สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

Cybersecurity Readiness and Index of Rajabhat University

[1*] สุภาพร พรมโส, [2#] ปราลี มณีรัตน์ และ [3#] ประสงค์ ปราณีตพลกรัง

[1, 2] สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

[3] กองการศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช

[1*] papim1968@kru.ac.th, [2#] paralee.ma@spu.ac.th, [3#] prasong_pr@rtaf.mi.th

Received : July 23, 2021

Revised : July 29, 2021

Accepted : November 17, 2021

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาและวิเคราะห์ 1) ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ 2) อุปสรรคที่ส่งผลต่อการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร 3) ความพร้อมของบุคลากรในมหาวิทยาลัยราชภัฏที่มีต่อความมั่นคงปลอดภัยไซเบอร์และ 4) พัฒนาตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ งานวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยทำการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ จำนวน 25 คน ด้วยการสัมภาษณ์แบบกึ่งโครงสร้าง ประกอบกับการสนทนากลุ่ม จากนั้นได้นำข้อมูลมาวิเคราะห์เนื้อหา ผลการวิจัยพบว่า ปัญหาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ได้แก่ ปัญหาเกี่ยวกับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดนโยบายองค์กร ปัญหาด้านบุคลากร และปัญหาการถูกโจมตี อุปสรรคที่ส่งผลต่อการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร พบว่า มหาวิทยาลัยราชภัฏ มีอุปสรรค ด้านนโยบายผู้บริหาร ด้านทักษะความรู้ ด้านวัฒนธรรมองค์กร ด้านความไม่เสถียรของระบบ ด้านสภาพความพร้อม และดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ผู้วิจัยได้นำเสนอตัวแบบตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย มาตรฐานของระบบ การปรับด้านโครงสร้างพื้นฐาน การใช้ประโยชน์ทางเทคโนโลยีดิจิทัล การพัฒนาศักยภาพบุคลากร สมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์และการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ อีกยังได้ค้นพบดัชนีความพร้อมด้านความปลอดภัยไซเบอร์ที่ประกอบด้วยปัจจัยหลัก 7 ด้าน และมี 24 ปัจจัยย่อย

คำสำคัญ : ความมั่นคงปลอดภัยไซเบอร์, ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์, ดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

Abstract

This study aims to study and analyze 1) the problems of cybersecurity in Rajabhat University, 2) obstacles affecting the development of personnel cybersecurity competency, 3) personnel readiness in cybersecurity of Rajabhat University and 4) to develop a model for cybersecurity readiness. A qualitative research method was performed in this study. Twenty-five experts were selected for in-depth semi-structured interview, including a focus group that approach to achieve cybersecurity problems, obstacles and cybersecurity readiness index of Rajabhat University, prior to the content analysis was done. The analysis of results concluded that the cybersecurity problems of Rajabhat University include: problems with cybersecurity measures, determination of organizational policy, personnel problems, and attack problems. The obstacles affected to develop personal's competencies of Rajabhat University are as follows: executive policy, knowledge skill, organizational culture and instability of network systems. In terms of readiness condition and cybersecurity readiness index of Rajabhat University, this study introduced a cybersecurity readiness model which comprised of system standard, infrastructure adjustment, digital technology utilization, personnel potential development, cybersecurity competency and cybersecurity transformation. In addition, the cybersecurity readiness index, contained 7 main factors and 24 sub-factors.

Keywords: Cybersecurity, Cybersecurity Readiness, Cybersecurity Index

1. บทนำ

ปัจจุบันความก้าวหน้าและอรรถประโยชน์ของเทคโนโลยีดิจิทัลได้นำมาใช้บริหารจัดการงานต่าง ๆ ภายในองค์กรทุกภาคส่วน ทั้งภาครัฐและเอกชนมีการปรับเปลี่ยนระบบการดำเนินงานเข้าสู่ยุคดิจิทัลเพื่อเพิ่มประสิทธิภาพการทำงาน [1] ซึ่งรัฐบาลไทยเล็งเห็นความสำคัญของเทคโนโลยีดิจิทัลที่มีต่อการพัฒนาประเทศ จึงกำหนดนโยบาย แผนแม่บทหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศระยะ 20 ปี (พ.ศ. 2561 – 2580) ให้มีการขับเคลื่อนประเทศสู่ความยั่งยืนโดยใช้เทคโนโลยีดิจิทัล [2] จึงพบการใช้ประโยชน์จากเทคโนโลยีดิจิทัลที่มีความหลากหลายในงานประเภทต่าง ๆ เช่น การส่งเสริมการเรียนรู้ การส่งเสริมสุขภาพ การศึกษา การสร้างธุรกิจใหม่ ๆ และการคมนาคมขนส่ง เป็นต้น

ทั้งนี้ เทคโนโลยีดิจิทัลที่มีการใช้งานมากที่สุดคือ การใช้อินเทอร์เน็ต เนื่องจากประชาชนสามารถเข้าถึงและใช้บริการด้านข้อมูลผ่านอินเทอร์เน็ตได้อย่างสะดวก รวดเร็ว ไม่จำกัดเวลา สถานที่ ทำให้เกิดความสะดวกสบายในการบริหารจัดการและการดำรงชีวิตเพิ่มขึ้น [3] แต่ขณะเดียวกันอาจมีการใช้อินเทอร์เน็ตที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ (Cyber Threats) ซึ่งเป็นภัยคุกคามที่ไร้พรหมแดน มีหลากหลายรูปแบบ เช่น การพยายามบุกรุกเข้าระบบ การโจมตีระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ การเผยแพร่ข้อมูลที่ไม่เป็นความจริง โดยการสร้างเว็บไซต์ปลอมเพื่อการหลอกลวง เป็นต้น [4], [5], [6] จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทยในปี พ.ศ. 2561 พบว่าการพยายามบุกรุกเข้าระบบ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์ที่มีมากที่สุด คิดเป็นร้อยละ 43.3 จากภัยคุกคามทั้งหมด 2,520 เรื่อง [7] สาเหตุสำคัญที่ก่อให้เกิดปัญหาภัยคุกคามไซเบอร์มีหลายประการ เช่น ความไม่พร้อมของระบบเทคโนโลยีดิจิทัล การขาดระบบการ

บริหารจัดการเครือข่ายที่ดี การขาดแคลนบุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีดิจิทัลและด้านความมั่นคงปลอดภัยไซเบอร์ เป็นต้น [8]

