การพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร

The Development of Information Security Behavioral Indicators of Naresuan University Staff

พรภัทร เกษาพร (Pornpat Kesaporn) [1] ทัตทริยา เรือนคำ (Tattariya Ruankam) ปอรยา สุวรรณสิทธิ์ (Poraya Suwannasit)

ราชัน ทวีคณะโชติ (Rachan Tawekanachot) ณัฐกานต์ ประจันบาน (Nattakan Prachanban) [2]

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) พัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร 2) ตรวจสอบความตรงเชิงโครงสร้างของตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร กลุ่มตัวอย่าง คือ บุคลากรมหาวิทยาลัยนเรศวร จำนวน 110 คน ใช้การคำนวณจากโปรแกรม SEM ของ Daniel Soper ด้วยการกำหนดค่า Effect size เท่ากับ .40 ค่า Probability level เท่ากับ .05 ค่า Desired power เท่ากับ .5 จำนวนตัวแปรแฝง เท่ากับ 6 จำนวนตัวแปรสังเกตได้ เท่ากับ 23 ได้จำนวนกลุ่มเป้าหมายขั้นต่ำสำหรับการศึกษา เท่ากับ 110 คน เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถามมาตรประมาณค่า 5 ระดับ วิเคราะห์ข้อมูลโดยใช้โปรแกรมสำเร็จรูปหาค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และสัมประสิทธิ์สหสัมพันธ์เพียร์สัน และวิเคราะห์องค์ประกอบเชิงยืนยันด้วยโปรแกรม Mplus เพื่อตรวจสอบความตรงเชิงโครงสร้าง ผลการพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ได้ตัวบ่งชี้หลัก 5 ตัวบ่งชี้ และ 23 ตัวบ่งชี้ย่อย โดย 5 ตัวบ่งชี้หลัก ได้แก่ 1. การรับรู้ภัยคุกคาม 2. การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย 3. การตระหนักถึงความปลอดภัย 4. การใช้ระบบสารสนเทศในองค์กร 5. พฤติกรรมด้านความเสี่ยง ผลการตรวจสอบคุณภาพของตัวบ่งชี้ที่พัฒนาขึ้น พบว่า มีความตรงเชิงโครงสร้าง ค่าน้ำหนักองค์ประกอบของตัวบ่งชี้หลักทั้ง 5 ตัวบ่งชี้ มีนัยสำคัญทางสถิติที่ระดับ .05 โดยมีค่าน้ำหนักองค์ประกอบของตัวแปรสังเกตได้ส่วนใหญ่มีค่าเป็นบวก มีขนาดตั้งแต่ 0.073 – 0.985 และมีนัยสำคัญทางสถิติที่ระดับ .05 ยกเว้นตัวบ่งชี้หลักด้านการตระหนักถึงความปลอดภัย มีตัวบ่งชี้ย่อย จำนวน 1 ตัว มีค่าเป็นลบ เท่ากับ -.043 โดยมีการแปรผันร่วมกับตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศ ประมาณร้อยละ 0.200 – 97.100 ผลการตรวจสอบความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ พบว่า ค่าสถิติไคสแควร์ (χ^2) เท่ากับ 229.324 ค่า df เท่ากับ 196.000 ค่า p-value เท่ากับ 0.052 ซึ่งไม่มีนัยสำคัญทางสถิติ ค่า CFI เท่ากับ 0.970 และค่า TLI เท่ากับ 0.961 มีค่าสูงเข้าใกล้ 1 และค่า RMSEA เท่ากับ 0.039 มีค่าเข้าใกล้ 0

คำสำคัญ ตัวชี้วัด พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศ

[1] นิสิตสาขาวิชาวิจัยและประเมินทางการศึกษา คณะศึกษาศาสตร์ มหาวิทยาลัยนเรศวร pornpatk63@nu.ac.th

[2] อาจารย์ประจำภาควิชาการศึกษา คณะศึกษาศาสตร์ มหาวิทยาลัยนเรศวร nattakanp@nu.ac.th

Abstract

The objectives of this study were 1) to develop information security behavioral indicators of Naresuan University staff 2) to check construct validity of information security behavioral indicators of Naresuan University staff. Sample size is 110 staffs in Naresuan University. The SEM software by Daniel Soper (Soper, 2019) were used to defined by configurated effect size = .40, probability level = .05, desired power = .5, latent variables = 6, observed variables = 23, the minimum sample size is 110 staffs. The research instrument was a five-point rating scale questionnaire. The statistics used to analyze the data were mean ($\bar{X}$), standard deviation (*SD*), Pearson's Correlation Coefficient (r_{xy}) and confirmatory factor analysis through Mplus program in order to check the construct validity. The result of study revealed that the information security behavioral of Naresuan University staff consist of 5 factors and 23 indicators. These 5 factors comprise with percieved threats, training and education, awareness, information using, and risk behavior. The measurement model of this study had a construct validity and fitted nicely to the empirical data. All the factor loadings were statistically significant at .05 significance level. The weighted values of all the observed variables were positive values ranged from 0.073 – 0.985 with statistical significance at .05. Only safety awareness factor showed negative value of indicator at level -.043 which variance with the indicator of information security behavioral of Naresuan University staff between 0.200 – 97.100 percentage. The validation of a goodness of fitted model yielded a Chi-square of 229.324 which closed to df = 196.000 and p = 0.052 which not statistically significant, CFI = 0.970, TLI = 0.961 which hight value and closest to one and RMSEA = 0.039 which closest value to zero.

Keywords: Indicators, Information Security Behavioral

บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร มีความสำคัญและมีแนวโน้มที่จะมีบทบาทมากยิ่งขึ้น ซึ่งทุกองค์กรทั้งภาครัฐและเอกชน ต่างก็นำมาประยุกต์ใช้ในองค์กรกันอย่างแพร่หลาย ดังที่ อภิญญา รัตนโกเมศ (2552) กล่าวว่า เทคโนโลยีสารสนเทศและการสื่อสารจึงนับเป็นเครื่องมืออันทรงพลังที่สามารถจัดการประมวลผลข้อมูลจำนวนมหาศาลให้ได้มาซึ่งสารสนเทศที่มีความถูกต้อง แม่นยำ รวดเร็ว มีประสิทธิภาพและประสิทธิผลมากที่สุด เนื่องจากเทคโนโลยีเป็นเครื่องมือในการดำเนินงานสารสนเทศ นับตั้งแต่การผลิต การจัดเก็บ การประมวลผล การเรียกใช้ การสื่อสารสารสนเทศ การแลกเปลี่ยนและใช้ทรัพยากรสารสนเทศร่วมกันให้เกิดประโยชน์อย่างเต็มที่ ซึ่งวิสุนีย์ เกลากลิ่น (2556) กล่าวว่า ระบบสารสนเทศในองค์กรจะถูกพัฒนาขึ้นเพื่อสนองความต้องการสารสนเทศในการบริหารงานในระดับต่างๆ เช่น 1. ระบบประมวลผลรายการ (TPS: Transaction Processing System) 2. ระบบสารสนเทศเพื่อการจัดการ (MIS: Management Information Systems) 3. ระบบสนับสนุนการตัดสิน (DSS: Decision Support Systems)

