshop on Information Systems Security Research*.

Warkentin, Merrill, & Willison, Robert. (2009). *Behavioral and policy issues in information systems security: the insider threat*. *EJIS, 18*(2), 101-105. doi: 10.1057/ejis.2009.12

Woon, Irene, Tan, Gek-Woo, & Low, R. (2005). *A Protection Motivation Theory Approach to Home Wireless Security*. http://aisel.aisnet.org/icis2005/31

Workman, Michael, Bommer, William H., & Straub, Detmar W. (2008). *Security lapses and the omission of information security measures: A threat control model and empirical test*. *Computers in Human Behavior, 24*(6), 2799-2816. doi: 10.1016/j.chb.2008.04.005

Zhang, Jie, Reithel, Brian J, & Li, Han. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

ภาคผนวก

ภาคผนวก ก
อาชญากรรมคอมพิวเตอร์ (Computer Crime)

อาชญากรรมคอมพิวเตอร์สามารถแบ่งได้เป็น 5 ประเภท ดังมีรายละเอียดดังนี้

(1) การโจมตีจากโปรแกรมที่มุ่งร้ายต่อระบบคอมพิวเตอร์

โปรแกรมที่มุ่งร้ายต่อระบบคอมพิวเตอร์ (Malicious Software) หรือเรียกสั้นๆ ว่า Malware ไม่ว่าจะเป็นไวรัสคอมพิวเตอร์ (Computer viruses) หนอน (Worms) โทรจัน (Trojan Hourse) นั้นล้วนแต่เป็นภัยคุกคามที่สำคัญอย่างยิ่งต่อเครื่องคอมพิวเตอร์ที่ไม่มีการป้องกันอย่างเหมาะสม เนื่องจาก Malware เป็นโปรแกรมคอมพิวเตอร์ที่พัฒนาขึ้นมาเพื่อก่อกวน/ทำลายระบบคอมพิวเตอร์ไม่ว่าจะเป็นข้อมูลชุดคำสั่ง หรืออุปกรณ์ต่างๆ และสามารถกระจายตัวได้โดยผ่านระบบเครือข่ายข้อมูล โดยทั่วไปโปรแกรมประเภทนี้ก่อให้เกิดความเสียหาย แต่ก็มีหลายชนิดที่ไม่ก่อให้เกิดความเสียหาย เพียงแต่ก่อให้เกิดความรำคาญเท่านั้น บางชนิดจะมีการตั้งเวลาให้ทำงานเฉพาะตามเงื่อนไข เช่น เมื่อถึงวันที่ที่กำหนดหรือเมื่อทำการขยายตัวได้ถึงระดับหนึ่ง ซึ่งเรียกว่าบอมบ์ (bomb) ข้อเสียอีกประการหนึ่งคือโปแกรมประเภทนี้จะบริโภคทรัพยากรคอมพิวเตอร์อย่างไร้ประโยชน์ หรืออาจบริโภคไปเป็นจำนวนมากจนทำให้เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ตามปกติ จากรายงาน Computer Crime and Security Survey ประจำปี 2010 ของประเทศสหรัฐอเมริกา พบว่าภัย Malware มีอัตราการเกิดสูงถึงร้อยละ 67.1 และเพิ่มสูงขึ้นอย่างต่อเนื่อง

ด้วยเหตุนี้บริษัทส่วนใหญ่จึงแต่งตั้งหรือมอบหมายเจ้าหน้าที่เพื่อรับผิดชอบในการป้องกันความเสี่ยงจากการถูกโจมตีโดยเฉพาะ นอกจากนี้ผู้ใช้คอมพิวเตอร์เองยังต้องให้ความสนใจและใส่ใจในการป้องกันภัยร่วมด้วย สำหรับวิธีการป้องกันภัยจากโปรแกรมที่มุ่งร้ายต่อระบบคอมพิวเตอร์ (Malicious Software) สามารถทำได้ดังนี้

- ใช้โปรแกรมตรวจจับและกำจัดไวรัส (anti-virus) ตรวจสอบเอกสารที่ download มาจากอินเทอร์เน็ต เอกสารบนอุปกรณ์ที่สามารถถอดหรือต่อพ่วงกับเครื่องได้ (Removable media devices) เช่น แผ่น CD หรือ Thumb drive เป็นต้น รวมทั้งเอกสารหรือโปรแกรมที่แนบมากับอีเมลก่อนที่จะเปิดอ่านหรือเก็บลงบนเครื่องคอมพิวเตอร์
- ควรติดตั้งโปรแกรมปรับปรุงระบบ (Patch) และมีการอัพเดทโปรแกรมที่ใช้ตรวจจับและกำจัดไวรัสอย่างสม่ำเสมอเพื่อให้ครอบคลุมถึงไวรัสชนิดใหม่ๆ หรือติดตั้งโปรแกรมตรวจจับและกำจัดไวรัส (anti-virus) มากกว่าหนึ่งชนิด เนื่องจากไม่มีโปรแกรมตรวจจับและกำจัดไวรัสใดสมบูรณ์แบบ

- เก็บเอกสารในรูปของ ASCII Text Mode หรือ Rich Text Format (RTF) โดยเฉพาะเอกสารที่ใช้ร่วมกันบนเครือข่าย

- ทำการสำรองข้อมูลและโปรแกรมบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ และไม่ควรเก็บข้อมูลสำรองไว้ในสถานที่เดียวกัน

(2) การโจมตีเครื่องคอมพิวเตอร์ผ่านเครือข่าย

การโจมตีเครื่องคอมพิวเตอร์ผ่านเครือข่ายจนไม่สามารถให้บริการได้หรือทำการยึดเครื่องคอมพิวเตอร์ เพื่อนำไปใช้ในการก่อเหตุอื่นๆ ภัยจากการคุกคามประเภทนี้มีด้วยกันหลายวิธี ยกตัวอย่างเช่น

- Botnets เป็นการโจมตีเครื่องคอมพิวเตอร์ที่กำลังออนไลน์กับระบบอินเทอร์เน็ตความเร็วสูง เช่น Cable Modem หรือ ADSL ที่ไม่มีการป้องกันเครื่องคอมพิวเตอร์อย่างปลอดภัยเพียงพอ ทำให้กลุ่มอาชญากรคอมพิวเตอร์สามารถยึดเครื่องเหล่านั้นและใช้เป็นเครื่องมือในการส่งสแปมเมล์หรือโปรแกรมโฆษณา (ADWARE) ไปยังคอมพิวเตอร์เครื่องอื่นๆ โดยเครื่องที่ถูกยึดนั้นเรียกว่า BOT หรือ Zombie หากยึดได้หลายเครื่องพร้อมกันเรียกว่า BOTNET หรือ RoBOT NETwork

- DoS Attack (Denial of Service) หมายถึงการขัดขวางหรือก่อกวนระบบเครือข่ายและเซิร์ฟเวอร์ จนทำให้ไม่สามารถให้บริการได้ตามปกติ ซึ่งการโจมตีด้วยวิธีการนี้โดยทั่วไปจะกระทำโดยการใช้ทรัพยากรของเซิร์ฟเวอร์ไปจนหมด ยกตัวอย่างเช่น การส่ง Packet TCP/SYN เข้าไปหาเครื่องเป้าหมายโดยใช้ IP address ที่ไม่มีอยู่จริงในการติดต่อ ทำให้เครื่องเป้าหมายนั้นต้องสำรองทรัพยากรไว้ส่วนหนึ่งเพื่อรองรับการเชื่อมต่อที่กำลังจะเกิดขึ้น เมื่อมีการเชื่อมต่อในรูปแบบนี้เข้ามามากเรื่อยๆ จะทำให้เครื่องเป้าหมายนั้นเกิดการใช้ทรัพยากรไปจนกระทั่งหมดและยุติการให้บริการในที่สุด

- Back doors เป็นโปรแกรมที่ทำหน้าที่เปิดทางให้ผู้ไม่ประสงค์ดี สามารถใช้โปรแกรมควบคุมเครื่องคอมพิวเตอร์ระยะไกล (Remote Desktop) เพื่อเข้าถึงเครื่องคอมพิวเตอร์ได้ ส่วนใหญ่แล้วจะมากับการติดตั้งแอพพลิเคชันหรือโปรแกรมที่ผิดกฎหมายของผู้ใช้งานโดยรู้เท่าไม่ถึงการณ์

- Spoofing ไม่ใช่ไวรัสคอมพิวเตอร์ แต่เป็นอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่งที่กำลังเป็นที่พบเห็นได้มากขึ้นเรื่อยๆ ในปัจจุบัน ซึ่งเป็นการปลอมแปลงอีเมล (E-mail Spoofing) และทำการสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนกับเว็บไซต์ของจริงและมี Address ใกล้เคียงกับเว็บไซต์จริง เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงิน หรือข้อมูล

ส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ

โปรแกรมแอนตี้ไวรัสรุ่นใหม่ๆ เริ่มมีความสามารถในการป้องกันภัยจากการโจมตีด้วยวิธีการ DoS และ DdoS แต่วิธีการที่ดีที่สุดในการป้องกันการโจมตีจากอินเทอร์เน็ตและเครือข่าย ที่ผู้ใช้สามารถดำเนินการได้ด้วยตนเองคือ การติดตั้งไฟร์วอลล์ส่วนตัว (Personal Firewall) ไฟร์วอลล์ส่วนตัวคือซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัวซึ่งทำหน้าที่ช่วยป้องกันผู้บุกรุกหรือผู้ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ส่วนตัวของเราหรือช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดีทั้งหลาย เช่น ไวรัส โทรจัน สปายแวร์ เป็นต้น ไฟร์วอลล์ทำงานโดยทำการตรวจสอบข้อมูลทั้งหมด (ไวรัส โทรจัน สปายแวร์ ก็ถือเป็นข้อมูลด้วย ที่เข้าหรือออกจากเครื่องคอมพิวเตอร์ส่วนตัวและจะอนุญาตให้ผ่านไปได้ก็ต่อเมื่อตรวจสอบแล้วและพบว่าไม่ละเมิดกับกฎเกณฑ์ของไฟร์วอลล์ที่กำหนดไว้ ในทางตรงกันข้าม หากมีการละเมิดไฟร์วอลล์ก็จะไม่อนุญาติให้ผ่านไป

(3) การลักลอบเข้าใช้งานโดยไม่ได้รับอนุญาต (Unauthorized Access and Use)

การลักลอบเข้าใช้งานคือการเข้าถึงเครื่องคอมพิวเตอร์และเครือข่ายโดยไม่มีสิทธิหรือไม่ได้รับอนุญาต รวมทั้งใช้เครื่องคอมพิวเตอร์และข้อมูลโดยที่ไม่ได้รับการอนุมัติหรือใช้ในกิจกรรมที่ผิดกฎหมาย ตัวอย่างเช่นการใช้อีเมลขององค์กรส่งข้อความที่เป็นเรื่องส่วนตัว ไม่มีความเกี่ยวข้องกันงาน หรือใช้โปรแกรมขององค์กรในกิจกรรมที่ผิดกฎหมายเช่นบันทึกข้อมูลการพนันบอล หรือใช้เครื่องคอมพิวเตอร์ขององค์กรเข้าถึงข้อมูลของธนาคารและทำการโอนเงินของลูกค้าเข้าบัญชีของตนเอง เป็นต้น รวมทั้งการลักลอบใช้งานเครือข่ายโดยไม่ได้รับอนุญาตซึ่งส่วนใหญ่จะเกิดกับผู้ใช้เครื่องคอมพิวเตอร์ที่บ้าน