เทคโนโลยีดิจิทัลเป็นเสมือนการสร้างเครือข่ายการทำงานแบบใยแมงมุม ผลจากภัยคุกคามทางไซเบอร์สามารถสร้างความเสียหายให้ทุกฝ่ายที่เกี่ยวข้องได้ไม่มากก็น้อย การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) จึงเป็นสิ่งที่ไม่สามารถมองข้ามได้ สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ [9] จึงมีความจำเป็นอย่างยิ่งที่ทุกองค์กรทั้งภาครัฐและเอกชนที่จะนำไปใช้ในการกำหนดทิศทางในการรับมือต่อการโจมตีทางไซเบอร์ที่ไม่อาจทราบได้ว่าจะเกิดขึ้นเมื่อไหร่ โดยเฉพาะในภาคการศึกษาที่มีฐานข้อมูลที่มีความสำคัญยิ่งทั้งบุคลากรสายวิชาการ และสายสนับสนุน รวมไปถึงการให้บริการข้อมูลต่าง ๆ ทั้งนักศึกษา บุคคลภายนอกที่มีความสนใจ [10], [11]

มหาวิทยาลัยราชภัฏทั้ง 38 แห่งของประเทศไทย เป็นหน่วยงานหนึ่งที่มีการนำเทคโนโลยีดิจิทัลมาใช้บริหารจัดการข้อมูลเกือบทุกประเภทภายในองค์กรด้วยจำนวนข้อมูลและจำนวนผู้ใช้งานอินเทอร์เน็ตที่มีความหลากหลาย ทั้งนักศึกษา บุคลากรสายการสอน และสายสนับสนุนรวมถึงความรู้และทักษะในการใช้เทคโนโลยีดิจิทัล จึงเป็นเงื่อนไขของการออกแบบระบบความมั่นคงปลอดภัยไซเบอร์ ที่อาจส่งผลกระทบให้การใช้งานเกิดความไม่สะดวก แต่ในทางกลับกันอาจเกิดความเสี่ยงที่ไซเบอร์จะถูกคุกคามหากระบบป้องกันข้อมูลมีประสิทธิภาพไม่เพียงพอ

อย่างไรก็ตาม เทคโนโลยีดิจิทัลในยุคปัจจุบันมีการเปลี่ยนแปลงอย่างรวดเร็ว การสร้างระบบป้องกันอันตรายจากภัยคุกคามไซเบอร์ จึงควรพิจารณาปัจจัยแวดล้อมและความพร้อมของหน่วยงานทุกมิติ เพื่อนำมาสู่การวางแผนจัดการระบบที่เท่าทันต่อการเปลี่ยนแปลงทางเทคโนโลยีดิจิทัล ดังนั้น การวิจัยครั้งนี้ จึงต้องการวิเคราะห์สถานภาพความพร้อมและตัวชี้วัดความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านปัญหาและอุปสรรคที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ รวมถึงความพร้อมของมหาวิทยาลัยราชภัฏแต่ละแห่ง เพื่อนำมาใช้เป็นข้อมูลพื้นฐานสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์แก่มหาวิทยาลัยราชภัฏในประเทศไทย

2. วัตถุประสงค์การวิจัย

2.1 เพื่อศึกษาปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

2.2 เพื่อศึกษาอุปสรรคที่ส่งผลต่อการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในมหาวิทยาลัยราชภัฏ

2.3 เพื่อวิเคราะห์ความพร้อมของบุคลากรในมหาวิทยาลัยราชภัฏที่มีต่อความมั่นคงปลอดภัยไซเบอร์

2.4 เพื่อพัฒนาตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

3. ขอบเขตงานวิจัย

งานวิจัยนี้มีขอบเขตด้านเนื้อหาครอบคลุมการศึกษาปัญหา อุปสรรค และความพร้อมของบุคลากรมหาวิทยาลัยราชภัฏทั้ง 38 แห่ง ผู้วิจัยได้ทำการเก็บรวบรวมข้อมูลตั้งแต่เดือนธันวาคม 2563 ถึงเดือนมีนาคม 2564

4. แนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้อง

4.1 แนวคิดด้านความมั่นคงปลอดภัยไซเบอร์

สำนักงานราชบัณฑิตยสภา [12] ให้นิยามของ ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ว่าคือ ภาวะที่เครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล พ้นจากภัยคุกคาม มีลักษณะสำคัญ 3 ประการ คือ คงความลับ คงความถูกต้องครบถ้วน และคงความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) กล่าวถึง “ความมั่นคง

ปลอดภัยไซเบอร์ (Cybersecurity)" ว่าเป็นนโยบายที่สร้างเครื่องมือในการรักษาความปลอดภัยทางไซเบอร์ให้แก่องค์กรและทรัพย์สินของผู้ใช้งาน รวมถึงการบริหารความเสี่ยงที่อาจส่งผลต่อการถูกคุกคามไซเบอร์ด้วยวิธีต่างๆ เช่น การปฏิบัติการอบรม และการรับประกันทางเทคโนโลยีดิจิทัล [13] ในวารสารสถาบันวิชาการป้องกันประเทศ นิยาม "ความมั่นคงปลอดภัยไซเบอร์" ว่าเป็นกระบวนการดำเนินงานเพื่อให้องค์กรปราศจากความเสี่ยงและความเสียหายของข้อมูลข่าวสารจากอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล 3 ประการ ได้แก่ (1) การรักษาความลับของข้อมูล (2) การรักษาความสมบูรณ์ของข้อมูล และ (3) การดูแลรักษาสภาพของข้อมูลให้สามารถเข้าถึงและพร้อมเรียกใช้งานได้ตลอดเวลา [14] ขณะที่ในมาตรา 3 ของพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์กล่าวถึงความหมายของ "ความมั่นคงปลอดภัยไซเบอร์" ไว้ว่าเป็นมาตรการและการดำเนินงานเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศทุกรูปแบบโดยเน้นเพื่อการสร้างความมั่นคงของชาติ ทั้งในทางการทหาร สังคม และเศรษฐกิจ [15]

4.2 กรอบแนวคิด NICE Workforce Model

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) เป็นหน่วยงานที่มีหน้าที่สร้างมาตรฐานอุตสาหกรรมที่เกี่ยวข้องกับเทคโนโลยีและส่งเสริมการพัฒนาทางวิทยาศาสตร์และเทคโนโลยีที่จะเป็นประโยชน์ต่อมวลมนุษยชาติ ได้ริเริ่มสร้างกรอบการดำเนินงานที่เรียกว่า แนวทางการทำงานสำหรับผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ (The National Initiative for Cybersecurity Education : NICE) เพื่อให้ทุกหน่วยงาน ทั้งภาครัฐ ภาคเอกชน สถาบันการศึกษา ใช้เป็นมาตรฐานดำเนินงานหรือนำไปประยุกต์ใช้กำหนดความรู้ ทักษะและความสามารถของบุคลากรที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ อย่างไรก็ตาม NICE แบ่งกลุ่มความชำนาญพิเศษออกเป็น 7 กลุ่มดังนี้

(1) กลุ่มปฏิบัติการและบำรุงรักษา เป็นกลุ่มผู้มีความสามารถในการให้บริการ และบำรุงรักษาระบบไอที

(2) กลุ่มป้องกันและรับมือ เป็นกลุ่มผู้มีความชำนาญพิเศษ ด้านการระบุและจัดการภัยคุกคามต่อระบบไอที

