# การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐในประเทศไทย

# The Social Protection from Cyber Threats by Government Organizations in Thailand

ธีระพงษ์ ทศวัฒน์
Teerapong Tossawut
อาจารย์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏราชนครินทร์
Lecturer from the Faculty of Humanities and Social Sciences Rajabhat Rajanagarindra University
*Corresponding Author Email:tteerapong10@gmail.com

Received: 25 June 2025 Revised: 14 July 2025 Accepted: 17 July 2025

**บทคัดย่อ**

บทความวิชาการนี้ มุ่งนำเสนอการป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐในประเทศไทย คือ 1) การเพิ่มความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรภาครัฐ เป็นกลยุทธ์สำคัญในการป้องกันสังคมในการให้บริการประชาชนที่ปลอดภัยจากภัยคุกคามทางไซเบอร์ ช่วยให้บุคลากรและประชาชนมีความรู้ความเข้าใจในการป้องกันตัวเองจากภัยคุกคามต่าง ๆ ช่วยสร้างความไว้วางใจในระบบสารสนเทศของรัฐและทำให้ประชาชนมีความมั่นใจในการใช้บริการภาครัฐ 2) การฝึกอบรมขององค์กรภาครัฐเพื่อช่วยการป้องกันสังคมได้อย่างมีประสิทธิภาพ เพิ่มขีดความสามารถของบุคลากรในการทำงานและการป้องกันสังคมได้อย่างมีประสิทธิภาพ ประชาชนมีคุณภาพชีวิตที่ดีขึ้นผ่านการพัฒนาและบริการขององค์กรภาครัฐ 3) องค์กรภาครัฐพัฒนาสังคมให้ปลอดภัยจากภัยคุกคามทางไซเบอร์จากเทคโนโลยี ป้องกันการโจมตีระบบคอมพิวเตอร์ ส่งผลให้ลดความเสี่ยงต่อการหลอกลวงให้บุคคลเปิดเผยข้อมูลส่วนตัว การหลอกลวงทางออนไลน์ของประชาชน และ 4) การพัฒนาประชาชนด้านการป้องกันสังคมเพื่อความปลอดภัยของข้อมูลและความสงบสุขของประชาชน โดยองค์กรภาครัฐควรมีมาตรการความปลอดภัยไซเบอร์อย่างครอบคลุม เตรียมแนวทางการรับมือที่มีประสิทธิภาพที่สุดเพื่อป้องกันการโจมตีที่ส่งผลกระทบต่อความมั่นคงขององค์กรภาครัฐและประชาชน 5) องค์กรภาครัฐพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ที่โดยบูรณาการความร่วมมือภาคประชาชน เร่งผลักดันการพัฒนาความรู้และทักษะด้านไซเบอร์ให้ครอบคลุมประชาชนคนไทยทุกช่วงวัย เพื่อก้าวสู่การเป็นผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

**คำสำคัญ:** การป้องกันสังคม, ภัยคุกคามทางไซเบอร์, องค์กรภาครัฐในประเทศไทย

**Abstract**

This academic consists purposes to present the protection of society from cyber threats by government organizations in Thailand, namely 1) Increasing cybersecurity awareness of government organizations is an

important strategy for protecting society in providing services to the public that are safe from cyber threats. It helps personnel and the public have knowledge and understanding in protecting themselves from various threats, helps build trust in government information systems, and makes the public confident in using government services 2) Training of government organizations to help protect society effectively, increases the capabilities of personnel in working and protecting society effectively, and the public has a better quality of life through the development and services of government organizations 3) Government organizations develop society to be safe from cyber threats from technology, prevent attacks on computer systems, resulting in a reduction in the risk of deceiving people to reveal personal information, and online fraud of the public 4) Developing people in terms of protecting society for the safety of information and public peace. Government organizations should have comprehensive cybersecurity measures, prepare the most effective response methods to prevent attacks that affect the security of government organizations and the public and 5) Government organizations develop mechanisms to cope with and respond to cyber threats by integrating cooperation from the public sector, and accelerate the development of knowledge and skills.

**Keywords:** Social Development, Cyber Threats, Government Organizations in Thailand

**บทนำ**

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอกมาตรฐานด้านการรักษาความ มั่นคง ปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์การประเมินความเสี่ยงด้านการรักษา ความมั่นคง ปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562 มาตรา 44 เพื่อรับมือกับภัยคุกคามทางไซเบอร์โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ (กรมกิจการเด็กและเยาวชน, 2566, น.4) การเข้าถึงระบบเครือข่ายสารสนเทศและอินเทอร์เน็ตทำได้ง่าย และสะดวกสบายต่อการใช้ชีวิตประจำ แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดและเสี่ยงที่จะเกิดภัยคุกคามต่อชีวิตเพิ่มขึ้น ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดีใช้อินเทอร์เน็ตในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ ภัยที่จะเกิดต่อระบบควบคุมดูแลการใช้งานอินเทอร์เน็ตและระบบปฏิบัติการที่เกี่ยวข้องกับโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ ซึ่งก่อให้เกิดผลกระทบต่อการใช้ชีวิตของประชาชน ก่อให้เกิดความขัดแย้ง ดังนั้น ภาครัฐจึงต้องดูแลรักษาความมั่นคงปลอดภัยเครือข่ายเทคโนโลยีสารสนเทศและอินเทอร์เน็ต ให้มีความมั่นคง ใช้งานได้อย่างต่อเนื่องสามารถป้องกัน แก้ไขปัญหาการถูกเจาะโจมตีระบบและฟื้นตัวกลับมาใช้งานได้ตามปกติได้อย่างรวดเร็วและไม่ให้อินเทอร์เน็ตถูก

นำไปใช้ในทางที่ผิด องค์กรภาครัฐจะต้องตระหนักและมีแนวทางการดำเนินงานของแต่ละหน่วยงาน เพื่อให้การขับเคลื่อนทางเศรษฐกิจ การเมือง สังคม และการป้องกันประเทศ มีภูมิคุ้มกันทางไซเบอร์และมีความสามารถในการแข่งขันกับประเทศอื่น ๆ (กระทรวงคมนาคม, 2566, น.1)

องค์กรภาครัฐ ถือเป็นองค์กรที่มีความสำคัญต่อการพัฒนาเศรษฐกิจและสังคมของประเทศ มีการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ เช่น การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากร การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ กำหนดโครงสร้างการรายงานเหตุการณ์ กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน การตอบสนองต่อเหตุการณ์ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563 จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อ และอุปกรณ์ติดต่อสื่อสารของบุคลากร กลไกรายงานเหตุการณ์ จัดเตรียมอุปกรณ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของกรมพัฒนาสังคมและ สวัสดิการ จัดทำแผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ กำหนดขั้นตอน วิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวข้อง เพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้กรมพัฒนาสังคมและสวัสดิการสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต (กรมพัฒนาสังคมและสวัสดิการ, 2567, น.2)

ปัจจุบันภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงปลอดภัย ความเชื่อมั่น และการให้บริการต่าง ๆ ผ่านอินเทอร์เน็ตมีความสำคัญเป็นลำดับต้น ๆ เมื่อหากมีการให้บริการแก่บุคคลภายนอก หรือภายใน แต่ยังคงอาศัยการเข้าการให้บริการสารสนเทศนั้น ย่อมมีความเสี่ยงต่อภัยคุกคามที่อาจจะเกิดได้ทุกเมื่อ ซึ่งเป็นเรื่องที่ทำความเข้าใจ และแนวทางการคุกคามหรือโจมตีเพื่อนำมาปรับใช้หรือป้องกันระบบใหม่ ความมั่นคงมากขึ้น ภัยคุกคามจากไซเบอร์มุ่งร้ายหรือเป็นสาเหตุของภัยอันตรายต่าง ๆ ที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์ในรูปแบบของการทำร้าย เปิดเผยข้อมูลและรวมถึงการที่ทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้งานได้ โดยภัยคุกคามจะเกิดขึ้นโดยเจตนาของผู้ที่ประสงค์ร้ายต่อระบบ โดยการโจมตีอาจจะเป็นการกระ ทำโดยพยายามที่จะข้ามผ่านระบบป้องกันหรือกระบวนการควบคุมความมั่นคงปลอดภัยของระบบ คอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ มีความเสี่ยงในด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือสถานการณ์ ทำให้เกิดความเสียหายหรือส่งผลกระทบต่อระบบคอมพิวเตอร์ข้อมูล (Cisco, 2021)

