วารสารปราชญ์ประชาคม
ปีที่ 2 ฉบับที่ 5 กันยายน-ตุลาคม 2567
Journal of Scholar Community
Vol.2 No.5 September- October 2024

การศึกษา

มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน

ธวัชชัย สุขสาย [1*]
ดิฐภัทร บวรชัย [2]

รับบทความ: 9 สิงหาคม 2567 แก้ไขบทความ: 18 ตุลาคม 2567 ตอบรับบทความ: 30 ตุลาคม 2567

บทคัดย่อ

บทความมีวัตถุประสงค์เพื่อ 1) ศึกษาสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน 2) เปรียบเทียบสภาพสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน จำแนกตามลักษณะข้อมูลส่วนบุคคล และ3) นำเสนอมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน การวิจัยครั้งนี้เป็นการวิจัยแบบผสานวิธี (Mixed Method Research) เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลได้แก่แบบสอบถาม (Questionnaire) กับกลุ่มตัวอย่าง 377 คน และการสัมภาษณ์แบบเชิงลึก (In-Depth Interview) กับผู้เชี่ยวชาญ จำนวน 8 คน สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ค่าความถี่ ร้อยละ สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน สถิติอ้างอิงได้แก่ One-way ANOVA ผลการวิจัยพบว่ามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวคิดในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภาครัฐด้านพลังงาน โดยมีข้อเสนอแนะที่สำคัญคือ นำมาตรการในการรักษาความมั่นคงปลอดภัยภาครัฐด้านพลังงานไปประยุกต์ใช้ในการบริหารจัดการโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงาน

คำสำคัญ: การรักษาความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ ภาครัฐด้านพลังงาน

[1] นักศึกษาหลักสูตร รป.ม. สาขาวิชาการจัดการความปลอดภัย คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ
[*] อีเมล: np2915@gmail.com
[2] รศ.ดร. อาจารย์ประจำหลักสูตร รป.ม. สาขาวิชาการจัดการความปลอดภัย คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ

A Study on Cybersecurity Measures in the Government Energy Sector

Thawatchai Suksai [1*]
Dithapart Borwornchai [2]

Abstract

The objectives of this article are: 1) to examine the current state of cybersecurity in the government energy sector, 2) to compare the current state of cybersecurity in the government energy sector categorized by personal data types, and 3) to propose measures for enhancing cybersecurity in the government energy sector. This research adopts a Mixed Method Research approach. The data collection tools used include a questionnaire with a sample of 377 participants and in-depth interviews with 8 experts. The statistical methods for data analysis include frequency, percentage, and descriptive statistics such as mean and standard deviation, while inferential statistics involve One-way ANOVA. The research findings reveal that key cybersecurity measures consist of prevention, response, and risk mitigation against cyber threats, following the concept of cybersecurity in the government energy sector. A key recommendation is to apply these cybersecurity measures to the management of critical information infrastructure in relevant agencies.

Keywords: Cybersecurity, Cyber threats, Government Energy Sector

[1] Student of the Master of Public Administration in Security Management, Faculty of Police Science, Royal Police Cadet Academy.
[*] Email: np2915@gmail.com
[2] Associate Professor Dr., Program Chair of the Master of Public Administration in Security Management Faculty of Police Science Royal Police Cadet Academy.

บทนำ

อุตสาหกรรมด้านพลังงานและสาธารณูปโภคนับเป็นโครงสร้างพื้นฐานสำคัญของประเทศ การสร้างความมั่นคงปลอดภัยไซเบอร์อย่างแข็งแกร่งในภาคส่วนนี้จึงเป็นสิ่งสำคัญอันดับต้นในการบริหารจัดการภายในโรงงานผลิตพลังงาน เพราะหากเกิดเหตุภัยคุกคามไซเบอร์ภายในโรงงาน ย่อมกระทบต่อทุกภาคส่วนและสร้างความเสียหายมหาศาลต่อประชาชนทั่วไป รวมไปถึงประเทศชาติด้วยในช่วงหลายปีที่ผ่านมานั้นมีเหตุอาชญากรรมไซเบอร์ที่มุ่งโจมตีอุตสาหกรรมพลังงานและสาธารณูปโภค ซึ่งสร้างผลกระทบต่อการดำรงชีวิตและการดำเนินงานของผู้คนในระดับมหภาค เช่น การโจมตีโรงไฟฟ้าในยูเครนผ่านฟิชชิ่ง อีเมล (Phishing Email) ทำให้ประชาชนกว่า 2 แสนคน ไม่มีไฟฟ้าใช้นานถึง 6 ชั่วโมง การโจมตีเรียกค่าไถ่โคโลเนียล ไปป์ไลน์ (Colonial Pipeline) บริษัทท่อส่งน้ำมันรายใหญ่ในสหรัฐอเมริกา ทำให้การส่งน้ำมันทางท่อต้องหยุดชะงักลง Kaspersky ICS CERT Report (2019)

