การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

Development of Information System for Evaluation of Risk and Readiness Of Cybersecurity

นางสาววิภารัตน์ ปทักขินัง รศ.ดร.ประสงค์ ปราณีตพลกรัง

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ วิเคราะห์ความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ การนำเสนอตัวแบบการประเมินความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ และ การพัฒนาระบบสารสนเทศสำหรับประเมินด้านความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยได้ใช้กรณีศึกษาของวิทยาลัยเทคโนโลยีสยาม และได้เก็บรวมรวบข้อมูลจากผู้ที่ทำหน้าที่เกี่ยวข้องกับไอซีทีเป็นกลุ่มตัวอย่าง

ผลการวิจัยพบว่า องค์ประกอบความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ จะประกอบไปด้วย 7 ด้าน ได้แก่ 1. ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ 2. ด้านกฎระเบียบที่เกี่ยวข้อง 3. ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ 4. ด้านการป้องกันอาญากรรมไซเบอร์ 5. ด้านการพัฒนากำลังพลด้านไซเบอร์ 6. ด้านงบประมาณการวิจัย และ 7. ด้านความร่วมมือกับหน่วยงานอื่น ๆ สำหรับตัวแบบการประเมินความเสี่ยงจะประกอบไปด้วย 4 ด้าน ได้แก่ 1. กำหนดหัวข้อการบริหารจัดการความเสี่ยง 2. การวิเคราะห์ความเสี่ยง 3. การวางแผนการลดความเสี่ยง และ 4. การรายงานและการประเมินผล นอกจากนั้น เมื่อนำตัวแบบดังกล่าวไปทำการประเมินวิทยาลัยเทคโนโลยีสยามแล้ว พบว่าระดับความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอยู่ในระดับที่มีความพร้อมมากที่สุด ส่วนการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอยู่ในระดับที่มีความเสี่ยงน้อย

คำสำคัญ: ความมั่นคงปลอดภัยทางไซเบอร์, ความเสี่ยง, ระดับความพร้อม

Abstract

This research study aims to risk and readiness analysis on cybersecurity propose risk and readiness model on cybersecurity and information system development for appraisal on organizational cybersecurity. The researchers used a case study of Siamtechnology College the data were collected from the sample groups which were lecturers and officers performing their ICT duties.

According to the results of this research, the cyber readiness elements comprised of 7 aspects, namely, 1. on cybersecurity strategy, 2. on rules and regulations in association with the cybersecurity, 3. on cybersecurity coordination and maintenance center, 4. on cyber crime prevention, 5. on manpower development of cybersecurity, 6. on budgets supporting basic and applied researches, and 7. on cooperation with other agencies. The risk appraisal model consisted of 4 aspects, namely, 1. on determining the risk management topics, 2. on risk analysis, 3. on planning for risk reduction, and 4. reporting and appraisal. Additionally, upon appraisal of Siam Technology College based upon the aforementioned models, the readiness on organizational cybersecurity is in the readiest level; meanwhile, the risk analysis on organizational cybersecurity is in the low risk level.

Keywords: Cybersecurity, Risk Management, Readiness.

1.บทนำ

การใช้เทคโนโลยีก็มีความเสี่ยงจากภัยคุกคามด้านสารสนเทศ และช่องโหว่ของระบบสารสนเทศ ที่เกี่ยวข้อง ซึ่งอาจถูกใช้เป็นช่องทางในการก่ออาชญากรรมในหลายรูปแบบ ทั้งที่อยู่ในลักษณะการใช้อินเทอร์เน็ตในการก่ออาชญากรรมโดยตรงซึ่งเรียกว่า “อาชญากรรม คอมพิวเตอร์” หรือในลักษณะที่มีการใช้อินเทอร์เน็ตเป็นสื่อในการก่ออาชญากรรมต่าง ๆ ดั้งนั้นหน่วยงานของรัฐ ภาคเอกชน และประชาชนควรมีความตระหนักถึงความรุนแรงของผลกระทบ และความเสียหายที่อาจจะเกิดขึ้น และมีการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งจะทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