มหาวิทยาลัยนเรศวร เป็นหน่วยงานที่ใช้ระบบสารสนเทศในการดำเนินงานตามพันธกิจทั้ง 5 ด้าน ของมหาวิทยาลัย ได้แก่ ด้านการผลิตบัณฑิต ด้านการวิจัย ด้านบริการวิชาการ ด้านทำนุบำรุงศิลปะและวัฒนธรรม และด้านบริหารจัดการ ผ่านระบบสารสนเทศขององค์กร โดยมีผู้ใช้งานทุกระดับ ตั้งแต่นิสิต บุคลากรและผู้บริหาร ซึ่งการใช้เทคโนโลยีสารสนเทศดังกล่าวถึงแม้จะมีประโยชน์มากมายแก่ผู้ใช้งาน แต่ขณะเดียวกันก็สามารถก่อให้เกิดผลกระทบทางลบกับผู้ใช้งาน ซึ่งปัญหาที่พบจากการใช้สารสนเทศโดยไม่ตระหนักถึงความปลอดภัย ได้แก่ ข่าวการแจ้งเตือน สิ่งที่แอบแฝงมาพร้อมกับการดาวน์โหลดและติดตั้งโปรแกรมบางตัวโดยไม่ได้ตั้งใจ หรือ Spyware เป็นโปรแกรมที่แฝงมาขณะใช้อินเทอร์เน็ต ทำให้ข้อมูลต่างๆ เช่น ชื่อ นามสกุล ที่อยู่ อีเมล บัตรเครดิต ในเครื่องคอมพิวเตอร์อาจจะไม่เป็นความลับอีกต่อไป หรือจะเป็นภัยคุกคามจากการที่มีบุคคลอื่นมาใช้คอมพิวเตอร์ของเราโดยไม่ได้รับอนุญาต ทั้งนี้ อาจเป็นเพราะบุคลากรยังไม่มีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร (สุพิชญา อาชวิรดา, 2559)

จากปัญหาที่กล่าวมาข้างต้นแสดงให้เห็นถึงภัยที่มาจากระบบสารสนเทศ ซึ่งอาจจะส่งผลให้เกิดความเสียหายแก่การดำเนินงานภายในมหาวิทยาลัยนเรศวรได้ และจากการศึกษาเอกสาร งานวิจัยที่เกี่ยวข้อง พบว่า ยังไม่ปรากฏงานวิจัยที่ศึกษาเกี่ยวกับการพัฒนาเครื่องมือที่เป็นมาตรฐานซึ่งเกี่ยวกับความปลอดภัยบนระบบสารสนเทศ

ดังนั้นคณะผู้วิจัยจึงมีความสนใจและตระหนักถึงความจำเป็นที่จะต้องศึกษาวิจัยเกี่ยวกับการพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร เพื่อศึกษาว่าตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรเป็นอย่างไร ซึ่งการศึกษาในครั้งนี้จะเป็นข้อมูลที่จำเป็นและนำไปสู่การพัฒนาความปลอดภัยของระบบสารสนเทศในระดับนโยบายของมหาวิทยาลัยต่อไป

วัตถุประสงค์

1. เพื่อพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร
2. เพื่อตรวจสอบความตรงเชิงโครงสร้างของตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร

ระเบียบวิธีวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงสำรวจ (Survey Research) ประชากรที่ศึกษาคือบุคลากรมหาวิทยาลัยนเรศวร ใช้การคำนวณจากโปรแกรม SEM ของ Daniel Soper (Soper, 2019) ด้วยการกำหนดค่า Effect size เท่ากับ .40 ค่า Probability level เท่ากับ .05 ค่า Desired power เท่ากับ .5 จำนวนตัวแปรแฝง เท่ากับ 6 จำนวนตัวแปรสังเกตได้ เท่ากับ 23 ได้จำนวนกลุ่มเป้าหมายขั้นต่ำสำหรับการศึกษา เท่ากับ 110 คน จากการเลือกกลุ่มตัวอย่างแบบบังเอิญ (Accidental sampling) เครื่องมือที่ใช้ คือ แบบสอบถามเป็นแบบมาตรประมาณค่า 5 ระดับ จำนวน 1 ฉบับ โดยใช้ Google Form ในการสร้างแบบสอบถามตามวัตถุประสงค์ของการวิจัยและนิยามศัพท์ และวิเคราะห์ข้อมูลโดยใช้โปรแกรมสำเร็จรูปวิเคราะห์ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และสัมประสิทธิ์สหสัมพันธ์เพียร์สัน และทำการวิเคราะห์องค์ประกอบเชิงยืนยันด้วยโปรแกรม Mplus เพื่อตรวจสอบความตรงเชิงโครงสร้าง

ผลการวิจัย

ผลการพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร โดยผลการตรวจสอบความเที่ยงตรงเชิงเนื้อหาด้วยการหาค่าดัชนีความสอดคล้อง (IOC) ระหว่างข้อคำถามกับนิยามศัพท์ พบว่า มีค่าอยู่ระหว่าง 0.67–1.00 โดยได้ตัวบ่งชี้หลักและตัวบ่งชี้ย่อยสำหรับการประเมินการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร จำนวน 5 ตัวบ่งชี้หลัก ได้แก่ 1. การรับรู้ภัยคุกคาม 2. การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย 3. การตระหนักถึงความปลอดภัย 4. การใช้ระบบสารสนเทศในองค์กร 5. พฤติกรรมด้านความเสี่ยง และ 23 ตัวบ่งชี้ย่อย ดังตารางที่ 1

ตารางที่ 1 ตัวบ่งชี้หลักและตัวบ่งชี้ย่อยสำหรับการประเมินการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร

ตัวบ่งชี้หลัก	ตัวบ่งชี้ย่อย
1. การรับรู้ภัยคุกคาม (Y1)	1.1 ท่านมีความรู้สึกไม่สบายใจเมื่อเพื่อนร่วมงานมาขอใช้เครื่องคอมพิวเตอร์ของท่าน (X1) 1.2 ท่านมีความกังวลใจหากเพื่อนร่วมงานมาใช้เครื่องคอมพิวเตอร์ของท่านโดยไม่ได้รับอนุญาต (X2) 1.3 ท่านมีความกังวลใจต่อพฤติกรรมของเพื่อนร่วมงานที่ใช้โปรแกรมที่ไม่มีมาตรฐาน (X3) 1.4 ท่านรู้สึกกังวลใจว่ามหาวิทยาลัยไม่มีมาตรการรักษาความปลอดภัยของระบบสารสนเทศจะส่งผลให้เกิดความเสียหายต่อผู้ใช้ระบบได้ (X4)
2. การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย (Y2)	2.1 การให้ความรู้เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้บุคลากรในมหาวิทยาลัยสามารถรักษาความปลอดภัยในระบบสารสนเทศของตัวเองมากยิ่งขึ้น (X5) 2.2 หากท่านเข้ารับการฝึกอบรมเกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศภายในองค์กร จะช่วยให้ท่านตระหนักถึงความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์ (X6)

ตัวบ่งชี้หลัก	ตัวบ่งชี้ย่อย
	2.3 การที่บุคลากรไม่ได้รับการฝึกอบรมหรือถ่ายทอดความรู้ที่เพียงพอจะส่งผลต่อการคำนึงถึงความปลอดภัยต่อการใช้ระบบสารสนเทศ (X7) 2.4 ท่านคิดว่าการแลกเปลี่ยนเรียนรู้ระหว่างเพื่อนร่วมงานเกี่ยวกับความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร สามารถสร้างความรู้ความเข้าใจให้กับท่านได้ (X8)
3. การตระหนักถึงความปลอดภัย (Y3)	3.1 ท่านมีการสำรองข้อมูลการทำงานในเครื่องคอมพิวเตอร์ไว้หลายๆ แหล่งเสมอ เพื่อป้องกันการสูญหายของข้อมูล เช่น One Drive, Flash Drive, External Hard Disk (X9) 3.2 ท่านคิดว่าในการกำหนดรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ ควรคำนึงถึงระดับความปลอดภัยในการใช้งานให้มากที่สุด (X10) 3.3 เมื่อท่านได้รับ e-mail ที่มีลิงค์แนบมากับ mail โดยระบุให้ท่านยืนยันข้อมูลส่วนบุคคล ท่านจะอ่านข้อความเหล่านั้นให้เข้าใจก่อนไปที่ลิ้งค์ดังกล่าวเสมอ (X11) 3.4 ท่านจะเปลี่ยนรหัสผ่านในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อสร้างความปลอดภัยในการใช้คอมพิวเตอร์และระบบสารสนเทศในองค์กร (X12)
4. การใช้ระบบสารสนเทศในองค์กร (Y4)	4.1 ท่านปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร (X13) 4.2 ท่านให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับขององค์กร (X14) 4.3 ท่านมีการติดตั้งโปรแกรมสแกนไวรัสไว้ที่คอมพิวเตอร์และสแกนโปรแกรมไวรัสทุกครั้ง (X15) 4.4 ท่านมักจะล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้มีการใช้งาน (X16) 4.5 ท่านมักจะนำอุปกรณ์อื่นๆ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ของท่านโดยไม่มีการสแกนไวรัสก่อนใช้งานทุกครั้ง (X17) 4.6 ท่านมักจะติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของท่าน (X18)
5. พฤติกรรมด้านความเสี่ยง (Y5)	5.1 ท่านได้ติดตั้งโปรแกรมหรือซอฟต์แวร์ที่ไม่ได้รับการยอมรับหรือไม่มีมาตรฐานบนเครื่องคอมพิวเตอร์ในมหาวิทยาลัย (X19) 5.2 ท่านบังเอิญเข้าถึงข้อมูลการสนทนาของผู้อื่นจากโปรแกรม เช่น ไลน์ เฟซบุ๊ก หรืออีเมล โดยไม่ตั้งใจ (X20) 5.3 ท่านทำการคาดเดารหัสผ่านการใช้งานเครื่องคอมพิวพ์เตอร์ของเพื่อนร่วมงาน เพื่อเรียกใช้ข้อมูลประกอบการทำงาน (X21) 5.4 ท่านแจ้งซ่อมเครื่องคอมพิวเตอร์โดยไม่ได้ทำการสำรองข้อมูลสำคัญ เพื่อป้องกันการสูญหาย (X22) 5.5 ท่านจดและแสดงรหัสผ่านเครื่องคอมพิวเตอร์ ไว้ในพื้นที่ที่สะดวกต่อการมองเห็นและไม่ปกปิดข้อมูลดังกล่าว (X23)

ผลการวิเคราะห์ข้อมูลเบื้องต้น พบว่า มีค่าเฉลี่ย อยู่ระหว่าง 1.840 – 4.039 มีส่วนเบี่ยงเบนมาตรฐาน อยู่ระหว่าง 2.897 – 4.583 และค่าสัมประสิทธิ์อัลฟาของครอนบาค พบว่า ค่าสัมประสิทธิ์อัลฟาของครอนบาคของการประเมินพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร มีค่าสูง เท่ากับ .804 และเมื่อพิจารณาเป็นรายตัวบ่งชี้หลัก พบว่า ค่าสัมประสิทธิ์อัลฟาของครอนบาคของการประเมินพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ส่วนใหญ่มีค่าอยู่ในระดับสูง (.794 – .861) ยกเว้นด้านการใช้ระบบสารสนเทศในองค์กร และด้านการตระหนักถึงความปลอดภัยที่มีค่าค่อนข้างต่ำเท่ากับ .596 และ .597 ตามลำดับ ดังตารางที่ 2

ตารางที่ 2 ผลการวิเคราะห์ข้อมูลเบื้องต้น และความเที่ยงแบบความสอดคล้องภายในของตัวบ่งชี้หลักสำหรับการประเมินพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร (N = 110)

ตัวบ่งชี้หลัก	จำนวนตัวบ่งชี้ย่อย	$\bar{X}$	SD	Cronbach's alpha coefficient
1. การรับรู้ภัยคุกคาม (Y1)	4	3.359	4.192	.800
2. การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย (Y2)	4	4.039	3.496	.861
3. การตระหนักถึงความปลอดภัย (Y3)	4	3.805	2.897	.597
4. การใช้ระบบสารสนเทศในองค์กร (Y4)	6	3.488	3.992	.596
5. พฤติกรรมด้านความเสี่ยง (Y5)	5	1.840	4.583	.794
รวม	23			.804