จากภัยคุกคามทางไซเบอร์ดังกล่าวการขับเคลื่อนให้คนไทยทุกกลุ่มเข้าถึงความมั่นคงของมนุษย์ จึงต้องมีหลักประกันด้านสังคมทุกด้าน ให้ความสำคัญต่อการป้องกันสังคมขององค์กรภาครัฐที่ แต่ยังพบปัญหาในการปฏิบัติงานด้านภัยทางไซเบอร์ ผลกระทบของเทคโนโลยีไซเบอร์ต่อการป้องกันสังคม จึงเป็นสิ่งจำเป็นต้องช่วยพัฒนาคุณภาพชีวิตของคนในสังคมที่ประสบปัญหา ซึ่งจะส่งผลทำให้เกิดความมั่นคงของมนุษย์และมีหลักประกันด้านสังคมทุกด้านอีกทั้งยังเป็นการการสร้างโอกาสและความเสมอภาคทางสังคม และยังพบปัญหาของการป้องกันสังคมจากภัยทางไซเบอร์ คือ อาสาสมัครที่จะช่วยพัฒนาสังคมขาดทักษะการใช้เทคโนโลยี ขาดความรู้ ความเข้าใจ เกี่ยวกับจริยธรรมและการรักษาข้อมูลส่วนตัว กฎหมาย ระเบียบปฏิบัติไม่เอื้ออำนวยในการส่งต่อข้อมูลส่วนบุคคล กลุ่มเป้าหมายบางส่วนเข้าไม่ถึงข้อมูลในการเข้ารับการช่วยเหลือ เนื่องจากไม่มีโทรศัพท์ สัญญาณอินเทอร์เน็ต

ในพื้นที่ห่างไกลไม่เสถียร มีต้นทุนค่าใช้จ่ายในการดำเนินงานเพิ่มขึ้น เช่น ค่าอินเทอร์เน็ต ไม่สามารถเก็บข้อมูลเคสได้อย่างละเอียดถี่ถ้วน มีการหลอกลวงเจ้าหน้าที่ในการขอรับความช่วยเหลือ โดยที่ไม่ได้ประสบปัญหาจริง ขาดสัมพันธภาพระหว่างผู้ให้บริการกับผู้รับการช่วยเหลือ ขาดความไว้เนื้อเชื่อใจในการเปิดเผยข้อมูลของบุคคล (กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์, 2566, น.7) ประชาชนยังขาดความตระหนักรู้เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ขาดการแสวงหาความร่วมมือกับต่างประเทศเพื่อผลประโยชน์ร่วมกันในการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ (อริสรา กาญจนอุดม, 2567) ความมั่นคงปลอดภัยทางไซเบอร์ เป็นการนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันองค์กรภาครัฐได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น Malware (พลากร ลาภอลงกรณ์, 2567)

ปัจจุบัน เทคโนโลยีทางไซเบอร์ได้มีการพัฒนาไปอย่างก้าวกระโดด ซึ่งพื้นที่ไซเบอร์ได้กลายเป็นปัจจัยหนึ่งสำหรับการดำรงชีวิตของคนในสังคม เมื่อเทคโนโลยีมีการพัฒนามากขึ้น การเข้าถึงเทคโนโลยีของผู้คนจึงเป็นไปได้โดยสะดวกมากขึ้นตาม โดยเทคโนโลยีทางไซเบอร์ที่พัฒนาและเป็นที่นิยมอย่างมากในปัจจุบัน ได้แก่ เทคโนโลยีทางไซเบอร์ในการค้นหาข้อมูล (Search Engine) เช่น Google Yahoo เป็นต้น เทคโนโลยีไซเบอร์ในรูปแบบพื้นที่ทางสังคม อาทิ Facebook Twitter Instagram Line Youtube หรือระบบการประชุมทางไกล ที่กลายมาเป็นช่องทางการติดต่อสื่อสารระหว่างองค์กรภาครัฐและประชาชน ซึ่งเมื่อประชาชนสามารถใช้พื้นที่ทางไซเบอร์ในการทำกิจกรรมต่าง ๆ ส่งผลให้รัฐจำเป็นจะต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยให้กับพื้นที่ทางไซเบอร์ (กนกนก โพธิ์หอม, 2564, น.50)

**บทวิเคราะห์**

การรักษาศักยภาพในการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ขององค์กรภาครัฐในอนาคตที่คาดว่าจะมีความรุนแรงมากขึ้นได้อย่างมีประสิทธิภาพได้นั้น ต้องอาศัยการสนับสนุนจากรัฐบาลเป็นสำคัญและมีการพัฒนาปรับปรุงระบบการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพมากขึ้น ผู้เขียนจึงมุ่งหวังนำเสนอการป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐในประเทศไทย ได้แก่ การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการเพิ่มความตระหนัก การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการฝึกอบรม การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการใช้เทคโนโลยี การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการสร้างมาตรฐาน และการป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการทำงานร่วมกันดังนี้

**1. การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการเพิ่มความตระหนัก**

การให้บริการประชาชนเพื่อให้อยู่ด้วยกันในสังคมด้วยความปลอดภัยและมีประสิทธิภาพ องค์กรภาครัฐมีความตระหนักในการให้ความรู้แก่บุคลากรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพิ่มความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของข้อมูล รวมถึงการตระหนักถึงความเสี่ยงทางไซเบอร์ ภัยคุกคาม และมาตรการป้องกันที่เหมาะสม ตระหนักถึงความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์ผ่านกลยุทธ์การศึกษา และการป้องกัน ซึ่งมีการเสนอแนวทาง เช่น การพัฒนาแพลตฟอร์มเกมสำหรับการศึกษาด้านความ มั่นคงปลอดภัยทางไซเบอร์ ซึ่งรวมถึง การเรียนรู้เกี่ยวกับการโจมตีทางไซเบอร์และ

กลไกการป้องกันต่าง ๆ และเป็นทางเลือกที่ดีกว่าสำหรับการให้ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ไม่ใช่ด้านไอทีและไม่ใช่มืออาชีพ รวมถึงใช้เครื่องมือตรวจจับการบุกรุก องค์กรภาครัฐยังคงมีบทบาทในการเพิ่มความตระหนักถึงสถานการณ์ทางไซเบอร์โดยให้คำแนะนำแก่ผู้ดูแลระบบและองค์กรภาครัฐในการลดความเสี่ยง และผลกระทบจากการโจมตีทางไซเบอร์ เพิ่มความตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในเพื่อการป้องกันสังคมเพิ่มความตระหนักรู้เกี่ยวกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์เพื่อการป้องกันสังคมขององค์กรภาครัฐ ทำให้ประชาชนทั่วไปที่มาใช้บริการองค์กรหรือหน่วยงานภาครัฐมีความรู้และระมัดระวังมากขึ้น โดยเฉพาะในสภาพแวดล้อมที่ต้องการความมั่นคงปลอดภัยโดยการถ่ายทอดความรู้สู่ประชาชนในการอยู่ร่วมกันในสังคม การพัฒนาความมั่นคงปลอดภัยใหม่ ๆ ในอนาคตเพื่อพัฒนาสังคมองค์กรภาครัฐ การส่งเสริมการศึกษาเพื่อให้ผู้เรียนหลังจากจบการศึกษาแล้วสามารถนำไปใช้ในการป้องกันสังคมองค์กรภาครัฐในอนาคต ลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายทางการเงินต่อองค์กรภาครัฐ เพื่อให้การบริหารจัดการทางการเงินที่นำไปสู่การให้บริการประชาชนอย่างเพียงพอละเหมาะสม การมีระบบความมั่นคงปลอดภัยที่เชื่อถือจะสร้างความเชื่อมั่นให้กับผู้คนในสังคม ซึ่งสามารถสร้างมูลค่าและความยั่งยืนให้แก่องค์กรภาครัฐในระยะยาวในระดับสังคม ทำให้ประชาชนในสังคมมีความรู้และระมัดระวังมากขึ้น ส่งผลให้การใช้งานอินเทอร์เน็ตและระบบคอมพิวเตอร์ในสังคมมีความมั่นคงปลอดภัยมากขึ้น (กฤษ ศรีเงิน, 2566, น.82) การป้องกันสังคมองค์กรภาครัฐจากภัยคุกคามทางไซเบอร์เกี่ยวกับการปฏิบัติขององค์กรภาครัฐที่ควรปฏิบัติเพื่อความปลอดภัย เช่น 1) การเปลี่ยน Default Password ของ Router ที่มาจากโรงงาน 2) เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ 3) กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น 4) ใช้ IoT Devices อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ (พลากร ลาภอลงกรณ์, 2567) การป้องกันสังคมขององค์กรภาครัฐจากภัยคุกคามทางไซเบอร์เกี่ยวกับการให้ความรู้พื้นฐานของหลักการตระหนักรู้ของบุคลากรในองค์กรภาครัฐในการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ 1) Confidentiality หรือการรักษาความลับของข้อมูล 2) Confidentiality หรือการรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น ข้อมูลส่วนเงินเดือนของบุคลากรจัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้บริหารบุคคลหรือบุคลากรที่เป็นเจ้าของเงินเดือนเท่านั้น เบอร์โทรของบุคลากรจัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ บุคลากรทุกคนในองค์กรภาครัฐ 3) Integrity หรือการรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์ และ 4) Availability หรือความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์ (พลากร ลาภอลงกรณ์, 2567) Herek (1986, p.99) กล่าวว่า ปัจจัยด้านสถานการณ์ที่ทำให้สังคมมีความตระหนักรู้ความปลอดภัยจากไซเบอร์ส่วนหนึ่งมาจากการรับรู้ข่าวสารทางสังคม ทัศนคติและความตระหนักรู้มีผลโดยตรงทำให้เกิดการเปลี่ยนแปลงพฤติกรรมการใช้ไซเบอร์ในสังคม เป็นปัจจัยที่มีส่วนทำให้เกิดการเปลี่ยนแปลงพฤติกรรม เช่นเดียวกันกับ Kim and Hunte (1993, p.331) อธิบายว่า ความตระหนักรู้ทำหน้าที่เป็นตัวกลางในการมีปฏิสัมพันธ์ทางสังคมเชิง ทัศนคติและพฤติกรรม ความตระหนักรู้สร้างความเต็มใจในการมีส่วนร่วมกับพฤติกรรมต่าง ๆ บนสื่อสังคมออนไลน์ Axel (2015, p.419) กล่าวว่า ในการพัฒนาระบบรักษาความปลอดภัยในโลกไซเบอรบนสื่อสังคมออนไลน์โดยใช้แนวคิดการ