จากประเด็นความสำคัญ และปัญหาดังกล่าวจึงควรมีการวิเคราะห์ความเสี่ยงและความพร้อม มีการกำหนดรูปแบบทางความคิดเพื่อที่จะสร้างตัวบ่งชี้ขึ้น เพื่อประเมินความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร และ พัฒนาระบบสารสนเทศสำหรับองค์กร เพื่อช่วยลดปัญหาภัยคุกคามทางไซเบอร์ที่กำลังจะเกิดขึ้นหรือมีแนวโน้มที่จะเกิดขึ้นกับองค์กร เพื่อเพิ่มประสิทธิภาพในภาพรวมต่อไป

2.ทฤษฎีที่เกี่ยวข้อง

2.1 การบริหารความเสี่ยง

ความเสี่ยง (Risk) คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจงบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จ ตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ

การจัดการความเสี่ยงหรือ การบริหารความเสี่ยง (Risk Management) คือ การจัดการความเสี่ยง ทั้งในกระบวนการในการระบุ วิเคราะห์ (Risk Analysis) ประเมิน (Risk Assessment) ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับ กิจกรรม หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง หรือเรียกว่า อุบัติภัย (Accident)

2.2 ความมั่นคง

ความมั่นคง (Security) หรืออีกนัยหนึ่งอาจหมายถึง “การรักษาความปลอดภัย” หรือ “ความปลอดภัย” ซึ่งก็ได้มีการนำไปใช้อย่างกว้างขวาง เป็นคำที่ใช้อยู่ในชีวิตประจำวันโดยทั่วไป อย่างไรก็ตาม ยังมีผู้กล่าวถึงความมั่นคงไปพร้อม ๆ กับคำว่าความปลอดภัยเสมอ ความมั่นคงเป็นคำที่มีความสำคัญอย่างยิ่งทางด้านการทหาร รวมทั้งด้านการบริหารประเทศ และการเมืองระหว่างประเทศ ความหมายของ “ความมั่นคง” ซึ่งกว้างขวาง ตั้งแต่ ความมั่นคงส่วนบุคคล (Individual Security) ความมั่นคงของกลุ่ม (Group Security) ความมั่นคงของรัฐ (State Security) และความมั่นคงระหว่างประเทศ (International Security) อย่างไรก็ตาม ความหมายพื้นฐานของความมั่นคง คือ “ความรู้สึกปลอดภัยจากการคุกคาม หรือ อันตราย” (To feel free from threats, anxiety, or danger) ความมั่นคงซึ่งเป็นสภาวะทางจิตใจของบุคคลไม่ว่าจะเป็นผู้นำทางการเมืองระดับสูงของประเทศ หรือประชาชนโดยทั่วไป ที่รู้สึกปลอดภัยจากอันตรายโดยบุคคลอื่น จึงกล่าวได้ว่า “ความมั่นคงของรัฐ หมายถึง รัฐ (หรือผู้นำรัฐ และประชาชน) เชื่อว่า ตนเองปลอดภัยจากความกลัวว่าจะถูกคุกคามจากรัฐอื่น หรือองค์กรอิสระต่างชาติ”

2.3 ความมั่นคงปลอดภัยไซเบอร์

การป้องกันอันตรายในโลกออนไลน์ ที่มีผลกระทบต่อตัวผู้ใช้งานและทรัพย์สิน (ข้อมูล) ซึ่งในปัจจุบันมีผู้ใช้งานออนไลน์ทั่วโลกเพิ่มมากขึ้น ทั้งนี้ เนื่องมาจากปัจจัยหลายๆ ด้าน เช่น การเพิ่มขึ้นของอุปกรณ์พกพา หรือ ค่าบริการที่ถูกลง ส่วนการรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง กระบวนการปกป้องเพื่อทำให้องค์กรสามารถลดความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยไซเบอร์ในทุกรูปแบบ นั่นคือทั้งในเชิงกายภาพและอิเล็กทรอนิกส์ เป็นการรักษาไว้ซึ่ง

การรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน การรักษาความมั่นคงปลอดภัยโปรแกรมประยุกต์ การรักษาความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์ ที่ใช้ในการเก็บ การเข้าถึง การประมวลผล และการกระจายข้อมูล การรักษาความมั่นคงปลอดภัยอินเทอร์เน็ต และการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งนี้ยังรวมถึงการระวังป้องกันต่อการก่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และ อุบัติเหตุ คำว่าการป้องกันอันตรายในโลกไซเบอร์มักนำมาใช้ร่วมกับคำว่าการรักษาความปลอดภัย แม้ว่าจะมีการทับซ้อนกันระหว่างการป้องกันอันตรายในโลกไซเบอร์และการรักษาความมั่นคงปลอดภัยทางข้อมูล แต่แนวคิด 2 อย่างนี้ก็ไม่เหมือนกันทั้งหมด ยิ่งกว่านั้น ยังมีการอธิบายว่า การป้องกันอันตรายในโลกไซเบอร์จะดำเนินการในขอบเขตของการรักษาความปลอดภัยทางข้อมูลแบบเดิมที่รวมถึงไม่เพียงแต่การป้องกันทรัพยากรข้อมูลแต่ยังรวมถึงทรัพย์สินอื่น ๆ รวมทั้งบุคคลคนนั้นด้วย ในการป้องกันอันตรายในโลกไซเบอร์ การอ้างอิงปัจจัยของมนุษย์มักสอดคล้องกับบทบาทของมนุษย์ในกระบวนการรักษาความมั่นคงปลอดภัย ในการป้องกันอันตรายในโลกไซเบอร์ ปัจจัยนี้มีมิติเพิ่มเติม เช่น มนุษย์เป็นกลุ่มเป้าหมายของการโจมตีบนโลกไซเบอร์ หรือการมีส่วนร่วมในการโจมตีโดยไม่รู้ตัว มิติเพิ่มเติมเหล่านี้มีความหมายเชิงจริยธรรมสำหรับสังคม ตั้งแต่การป้องกันกลุ่มที่มีความอ่อนแอ และ เด็กก็เป็นความรับผิดชอบทางสังคม

2.4 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติแบ่งออกเป็น 8 ยุทธศาสตร์ได้แก่ 1) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ 2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางด้านความมั่นคงปลอดภัยไซเบอร์ 3) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ 5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ 7) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ และ 8) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

2.5 งานวิจัยที่เกี่ยวข้อง

S. Cheang ได้วิจัยเรื่อง กรอบแนวคิดสำหรับการประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับสถาบันอุดมศึกษาในการพัฒนาประเทศ: กรณีศึกษาประเทศกัมพูชา ผลการวิจัยได้ค้นพบดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐในประเทศกัมพูชาไว้ประกอบด้วย 1) ด้านทรัพยากรมนุษย์ 2) ด้านโครงสร้างพื้นฐาน และ 3) ด้านสิ่งแวดล้อม

มหาวิทยาลัยวาซาดะ (Waseda University) ประเทศญี่ปุ่นซึ่งเป็นองค์กรทางการศึกษาที่มีชื่อเสียงในการจัดอันดับรัฐบาลอิเล็กทรอนิกส์และในปี 2556 ซึ่งได้กำหนดดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ไว้ประกอบด้วย 1) ด้านกฎหมายไซเบอร์ 2) ด้านองค์การการรักษาความมั่นคงปลอดภัยทางอินเทอร์เน็ต และ 3) ด้านอาชญากรรมไซเบอร์

อย่างไรก็ดี ทาง ITU ยังได้ร่วมมือกับบริษัท ABI Research จัดทำดัชนีความมั่นคงปลอดภัยไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) ซึ่งได้กำหนดดัชนีความมั่นคงปลอดภัยไว้ ดังต่อไปนี้ 1) มาตรการทางกฎหมาย 2) มาตรการทางด้านเทคนิค 3) มาตรการทางองค์กร 4) มาตรการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ และ 5) มาตรการความร่วมมือกับหน่วยงานอื่น ๆ