สำหรับแนวทางในการป้องกันการเข้าใช้งานโดยไม่ได้รับอนุญาตสามารถทำได้ทั้งในระบบองค์กรและบุคคล ในระดับองค์กรคือควรมีการประกาศ Acceptance usage policy (AUP) ที่กำหนดขอบเขตในการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของผู้ใช้งานอย่างชัดเจน หรือบางองค์กรจะปิดการเชื่อมต่ออินเทอร์เน็ตและเครือข่ายในช่วงเวลาพักกลางวันและนอกเหนือจากชั่วโมงทำงานปกติ ส่วนในระดับบุคคลสามารถป้องกันได้โดยปิดการใช้งาน file and printer sharing ในระหว่างการเชื่อมต่ออินเทอร์เน็ตหรือเครือข่าย เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้ นอกจากนี้ยังสามารถทำได้โดยการระบุตัวตนและการรับรองผู้ใช้ (User Identification and authentication) เพื่อเป็นการพิสูจน์ว่าผู้ใช้ที่กำลังใช้งานอยู่คือใคร มีสิทธิ์เข้าใช้ระบบหรือเครื่องคอมพิวเตอร์หรือไม่ เพียงใด โดยส่วนใหญ่การเข้าถึงข้อมูลที่มีความสำคัญ ข้อมูลที่เป็นความลับ ข้อมูลส่วนตัวและข้อมูลทางการเงิน จะต้องมีการตรวจสอบสิทธิก่อนการเข้าใช้งานเสมอ

วิธีการที่ถูกนำมาใช้ในการพิสูจน์ตัวตนและตรวจสอบสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์และระบบงานมี 3 รูปแบบดังนี้

- การใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ซึ่งต้องไม่ซ้ำซ้อนกันในระบบ รหัสผ่านจะต้องมีความเหมาะสม และไม่ง่ายจนเกินไปเช่นชื่อ นามสกุล เบอร์โทรศัพท์ วันเกือนปีเกิด ซึ่งจะสามารถคาดเดาได้โดยง่าย ไม่ใช้คำศัพท์ที่มีความหมายเนื่องจากแฮกเกอร์สามารถใช้โปรแกรมเดารหัสผ่านได้ รหัสผ่านควรมีความยาวอยู่ระหว่าง 6-16 ตัวอักษร และที่สำคัญต้องไม่บันทึกรหัสผ่านไว้ในที่ที่ผู้อื่นสามารถพบเจอได้ และไม่ควรใช้ฟังก์ชันช่วยจำ User name และ Password ของเว็บไซต์ หรือโปรแกรมใดๆ เพราะอาจเป็นสาเหตุให้ถูกขโมยได้ง่าย รวมทั้งต้องมีการเปลี่ยนรหัสผ่านเป็นประจำสม่ำเสมอ

- การใช้วัตถุในการตรวจสอบ (Possessed Objects) คือสิ่งของที่ผู้ใช้สามารถพกพาติด ตัวไปเพื่อใช้ในการตรวจสอบ เช่น บัตรผ่าน อาจใช้ร่วมกับรหัสผ่านได้

- การตรวจสอบทางชีวภาพ (Biometric Device) คือ การตรวจสอบลักษณะทางชีวภาพว่าตรงกับลักษณะทางชีวภาพที่บันทึกไว้หรือไม่ เช่น ม่านตา ลายนิ้วมือเป็นต้น

(4) การขโมยและทำลายฮาร์ดแวร์ (Hardware Theft)

การขโมยเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์เป็นการขโมยแบบดั้งเดิมทางกายภาพโดยไม่ต้องใช้เทคนิคทางคอมพิวเตอร์ จากการสำรวจในประเทศสหรัฐอเมริกาพบว่ามีอัตราสูงถึงร้อยละ 33.5 ของการเกิดอาชญากรรมคอมพิวเตอร์ทั้งหมด โดยส่วนใหญ่จะเกิดกับเครื่องคอมพิวเตอร์แบบพกพาหรืออุกรณ์เก็บข้อมูลที่สามารถพกพาได้ การขโมยการขโมยเครื่องคอมพิวเตอร์อาจมีวัตถุประสงค์เพื่อนำตัวเครื่องไปจำหน่ายหรือนำข้อมูลที่อยู่บนเครื่องเช่น ข้อมูลส่วนบุคคล เบอร์โทรศัพท์ ที่อยู่ อีเมล์ รหัสบัตรเครดิต เลขประจำตัวประชาชนเป็นต้น ไปจำหน่ายจ่ายแจก เผยแพร่หรือส่งต่อทำให้เกิดความเสียหาย

สำหรับวิธีการป้องกันในระดับองค์กรคือการสร้างความปลอดภัยทางด้านกายภาพ เช่น การควบคุมการเข้าถึง การล็อคประตูหน้าต่าง หรือการใช้อุปกรณ์ป้องกันอื่นที่เหมาะสม บางองค์กรอาจใช่ระบบแสดงตำแหน่งในเวลาจริง (Real Time Location System:RTLS) เพื่อค้นหาและแสดงตำแหน่ง สามารถตรวจสอบได้ทันทีว่าอุปกรณ์นั้นอยู่ในพื้นที่ใดและหากสิ่งนั้นเคลื่อนที่ก็สามารถทราบความเปลี่ยนแปลงได้ ส่วนผู้ใช้เครื่องคอมพิวเตอร์เองก็จะต้องให้ความระมัดระวังเป็นพิเศษและต้องตระหนักถึงความเสี่ยงที่สามารถเกิดขึ้นได้ วิธีการป้องกันไม่ให้ถูกขโมยสามารถทำได้หลายวิธี ยกตัวอย่างเช่น

- ใช้สายเคเบิลรักษาความปลอดภัยคล้องคอมพิวเตอร์เข้ากับวัตถุที่เคลื่อนที่ไม่ได้

- ติดตั้งระบบความปลอดภัยบนเครื่องคอมพิวเตอร์ โดยโปรแกรมประเภทนี้จะส่งสัญญาณเตือนเมื่อเครื่องคอมพิวเตอร์ถูกเคลื่อนย้ายจากพื้นที่ที่กำหนดไว้

- ติดตั้งระบบติดตามไว้บนเครื่องคอมพิวเตอร์เมื่อถูกขโมยจะได้ทราบตำแหน่งและสามารถติดตามกลับคืนมาได้

- ใช้การพิสูจน์ตัวตนเช่น รหัสผ่าน การแสกนลายนิ้วมือหรือวิธีการอื่นๆ ในการเข้าสู่เครื่องคอมพิวเตอร์ วิธีนี้ถึงแม้จะไม่เป็นการป้องกันการถูกขโมยแต่ป้องกันข้อมูลภายในได้

- สำหรับอุปกรณ์เก็บข้อมูลแบบพกพา เช่น USB Flash Drive และ External Hard-disk เป็นต้น สามารถใช้รหัสผ่านในการเข้าถึงข้อมูลภายใน นอกจากนี้ควรสำรองข้อมูล (Backup) ไว้เป็นระยะหรือควรมีการเข้ารหัสข้อมูล (Data Encryption) ถึงแม้จะถูกขโมยแต่กลุ่มอาชญากรคอมพิวเตอร์ก็ไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้

(5) การขโมยข้อมูล (Information Theft)

การขโมยข้อมูลคือการที่ผู้ไม่ประสงค์ดีเข้ามาขโมยข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับ ซึ่งทำให้เกิดความเสียหาย ทั้งผู้ใช้งานในองค์กรและที่บ้านสามารถตกเป็นเหยื่อการขโมยข้อมูลได้ เช่นบริษัทที่ไร้จรรยาบรรณอาจขโมยหรือซื้อข้อมูลที่ถูกขโมยเพื่อนำไปใช้สร้างความได้เปรียบในการแข่งขัน หรือการขโมยเลขที่บัตรเครดิตเพื่อนำไปใช้ฉ้อโกงทางการเงิน ข้อมูลที่ส่งผ่านบนเครือข่ายมีความเสี่ยงสูงที่จะถูกขโมยเพราะผู้ไม่ประสงค์ดีจะใช้ช่องทางนี้ในการดักจับข้อมูล หรือแม้แต่ข้อมูลที่อยู่บนเครื่องคอมพิวเตอร์ก็มีความเสี่ยงเช่นกันถ้าผู้ไม่ประสงค์ดีเหล่านั้นลักลอบเข้ามาได้

วิธีการระบุตัวตนและตรวจสอบสิทธิของผู้ใช้ เป็นวิธีที่เหมาะสมในการปกป้องข้อมูลบนคอมพิวเตอร์ที่ได้จัดวางไว้ในสถานที่ปลอดภัย แต่สำหรับข้อมูลที่ต้องส่งผ่านอินเทอร์เน็ตหรือเครือข่าย สามาถทำได้โดยใช้เทคนิคการเข้ารหัสข้อมูล (Encryption) ซึ่งเป็นกระบวนการแปลงข้อความที่สามารถอ่านได้ (plain text) ไปเป็นข้อความที่ไม่สามารถอ่านได้ (cipher text) ซึ่งหากไม่ใช่ผู้ที่เกี่ยวข้องหรือได้รับอนุญาตในการเข้าดูเอกสารดังกล่าว จะไม่สามารถถอดรหัสข้อมูลได้ และจะทำให้ไม่สามารถเข้าถึงเนื้อหาได้ นอกจากนี้ยังมีวิธีการง่ายๆ ที่คนมักจะละเลยไม่ให้ความสำคัญ คือ การประกาศ (Post) ข้อมูลที่เป็นส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ เลขที่บัตรประชาชน เลขที่บัตรเครดิต เป็นต้น บนเว็บไซต์หรือนำไปใช้บนเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งถ้าผู้อื่นมาพบอาจนำข้อมูลไปใช้ต่อทำให้เกิดความเสียหายก็เป็นได้

ภาคผนวก ข
เครื่องมือที่ใช้ในการวิจัย

แบบสอบถาม

ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

คำชี้แจง

แบบสอบถามนี้จัดทำขึ้น เพื่อเก็บรวบรวมข้อมูลในการทำวิทยานิพนธ์ โดยข้อคำถามแบ่งออกเป็น 3 ตอน ดังนี้

ส่วนที่ 1 เป็นคำถามเกี่ยวกับข้อมูลภูมิหลัง และข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศอายุ ระดับการศึกษา ตำแหน่งงาน หรือสาขาวิชาที่ศึกษา

ส่วนที่ 2 เป็นคำถามเกี่ยวกับการใช้คอมพิวเตอร์และความปลอดภัยคอมพิวเตอร์

ส่วนที่ 3 เป็นคำถามเกี่ยวกับการวัดค่าปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์

การแสดงความคิดเห็นไม่มีข้อใดถูกหรือผิด ผู้วิจัยจึงใคร่ขอความกรุณาจากท่านได้โปรดตอบ แบบสอบถามทุกข้อตามความจริงและขอรับรองว่าคำตอบของท่านจะไม่มีผลกระทบใดๆกับตัวท่านทั้งสิ้น ข้อมูลทั้งหมดจะถือเป็นความลับและนำไปใช้ในการศึกษาเท่านั้น ขอขอบคุณทุกท่านที่ให้ความร่วมมือในการตอบแบบสอบถามเป็นอย่างดี มา ณ โอกาสนี้

ส่วนที่ 1 ข้อมูลส่วนตัวของผู้ตอบแบบสอบถาม

1. เพศ ☐ หญิง ☐ชาย
2. อายุ ☐ ต่ำกว่า 18 ปี ☐ 18–24 ปี ☐ 25–34 ปี
   ☐ 35–44 ปี ☐ 45–54 ปี ☐ มากกว่า 55 ปี
3. การศึกษา ☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี
4. ตำแหน่ง/ลักษณะงานที่ทำ_____
   หรือสาขาวิชาที่ศึกษา_____
5. อายุงาน ☐ ยังไม่ได้ทำงาน ☐ ต่ำกว่า1 ปี ☐ 1-5 ปี
   ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ส่วนที่ 2 ข้อมูลเกี่ยวกับการใช้คอมพิวเตอร์