สำหรับภัยคุกคามทางไซเบอร์ของภาครัฐด้านพลังงานในประเทศไทย โดยศูนย์ปฏิบัติการ CERT รายงานว่าในปี 2566 พบการโจมตีทางไซเบอร์ จำนวน 775 ครั้ง ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภาครัฐด้านพลังงานหรือระบบงานที่มีความสำคัญอื่น ๆ ได้รับผลกระทบจำนวน 485 รายการ

ตารางที่ 1 จำแนกตามทรัพย์สินทางสารสนเทศที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	33
เครื่องเวิร์กสเตชัน (Workstation)	171
สวิตช์ (Switch) /เราเตอร์ (Router)	241
เว็บไซต์ (Website)	8
อื่น ๆ	33

ตารางที่ 2 จำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

คำอธิบาย	จำนวน
เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	1
การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	30
การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	358
การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	0

คำอธิบาย	จำนวน
การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	8
การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	46
การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	0
การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	35
เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	0
เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	8

จากการที่อุตสาหกรรมพลังงานและสาธารณูปโภคตกเป็นเป้าโจมตีทางไซเบอร์อันดับต้น ๆ นั้น ในภาพรวมแล้ว โรงงานผลิตพลังงานและให้บริการสาธารณูปโภคในประเทศไทยก็มีการตื่นตัวและเตรียมความพร้อมในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตั้งแต่การเปลี่ยนระบบสกาดา (SCADA) ภายในโรงผลิตพลังงานให้ทันสมัยขึ้นและการแบ่ง เซ็กเมนต์ (Segment) ของการแบ่งเครือข่าย (Network Segmentation) เพื่อรองรับการทำงานร่วมกันอย่างมั่นคงปลอดภัยของระบบไอที (IT)และโอที (OT) ไปจนถึงการจัดการการเข้าถึงข้อมูลภายในโรงงาน พร้อมการจัดหาผู้เชี่ยวชาญเข้ามาสนับสนุนดูแลด้านความมั่นคงปลอดภัยไซเบอร์

จากแนวคิดและปัญหาดังกล่าวข้างต้น ผู้วิจัยจึงสนใจที่จะศึกษามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน เพื่อเป็นประโยชน์การเป็นแนวทางการส่งเสริม การจัดทำแผน และการพัฒนาบุคลากรในการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านพลังงาน เพื่อจะช่วยให้ภาครัฐด้านพลังงานมีเป้าหมายและทิศทางในการบริหารและพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน
2. เพื่อเปรียบเทียบสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน จำแนกตามลักษณะข้อมูลส่วนบุคคล
3. เพื่อนำเสนอมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน

ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. เป็นข้อมูลที่หน่วยงานที่มีบทบาทหน้าที่เกี่ยวอุตสาหกรรมด้านพลังงาน โดยการสร้างเครือข่ายความร่วมมือ การจัดทำนโยบายและวางแผนพัฒนาในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เกิดความยั่งยืนในด้านพลังงาน

2.ให้หน่วยงานของรัฐที่เกี่ยวข้องด้านพลังงาน สามารถกำหนดยุทธศาสตร์ กลยุทธ์ และแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อความมั่นคงทางด้านพลังงาน

3. เพื่อเป็นแนวทางในการศึกษาสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่ต้องการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

4. ได้แนวทางในการปรับปรุง พัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์