หากพิจารณาองค์ประกอบเป็นรายด้านจะพบว่า ดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์จากทั้ง 4 แหล่งจะสอดคล้องกันคือ 1) มาตรการทางองค์กร ที่เกี่ยวกับนโยบาย แผนการดำเนินงาน หน่วยงานที่รับผิดชอบ 2) ด้านการพัฒนาบุคลากรเกี่ยวกับด้านความมั่นคงปลอดภัยทางไซเบอร์โดยการพัฒนามาตรฐานวิชาชีพ 3) ด้านความร่วมมือกับหน่วยงานอื่น ๆ ซึ่งเป็นความร่วมมือทั้งภายในและภายนอกองค์กร ส่วนมาตรการทางกฎหมายใน ที่นี้จะมีความเห็นสอดคล้องกันเพียง 2 กลุ่มคือ มหาวิทยาลัย Waseda และ ITU & ABI Research

3. วิธีดำเนินการวิจัย

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัย คืออาจารย์และบุคลากรในวิทยาลัยเทคโนโลยีสยาม กลุ่มตัวอย่างที่ใช้ในการวิจัยคือผู้ที่ทำหน้าที่ในฝ่ายเทคโนโลยีสารสนเทศจำนวน 35 คน

3.2 เครื่องมือที่ใช้ในการวิจัย

ใช้แบบสอบถามเก็บรวบรวมข้อมูลโดยการส่งแบบสอบถามให้กับกลุ่มตัวอย่าง จำนวน 35 ชุด ตอบกลับมา 35 ชุด คิดเป็นร้อยละ 100

3.3 การวิเคราะห์ข้อมูล

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณด้วยการรวมรวมข้อมูลจากแบบสอบถาม และใช้การวิเคราะห์ข้อมูลด้วยวิธีการทางสถิติคือ หาค่าเฉลี่ย (Mean) หาค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation : S.D.)

4 ผลการวิจัย

4.1 ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ผลการวิจัยสามารถอธิบายแยกเป็น 7 ด้านดังตารางที่ 1

ตารางที่ 1 ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

มิติด้านความมั่นคงปลอดภัย	$\overline{X}$	S.D.	ระดับความพร้อม
ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์	4.19	0.622	มีความพร้อมมาก
ด้านกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์	4.39	0.668	มีความพร้อมมากที่สุด
ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์	3.96	0.610	มีความพร้อมมาก
ด้านการป้องกันอาญากรรมไซเบอร์	3.99	0.760	มีความพร้อมมาก
ด้านการพัฒนากำลังพลต่อความมั่นคงปลอดภัยไซเบอร์	4.13	0.598	มีความพร้อมมาก
ด้านงบประมาณสนับสนุนการวิจัยพื้นฐานและวิจัยเชิงประยุกต์	3.88	0.781	มีความพร้อมมาก
ด้านความร่วมมือกับหน่วยงานอื่นๆ	4.09	0.478	มีความพร้อมมาก
ค่าเฉลี่ยโดยรวม	4.09	0.103	มีความพร้อมมาก

จากตารางที่ 1 สามารถอธิบายรายละเอียดในแต่ละด้าน 7 ด้าน เพื่อแยกให้เห็นถึงผลในแต่ละด้านดังนี้

4.1.1 ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ มีระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.19 แสดงให้เห็นว่าองค์กรมีการกำหนดนโยบายและยุทธศาสตร์ด้านความมั่นคงปลอดภัย มีการประกาศให้บุคลากรได้ทราบถึงยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์รวมถึงมีผู้ดูแลรับผิดชอบ

4.1.2 ด้านบุคลากร มีความมั่นคงปลอดภัยอยู่ในระดับปานกลาง โดยมีค่าเฉลี่ย = **2.91** แสดงว่าบุคลากรของสถาบันการพลศึกษา เห็นว่าควรหน่วยงานมีการ คัดเลือกบุคลากร กำหนดเงื่อนไขการจ้างงาน การส่งมอบงานและตรวจสอบทรัพย์สิน ยกเลิกสิทธิ การจัดอบรมและสร้างความตระหนักให้กับบุคลากรเกี่ยวกับความมั่นคงปลอดภัยอยู่ในระดับปานกลาง