ตระหนักรู้ในสถานการณ์ มาประยุกต์ใช้ทำให้ต้องมีการวิเคราะห์สถานการณ์ มีการจำลอง สถานการณ์ขั้นสูงโดยสร้างเป็นระบบ OODA ได้แก่ สังเกต (Observe) ปรับทิศทาง (Orient) ตัดสินใจ (Decide) การลงมือทำ (Act) เพื่อสร้างทำแผนรองรับสถานการณ์ ทำความรู้ความเข้าใจในแบบเรียลไทม์ใกล้เคียงกับสภาพแวดล้อมขององค์กร และภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบที่อาจเกิดขึ้น

การเพิ่มความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรภาครัฐ เป็นกลยุทธ์สำคัญในการป้องกันสังคมต่อการให้บริการประชาชนที่ปลอดภัยจากภัยคุกคามทางไซเบอร์ การพัฒนาความตระหนักจะช่วยให้บุคลากรและประชาชนในประเทศไทยมีความรู้ความเข้าใจในการป้องกันตัวเองและระบบสารสนเทศจากภัยคุกคามต่าง ๆ เพื่อให้ประชาชนได้รับทราบและเข้าใจภัยคุกคามทางไซเบอร์ การสร้างความตระหนักจะสามารถลดความเสี่ยงจากการโจมตีทางไซเบอร์ช่วยให้บุคลากรและประชาชนระมัดระวังและป้องกันตนเองจากภัยคุกคามต่าง ๆ ได้ การเพิ่มความตระหนักจะช่วยให้องค์กรภาครัฐสามารถตอบสนองต่อเหตุการณ์การโจมตีได้อย่างรวดเร็วและมีประสิทธิภาพ ช่วยสร้างความไว้วางใจในระบบสารสนเทศของรัฐและทำให้ประชาชนมีความมั่นใจในการใช้บริการภาครัฐ การเพิ่มความตระหนักจะช่วยสร้างสภาพแวดล้อมที่ปลอดภัยสำหรับการพัฒนาเศรษฐกิจดิจิทัล อีกทั้งการเพิ่มความตระหนักไซเบอร์ขององค์กรภาครัฐเป็นสิ่งจำเป็นเพื่อให้สังคมไทยสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและยั่งยืน

**2. การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการฝึกอบรม**

องค์กรภาครัฐมีการให้บริการประชาชนให้สามารถอยู่ร่วมกันในสังคมอย่างมีคุณภาพ โดยพัฒนาหลักสูตรการฝึกอบรมเกี่ยวกับความปลอดภัยทางไซเบอร์สำหรับบุคลากรทุกคน เพื่อให้บุคลากรสามารถบริการประชาชนในสังคมด้วยความปลอดภัยจากภัยคุกคามทางไซเบอร์ มีการจัดอบรมให้บุคลากรเกี่ยวกับภัยคุกคามทางไซเบอร์ วิธีป้องกันตัวเองเบื้องต้น การปฏิบัติตัวที่ปลอดภัยภายในระบบเครือข่าย และการตอบสนองต่อภัยคุกคามอย่างทันท่วงที และการอบรมบุคลากรให้มีความรู้และทักษะในการรับมือกับภัยคุกคามทางไซเบอร์ตามกรอบมาตรฐาน จัดอบรมการเข้าถึงข้อมูลความเสี่ยงที่เกิดขึ้น และนโยบายหรือกฎหมายที่เกี่ยวข้อง จัดอบรมหรือสัมมนาเพื่อให้บุคลากรทุกคนเข้าใจความสำคัญ และสร้างความตระหนักของการรักษาความปลอดภัยไซเบอร์ด้านความมั่นคงปลอดภัยที่หน่วยงานต้องใช้ เพื่อให้บุคลากรสามารถปฏิบัติตามได้อย่างถูกต้อง มีการพัฒนาหลักสูตรอบรมที่แตกต่างกันสำหรับบุคลากรแต่ละประเภท เพื่อให้เนื้อหามีความเหมาะสมกับหน้าที่ ความรับผิดชอบเฉพาะในบุคลากรประเภทนั้น ๆ พัฒนาหลักสูตรอบรมเข้าไปในกระบวนการของการพัฒนาบุคลากรประจำปีของฝ่ายทรัพยากรบุคคล รวมถึงการสร้างข้อบังคับให้บุคลากรใหม่ต้องเข้ารับการอบรมหลักสูตรดังกล่าว มีการประเมินผลการอบรมที่เหมาะสม องค์กรภาครัฐวางแผนการฝึกอบรมบุคลากรที่ทำหน้าที่ในการดูแลการรับมือเหตุการณ์ได้ควรได้รับการฝึกอบรมเพิ่มเติมอย่างสม่ำเสมอ มีการฝึกอบรมผู้ดูแลระบบคลาวด์สม่ำเสมอ เพื่อเสริมสร้างความรู้และเตรียมความพร้อมผู้ดูแลระบบให้รู้ทันภัยคุกคามใหม่ ๆ และการรับมือภัยคุกคาม และปฏิบัติตามแนวทางปฏิบัติที่ดีที่มีการปรับปรุงให้ทันสมัย มีการฝึกอบรมนักพัฒนาระบบสม่ำเสมอ เพื่อเสริมสร้างความรู้และเตรียมความพร้อม นักพัฒนาระบบให้รู้ทันภัยคุกคามใหม่ ๆ และการรับมือภัยคุกคาม และเสริมสร้างความตระหนักรู้ของ บุคลากร มีช่องทางในการแจ้งเหตุให้กับบุคลากร และมีวิธีการ สร้างขวัญ และกำลังใจให้บุคลากร เช่น ป๊อปอัพแสดงข้อความขอบคุณ หรือการสะสมคะแนน องค์กรภาครัฐมีการจัดฝึกอบรมความตระหนักในการใช้อุปกรณ์พกพาอย่างปลอดภัยอย่าง สม่ำเสมอร้างวัฒนธรรมความปลอดภัยภายในหน่วยงาน ส่งเสริมให้บุคลากรตระหนักถึงความสำคัญของความปลอดภัย จัดกิจกรรมสร้างความรู้

อบรมบุคลากรให้รู้จักวิธีการรับมือกับภัยไซเบอร์ และรายงานเหตุการณ์ที่น่าสงสัย และความรับผิดชอบของแต่ละคน เช่น บุคลากรฝ่ายไอทีต้องรู้จักวิธีการรักษาความปลอดภัยระบบซึ่งลงลึกทางเทคนิค และการตรวจสอบอีเมลฟิชชิ่ง เข้าร่วมกิจกรรมอบรม และสัมมนาเพื่อแลกเปลี่ยนความรู้และประสบการณ์ด้านความปลอดภัยกับหน่วยงานอื่น ๆ เพื่อสร้างความร่วมมือ เพื่อให้การบริการสังคม รักษาความมั่นคง ความปลอดภัยของประชาชน (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์กรมหาชน), 2567, น.5)

องค์กรภาครัฐได้พัฒนาหลักสูตร Cybersecurity Workshop for Government Agency ภายใต้การดำเนินงานของหลักสูตรนี้จัดทำขึ้นมาเพื่อให้บุคลากรภาครัฐ เจ้าหน้าที่หรือผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล/เทคโนโลยีสารสนเทศ ในองค์กรหน่วยงานของรัฐ ได้รับความรู้ความเข้าใจ เกิดความตระหนักเกี่ยวกับหลักการและความสำคัญของกฎหมาย ระเบียบ ประกาศ ขั้นตอนการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์, NIST Cybersecurity Framework เป็นต้น ทั้งนี้ ความรู้ ประสบการณ์ และเครื่องมือต่าง ๆ ผู้เข้าร่วมอบรมสามารถที่จะนำไปใช้งานประยุกต์ปรับใช้ในองค์กร ร่วมกับการกำหนดนโยบาย เพื่อยกระดับการบริหารงาน และการปฏิบัติงานขององค์กรสู่รูปแบบดิจิทัลที่มีความมั่นคงปลอดภัยสอดคล้องกับกฎหมาย ตลอดจนสามารถให้บริการประชาชนได้อย่างมีมั่นใจ มีความปลอดภัย กลุ่มเป้าหมายผู้เข้าอบรม ผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล และเทคโนโลยีสารสนเทศ และบุคลากรภาครัฐที่สนใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางการรับมือกับเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้การบริการสาธารณะขององค์กรภาครัฐที่ ตอบสนองความต้องการและความปลอดภัยของประชาชนที่ใช้บริการทางไซเบอร์และพัฒนาคุณภาพชีวิต เช่น การดูแลสาธารณสุข การศึกษา และการขนส่งสาธารณะ การบริการมีบทบาทสำคัญในการสร้างสังคมที่มั่นคงปลอดภัยและมีคุณภาพชีวิตที่ดีสำหรับประชาชน เป็นการบริการที่มุ่งเน้นเพื่อประโยชน์ของประชาชนโดยรวม ภายใต้การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐโดยการฝึกอบรมให้แก่บุคลากรภาครัฐ ภายใต้การกำกับดูแลและควบคุมของรัฐเพื่อให้มั่นใจว่ามีการดำเนินงานอย่างมีประสิทธิภาพและความปลอดภัย การบริการต้องสามารถตอบสนองความต้องการที่หลากหลายของประชาชนในสังคมได้อย่างเท่าเทียมกัน การบริการต้องมีคุณภาพสูงและเป็นไปตามมาตรฐานที่กำหนดไว้เพื่อให้ประชาชนได้รับประโยชน์สูงสุด การบริการในสังคมที่ช่วยพัฒนาคุณภาพชีวิตของประชาชน การบริการที่ช่วยให้ประชาชนเข้าถึงโอกาสและการเข้าถึงการให้บริการทางไซเบอร์และเทคโนโลยีดิจิทัลเท่าเทียมกัน ลดความเหลื่อมล้ำทางสังคม การบริการที่ช่วยสร้างสังคมที่เข้มแข็งและมีความยั่งยืน โดยการสนับสนุนการพัฒนาท้องถิ่นและการแก้ไขปัญหาทางสังคม การบริการที่ช่วยสร้างความมั่นคงทางเศรษฐกิจของประเทศ การบริการที่องค์กรภาครัฐเป็นผู้จัดทำเพื่อตอบสนองความต้องการของประชาชนทั่วประเทศ เช่น การรักษาความมั่นคงและความเป็นระเบียบเรียบร้อยของสังคม (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), 2566, น.6)

นอกจากนี้ องค์กรภาครัฐยังมีการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ประกอบด้วย 1) ด้านการศึกษา โดยปลูกฝังความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ระดับวัย อุดมศึกษาจบถึงระดับมหาวิทยาลัยต้องมีความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือด้าน IT เพราะการศึกษาจะช่วยให้เข้าใจถึงหลักแนวคิดทฤษฎี และเทคนิคที่ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นการเตรียมความพร้อมที่สำคัญในการพัฒนาบุคลากรในด้าน หลักสูตรต่าง ๆ ที่จำเป็นต่อการทำงานหรือตามความสนใจของผู้ศึกษา ดังนั้น การศึกษาจึงเป็นการวางแผนแนวทางการพัฒนาทักษะของบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นในอนาคต พัฒนาบุคลากรให้มีจำนวนที่ตอบสนองต่อความต้องการและเท่าทันต่อภัยคุกคามที่เกิดขึ้น แต่ละระดับ การศึกษาของบุคลากรนั้นอาจแตกต่างกันไปตามภารกิจและหน้าที่ความรับผิดชอบ

ของแต่ละสายงาน บุคลากรในสายงานทางไซเบอร์จะต้องได้รับการศึกษาให้เกิดความทักษะและเชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นหน้าที่และภารกิจหลักของสำนักงานในการดำเนินการให้เป็นไปตามยุทธศาสตร์ชาติ 20 ปี ของประเทศ 2) ด้านการฝึกอบรม โดยภาคปฏิบัติที่ให้บุคลากรได้ฝึกปฏิบัติในสถานการณ์จำลองเสมือนจริง และได้รับฟังความรู้จากผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดไซเบอร์ที่มีประสบการณ์โดยตรง ทำให้บุคลากรได้รับความรู้และประสบการณ์เกิดความเข้าใจและเชี่ยวชาญในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น การฝึกอบรมจะช่วยเสริมในเนื้อหาของการศึกษาระดับพื้นฐานให้ชัดเจนและเฉพาะทางมากยิ่งขึ้น ซึ่งเป็นวิธีการปฏิบัติการนำความรู้ที่ได้รับจากการศึกษามาต่อยอดหรือประยุกต์ใช้ในสถานการณ์จริง เพื่อให้ผู้เข้ารับการฝึกอบรม ได้ซักซ้อมทั้งวิธีการและแนวคิดมาปรับใช้กับภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคต ซึ่งเป็นการเพิ่มเติมความรู้จากด้านการศึกษาอีกระดับหนึ่ง และยังช่วยให้เกิดการแลกเปลี่ยนบุคลากรที่มีความเชี่ยวชาญทางด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ เพื่อแลกเปลี่ยนเรียนรู้ประสบการณ์ทางด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งสำนักงานได้มีการจัดฝึกอบรมให้กับบุคลากรทั้งภายใน แนะภายนอกสำนักงาน 3) ด้านการพัฒนา โดยการต่อยอดทักษะความรู้จากสิ่งที่ได้ศึกษาอบรมมาอย่างต่อเนื่องให้มีการพัฒนามากขึ้นกว่าเดิม การพัฒนาจะดูแนวโน้มของอนาคตและสถานการณ์ของโลกที่เปลี่ยนแปลงไปเพื่อที่จะพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ตรงต่อการเปลี่ยนแปลงและเป้าประสงค์ของประเทศ เช่น การรพัฒนาทักษะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่นอกเหนือจากการป้องกัน รับมือ และตอบสนองต่อภัยคุกคาม การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเดียวอาจไม่เพียงพอต่อการป้องกันภัยคุกคามที่เกิดขึ้น (วราภรณ์ เพลิดเพลิน, 2565, น.68) องค์กรภาครัฐจึงต้องสร้างโปรแกรมการฝึกอบรมความรู้ด้านความปลอดภัยทางไซเบอร์ให้กับพนักงานซึ่งเป็นแนวป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด่านแรกจากการโจมตีทางไซเบอร์ การฝึกอบรมพนักงานจึงมีความสำคัญอย่างยิ่งต่อความปลอดภัยทางไซเบอร์โปรแกรมฝึกอบรมด้านความปลอดภัยทางไซเบอร์จะช่วยให้พนักงานได้รับข้อมูลที่จำเป็นในการทำความเข้าใจการโจมตีทางไซเบอร์ มีทักษะในการระบุการโจมตี และคำแนะนำในการปฏิบัติตามเมื่อต้องรับมือกับกิจกรรมที่น่าสงสัย โปรแกรมฝึกอบรมดังกล่าวจะช่วยส่งเสริมวัฒนธรรมที่ให้ความสำคัญกับความปลอดภัยเป็นอันดับแรก ซึ่งครอบคลุมพนักงานทุกประเภทไม่ใช่แค่ทีมรักษาความปลอดภัยเท่านั้น (Gruner, 2024)

ดังนั้น การฝึกอบรมขององค์กรภาครัฐเพื่อพัฒนาสังคมที่ภาครัฐจัดขึ้นเพื่อพัฒนาบุคลากรในองค์กรภาครัฐให้มีความรู้ความสามารถในการดำเนินงานด้านการป้องกันสังคมได้อย่างมีประสิทธิภาพ รวมถึงการส่งเสริมการมีส่วนร่วมของประชาชนในกิจกรรมการป้องกันสังคมโดยเฉพาะการให้บริการเพื่อพัฒนาสังคม มุ่งเน้นให้ประชาชนในสังคมมีความรู้ความเข้าใจจากภัยคุกคามทางไซเบอร์ การประเมินปัญหาจากภัยคุกคามทางไซเบอร์ทางสังคม การวางแผนและดำเนินการช่วยเหลือ การฝึกอบรมเพื่อเพิ่มขีดความสามารถของบุคลากรองค์กรภาครัฐอย่างต่อเนื่อง จะช่วยให้บุคลากรภาครัฐมีความรู้ความสามารถในการทำงานและการป้องกันสังคมได้อย่างมีประสิทธิภาพ ช่วยให้ประชาชนมีส่วนร่วมในการป้องกันสังคมได้อย่างจริงจัง อีกทั้งยังพัฒนาคุณภาพชีวิตของประชาชนที่ดีขึ้น ผ่านการพัฒนาและบริการขององค์กรภาครัฐ และการฝึกอบรมให้กับบุคลากรองค์กรภาครัฐเพื่อพัฒนาสังคมมีบทบาทสำคัญในการขับเคลื่อนการพัฒนาประเทศให้ก้าวหน้าและยั่งยืน

**3. การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการใช้เทคโนโลยี**

องค์กรภาครัฐมีการป้องกันสังคมจากภัยคุกคามทางไซเบอร์ในการเอื้อประโยชน์ให้กับสังคมได้ดีขึ้น โดยรัฐใช้ประโยชน์จากเทคโนโลยีสารสนเทศ และการเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้อย่างเหมาะสม อีกทั้งยังเปิดโอกาสให้องค์กรภาครัฐสามารถสื่อสารกับประชาชนในสังคม ตัวอย่าง การใช้เทคโนโลยีสารสนเทศที่เอื้อประโยชน์ให้รัฐได้ เช่น การรวบรวมและใช้ประโยชน์จากข้อมูลที่มีมากขึ้น การลดขั้นตอนกระบวนการ การลดการใช้กระดาษ ทั้งนี้เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการภาครัฐต่อประชาชน รวมไปถึงการเพิ่มประสิทธิภาพกระบวนการภายในขององค์กรภาครัฐเอง อย่างไรก็ตามการใช้ประโยชน์จากเทคโนโลยีสารสนเทศที่เพิ่มขึ้นก็ทำให้รัฐมีความเสี่ยงกับภัยคุกคามร้ายแรงเพิ่มขึ้น ทั้งต่อความมั่นคงของชาติ โครงสร้างพื้นฐาน ข้อมูล และความสัมพันธ์ระหว่างประเทศ ทั้งนี้การระบุและจัดการภัยคุกคามเป็นเรื่องสำคัญต่อการสร้างยุทธศาสตร์ที่แข็งแกร่งและยืดหยุ่นในด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับการทำงานผ่านเครือข่ายอินเทอร์เน็ตในหลายประเทศ พัฒนาบุคลากรเข้ามาดูแลงานเทคโนโลยีสารสนเทศ เพื่อให้มีความเข้าใจและจัดการเรื่องเทคโนโลยีสารสนเทศ มีความพร้อมในการจัดการภัยคุกคามด้านเทคโนโลยีสารสนเทศ จะจัดการเรื่องนี้แบบองค์รวม โดยมีกิจกรรมตัวอย่าง เช่น 1) จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ 2) ให้ความรู้ความเข้าใจกับเจ้าหน้าที่รัฐและประชาชนโดยทั่วไป 3) มีกระบวนการจัดซื้อจัดจ้างที่มั่นคงปลอดภัยเพื่อลดความเสียหายจากภัยคุกคามประเภทมัลแวร์และไวรัส มีการพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อใช้งานในภาครัฐและบริการออนไลน์ โดยองค์กรภาครัฐมีบทบาทสำคัญในเชิงบวกที่สามารถเพิ่มการมีส่วนร่วมกับประชาชน ระบบสาธารณูปโภคและระบบการป้องกันประเทศมีการใช้งานผ่านเครือข่ายเทคโนโลยีสารสนเทศมากขึ้น องค์กรภาครัฐมีการพัฒนาการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม รัฐและประชาชนได้รับการพัฒนาด้านความเป็นส่วนตัว การจารกรรมข้อมูล และความปลอดภัยในการใช้บริการสาธารณะ มีการจัดเก็บข้อมูลสาธารณะและข้อมูลส่วนตัวปริมาณมากจัดเก็บและให้เข้าถึงได้ผ่านระบบเทคโนโลยีสารสนเทศของภาครัฐ มีการเผยแพร่ผ่านช่องทางบริการออนไลน์ของภาครัฐ เช่น เลขประจำตัวประชาชน ข้อมูลภาษี อีเมลที่ใช้ในการสื่อสารภายในรัฐบาล และข้อมูลด้านความมั่นคงปลอดภัยที่เป็นความลับ ข้อมูลในแต่ละระดับชั้นความลับที่ต้องการความปลอดภัยและการป้องกันที่ต่างกัน มีการพัฒนาการใช้ทรัพยากรและการใช้จ่ายเพื่อสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศบนเครือข่ายอินเทอร์เน็ต รวมทั้งการพัฒนาเว็บไซต์เพื่อบริการออนไลน์ภาครัฐ องค์กรภาครัฐทุกองค์กรมีการพัฒนาแผนการเนินการในการสร้างยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ยุทธศาสตร์ความมั่นคงด้านเทคโนโลยีสารสนเทศที่ดี มีการพัฒนารแบบองค์รวม และมีความสามารถในการรับมือกับการโจมตี การป้องกัน การตอบสนองและยกระดับของความเข้าใจในหมู่ประชาชนทั่วไปด้วยการให้ความรู้แก่เจ้าของธุรกิจ นักเรียน และหน่วยงานของรัฐ ในเรื่องภัยคุกคามที่มีอยู่ รวมทั้งวิธีปกป้องเครือข่ายของตนจากการโจมตี (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2558) นอกจากนี้ องค์กรภาครัฐมีการพัฒนาโครงสร้างทางด้านความมั่นคงปลอดภัยทางไซเบอร์และเทคโนโลยีสารสนเทศสำหรับสำนักงาน ควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่าง ๆ ภายในสำนักงาน และเพื่อเป็นแนวทางการควบคุมอุปกรณ์สารสนเทศ และการปฏิบัติงานจากภายนอกให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ เช่น การจัดโครงสร้างภายในองค์กร มีกำหนดบทบาทหน้าที่ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีความมั่นคงปลอดภัยทางไซเบอร์ และนโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์สารสนเทศและการ

ปฏิบัติงานจากภายนอกสำนักงาน มีนโยบายกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและเหมาะสม (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), 2567, น.7) แม้ว่าเว็บไซต์เครือข่ายสังคมจะนำเสนอเทคโนโลยีและการติดต่อสื่อสารที่ทันสมัย แต่ก็ยังต้องเผชิญกับความท้าทายใหม่ ๆ เกี่ยวกับประเด็นเรื่องความเป็นส่วนตัวและความปลอดภัย งานชิ้นนี้เชื่อว่าความก้าวหน้าของเทคโนโลยีใหม่ ๆ ในเว็บไซต์ทั่วไปและสังคมจะนำความเสี่ยงด้านความปลอดภัยใหม่ ๆ ที่อาจเป็นโอกาสสำหรับผู้สร้างไวรัส และผู้บุกรุก อย่างไรก็ตามผู้เชี่ยวชาญ ด้านความปลอดภัยข้อมูล เจ้าหน้าที่ของรัฐและหน่วยข่าวกรองอื่น ๆ ต้องพัฒนาเครื่องมือใหม่ ๆ เพื่อป้องกันและปรับตัวให้เข้ากับความเสี่ยงและภัยคุกคามในอนาคต นอกจากนี้ยังต้องพัฒนาให้ระบบสามารถจัดการกับข้อมูลจำนวนมากได้อย่างปลอดภัยในอินเทอร์เน็ตและในเว็บไซต์ทางสังคมด้วย

องค์กรภาครัฐมีการป้องกันสังคมให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ ซึ่งเป็นภัยคุกคามที่เกิดขึ้นได้จากเทคโนโลยี ป้องกันการโจมตีระบบคอมพิวเตอร์หรือเครือข่ายเพื่อวัตถุประสงค์ต่าง ๆ เช่น การขโมยข้อมูล, การทำลายระบบ หรือการหยุดการทำงานของระบบ โปรแกรมที่เป็นอันตราย ซึ่งสามารถเข้าสู่ระบบและก่อให้เกิดความเสียหาย การหลอกลวงให้บุคคลเปิดเผยข้อมูลส่วนตัวการหลอกลวงทางออนไลน์เพื่อขอข้อมูลที่สำคัญเพื่อถ่ายทอดให้ความรู้ต่อไปยังประชาชน เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การโจมตีที่ทำให้ระบบหรือบริการไม่สามารถให้บริการประชาชนได้เนื่องจากมีปริมาณการเข้าถึงที่มากเกินไป อีเมลขยะหรือข้อความไม่พึงประสงค์จำนวนมาก การดักข้อมูลที่ส่งระหว่างคอมพิวเตอร์หรือเครือข่ายการใช้เทคโนโลยีเพื่อพัฒนาสังคม เช่น การศึกษา การใช้เทคโนโลยีในการเรียนรู้และพัฒนาทักษะผ่านการเรียนรู้ทางออนไลน์ ระบบจัดการเรียนรู้ และแอปพลิเคชันต่าง ๆ ใช้เทคโนโลยีในการปรับปรุงวิธีการเกษตร เพิ่มผลผลิต และลดต้นทุนการผลิตของประชาชน การใช้เทคโนโลยีในการสื่อสารกับผู้อื่น แลกเปลี่ยนข้อมูล และสร้างเครือข่ายสังคม การป้องกันข้อมูลส่วนตัวและข้อมูลสำคัญขององค์กรภาครัฐเพื่อบริการประชาชน การลดความเสี่ยงจากการถูกหลอกลวงและจากอาชญากรรมทางไซเบอร์ การใช้โปรแกรมป้องกันไวรัสและมัลแวร์ การตั้งรหัสผ่านที่ไม่ซ้ำกัน การตรวจสอบความน่าเชื่อถือของเว็บไซต์และลิงก์ การไม่เปิดไฟล์แนบจากผู้ที่ไม่ได้รู้จักและการอัพเดทซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ

**4. การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการสร้างมาตรฐาน**

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวล แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการ ดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรภาครัฐ พื้นฐานสำคัญทางสารสนเทศรวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือร้ายแรงต่อระบบสารสนเทศของประเทศ ให้บริการข้อมูลองค์ความรู้ผ่านระบบเทคโนโลยีสารสนเทศ สื่อสังคมออนไลน์ และโมบายแอปพลิเคชั่น จึงมีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ เพื่อให้องค์กรภาครัฐสามารถบริการประชาชนได้อย่างมีประสิทธิภาพ (สำนักยุทธศาสตร์และสารสนเทศ, 2567, น.9) นอกจากนี้องค์กรภาครัฐมีผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ บริการให้คำปรึกษาเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ ด้วยเทคโนโลยีที่สามารถแก้ไขปัญหาและเสริมสร้างความปลอดภัยให้กับระบบที่มีความซับซ้อนในการ

บริหารจัดการความเสี่ยงได้อย่างเหมาะสมในการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ เสริมสร้างระบบความปลอดภัยให้เป็นไปตามมาตรฐานความปลอดภัย ช่วยประเมินความเสี่ยงเพื่อหาช่องโหว่ที่อาจเกิดขึ้น เพื่อช่วยจัดการระบบการรักษาความปลอดภัยในองค์กรให้มีประสิทธิภาพ พร้อมรับมือกับภัยคุกคามทางไซเบอร์ได้โดยทันที และมีพัฒนามาตรฐานด้านความปลอดภัยทางไซเบอร์สำหรับองค์กรและหน่วยงานต่าง ๆ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ และการป้องกันภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐ ลดความเสี่ยงที่เกิดจากอาชญากรรมทางไซเบอร์ และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยได้อย่างเหมาะสม และการพัฒนาปรับแต่งระบบ การใช้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ เป็นสิ่งจำเป็นสำหรับการป้องกันคุกคามทางไซเบอร์และรับประกันความมั่นคงปลอดภัยของระบบสารสนเทศ การรับรองตัวเองตามมาตรฐานความ มั่นคงปลอดภัยเช่น ISO 27001, ISO 27017, ISO 27701 และการใช้นโยบายความมั่นคงปลอดภัยที่เหมาะสมเพื่อบริการประชาชนให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ (กฤษ ศรีเงิน, 2566, น.81)

การรักษาความปลอดภัยไซเบอร์ขององค์กรภาครัฐ เป็นสิ่งที่จำเป็นต่อการพัฒนาประชาชนด้านการป้องกันสังคมที่จะต้องมุ่งมั่นทำเพื่อความปลอดภัยของข้อมูลและความสงบสุขของประชาชน องค์กรภาครัฐควรมีมาตรการความปลอดภัยไซเบอร์อย่างครอบคลุม เตรียมแนวทางการรับมือที่มีประสิทธิภาพที่สุดเพื่อป้องกันการโจมตี รวมไปถึงการมีมาตรฐานตรวจจับและตอบสนองต่อเหตุการณ์ทางไซเบอร์ในปัจจุบันเป็นสิ่งที่มีความสำคัญอย่างยิ่ง เนื่องจากวิธีการและเทคนิคของผู้โจมตียังคงมีการพัฒนาอย่างต่อเนื่องและมีโอกาสเกิดขึ้นแบบต่อเนื่อง การโจมตีเหล่านี้สามารถส่งผลกระทบต่อความมั่นคงขององค์กรภาครัฐและประชาชนได้ อีกทั้งหน่วยงานของรัฐยังต้องเผชิญกับความเสี่ยงด้านไซเบอร์ที่มีความซับซ้อน หน่วยงานบางแห่งอาจขาดความเชี่ยวชาญด้านความปลอดภัยไซเบอร์ ไม่สามารถตรวจจับการโจมตีได้อย่างทันท่วงที

**5. การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการทำงานร่วมกัน**

องค์กรภาครัฐและภาคเอกชนควรทำงานร่วมกันในการป้องกันและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งองค์กรภาครัฐ จึงควรมีการบูรณาการข้อมูลเพื่อให้ความเข้าใจที่ตรงกัน สร้างความเข้าใจกับภาคประชาชน เพื่อให้ได้รับความร่วมมือจากประชาชนอย่างเต็มที่ เพื่อให้การดำเนินงานขององค์กรภาครัฐเป็นไปอย่างสะดวกมากขึ้น ควรดำเนินการเสริมสร้างการรับรู้ความเข้าใจและความน่าเชื่อถือในการดำเนินงานแก่ประชาชนเพื่อให้สามารถดำเนินการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและลดแรงต่อต้านจากภาคประชาชน (กนกนก โพธิ์หอม, 2564, น.45) องค์กรภาครัฐมีเป้าหมายหลัก คือ การสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อม เอื้ออำนวย โดยมุ่งเน้นให้มีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างพื้นฐานสำคัญ การสร้างความร่วมมือทุกภาคส่วน และการสร้างความร่วมมือกับต่างประเทศเพื่อสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น (ราชกิจจานุเบกษา, 2562, น.20) สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่าง ๆ นอกเหนือจากองค์กรภาครัฐ โดยเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐในการพัฒนาและปรับปรุงเทคโนโลยี และการดำเนินกิจกรรมทางไซเบอร์ เพื่อให้ตรงตามความประสงค์ของประชาชนผู้รับบริการด้านการป้องกันสังคม ทั้งในด้านการพัฒนาองค์ความรู้ และเทคโนโลยี การพัฒนาบุคลากร การรักษาความมั่นคงปลอดภัย เพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม มียุทธศาสตร์ แผนงาน กฎระเบียบที่มีประสิทธิภาพเหมาะสมต่อระบบเศรษฐกิจดิจิทัลได้มาตรฐาน ส่งเสริมเศรษฐกิจดิจิทัลกับองค์กรภาครัฐ ส่งเสริมการใช้เทคโนโลยี

ดิจิทัลในวงกว้าง ปรับปรุงยุทธศาสตร์ แผนหรือแผนงาน ตลอดจนกฎหมาย ระเบียบปฏิบัติ ที่เหมาะสมสอดคล้องและเอื้ออำนวยต่อเศรษฐกิจดิจิทัล พร้อมทั้งมีการประเมินผลและทบทวนอย่างสม่ำเสมอ โดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์ แผนหรือแผนงานดังกล่าว ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชน และภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ในลักษณะองค์รวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบาย จากรัฐสู่เอกชนและภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหา ประเมินผลการดำเนิน นโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์ทุกภาคส่วนที่เกี่ยวข้อง ทั้งภาครัฐ เอกชน และภาคประชาชน ให้ความร่วมมือและมีส่วนร่วมในการสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ (สำนักงานสภาความมั่นคงแห่งชาติ, 2564, น.3) ดังนั้น องค์กรภาครัฐมีการพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ที่เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์โดยบูรณาการความร่วมมือภาคประชาชน เร่งผลักดันการพัฒนาความรู้และทักษะด้านไซเบอร์ให้ครอบคลุมประชาชนคนไทยทุกช่วงวัย อีกทั้งยังส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจน ดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างเยาวชนขยายผลสู่โรงเรียนทั่วประเทศมุ่งส่งเสริมความรู้ประชาชนในสังคม เพื่อพัฒนาอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมให้ประชาชนได้ใช้เวลาทำกิจกรรมร่วมกันเพื่อสร้างภูมิคุ้มกันภัยไซเบอร์และขยายผลสู่ครอบครัวและชุมชนเสริมความแข็งแกร่ง เช่น กิจกรรมจัดการแข่งขันทักษะทางไซเบอร์ สร้างแพลตฟอร์มออนไลน์ NCSA MOOC และ E-Learning เพื่อให้ทุกคนสามารถเข้าถึงและเรียนรู้เกี่ยวกับไซเบอร์ ร่วมมือการพัฒนาบุคลากรในระดับประเทศและในภูมิภาคอาเซียน ขยายผลความรู้ด้านความมั่นคงปลอดภัยไซเบอร์สู่ทุกภาคส่วน ส่งเสริมพลเมืองดิจิทัลด้านความมั่นคงปลอดภัยไซเบอร์ทั่วประเทศ ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาสังคมให้กับประชาชนทุกช่วงวัยให้ประเทศไทยให้มีความปลอดภัยไซเบอร์ที่แข็งแกร่งจากร่วมมือจากทุกภาคส่วน และขับเคลื่อนให้ประเทศไทยก้าวสู่การเป็นผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