วรรณกรรมและทฤษฎีที่เกี่ยวข้อง

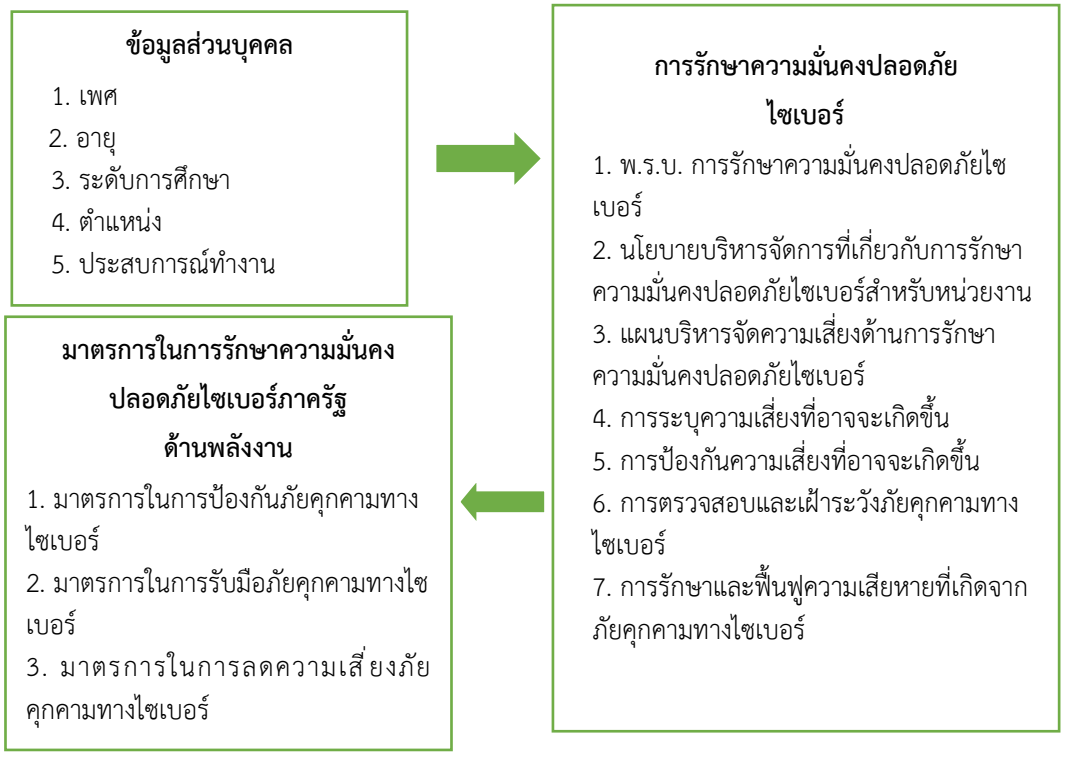
มาตรการในการรักษาความมั่นคงไซเบอร์ภาครัฐด้านพลังงาน คือชุดเครื่องมือที่นำมาใช้ในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งอยู่ในรูปแบบ กฎหมาย ประกาศ นโยบายแบวปฏิบัติต่าง ๆ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีบทบัญญัติเพื่อ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่จะทำให้เกิดผลกระทบต่อภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562) ประกาศคณะกรรมการ กกม. เรื่อง ลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 มีวัตถุประสงค์เพื่อกำหนดลักษณะภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤต ที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ (ประกาศคณะกรรมการ กกม., 2564) และการจัดการระบบเทคโนโลยีสารสนเทศ โดยมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้แก่ NIST Cybersecurity ถูกแบ่งออกเป็น 5 ส่วน ดังนี้ 1) Identify 2) Protect 3) Detect กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ 4) Response และ 5) Recover (NIST, 2018) ISO/IEC 27001 การจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ดังนี้ 1) Security Policy 2) Organization of Information Security 3) Human Resource Security 4) Asset Management 5) Access Control 6) Cryptography 7) Physical and Environmental Security 8) Communications Security) และ 9) Compliance (ISO, (n.d.). และ ISACA Germany Chapter e.V., (n.d.) และ COBIT ย่อมาจาก (Control Objectives for Information and Related Technology) มี 5 กระบวนการ ดังนี้ 1) การตอบสนองความต้องการของผู้มีส่วนได้เสีย 2) การกำกับดูแลระบบเทคโนโลยีสารสนเทศทั่วทั้งองค์กร 3) ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว 4) วิธีปฏิบัติแบบองค์รวม ในการกำกับดูแลและการบริหารจัดการระบบเทคโนโลยีสารสนเทศ 5) แบ่งแยกการกำกับดูแลออกจากการบริหาร (ISACA, 2018)

สรุปได้ว่า การศึกษามาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน จากการทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง พบว่า สภาพปัจจุบันและสภาพที่พึงประสงค์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน ประกอบด้วย พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน แผนบริหารจัดความ

เสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การระบุความเสี่ยงที่อาจจะเกิดขึ้น การป้องกันความเสี่ยงที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ และนำเสนอแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 3 มาตรการ ดังนี้ มาตรการในการป้องกันภัยคุกคามทางไซเบอร์ มาตรการในการรับมือภัยคุกคามทางไซเบอร์ และ มาตรการในการลดความเสี่ยงภัยคุกคามทางไซเบอร์

กรอบแนวคิด

จากการศึกษาวรรณกรรมและทฤษฎีที่เกี่ยวข้อง สามารถสรุปเป็นกรอบแนวคิดในการวิจัยได้ ดังนี้



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีดำเนินการวิจัย

1. รูปแบบของการวิจัย งานวิจัยนี้เป็นงานวิจัยแบบวิจัยแบบผสานวิธี (Mixed Method Research) ซึ่งประกอบด้วยการวิจัยเชิงปริมาณ ศึกษาสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน เพื่อเปรียบเทียบสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน จำแนกตามลักษณะข้อมูลส่วนบุคคล และการวิจัยเชิงคุณภาพ เพื่อนำเสนอมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน ทั้งนี้ในการศึกษาวิจัยเชิงปริมาณ (Quantitative Research) เก็บรวบรวมข้อมูลโดยใช้แบบสอบถามจากกลุ่มตัวอย่างเจ้าหน้าที่ภาครัฐด้านพลังงาน ส่วนการศึกษาวิจัยเชิงคุณภาพ