(3) กลุ่มตรวจสอบ เป็นกลุ่มผู้มีความชำนาญ ด้านการตรวจสอบเหตุการณ์หรือการกระทำผิดที่เกี่ยวกับระบบไอที

(4) กลุ่มเก็บรวบรวมและปฏิบัติการ เป็นกลุ่มผู้มีความชำนาญด้านการเก็บรวบรวมข้อมูลเพื่อตัดสินใจ

(5) กลุ่มวิเคราะห์ เป็นกลุ่มผู้มีความชำนาญพิเศษด้านการวิเคราะห์ ตรวจทาน และการประเมินผล

(6) กลุ่มจัดทำและส่งมอบ เป็นกลุ่มผู้มีความชำนาญพิเศษด้านการออกแบบ และจัดสร้างระบบไอที ที่มั่นคงปลอดภัย

(7) กลุ่มควบคุมและพัฒนา เป็นกลุ่มผู้มีความชำนาญพิเศษด้านการบริหาร กำหนดทิศทาง และการพัฒนา

ด้วยบทบาทหน้าที่ของกลุ่มงานตามกรอบการดำเนินงานของ NICE จึงเกิดเป็นแนวทางการกำหนดความรู้ (Knowledge) ความสามารถ (Ability) และทักษะ(Skill) หรือ KSA ให้เกิดความเหมาะสมกับตำแหน่งงานด้านความมั่นคงปลอดภัยไซเบอร์[16] ควบคู่กับการกำหนดแนวทางในการประเมินสมรรถนะ ที่จำเป็นในการปฏิบัติงาน หากประเมินสมรรถนะตามความความหมายของจิรประภา อัครบวร [17] หมายถึงความรู้ (Knowledge) ทักษะ (Skills) และคุณลักษณะ (Attributes) ที่ทำให้ประสบความสำเร็จและมีความโดดเด่น ทั้งนี้นอกจากองค์ประกอบสำคัญข้างต้นแล้ว การทำให้เกิดความสำเร็จตามเกณฑ์มาตรฐานหรือสูงกว่า ควรมีพฤติกรรมที่ถึงพร้อมด้วยจริยธรรม บุคลิกภาพ คุณลักษณะทางกายภาพ และอื่น ๆ ซึ่งสอดคล้องกับภาระงานตามตำแหน่งนั้น ๆ [18]

4.3 โครงสร้างพื้นฐานทางระบบเทคโนโลยีดิจิทัล

ปัญหาโดยรวมของระบบเทคโนโลยีดิจิทัลสมัยใหม่ ในองค์กรขนาดใหญ่ส่วนหนึ่งเกิดจากการขาดแคลนโครงสร้างพื้นฐานที่จำเป็นในการสนับสนุนระบบงานต่าง ๆ ที่จะเกิดขึ้น โครงสร้างพื้นฐานระบบเทคโนโลยีดิจิทัลสามารถแยกส่วนเป็นระบบเครือข่ายอุปกรณ์ คอมพิวเตอร์ ระบบข้อมูลเป็นหลัก รวมไปถึงระบบเครือข่ายคอมพิวเตอร์ที่ครอบคลุมทุกหน่วยงานอย่างมีประสิทธิภาพ เพื่อให้ระบบงานที่พัฒนาขึ้นสามารถติดต่อแลกเปลี่ยนข้อมูล สามารถกระจายไปถึงจุดการใช้งานต่าง ๆ ได้อย่างทั่วถึงและมีประสิทธิภาพ

อย่างไรก็ตาม เนื่องจากเทคโนโลยีดิจิทัลในปัจจุบันอ้างอิงการพัฒนาระบบข้อมูลแบบรวมศูนย์ให้มีการกระจายการใช้งานข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ทำให้ผู้ใช้งานไม่จำเป็นต้องเรียนรู้ถึงความยุ่งยากซับซ้อนของระบบงานเพียงแต่มุ่งเน้นการใช้งานให้เกิดประโยชน์สูงสุด ส่วนความยุ่งยากซับซ้อนในการพัฒนาหรือบริหารจัดการระบบ และติดตั้งเทคโนโลยีดิจิทัล เป็นหน้าที่ของผู้เชี่ยวชาญด้านดิจิทัลโดยเฉพาะเท่านั้น เมื่อเรียกรวมกันทั้งระบบดิจิทัลจะได้ว่า “โครงสร้างพื้นฐานดิจิทัล” อันประกอบไปด้วย

1. เครื่องคอมพิวเตอร์ลูกข่าย (เช่น PC, Tablet, iPad, Note 10.1 หรือ Smart Phone เป็นต้น)
2. โปรแกรมระบบปฏิบัติการ (Windows, Linux, RedHat, Unix, MacOS เป็นต้น)
3. โปรแกรมสำเร็จรูป (Word, Excel, PowerPoint เป็นต้น)
4. ระบบเครือข่ายสื่อสารข้อมูล (ระบบอินเทอร์เน็ต อินทราเน็ต ระบบ LAN ระบบ WAN เป็นต้น)
5. ระบบเครื่องคอมพิวเตอร์แม่ข่าย (เช่น Internet Server, Proxy Server, Mail Server, Application Server, Database Server เป็นต้น) ระบบแอปพลิเคชัน (Application) หรือระบบโปรแกรมประยุกต์ของแต่ละฟังก์ชันงาน เช่น ระบบบริหารงานบุคคล ระบบการเงินการคลังและงบประมาณ ระบบงานบัญชี และอื่น ๆ ซึ่งมีการพัฒนาให้สามารถใช้งานได้ผ่านระบบอินเทอร์เน็ต/ติดตั้งใช้งานเฉพาะที่เครื่องคอมพิวเตอร์
6. การบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น การโจมตีระบบสารสนเทศผ่านอินเทอร์เน็ต ทำให้เครื่องคอมพิวเตอร์แม่ข่ายไม่ทำงาน หรือปิดการทำงาน (Shutdown) หรือติดไวรัส เป็นต้น นอกจากนั้น กรณีที่เครื่องแม่ข่ายให้บริการเกี่ยวกับงานการเงินการคลัง ควรมีการเฝ้าระวังเป็นพิเศษ เป็นต้น

4.4 งานวิจัยที่เกี่ยวข้อง

ณรงค์เวตย์ เรืองจวง [19] ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ พบว่า บุคลากรมีระดับความสามารถด้านการปฏิบัติเชิงรับอยู่ในระดับดี และการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง การปฏิบัติงานเกือบทุกด้านมีการกำหนดนโยบาย กระบวนการแผนแม่บท และแผนงานเพื่อรองรับการใช้งาน แต่ขาดแนวความคิดการปฏิบัติการด้านไซเบอร์ หากพิจารณาด้านระบบและอุปกรณ์ พบว่ามีความทันสมัย มีประสิทธิภาพสูง แต่บุคลากรที่ปฏิบัติงานด้านไซเบอร์มีจำนวนไม่เพียงพอ ขาดความรู้และทักษะในการปฏิบัติงานด้านไซเบอร์ อีกทั้งโครงสร้างการจัดหน่วยข้อมูลสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น