**องค์ความรู้ใหม่เชิงวิชาการ**

ผู้เขียนสามารถจำแนกเป็นตารางได้ ดังนี้

**ตารางที่ 1** องค์ความรู้ใหม่เชิงวิชาการ

| การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการเพิ่มความตระหนัก | การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการฝึกอบรม | การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการใช้เทคโนโลยี | การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการสร้างมาตรฐาน | การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการทำงานร่วมกัน |
|---|---|---|---|---|
| - เพิ่มความตระหนักรู้ด้านความมั่นคง | - พัฒนาหลักสูตรการฝึกอบรมเกี่ยวกับ | - การป้องกันสังคมจากภัยคุกคามทางไซ | - ปฏิบัติตามพระราชบัญญัติการรักษาความ | - ควรมีการบูรณาการข้อมูลเพื่อให้ความ |

| | | | | |
|---|---|---|---|---|
| ปลอดภัยทางไซเบอร์ของข้อมูล รวมถึงการตระหนักถึงความเสี่ยงทางไซเบอร์ ภัยคุกคาม<br>- เพิ่มความตระหนักถึงความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์ผ่านกลยุทธ์การศึกษา และการป้องกันด้วยการพัฒนาแพลตฟอร์มด้านความมั่นคงปลอดภัยทางไซเบอร์ การใช้เครื่องมือตรวจจับการบุกรุก<br>- เพิ่มความตระหนักถึงสถานการณ์ทางไซเบอร์โดยให้คำแนะนำแก่ผู้ดูแลระบบและองค์กรภาครัฐในการลดความเสี่ยง และผลกระทบจากการโจมตีทางไซเบอร์<br>- เพิ่มความตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ขององค์กรภาครัฐที่ทำให้ประชาชนทั่วไปที่มาใช้บริการองค์กรหรือ | ความปลอดภัยทางไซเบอร์สำหรับบุคลากรทุกคน เพื่อให้บุคลากรสามารถบริการประชาชนในสังคมด้วยความปลอดภัยจากภัยคุกคามทางไซเบอร์<br>- จัดอบรมวิธีป้องกันตัวเองเบื้องต้น การปฏิบัติตัวที่ปลอดภัยภายในระบบเครือข่าย และการตอบสนองต่อภัยคุกคามอย่างทันท่วงที<br>- จัดอบรมบุคลากรให้มีความรู้และทักษะในการรับมือกับภัยคุกคามทางไซเบอร์ตามกรอบมาตรฐาน จัดอบรมการเข้าถึงข้อมูลความเสี่ยงที่เกิดขึ้น และนโยบายหรือกฎหมายที่เกี่ยวข้องกับการป้องกันสังคมจากภัยคุกคามทางไซเบอร์<br>- พัฒนาหลักสูตรอบรมเข้าไปในกระบวนการของการพัฒนาบุคลากร | เบอร์ในการเอื้อประโยชน์ให้กับสังคมได้ดีขึ้น และการเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้อย่างเหมาะสม<br>- การใช้เทคโนโลยีสารสนเทศที่เอื้อประโยชน์ให้รัฐได้ เช่น การรวบรวมและใช้ประโยชน์จากข้อมูลที่มีมากขึ้น การลดขั้นตอนกระบวนการ การลดการใช้กระดาษ<br>- จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในองค์กรภาครัฐ<br>- จัดเก็บข้อมูลสาธารณะและข้อมูลส่วนตัวปริมาณมาก จัดเก็บและให้เข้าถึงได้ผ่านระบบเทคโนโลยีสารสนเทศของภาครัฐ<br>- พัฒนาเว็บไซต์เพื่อบริการออนไลน์ภาครัฐ<br>- พัฒนาโครงสร้างและควบคุมทางด้านความมั่นคงปลอดภัยทางไซเบอร์และเทคโนโลยี | มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>- กำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เหตุการณ์ที่ส่งผลกระทบร้ายแรงต่อระบบสารสนเทศของประเทศ<br>- การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้วยการสร้างมาตรฐานบริการข้อมูลองค์ความรู้ผ่านระบบเทคโนโลยีสารสนเทศ สื่อสังคมออนไลน์ และโมบายแอปพลิเคชั่นเพื่อบริการประชาชนได้อย่างมีประสิทธิภาพ<br>- มีผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ บริการให้ | เข้าใจที่ตรงกัน สร้างความเข้าใจกับภาคประชาชน เพื่อให้ได้รับความร่วมมือจากประชาชนอย่างเต็มที่<br>- เสริมสร้างการรับรู้ความเข้าใจและความน่าเชื่อถือในการดำเนินงานแก่ประชาชนเพื่อให้สามารถดำเนินการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ<br>เอื้ออำนวย โดยมุ่งเน้นให้มีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ<br>- เปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐในการพัฒนา และปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์<br>- ยกระดับขีดความสามารถในการรักษาความมั่นคง |

| | | | | |
|---|---|---|---|---|
| หน่วยงานภาครัฐมีความรู้และระมัดระวังมากขึ้น<br>- การส่งเสริมการศึกษาเพื่อให้ผู้เรียนหลังจากจบการศึกษาแล้วสามารถนำไปใช้ในการป้องกันสังคมองค์กรภาครัฐในอนาคต<br>- การเปลี่ยน Default Password ของ Router เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ<br>- การตระหนักรู้ในการรักษาความลับของข้อมูล การรักษาความถูกต้องของข้อมูล การเตรียมความพร้อมใช้งานของข้อมูล<br>- การตระหนักรู้ความปลอดภัยจากไซเบอร์จากการรับรู้ข่าวสารบนสื่อออนไลน์ สังคมโดยตรงที่ทำให้เกิดการเปลี่ยนแปลงพฤติกรรมการใช้ไซเบอร์ในสังคม | ประจำปีของฝ่ายทรัพยากรบุคคล รวมถึงการสร้างข้อบังคับให้บุคลากรใหม่ต้องเข้ารับการอบรมหลักสูตร<br>- เสริมสร้างความรู้ด้วยการจัดฝึกอบรมเพื่อเตรียมความพร้อมผู้ดูแลระบบให้รู้ทันภัยคุกคามใหม่ ๆ และการรับมือภัยคุกคามและปฏิบัติตามแนวทางปฏิบัติที่ดีที่มีการปรับปรุงให้ทันสมัย<br>- มีช่องทางในการแจ้งการป้องกันสังคมจากภัยคุกคามทางไซเบอร์ให้กับบุคลากร<br>- จัดกิจกรรมสร้างความรู้เพื่อสร้างความร่วมมือ เพื่อให้การบริการสังคม รักษาความมั่นคง ความปลอดภัยของประชาชน<br>- มีหลักสูตรการจัดอบรมด้านกฎหมาย ประกาศ ระเบียบและข้อบังคับเกี่ยวกับ | สารสนเทศสำหรับสำนักงาน กำกับและติดตามการปฏิบัติหน้าที่การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ด้านการใช้เทคโนโลยี<br>- มีกำหนดบทบาทหน้าที่ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีความมั่นคงปลอดภัยทางไซเบอร์ และนโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก | คำปรึกษาเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ<br>- เสริมสร้างระบบความปลอดภัยให้เป็นไปตามมาตรฐานความปลอดภัย มีประสิทธิภาพ มีการรับรองตัวเองตามมาตรฐานความมั่นคงปลอดภัย เช่น ISO 27001, ISO 27017, ISO 27701 | ปลอดภัยไซเบอร์ของประเทศแบบองค์รวมเพื่อให้ได้มาตรฐาน<br>- มียุทธศาสตร์ แผนงาน กฎระเบียบที่มีประสิทธิภาพเหมาะสมต่อระบบเศรษฐกิจดิจิทัลที่ได้มาตรฐาน<br>- ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชน และภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดด้านไซเบอร์ที่ได้มาตรฐาน<br>- พัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ที่เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์โดยบูรณาการความร่วมมือภาคประชาชน<br>- สร้างแพลตฟอร์มออนไลน์เพื่อให้ทุกคนสามารถเข้าถึงและเรียนรู้เกี่ยวกับไซเบอร์โดยร่วมมือการพัฒนา |

| | | | | |
|---|---|---|---|---|
| | ขั้นตอนการปฏิบัติงานต่าง ๆ ในการป้องกันสังคมจากภัยคุกคามทางไซเบอร์<br>- สร้างสังคมที่มั่นคงปลอดภัยและมีคุณภาพชีวิตที่ดีสำหรับประชาชน เป็นการบริการที่มุ่งเน้นเพื่อประโยชน์ของประชาชนโดยรวมภายใต้การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐ | | | บุคลากรในระดับประเทศและในภูมิภาคอาเซียนเพื่อสร้างมาตรฐานร่วมกัน<br>- ส่งเสริมพลเมืองดิจิทัลด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาสังคมให้กับประชาชนทุกช่วงวัยให้ประเทศไทยให้มีความปลอดภัยไซเบอร์ที่แข็งแกร่งจากร่วมมือจากทุกภาคส่วนสู่ระดับสากล |