(Qualitative Research) เก็บรวบรวมข้อมูลโดยการสัมภาษณ์เชิงลึก (In-depth Interview) กับกลุ่มผู้ให้ข้อมูลสำคัญ (Key informant) ที่เกี่ยวข้อง ได้แก่ เจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน และอาจารย์/ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์พื้นที่วิจัย คือ กรุงเทพมหานคร

2. ประชากรและกลุ่มตัวอย่าง ประชากร คือ บุคลากรในหน่วยงานของรัฐที่มีส่วนเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน 20,000 คน กลุ่มตัวอย่าง คือ เจ้าหน้าที่ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน จำนวน 377 คน ใช้วิธีการคัดเลือกแบบแบ่งประชากรออกเป็น 4 ชั้น โดยใช้หน่วยงานเป็นเกณฑ์ในการแบ่งตามลักษณะของประชากรที่เป็นอยู่และเลือกวิธีการสุ่มแบบแบ่งชั้น กำหนดขนาดกลุ่มตัวอย่าง ในที่นี้ใช้ตารางสำเร็จรูปกำหนดขนาดกลุ่มตัวอย่างของ Krejcie และ Morgan ที่ความเชื่อมั่น 95% และที่ระดับความคลาดเคลื่อน 5% จะได้ขนาดของกลุ่มตัวอย่าง 377 คน สุ่มตัวอย่างแต่ละชั้นด้วยวิธีการสุ่มอย่างง่ายแบบ

3. การสร้างเครื่องมือที่ใช้ในการวิจัย มี 2 ชนิด ได้แก่ 1) แบบสอบถาม เป็นลักษณะเป็นแบบเลือกตอบ (Check List) และใช้มาตรส่วนประมาณค่า (Rating scale) โดยใช้เทคนิคของลิเคริท (Likert Scale) การหาดัชนีความสอดคล้องระหว่างข้อคำถามและวัตถุประสงค์ (Index of Item-Objective Congruence: IOC) ในการศึกษาครั้งนี้มีผู้เชี่ยวชาญให้ค่า IOC จำนวน 3 คน วีระยุทธ พรพจน์ธนมาศ (2565)หาค่าความเชื่อมั่น (Reliability) โดยการหาค่าสัมประสิทธิ์อัลฟ่าของครอนบัด (Cronbach’s alpha coefficient) จะต้องมีค่ามากกว่า 0.70 ยุทธ ไกยวรรณ์ (2555) ใช้ศึกษาเจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน 2) แบบสัมภาษณ์ การสัมภาษณ์เชิงลึก (In-depth Interview) ใช้ศึกษา เจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน และอาจารย์/ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4. การเก็บรวบรวมข้อมูล โดยขออนุญาตผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารหน่วยงานด้านพลังงาน ผ่านทางคณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ เพื่อเข้าทำการเก็บข้อมูลแบบสอบถาม ระหว่างเดือน มิถุนายน ถึงเดือน กรกฎาคม พ.ศ. 2567

5. การวิเคราะห์ข้อมูล นำข้อมูลเชิงปริมาณมาวิเคราะห์ด้วยสถิติค่าความถี่ ร้อยละ สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน สถิติอ้างอิงได้แก่ One-way ANOVA ส่วนข้อมูลเชิงคุณภาพ ใช้การวิจัยเอกสาร วิเคราะห์ สังเคราะห์ข้อมูลแล้วนำมาเขียนบรรยายเชิงพรรณนา

ผลการวิจัย

วัตถุประสงค์ที่ 1 ผลการวิจัยพบว่า 1) ข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม ผลการศึกษาพบว่ากลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย จำนวน 276 คน มีอายุระหว่าง 31-40 ปี มีการศึกษาในระดับปริญญาตรี 265 คน มีตำแหน่งเป็นนักระบบงานคอมพิวเตอร์ 164 คน และมีประสบการณ์การทำงาน 11 – 20 ปี จำนวน

262 คน จากกลุ่มตัวอย่างทั้งหมด 377 คน และสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน พบว่าระดับสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน ของผู้ตอบแบบสอบถามมีภาพรวมอยู่ในระดับมาก ($\overline{X}$ = 4.03, S.D. = .38) เมื่อพิจารณาแต่ละด้านพบว่ารายการที่มีค่าเฉลี่ยสูงสุด คือ ด้านแผนบริหารจัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ($\overline{X}$ = 4.08, S.D. = .38) ด้านการระบุความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 4.08, S.D. = .37) รองลงมา คือ ด้านนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน ซึ่งค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 4.05, S.D= .47) วัตถุประสงค์ที่ 2 ผลการวิจัยพบว่า ข้อมูลส่วนบุคคลที่มีเพศ มีภาพรวมไม่แตกต่างกัน ข้อมูลส่วนบุคคลที่มีอายุ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .01 ระดับการศึกษา แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ตำแหน่งปัจจุบัน แตกต่างกัน มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .01 ประสบการณ์ทำงาน แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ .01