1. ท่านมีประสบการณ์ในการใช้คอมพิวเตอร์ ประมาณ (ปี).....
2. วัตถุประสงค์ในการใช้งานคอมพิวเตอร์ของท่าน (ส่วนใหญ่)

   ☐ ใช้ในเรื่องที่เกี่ยวข้องกับการทำงาน

   ☐ ใช้ในเรื่องส่วนตัวเช่นซื้อของออนไลน์ หรือเพื่อความบันเทิง เช่น ดูหนัง/ ฟังเพลง/ เล่นเกมส์
3. คอมพิวเตอร์ที่ท่านใช้งานอยู่เป็นแบบใด

   ☐ พีซี

   ☐ โน๊ตบุ๊ค/เน็ตบุ๊ค/แล็บท็อป

   ☐ อื่นๆ โปรดระบุ_____
4. ท่านสามารถติดตั้งซอฟท์แวร์ลงบนเครื่องคอมพิวเตอร์ที่ท่านใช้งานได้เอง

   ☐ ได้ ☐ ไม่ได้ ☐ ไม่แน่ใจ
5. ข้อมูลใดบ้างที่มีความสำคัญและเป็นความลับสำหรับท่าน

   _____

   _____
6. ท่านเก็บข้อมูลที่มีความสำคัญและเป็นความลับ (ตามข้อที่แล้ว) ในคอมพิวเตอร์

   ☐ ใช่ ☐ ไม่ใช่
7. การใช้งานคอมพิวเตอร์ภายในองค์กรของท่านมีการป้องกันด้านความปลอดภัยหรือไม่

   ☐ มี ☐ ไม่มี ☐ ไม่แน่ใจ
8. การใช้งานคอมพิวเตอร์ภายในบ้านของท่านมีการป้องกันด้านความปลอดภัยหรือไม่

   ☐ มี ☐ ไม่มี ☐ ไม่แน่ใจ
9. ท่านรับรู้ข้อมูลข่าวสารด้านคอมพิวเตอร์และอาชญากรรมคอมพิวเตอร์จากแหล่งใด

   ☐ อินเทอร์เน็ต ☐ วารสารหรือหนังสือ

   ☐ โทรทัศน์ ☐ อื่นๆ โปรดระบุ_____

ส่วนที่ 3 ความคิดเห็นต่อปัจจัยที่ส่งผลต่อการแสดงพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์

โปรดพิจารณาประเด็นในแต่ละข้อ แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุดเพียงช่องเดียว โดยมีเกณฑ์ในการพิจารณาดังนี้

คุณมีความคิดเห็นเกี่ยวกับปัจจัยเหล่านี้อย่างไร	**ระดับคะแนน**				
	5	4	3	2	1
1.คุณสามารถทำงานที่ได้รับมอบหมายอย่างมีประสิทธิภาพ					
2.คุณเป็นคนมีระเบียบวินัย					
3. คุณเป็นคนที่ชอบความสมบูรณ์แบบ					
4.คุณคิดอย่างรอบคอบก่อนที่จะพูดหรือลงมือทำใดๆ					
5.คุณคิดว่าข้อมูลของคุณควรได้รับปกป้องจากอาชญากรรมคอมพิวเตอร์					
6.คุณรู้สึกกังวลว่าข้อมูลในเครื่องคอมพิวเตอร์ของคุณไม่ปลอดภัย					
7.คุณคิดว่าข้อมูลต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ของคุณมีความสำคัญ					
8.คุณจะได้รับความเสียหาย ถ้าข้อมูลในเครื่องคอมพิวเตอร์ของคุณถูกขโมย					
9.คุณเคยประสบปัญหาจากอาชญากรรมคอมพิวเตอร์					
10.ครอบครัว เพื่อน หรือบุคคลใกล้ชิดของคุณเคยประสบปัญหาจากอาชญากรรมคอมพิวเตอร์					
11.คุณเคยได้รับความเสียหายจากอาชญากรรมคอมพิวเตอร์					
12.คุณสงสัยว่าเครื่องคอมพิวเตอร์ของคุณอาจจะเคยถูกคุกคามจากอาชญากรรมคอมพิวเตอร์					
13.เพื่อนกระตุ้นหรือชักชวนให้คุณดำเนินการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์					
14. หน่วยงานด้านความปลอดภัยกระตุ้นให้คุณดำเนินการด้านความปลอดภัยคอมพิวเตอร์					
15.ครอบครัวของคุณสนับสนุนให้คุณดำเนินการเพื่อป้องกันภัยจากอาชญากรรมคอมพิวเตอร์					
16.หัวหน้างานหรือบุคคลที่คุณให้ความเชื่อถือกระตุ้นให้คุณดำเนินการด้านความปลอดภัย					
17.คุณได้รับการฝึกอบรมหรือได้รับความรู้เกี่ยวกับการใช้งานคอมพิวเตอร์อย่างปลอดภัย					

คุณมีความคิดเห็นเกี่ยวกับปัจจัยเหล่านี้อย่างไร	**ระดับคะแนน**				
	5	4	3	2	1
18.คุณอ่านข่าวสารหรือข้อมูลด้านความปลอดภัยคอมพิวเตอร์จากสื่อต่างๆ					
19.คุณให้ความสนใจและติดตามข้อมูลเกี่ยวกับการรักษาความปลอดภัยคอมพิวเตอร์					
20.คุณคิดว่าคู่มือหรือคำแนะนำด้านความปลอดภัยช่วยให้คุณรู้วิธีในการป้องกันภัย					
21.คุณคิดว่าการติดตั้งและการใช้ซอฟต์แวร์ด้านความปลอดภัยจะทำให้โปรแกรมอื่นๆ บนเครื่องคอมพิวเตอร์เกิดปัญหาหรือเกิดความไม่สะดวกในการใช้งาน					
22.คุณคิดว่าการติดตั้งและการใช้ซอฟต์แวร์ด้านความปลอดภัยบนเครื่องคอมพิวเตอร์มีขั้นตอนยุ่งยาก					
23.คุณคิดว่าการติดตั้งและการใช้ซอฟต์แวร์ด้านความปลอดภัยบนเครื่องคอมพิวเตอร์นั้นเสียเวลา					
24.คุณคิดว่าเครื่องมือหรือซอฟต์แวร์ที่นำมาใช้ป้องกันภัยมีราคาแพงเกินไป					
25.คุณคิดว่าทุกคนมีโอกาสถูกคุกคามจากอาชญากรรมคอใพิวเตอร์มากขึ้นถ้าเคยถูกคุกคามมาก่อน					
26.คุณคิดว่าทุกคนมีความเสี่ยงที่จะถูกคุกคามจากอาชญากรรมคอมพิวเตอร์					
27.ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ก่อให้เกิดความเสียหายต่อคอมพิวเตอร์และข้อมูลของคุณ					
28.คุณคิดว่าในปัจจุบันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์มีอัตราเพิ่มขึ้น					
29.คุณเชื่อมั่นว่าคุณมีทักษะเพียงพอในการดำเนินการป้องกันภัยคอมพิวเตอร์					
30.คุณเชื่อมั่นว่าภัยคุกคามจากอาชญากรรมคอมพิวเตอร์นั้นสามารถป้องกันได้					
31.คุณสามารถดำเนินการป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ด้วยตัวเอง					
32.ถ้าคอมพิวเตอร์ถูกคุกคามจากอาชญากรรมคอมพิวเตอร์คุณรู้ว่าจะจัดการกับปัญหานี้อย่างไร					

คุณมีความคิดเห็นเกี่ยวกับปัจจัยเหล่านี้อย่างไร	**ระดับคะแนน**				
	5	**4**	**3**	**2**	**1**
33.คุณตั้งใจจะนำมาตรการหรือเครื่องมือต่างมาใช้เพื่อหลีกเลี่ยงภัยคุกคามจากอาชญากรรมคอมพิวเตอร์					
34.เมื่อคุณได้รับข้อมูลหรือข่าวสารเกี่ยวกับอาชญากรรมคอมพิวเตอร์ คุณจะหาวิธีการป้องกันไม่ให้คอมพิวเตอร์ของคุณถูกคุกคาม					
35.คุณมุ่งมั่นที่จะปฏิบัติหรือดำเนินการตามคำแนะนำเพื่อป้องกันภัยจากอาชญากรรมคอมพิวเตอร์					
36.คุณพยายามหาวิธีการต่างๆ มาใช้เพื่อป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ถึงแม้คุณจะไม่เคยถูกคุกคามมาก่อน					
37.คุณทำการปกป้องคอมพิวเตอร์และข้อมูลของคุณเพื่อไม่ให้ถูกคุกคาม					
38.คุณใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัยเพื่อป้องกันการถูกคุกคาม					
39.คุณปฏิบัติตามคำแนะนำต่างๆ ที่ได้รับคำแนะนำเพื่อไม่ให้ถูกคุกคามจากอาชญากรรมคอมพิวเตอร์					

ภาคผนวก ค
ตำแหน่งงานและสาขาวิชาด้านเทคโนโลยีสารสนเทศ

ตำแหน่งงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สำหรับคำนิยามและแนวคิดของผู้ทำงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เป็นการจัดจำแนกประเภทอาชีพตาม International Standard Classification of Occupation, 2008 (ISCO-08) ขององค์การแรงงานระหว่างประเทศ (ILO) ซึ่งสามารถจัดแบ่งตามรหัสอาชีพ ได้ดังนี้

รหัส 13 ผู้จัดการด้านการผลิตและการบริการเฉพาะอย่าง

1330 ผู้จัดการด้านการบริการเทคโนโลยีสารสนเทศและการสื่อสาร

รหัส 23 ผู้ประกอบวิชาชีพด้านการสอน

2356 ผู้ฝึกอบรมด้านเทคโนโลยีสารสนเทศ

รหัส 25 ผู้ประกอบวิชาชีพด้านเทคโนโลยีสารสนเทศและการสื่อสาร

2511 นักวิเคราะห์ระบบคอมพิวเตอร์

2512 นักพัฒนาซอฟต์แวร์

2513 นักพัฒนาเว็บไซต์และสื่อผสม

2514 โปรแกรมเมอร์

2519 นักวิเคราะห์และพัฒนาซอฟต์แวร์และโปรแกรม ประยุกต์ ซึ่งมิได้จัดประเภทไว้ในที่อื่น

2521 นักออกแบบและผู้บริหารฐานข้อมูล

2522 ผู้บริหารระบบงานคอมพิวเตอร์

2523 ผู้ประกอบวิชาชีพด้านเครือข่ายคอมพิวเตอร์

2529 ผู้ประกอบวิชาชีพด้านฐานข้อมูลและเครือข่าย ซึ่งมิได้ จัดประเภทไว้ในที่อื่น

รหัส 35 ช่างเทคนิคด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3511 ช่างเทคนิคปฏิบัติการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3512 ช่างเทคนิคให้ความช่วยเหลือและแก้ปัญหาด้าน เทคโนโลยีสารสนเทศและการสื่อสารกับผู้ใช้งาน

3513 ช่างเทคนิคด้านเครือข่ายและระบบคอมพิวเตอร์

3514 ช่างเทคนิคด้านเว็บไซต์

3521 ช่างเทคนิคด้านการแพร่ภาพกระจายเสียงและ โสตทัศนูปกรณ์

3522 ช่างเทคนิควิศวกรโทรคมนาคม

รหัส 74 ช่างไฟฟ้าอิเล็กทรอนิกส์

7411 ช่างเดินสายไฟภายในอาคารและอุปกรณ์ไฟฟ้าที่ เกี่ยวข้อง

7412 ช่างเครื่องและช่างปรับอุปกรณ์ไฟฟ้า

7413 ช่างติดตั้งและซ่อมสายส่งกระแสไฟฟ้า

7421 ช่างเครื่องและผู้ให้บริการด้านอุปกรณ์อิเล็กทรอนิกส์

7422 ช่างติดตั้งและผู้ให้บริการด้านอุปกรณ์ เทคโนโลยี สารสนเทศและการสื่อสาร

สาขาวิชาด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานสถิติแห่งชาติ () ได้พิจารณาจัดจำแนกตามมาตรฐานการจัดจำแนกการศึกษา : สาขาวิชาของประเทศสำหรับสาขาวิชาการศึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ดังนี้