ผลการตรวจสอบความตรงเชิงโครงสร้างด้วยการวิเคราะห์องค์ประกอบเชิงยืนยันของตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร พบว่า โมเดลการวัดตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร มีความตรงเชิงโครงสร้าง โดยโมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ มีค่าสถิติไคสแควร์ (X^2) เท่ากับ 229.324 ซึ่งมีค่าใกล้เคียงกับค่า df เท่ากับ 196.000 ค่า p-value เท่ากับ 0.052 ซึ่งไม่มีนัยสำคัญทางสถิติ ค่า CFI เท่ากับ 0.970 และค่า TLI เท่ากับ 0.961 มีค่าสูงเข้าใกล้ 1 และค่า RMSEA เท่ากับ 0.039 มีค่าเข้าใกล้ 0 นอกจากนี้ พบว่า ค่าน้ำหนักองค์ประกอบของตัวแปรสังเกตได้ส่วนใหญ่มีค่าเป็นบวก ซึ่งมีขนาดตั้งแต่ 0.073 – 0.985 และมีนัยสำคัญทางสถิติที่ระดับ .05 ยกเว้นตัวบ่งชี้ย่อยที่บุคลากรมักจะติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ในเครื่องคอมพิวเตอร์ (X18) มีค่าเป็นลบ เท่ากับ -.043 โดยมีการแปรผันร่วมกับตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ประมาณร้อยละ 0.200 – 97.100 ดังตารางที่ 3

ตารางที่ 3 ผลการตรวจสอบความตรงเชิงโครงสร้างด้วยการวิเคราะห์องค์ประกอบเชิงยืนยันของตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร

ตัวบ่งชี้	β	SE	*t*	R^2
1. การรับรู้ภัยคุกคาม (Y1)				
1.1 ท่านมีความรู้สึกไม่สบายใจเมื่อเพื่อนร่วมงานมาขอใช้เครื่องคอมพิวเตอร์ของท่าน (X1)	.882	.043	20.497	.778
1.2 ท่านมีความกังวลใจหากเพื่อนร่วมงานมาใช้เครื่องคอมพิวเตอร์ของท่านโดยไม่ได้รับอนุญาต (X2)	.836	.045	18.664	.699
1.3 ท่านมีความกังวลใจต่อพฤติกรรมของเพื่อนร่วมงานที่ใช้โปรแกรมที่ไม่มีมาตรฐาน (X3)	.640	.063	10.157	.410
1.4 ท่านรู้สึกกังวลใจว่ามหาวิทยาลัยไม่มีมาตรการรักษาความปลอดภัยของระบบสารสนเทศ จะส่งผลให้เกิดความเสียหายต่อผู้ใช้ระบบได้ (X4)	.418	.090	4.667	.175
2. การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย (Y2)				
2.1 การให้ความรู้เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร จะช่วยให้บุคลากรในมหาวิทยาลัยสามารถรักษาความปลอดภัยในระบบสารสนเทศของตัวเองมากยิ่งขึ้น (X5)	.814	.040	20.232	.663
2.2 หากท่านเข้ารับการฝึกอบรมเกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศภายในองค์กร จะช่วยให้ท่านตระหนักถึงความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์ (X6)	.807	.042	19.184	.651
2.3 การที่บุคลากรไม่ได้รับการฝึกอบรมหรือถ่ายทอดความรู้ที่เพียงพอจะส่งผลต่อการคำนึงถึงความปลอดภัยต่อการใช้ระบบสารสนเทศ (X7)	.751	.049	15.464	.564
2.4 ท่านคิดว่าการแลกเปลี่ยนเรียนรู้ระหว่างเพื่อนร่วมงาน เกี่ยวกับความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร สามารถสร้างความรู้ความเข้าใจให้กับท่านได้ (X8)	.737	.052	14.276	.544
3. การตระหนักถึงความปลอดภัย (Y3)				
3.1 ท่านมีการสำรองข้อมูลการทำงานในเครื่องคอมพิวเตอร์ไว้หลาย ๆ แหล่งเสมอ เพื่อป้องกันการ สูญหายของข้อมูล เช่น One Drive, Flash Drive, External Hard Disk (X9)	.513	.081	6.298	.263
3.2 ท่านคิดว่าในการกำหนดรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ควรคำนึงถึงระดับความปลอดภัยในการใช้งานให้มากที่สุด (X10)	.795	.052	15.274	.632
3.3 เมื่อท่านได้รับ e-mail ที่มีลิงค์แนบมากับ mail โดยระบุให้ท่านยืนยันข้อมูลส่วนบุคคล ท่านจะอ่านข้อความเหล่านั้นให้เข้าใจก่อนไปที่ลิ้งค์	.581	.073	7.920	.338

ตัวบ่งชี้	β	SE	*t*	R^2
ดังกล่าวเสมอ (X11)				
3.4 ท่านจะเปลี่ยนรหัสผ่านในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อสร้างความปลอดภัยในการใช้คอมพิวเตอร์และระบบสารสนเทศในองค์กร(X12)	.073	.102	.711	.005
4. การใช้ระบบสารสนเทศในองค์กร (Y4)				
4.1 ท่านปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร (X13)	.777	.048	16.207	.604
4.2 ท่านให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับขององค์กร(X14)	.887	.040	22.183	.787
4.3 ท่านมีการติดตั้งโปรแกรมสแกนไวรัสไว้ที่คอมพิวเตอร์ และสแกนโปรแกรมไวรัสทุกครั้ง (X15)	.286	.092	3.115	.082
4.4 ท่านมักจะล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้มีการใช้งาน (X16)	.445	.082	5.451	.198
4.5 ท่านมักจะนำอุปกรณ์อื่นๆ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ของท่านโดยไม่มีการสแกนไวรัสก่อนใช้งานทุกครั้ง (X17)	.208	.091	2.286	.043
4.6 ท่านมักจะติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของท่าน (X18)	-043	.065	-.657	.002
5. พฤติกรรมด้านความเสี่ยง (Y5)				
5.1 ท่านได้ติดตั้งโปรแกรมหรือซอฟต์แวร์ที่ไม่ได้รับการยอมรับหรือไม่มีมาตรฐานบนเครื่องคอมพิวเตอร์ในมหาวิทยาลัย (X19)	.244	.076	3.206	.059
5.2 ท่านบังเอิญเข้าถึงข้อมูลการสนทนาของผู้อื่นจากโปรแกรม เช่น ไลน์ เฟซบุ๊ก หรืออีเมล โดยไม่ตั้งใจ (X20)	.822	.042	19.433	.675
5.3 ท่านทำการคาดเดารหัสผ่านการใช้งานเครื่องคอมพิวเตอร์ของเพื่อนร่วมงาน เพื่อเรียกใช้ข้อมูลประกอบการทำงาน (X21)	.985	.033	30.149	.971
5.4 ท่านแจ้งซ่อมเครื่องคอมพิวเตอร์โดยไม่ได้ทำการสำรองข้อมูลสำคัญเพื่อป้องกันการสูญหาย (X22)	.464	.074	6.258	.215
5.5 ท่านจดและแสดงรหัสผ่านเครื่องคอมพิวเตอร์ไว้ในพื้นที่ที่สะดวกต่อการมองเห็นและไม่ปกปิดข้อมูลดังกล่าว (X23)	.462	.082	5.646	.213
ดัชนีวัดความสอดคล้อง	χ^2(196, N = 110) = 229.324, p = .052, CFI = .970, TLI = .961, RMSEA = .039, SRMR = .108			