ตารางที่ 3 จำนวนและร้อยละลักษณะข้อมูลส่วนบุคคล จำแนกตามเพศ

สถานภาพของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
เพศ	ชาย	276	73.2
	หญิง	101	26.8
	รวม	377	100

จากตารางที่ 3 ผู้ตอบแบบสอบถามจำนวน 377 คน จำแนกตามเพศ พบว่าส่วนใหญ่เป็นเพศชาย จำนวน 276 คน คิดเป็นร้อยละ 73.2 และเพศหญิง จำนวน 101 คน คิดเป็นร้อยละ 26.8

ตารางที่ 4 จำนวนและร้อยละลักษณะข้อมูลส่วนบุคคล จำแนกตามอายุ

สถานภาพของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
อายุ	ไม่เกิน 30 ปี	9	2.4
	31 – 40 ปี	256	67.9
	41 – 50 ปี	89	23.6
	มากกว่า 50 ปี	23	6.1
	รวม	377	100

จากตารางที่ 4 ผู้ตอบแบบสอบถามจำนวน 377 คน จำแนกตามอายุ พบว่าส่วนใหญ่มีอายุระหว่าง 31 – 40 จำนวน 256 คน คิดเป็นร้อยละ 67.9 รองมามีอายุระหว่าง 41 – 50 ปี จำนวน 89 คน คิดเป็นร้อยละ 23.6 อายุมากกว่า 50 ปี จำนวน 23 คน คิดเป็นร้อยละ 6.1 และ อายุไม่เกิน 30 ปี จำนวน 9 คน คิดเป็นร้อยละ 2.4 ตามลำดับ

ตารางที่ 5 จำนวนและร้อยละลักษณะข้อมูลส่วนบุคคล จำแนกตามระดับการศึกษา

สถานภาพของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
3. ระดับการศึกษา	ต่ำกว่าปริญญาตรี	7	1.9
	ปริญญาตรี	265	70.3
	ปริญญาโท	101	26.8
	ปริญญาเอก	4	1.1
	รวม	377	100

จากตารางที่ 5 ผู้ตอบแบบสอบถามจำนวน 377 คน จำแนกตามระดับการศึกษา พบว่าส่วนใหญ่มีระดับการศึกษาปริญญาตรี จำนวน 265 คน คิดเป็นร้อยละ 70.3 รองลงมามีระดับการศึกษาปริญญาโท จำนวน 101 คน คิดเป็นร้อยละ 26.8 ระดับการศึกษาต่ำกว่าปริญญาตรี จำนวน 7 คน คิดเป็นร้อยละ 1.9 และระดับการศึกษาปริญญาเอก จำนวน 4 คน คิดเป็นร้อยละ 1.1 ตามลำดับ

ตารางที่ 6 จำนวนและร้อยละลักษณะข้อมูลส่วนบุคคล จำแนกตามตำแหน่งปัจจุบัน

สถานภาพของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
ตำแหน่งปัจจุบัน	ผู้อำนวยฝ่าย/กอง	11	2.9
	รองผู้อำนวยฝ่าย/กอง	5	1.3
	ผู้ช่วยผู้อำนวยฝ่าย/กอง	11	2.9
	หัวหน้าฝ่าย/กลุ่ม/แผนก	15	4.0
	วิศวกร	108	28.6
	นักระบบงานคอมพิวเตอร์	164	43.5
	นักคอมพิวเตอร์	58	16.4
	อื่น ๆ โปรดระบุ	5	1.3
	รวม	377	100

จากตารางที่ 6 ผู้ตอบแบบสอบถามจำนวน 377 คน จำแนกตามตำแหน่งปัจจุบัน พบว่าส่วนใหญ่มีตำแหน่งนักระบบงานคอมพิวเตอร์ จำนวน 164 คน คิดเป็นร้อยละ 43.5 รองลงมามีตำแหน่งวิศวกร จำนวน 108 คน คิดเป็นร้อยละ 28.6 ตำแหน่งนักคอมพิวเตอร์ จำนวน 58 คน คิดเป็นร้อยละ 16.4 ตำแหน่งหัวหน้าฝ่าย/กลุ่ม/แผนก จำนวน 15 คิดเป็นร้อยละ 4.0 ตำแหน่งผู้อำนวยฝ่าย/กอง จำนวน 11 คน คิดเป็นร้อยละ 2.9 ตำแหน่งผู้ช่วยผู้อำนวยฝ่าย/กอง จำนวน 11 คน คิดเป็นร้อยละ 2.9 ตำแหน่งรองผู้อำนวยฝ่าย/กอง จำนวน 5 คน คิดเป็นร้อยละ 1.3 และตำแหน่งอื่น ๆ เช่น นักวิชาการระดับ 10 นักประมวลผลข้อมูล พนักงาน และ พนักงานคอมพิวเตอร์ จำนวน 5 คน คิดเป็นร้อยละ 1.3 ตามลำดับ