รหัส 46 คณิตศาสตร์และสถิติ

- คณิตศาสตร์ การวิจัยดำเนินงาน การวิเคราะห์เชิงตัวเลข วิทยาการประกันภัย สถิติและสาขาอื่นๆ ที่เกี่ยวข้อง

รหัส 48 คอมพิวเตอร์

- วิทยาการคอมพิวเตอร์ ได้แก่ การออกแบบระบบ การเขียนโปรแกรมคอมพิวเตอร์ การประมวลผลข้อมูล ระบบเครือข่าย การพัฒนาซอฟต์แวร์ของระบบปฏิบัติการ

รหัส 52 วิศวกรรมศาสตร์

- การออกแบบด้านวิศวกรรม วิศวกรรมเครื่องกล วิศวกรรมโลหะ วิศวกรรมไฟฟ้า วิศวกรรมอิเล็กทรอนิกส์ วิศวกรรมโทรคมนาคม วิศวกรรมพลังงาน และวิศวกรรมเคมี การบำรุงรักษายานยนต์ การสำรวจ
- การพัฒนาฮาร์ดแวร์

ภาคผนวก ง
ตัวอย่างผลการวิเคราะห์โมเดลเชิงสาเหตุพฤติกรรมการป้องกันภัย จากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

DATE: 4/20/2015

TIME: 1:34

L I S R E L 8.72

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140

Website: www.ssicentral.com

The following lines were read from file C:\Users\ADMIN\Lisrel_Result\ALL\allsample.lpj:

```
TI COMPUTER CRIME PROTECTION BEHAVIOR
!DA NI=39 NO=600 MA=CM
SY='C:\ Users\ADMIN\Lisrel_Result\ALL\allsample.DSF'
SE
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
21 22 23 24 /
MO NX=24 NY=15 NK=6 NE=4 LX = FU,FI LY = FU,FI GA = FU,FI BE = FU,FI TD =FU,FI TE = FU,FI
LE
TA CA PM PB
```

LK

CP PV PE SN SK SC

FR LY(2,1) LY(3,1) LY(4,1) LY(6,2) LY(7,2) LY(8,2) LY(10,3) LY(11,3) LY(12,3)

FR LY(14,4) LY(15,4) LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,2) LX(6,2) LX(7,2)

FR LX(8,2) LX(9,3) LX(10,3) LX(11,3) LX(12,3) LX(13,4) LX(14,4) LX(15,4) LX(16,4)

FR LX(17,5) LX(18,5) LX(19,5) LX(20,5) LX(21,6) LX(22,6) LX(23,6) LX(24,6) BE(3,1) LY(1,1) LY(5,2) LY(9,3) LY(13,4)

FR BE(3,2) BE(4,1) BE(4,2) BE(4,3) GA(1,1) GA(1,2) GA(1,3) GA(1,4) GA(2,1)

FR GA(2,4) GA(2,5) GA(2,6)

FR TE(1,1) TE(2,2) TE(3,3) TE(4,4) TE(5,5) TE(6,6) TE(7,7) TE(8,8) TE(9,9) TE(10,10) TE(11,11) TE(12,12) TE(13,13) TE(14,14) TE(15,15)

FR TD(1,1) TD(2,2) TD(3,3) TD(4,4) TD(5,5) TD(6,6) TD(7,7) TD(8,8) TD(9,9) TD(10,10) TD(11,11) TD(12,12) TD(13,13) TD(14,14) TD(15,15) TD(16,16) TD(17,17) TD(18,18) TD(19,19) TD(20,20) TD(21,21) TD(22,22) TD(23,23) TD(24,24)

FR TD(14,13) TE(4,3) TD(11,10) TD(24,21) TE(14,6) TE(12,6) TE(12,10) TD(2,1) TE(15,5) TE(4,2) TD(18,17) TD(12,10) TE(12,5) TD(19,17) TD(24,2) TD(18,11) TE(13,12) TE(15,6) TE(2,1) TD(24,23) TD(10,7) TE(14,1) TD(24,20) TE(10,1) TE(12,3) TE(11,8) TD(22,10) TE(13,6) TD(3,2) TD(4,1)

FR TD(19,18) TD(20,11) TE(9,8) TE(14,9) TD(4,2) TE(7,4) TE(6,4) TD(21,9)

FR TH(18,2) TH(21,3) TH(19,6) TH(19,12) TH(17,3) TH(24,11) TH(4,8) TH(3,3)

PD

OU EF ND=3

TI COMPUTER CRIME PROTECTION BEHAVIOR

Number of Input Variables 39

Number of Y - Variables 15

Number of X - Variables 24

Number of ETA - Variables 4

Number of KSI - Variables 6

Number of Observations 600

TI COMPUTER CRIME PROTECTION BEHAVIOR

Covariance Matrix

	TA1	TA2	TA3	TA4	CA1	CA2
TA1	0.564					
TA2	0.429	0.617				
TA3	0.469	0.424	0.526			
TA4	0.590	0.593	0.486	0.927		
CA1	0.186	0.165	0.181	0.183	0.600	
CA2	0.248	0.205	0.226	0.298	0.399	0.697
CA3	0.287	0.256	0.266	0.343	0.401	0.537
CA4	0.282	0.259	0.252	0.320	0.400	0.533
PM1	0.209	0.143	0.178	0.222	0.250	0.249
PM2	0.218	0.147	0.173	0.223	0.249	0.261
PM3	0.212	0.181	0.199	0.237	0.170	0.181
PM4	0.239	0.178	0.180	0.272	0.277	0.296
PB1	0.282	0.189	0.249	0.261	0.345	0.381
PB2	0.210	0.192	0.221	0.235	0.320	0.473
PB3	0.269	0.224	0.237	0.296	0.258	0.355
CP1	0.190	0.200	0.191	0.218	0.119	0.181
CP2	0.178	0.216	0.184	0.245	0.123	0.183
CP3	0.208	0.236	0.225	0.237	0.159	0.208
CP4	0.241	0.240	0.220	0.255	0.131	0.214
PV1	0.131	0.138	0.134	0.152	0.052	0.093
PV2	0.131	0.135	0.137	0.154	0.075	0.098
PV3	0.128	0.137	0.133	0.141	0.089	0.113
PV4	0.128	0.155	0.144	0.173	0.091	0.138
PE1	0.246	0.239	0.205	0.312	0.206	0.286
PE2	0.247	0.226	0.188	0.278	0.192	0.209
PE3	0.226	0.202	0.165	0.263	0.179	0.217
PE4	0.254	0.203	0.197	0.284	0.196	0.293
SN1	0.210	0.209	0.202	0.245	0.108	0.148
SN2	0.230	0.220	0.220	0.273	0.113	0.162
SN3	0.194	0.173	0.174	0.224	0.093	0.176
SN4	0.224	0.209	0.209	0.268	0.111	0.139
SK1	0.206	0.201	0.235	0.189	0.253	0.299

SK2	0.212	0.261	0.213	0.230	0.348	0.382
SK3	0.217	0.247	0.213	0.264	0.297	0.423
SK4	0.221	0.233	0.231	0.225	0.315	0.360
SC1	-0.106	-0.100	-0.152	-0.113	-0.166	-0.191
SC2	-0.110	-0.086	-0.120	-0.102	-0.169	-0.187
SC3	-0.118	-0.106	-0.137	-0.115	-0.170	-0.191
SC4	-0.139	-0.107	-0.143	-0.116	-0.185	-0.215

Covariance Matrix

	CA3	CA4	PM1	PM2	PM3	PM4
CA3	0.685					
CA4	0.593	0.903				
PM1	0.270	0.317	0.654			
PM2	0.279	0.280	0.371	0.519		
PM3	0.231	0.274	0.364	0.326	0.586	
PM4	0.236	0.228	0.457	0.296	0.344	0.755
PB1	0.451	0.453	0.313	0.293	0.232	0.355
PB2	0.463	0.464	0.239	0.259	0.217	0.271
PB3	0.470	0.488	0.281	0.261	0.234	0.271
CP1	0.211	0.212	0.184	0.117	0.119	0.146
CP2	0.236	0.221	0.194	0.147	0.166	0.186
CP3	0.258	0.256	0.180	0.149	0.153	0.163
CP4	0.261	0.299	0.166	0.138	0.159	0.153
PV1	0.120	0.122	0.044	0.051	0.060	0.036
PV2	0.125	0.117	0.060	0.074	0.069	0.055
PV3	0.130	0.132	0.039	0.068	0.059	0.049
PV4	0.160	0.139	0.083	0.079	0.082	0.075
PE1	0.273	0.310	0.193	0.153	0.194	0.209
PE2	0.232	0.282	0.228	0.164	0.198	0.211
PE3	0.260	0.297	0.188	0.152	0.192	0.171
PE4	0.296	0.321	0.164	0.160	0.169	0.149
SN1	0.188	0.214	0.138	0.122	0.086	0.090
SN2	0.208	0.228	0.138	0.113	0.077	0.097

SN3	0.210	0.221	0.140	0.106	0.082	0.102
SN4	0.186	0.185	0.099	0.102	0.057	0.069
SK1	0.350	0.337	0.199	0.209	0.181	0.123
SK2	0.417	0.459	0.223	0.209	0.240	0.183
SK3	0.381	0.421	0.198	0.165	0.187	0.229
SK4	0.391	0.390	0.239	0.222	0.229	0.198
SC1	-0.244	-0.225	-0.193	-0.115	-0.189	-0.180
SC2	-0.231	-0.234	-0.191	-0.135	-0.175	-0.152
SC3	-0.238	-0.217	-0.206	-0.134	-0.176	-0.183
SC4	-0.232	-0.252	-0.202	-0.136	-0.124	-0.136

Covariance Matrix

	PB1	PB2	PB3	CP1	CP2	CP3
PB1	0.879					
PB2	0.584	0.878				
PB3	0.585	0.558	0.842			
CP1	0.198	0.191	0.249	0.568		
CP2	0.190	0.186	0.263	0.358	0.519	
CP3	0.203	0.198	0.270	0.366	0.356	0.522
CP4	0.193	0.185	0.261	0.308	0.278	0.385
PV1	0.105	0.095	0.082	0.088	0.065	0.087
PV2	0.116	0.120	0.097	0.063	0.056	0.060
PV3	0.129	0.142	0.108	0.064	0.057	0.076
PV4	0.142	0.133	0.144	0.073	0.096	0.097
PE1	0.238	0.259	0.273	0.259	0.169	0.231
PE2	0.194	0.206	0.231	0.246	0.193	0.234
PE3	0.200	0.244	0.246	0.257	0.164	0.230
PE4	0.264	0.283	0.290	0.251	0.174	0.216
SN1	0.193	0.160	0.183	0.173	0.133	0.162
SN2	0.217	0.183	0.195	0.178	0.121	0.157
SN3	0.238	0.177	0.217	0.165	0.112	0.163
SN4	0.211	0.168	0.197	0.153	0.092	0.154
SK1	0.265	0.348	0.294	0.230	0.182	0.208