อภิปรายผลการวิจัย

1. ผลการพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร พบว่า จากการสังเคราะห์แนวคิด ทฤษฎี งานวิจัยที่เกี่ยวข้อง ทำให้ได้ตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ทั้งหมด 5 ตัวบ่งชี้หลัก 23 ตัวบ่งชี้ย่อย ประกอบไปด้วย ตัวบ่งชี้หลักที่ 1 การรับรู้ภัยคุกคาม ตัวบ่งชี้หลักที่ 2 การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย ตัวบ่งชี้หลักที่ 3 การตระหนักถึงความปลอดภัย ตัวบ่งชี้หลักที่ 4 การใช้ระบบสารสนเทศในองค์กร ตัวบ่งชี้หลักที่ 5 พฤติกรรมด้านความเสี่ยง ซึ่งจากการประเมินความเหมาะสมของ ตัวบ่งชี้หลักและตัวบ่งชี้ย่อยของพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวรนั้น ยังคงเดิม แต่มีปรับแก้ข้อความให้มีความชัดเจนสอดคล้องกับนิยามศัพท์มากขึ้น

จากผลการสังเคราะห์ตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวรนั้น ในตัวบ่งชี้หลักที่ 1 การรับรู้ภัยคุกคาม สอดคล้องกับสุพิชญา อาชวิรดา (2559) กล่าวว่า การรับรู้ถึงภัยคุกคามจะส่งผลต่อการตระหนักถึงความปลอดภัยในองค์กร ทั้งนี้ การรักษาความมั่นคงปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรถือเป็นเรื่องสำคัญ องค์กรจำเป็นต้องทบทวนบทบาทและเพิ่มระดับการรักษาความมั่นคงปลอดภัยให้มากขึ้น ในตัวบ่งชี้หลักที่ 2 การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย สอดคล้องกับ Greg Hale (2012) โดยแสดงแบบจำลองในการรักษาความมั่นคงปลอดภัย จะเห็นได้ว่าการฝึกอบรมถือเป็นส่วนสำคัญในการทำให้พนักงานเกิดความตระหนักและยังส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นด้วย เนื่องจากหากผู้ใช้ไม่ทราบถึงกระบวนการในการรักษาความมั่นคงปลอดภัยของข้อมูล มาตรฐาน หรือแม้แต่ภัยที่อาจเกิดขึ้น จึงเป็นเรื่องยาก ที่จะนำความรู้เกี่ยวกับกระบวนการการรักษาความมั่นคงปลอดภัย ในตัวบ่งชี้หลักที่ 3 การตระหนักถึงความปลอดภัย สอดคล้องกับทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior หรือ TPB) กล่าวคือ เมื่อบุคคลเกิดทัศนคติที่มีต่อพฤติกรรม จึงแสดงออกเป็นพฤติกรรม ซึ่งการตระหนักถึงความปลอดภัยจะส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร ในตัวบ่งชี้หลักที่ 4 การใช้ระบบสารสนเทศในองค์กร สอดคล้องกับสุพิชญา อาชวิรดา (2559) กล่าวว่า การใช้งานระบบสารสนเทศอย่างแพร่หลายในชีวิตประจำวัน ทำให้เกิดการคาบเกี่ยวของการใช้งานอุปกรณ์ไอทีสำหรับการทำงานและเรื่องส่วนตัว จึงต้องมีวิธีบริหารจัดการอย่างไรเพื่อให้การทำงานมีความปลอดภัยและป้องกันการสูญหายของข้อมูลได้มากที่สุด และในตัวบ่งชี้หลักที่ 5 พฤติกรรมด้านความเสี่ยง สอดคล้องกับ Nor Natasha Ashira Shamsudin (2019) กล่าวว่า การกระทำจากการใช้ระบบสารสนเทศ ซึ่งส่งผลกระทบหรือสร้างความเสียหายให้กับองค์กร อาจเป็นพฤติกรรมที่สร้างความเสี่ยงโดยเจตนา หรือพฤติกรรมที่สร้างความโดยรู้เท่าไม่ถึงการณ์

2. ผลการตรวจสอบความตรงเชิงโครงสร้างด้วยการวิเคราะห์องค์ประกอบเชิงยืนยันของตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร พบว่า

2.1 ตัวบ่งชี้หลักที่ 1 การรับรู้ภัยคุกคาม ประกอบด้วย 4 ตัวบ่งชี้ย่อย มีค่าน้ำหนักองค์ประกอบระหว่าง 0.418 – 0.882 คือ ท่านมีความรู้สึกไม่สบายใจเมื่อเพื่อนร่วมงานมาขอใช้เครื่องคอมพิวเตอร์ของท่าน ท่านมีความกังวลใจหากเพื่อนร่วมงานมาใช้เครื่องคอมพิวเตอร์ของท่านโดยไม่ได้รับอนุญาต ท่านมีความกังวลใจต่อพฤติกรรมของเพื่อนร่วมงานที่ใช้โปรแกรมที่ไม่มีมาตรฐาน และท่านรู้สึกกังวลใจว่ามหาวิทยาลัยไม่มีมาตรการรักษาความปลอดภัยของระบบสารสนเทศ จะส่งผลให้เกิดความไม่ปลอดภัยในการใช้งานในระบบสารสนเทศ จนเกิดความเสียหายได้ ซึ่งสอดคล้องกับพัทธ์ธีรา สุวรรณสิทธิ์ (2556) ซึ่งได้ทำการวิเคราะห์ปัญหาและวางแผนการพัฒนาระบบสารสนเทศทางการบัญชีของศูนย์พัฒนาโครงการหลวง มูลนิธิโครงการหลวงจังหวัดเชียงใหม่ ทำให้สามารถแบ่งปัญหาหลักของหน่วยงานได้และหาทางแก้ไขปัญหาที่ได้ระบุไว้พร้อม