Cheang, S. [20] ประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันอุดมศึกษา เพื่อการพัฒนาประเทศกัมพูชา ผลการวิจัยพบว่า ประเทศกัมพูชามีความพร้อมด้านทรัพยากรมนุษย์ ด้านโครงสร้างพื้นฐาน และด้านสิ่งแวดล้อมที่เอื้อต่อการสร้างระบบความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ

Wendy และ Gunawan [21] ศึกษางานด้านความมั่นคงปลอดภัยไซเบอร์ในหัวข้อเรื่อง Manage Security (APO13), Manage Security Services (DSS05) ภายใต้ COBIT5.0 เพื่อประเมินผู้ปฏิบัติงานในแผนกไอทีของมหาวิทยาลัย XYZ โดยใช้ค่าเฉลี่ยมาจัดระดับความสามารถเพื่อตรวจหาช่องโหว่ของความมั่นคงปลอดภัยในระบบประมวลผลแบบคลาวด์ พร้อมกับเสนอวิธีการแก้ปัญหาที่เกิดขึ้น ด้วยกระบวนการของ COBIT5.0 และ ISO27001: 2013

Obi และ Iwasaki [22] กำหนดว่า ความมั่นคงปลอดภัยไซเบอร์ควรประกอบด้วยดัชนีความพร้อม 3 ด้าน คือ ด้านกฎหมายไซเบอร์ ด้านองค์กรการรักษาความมั่นคงปลอดภัยทางอินเทอร์เน็ต และด้านอาชญากรรมไซเบอร์

5. วิธีดำเนินการวิจัย

งานวิจัยนี้ใช้รูปแบบการวิจัยเชิงคุณภาพ เริ่มต้นจากการค้นคว้าเอกสารนโยบาย บทความ รวบรวมข้อมูลจากงานวิจัยที่เกี่ยวข้อง เพื่อนำมากำหนดเป็นคำถามเชิงลึกสำหรับการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ทรงคุณวุฒิ และการสนทนากลุ่ม (Focus Group) กับผู้เชี่ยวชาญด้านดิจิทัลและด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านทางโทรศัพท์และระบบออนไลน์ เช่น Google Meet, Zoom ควบคู่กับการจดบันทึกและบันทึกเสียงการสนทนา สำหรับนำข้อมูลมาวิเคราะห์เขียนสรุป และนำเสนอข้อมูลเชิงพรรณนา

องค์ประกอบของการทำวิจัยดังนี้

5.1 กลุ่มผู้ให้ข้อมูล (Key Informant) คัดเลือกจากบุคลากรสายวิชาการของมหาวิทยาลัยราชภัฏจำนวน 38 แห่ง ได้จำนวนทั้งสิ้น 25 คน คัดเลือกด้วยวิธีแบบเฉพาะเจาะจงจากเกณฑ์ต่อไปนี้ (1) เป็นผู้มีประสบการณ์การทำงานในมหาวิทยาลัยราชภัฏอย่างน้อย 3 ปี และ (2) เป็นผู้ปฏิบัติงานในตำแหน่งต่อไปนี้ เป็นผู้บริหารของมหาวิทยาลัยราชภัฏที่ดูแลงานด้านสารสนเทศ เป็นอาจารย์ผู้สอนเป็นผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ เป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้เชี่ยวชาญที่ทำงานด้านระบบไอทีตำแหน่งละ 5 คน

5.2 เครื่องมือในการวิจัยนี้ใช้การสัมภาษณ์เชิงลึก (In-Depth Interview) ที่ใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง จำนวน 7 ข้อ

ข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม จะถูกนำมาวิเคราะห์ด้วยวิธีการวิเคราะห์แก่นสาระ (Thematic Analysis) และนำเสนอข้อมูลในรูปแบบร้อยละร่วมกับการบรรยายเชิงพรรณนา

6. ผลการวิจัย

6.1 ผลการศึกษาปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

การศึกษาสาเหตุของปัญหาที่มีผลต่อความมั่นคงปลอดภัยไซเบอร์ในมหาวิทยาลัยราชภัฏ พบว่ามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เป็นปัจจัยสำคัญที่สุด คิดเป็น 33% รองลงมาคือ ปัญหาด้านบุคลากร การกำหนดนโยบาย การถูกโจมตีจากภายนอก คิดเป็น 31%, 27% และ 10% ตามลำดับ (ตารางที่ 1) จากการศึกษาได้ข้อค้นพบเพิ่มเติมว่า ผู้บริหารควรกำหนดนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนและมีมาตรฐาน มีการส่งเสริมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรในองค์กร ควบคู่กับการสร้างความตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 1 ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

สาเหตุของปัญหา	ระดับ (%)
1. มาตรการความมั่นคงปลอดภัยไซเบอร์	33%
2. การกำหนดนโยบาย	27%
3. บุคลากร	31%
4. การถูกโจมตีจากภายนอก	10%

6.2 ผลการศึกษาอุปสรรคที่ส่งผลต่อการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในมหาวิทยาลัยราชภัฏ

การศึกษาอุปสรรคของการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในมหาวิทยาลัยราชภัฏ พบว่า อุปสรรคที่เป็นประเด็นสำคัญที่สุด คือ การกำหนดนโยบายของผู้บริหารคิดเป็น 30% สืบเนื่องมาจากผู้บริหารให้ความสำคัญด้านความมั่นคงปลอดภัยกับองค์กรค่อนข้างน้อย รองลงมาคือ อุปสรรคด้านทักษะความรู้ คิดเป็น 29% มีข้อมูลการสำรวจที่น่าสนใจเพิ่มเติมกล่าวคือ ผู้ตอบแบบสอบถามมีความคิดเห็นว่า บุคลากรในองค์กรยังขาดความรู้และทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนใหญ่เป็นการปฏิบัติงานด้านการบริหารจัดการข้อมูล และบุคลากรมีการพัฒนาตนเองในงานด้านความมั่นคงปลอดภัยไซเบอร์ค่อนข้างน้อย สำหรับอุปสรรคด้านวัฒนธรรมองค์กร คิดเป็น 21% และด้านความไม่เสถียรของระบบอินเทอร์เน็ต คิดเป็น 20% ตามลำดับ (ตารางที่ 2)

ตารางที่ 2 อุปสรรคของการพัฒนาสมรรถนะบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

อุปสรรคของการพัฒนาสมรรถนะ	**ระดับ (%)**
1. ด้านนโยบายผู้บริหาร	30%
2. ด้านทักษะความรู้	29%
3. ด้านวัฒนธรรมองค์กร	21%
4. ด้านความไม่เสถียรของระบบอินเทอร์เน็ต	20%

6.3 ผลการศึกษาความพร้อมของมหาวิทยาลัยราชภัฏที่มีต่อความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 3 พบว่าความพร้อมของบุคลากรของมหาวิทยาลัยราชภัฏต่อความมั่นคงปลอดภัยไซเบอร์ ด้านความพร้อมขององค์กร คิดเป็น 33% ด้านความพร้อมบุคลากรคิดเป็น 28% ความพร้อมด้านกระบวนการคิดเป็น 22% ความพร้อมด้าน เทคโนโลยี 17% ตามลำดับ จากการศึกษา จึงได้ข้อค้นพบ ความพร้อมด้านองค์กร ในมุมมองงบประมาณสนับสนุนในแต่ละองค์กรมีความพร้อมแตกต่างกันตามแต่ขนาด จึงส่งผลถึงความพร้อมด้านบุคลากร ที่มีความแตกต่างกันในเรื่องความรู้ ทักษะ ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้องค์กรยังขาดบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ อีกทั้ง ยังส่งผลถึงกระบวนการทำงานในองค์กรที่ขาดการประเมินกระบวนการ ติดตามผล และความพร้อมด้านเทคโนโลยี บางองค์กรที่มีงบประมาณสนับสนุนเพียงพอแต่องค์กรที่มีขนาดเล็กมักขาดเงินทุนสนับสนุนเพื่อจัดหาเทคโนโลยีดิจิทัลที่สมัยและเพียงพอ

ตารางที่ 3 ความพร้อมของบุคลากรของมหาวิทยาลัยราชภัฏต่อความมั่นคงปลอดภัยไซเบอร์

ความพร้อมของบุคลากร	**ระดับ (%)**
1. ความพร้อมขององค์กร	33%
2. ความพร้อมด้านบุคลากร	28%
3. ความพร้อมด้านกระบวนการ	22%
4. ความพร้อมด้านเทคโนโลยี	17%

6.4 สภาพความพร้อมขององค์กร 5 ด้าน ได้แก่ นโยบายขององค์กร สภาพแวดล้อมภายในองค์กร ด้านขีดความสามารถทางความมั่นคงปลอดภัยไซเบอร์ ด้านสิ่งสนับสนุนทางเทคโนโลยี และด้านการบริหารจัดการ ส่งผลต่อการ

พัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร จากการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญรวมทั้งการสนทนากลุ่ม พบข้อมูลเรียงตามลำดับความสำคัญ ดังตารางที่ 4

ตารางที่ 4 สภาพความพร้อมองค์กร 5 ด้าน

ความพร้อมองค์กร	ลำดับความสำคัญ
1. นโยบายขององค์กร	ลำดับที่ 1
2. สิ่งสนับสนุนการเรียนรู้	ลำดับที่ 2
3. สิ่งสนับสนุนทางเทคโนโลยี	ลำดับที่ 3
4. ขีดความสามารถทางความมั่นคงปลอดภัยไซเบอร์	ลำดับที่ 4
5. สภาพแวดล้อมภายใน	ลำดับที่ 5

ในตารางที่ 4 พบว่า เมื่อเรียงลำดับความสำคัญสภาพแวดล้อมองค์กร 5 ด้านพบว่า นโยบายองค์กร จัดอยู่ในลำดับที่ 1 รองลงมาคือ สิ่งสนับสนุนการเรียนรู้ สิ่งสนับสนุนทางเทคโนโลยี ขีดความสามารถทางความมั่นคงปลอดภัยไซเบอร์ และลำดับสุดท้ายคือสภาพแวดล้อมภายใน ตามลำดับ จากการศึกษาได้ข้อค้นพบว่า นโยบายองค์กร ถือเป็นหัวใจหลักด้านความมั่นคงปลอดภัยไซเบอร์ ที่องค์กรต้องมีนโยบายชัดเจนในการป้องกันปัญหาความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะส่งผลไปถึงองค์ประกอบอื่นด้วย

6.5 ปัจจัยที่มีอิทธิพลต่อการพัฒนาสมรรถนะความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในมหาวิทยาลัยราชภัฏ จากการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญรวมทั้งการสนทนากลุ่ม ได้ข้อสรุปดังตารางที่ 5

ตารางที่ 5 ปัจจัยที่มีอิทธิพลต่อการพัฒนาสมรรถนะความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในมหาวิทยาลัยราชภัฏ

ความพร้อมของบุคลากร	ระดับ (%)
1. ปัจจัยด้านคน	28%
2. ปัจจัยด้านงบประมาณ	14%
3. ปัจจัยด้านบริหารจัดการ	22%
4. ปัจจัยด้านแรงจูงใจ	18%
5. ปัจจัยด้านการตระหนักรู้	19%

6.6 ดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

จากการศึกษาปัญหา อุปสรรค และสถานภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏตามข้อที่ 6.1 – 6.5 ข้างต้น ผู้วิจัยได้ทำการพัฒนาดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ที่อิงดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) ที่จัดทำโดยสหภาพโทรคมนาคมสากล ร่วมกับสถาบัน ABI Research [23] ประกอบด้วย 5 ด้าน ได้แก่ มาตรการทางกฎหมาย (Legal Measures) มาตรการเทคนิค (Technical Measures) มาตรการการจัดสร้างองค์กร (Organizational Measures) การพัฒนาศักยภาพบุคลากร (Capacity Building) และการสร้างความร่วมมือ (Cooperation) จากปัจจัยหลัก 5 ด้าน ประกอบด้วย 17 ปัจจัยย่อย

ผู้วิจัยพิจารณาถึงปัจจัยดังกล่าวผ่านทางการสนทนากลุ่มกับผู้เชี่ยวชาญ พบว่าควรเพิ่มปัจจัยหลัก/ปัจจัยย่อย เพื่อพัฒนาเป็นดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ดังที่นำเสนอจะเห็นได้ว่ามีรายละเอียดความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ 7 ด้าน 24 ปัจจัยย่อย

ตารางที่ 6 ดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ

ปัจจัยหลัก	ปัจจัยย่อย
1. มาตรฐานทางกฎหมาย (Legal Measures)	1.1 กฎหมายอาญา (Criminal Legislation) เกี่ยวกับการควบคุมการกระทำความผิดทางคอมพิวเตอร์
	1.2 การมีกฎระเบียบและการปฏิบัติตามกฎระเบียบ Regulation and Compliance) หมายถึง การมีกฎที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์เฉพาะเรื่อง เช่น กฎหมายการใช้ลายเซ็นอิเล็กทรอนิกส์ เป็นต้น
2. มาตรการทางเทคนิค (Technical Measures)	2.1 การจัดตั้งหน่วยงานระดับ ชาติเพื่อตอบสนองเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), Computer Security incident Response Team (CSIRT))
	2.2 มาตรฐาน (Standards)
	2.3 การออกใบรับรอง (Certifications)
3. มาตรฐานด้านโครงสร้างองค์กร (Organizational Measures)	3.1 นโยบาย (Policy)
	3.2 แผนด้านการกำกับข้อมูลดูแล (Roadmap for Governance)
	3.3 หน่วยงานที่รับผิดชอบ (Response Agency)
	3.4 การเทียบเคียงกับหน่วยงานระดับชาติ (National Benchmarking)
4. การพัฒนาศักยภาพบุคลากร (Capacity Building)	4.1 การกำหนดมาตรฐานในการพัฒนาบุคลากร (Standardization Development)
	4.2 การพัฒนาบุคลากร (Manpower Development)
	4.3 การให้การรับรองแก่ผู้เชี่ยวชาญ (Professional Certification)
	4.4 การให้การรับรองหน่วยงาน (Agency Certification)
5. การสร้างความร่วมมือ (Cooperation)	5.1 การสร้างความร่วมมือระหว่างรัฐ (Intra-State Cooperation)
	5.2 การสร้างความร่วมมือระหว่างหน่วยงาน (Intra-Agency Cooperation)
	5.3 การสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชน (Public-private partnerships (PPP))
	5.4 การสร้างความร่วมมือระหว่างประเทศ (International Cooperation)
6. การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์	6.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
	6.2 ด้านการยอมรับในเทคโนโลยี
	6.3 ด้านบุคลากร
	6.4 ด้านความพร้อมใช้งาน
7. ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์	7.1 ความพร้อมด้านบุคลากร
	7.2 ความพร้อมด้านกระบวนการ
	7.3 ความพร้อมด้านเทคโนโลยี

อย่างไรก็ตาม ผู้วิจัยสามารถสรุปปัญหาและอุปสรรคที่มีผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏทั้ง 38 แห่ง ได้ดังนี้

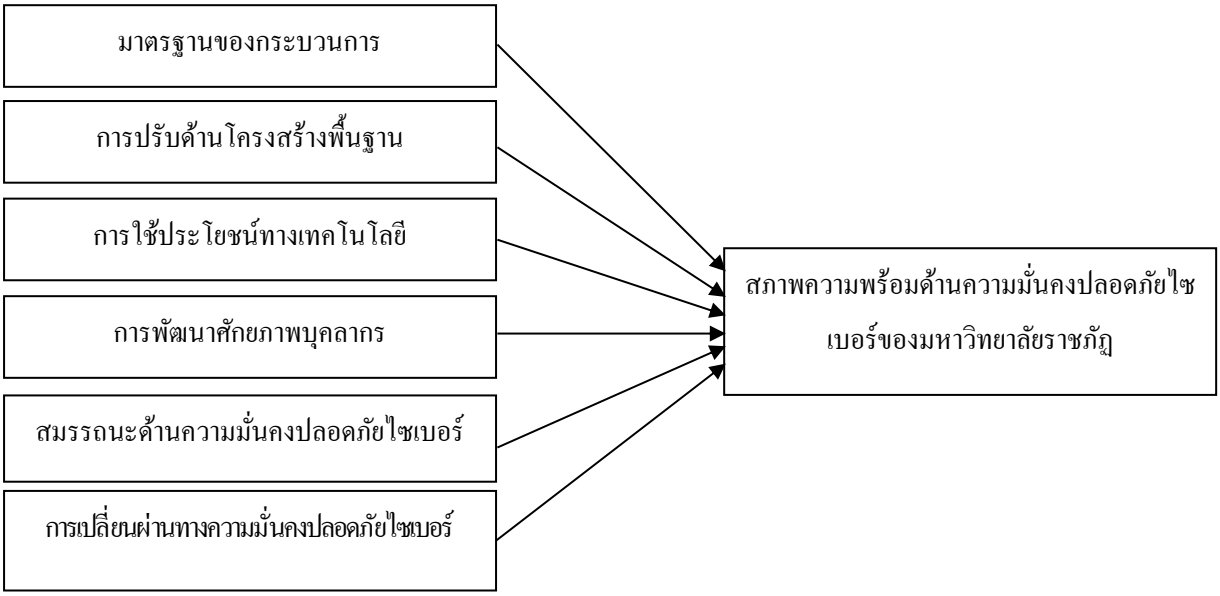
(1) ขาดระบบการเฝ้าระวังและเตือนภัยด้านไซเบอร์ที่มีประสิทธิภาพ

(2) ขาดแคลนบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(3) ขาดนโยบายและแนวปฏิบัติตามกฎหมายเกี่ยวกับการรักษาความปลอดภัยไซเบอร์ที่ชัดเจนเป็นรูปธรรม

(4) งบประมาณที่จัดสรรเพื่อส่งเสริมการจัดระบบเฝ้าระวังและเตือนภัยด้านไซเบอร์มีจำกัด

ผู้วิจัยนำผลการศึกษาทั้งหมดมาพัฒนาเป็นตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ด้วยการนำเสนอไว้ในรูปที่ 1 มีรายละเอียดดังต่อไปนี้



รูปที่ 1 ตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

1. มาตรฐานของกระบวนการคือ กลไกในการบริหารจัดการของมหาวิทยาลัยราชภัฏต่อความมั่นคงปลอดภัยไซเบอร์

2. การปรับด้านโครงสร้างพื้นฐานคือ แนวทางนโยบาย ข้อปฏิบัติและแผนด้านการกำกับข้อมูล ดูแลข้อมูล ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

3.การใช้ประโยชน์ทางเทคโนโลยี คือมหาวิทยาลัยที่มีความพร้อมด้านเทคโนโลยีที่ทันสมัย มีงบประมาณเพียงพอที่สามารถจัดสรรจัดสรรในการจัดซื้อจัดจ้างหาเทคโนโลยีที่เหมาะสมกับองค์กรได้

4. การพัฒนาศักยภาพบุคลากรคือ การพัฒนาบุคลากรของมหาวิทยาลัยราชภัฏแต่ละแห่งให้มี ความรู้ ทักษะ และความสามารถ รวมทั้งสามารถแก้ไขปัญหาได้ด้วยตนเองและเท่าเทียมกันต่อความมั่นคงปลอดภัยไซเบอร์

5. สรรถนะด้านความมั่นคงปลอดภัยไซเบอร์คือ บุคลากรในมหาวิทยาลัยราชภัฏ มีความรู้ ทักษะและความสามารถในการป้องกัน ภาวะฟ้นจากภัยคุกคามที่มีต่อระบบเครือข่ายคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วนและความพร้อมใช้งาน

6. การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์คือ กระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการเปลี่ยนทัศนคติและสร้างวัฒนธรรมทางความมั่นคงปลอดภัยไซเบอร์ที่หยั่งรากลึกในระดับบุคคลและองค์กรให้เกิดภูมิคุ้มกันและมีจริยธรรมทางความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำให้บุคคลและองค์กรมีขีดความสามารถด้านไซเบอร์ในอันที่จะป้องกัน ต่อต้าน ตรวจจับและตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้เกิดความเสียหายได้

7. สรุปผลการวิจัย

ผลการวิจัยสถานภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์และดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ พบว่า สถานภาพทั้งหมดด้านความมั่นคงปลอดภัยไซเบอร์ ประเด็นหลักที่เป็นปัญหาคือ มาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการกำหนดนโยบายองค์กร ปัญหาบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ส่วนอุปสรรคพบว่า ด้านนโยบายผู้บริหาร อุปสรรคด้านความไม่มีเสถียรภาพของระบบอินเทอร์เน็ต อุปสรรคด้านวัฒนธรรมองค์กร อุปสรรคด้านทักษะความรู้ ความสามารถและความเชี่ยวชาญ และอุปสรรคด้านงบประมาณที่จะสนับสนุนการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์นั้นมีจำกัด

สำหรับการวิจัยสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏในครั้งนี้ยังได้ค้นพบตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ประกอบด้วย 6 ด้าน ได้แก่ 1) มาตรฐานของกระบวนการ 2) การปรับด้านโครงสร้างพื้นฐาน 3) การใช้ประโยชน์ทางเทคโนโลยี 4) การพัฒนาศักยภาพบุคลากร 5) สมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ และ 6) การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

8. อภิปรายผลการวิจัย

ผลการวิจัยมีประเด็นที่น่าสนใจในการอภิปรายผลดังนี้

8.1 ผลการศึกษา ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ จากการสัมภาษณ์เชิงลึกรวมทั้งการสนทนากลุ่มกับผู้เชี่ยวชาญ ในมุมมองของแต่ละท่านและนำมาวิเคราะห์ ผลการวิจัยพบว่า สาเหตุของปัญหา ได้แก่ มาตรการด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดนโยบาย บุคลากร และการถูกโจมตีทางไซเบอร์ ผลการค้นพบคือ ผู้บริหารควรมีนโยบายพัฒนาความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ บุคลากรในองค์กรให้เกิดความตระหนักรู้ถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์

8.2 อุปสรรคที่ส่งผลต่อสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ ค้นพบว่า ผู้บริหารยังให้ความสำคัญด้านความมั่นคงปลอดภัยน้อย บุคลากร ไม่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรจึงควรส่งเสริมและพัฒนาทักษะให้กับบุคลากรให้มีความรู้ ความเชี่ยวชาญด้านไซเบอร์

8.3 การศึกษาเพื่อวิเคราะห์ดัชนีความพร้อมความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ผู้วิจัยได้ทำการศึกษาปัญหา อุปสรรครวมถึงสถานภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ทั้งนี้ผู้วิจัยได้ทำการพัฒนาดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ที่อิงดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) ที่ประกอบด้วย 5 ด้าน ได้แก่ มาตรการทางกฎหมาย (Legal Measures) มาตรการเทคนิค (Technical Measures) มาตรการการจัดสร้างองค์กร (Organizational Measures) การพัฒนาศักยภาพบุคลากร (Capacity Building) และการสร้างความร่วมมือ (Cooperation) จากปัจจัยหลัก 5 ด้าน ประกอบด้วย 17 ปัจจัยย่อยเพื่อนำมาประกอบการพัฒนาตัวชี้วัด [24]

ผู้วิจัย ได้พิจารณาถึงปัจจัยดังกล่าว และได้นำเข้าสู่การสนทนากลุ่ม ทำให้ได้ปัจจัยหลัก/ปัจจัยย่อย เพื่อพัฒนาเป็นดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ มีรายละเอียด จำนวน 7 ด้าน และประกอบด้วย 24 ปัจจัย และการศึกษาวิจัยได้ค้นพบตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ประกอบด้วย 6 ด้าน ได้แก่ 1) มาตรฐานของกระบวนการ 2) การปรับด้านโครงสร้างพื้นฐาน 3) การใช้ประโยชน์จากเทคโนโลยี 4) การพัฒนาศักยภาพบุคลากร 5) สมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ และ 6) การเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์

9. ข้อเสนอแนะ

สืบเนื่องจากข้อมูลที่ค้นพบในการวิจัยครั้งนี้ ผู้วิจัยมีข้อเสนอแนะสำหรับการนำผลงานวิจัยไปใช้งานในแต่ละมิติ ดังนี้

9.1 ข้อเสนอแนะสำหรับองค์กร

(1) งานวิจัยนี้ ทำให้ทราบถึงระดับความสำคัญของปัญหาในมหาวิทยาลัยราชภัฏ ที่มีผลต่อความมั่นคงปลอดภัยไซเบอร์ ซึ่งองค์กรสามารถนำข้อมูลที่ได้มาวางแผนกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยการออกข้อกำหนดนโยบาย กำหนดทิศทางและกิจกรรมการทำงานให้แก่หน่วยงาน มีการเปิดโอกาสให้บุคลากรเข้ารับการพัฒนาตนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กร

(2) จากงานวิจัยนี้ ทำให้พบอุปสรรคที่สำคัญของมหาวิทยาลัยราชภัฏในการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น อยู่ที่ความสามารถในการนำนโยบายขององค์กรที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ไปใช้ในเชิงปฏิบัติ ดังนั้น องค์กรควรมีการกำหนดแนวทางปฏิบัติที่ชัดเจน ควบคู่กับการกำหนดระดับมาตรฐานของความเข้มงวดในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ผู้บริหารระดับต่าง ๆ ภายในองค์กรสามารถนำนโยบายไปบริหารจัดการสารสนเทศและรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นรูปธรรม

(3) มหาวิทยาลัยราชภัฏอาจนำข้อมูลที่ได้ในครั้งนี้ไปประยุกต์ใช้งานเพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีการที่เหมาะสมกับบริบทของแต่ละมหาวิทยาลัย

(4) จากปัญหาและอุปสรรคด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏนั้น มาตรการแก้ปัญหาที่สามารถพึ่งพาตนเองได้อย่างยั่งยืนคือการพัฒนายกระดับทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือสมรรถนะด้านการใช้ดิจิทัล (Digital Literacy) ให้แก่บุคลากรในทุกระดับของมหาวิทยาลัยราชภัฏ อีกทั้งยังต้องทำการจัดการความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ อาจทำการพัฒนาแพลตฟอร์มสถานการณ์จำลองสำหรับการทดลองเจาะระบบ ป้องกันระบบ หรือการแข่งขันทางไซเบอร์ ซึ่งจะทำให้บุคลากรมีองค์ความรู้ใหม่ มีความชำนาญในการป้องกันตนเองและสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ หรือองค์กรสามารถคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) รวมทั้งยังจะสามารถช่วยลดภาระทางงบประมาณและลดการพึ่งพาผู้เชี่ยวชาญจากภายนอกหน่วยงานได้อีกด้วย