SK2	0.324	0.412	0.322	0.256	0.181	0.238
SK3	0.285	0.379	0.294	0.279	0.237	0.247
SK4	0.302	0.364	0.330	0.259	0.191	0.242
SC1	-0.176	-0.163	-0.164	-0.139	-0.159	-0.155
SC2	-0.175	-0.203	-0.204	-0.109	-0.103	-0.117
SC3	-0.177	-0.205	-0.196	-0.132	-0.127	-0.130
SC4	-0.184	-0.252	-0.217	-0.130	-0.082	-0.131

Covariance Matrix

	CP4	PV1	PV2	PV3	PV4	PE1
CP4	0.580					
PV1	0.119	0.408				
PV2	0.087	0.317	0.393			
PV3	0.099	0.320	0.375	0.461		
PV4	0.092	0.265	0.322	0.316	0.509	
PE1	0.260	0.120	0.119	0.121	0.146	0.938
PE2	0.242	0.100	0.112	0.075	0.123	0.684
PE3	0.245	0.111	0.101	0.086	0.101	0.637
PE4	0.251	0.112	0.111	0.113	0.142	0.719
SN1	0.175	0.191	0.189	0.198	0.184	0.170
SN2	0.171	0.188	0.194	0.202	0.188	0.189
SN3	0.167	0.179	0.190	0.199	0.204	0.182
SN4	0.162	0.177	0.194	0.203	0.203	0.212
SK1	0.185	0.097	0.115	0.118	0.134	0.264
SK2	0.247	0.136	0.130	0.145	0.152	0.289
SK3	0.236	0.106	0.108	0.110	0.128	0.267
SK4	0.238	0.101	0.116	0.124	0.146	0.256
SC1	-0.131	-0.082	-0.069	-0.082	-0.107	-0.139
SC2	-0.123	-0.072	-0.068	-0.085	-0.085	-0.142
SC3	-0.142	-0.084	-0.085	-0.101	-0.107	-0.153
SC4	-0.151	-0.076	-0.077	-0.093	-0.110	-0.193

Covariance Matrix

	PE2	PE3	PE4	SN1	SN2	SN3
PE2	0.924					
PE3	0.710	0.850				
PE4	0.617	0.645	0.892			
SN1	0.157	0.144	0.167	0.555		
SN2	0.154	0.148	0.188	0.515	0.565	
SN3	0.166	0.158	0.193	0.421	0.459	0.576
SN4	0.178	0.178	0.200	0.356	0.402	0.426
SK1	0.289	0.297	0.297	0.162	0.171	0.158
SK2	0.313	0.371	0.301	0.138	0.144	0.153
SK3	0.283	0.299	0.290	0.183	0.190	0.207
SK4	0.286	0.334	0.311	0.141	0.156	0.178
SC1	-0.042	-0.044	-0.064	-0.074	-0.071	-0.056
SC2	-0.097	-0.106	-0.096	-0.046	-0.032	-0.033
SC3	-0.062	-0.096	-0.097	-0.075	-0.064	-0.071
SC4	-0.093	-0.125	-0.133	-0.082	-0.073	-0.083

Covariance Matrix

	SN4	SK1	SK2	SK3	SK4	SC1
SN4	0.604					
SK1	0.143	0.656				
SK2	0.111	0.458	0.838			
SK3	0.152	0.457	0.578	0.791		
SK4	0.111	0.561	0.652	0.619	0.836	
SC1	-0.020	-0.197	-0.210	-0.221	-0.220	0.786
SC2	-0.005	-0.206	-0.248	-0.197	-0.264	0.585
SC3	-0.035	-0.236	-0.261	-0.239	-0.285	0.634
SC4	-0.071	-0.251	-0.286	-0.224	-0.276	0.540

Covariance Matrix

	SC2	SC3	SC4
SC2	0.758		
SC3	0.655	0.771	
SC4	0.673	0.669	0.836

TI COMPUTER CRIME PROTECTION BEHAVIOR

Parameter Specifications

LAMBDA-Y

	TA	CA	PM	PB
TA1	0	0	0	0
TA2	1	0	0	0
TA3	2	0	0	0
TA4	3	0	0	0
CA1	0	0	0	0
CA2	0	4	0	0
CA3	0	5	0	0
CA4	0	6	0	0
PM1	0	0	0	0
PM2	0	0	7	0
PM3	0	0	8	0
PM4	0	0	9	0
PB1	0	0	0	0
PB2	0	0	0	10
PB3	0	0	0	11

LAMBDA-X

	CP	PV	PE	SN	SK	SC
CP1	12	0	0	0	0	0
CP2	13	0	0	0	0	0
CP3	14	0	0	0	0	0
CP4	15	0	0	0	0	0
PV1	0	16	0	0	0	0
PV2	0	17	0	0	0	0
PV3	0	18	0	0	0	0
PV4	0	19	0	0	0	0
PE1	0	0	20	0	0	0
PE2	0	0	21	0	0	0
PE3	0	0	22	0	0	0
PE4	0	0	23	0	0	0
SN1	0	0	0	24	0	0
SN2	0	0	0	25	0	0
SN3	0	0	0	26	0	0
SN4	0	0	0	27	0	0
SK1	0	0	0	0	28	0
SK2	0	0	0	0	29	0
SK3	0	0	0	0	30	0
SK4	0	0	0	0	31	0
SC1	0	0	0	0	0	32
SC2	0	0	0	0	0	33
SC3	0	0	0	0	0	34
SC4	0	0	0	0	0	35

BETA

	TA	CA	PM	PB
TA	0	0	0	0
CA	0	0	0	0
PM	36	37	0	0
PB	38	39	40	0

GAMMA

	CP	PV	PE	SN	SK	SC
TA	41	42	43	44	0	0
CA	45	0	0	46	47	48
PM	0	0	0	0	0	0
PB	0	0	0	0	0	0

PHI

	CP	PV	PE	SN	SK	SC
CP	0					
PV	49	0				
PE	50	51	0			
SN	52	53	54	0		
SK	55	56	57	58	0	
SC	59	60	61	62	63	0

PSI

TA	CA	PM	PB
64	65	66	67

THETA-EPS

	TA1	TA2	TA3	TA4	CA1	CA2
TA1	68					
TA2	69	70				
TA3	0	0	71			
TA4	0	72	73	74		
CA1	0	0	0	0	75	
CA2	0	0	0	76	0	77
CA3	0	0	0	78	0	0
CA4	0	0	0	0	0	0
PM1	0	0	0	0	0	0
PM2	83	0	0	0	0	0
PM3	0	0	0	0	0	0
PM4	0	0	87	0	88	89
PB1	0	0	0	0	0	92
PB2	95	0	0	0	0	96
PB3	0	0	0	0	99	100

THETA-EPS

	CA3	CA4	PM1	PM2	PM3	PM4
CA3	79					
CA4	0	80				
PM1	0	81	82			
PM2	0	0	0	84		
PM3	0	85	0	0	86	
PM4	0	0	0	90	0	91
PB1	0	0	0	0	0	93
PB2	0	0	97	0	0	0
PB3	0	0	0	0	0	0

THETA-EPS

	PB1	PB2	PB3
PB1	94		
PB2	0	98	
PB3	0	0	101

THETA-DELTA-EPS

	TA1	TA2	TA3	TA4	CA1	CA2
CP1	0	0	0	0	0	0
CP2	0	0	0	0	0	0
CP3	0	0	105	0	0	0
CP4	0	0	0	0	0	0
PV1	0	0	0	0	0	0
PV2	0	0	0	0	0	0
PV3	0	0	0	0	0	0
PV4	0	0	0	0	0	0
PE1	0	0	0	0	0	0
PE2	0	0	0	0	0	0
PE3	0	0	0	0	0	0
PE4	0	0	0	0	0	0
SN1	0	0	0	0	0	0
SN2	0	0	0	0	0	0
SN3	0	0	0	0	0	0
SN4	0	0	0	0	0	0
SK1	0	0	128	0	0	0
SK2	0	130	0	0	0	0
SK3	0	0	0	0	0	134
SK4	0	0	0	0	0	0
SC1	0	0	141	0	0	0
SC2	0	0	0	0	0	0
SC3	0	0	0	0	0	0
SC4	0	0	0	0	0	0

THETA-DELTA-EPS

	CA3	CA4	PM1	PM2	PM3	PM4
CP1	0	0	0	0	0	0
CP2	0	0	0	0	0	0
CP3	0	0	0	0	0	0
CP4	0	108	0	0	0	0
PV1	0	0	0	0	0	0
PV2	0	0	0	0	0	0
PV3	0	0	0	0	0	0
PV4	0	0	0	0	0	0
PE1	0	0	0	0	0	0
PE2	0	0	0	0	0	0
PE3	0	0	0	0	0	0
PE4	0	0	0	0	0	0
SN1	0	0	0	0	0	0
SN2	0	0	0	0	0	0
SN3	0	0	0	0	0	0
SN4	0	0	0	0	0	0
SK1	0	0	0	0	0	0
SK2	0	0	0	0	0	0
SK3	0	0	0	0	0	135
SK4	0	0	0	0	0	0
SC1	0	0	0	0	0	0
SC2	0	0	0	0	0	0
SC3	0	0	0	0	0	0
SC4	0	0	0	0	147	0

THETA-DELTA-EPS

	PB1	PB2	PB3
CP1	0	0	0
CP2	0	0	0
CP3	0	0	0
CP4	0	0	0
PV1	0	0	0
PV2	0	0	0
PV3	0	0	0
PV4	0	0	0
PE1	0	0	0
PE2	0	0	0
PE3	0	0	0
PE4	0	0	0
SN1	0	0	0
SN2	0	0	0
SN3	0	0	0
SN4	0	0	0
SK1	0	0	0
SK2	0	0	0
SK3	0	0	0
SK4	0	0	0
SC1	0	0	0
SC2	0	0	0
SC3	0	0	0
SC4	0	0	0

THETA-DELTA

	CP1	CP2	CP3	CP4	PV1	PV2
CP1	102					
CP2	103	104				
CP3	0	106	107			
CP4	109	110	0	111		
PV1	0	0	0	0	112	
PV2	0	0	0	0	0	113
PV3	0	0	0	0	0	0
PV4	0	0	0	0	0	0
PE1	0	0	0	0	0	0
PE2	0	0	0	0	0	0
PE3	0	0	0	0	0	0
PE4	0	0	0	0	0	0
SN1	0	0	0	0	0	0
SN2	0	0	0	0	0	0
SN3	0	0	0	0	0	0
SN4	0	0	0	0	0	0
SK1	0	0	0	0	0	0
SK2	0	0	0	0	0	0
SK3	0	0	0	0	0	0
SK4	0	0	0	0	0	0
SC1	0	0	0	0	0	0
SC2	0	0	0	0	0	0
SC3	0	0	0	0	0	0
SC4	0	148	0	0	0	0

THETA-DELTA

	PV3	PV4	PE1	PE2	PE3	PE4
PV3	114					
PV4	0	115				
PE1	0	0	116			
PE2	117	0	0	118		
PE3	0	0	0	119	120	
PE4	0	0	0	121	0	122
SN1	0	0	0	0	0	0
SN2	0	0	0	0	0	0
SN3	0	0	0	0	0	0
SN4	0	0	0	0	0	0
SK1	0	0	0	0	0	0
SK2	0	0	0	0	131	0
SK3	0	0	0	0	0	0
SK4	0	0	0	0	139	0
SC1	0	0	142	0	0	0
SC2	0	0	0	144	0	0
SC3	0	0	0	0	0	0
SC4	0	0	0	0	0	0

THETA-DELTA

	SN1	SN2	SN3	SN4	SK1	SK2
SN1	123					
SN2	124	125				
SN3	0	0	126			
SN4	0	0	0	127		
SK1	0	0	0	0	129	
SK2	0	0	0	0	132	133
SK3	0	0	0	0	136	137
SK4	0	0	0	0	0	0

SC1	0	0	0	0	0	0
SC2	0	0	0	0	0	0
SC3	0	0	0	0	0	0
SC4	0	0	0	0	0	0

THETA-DELTA

	SK3	SK4	SC1	SC2	SC3	SC4
SK3	138					
SK4	0	140				
SC1	0	0	143			
SC2	0	0	0	145		
SC3	0	0	0	0	146	
SC4	0	149	150	0	151	152

TI COMPUTER CRIME PROTECTION BEHAVIOR

Number of Iterations = 21

LISREL Estimates (MAXimum Likelihood)

LAMBDA-Y

	TA	CA	PM	PB
TA1	0.718	- -	- -	- -
TA2	0.654	- -	- -	- -
	(0.024)			
	27.103			
TA3	0.652	- -	- -	- -

	(0.019)			
	34.296			
TA4	0.807	- -	- -	- -
	(0.028)			
	28.895			
CA1	- -	0.556	- -	- -
CA2	- -	0.712	- -	- -
	(0.035)			
	20.066			
CA3	- -	0.761	- -	- -
	(0.035)			
	21.800			
CA4	- -	0.772	- -	- -
	(0.039)			
	19.566			
PM1	- -	- -	0.647	- -
PM2	- -	- -	0.571	- -
	(0.029)			
	19.502			
PM3	- -	- -	0.545	- -
	(0.029)			
	19.066			
PM4	- -	- -	0.662	- -
	(0.035)			
	18.931			

PB1 - - - - - - 0.771

PB2 - - - - - - 0.748
(0.034)
21.719

PB3 - - - - - - 0.745
(0.033)
22.263

LAMBDA-X

	CP	PV	PE	SN	SK	SC
CP1	0.592	- -	- -	- -	- -	- -
	(0.029)					
	20.436					
CP2	0.521	- -	- -	- -	- -	- -
	(0.034)					
	15.540					
CP3	0.614	- -	- -	- -	- -	- -
	(0.026)					
	23.626					
CP4	0.627	- -	- -	- -	- -	- -
	(0.028)					
	22.036					
PV1	- -	0.518	- -	- -	- -	- -
		(0.022)				
		23.913				

PV2	- -	0.612	- -	- -	- -	- -
	(0.019)					
	32.430					
PV3	- -	0.613	- -	- -	- -	- -
	(0.022)					
	28.418					
PV4	- -	0.525	- -	- -	- -	- -
	(0.025)					
	20.816					
PE1	- -	- -	0.841	- -	- -	- -
		(0.032)				
		26.007				
PE2	- -	- -	0.819	- -	- -	- -
		(0.033)				
		24.511				
PE3	- -	- -	0.768	- -	- -	- -
		(0.031)				
		24.383				
PE4	- -	- -	0.850	- -	- -	- -
		(0.031)				
		27.350				
SN1	- -	- -	- -	0.608	- -	- -
			(0.026)			
			23.284			
SN2	- -	- -	- -	0.666	- -	- -
			(0.025)			
			26.669			

SN3	--	--	--	0.685	--	--
			(0.025)			
			27.403			
SN4	--	--	--	0.617	--	--
			(0.027)			
			22.639			
SK1	--	--	--	--	0.701	--
				(0.028)		
				24.872		
SK2	--	--	--	--	0.806	--
				(0.031)		
				26.350		
SK3	--	--	--	--	0.781	--
				(0.031)		
				25.097		
SK4	--	--	--	--	0.793	--
				(0.031)		
				25.949		
SC1	--	--	--	--	--	0.737
					(0.029)	
					25.471	
SC2	--	--	--	--	--	0.785
					(0.028)	
					27.836	
SC3	--	--	--	--	--	0.842
					(0.027)	

31.098

SC4 - - - - - - - - - - 0.878
(0.030)
29.380

BETA

	TA	CA	PM	PB
TA	- -	- -	- -	- -
CA	- -	- -	- -	- -
PM	0.257	0.443	- -	- -
	(0.040)	(0.045)		
	6.419	9.778		
PB	0.048	0.689	0.180	- -
	(0.035)	(0.052)	(0.042)	
	1.380	13.347	4.282	

GAMMA

	CP	PV	PE	SN	SK	SC
TA	0.340	0.113	0.149	0.215	- -	- -
	(0.045)	(0.040)	(0.042)	(0.045)		
	7.601	2.811	3.583	4.750		
CA	0.199	- -	- -	0.148	0.483	-0.105
	(0.041)			(0.036)	(0.046)	(0.033)
	4.828			4.080	10.605	-3.131

PM - - - - - - - - - - - -

PB - - - - - - - - - - - -

Covariance Matrix of ETA and KSI

	TA	CA	PM	PB	CP	PV
TA	1.000					
CA	0.350	1.000				
PM	0.412	0.533	1.000			
PB	0.364	0.802	0.568	1.000		
CP	0.518	0.525	0.366	0.453	1.000	
PV	0.320	0.256	0.196	0.227	0.203	1.000
PE	0.407	0.386	0.276	0.335	0.475	0.226
SN	0.453	0.396	0.292	0.347	0.395	0.483
SK	0.338	0.670	0.384	0.547	0.495	0.265
SC	-0.161	-0.363	-0.202	-0.294	-0.277	-0.161

Covariance Matrix of ETA and KSI

	PE	SN	SK	SC
PE	1.000			
SN	0.333	1.000		
SK	0.468	0.326	1.000	
SC	-0.156	-0.118	-0.385	1.000

PHI

	CP	PV	PE	SN	SK	SC
CP	1.000					

PV 0.203 1.000
(0.042)
4.816

PE 0.475 0.226 1.000
(0.036) (0.041)
13.324 5.516

SN 0.395 0.483 0.333 1.000
(0.039) (0.034) (0.040)
10.111 14.134 8.350

SK 0.495 0.265 0.468 0.326 1.000
(0.034) (0.039) (0.034) (0.039)
14.719 6.836 13.956 8.434

SC -0.277 -0.161 -0.156 -0.118 -0.385 1.000
(0.040) (0.040) (0.041) (0.042) (0.035)
-6.951 -4.006 -3.815 -2.807 -11.024

PSI
Note: This matrix is diagonal.

TA	CA	PM	PB
0.630	0.476	0.657	0.328
(0.044)	(0.050)	(0.059)	(0.036)
14.452	9.565	11.215	8.980

Squared Multiple Correlations for Structural Equations

TA	CA	PM	PB
0.370	0.524	0.343	0.672

Squared Multiple Correlations for Reduced Form

TA	CA	PM	PB
0.370	0.524	0.207	0.364

Reduced Form

	CP	PV	PE	SN	SK	SC
TA	0.340	0.113	0.149	0.215	- -	- -
	(0.045)	(0.040)	(0.042)	(0.045)		
	7.601	2.811	3.583	4.750		
CA	0.199	- -	- -	0.148	0.483	-0.105
	(0.041)		(0.036)	(0.046)	(0.033)	
	4.828		4.080	10.605	-3.131	
PM	0.175	0.029	0.038	0.121	0.214	-0.046
	(0.026)	(0.011)	(0.012)	(0.022)	(0.027)	(0.015)
	6.831	2.578	3.130	5.520	7.820	-3.028
PB	0.185	0.011	0.014	0.134	0.372	-0.080
	(0.033)	(0.005)	(0.006)	(0.029)	(0.036)	(0.026)
	5.554	1.967	2.179	4.651	10.181	-3.119

THETA-EPS

	TA1	TA2	TA3	TA4	CA1	CA2
TA1	0.044					
	(0.010)					
	4.298					
TA2	-0.039	0.194				
	(0.010)	(0.017)				
	-3.858	11.403				
TA3	- -	- -	0.100			
			(0.010)			
			10.003			
TA4	- -	0.064	-0.040	0.263		
		(0.015)	(0.011)	(0.021)		
		4.205	-3.487	12.331		
CA1	- -	- -	- -	- -	0.303	
					(0.019)	
					16.005	
CA2	- -	- -	- -	0.036	- -	0.197
				(0.010)		(0.015)
				3.666		13.452
CA3	- -	- -	- -	0.035	- -	- -
				(0.009)		
				3.987		
CA4	- -	- -	- -	- -	- -	- -
PM1	- -	- -	- -	- -	- -	- -

PM2 0.019 - - - - - - - - - -
(0.006)
3.103

PM3 - - - - - - - - - - - -

PM4 - - - - -0.027 - - 0.077 0.077
(0.008) (0.014) (0.013)
-3.437 5.495 6.104

PB1 - - - - - - - - - - -0.039
(0.014)
-2.826

PB2 -0.033 - - - - - - - - 0.038
(0.008) (0.015)
-4.344 2.596

PB3 - - - - - - - - -0.076 -0.070
(0.014) (0.014)
-5.482 -5.078

THETA-EPS

	CA3	CA4	PM1	PM2	PM3	PM4
CA3	0.109					
	(0.010)					
	10.443					
CA4	- -	0.313				
		(0.021)				
		15.140				

PM1 - - 0.040 0.223
(0.013) (0.018)
3.113 12.644

PM2 - - - - - - 0.182
(0.016)
11.177

PM3 - - 0.050 - - - - 0.281
(0.014) (0.019)
3.678 15.109

PM4 - - - - - - -0.099 - - 0.312
(0.014) (0.025)
-7.187 12.358

PB1 - - - - - - - - - - 0.069
(0.015)
4.495

PB2 - - - - -0.040 - - - - - -
(0.013)
-3.067

PB3 - - - - - - - - - - - -

THETA-EPS

	PB1	PB2	PB3
PB1	0.277		
	(0.022)		
	12.424		

PB2 - - 0.320

(0.024)

13.290

PB3 - - - - 0.272

(0.022)

12.536

Squared Multiple Correlations for Y - Variables

TA1	TA2	TA3	TA4	CA1	CA2
0.921	0.688	0.810	0.712	0.506	0.720

Squared Multiple Correlations for Y - Variables

CA3	CA4	PM1	PM2	PM3	PM4
0.842	0.656	0.652	0.641	0.514	0.584

Squared Multiple Correlations for Y - Variables

PB1	PB2	PB3
0.682	0.637	0.671

THETA-DELTA-EPS

	TA1	TA2	TA3	TA4	CA1	CA2
CP1	- -	- -	- -	- -	- -	- -
CP2	- -	- -	- -	- -	- -	- -

CP3	--	--	0.018	--	--	--
			(0.006)			
			3.263			
CP4	--	--	--	--	--	--
PV1	--	--	--	--	--	--
PV2	--	--	--	--	--	--
PV3	--	--	--	--	--	--
PV4	--	--	--	--	--	--
PE1	--	--	--	--	--	--
PE2	--	--	--	--	--	--
PE3	--	--	--	--	--	--
PE4	--	--	--	--	--	--
SN1	--	--	--	--	--	--
SN2	--	--	--	--	--	--
SN3	--	--	--	--	--	--
SN4	--	--	--	--	--	--
SK1	--	--	0.024	--	--	--
			(0.007)			
			3.645			

SK2 - - 0.039 - - - - - - - -
(0.009)
4.222

SK3 - - - - - - - - - - 0.057
(0.011)
5.224

SK4 - - - - - - - - - - - -

SC1 - - - - -0.027 - - - - - -
(0.007)
-4.151

SC2 - - - - - - - - - - - -

SC3 - - - - - - - - - - - -

SC4 - - - - - - - - - - - -

THETA-DELTA-EPS

	CA3	CA4	PM1	PM2	PM3	PM4
CP1	- -	- -	- -	- -	- -	- -
CP2	- -	- -	- -	- -	- -	- -
CP3	- -	- -	- -	- -	- -	- -
CP4	- -	0.040	- -	- -	- -	- -
		(0.012)				
		3.248				