ทั้งจัดทำแผนพัฒนาระบบสารสนเทศทางการบัญชีโดยประกอบไปด้วยแผนระยะสั้น แผนระยะกลาง และแผนระยะยาว อีกทั้ง สุพิชญา อาชวิรดา (2559) กล่าวว่า การรับรู้ถึงภัยคุกคาม การฝึกอบรมและให้ความรู้ความเข้าใจในระบบสารสนเทศล้วนส่งผลต่อการตระหนักถึงความปลอดภัย และเมื่อพนักงานเกิดความตระหนักแล้วยังส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร ทำให้เกิดความตระหนักในการใช้งานมากขึ้น สุดท้ายก่อให้เกิดระดับการรักษาความมั่นคงปลอดภัยที่สูงขึ้นนั่นเอง

2.2 ตัวบ่งชี้หลักที่ 2 การฝึกอบรมและให้ความรู้ด้านการรักษาความปลอดภัย ประกอบด้วย 4 ตัวบ่งชี้ย่อย มีค่าน้ำหนักองค์ประกอบระหว่าง 0.737 – 0.814 คือ การให้ความรู้เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศในองค์กรจะช่วยให้บุคลากรในมหาวิทยาลัยสามารถรักษาความปลอดภัยในระบบสารสนเทศของตัวเองมากยิ่งขึ้น หากท่านเข้ารับการฝึกอบรมเกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศภายในองค์กรจะช่วยให้ท่านตระหนักถึงความปลอดภัยของข้อมูลในเครื่องคอมพิวเตอร์ การที่บุคลากรไม่ได้รับการฝึกอบรมหรือถ่ายทอดความรู้ที่เพียงพอจะส่งผลต่อการคำนึงถึงความปลอดภัยต่อการใช้ระบบสารสนเทศ และท่านคิดว่าการแลกเปลี่ยนเรียนรู้ระหว่างเพื่อนร่วมงานเกี่ยวกับความปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กรสามารถสร้างความรู้ความเข้าใจให้กับท่านได้ เพื่อให้บุคลากรเกิดความตระหนักและเข้าใจวิธีการรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศ ซึ่งสอดคล้องกับศรวัสย์ สนธิ (2557) กล่าวว่า เจ้าหน้าที่ที่ผ่านการฝึกอบรมมาแล้วจะมีความรู้ความเข้าใจในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและพฤติกรรมความเสี่ยงด้านของข้อมูลต่างๆ ได้ดีกว่าเจ้าหน้าที่ที่ยังไม่ได้รับการฝึกอบรม อีกทั้ง กลุ่มผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (2559) กล่าวว่า ความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นสิ่งที่ผู้ดูแลระบบต้องให้ความสำคัญด้วยประโยชน์ที่หลากหลายของการเข้าถึงได้ทุกที่ทุกเวลา บนเครือข่ายอินเทอร์เน็ต สิ่งที่ต้องพึงระวัง คือ ภัยคุกคามที่มีผลกระทบต่อความปลอดภัยในชีวิตและทรัพย์สินของบุคคลและหน่วยงาน ทั้งในรูปแบบการโจรกรรมข้อมูลส่วนบุคคลอันเป็นความลับ การจารกรรมทางอิเล็กทรอนิกส์

2.3 ตัวบ่งชี้หลักที่ 3 การตระหนักถึงความปลอดภัย ประกอบด้วย 4 ตัวบ่งชี้ย่อย มีค่าน้ำหนักองค์ประกอบระหว่าง 0.073 – 0.795 คือ ท่านมีการสำรองข้อมูลการทำงานในเครื่องคอมพิวเตอร์ไว้หลายๆ แหล่งเสมอ เพื่อป้องกันการสูญหายของข้อมูล เช่น One Drive, Flash Drive, External Hard Disk ท่านคิดว่าในการกำหนดรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ ควรคำนึงถึงระดับความปลอดภัยในการใช้งานให้มากที่สุด เมื่อท่านได้รับ e-mail ที่มีลิงค์แนบมากับ mail โดยระบุให้ท่านยืนยันข้อมูลส่วนบุคคล ท่านจะอ่านข้อความเหล่านั้นให้เข้าใจก่อนไปที่ลิ้งค์ดังกล่าวเสมอ และท่านจะเปลี่ยนรหัสผ่านในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อสร้างความปลอดภัยในการใช้คอมพิวเตอร์และระบบสารสนเทศในองค์กร โดยความสามารถของบุคลากรในการรับรู้ถึงความปลอดภัยจากระบบสารสนเทศโดยการสำรองข้อมูล การกำหนดรหัส การระมัดระวังต่อ e-mail แปลกปลอมในคอมพิวเตอร์ของตนเอง ซึ่งสอดคล้องกับสุพล พรหมมาพันธุ์ (2562) กล่าวว่า ปัจจัยที่มีผลกระทบต่อจริยธรรม และความความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ คือ พฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์มีค่าเฉลี่ยสูงสุด แสดงให้เห็นว่า พฤติกรรมการเรียนรู้ของคนในสังคมเปลี่ยนแปลงไป ด้วยการหันมาใช้คอมพิวเตอร์และสื่อสังคมออนไลน์กันมากขึ้น ไม่ว่าจะเป็น Google Facebook Line YouTube ส่วนด้านที่มีค่าเฉลี่ยต่ำที่สุด คือ ด้านความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) อันเป็นการบ่งชี้ว่าผู้คนส่วนหนึ่งยังขาดความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ นอกจากนี้ บุษบา ไชยยะนาค และโกวิท รพีพิศาล (2561) กล่าวว่า พนักงานส่วนใหญ่มีความรู้ความเข้าใจต่อการรักษาความมั่นคงปลอดภัยของ สารสนเทศภายในบริษัทมากที่สุด ตัวชี้วัดที่สำคัญที่ใช้วัดความตระหนักรู้ 3 ประการ คือ ความรู้ความเข้าใจ ทัศนคติ และพฤติกรรม