ตารางที่ 7 จำนวนและร้อยละลักษณะข้อมูลส่วนบุคคล จำแนกตามประสบการณ์ทำงาน

สถานภาพของผู้ตอบแบบสอบถาม		จำนวน	ร้อยละ
ประสบการณ์ทำงาน	ต่ำกว่า 10 ปี	13	3.4
	11 - 20 ปี	262	69.5
	21 - 30 ปี	83	22
	30 ปี ขึ้นไป	19	5.0
	รวม	377	100

จากตารางที่ 7 ผู้ตอบแบบสอบถามจำนวน 377 คน จำแนกตามประสบการณ์ทำงานพบว่าส่วนใหญ่มีประสบการณ์ระหว่าง 11 - 20 ปี จำนวน 262 คน คิดเป็นร้อยละ 69.5 รองลงมามีประสบการณ์ระหว่าง 21 - 30 ปี จำนวน 83 คน คิดเป็นร้อยละ 22 ประสบการณ์ทำงาน 30 ปี ขึ้นไป จำนวน 19 คน คิดเป็นร้อยละ 5.0 และ ประสบการณ์ทำงานต่ำกว่า 10 ปี จำนวน 13 คน คิดเป็นร้อยละ 3.4 ตามลำดับ

ตารางที่ 8 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน สภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน

สภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน	สภาพปัจจุบัน		แปลผล
	$\bar{X}$	S.D.	
1.ด้านพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์	4.00	.45	มาก
2. ด้านนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน	4.05	.47	มาก
3. ด้านแผนบริหารจัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	4.08	.38	มาก
4. ด้านการระบุความเสี่ยงที่อาจจะเกิดขึ้น	4.08	.34	มาก
5. ด้านการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	3.99	.39	มาก
6. ด้านการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	4.00	.55	มาก
7. ด้านการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	4.02	.58	มาก
รวม	**4.03**	**.38**	**มาก**

จากตารางที่ 8 พบว่าระดับสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน ของผู้ตอบแบบสอบถามมีภาพรวมอยู่ในระดับมาก ($\overline{X}$ = 4.03, S.D. = .378) เมื่อพิจารณาแต่ละด้านพบว่ารายการที่มีค่าเฉลี่ยสูงสุด คือ ด้านการระบุความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 4.08, S.D. = .337) และด้านแผนบริหารจัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 4.08, S.D= .383) รองลงมา คือ ด้านนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน ซึ่งค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 4.05, S.D= .472)

วัตถุประสงค์ที่ 2 ผลการวิจัยพบว่า ข้อมูลส่วนบุคคลจำแนกตามเพศ มีภาพรวมไม่แตกต่างกัน ข้อมูลส่วนบุคคลจำแนกตามอายุ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .01 ข้อมูลส่วนบุคคลจำแนกระดับการศึกษา แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ข้อมูลส่วนบุคคลจำแนกตำแหน่งปัจจุบัน แตกต่างกัน มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .01 และข้อมูลส่วนบุคคลจำแนกประสบการณ์ทำงานแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ .01

วัตถุประสงค์ที่ 3 ผลการวิจัยพบว่า มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน มีดังนี้ 1) มาตรการในการป้องกันภัยคุกคามทางไซเบอร์ 2) มาตรการในนการรับมือภัยคุกคามทางไซเบอร์ และ 3) มาตรการในการลดความเสี่ยงภัยคุกคามทางไซเบอร์ ดังภาพที่ 2

ภาพที่ 2 มาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภาครัฐด้านพลังงาน

จากภาพที่ 2 **มาตรการในการป้องกันภัยคุกคามทางโซเบอร์** มาตรการย่อยที่ 1.1 การประเมินความเสี่ยงและการวางแผน คือ ทำการประเมินความเสี่ยงทางไซเบอร์อย่างสม่ำเสมอเพื่อระบุภัยคุกคามและช่องโหว่ที่เกี่ยวข้องกับระบบพลังงาน มาตรการย่อยที่ 1.2 การควบคุมการเข้าถึงและการจัดการข้อมูล คือ การยืนยันตัวตนแบบหลายปัจจัยและการเข้ารหัสข้อมูลสำหรับการส่งข้อมูลที่สำคัญ มาตรการย่อยที่ 1.3 การป้องกัน