PV1	--	--	--	--	--	--
PV2	--	--	--	--	--	--
PV3	--	--	--	--	--	--
PV4	--	--	--	--	--	--
PE1	--	--	--	--	--	--
PE2	--	--	--	--	--	--
PE3	--	--	--	--	--	--
PE4	--	--	--	--	--	--
SN1	--	--	--	--	--	--
SN2	--	--	--	--	--	--
SN3	--	--	--	--	--	--
SN4	--	--	--	--	--	--
SK1	--	--	--	--	--	--
SK2	--	--	--	--	--	--
SK3	--	--	--	--	--	0.069
				(0.014)		
				5.044		
SK4	--	--	--	--	--	--
SC1	--	--	--	--	--	--

SC2	--	--	--	--	--	--
SC3	--	--	--	--	--	--
SC4	--	--	--	--	0.040	--
					(0.010)	
					4.086	

THETA-DELTA-EPS

	PB1	PB2	PB3
CP1	--	--	--
CP2	--	--	--
CP3	--	--	--
CP4	--	--	--
PV1	--	--	--
PV2	--	--	--
PV3	--	--	--
PV4	--	--	--
PE1	--	--	--
PE2	--	--	--
PE3	--	--	--

PE4 - - - - - -

SN1 - - - - - -

SN2 - - - - - -

SN3 - - - - - -

SN4 - - - - - -

SK1 - - - - - -

SK2 - - - - - -

SK3 - - - - - -

SK4 - - - - - -

SC1 - - - - - -

SC2 - - - - - -

SC3 - - - - - -

SC4 - - - - - -

THETA-DELTA

	CP1	CP2	CP3	CP4	PV1	PV2
CP1	0.217					
	(0.020)					
	10.654					

CP2	0.049	0.248				
	(0.018)	(0.027)				
	2.801	9.145				
CP3	- -	0.036	0.145			
		(0.017)	(0.016)			
		2.141	9.175			
CP4	-0.062	-0.046	- -	0.186		
	(0.016)	(0.017)		(0.020)		
	-3.925	-2.684		9.330		
PV1	- -	- -	- -	- -	0.140	
				(0.009)		
				15.782		
PV2	- -	- -	- -	- -	- -	0.019
					(0.004)	
					4.168	
PV3	- -	- -	- -	- -	- -	- -
PV4	- -	- -	- -	- -	- -	- -
PE1	- -	- -	- -	- -	- -	- -
PE2	- -	- -	- -	- -	- -	- -
PE3	- -	- -	- -	- -	- -	- -
PE4	- -	- -	- -	- -	- -	- -
SN1	- -	- -	- -	- -	- -	- -

SN2 -- -- -- -- -- --

SN3 -- -- -- -- -- --

SN4 -- -- -- -- -- --

SK1 -- -- -- -- -- --

SK2 -- -- -- -- -- --

SK3 -- -- -- -- -- --

SK4 -- -- -- -- -- --

SC1 -- -- -- -- -- --

SC2 -- -- -- -- -- --

SC3 -- -- -- -- -- --

SC4 -- 0.037 -- -- -- --
(0.009)
4.282

THETA-DELTA

	PV3	PV4	PE1	PE2	PE3	PE4
PV3	0.085					
	(0.007)					
	12.757					
PV4	--	0.233				
		(0.014)				

16.450

PE1 - - - - 0.232
(0.020)
11.797

PE2 -0.028 - - - - 0.246
(0.007) (0.026)
-4.063 9.404

PE3 - - - - - - 0.072 0.264
(0.019) (0.020)
3.813 13.292

PE4 - - - - - - -0.079 - - 0.169
(0.015) (0.018)
-5.392 9.299

SN1 - - - - - - - - - - - -

SN2 - - - - - - - - - - - -

SN3 - - - - - - - - - - - -

SN4 - - - - - - - - - - - -

SK1 - - - - - - - - - - - -

SK2 - - - - - - - - 0.059 - -
(0.012)
5.028

SK3 - - - - - - - - - - - -

SK4 - - - - - - - - 0.028 - -
(0.010)
2.806

SC1 - - - - -0.028 - - - - - -
(0.011)
-2.628

SC2 - - - - - - -0.030 - - - -
(0.008)
-3.585

SC3 - - - - - - - - - - - -

SC4 - - - - - - - - - - - -

THETA-DELTA

	SN1	SN2	SN3	SN4	SK1	SK2
SN1	0.185					
	(0.014)					
	12.807					
SN2	0.109	0.121				
	(0.012)	(0.012)				
	9.145	10.216				
SN3	- -	- -	0.107			
			(0.012)			
			9.104			

SN4 - - - - - - 0.223
(0.016)
14.288

SK1 - - - - - - - - 0.161
(0.018)
8.879

SK2 - - - - - - - - -0.121 0.165
(0.015) (0.022)
-7.800 7.654

SK3 - - - - - - - - -0.072 -0.055
(0.016) (0.017)
-4.650 -3.200

SK4 - - - - - - - - - - - -

SC1 - - - - - - - - - - - -

SC2 - - - - - - - - - - - -

SC3 - - - - - - - - - - - -

SC4 - - - - - - - - - - - -

THETA-DELTA

	SK3	SK4	SC1	SC2	SC3	SC4
SK3	0.199					
	(0.022)					
	8.920					

SK4	- -	0.203				
	(0.018)					
	11.107					
SC1	- -	- -	0.220			
		(0.015)				
		14.426				
SC2	- -	- -	- -	0.152		
			(0.012)			
			12.215			
SC3	- -	- -	- -	- -	0.061	
				(0.011)		
				5.474		
SC4	- -	0.027	-0.105	- -	-0.060	0.084
	(0.008)	(0.012)		(0.014)	(0.020)	
	3.450	-8.505		-4.169	4.290	

Squared Multiple Correlations for X - Variables

CP1	CP2	CP3	CP4	PV1	PV2
0.617	0.523	0.722	0.680	0.658	0.953

Squared Multiple Correlations for X - Variables

PV3	PV4	PE1	PE2	PE3	PE4
0.815	0.542	0.753	0.732	0.691	0.811

Squared Multiple Correlations for X - Variables

SN1	SN2	SN3	SN4	SK1	SK2
0.666	0.786	0.814	0.630	0.753	0.797

Squared Multiple Correlations for X - Variables

SK3	SK4	SC1	SC2	SC3	SC4
0.754	0.756	0.712	0.802	0.921	0.902

Goodness of Fit Statistics

Degrees of Freedom = 628

MINimum Fit Function Chi-Square = 1326.290 (P = 0.0)

Normal Theory Weighted Least Squares Chi-Square = 1241.338 (P = 0.0)

Estimated Non-centrality Parameter (NCP) = 613.338

90 Percent Confidence Interval for NCP = (517.016 ; 717.435)

MINimum Fit Function Value = 2.214

Population Discrepancy Function Value (F0) = 1.024

90 Percent Confidence Interval for F0 = (0.863 ; 1.198)

Root Mean Square Error of Approximation (RMSEA) = 0.0404

90 Percent Confidence Interval for RMSEA = (0.0371 ; 0.0437)

P-Value for Test of Close Fit (RMSEA < 0.05) = 1.00

Expected Cross-Validation Index (ECVI) = 2.580

90 Percent Confidence Interval for ECVI = (2.419 ; 2.754)

ECVI for Saturated Model = 2.604

ECVI for Independence Model = 87.386

Chi-Square for Independence Model with 741 Degrees of Freedom = 52266.401

Independence AIC = 52344.401

Model AIC = 1545.338

Saturated AIC = 1560.000

Independence CAIC = 52554.881

Model CAIC = 2365.672

Saturated CAIC = 5769.605

Normed Fit Index (NFI) = 0.975

Non-Normed Fit Index (NNFI) = 0.984

Parsimony Normed Fit Index (PNFI) = 0.826

Comparative Fit Index (CFI) = 0.986

Incremental Fit Index (IFI) = 0.986

Relative Fit Index (RFI) = 0.970

Critical N (CN) = 323.189

Root Mean Square Residual (RMR) = 0.0304

Standardized RMR = 0.0446

Goodness of Fit Index (GFI) = 0.904

Adjusted Goodness of Fit Index (AGFI) = 0.881

Parsimony Goodness of Fit Index (PGFI) = 0.728

TI COMPUTER CRIME PROTECTION BEHAVIOR

Total and Indirect Effects

Total Effects of KSI on ETA

	CP	PV	PE	SN	SK	SC
TA	0.340	0.113	0.149	0.215	- -	- -
	(0.045)	(0.040)	(0.042)	(0.045)		
	7.601	2.811	3.583	4.750		
CA	0.199	- -	- -	0.148	0.483	-0.105
	(0.041)		(0.036)	(0.046)	(0.033)	
	4.828		4.080	10.605	-3.131	

PM	0.175	0.029	0.038	0.121	0.214	-0.046
	(0.026)	(0.011)	(0.012)	(0.022)	(0.027)	(0.015)
	6.831	2.578	3.130	5.520	7.820	-3.028
PB	0.185	0.011	0.014	0.134	0.372	-0.080
	(0.033)	(0.005)	(0.006)	(0.029)	(0.036)	(0.026)
	5.554	1.967	2.179	4.651	10.181	-3.119

Indirect Effects of KSI on ETA

	CP	PV	PE	SN	SK	SC
TA	- -	- -	- -	- -	- -	- -
CA	- -	- -	- -	- -	- -	- -
PM	0.175	0.029	0.038	0.121	0.214	-0.046
	(0.026)	(0.011)	(0.012)	(0.022)	(0.027)	(0.015)
	6.831	2.578	3.130	5.520	7.820	-3.028
PB	0.185	0.011	0.014	0.134	0.372	-0.080
	(0.033)	(0.005)	(0.006)	(0.029)	(0.036)	(0.026)
	5.554	1.967	2.179	4.651	10.181	-3.119

Total Effects of ETA on ETA

	TA	CA	PM	PB
TA	- -	- -	- -	- -
CA	- -	- -	- -	- -
PM	0.257	0.443	- -	- -

(0.040) (0.045)
6.419 9.778

PB 0.094 0.769 0.180 - -
(0.034) (0.051) (0.042)
2.747 15.105 4.282

Largest Eigenvalue of B*B' (Stability Index) is 0.727

Indirect Effects of ETA on ETA

	TA	CA	PM	PB
TA	- -	- -	- -	- -
CA	- -	- -	- -	- -
PM	- -	- -	- -	- -
PB	0.046	0.080	- -	- -
	(0.013)	(0.019)		
	3.585	4.132		

Total Effects of ETA on Y

	TA	CA	PM	PB
TA1	0.718	- -	- -	- -
TA2	0.654	- -	- -	- -
	(0.024)			
	27.103			

TA3 0.652 - - - - - -
(0.019)
34.296

TA4 0.807 - - - - - -
(0.028)
28.895

CA1 - - 0.556 - - - -

CA2 - - 0.712 - - - -
(0.035)
20.066

CA3 - - 0.761 - - - -
(0.035)
21.800

CA4 - - 0.772 - - - -
(0.039)
19.566

PM1 0.166 0.287 0.647 - -
(0.026) (0.029)
6.419 9.778

PM2 0.147 0.253 0.571 - -
(0.023) (0.026) (0.029)
6.389 9.914 19.502

PM3 0.140 0.242 0.545 - -
(0.022) (0.025) (0.029)
6.334 9.494 19.066

PM4 0.170 0.294 0.662 - -

(0.026) (0.030) (0.035)
6.466 9.778 18.931

PB1 0.073 0.593 0.139 0.771
(0.027) (0.039) (0.032)
2.747 15.105 4.282

PB2 0.071 0.575 0.135 0.748
(0.026) (0.039) (0.031) (0.034)
2.749 14.769 4.285 21.719

PB3 0.070 0.573 0.134 0.745
(0.026) (0.041) (0.031) (0.033)
2.746 14.117 4.292 22.263

Indirect Effects of ETA on Y

	TA	CA	PM	PB
TA1	- -	- -	- -	- -
TA2	- -	- -	- -	- -
TA3	- -	- -	- -	- -
TA4	- -	- -	- -	- -
CA1	- -	- -	- -	- -
CA2	- -	- -	- -	- -
CA3	- -	- -	- -	- -
CA4	- -	- -	- -	- -