4.1.3 ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 3.96 แสดงให้เห็นว่า องค์กรมีศูนย์ประสานงานหรือการตอบสนองต่อการแจ้งเหตุภัยคุกคามทางไซเบอร์ มีการประสานงานเพื่อแลกเปลี่ยนข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างหน่วยงาน มีการควบคุมข้อมูลสารสนเทศ กรณีส่งผ่านทางอีเมล์ เอสเอ็มเอส และอื่นๆ

4.1.4 ด้านการป้องกันอาญากรรมไซเบอร์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = **3**.99 แสดงให้เห็นว่า องค์กรมีนโยบายด้านการป้องกันข้อมูลสารสนเทศอย่างเข้มแข็ง มีระบบจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือการนำไปใช้ในทางที่ผิด มีบุคลากรคอยตรวจจับและตอบโต้การคุกคาม มีการแจ้งเตือนผู้ใช้ให้ระมัดระวังการโจมตีจากภัยคุกคาม และ จำกัดการเข้าถึงสารสนเทศตามนโยบายการป้องกันข้อมูลสารสนเทศ

4.1.5 ด้านการพัฒนากำลังพลต่อความมั่นคงปลอดภัยไซเบอร์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.13 แสดงให้เห็นว่า องค์กรมีการพัฒนาบุคลากรโดยการส่งไปฝึกอบรม หรือ ดูงานด้านความมั่นคงปลอดภัยไซเบอร์นอกสถานที่ บุคลากรขององค์กรเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตน และ ปลุกจิตสำนึก ให้ความรู้ และเตือนความจำ เกี่ยวกับเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ให้แก่บุคลากรทุกคน

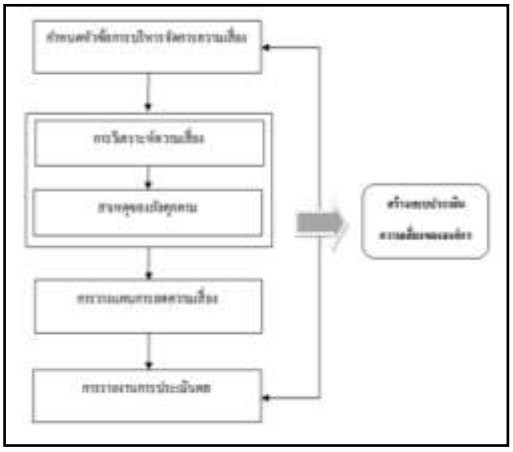
4.1.6 ด้านงบประมาณสนับสนุนการวิจัยพื้นฐานและวิจัยเชิงประยุกต์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 3.88 แสดงให้เห็นว่า องค์กรสนับสนุนการ

วิจัยพื้นฐานและวิจัยเชิงประยุกต์ด้านความมั่นคงปลอดภัยไซเบอร์ มีงบประมาณสนับสนุนในการตีพิมพ์บทความการวิจัย และมีงบประมาณสนับสนุนในการจัดสัมมนาทางด้านความมั่นคงปลอดภัยไซเบอร์

4.1.7 ด้านความร่วมมือกับหน่วยงานอื่นๆ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.09 แสดงให้เห็นว่า องค์กรมีความพร้อมด้านความร่วมมือกับองค์กรภายนอกสถาบันเกี่ยวกับความมั่นคงปลอดภัย มีการจัดตั้งศูนย์ด้านความมั่นคงปลอดภัยเพื่อแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ และมีการจัดบุคลากรเพื่อรับผิดชอบและประสานงานด้านความมั่นคงปลอดภัยไซเบอร์

4.2 ตัวแบบการประเมินความเสี่ยงด้านไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม

ตัวแบบการประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม อธิบายรายละเอียดดังขั้นตอนต่อไปนี้



ภาพที่ 1 ตัวแบบการประเมินความเสี่ยงด้านไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม

1.การกำหนดขอบเขตการจัดการความเสี่ยง (Context Establishment) เช่น ชื่องาน ทำอะไร ขั้นตอนการทำงาน สถานที่ทำงาน เครื่องมือ บุคลากร กำหนดเกณฑ์การประเมินค่าความเสี่ยง กำหนดเกณฑ์ผลกระทบ กำหนดเกณฑ์การยอมรับความเสี่ยง

2. การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นกระบวนการที่ใช้ในการระบุความเสี่ยงการวิเคราะห์ความเสี่ยงและการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงเพื่อมุ่งหวังให้องค์กรบรรลุผลตามเป้าประสงค์ ดังนี้ การวิเคราะห์ความเสี่ยงประกอบด้วย ด้านทรัพย์สินสารสนเทศ ด้านเครือข่าย ซอฟต์แวร์ ฮาร์ดแวร์ ข้อมูล สาเหตุภัยคุกคาม ภายในองค์กร ภายนอกองค์กร

3. การวางแผนการลดความเสี่ยง คือ การดำเนินการเพื่อจัดการหรือตอบสนองต่อความเสี่ยง โดยมีการวางแผนบริหารจัดการความเสี่ยงอย่างเป็นขั้นตอนเพื่อลดความเสี่ยงลง

4. การรายงานและการประเมินผล เพื่อป้องกันการเปลี่ยนแปลงไปจากวัตถุประสงค์ขององค์กรที่กำหนดไว้ และเพื่อบำรุงรักษา ทบทวนความเสี่ยงและดำเนินการประเมินความเสี่ยงอย่างต่อเนื่องโดยกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้นำมากำหนดแผนภาพขั้นตอนเพื่อให้มองกระบวนการประเมินความเสี่ยงได้อย่างชัดเจน

5. สรุปผลการวิจัย

5.1 เพื่อศึกษาและวิเคราะห์ความเสี่ยง และความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม ผลการวิจัยพบว่า ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยามโดยรวมอยู่ในระดับมีความพร้อมมาก

5.2 เพื่อนำเสนอตัวแบบการะประเมินความเสี่ยง และความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม ผลการวิเคราะห์หาระดับความเสี่ยงของตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับวิทยาลัยเทคโนโลยีสยาม ใช้การหาค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน พบว่า ระดับความเสี่ยงในการนำไปใช้งานสำหรับวิทยาลัยเทคโนโลยีสยามโดยรวมอยู่ในระดับความเสี่ยงน้อย

6. ข้อเสนอแนะ

มาตรฐานสากลที่นำมาพิจารณาประกอบการวิจัย : มาตรฐานด้านความมั่นคงปลอดภัยและมาตรฐานการบริหารความเสี่ยงมีมากมายที่สามารถนำมาประยุกต์ใช้ โดยคำนึงถึงความสอดคล้องกับวิสัยทัศน์ พันธกิจและยุทธศาสตร์ขององค์กรนั้น ๆ

7. เอกสารอ้างอิง

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554-2563 ของประเทศไทย, ครั้งที่ 1, 2554.

[2] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, แผนแม่บท ICT-Security แห่งชาติ, 2550.

[3] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, กรอบนโยบายความมั่นคงปลอดภัยไซเบอร์, 2550.

[4] ธนกร มีหินกอง, ตัวแบบการตรวจหาการบุกรุกเชิงเวลาจริงแบบปรับตัวในการรักษาความมั่นคงปลอดภัยไซเบอร์บนพื้นฐานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์, 2556.

[5] น้ำหนึ่ง กล้าหาญ, โปรแกรมประยุกต์สำหรับการประเมินความมั่นคงปลอดภัยสารสนเทศในองค์กรปกครองส่วนท้องถิ่นในจังหวัดสุพรรณบุรี, 2555.