และการตรวจจับ คือ ติดตั้งระบบป้องกันการบุกรุก (IPS) และระบบตรวจจับการบุกรุก (IDS) เพื่อตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ มาตรการย่อยที่ 1.4 การตรวจสอบและกำหนดมาตรฐานทางไซเบอร์ คือ กำหนดค่าขั้นต่ำด้านความปลอดภัย เครื่องผู้ใช้งาน เครื่องแม่ข่าย และอุปกรณ์ และมาตรการย่อยที่ 1.5 การฝึกอบรมและการสร้างความตระหนัก คือ จัดการฝึกอบรมและลงทุนกับระบบความปลอดภัย **มาตรการในการรับมือภัยคุกคามทางไซเบอร์** มาตรการย่อยที่ 2.1 การตรวจจับและการระบุเหตุการณ์ คือ กระบวนการและเครื่องมือในการระบุและจำแนกประเภทของภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับระบบพลังงาน มาตรการย่อยที่ 2.2 การประเมินผลกระทบและการตอบสนอง คือ ประเมินผลกระทบที่เกิดจากเหตุการณ์ไซเบอร์ต่อระบบพลังงานและกำหนดลำดับความสำคัญในการตอบสนอง มาตรการย่อยที่ 2.3 การติดตามและการตอบสนองต่อเหตุการณ์ คือ ระบบการติดตามและการตอบสนองต่อเหตุการณ์ ไซเบอร์ที่มีประสิทธิภาพ มาตรการย่อยที่ 2.4 การทบทวนและการปรับปรุงเหตูการทางไซเบอร์ คือ ปรับปรุงแผนการตอบสนองต่อเหตุการณ์ไซเบอร์ มาตรการย่อยที่ 2.5 การสื่อสารและการรายงาน คือ รายงานเหตุการณ์ไซเบอร์และผลกระทบต่อหน่วยงานรัฐบาลหรือหน่วยงานความมั่นคงไซเบอร์แห่งชาติตามกฎหมาย **มาตรการในการลดความเสี่ยงภัยคุกคามทางไซเบอร์** มาตรการย่อยที่ 3.1 การวางแผนและการประเมินความเสี่ยง คือ การประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อระบุภัยคุกคามและช่องโหว่ มาตรการย่อยที่ 3.2 การฟื้นฟูและการกู้คืน คือ ดำเนินการฟื้นฟูระบบและข้อมูลที่ได้รับผลกระทบจากเหตุการณ์ไซเบอร์ มาตรการย่อยที่ 3.3 การปรับปรุงและการทบทวนความมั่นคงปลอดภัยไซเบอร์ คือ ทบทวน ปรับปรุงนโยบาย และซ้อมแผนทางไซเบอร์ มาตรการที่ 3.4 การสำรองข้อมูลและการกู้คืน คือ จัดทำแผนการสำรองข้อมูลและการกู้คืนข้อมูลได้ในกรณีเกิดเหตุการณ์ไซเบอร์ มาตรการย่อยที่ 3.5 การร่วมมือและการแบ่งปันข้อมูล คือ ร่วมมือกับหน่วยงานรัฐและองค์กรอื่น ๆ ในการแบ่งปันข้อมูลและแนวทางปฏิบัติที่ดีที่สุดในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์

อภิปรายผล

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า สภาพปัจจุบันอยู่ในระดับมากเมื่อพิจารณาสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงานที่มีค่าเฉลี่ยสูงสุดคือมีการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซบอร์เนื่องจากหน่วยงานภาครัฐด้านพลังงานให้ความสำคัญกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งสอดคล้องกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2562) ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรา 45 สอดคล้องกับ National Institute of Standards and Technology: NIST (2018) Framework ที่ 1 Identify กิจกรรมการระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ การประเมินช่องโหว่และการทดสอบเจาะระบบ

(Vulnerability Assessment and Penetration Testing) ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยไซเบอร์และการควบคุม

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า ความคิดเห็นที่มีลักษณะข้อมูลส่วนบุคคลจำแนกตามเพศ ไม่มีผลต่อสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนที่จำแนกตามอายุ ระดับการศึกษา ตำแหน่งและประสบการณ์ทำงาน แตกต่างกัน มีผลต่อสภาพปัจจุบันในการรักษาความมั่นคงปลอดภัยไซเบอร์ มีภาพรวมแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .01 สอดคล้องกับ สุธาเทพ รุณเรศ (2561) ที่พบว่าปัจจัยทางด้านลักษณะทางประชากรมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต เพศไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .05 ส่วนที่จำแนกตามอายุ และประสบการณ์ทำงาน แตกต่างกัน อย่างมีนัยสำคัญที่ระดับ .05 แสดงว่า กลุ่มตัวอย่าง ที่มีอายุมากว่า 50 ปี ข้อมูลส่วนบุคคลที่มีประสบการณ์ทำงานมากกว่า 30 ปี เข้าใจมีความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่า มาตรการในการป้องกันภัยคุกคามทางไซเบอร์ จะเห็นได้ว่าการการป้องกันภัยคุกคามทางไซเบอร์ เป็นสิ่งสำคัญจำเป็น ควรมีการดำเนินการเป็นลำดับแรกในการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐด้านพลังงาน ซึ่งสอดคล้องกับ National Institute of Standards and Technology: NIST (2018) Framework ที่ 2 Protect กิจกรรมการวางมาตรฐานควบคุมเพื่อปกป้อง แนวทางในการรับมือภัยคุกคามทางไซเบอร์ สอดคล้องกับ ชรินทร์ทิพย์ ปั้นสุวรรณ (2564) กล่าวไว้ว่า แนวทางการรับมือภัยคุกคามทางไซเบอร์และการกำกับดูแลการบริหารจัดการที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 4 ขั้นตอน 1) การกำกับดูแลและการบริหารความเสี่ยง 2) มาตรฐานและมาตรการเฝ้าระวังภัยไซเบอร์ 3) การประสานความร่วมมือและถ่ายทอดสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสีย และ 4) การติดตามและประเมินผลลัพธ์ แนวทางในการลดความเสี่ยงภัยคุกคามทางไซเบอร์ จะเห็นได้ว่าการรับมือภัยคุกคามทางไซเบอร์ เป็นลำดับสุดท้าย ซึ่งสอดคล้องกับ National Institute of Standards and Technology: NIST (2018) Framework ที่ 3 Detect กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ต้องสร้างกลไกและกระบวนการเพื่อตรวจรับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