2.4 ตัวบ่งชี้หลักที่ 4 การใช้ระบบสารสนเทศในองค์กร ประกอบด้วย 6 ตัวบ่งชี้ย่อย มีค่าน้ำหนักองค์ประกอบระหว่าง -0.043 – 0.887 คือ ท่านปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร ท่านให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับขององค์กร ท่านมีการติดตั้งโปรแกรมสแกนไวรัสไว้ที่คอมพิวเตอร์และสแกนโปรแกรมไวรัสทุกครั้ง ท่านมักจะล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้มีการใช้งาน ท่านมักจะนำอุปกรณ์อื่นๆ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ของท่านโดยไม่มีการสแกนไวรัสก่อนใช้งานทุกครั้ง และท่านมักจะติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของท่าน โดยความสามารถของบุคลากรในการให้ความสำคัญกับการจัดเก็บข้อมูลที่เป็นความลับ รวมถึงการใช้อุปกรณ์โดยคำนึงถึงความปลอดภัยและการรับรู้ถึงมาตรการที่ควรปฏิบัติต่อความปลอดภัยของการใช้ระบบสารสนเทศในองค์กร ซึ่งสอดคล้องกับอภิญญา รัตนโกเมศ (2552) กล่าวว่า มีการใช้เทคโนโลยีสารสนเทศเพื่อการบริหารเกี่ยวกับการเรียนการสอน อยู่ในระดับมาก นอกจากนี้ สุรัตน์ ไชยชมพู (2556) กล่าวว่า การบริหารจัดการที่ดี เพื่อนำระบบสารสนเทศไปใช้กับระบบการจัดการภายในที่ลดหลั่นกันลงไปตามระดับการบริหารจัดการและระดับความรับผิดชอบตามอำนาจหน้าที่ นอกจากนี้ยังต้องมีการปรับตัวขององค์กรในยุคสารสนเทศโดยเฉพาะการพัฒนาบุคลากรที่รับผิดชอบเพื่อให้ก้าวทันเทคโนโลยีอนาคตอย่างต่อเนื่อง

2.5 ตัวบ่งชี้หลักที่ 5 พฤติกรรมด้านความเสี่ยง ประกอบด้วย 5 ตัวบ่งชี้ย่อย มีค่าน้ำหนักองค์ประกอบระหว่าง 0.244 – 0.985 คือ ท่านได้ติดตั้งโปรแกรมหรือซอฟต์แวร์ที่ไม่ได้รับการยอมรับหรือไม่มีมาตรฐานบนเครื่องคอมพิวเตอร์ในมหาวิทยาลัย ท่านบังเอิญเข้าถึงข้อมูลการสนทนาของผู้อื่นจากโปรแกรม เช่น ไลน์ เฟซบุ๊กหรืออีเมล โดยไม่ตั้งใจ ท่านทำการคาดเดารหัสผ่านการใช้งานเครื่องคอมพิวเตอร์ของเพื่อนร่วมงาน เพื่อเรียกใช้ข้อมูลประกอบการทำงาน ท่านแจ้งซ่อมเครื่องคอมพิวเตอร์โดยไม่ได้ทำการสำรองข้อมูลสำคัญ เพื่อป้องกันการสูญหาย และท่านจดและแสดงรหัสผ่านเครื่องคอมพิวเตอร์ไว้ในพื้นที่ที่สะดวกต่อการมองเห็นและไม่ปกปิดข้อมูลดังกล่าว โดยการกระทำหรือการปฏิบัติของบุคลากรที่อาจเกิดขึ้นจากการใช้ระบบสารสนเทศ ซึ่งเป็นพฤติกรรมที่สร้างความเสี่ยงโดยเจตนา หรือโดยรู้เท่าไม่ถึงการณ์ ซึ่งสอดคล้องกับวรัญญาภรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย (2558) กล่าวว่า ประเด็นความเสี่ยงด้าน ICT ของหน่วยงานของรัฐมีลักษณะที่คล้ายกัน และมีสาเหตุหลักมาจากงบประมาณที่ได้รับน้อยกว่างบประมาณที่กำหนด การขาดแคลนบุคลากรด้าน ICT และการบริหารจัดการและขั้นตอนการดำเนินการที่ไม่เอื้อต่อการตอบสนองด้าน ICT อีกทั้ง สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์(2562) กล่าวว่า เมื่อผู้ประกอบธุรกิจมีการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เพียงพอเหมาะสมแล้ว ย่อมส่งผลต่อองค์กรในการสร้างความมั่นใจในการปรับใช้หรือพัฒนาเทคโนโลยีสารสนเทศในบริการหรือผลิตภัณฑ์ใหม่ รวมทั้งเสริมสร้างหรือพัฒนากระบวนการการดำเนินธุรกิจในปัจจุบัน นอกจากนี้ ยังเป็นการสร้างข้อได้เปรียบทางด้านธุรกิจที่ยั่งยืน

โมเดลตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวรที่พัฒนาขึ้นสอดคล้องกับข้อมูลเชิงประจักษ์ มีค่าสถิติวัดระดับความกลมกลืนระหว่างโมเดลกับข้อมูลเชิงประจักษ์ ดังนี้ ค่าสถิติไคสแควร์เท่ากับ 229.324 ที่องศาอิสระเท่ากับ 196.000 ค่าดัชนีวัดระดับความกลมกลืนเปรียบเทียบ (CFI) เท่ากับ 0.970 ซึ่งสอดคล้องกับแนวคิดของ Diamantopoulos & Siguaw (2000) และ Kaplan (2000) เสนอเกณฑ์ไว้ว่า ดัชนี CFI มีค่าตั้งแต่ 0.90 ขึ้นไป แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ ค่าดัชนี Tucker-Lewis (TLI) เท่ากับ 0.961 จะมีค่าระหว่าง 0 - 1 มีความสอดคล้องกับแนวคิด Shamer, Mukherjee, Kumar & Dillon (2005) เสนอว่าดัชนี TLI มีค่ามากกว่า 0.90 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โมเดลค่าดัชนีรากของกำลังสองเฉลี่ยของเศษเหลือมาตรฐาน

(SRMR) เท่ากับ 0.108 มีความสอดคล้องกับแนวคิดของ Schumacker & Lomax (2010) เสนอว่าค่าดัชนีความสอดคล้องมากกว่า 0.08 มีความสอดคล้องในระดับต่ำและค่าดัชนีรากที่สองเฉลี่ยของความคลาดเคลื่อนในการประมาณค่าเท่ากับ (RMSEA) เท่ากับ 0.039 มีความสอดคล้องระดับต่ำ เมื่อค่า RMSEA มีค่าน้อยกว่า 0.05 ตามแนวคิดของ Diamantopoulos, & Siguaw (2000)

ข้อเสนอแนะ

ข้อเสนอแนะจากการวิจัย

1. ควรนำตัวบ่งชี้สำหรับการพัฒนาพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ไปใช้ประเมินด้านการพัฒนาพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศหรือประเมินความต้องการจำเป็นของบุคลากรมหาวิทยาลัยนเรศวร โดยเปรียบเทียบความแตกต่างหรือช่องว่างระหว่างการพัฒนาพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวรที่เป็นอยู่กับที่คาดหวังที่จำเป็นต้องได้รับการแก้ไขหรือปรับปรุง จากนั้นจึงนำผลการประเมินไปใช้ในการปรับปรุง/ตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวรให้มีประสิทธิภาพมากยิ่งขึ้น

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ผลการวิจัย พบว่า ตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร ประกอบด้วย 5 ตัวบ่งชี้หลัก และ 23 ตัวบ่งชี้ย่อย ดังนั้น ในการวิจัยครั้งต่อไปควรจะมีการนำตัวบ่งชี้ย่อยทั้ง 23 ตัวบ่งชี้ไปทดลองใช้ในสถานการณ์จริงในพื้นที่อื่นๆ แล้วติดตามผล

2. การวิจัยครั้งนี้ ผู้วิจัยทำการทดสอบความสอดคล้องของโมเดลโครงสร้างพฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรมหาวิทยาลัยนเรศวร จึงควรมีการศึกษาวิจัยต่อโดยการนำตัวบ่งชี้ที่ได้จากการวิจัยในครั้งนี้ไปเป็นแนวทางในการพัฒนาตัวบ่งชี้พฤติกรรมในการจัดการความปลอดภัยบนระบบสารสนเทศของบุคลากรในหน่วยงานอื่นๆ ตามบริบทเชิงพื้นที่ที่ไม่เหมือนกัน

เอกสารอ้างอิง

กลุ่มผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ. (2559). *สรุปองค์ความรู้ /แนวปฏิบัติที่ดี ประเด็นการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับผู้ดูแลระบบ*. สืบค้นเมื่อ 23 มิถุนายน 2564, จาก https://erp.mju.ac.th/acticleDetail.aspx?qid=549.

บุษบา ไชยยะนาค และ โกวิท รพีพิศาล. (2561). *ความตระหนักรู้ต่อการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศขั้นพื้นฐานของพนักงาน บริษัท ผลิตกระแสไฟฟ้าในภาคตะวันออก*. สืบค้นเมื่อ 23 มิถุนายน 2564, จาก https://rsucon.rsu.ac.th/files/proceedings/nation2018/G2-NA18-064.pdf.

พัทธ์ธีรา สุวรรณสิทธิ์. (2556). *การวิเคราะห์ปัญหาและการวางแผนการพัฒนาระบบสารสนเทศทางการบัญชี*. สืบค้นเมื่อ 24 มิถุนายน 2564, จาก https://doi.nrct.go.th//ListDoi/listDetail?Resolve_DOI=10.14458/RSU.res.2013.48

ชื่อผู้แต่ง./(ปีพิมพ์).//ชื่อบทความ.//ชื่อวารสาร,/เลขของปีที่/(เลขของฉบับที่),/เลขหน้า.

วรัญญาภรณ์ สิริพิพัฒนพร และ สมชาย นำประเสริฐชัย. (2557). การวิเคราะห์และแนวทางจัดการความเสี่ยงด้าน

ไอทีของหน่วยงานภาครัฐ. *วิศวกรรมสาร มก., 93 (*28*),* 31-40.

วิสุนีย์ เกลากลิ่น. (2556). *ระบบสารสนเทศเพื่อการบริหาร.* สืบค้นเมื่อ 5 พฤษภาคม 2564, จาก http://www.elfhs.ssru.ac.th/wipada_ch/pluginfile.php/882/course/summary/Chapter7-support%20system.pdf

ศรวัสย์ สนธิ. (2557). *ความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา : ข้าราชการกองบัญชาการกองทัพไทย*. สืบค้นเมื่อ 23 มิถุนายน 2564, จาก https://opacdb01.dpu.ac.th/cgi-bin/koha/opac- detail.pl?biblionumber=105160.

สุพล พรหมมาพันธุ์. (2562). *ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษาสถาบันอุดมศึกษาในเขตกรุงเทพมหานครและปริมณฑล*. สืบค้นเมื่อ 23 มิถุนายน 2564, จาก http://dspace.spu.ac.th/handle/123456789/6465

สุพิชญา อาชวิรดา. (2559). *ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร*. วารสารระบบสารสนเทศด้านธุรกิจ, 2(2). 66 – 79.

สุรัตน์ ไชยชมพู (2556). *ภาวะผู้นำเชิงจริยธรรมในการบริหารสถานศึกษา*. สืบค้นเมื่อ 24 มิถุนายน 2564, จาก http://dspace.lib.buu.ac.th/handle/1234567890/3374

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2562). *แนวทางการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ*. สืบค้นเมื่อ 23 มิถุนายน 2564, จาก https://publish.sec.or.th/nrs/8283s.pdf.

อภิญญา รัตนโกเมศ. (2552). *การใช้เทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กร กรณีศึกษา มหาวิทยาลัยมหาจุฬาลงกรณ์ราชวิทยาลัย.* สืบค้นเมื่อ 23 มิถุนายน 2564, จาก http://libdoc.dpu.ac.th/thesis/Vanhnasone.Cha.pdf.

Diamantopoulos, A. & Siguaw, J. A. (2000). *Introduction to LISREL: A guide for the uninitiated.* London: SAGE Publications, Inc,

Greg Hale, (2012). *SCADA Security is a Mindset*. Retrieved April 20, 2015 from https://www.tofinosecurity.com/blog/scada-security-mindset-isssource-explains-why-belden-design-seminar

Kaplan, D., *(2000). Structural Equation Modeling. California: Sage Publications, Thosand Oaks.*

Nor Natasha Ashira Shamsudin. (2019). *Information Security Behaviors among Employees.* Retrieved on 10 May 2021, from https://www.researchgate.net/publication/340445256_Information_Security_Behaviors_among_Employees

Schumacker, R. E., & Lomax, R. G. (2010). *A beginner's guide to structural equation modelling (3rd ed).* New York: Routledge Academic.

Shamer, S., Mukherjee, A., Kumar, A. & Dillon, W. R. (2005). *A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models*. Journal of Business Research, 58, 935-943.

Soper, D.S. (2019). *A-priori Sample Size Calculator for Structural Equation Models* (Software). Retrieved on 10 May 2021, from https://www.danielsoper.com/statcalc