PM1 0.166 0.287 - - - -
(0.026) (0.029)
6.419 9.778

PM2 0.147 0.253 - - - -
(0.023) (0.026)
6.389 9.914

PM3 0.140 0.242 - - - -
(0.022) (0.025)
6.334 9.494

PM4 0.170 0.294 - - - -
(0.026) (0.030)
6.466 9.778

PB1 0.073 0.593 0.139 - -
(0.027) (0.039) (0.032)
2.747 15.105 4.282

PB2 0.071 0.575 0.135 - -
(0.026) (0.039) (0.031)
2.749 14.769 4.285

PB3 0.070 0.573 0.134 - -
(0.026) (0.041) (0.031)
2.746 14.117 4.292

Total Effects of KSI on Y

	CP	PV	PE	SN	SK	SC
TA1	0.244	0.081	0.107	0.154	- -	- -
	(0.032)	(0.029)	(0.030)	(0.032)		
	7.601	2.811	3.583	4.750		
TA2	0.222	0.074	0.097	0.141	- -	- -
	(0.030)	(0.026)	(0.027)	(0.030)		
	7.446	2.803	3.567	4.712		
TA3	0.221	0.074	0.097	0.140	- -	- -
	(0.030)	(0.026)	(0.027)	(0.030)		
	7.492	2.807	3.577	4.733		
TA4	0.274	0.091	0.120	0.173	- -	- -
	(0.037)	(0.033)	(0.034)	(0.037)		
	7.452	2.804	3.566	4.711		
CA1	0.110	- -	- -	0.082	0.269	-0.058
	(0.023)		(0.020)	(0.025)	(0.019)	
	4.828		4.080	10.605	-3.131	
CA2	0.141	- -	- -	0.105	0.344	-0.075
	(0.029)		(0.026)	(0.031)	(0.024)	
	4.893		4.119	11.227	-3.149	
CA3	0.151	- -	- -	0.112	0.367	-0.080
	(0.031)		(0.027)	(0.032)	(0.025)	
	4.908		4.128	11.516	-3.152	
CA4	0.153	- -	- -	0.114	0.373	-0.081
	(0.032)		(0.028)	(0.033)	(0.026)	
	4.854		4.114	11.146	-3.143	

PM1	0.113	0.019	0.025	0.078	0.139	-0.030
	(0.017)	(0.007)	(0.008)	(0.014)	(0.018)	(0.010)
	6.831	2.578	3.130	5.520	7.820	-3.028
PM2	0.100	0.017	0.022	0.069	0.122	-0.026
	(0.015)	(0.006)	(0.007)	(0.012)	(0.016)	(0.009)
	6.819	2.575	3.125	5.519	7.869	-3.030
PM3	0.096	0.016	0.021	0.066	0.117	-0.025
	(0.014)	(0.006)	(0.007)	(0.012)	(0.015)	(0.008)
	6.726	2.572	3.120	5.465	7.666	-3.024
PM4	0.116	0.019	0.025	0.080	0.142	-0.031
	(0.017)	(0.007)	(0.008)	(0.015)	(0.018)	(0.010)
	6.814	2.581	3.136	5.511	7.680	-3.020
PB1	0.142	0.008	0.011	0.103	0.287	-0.062
	(0.026)	(0.004)	(0.005)	(0.022)	(0.028)	(0.020)
	5.554	1.967	2.179	4.651	10.181	-3.119
PB2	0.138	0.008	0.011	0.100	0.278	-0.060
	(0.025)	(0.004)	(0.005)	(0.022)	(0.028)	(0.019)
	5.545	1.968	2.181	4.642	10.066	-3.116
PB3	0.138	0.008	0.010	0.100	0.277	-0.060
	(0.025)	(0.004)	(0.005)	(0.021)	(0.027)	(0.019)
	5.552	1.967	2.179	4.650	10.147	-3.118

Time used: 0.593 Seconds

ภาคผนวก จ
ตัวอย่างคำสั่งที่ใช้ในการวิเคราะห์กลุ่มพหุ

1. ตัวอย่างคำสั่งการวิเคราะห์โมเดลที่ไม่มีการกำหนดเงื่อนไขบังคับพารามิเตอร์เท่ากันระหว่างกลุ่มทักษะด้านเทคโนโลยีสารสนเทศ

```
IT People
!DA NI=39 NO=300 NG=2 MA=CM
SY='C:\IT.dsf' NG=2
SE
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
21 22 23 24 /
MO NX=24 NY=15 NK=6 NE=4 LX = FU,FI LY = FU,FI GA = FU,FI BE = SD,FI TD =FU,FI TE = FU,FI
LE
TA CA PM PB
LK
CP PV PE SN SK SC
FR LY(4,1) LY(2,1) LY(3,1) LY(8,2) LY(6,2) LY(7,2) LY(12,3) LY(10,3) LY(11,3) LY(15,4) LY(14,4)
FR LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,2) LX(6,2) LX(7,2) LX(8,2) LX(9,3) LX(10,3) LX(11,3) LX(12,3)
LX(13,4) LX(14,4) LX(15,4) LX(16,4) LX(17,5) LX(18,5) LX(19,5) LX(20,5) LX(21,6) LX(22,6) LX(23,6)
LX(24,6)
FR BE(3,1) BE(3,2) BE(4,1) BE(4,2) BE(4,3) GA(1,1) GA(1,2) GA(1,3) GA(1,4) GA(2,1) GA(2,4) GA(2,5)
GA(2,6)
FR TE(1,1) TE(2,2) TE(3,3) TE(4,4) TE(5,5) TE(6,6) TE(7,7) TE(8,8) TE(9,9) TE(10,10) TE(11,11) TE(12,12)
TE(13,13) TE(14,14) TE(15,15)
FR TD(1,1) TD(2,2) TD(3,3) TD(4,4) TD(5,5) TD(6,6) TD(7,7) TD(8,8) TD(9,9) TD(10,10) TD(11,11)
TD(12,12) TD(13,13) TD(14,14) TD(15,15) TD(16,16) TD(17,17) TD(18,18) TD(19,19) TD(20,20)
TD(21,21) TD(22,22) TD(23,23) TD(24,24)
VA 1.00 LY(1,1)
VA 1.00 LY(5,2)
VA 1.00 LY(9,3)
VA 1.00 LY(13,4)
FR TD(14,13) TE(2,1) TD(24,22) TD(12,9) TH(19,6) TD(2,1) TE(12,10) TH(24,11) TE(12,8) TD(10,9)
TE(12,7) TE(14,6) TD(24,2) TD(10,7) TH(19,10) TH(23,8) TE(15,5) TH(19,12) TH(18,2) TH(20,8) TE(4,2)
PD
```

OU SE TV MI RS SS SC AD=OFF IT=1000 ND=3

NON-IT People

!DA NI=39 NO=300 NG=2 MA=CM

SY='C:\Users\IBM_ADMIN\Desktop\Lisrel_Result\NIT\NIT2.dsf' NG=2

SE

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 /

MO NX=24 NY=15 NK=6 NE=4 LX = PS LY = PS PH = PS PS = PS TD = PS TE = PS GA = PS BE = PS LE

TA CA PM PB

LK

CP PV PE SN SK SC

FR TE(2,1) TD(22,21) TD(18,17) TE(14,6) TH(21,3) TH(4,8) TD(18,12) TE(4,3) TE(13,4) TD(19,17) TH(17,12) TH(1,9) TH(17,6) TD(20,3) TD(3,2) TE(11,8) TE(7,6)

OU SE TV MI RS EF SS SC AD=OFF IT=1000 ND=3

2. ตัวอย่างคำสั่งการวิเคราะห์โมเดลที่มีการกำหนดเงื่อนไขบังคับพารามิเตอร์เท่ากันระหว่างกลุ่มทักษะด้านเทคโนโลยีสารสนเทศ

IT People

!DA NI=39 NO=300 NG=2 MA=CM

SY='C:\IT.dsf' NG=2

SE

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 /

MO NX=24 NY=15 NK=6 NE=4 LX = FU,FI LY = FU,FI GA = FU,FI BE = SD,FI TD =FU,FI TE = FU,FI

LE

TA CA PM PB

LK

CP PV PE SN SK SC

FR LY(4,1) LY(2,1) LY(3,1) LY(8,2) LY(6,2) LY(7,2) LY(12,3) LY(10,3) LY(11,3) LY(15,4) LY(14,4)

FR LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,2) LX(6,2) LX(7,2) LX(8,2) LX(9,3) LX(10,3) LX(11,3) LX(12,3) LX(13,4) LX(14,4) LX(15,4) LX(16,4) LX(17,5) LX(18,5) LX(19,5) LX(20,5) LX(21,6) LX(22,6) LX(23,6) LX(24,6)

FR BE(3,1) BE(3,2) BE(4,1) BE(4,2) BE(4,3) GA(1,1) GA(1,2) GA(1,3) GA(1,4) GA(2,1) GA(2,4) GA(2,5) GA(2,6)

FR TE(1,1) TE(2,2) TE(3,3) TE(4,4) TE(5,5) TE(6,6) TE(7,7) TE(8,8) TE(9,9) TE(10,10) TE(11,11) TE(12,12) TE(13,13) TE(14,14) TE(15,15)

FR TD(1,1) TD(2,2) TD(3,3) TD(4,4) TD(5,5) TD(6,6) TD(7,7) TD(8,8) TD(9,9) TD(10,10) TD(11,11) TD(12,12) TD(13,13) TD(14,14) TD(15,15) TD(16,16) TD(17,17) TD(18,18) TD(19,19) TD(20,20) TD(21,21) TD(22,22) TD(23,23) TD(24,24)

VA 1.00 LY(1,1) LY(5,2) LY(9,3) LY(13,4)

FR TD(14,13) TE(2,1) TD(24,22) TD(12,9) TH(19,6) TD(2,1) TE(12,10) TE(14,6) TH(24,11) TE(12,8) TE(12,7) TD(10,9) TE(15,5) TE(14,1) TE(14,4) TD(19,17)TD(10,7) TD(24,2) TD(21,19) TE(3,2) TE(10,1) TE(9,7) TH(18,2) TD(6,3) TD(20,17) TD(19,18) TD(22,20)

PD

OU SE TV MI RS SS SC AD=OFF IT=1000 ND=3

NON-IT People

!DA NI=39 NO=300 NG=2 MA=CM

SY='C:\NIT.dsf' NG=2

SE

25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 /

MO NX=24 NY=15 NK=6 NE=4 LX = PS LY = PS PH = PS PS = PS TD = PS TE = PS GA = IN BE = IN LE

TA CA PM PB

LK

CP PV PE SN SK SC

FR TE(2,1) TD(22,21) TD(18,17) TD(4,2) TD(18,12) TH(21,3) TE(4,3) TE(13,4) TE(11,8) TD(4,1) TH(4,8)

OU SE TV MI RS EF SS SC AD=OFF IT=1000 ND=3

ประวัติผู้เขียน

ชื่อ	นางสาวศิริรัตน์ ศรีสว่าง
วันเดือนปีเกิด	11 กุมภาพันธ์ 2527
ประสบการณ์ทำงาน	2556-ปัจจุบัน: Process Architect/Governor บริษัท ไอบีเอ็ม โซลูชั่นส์ ดิลิเวอรี่ จำกัด 2549-2556: วิศวกรคอมพิวเตอร์ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