สรุปและข้อเสนอแนะ

สรุปผลการวิจัย

มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ภาครัฐพลังงาน คือ การป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ ซึ่งเป็นการปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพและประสิทธิผล เพื่อสร้างแนวคิดความปลอดภัย (Security Mindset) เสริมเกราะป้องกันความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นแก่เจ้าหน้าที่ผู้ปฏิบัติงาน ตลอดจนผู้บริหารระดับสูง

ข้อเสนอแนะเชิงนโยบาย

1. ควรจัดตั้งศูนย์ CSOC ของภาครัฐด้านพลังงาน เป็นศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ Cyber Security Operation Center เพื่อปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ตลอด 24 ชั่วโมง และยังคอยให้คำปรึกษา แนะนำวิธีการรับมือ และวิธีการแก้ไขปัญหาต่าง ๆ ที่เกี่ยวกับภัยคุกคามแบบตรงจุด เพื่อแก้ไขปัญหาได้อย่างรวดเร็ว ลดระดับความรุนแรงของผลกระทบที่อาจจะสร้างความเสียหายทางธุรกิจภาครัฐด้านพลังงานเป็นวงกว้าง

2. ภาครัฐควรให้การสนับสนุน และการดำเนินการวิจัยและพัฒนาเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับการรับมือกับอาชญากรรมไซเบอร์อย่างจริงจัง ซึ่งการวิจัยพัฒนาเป็นส่วนสำคัญในการสร้างความแข็งแกร่งให้แก่หน่วยงาน บุคลากร และยังช่วยประหยัดงบประมาณที่ต้องนาเข้านวัติกรรมและเทคโนโลยีจากต่างประเทศ

ข้อเสนอสำหรับการทำวิจัยครั้งต่อไป

1. ควรการศึกษาเปรียบเทียบประสิทธิผลและประสิทธิภาพของการบริหารจัดการกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่น เช่น ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ เพื่อเรียนรู้และค้นหาแนวทางในการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อป้องกันภัยคุกคามทางไซเบอร์

2. หน่วยงานภาครัฐด้านพลังงาน ควรทบทวนนโยบาย ประกาศ และ แนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์เป็นประจำ และพัฒนามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ให้หลากหลาย เท่าทันกับเทคโนโลยีไซเบอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อสามารถป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามไซเบอร์ใหม่ ๆ ที่อาจพัฒนามาในรูปแบบที่แตกต่างไปจากเดิม

บรรณานุกรม

จิตราภรณ์ โสตถิกุล. (2565). *การก่อการร้ายทางไซเบอร์: ปัญหาการนิยาม เขตอำนาจ และการบังคับใช้กฎหมาย.* ปริญญานิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์.

ชฎาภรณ์ สิงห์แก้ว. (2563). *บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม.* ปริญญาปรัชญาดุษฎีบัณฑิต. มหาวิทยาลัยรามคำแหง.

ชรินทร์ทิพย์ ปั้นสุวรรณ. (2565). *แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล.* ปริญญาศิลปศาสตรดุษฎีบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (27 พฤษภาคม 2562). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนพิเศษ 96 ก หน้า 20 - 51.

วิทวัส สุขชีพ และจรัญ แสนราช. (2566). การตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์. *Industrial Technology Journal, 8*(1), 17-30.

หยัดซารี เล๊าะเหล๊ะ. (2564). *การประเมินช่องโหว่ของเว็บไซต์ในองค์กร เพื่อป้องกันการถูกโจมตีทางไซเบอร์.* ปริญญาวิทยาศาสตรมหาบัณฑิต. มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

KasperskyICSCERT. (30 September 2019). *Threat landscape for industrial automation systems, H1 2019.* KasperskyICSCERT. https://ics-cert.kaspersky.com/publications/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/

ISACA. (2018). *COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY. Temple University.* https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and- Methodology _res_eng_1118.pdf

_____. (2016). *Implementation Guideline ISO/IEC 27001:2013. ISACA Germany Chapter e.v.* https://www.qal-iran.ir/WebsiteImages/iso/21.PDF

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity. NIST.* https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf