บทความวิจัย

การวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง

รุ่งโรจน์ สุบรรณจุ้ย*
สาขาวิชาคอมพิวเตอร์ธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ วิทยาเขตระยอง

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 0 3862 7000 ต่อ 551 อีเมล: rungroj.s@fba.kmutnb.ac.th DOI: 10.14416/j.kmutnb.2022.02.008
รับเมื่อ 26 พฤศจิกายน 2563 แก้ไขเมื่อ 23 ธันวาคม 2563 ตอบรับเมื่อ 12 มกราคม 2564 เผยแพร่ออนไลน์ 17 กุมภาพันธ์ 2565

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง และตรวจสอบความสอดคล้องโมเดลโครงสร้างองค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองกับข้อมูลเชิงประจักษ์ กลุ่มตัวอย่างจำนวน 263 คน คัดเลือกแบบเจาะจง เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถามเรื่องการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง ประกอบด้วย 6 องค์ประกอบ มีค่าความเชื่อมั่นภายในเท่ากับ 0.95 วิเคราะห์ข้อมูลโดยใช้โปรแกรม AMOS ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก พบค่าดัชนีทุกตัวผ่านเกณฑ์ (CMIN = 76.23, CMIN/DF = 1.29, *p*-value = 0.06, CFI = 0.98, GFI = 0.96, AGFI = 0.93, RMR = 0.03, SRMR = 0.04 และ RMSEA = 0.03) น้ำหนักองค์ประกอบ 0.44-0.87 มีนัยสำคัญทางสถิติที่ .01 และผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง พบค่าดัชนีทุกตัวผ่านเกณฑ์ (CMIN = 69.05, CMIN/DF = 1.23, *p*-value = 0.11, CFI = 0.99, GFI = 0.96, AGFI = 0.93, RMR = 0.03, SRMR = 0.04 และ RMSEA = 0.03) น้ำหนักองค์ประกอบ 0.22-0.96 มีนัยสำคัญทางสถิติที่ .01 โดยองค์ประกอบที่มีค่าน้ำหนักเรียงจากมากไปหาน้อย ได้แก่ ด้านความมั่นคงปลอดภัย ด้านการกลั่นแกล้งทางไซเบอร์ ด้านตระหนักรู้ ด้านแรงจูงใจ ด้านความรู้ และด้านพฤติกรรม ตามลำดับ เพื่อเป็นแนวทางในการพัฒนาหรือส่งเสริมการป้องกันความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรม

คำสำคัญ: การวิเคราะห์องค์ประกอบเชิงยืนยัน การศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต พนักงานระดับปฏิบัติการ จังหวัดระยอง

การอ้างอิงบทความ: รุ่งโรจน์ สุบรรณจุ้ย, "การวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 32, ฉบับที่ 4, หน้า 1014–1024, ต.ค.–ธ.ค. 2565.

Research Article

A Confirmatory Factor Analysis for the Risk of Internet Threat to Operational Staff in Industrial Business in Rayong Province

Rungroj Subanjui*
Department of Business Computer, Faculty of Business Administration, King Mongkut's University of Technology North Bangkok Rayong Campus, Rayong, Thailand

* Corresponding Author, Tel. 0 3862 7000 Ext. 551, E–mail: rungroj.s@fba.kmutnb.ac.th DOI: 10.14416/j.kmutnb.2022.02.008
Received 26 November 2020 ; Revised 23 December 2020 ; Accepted 12 January 2021; Published online: 17 February 2022

Abstract

The current study aims to: 1) analyze the confirmation factor of the risk of internet threat on operational staff in industrial business in Rayong Province, and 2) verify the consistency between the confirmation factor of the risk of internet threat on operational staff in industrial business in Rayong Province and the empirical data. The sample was purposively selected, accounting for 263 participants. The instrument used was a questionnaire consisting of six components with the internal validity of 0.95. The data was analyzed with AMOS. The results of the first order CFA showed that all indices meet the fit indices criteria (CMIN = 76.23, CMIN/DF = 1.29, *p*-value = 0.06, CFI = 0.98, GFI = 0.96, AGFI = 0.93, RMR = 0.03, SRMR = 0.03 and RMSEA = 0.03), factor loading ranged from 0.44 to 0.87, p = .01. The results of the second order CFA also showed that all indices meet the fit indices criteria (CMIN = 69.05, CMIN/DF = 1.23, *p*-value = 0.11, CFI = 0.99, GFI = 0.96, AGFI = 0.93, RMR = 0.03, SRMR = 0.04 and RMSEA = 0.03), the factor loading ranged from 0.22 to 0.96, p = .01. The components with the factor loading ranging from the highest to the lowest included: Security, Cyberbully, Awareness, Motivation, Knowledge and Behavior, respectively. The results of this study can be applied for improving the prevention of internet threats on the operational staff of industrial business.

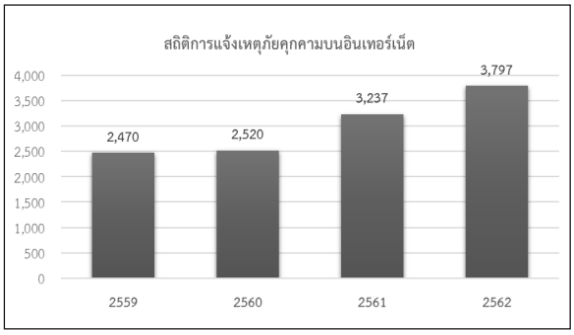
Keywords: Confirmatory Factor Analysis, The Study of Risk for Internet Threat, Operational Staff, Rayong Province

Please cite this article as: R. Subanjui, "A confirmatory factor analysis for the risk of internet threat to operational staff in industrial business in Rayong province," *The Journal of KMUTNB*, vol. 32, no. 4, pp. 1014–1024, Oct.–Dec. 2022 (in Thai).

1. บทนำ

ในปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทในชีวิตประจำวันมากขึ้นเรื่อยๆ จนแทบจะกลายเป็นส่วนหนึ่งของชีวิต บทบาทของเทคโนโลยีสารสนเทศต่อการจัดการความรู้ขององค์กรพบว่า เทคโนโลยีสารสนเทศเป็นเครื่องมือที่ช่วยให้เกิดการติดต่อและเชื่อมโยงคนในองค์กร และการแลกเปลี่ยนเรียนรู้ทำได้เร็วขึ้น [1] เช่น เทคโนโลยีการสื่อสาร (Communication Technology) ช่วยให้บุคลากรสามารถเข้าถึงความรู้ ติดต่อสื่อสาร ค้นหาข้อมูลสารสนเทศผ่านทางเครือข่ายอินทราเน็ต เอ็กซ์ทราเน็ตหรืออินเทอร์เน็ต ปัจจุบันมีผู้กล่าวถึงเทคโนโลยีสารสนเทศอย่างกว้างขวาง โดยจะรู้จักกันทั่วไปในชื่อสั้นๆ ว่า ไอที (IT) เทคโนโลยีสารสนเทศนั้นมีลักษณะเด่นคือมีการเปลี่ยนแปลงที่รวดเร็วมาก เทคโนโลยีใหม่ๆ ที่ทันสมัยเกิดขึ้นมาเรื่อยๆ ทุกวัน ถึงแม้ว่าเทคโนโลยีสารสนเทศจะมีประโยชน์มากมายมหาศาล แต่อีกด้านหนึ่งของเทคโนโลยีสารสนเทศยังแอบแฝงไปด้วยภัยคุกคามต่างๆ โดยเฉพาะภัยคุกคามที่มาจากการใช้อินเทอร์เน็ต ซึ่งเป็นปัญหาหลักสำคัญที่ผู้ใช้ควรตระหนักรู้และหาแนวทางในการเสริมสร้างทักษะ เพื่อเป็นการป้องกันและช่วยให้สามารถใช้เทคโนโลยีสารสนเทศได้อย่างรู้เท่าทันต่อความเสี่ยงที่อาจจะเกิดขึ้นจากภัยคุกคามดังกล่าว [2]

ปัญหาความมั่นคงทางอินเทอร์เน็ตเพิ่มจำนวนอย่างต่อเนื่องตามกระแสเทคโนโลยีเปลี่ยนโลก หรือ “Disruptive Technology” ซึ่งเป็นพัฒนาการของเทคโนโลยีที่มีความก้าวหน้า และมีอิทธิพลต่อการเปลี่ยนแปลงโลก สามารถเปลี่ยนรูปแบบการดำเนินชีวิต การประกอบธุรกิจ และทิศทางเศรษฐกิจโลก ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเทอร์เน็ต หรือที่เรียกว่า Internet of Things (IoT) นอกจากนั้นการมีอิทธิพลเพิ่มขึ้นของเครือข่ายสังคมออนไลน์ โทรศัพท์เคลื่อนที่ประเภทสมาร์ตโฟน หรือ Cloud Computing Services ที่เป็นการให้บริการที่ครอบคลุมถึงการให้ใช้กำลังประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่างๆ แก่ผู้ใช้บริการทางอินเทอร์เน็ตยิ่งก่อให้เกิดภัยคุกคามใหม่ๆ ทางไซเบอร์เพิ่มขึ้นในยุคประเทศไทย 4.0 เช่น ระบบการเงินการธนาคาร



รูปที่ 1 สถิติการแจ้งเหตุภัยคุกคามบนอินเทอร์เน็ตของ พ.ศ. 2559–2562 [4]

ระบบควบคุมการผลิตไฟฟ้า ระบบควบคุมการผลิตน้ำประปา หรือระบบควบคุมโทรศัพท์ ผลกระทบที่เกิดขึ้นก็จะกระทบกับการดำรงชีวิตโดยปกติของประชาชน และหากผลกระทบที่เกิดขึ้นเป็นวงกว้างก็อาจจะเกิดเหตุวุ่นวายจนอาจจะเป็นการจลาจลขึ้นในประเทศได้ [3]

จากข้อมูลพบว่า ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย ได้ทำการสำรวจและจัดทำสถิติภัยคุกคามบนอินเทอร์เน็ตในปี 2559 มีสถิติการแจ้งเหตุภัยคุกคามบนอินเทอร์เน็ต จำนวน 2,470 ครั้ง ใน พ.ศ. 2560 จำนวน 2,520 ครั้ง ใน พ.ศ. 2561 จำนวน 3,237 ครั้ง และใน พ.ศ. 2562 จำนวน 3,797 ครั้ง ดังรูปที่ 1

จากการศึกษาเกี่ยวกับความเสียหายที่เกิดจากภัยคุกคามบนอินเทอร์เน็ตได้แสดงให้เห็นว่าพฤติกรรมการใช้อินเทอร์เน็ตและการใช้เวลาอยู่บนโลกออนไลน์ของคนส่วนใหญ่ในปัจจุบันมีอัตราที่เพิ่มสูงขึ้น กิจกรรมที่นิยมทำบนอินเทอร์เน็ตคือ การทำธุรกรรมออนไลน์ การซื้อขายสินค้าออนไลน์ การใช้สื่อสังคมออนไลน์หรือโซเชียลเน็ตเวิร์ก พฤติกรรมบนโลกออนไลน์ดังกล่าวนำมาซึ่งความเสี่ยงจากการใช้อินเทอร์เน็ตที่ส่งผลกระทบทั้งส่วนบุคคล และต่อองค์การ หน่วยงานระดับชาติได้ทำการสำรวจ และทำการวิจัยความเสี่ยงที่เกิดภัยคุกคามบนอินเทอร์เน็ต ซึ่งพบว่า ในแต่ละปีความเสียหายที่เกิดขึ้นจากอาชญากรรมคอมพิวเตอร์มีแนวโน้มที่จะขยายตัวไปอีกเรื่อยๆ สิ่งที่แฝงมาจากการใช้อินเทอร์เน็ต คือภัยร้ายที่อาจคุกคามชีวิตและทำให้สูญเสีย

ทรัพย์สินเงินทอง รวมไปถึงข้อมูลสำคัญต่างๆ ได้อย่างง่ายดาย เหตุจูงใจในการก่ออาชญากรรมคอมพิวเตอร์ประกอบไปด้วยเหตุผลด้านการเงิน เหตุผลด้านความคิดที่ไม่ตรงกัน เหตุผลด้านความสนุกสนาน อยากรู้อยากเห็น

เนื่องจากภัยคุกคามบนอินเทอร์เน็ตอาจสร้างความเสียหายต่อข้อมูลทั้งในระดับบุคคลและระดับองค์กร ทำให้เกิดผลกระทบต่อความมั่นคงปลอดภัยต่อธุรกรรมบนระบบเครือข่ายอินเทอร์เน็ต ภัยคุกคามเหล่านี้ล้วนแล้วแต่มีการพัฒนาอย่างรวดเร็วตามความก้าวหน้าของเทคโนโลยี การป้องกันหรือติดตามจับกุมการกระทำความผิดเป็นเรื่องที่ทำได้ยากและสลับซับซ้อน ด้วยเหตุนี้ ผู้วิจัยจึงสนใจศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองด้วยการวิเคราะห์โมเดลองค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) เพื่อตรวจสอบความตรงเชิงโครงสร้างของโมเดลสมมติฐานตามทฤษฎีการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยีกับข้อมูลเชิงประจักษ์ และจะได้เป็นประโยชน์ในการนำผลการวิจัยในครั้งนี้ไปใช้เป็นเครื่องมือในการพัฒนาหรือส่งเสริมการป้องกันความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรม

ผู้วิจัยได้มีการศึกษาวรรณกรรมที่เกี่ยวข้องดังนี้

1) แนวคิดเกี่ยวกับความตระหนัก ความหมายของความตระหนัก พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2542 ได้ให้ความหมาย ความตระหนักว่าเป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง โดยสอดคล้องกับพจนานุกรมของ Good [5] โดยได้ให้ความหมายไว้ว่า การแสดงออกจากการระลึกได้หรือจดจำได้ นอกจากนี้ยังมี Bloom และคณะ [6] ได้ให้นิยามความตระหนักไว้ว่า คือ ภาคต่ำสุดทางภาคอารมณ์ ซึ่งความตระหนักนั้นคล้ายกับอารมณ์ความรู้สึก (Affective Domain) แต่ความตระหนักต่างกับความรู้สึกตรงที่ความตระหนักไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนัก

2) แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ Payne และ Goedeke [7] กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง การรังแกและคุกคามผ่านอุปกรณ์อิเล็กทรอนิกส์ เช่น อีเมล โทรศัพท์ มือถือ ข้อความโต้ตอบแบบทันที (IM) ข้อความสั้น (SMS) บล็อก และเว็บไซต์ ซึ่งทำให้เกิดอาชญากรรมคอมพิวเตอร์ได้ การกลั่นแกล้งทางไซเบอร์เป็นการกระทำโดยเจตนาและนำไปสู่ความตึงเครียดทางอารมณ์ ทำให้เกิดความทุกข์อย่างซ้ำๆ จากข้อความ อิเล็กทรอนิกส์หนึ่งข้อความ การกลั่นแกล้งทางไซเบอร์อาจรวมถึงการคุกคามและกล่าวถึงเรื่องทางเพศด้วยการใช้คำพูดที่รุนแรง การดูถูกดูแคลน รวมทั้งการส่งอีเมลไปรบกวนผู้อื่นที่ไม่ต้องการติดต่อกับผู้ส่งด้วย ส่วน Smith [8] กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง พฤติกรรมความก้าวร้าวของบุคคลหรือกลุ่มบุคคลที่เจตนาใช้เครื่องมืออิเล็กทรอนิกส์ทำร้ายเหยื่อ ซึ่งยากที่จะป้องกันตนเอง โดยกระทำอย่างซ้ำๆ ซึ่งการกลั่นแกล้งทางไซเบอร์นั้นเพิ่งเกิดขึ้นในช่วงไม่กี่ปีที่ผ่านมา โดยเกิดขึ้นอย่างมากโดยเฉพาะทางโทรศัพท์มือถือและอินเทอร์เน็ต

3) แนวคิดเกี่ยวกับภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต หมายถึง สิ่งที่อาจก่อให้เกิดความเสียหายแก่คุณสมบัติของข้อมูลหรือสารสนเทศในด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน โดยอาจเกิดจากธรรมชาติหรือบุคคลอาจจะตั้งใจหรือไม่ก็ตาม [9] เช่น ไวรัส เวิร์ม โทรจัน หรือสปายแวร์

2. วัสดุ อุปกรณ์และวิธีการวิจัย

การวิจัยเรื่อง การวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง ได้กำหนดขั้นตอนในการดำเนินการวิจัย ดังนี้

2.1 ประชากรและกลุ่มตัวอย่าง

งานวิจัยได้ข้อกำหนดประชากรและกลุ่มตัวอย่างดังนี้

2.1.1 ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ พนักงานระดับปฏิบัติการในภาคอุตสาหกรรมจังหวัดระยอง จำนวน 170,752 คน [10]

2.1.2 กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ ได้ขนาดกลุ่มตัวอย่างทั้งสิ้น 263 คน โดยผู้วิจัยได้กำหนดขนาดของกลุ่มตัวอย่างจากหลักการวิเคราะห์องค์ประกอบเชิงยืนยันที่ต้อง

มีจำนวน 200 คน [11] ซึ่งเป็นจำนวนที่ถือว่าพอใช้ได้ [12] และเป็นจำนวนที่เหมาะสมกับโมเดลขนาดกลาง [13]

2.2 การสร้างเครื่องที่ใช้ในการวิจัย

ผู้วิจัยได้ทำการสร้างเป็นแบบสอบถาม (Questionnaire) แบ่งเป็น 7 ขั้นตอน ตามลำดับดังนี้

2.2.1 ศึกษาหลักการสร้างแบบสอบถาม และกำหนดกรอบแนวความคิดในการวิจัย

2.2.2 ศึกษาข้อมูลจากหนังสือ เอกสาร บทความ และผลงานวิจัยที่เกี่ยวข้อง รวมทั้งสัมภาษณ์ผู้มีประสบการณ์ในวงการอุตสาหกรรม เพื่อเป็นแนวทางนำมาสร้างข้อคำถาม (Item) ของแบบสอบถาม

2.2.3 กำหนดประเด็นและขอบเขตของคำถามให้สอดคล้องกับวัตถุประสงค์ และประโยชน์ของการวิจัย

2.2.4 ดำเนินการสร้างแบบสอบถามฉบับร่าง

2.2.5 ผู้วิจัยนำแบบสอบถามฉบับร่างที่ได้ผ่านการแก้ไขจากผู้เชี่ยวชาญแล้ว ไปทดลองใช้ (Try-Out) กับกลุ่มประชากรที่มีลักษณะคล้ายคลึงกับประชากรที่ต้องการศึกษา

2.2.6 คำนวณหาค่าอำนาจจำแนกและค่าความเชื่อมั่นของแบบสอบถามฉบับร่างภายหลังการนำไปทดลองใช้ โดยแบบสอบถามที่มีลักษณะเป็นแบบตรวจสอบรายการ (Check-List) จะคำนวณหาค่าอำนาจจำแนก (Discrimination) ด้วยวิธีวิเคราะห์ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation; SD) ในส่วนของแบบสอบถามที่มีลักษณะเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) คำนวณหาค่าความเชื่อมั่นของแบบสอบถาม (Reliability) ด้วยวิธีวิเคราะห์ค่าสัมประสิทธิ์แอลฟา

2.2.7 ปรับปรุงแก้ไขแบบสอบถามตามผลจากการวิเคราะห์ คำนวณหาค่าอำนาจจำแนกและค่าความเชื่อมั่นของแบบสอบถามก่อนนำไปใช้จริง

2.3 ข้อตกลงเบื้องต้น

มีข้อตกลงเบื้องต้นของการวิจัยเป็น 3 ข้อ ดังนี้

2.3.1 การบรรยายรายละเอียดของตัวเลือก “อื่นๆ (โปรดระบุ)” ในข้อคำถามจะแสดงต่อเมื่อผู้ตอบเลือกตอบในตัวเลือกนี้มากกว่าร้อยละ 10 โดยนำรายการที่มีผู้ตอบมากที่สุดเพียง 1 รายการ แสดงไว้ต่อท้ายผลของการวิจัยในหัวข้อนั้นๆ

2.3.2 การคำนวณตัวเลขตัวสุดท้ายจะใช้วิธีการปัดทศนิยม เพิ่มหรือลดเพื่อให้ได้ค่าเต็ม 100% โดยยึดตามหลักการสากลของมาตรฐานการเงินและบัญชีที่ยอมรับกันทั่วไป

2.3.3 กรณีผลการวิเคราะห์งานวิจัยมีค่าเป็น 0 จะไม่อ่านค่าและอธิบายผล

2.4 การตรวจสอบคุณภาพของเครื่องมือ

ผู้วิจัยได้ทำการทดสอบความเที่ยงตรง (Validity) เชิงเนื้อหา และการทดสอบหาค่าความเชื่อมั่นของแบบสอบถาม เพื่อนำแบบสอบถามมาปรับปรุงให้ได้ความเหมาะสมตรงกับเรื่องที่จะศึกษา

2.4.1 การทดสอบหาค่าความเที่ยงตรงเชิงเนื้อหาด้วยการนำแบบสอบถามที่ผู้วิจัยได้พัฒนาขึ้นนำเสนอให้ผู้เชี่ยวชาญและนักวิชาการจำนวน 3 ท่าน ทำการตรวจสอบคุณภาพของความเที่ยงตรงด้านเนื้อหา เพื่อหาค่าความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ที่ต้องการวัด (Item Objective Congruence; IOC) เกณฑ์การตัดสินดัชนีความสอดคล้องระหว่างข้อคำถามกับเนื้อหาหรือจุดประสงค์ (IOC) ถ้า IOC > 0.05 ถือว่า ข้อคำถามนี้ใช้ได้ สอดคล้องกับเนื้อหาหรือจุดประสงค์ ถ้า IOC ≤ 0.05 ถือว่า ข้อคำถามนี้ใช้ไม่ได้ ไม่สอดคล้องกับเนื้อหาหรือจุดประสงค์

2.4.2 การทดสอบหาค่าความเชื่อมั่นผู้วิจัยทำการวัดค่าความเชื่อมั่นด้วยการหาค่าสัมประสิทธิ์แอลฟาของครอนบาก (Cronbach’s Alpha Coefficient) [14] ด้วยคอมพิวเตอร์ นำแบบสอบถามที่ดำเนินการปรับปรุงแล้วนำไปทดลองใช้กับกลุ่มประชากรที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างจำนวน 30 ชุด เพื่อตรวจสอบความสมบูรณ์ของข้อคำถามและวัดความสอดคล้องภายใน (Internal Consistency Model) โดยใช้หลักเกณฑ์สัมประสิทธิ์แอลฟายอมรับที่ค่า α มากกว่าหรือเท่ากับ 0.8 ซึ่งเป็นเกณฑ์ที่สามารถเชื่อถือได้

ตารางที่ 1 ผลการทดสอบหาค่าความเชื่อมั่น

Case Processing Summary	N	%
Case Valid	30	100
Excluded	0	0
Total	30	100
Reliability Statistics Cronbach's Alpha	0.902	

จากตารางที่ 1 ได้เกณฑ์ความเชื่อมั่นที่ 0.902 สรุปว่าแบบสอบถามนี้มีความน่าเชื่อถือหรือมีความเชื่อมั่นสูง

2.5 ขั้นตอนการสังเคราะห์องค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต

ผู้วิจัยได้สังเคราะห์องค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต ดังนี้

2.5.1 ศึกษาเอกสาร แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวกับการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต

2.5.2 คัดเลือกตัวแปรและองค์ประกอบที่เกี่ยวกับความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต ซึ่งประกอบด้วย ด้านตระหนักรู้ ด้านการกลั่นแกล้งทางไซเบอร์ ด้านความมั่นคงปลอดภัย ด้านความรู้ ด้านพฤติกรรม และด้านแรงจูงใจ ดังนั้นองค์ประกอบที่เกี่ยวกับการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตจึงประกอบด้วย 6 องค์ประกอบ พร้อมให้นิยามเชิงปฏิบัติการที่สามารถวัดค่าได้

2.5.3 สร้างกรอบแนวคิดในการวิจัยโดยเสนอโมเดลเชิงสมมติฐานองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตขึ้นเป็นสมมติฐานของการวิจัย

2.5.4 นำผลการสังเคราะห์ไปสร้างแบบสอบถามการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต เพื่อใช้ในการวิจัยต่อไป

2.6 ขั้นตอนการวิเคราะห์องค์ประกอบเชิงสำรวจ การวิเคราะห์องค์ประกอบเชิงสำรวจ

มีขั้นตอนดังนี้

2.6.1 คัดเลือกกลุ่มตัวอย่างจำนวน 263 คน จากกลุ่มประชากรกลุ่มพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง โดยใช้วิธีคัดเลือกแบบเจาะจง

2.6.2 นำข้อมูลจากกลุ่มตัวอย่างมาสกัดองค์ประกอบขั้นต้น และหมุนแกนองค์ประกอบแบบตั้งฉาก เพื่อระบุองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง และพิจารณาคัดเลือกองค์ประกอบที่มีความเหมาะสมดังต่อไปนี้

1) องค์ประกอบต้องมีความแปรปรวนมากกว่า 1 ขึ้นไป

2) ค่าของตัวแปรสังเกตได้แต่ละตัวในแต่ละองค์ประกอบต้องมีค่าน้ำหนักองค์ประกอบตั้งแต่ .30 ขึ้นไป

3) องค์ประกอบแต่ละตัวจะต้องมีตัวแปรสังเกตได้อธิบายตั้งแต่สามตัวขึ้นไป

2.6.3 นำผลการวิเคราะห์องค์ประกอบเชิงสำรวจมาประกอบเป็นกรอบแนวคิดในการสร้างโมเดลองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตเพื่อวิเคราะห์องค์ประกอบเชิงยืนยันต่อไป

2.7 ขั้นตอนการวิเคราะห์องค์ประกอบเชิงยืนยัน การวิเคราะห์องค์ประกอบเชิงยืนยัน

โดยการนำผลการวิเคราะห์องค์ประกอบเชิงสำรวจมาประกอบเป็นกรอบแนวคิดในการสร้างโมเดล มีขั้นตอนการวิเคราะห์ดังนี้

2.7.1 นำข้อมูลจากกลุ่มตัวอย่างมาวิเคราะห์หาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตได้ เพื่อใช้เป็นข้อมูลนำเข้าในโมเดลองค์ประกอบเชิงยืนยัน และพิจารณาลักษณะของตัวแปรสังเกตได้ที่มีความเหมาะสมต่อการนำไปวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ต จากค่าสถิติดังต่อไปนี้

1) Bartlett's Test of Sphericty ต้องมีค่ามากๆ แตกต่างจาก 0 อย่างมีนัยสำคัญทางสถิติ

2) Kaiser-Meyer-Olkin Measure of Sampling Adequacy ต้องมีค่าเข้าใกล้ 1

2.7.2 นำเมทริกซ์สหสัมพันธ์ของข้อมูลมาวิเคราะห์องค์ประกอบเชิงยืนยันด้วยโปรแกรม AMOS เพื่อตรวจสอบ

ความสอดคล้องของโมเดลองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตกับข้อมูลเชิงประจักษ์

3. ผลการทดลอง

การวิจัยครั้งนี้เป็นการวิเคราะห์องค์ประกอบเชิงยืนยันการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง และตรวจสอบความสอดคล้องของโมเดลองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตกับข้อมูลเชิงประจักษ์ ผู้วิจัยได้แบ่งการนำเสนอผลการวิเคราะห์ดังต่อไปนี้

3.1 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ

การวิเคราะห์องค์ประกอบเชิงสำรวจใช้ข้อมูลจากการตอบแบบสอบถามจำนวน 40 ข้อ ใช้กลุ่มตัวอย่างจำนวน 263 คน โดยสกัดองค์ประกอบขั้นตอนด้วยวิธีวิเคราะห์องค์ประกอบหลัก (Principle Component Analysis) และหมุนแกนองค์ประกอบแบบมุมแหลมด้วยวิธีแวริแมกซ์ (Varimax) ผลการวิเคราะห์พิจารณาค่าน้ำหนักองค์ประกอบจำนวนตัวแปรที่ร่วมชี้วัด และค่าความแปรปรวนของแต่ละองค์ประกอบตามเกณฑ์ที่กำหนดได้จำนวน 6 องค์ประกอบ ได้แก่ ด้านตระหนักรู้ ด้านการกลั่นแกล้งทางไซเบอร์ ด้านความมั่นคงปลอดภัย ด้านความรู้ ด้านพฤติกรรม และด้านแรงจูงใจ เนื่องจากผู้วิจัยพิจารณาตามเกณฑ์ที่กำหนดไว้คือ องค์ประกอบจะต้องมีค่าความแปรปรวนมากกว่า 1 ขึ้นไป ค่าของตัวแปรแต่ละตัวในองค์ประกอบจะต้องมีน้ำหนักองค์ประกอบ (Factor Loading) มากกว่า 0.3 ขึ้นไป และองค์ประกอบแต่ละตัวจะต้องมีตัวแปรนั้นๆ บรรยายตั้งแต่ 3 ตัวขึ้นไป การพิจารณาตัวแปรมีค่าน้ำหนักองค์ประกอบต่ำกว่า 0.3 และตัวแปรที่ไม่สามารถชี้วัดองค์ประกอบใดองค์ประกอบหนึ่งถูกตัดออกไป ซึ่งทำให้จำนวนค่าตัวแปรในองค์ประกอบแต่ละด้านที่ได้มีความแตกต่างไปบ้างจากกรอบแนวคิดเดิม ซึ่งองค์ประกอบแต่ละด้านเรียงลำดับตามค่าผลรวมความแปรปรวนจากมากไปน้อย

ผลการวิเคราะห์องค์ประกอบเชิงสำรวจของตัวแปรการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง ได้องค์ประกอบ 6 องค์ประกอบ และกำหนดชื่อองค์ประกอบแต่ละด้าน โดยพิจารณาจากลักษณะที่ตัวแปรเหล่านั้นมุ่งชี้ร่วมกันตามกรอบแนวคิด ทฤษฎี เพื่อให้ได้ชื่อองค์ประกอบสำหรับบ่งชี้ด้านนั้นๆ ได้ดังตารางที่ 1

ตารางที่ 2 สรุปผลการวิเคราะห์องค์ประกอบเชิงสำรวจของตัวแปรการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง

ชื่อองค์ประกอบ	ตัวแปร (ข้อ)
องค์ประกอบที่ 1 ด้านตระหนักรู้	11
องค์ประกอบที่ 2 ด้านการกลั่นแกล้งทางไซเบอร์	9
องค์ประกอบที่ 3 ด้านความมั่นคงปลอดภัย	5
องค์ประกอบที่ 4 ด้านความรู้	6
องค์ประกอบที่ 5 ด้านพฤติกรรม	4
องค์ประกอบที่ 6 ด้านแรงจูงใจ	5
รวมทั้งหมด	40

จากตารางที่ 2 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจของตัวแปรการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง ประกอบด้วย ด้านตระหนักรู้ จำนวน 11 ตัวแปร ด้านการกลั่นแกล้งทางไซเบอร์ จำนวน 9 ตัวแปร ด้านความมั่นคงปลอดภัย จำนวน 5 ตัวแปร ด้านความรู้ จำนวน 6 ตัวแปร ด้านพฤติกรรม จำนวน 4 ตัวแปร และด้านแรงจูงใจ จำนวน 5 ตัวแปร รวมจำนวน 40 ตัวแปร โดยไม่พบตัวแปรที่ไม่ผ่านการพิจารณา คือ มีค่าน้ำหนักองค์ประกอบต่ำกว่า 0.3 และไม่สามารถชี้วัดองค์ประกอบใดองค์ประกอบหนึ่ง

3.2 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก

ในขั้นตอนนี้ผู้วิจัยใช้เทคนิคการวิเคราะห์องค์ประกอบ (Factor Analysis) ซึ่งประกอบด้วยการวิเคราะห์

องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis; EFA) เพื่อใช้ในการจัดหมวดหมู่ตัวแปรจำนวนมากที่นำมาสร้างเป็นกรอบแนวคิดในการวิจัย การวิเคราะห์ปัจจัยเชิงสำรวจยังเป็นเทคนิคหรือเครื่องมือทางสถิติที่ใช้ในการลดตัวแปรหลายๆ ตัวแปรที่มีความซับซ้อนและมีความสัมพันธ์กันให้อยู่ในรูปแบบที่เข้าใจง่าย และการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก (Confirmatory Factor Analysis; CFA) เพื่อตรวจสอบความตรงเชิงโครงสร้างของมาตรวัดตัวแปรสังเกตในการวิจัย

ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก (ก่อนปรับโมเดล) ค่าสถิติไคสแควร์ (CMIN) = 2136.90 ค่าไคสแควร์สัมพัทธ์ (CMIN/DF) = 2.94, *p*-value = 0.00 ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนเปรียบเทียบ (CFI) = 0.77 ค่าดัชนีวัดระดับความกลมกลืน (GFI) = 0.69 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) = 0.65 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือ (RMR) = 0.07 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือในรูปคะแนนมาตรฐาน (SRMR) = 0.08 ดัชนีรากที่สองของความคลาดเคลื่อนในการประมาณค่า (RMSEA) = 0.08 แสดงว่าตัวแบบยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยจึงทำการปรับโมเดล ได้ผลการวิเคราะห์ดังนี้

ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก (หลังปรับโมเดล) ค่าสถิติไคสแควร์ (CMIN) = 76.23 ค่าไคสแควร์สัมพัทธ์ (CMIN/DF) = 1.29, *p*-value = 0.06 ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนเปรียบเทียบ (CFI) = 0.98 ค่าดัชนีวัดระดับความกลมกลืน (GFI) = 0.96 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) = 0.93 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือ (RMR) = 0.03, ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือในรูปคะแนนมาตรฐาน (SRMR) = 0.04 ดัชนีรากที่สองของความคลาดเคลื่อนในการประมาณค่า (RMSEA) = 0.03 ค่าดัชนีผ่านเกณฑ์ทุกตัว แสดงว่าตัวแบบสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ดังตารางที่ 2

เมื่อพิจารณาค่าน้ำหนักองค์ประกอบในรูปคะแนนมาตรฐานของตัวแปรสังเกตได้ในโมเดลการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง พบว่าน้ำหนักองค์ประกอบทั้งหมดมีค่าเป็นบวก 0.44-0.87 มีนัยสำคัญทางสถิติที่ระดับ .01 โดยทั่วไปค่าน้ำหนักองค์ประกอบที่ยอมรับได้คือ ±.5 ขึ้นไป [15] โดยองค์ประกอบที่ 1 ด้านตระหนักรู้ (Awareness) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.59–0.82 องค์ประกอบที่ 2 ด้านการกลั่นแกล้งทางไซเบอร์ (Cyberbully) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.76–0.87 องค์ประกอบที่ 3 ด้านความมั่นคงปลอดภัย (Security) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.80–0.81 องค์ประกอบที่ 4 ด้านความรู้ (Knowledge) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.63–0.78 องค์ประกอบที่ 5 ด้านพฤติกรรม (Behavior) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.44–0.77 และองค์ประกอบที่ 7 ด้านแรงจูงใจ (Motivation) มีค่าน้ำหนักองค์ประกอบตั้งแต่ 0.70–0.74 แสดงว่าข้อคำถามทั้ง 40 ข้อนี้ สามารถวัดความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองได้

3.3 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง

ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง (ก่อนปรับโมเดล) ค่าสถิติไคสแควร์ (CMIN) = 178.988 ค่าไคสแควร์สัมพัทธ์ (CMIN/DF) = 2.63 *p*-value = 0.00 ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนเปรียบเทียบ (CFI) = 0.92 ค่าดัชนีวัดระดับความกลมกลืน (GFI) = 0.90 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) = 0.86 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือ (RMR) = 0.06 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือในรูปคะแนนมาตรฐาน (SRMR) = 0.07 ดัชนีรากที่สองของความคลาดเคลื่อนในการประมาณค่า (RMSEA) = 0.07 แสดงว่าตัวแบบยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยจึงทำการปรับโมเดล ได้ผลการวิเคราะห์ดังนี้

ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง (หลังปรับโมเดล) ค่าสถิติไคสแควร์ (CMIN) = 69.05 ค่าไคสแควร์สัมพัทธ์ (CMIN/DF) = 1.23 *p*-value = 0.11 ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนเปรียบเทียบ (CFI) = 0.99 ค่าดัชนีวัดระดับความกลมกลืน (GFI) = 0.96 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) = 0.93 ค่าดัชนีรากที่สองกำลังเฉลี่ยที่เหลือ (RMR) = 0.03 ค่าดัชนีรากที่สองกำลัง

เฉลี่ยที่เหลือในรูปคะแนนมาตรฐาน (SRMR) = 0.04 ดัชนีรากที่สองของความคลาดเคลื่อนในการประมาณค่า (RMSEA) = 0.03 ค่าดัชนีผ่านเกณฑ์ทุกตัว แสดงว่าตัวแบบสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ดังตารางที่ 3 และรูปที่ 2

ตารางที่ 3 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก

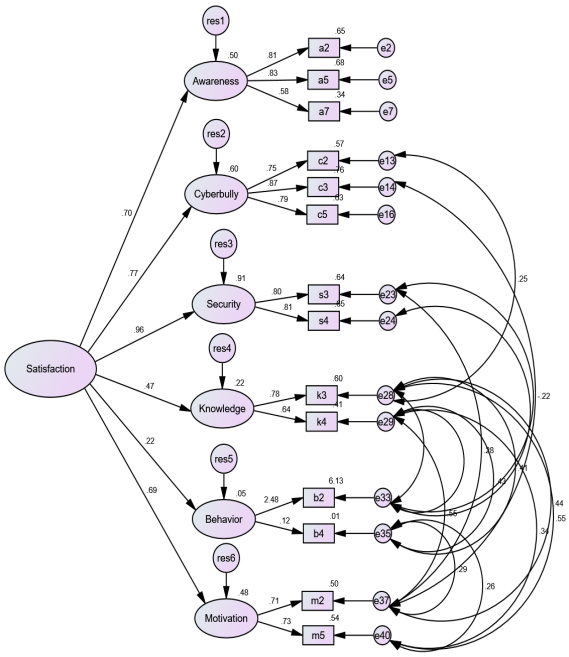
ดัชนีความกลมกลืน	เกณฑ์การพิจารณา [15]	ค่าดัชนีจากการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก	ผลการพิจารณา
CMIN	ไม่มีนัยสำคัญทางสถิติ	76.23	-
CMIN/DF	<2	1.29	ผ่านเกณฑ์
p-value	>0.05	0.06	ผ่านเกณฑ์
CFI	>0.90	0.98	ผ่านเกณฑ์
GFI	>0.90	0.96	ผ่านเกณฑ์
AGFI	>0.90	0.93	ผ่านเกณฑ์
RMR	<0.05	0.03	ผ่านเกณฑ์
SRMR	<0.05	0.04	ผ่านเกณฑ์
RMSEA	<0.05	0.03	ผ่านเกณฑ์

p = .01

ตารางที่ 4 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง

ดัชนีความกลมกลืน	เกณฑ์การพิจารณา [15]	ค่าดัชนีจากการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสอง	ผลการพิจารณา
CMIN	ไม่มีนัยสำคัญทางสถิติ	69.05	-
CMIN/DF	<2	1.23	ผ่านเกณฑ์
p-value	>0.05	0.11	ผ่านเกณฑ์
CFI	>0.90	0.99	ผ่านเกณฑ์
GFI	>0.90	0.96	ผ่านเกณฑ์
AGFI	>0.90	0.93	ผ่านเกณฑ์
RMR	<0.05	0.03	ผ่านเกณฑ์
SRMR	<0.05	0.04	ผ่านเกณฑ์
RMSEA	<0.05	0.03	ผ่านเกณฑ์

p = .01



รูปที่ 2 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับสองหลังการปรับโมเดล

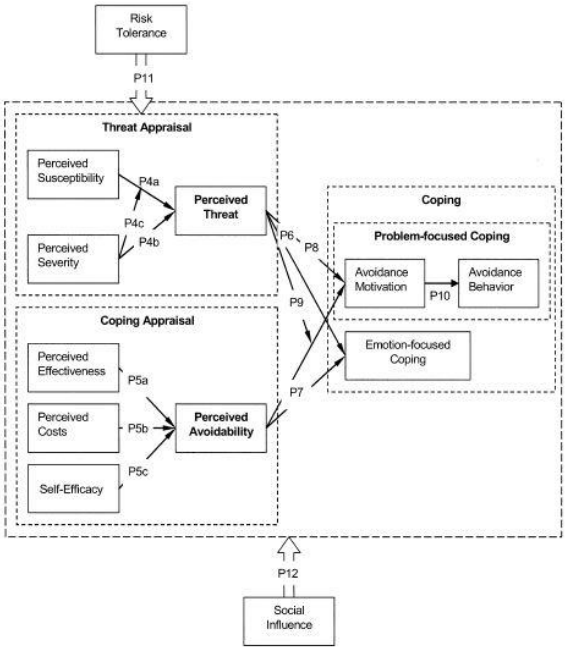
เมื่อพิจารณาค่าน้ำหนักในแต่ละองค์ประกอบ พบว่าน้ำหนักองค์ประกอบทั้งหมดมีค่าเป็นบวก 0.22–0.96 มีนัยสำคัญทางสถิติที่ระดับ .01 โดยองค์ประกอบที่ 3 ด้านความมั่นคงปลอดภัย มีค่าน้ำหนักองค์ประกอบมากที่สุด เท่ากับ 0.96 รองลงมา ได้แก่ องค์ประกอบที่ 2 ด้านการกลั่นแกล้งทางไซเบอร์ มีค่าน้ำหนักองค์ประกอบเท่ากับ 0.77 องค์ประกอบที่ 1 ด้านตระหนักรู้ มีค่าน้ำหนักองค์ประกอบเท่ากับ 0.70 องค์ประกอบที่ 7 ด้านแรงจูงใจ มีค่าน้ำหนักองค์ประกอบเท่ากับ 0.69 องค์ประกอบที่ 4 ด้านความรู้ มีค่าน้ำหนักองค์ประกอบเท่ากับ 0.47 และองค์ประกอบที่ 5 ด้านพฤติกรรม มีค่าน้ำหนักองค์ประกอบเท่ากับ 0.22 ตามลำดับ โดยแต่ละองค์ประกอบมีความเชื่อมั่นในการวัด (R2) อยู่ระหว่าง 0.12–2.48 แสดงว่าองค์ประกอบทั้ง 6 ด้าน สามารถวัดความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองได้ และโมเดลการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการใน

ภาคธุรกิจอุตสาหกรรมจังหวัดระยอง มีความสอดคล้องกับข้อมูลเชิงประจักษ์

4. อภิปรายผลและสรุป

จากผลการวิเคราะห์องค์ประกอบแสดงให้เห็นว่าโมเดลองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยผลการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับแรก และอันดับสอง พบว่า น้ำหนักองค์ประกอบมีค่าเป็นบวก โดยน้ำหนักองค์ประกอบเชิงยืนยันอันดับแรกมีค่าระหว่าง 0.44–0.87 มีนัยสำคัญทางสถิติที่ระดับ 0.01 และน้ำหนักองค์ประกอบเชิงยืนยันอันดับสองมีค่าระหว่าง 0.22–0.96 มีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยองค์ประกอบที่มีค่าน้ำหนักมากที่สุด ได้แก่ ด้านความมั่นคงปลอดภัย รองลงมาได้แก่ ด้านการกลั่นแกล้งทางไซเบอร์ ด้านตระหนักรู้ ด้านแรงจูงใจ ด้านความรู้ และด้านพฤติกรรม ตามลำดับ โดยมีดัชนีวัดระดับความกลมกลืนระหว่างโมเดลกับข้อมูลเชิงประจักษ์ได้ค่า CMIN = 69.05, CMIN/DF = 1.23, *p*-value = 0.11, CFI = 0.99, GFI = 0.96, AGFI = 0.93, RMR = 0.03, SRMR = 0.04 และ RMSEA = 0.03 แสดงว่าโมเดลองค์ประกอบการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยองมีความตรงเชิงโครงสร้าง และตัวแปรทั้ง 40 ตัวแปรเป็นตัวแปรที่สำคัญของการศึกษาความเสี่ยงจากการเกิดภัยคุกคามทางอินเทอร์เน็ตของพนักงานระดับปฏิบัติการในภาคธุรกิจอุตสาหกรรมจังหวัดระยอง

การวิเคราะห์ข้อมูลครั้งนี้ ผู้วิจัยใช้เทคนิคการวิเคราะห์องค์ประกอบเชิงสำรวจและการวิเคราะห์องค์ประกอบเชิงยืนยันกับข้อมูลจำนวน 263 คน เพื่อตรวจสอบสมมติฐานของการวิจัย และผลจากการวิเคราะห์ข้อมูลเชิงสำรวจ จึงทำให้ผลการวิจัยเชื่อถือได้มากขึ้น เนื่องจากผลการวิเคราะห์องค์ประกอบเชิงสำรวจทำให้ลดจำนวนตัวแปรลงเหลือเฉพาะตัวแปรที่สามารถวัดแต่ละองค์ประกอบได้โดยตรง แล้วจึงนำผลที่ได้จากการวิเคราะห์องค์ประกอบเชิงสำรวจไปประกอบกับ



รูปที่ 3 แบบจำลองการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยี [16]

สมมติฐานการวิจัย เพื่อเป็นกรอบแนวคิดในการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับที่หนึ่ง และการวิเคราะห์องค์ประกอบเชิงยืนยันอันดับที่สองอีกครั้งหนึ่ง ทำให้ผลการวิเคราะห์ได้โมเดลที่สอดคล้องกับข้อมูลเชิงประจักษ์อยู่ในเกณฑ์ดี จึงเป็นเทคนิคการวิเคราะห์ข้อมูลที่เหมาะสมสำหรับใช้วิเคราะห์องค์ประกอบเชิงยืนยันแนวคิดหรือทฤษฎีที่มาจากต่างประเทศอย่างแบบจำลองการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยี (Technology Threat Avoidance Mode; TTAT) ที่พัฒนาโดย Liang และ Xue [16] เป็นทฤษฎีแยกแยะผู้ใช้บริการว่ามีความเข้าใจในเทคโนโลยี ซึ่งส่งผลต่อพฤติกรรมการหลีกเลี่ยงความเสี่ยงจากภัยคุกคาม

จากรูปที่ 3 ภายในกรอบการประเมินภัยคุกคาม (Threat Appraisal) ประกอบด้วย การรับรู้ถึงความอ่อนไหวง่าย (Perceived Susceptibility) การรับรู้ถึงความรุนแรง (Perceived Severity) การรับรู้ถึงภัยคุกคาม (Perceived Threat) กรอบการประเมินการรับมือความเสี่ยง (Coping Appraisal) ประกอบด้วย การรับรู้ประสิทธิผล (Perceived

Effectiveness) การรับรู้ค่าใช้จ่าย (Perceived Costs) ประสิทธิภาพของตนเอง (Self-Efficacy) การรับรู้ความสามารถในการหลีกเลี่ยง (Perceived Avoidability) และกรอบการรับมือ (Coping) ประกอบด้วย แรงจูงใจในการหลีกเลี่ยง (Avoidance Motivation) พฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) การรับมือทางอารมณ์ (Emotion-focused) ความเสี่ยงและอิทธิพลทางสังคม (Coping Risk Tolerance and Social Influence)

เอกสารอ้างอิง

[1] B. Boonyakit, *Knowledge Management from Theory to Practice*. Bangkok: Jirawat Express, 2004 (in Thai).

[2] N. Wongyai, "Enhancing information skills in the labor market to prevent the threats of internet," *TLA Bulletin*, vol. 61, no. 2, pp. 64–75, 2017 (in Thai).

[3] National Intelligence Agency. (2019, April). Terrorism prevention guide. National Intelligence Agency, Thailand. [Online]. Available: https://www.nia.go.th/iwebtemp/25631126/91288995910373.pdf

[4] Thailand Computer Emergency Response Team. (2020, September). Internet threat statistics 2016-2019. Thailand Computer Emergency Response Team, Thailand. [Online]. Available:https://www.thaicert.or.th/statistics/statistics.html

[5] C. V. Good, *Dictionary of Education*. New York: McGraw-Hill Book, 1973.

[6] B. S. Bloom, J. T. Hastings, and G. F. Madaus, *Hand Book on Formative and Summative Evaluation of Student Learning*. New York: McGraw-Hill Book, 1971.

[7] D. Payne and S. Goedeke, "Holding together: Caring for clients undergoing assisted reproductive technologies," *Journal of Advanced Nursing*, vol. 60, pp. 645–653, 2007.

[8] J. A. Smith, "Hermeneutics, human sciences and health: Linking theory and practice," *International Journal of Qualitative Studies on Health & Well-Being*, vol. 2, no. 1, pp. 3–11, 2007.

[9] K. Onvimol. (2020, September). Information system security. Songkhla Rajabhat University, Thailand. [Online]. Available: https://sites.google.com/site/ges0503chiwitkabthekhnoloyi/bth-thi-5-khwam-mankhng-plxdphay-khxng-rabb-sarsnthes/7-phay-khukkham

[10] Deparment of Industrial Works. (2019, August). Industry statistics. Department of Industrial Works, Thailand. [Online]. Available: https://www.diw.go.th/hawk/content.php?mode=spss63

[11] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 7th ed. Upper saddle River, NJ: Pearson Education International, 2010.

[12] A. L. Comrey and H. B. Lee, *A First Course in Factor Analysis*, 2nd ed. Psychology Press, 2016.

[13] B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*. Boston, MA: Pearson Education, 2007.

[14] L. J. Cronbach, *Essentials of Psychological Test*, 5th ed. Harper Collins, 1970.

[15] R. E. Schumacker and R. G. Lomax, *A Beginner's Guide to Structural Equation Modeling*, Routledge, 2010.

[16] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly*, vol. 33, no. 1, pp. 71–90, 2009.