9.2 ข้อเสนอแนะเชิงสาธารณะ

(1) การนำประเด็นปัญหา อุปสรรค และการเตรียมความพร้อมของการพัฒนา/รักษาความมั่นคงปลอดภัยไซเบอร์ในระดับมหาวิทยาลัยราชภัฏไปต่อยอดสู่องค์กรภาครัฐและเอกชน ด้วยการกำหนดนโยบาย วางแผนยุทธศาสตร์ และตัวชี้วัด ที่ครอบคลุมและสอดคล้องบริบทแวดล้อมของการทำงานในแต่ละองค์กร

(2) ในส่วนของการสร้างความมั่นคงปลอดภัยไซเบอร์ให้เกิดประสิทธิภาพสูงสุด ควรเกิดจากความร่วมมือร่วมใจของทุกมิติของการดำเนินงานทุกภาคส่วนในองค์กร ไม่ว่าจะเป็นการกำหนดนโยบาย การกำหนดขั้นตอนการดำเนินงาน การสนับสนุนทรัพยากรการทำงาน และการปฏิบัติตนด้วยความรู้ความสามารถอย่างเต็มที่ ควบคู่กับการสร้างจิตสำนึกให้ผู้มีส่วนร่วมในการใช้เทคโนโลยีดิจิทัลร่วมกันรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมกับการละเว้นการ

ปฏิบัติตนที่อาจเป็นการคุกคามไซเบอร์ไม่ว่าทางใดทางหนึ่ง จึงจะเป็นการสร้างความเข้มแข็งด้านเทคโนโลยีให้กับองค์กรได้อย่างแท้จริง

9.3 ข้อเสนอแนะสำหรับการทำวิจัยครั้งต่อไป

(1) ควรนำข้อมูลพื้นฐานที่ได้จากการวิจัยครั้งนี้ไปพัฒนาตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏที่มีความแตกต่างกันตามบริบทของแต่ละสถาบัน

(2) ควรนำผลการวิจัยไปขยายผลเพื่อการพัฒนาตัวแบบสถานภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานการศึกษาในระดับมหาวิทยาลัยทั่วประเทศ ทั้งมหาวิทยาลัยแห่งรัฐและเอกชน

10. เอกสารอ้างอิง

[1] Dutta, S., Geiger, T. and Lanvin, B. (2015). **The global information technology report 2015: ICTs for inclusive growth.** Geneva: World Economic Forum.

[2] **แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม**, กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2559). แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ระยะ 3 ปี พ.ศ. 2559-2561.

[3] Irfan, M., Putra, S. J., & Ramdhani, M. A. (2019, March). **The readiness model of information technology implementation among universities in Indonesia.** In *Journal of Physics: Conference Series* (Vol. 1175, No. 1, p. 012267). IOP Publishing.

[4] Narwal, B., Mohapatra, A. K., & Usmani, K. A. (2019). **Towards a taxonomy of cyber threats against target applications**. *Journal of Statistics and Management Systems*, *22*(2), 301-325.

[5] Assenza, G., Faramondi, L., Oliva, G., & Setola, R. (2020). **Cyber threats for operational technologies.** *International Journal of System of Systems Engineering*, *10*(2), 128-142.

[6] Sapienza, A., Ernala, S. K., Bessi, A., Lerman, K., & Ferrara, E. (2018, April). **Discover: Mining online chatter for emerging cyber threats.** *In Companion Proceedings of the The Web Conference 2018* (pp. 983-990).

[7] ThaiCERT ETDA. (2018). **สถิติภัยคุกคาม.**สืบค้น 23 มกราคม 2563, จากThaicert.or.th/statistic 2018.html.

[8] สำนักงานส่งเสริมการค้าในต่างประเทศ ณ กรุงเฮก ประเทศเนเธอร์แลนด์. (2017). **ความปลอดภัยทางไซเบอร์.**สืบค้น 23 มกราคม 2563 จากhttps://www.ditp.go.th/contents_attach/207952/207952.pdf.

[9] Bahuguna, A., Bisht, R. K., & Pande, J. (2019). **Assessing Cybersecurity maturity of organizations: An empirical investigation in the Indian context.** *Information Security Journal: A Global Perspective*, 28(6), 164-177.

[10] Lehto, M. (2018). **Cybersecurity Education and Research in the Finland's Universities and Universities of Applied Sciences.** In Cybersecurity and Threats: Concepts, Methodologies, Tools, and Applications (pp. 248-267). IGI Global.

[11] Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019, December). **The impact of age, gender, and educational level on the Cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities.** *In Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012098). IOP Publishing.

[12] คณะกรรมการจัดทำพจนานุกรมศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ. มติเมื่อ 28 มิถุนายน 2562, สำนักงานราชบัณฑิตยสภา.

[13] ศิวลีย์ ศิริโรจน์บริรักษ์. (2015).**การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของกระทรวงกลาโหมม,**วารสารสถาบันวิชาการป้องกันประเทศ. ปีที่6 ฉบับที่ 3 พฤษภาคม-สิงหาคม 2558.หน้า 21.

[14] ยุทธนา เจียมตระการ. (2561). การจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่.(รายงานวิจัยตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60, วิทยาลัยป้องกันราชอาณาจักร).

[15] ราชกิจจานุเบกษา. (2562**). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.**

[16] กิตติ โฆษะวิสุทธิ์, ธาวินี วงศ์วิศว์, กิติศักดิ์ จิร วรรณกูล, ปิลัญญา เชิญถนอมวงศ์ และชญานิน แก้วหาญ. (2564). **ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร.**สมาคมธนาคารไทย, นนทบุรี. 78 หน้า.

[17] จิรประภา อัครบวร. (2549). **สร้างคนสร้างผลงาน.** กรุงเทพมหานคร: ก.พลพิมพ์ (1996).

[18] อนันต์ นามทองต้น. (2554). **มองทางลัดสู่การปฏิบัติที่เป็นเลิศ.** พิมพ์ครั้งที่ 3. นนทบุรี: สหมิตร พริ้นติ้งแอนพับลิสชิ่ง.

[19] ณรงค์เวตย์ เรืองจวง. (2561). แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ. รัฏฐาภิรักษ์, 60 (3): 22-33.

[20] S. Cheang. (2009). Conceptual Model for Cybersecurity Readiness Assessment for Public Institutions in Developing Country: Cambodia**.** *4th International Conference on Computer Sciences and Convergence Information Technology*.

[21] Wendy and W. Gunawan. (2019). Measuring information security and Cybersecurity on private cloud computing. *Journal of Theoretical and Applied Information Technology*, 96 (1): 156-168.

[22] Obi, T., and Iwasaki, N. (2015). **The Waseda University E-Government Rankings**. IOS Press.

[23] Global Cybersecurity Index (2015). The Global Cybersecurity Index and Cyber Wellness Profiles Report. International Telecommunication Union and ABI Research. สืบค้นจาก http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015- PDF-E.pdf.

[24]. สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์กรมหาชน). 2559 . **Global Cybersecurity Index.** International Telecommunication Union (ITU), https://www.dga.or.th/wp-content/uploads/2021/ 02/7.pdf, online.