[6] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), CYBERSECURITY IS OUT MISSION, 2555.

[7] CHEANG, S. “Conceptual Model for Cybersecurity Readiness Assessement for Public Institutions In Developing Country: Cambodia” IEEE Xplore Digital Library, 2009.

[8] ITU-T X.1200-X.1299, Series X: Data Networks, “Open System Communications and Security,” [Online] Available at : http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU NationalCybersecurityStrategy Guide.pdf, [Accessed: June 15, 2014].

[9] Rossouw von Solms. **“**From information security to cyber security**”** Computers & Security, 2013.

ประวัติผู้เขียน: นางสาววิภารัตน์ ปทักขินัง

E- mail: wiparatkataa@yahoo.com

การศึกษา: ปริญญาตรีบริหารธุรกิจบัณฑิต (บ.ธบ.) สาขาคอมพิวเตอร์ธุรกิจ
จาก วิทยาลัยเทคโนโลยีสยาม

ปัจจุบัน:

- เลขานุการบริหาร สำนักงานอธิการบดีกิตติคุณ วิทยาลัยเทคโนโลยีสยาม
- กรรมการและผู้ช่วยเลขานุการคณะจัดงาน The fourth National and International Congress on Interdisciplinary Research and Development
- กรรมการคณะจัดงาน The Tenth International Conference on eLearning for Knowledge-Based Society
- คณะจัดทำวารสาร International Journal of the Computer, The Internet and Management (IJCIM)

ประวัติผู้เขียน: รศ.ดร.ประสงค์ ปราณีตพลกรัง

การศึกษา:

- ปริญญาตรี สาขาวิชาวิศวกรรมไฟฟ้า (เกียรตินิยมอันดับ 1) จากโรงเรียนนายเรืออากาศ พ.ศ. 2530
- ปริญญาโท สาขาวิชาวิศวกรรมคอมพิวเตอร์และ ปริญญาโท สาขาวิชาวิศวกรรมไฟฟ้า พ.ศ. 2532 และ 2536 ตามลำดับ จากสถาบันเทคโนโลยีแห่งรัฐฟลอริดา
- ปริญญาเอก สาขาวิชาวิศวกรรมคอมพิวเตอร์ พ.ศ. 2537 จากสถาบันเทคโนโลยีแห่งรัฐฟลอริดา (Florida Institute of Technology) สหรัฐอเมริกา

ปัจจุบัน:

- อาจารย์ผู้ทรงคุณวุฒิประจำคณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
- อุปนายกสมาคมคอมพิวเตอร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์
- ที่ปรึกษา วิศวกรรมสถานแห่งประเทศไทยในพระบรมราชูปถัมภ์ (วสท.) ในสาขาวิศวกรรมคอมพิวเตอร์
- มีความสนใจและทำวิจัยเกี่ยวกับ Computer and Information Security, Cybersecurity, Information Technology Management, e-Learning Technology, e-Business Innovation, Knowledge Management, และ Software Engineering ปัจจุบันมีผลงานทางวิชาการที่ได้รับการตีพิมพ์ทั้งในและต่างประเทศมากกว่า 120 เรื่อง ตำราวิชาการกว่า 10 เล่ม
- **นักวิจัยแห่งชาติด้านเทคโนโลยีสารสนเทศ NR: 52-11-0036**
- **วิศวกรยอดเยี่ยมแห่งชาติ** ด้าน Computer Security ประจำปี พ. ศ. ๒๕๕๕ โดยสมาคมวิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท). สาขาวิศวกรรมคอมพิวเตอร์
- รางวัล **"บุคคลคุณภาพตัวอย่างแห่งปี ๒๕๕๖" สาขาเทคโนโลยีสารสนเทศและการสื่อสาร** จาก มูลนิธิสภาวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย (มสวท.) กระทรวงวิทยาศาสตร์และเทคโนโลยี
- รางวัล **วิศวกรยอดเยี่ยมของอาเซียน** (ASEAN Outstanding Engineering Achievement – Contribution Award) ปี ๒๕๕๖