**บทสรุป**

การป้องกันสังคมจากภัยคุกคามทางไซเบอร์ขององค์กรภาครัฐในประเทศไทย สิ่งสำคัญคือ 1) การเพิ่มความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรภาครัฐ เป็นกลยุทธ์สำคัญในการป้องกันสังคมต่อการให้บริการประชาชนที่ปลอดภัยจากภัยคุกคามทางไซเบอร์ ช่วยให้บุคลากรและประชาชนในประเทศไทยมีความรู้ความเข้าใจในการป้องกันตัวเองและระบบสารสนเทศจากภัยคุกคามต่าง ๆ เพื่อให้ประชาชนได้รับทราบและเข้าใจภัยคุกคามทางไซเบอร์ สามารถลดความเสี่ยงจากการโจมตีทางไซเบอร์ช่วยให้บุคลากรและประชาชนระมัดระวังและป้องกันตนเองจากภัยคุกคามต่าง ๆ ช่วยให้องค์กรภาครัฐสามารถตอบสนองต่อเหตุการณ์การโจมตีได้อย่างรวดเร็วและมีประสิทธิภาพ ช่วยสร้างความไว้วางใจในระบบสารสนเทศของรัฐและทำให้ประชาชนมีความมั่นใจในการใช้บริการภาครัฐ ช่วยสร้างสภาพแวดล้อมที่ปลอดภัยสำหรับการพัฒนาเศรษฐกิจดิจิทัล อีกทั้งการเพิ่มความตระหนักไซเบอร์ขององค์กรภาครัฐเป็นสิ่งจำเป็นเพื่อให้สังคมไทยสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและยั่งยืน 2) การฝึกอบรมขององค์กรภาครัฐเพื่อพัฒนาสังคมที่ภาครัฐจัดขึ้นเพื่อพัฒนาบุคลากรในองค์กรภาครัฐให้มีความรู้ความสามารถในการดำเนินงานด้านการป้องกันสังคมได้อย่างมีประสิทธิภาพ รวมถึงการส่งเสริมการมีส่วนร่วมของประชาชนในกิจกรรมการป้องกันสังคม การฝึกอบรมเพื่อเพิ่มขีดความสามารถของบุคลากรองค์กรภาครัฐอย่างต่อเนื่องจะช่วยให้บุคลากรภาครัฐมีความรู้ความสามารถในการทำงานและการป้องกันสังคมได้อย่างมีประสิทธิภาพ ช่วยให้ประชาชนมีส่วนร่วมในการป้องกันสังคมได้อย่างจริงจัง อีกทั้งยังพัฒนาคุณภาพชีวิตของประชาชนที่ดีขึ้นผ่านการพัฒนาและบริการขององค์กรภาครัฐ 3) องค์กรภาครัฐมีการป้องกันสังคมให้ปลอดภัยจากภัยคุกคามทางไซเบอร์จากเทคโนโลยี ป้องกันการโจมตีระบบคอมพิวเตอร์หรือเครือข่าย

เพื่อวัตถุประสงค์ต่าง ๆ เช่น การขโมยข้อมูลการทำลายระบบ โปรแกรมที่เป็นอันตราย การหลอกลวงให้บุคคลเปิดเผยข้อมูลส่วนตัว การหลอกลวงทางออนไลน์เพื่อขอข้อมูลที่สำคัญเพื่อถ่ายทอดให้ความรู้ต่อไปยังประชาชน เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การโจมตีที่ทำให้ระบบหรือบริการไม่สามารถให้บริการประชาชนได้ การใช้เทคโนโลยีในการสื่อสารกับผู้อื่น แลกเปลี่ยนข้อมูล และสร้างเครือข่ายสังคม การป้องกันข้อมูลส่วนตัวและข้อมูลสำคัญขององค์กรภาครัฐเพื่อบริการประชาชน การลดความเสี่ยงจากการถูกหลอกลวงทางไซเบอร์ การใช้โปรแกรมป้องกันไวรัสและมัลแวร์ การตั้งรหัสผ่านที่ไม่ซ้ำกัน การตรวจสอบความน่าเชื่อถือของเว็บไซต์และลิงก์ การไม่เปิดไฟล์แนบจากผู้ที่ไม่ได้รู้จักและการอัพเดทซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ 4) การพัฒนาประชาชนด้านการป้องกันสังคมที่จะต้องมุ่งมั่นทำเพื่อความปลอดภัยของข้อมูลและความสงบสุขของประชาชน องค์กรภาครัฐควรมีมาตรการความปลอดภัยไซเบอร์อย่างครอบคลุม เตรียมแนวทางการรับมือที่มีประสิทธิภาพที่สุดเพื่อป้องกันการโจมตีที่ส่งผลกระทบต่อความมั่นคงขององค์กรภาครัฐและประชาชน 5) องค์กรภาครัฐพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ที่เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์โดยบูรณาการความร่วมมือภาคประชาชน เร่งผลักดันการพัฒนาความรู้และทักษะด้านไซเบอร์ให้ครอบคลุมประชาชนคนไทยทุกช่วงวัย เพื่อให้ทุกคนสามารถเข้าถึงและเรียนรู้เกี่ยวกับไซเบอร์ ร่วมมือการพัฒนาบุคลากรเพื่อพัฒนาสังคมโดยขยายผลความรู้ด้านความมั่นคงปลอดภัยไซเบอร์สู่ทุกภาคส่วน ส่งเสริมพลเมืองดิจิทัลด้านความมั่นคงปลอดภัยไซเบอร์ทั่วประเทศด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาสังคมให้กับประชาชนทุกช่วงวัยให้ประเทศไทยให้มีความปลอดภัยไซเบอร์ที่แข็งแกร่งจากร่วมมือจากทุกภาคส่วนเพื่อขับเคลื่อนให้ประเทศไทยก้าวสู่การเป็นผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

**เอกสารอ้างอิง**


กนกนก โพธิ์หอม. (2564) พลวัตความมั่นคงทางไซเบอร์ของประเทศไทย. *วารสารมุมมองความมั่นคง, 7*(มิ.ย-ก.ค), 45-54.

กรมกิจการเด็กและเยาวชน. (2566). *แผนรับมือเหตุภัยคุกคามทางไซเบอร์.* กรุงเทพฯ: กรมกิจการเด็กและเยาวชน.

กรมพัฒนาสังคมและสวัสดิการ. (2567). *แผนรับมือเหตุภัยคุกคามทางไซเบอร์.* กรุงเทพฯ: กรมพัฒนาสังคมและสวัสดิการ.

กฤษ ศรีเงิน. (2566). *การพัฒนาป้องกันการแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์ เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์.* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร: มหาวิทยาลัยศรีปทุม.

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์. (2566). *แนวทางการป้องกันภัยคุกคามทางไซเบอร์.* กรุงเทพฯ: กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์.

กระทรวงคมนาคม. (2566). *แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงคมนาคมพ.ศ. 2562 - 2566*. กรุงเทพฯ: กระทรวงคมนาคม.

พลากร ลาภอลงกรณ์. (2567). *การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์.* สืบค้นวันที่ 10 เมษายน 2567, จาก https://ict.dmh.go.th/

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*. กรุงเทพฯ: คณะรัฐมนตรี.

วราภรณ์ เพลิดเพลิน. (2565). *การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรสำนักงาน*

*คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ*. (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง.

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์กรมหาชน). (2567). *วิธีปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ภาครัฐ (Practices for Government Cybersecurity)*. กรุงเทพฯ: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์กรมหาชน).

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์กรมหาชน). (2566). *หลักสูตร Cybersecurity Workshop for Government Agency.* กรุงเทพฯ: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

สำนักยุทธศาสตร์และสารสนเทศ. (2567). *กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework).* กรุงเทพฯ: สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน).

สำนักงานสภาความมั่นคงแห่งชาติ. (2564). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564.* กรุงเทพฯ: สำนักงานสภาความมั่นคงแห่งชาติ.

อริสรา กาญจนอุดม. (2567). *ภัยคุกคามทางไซเบอร์ : การรับมือของประเทศไทย.* สืบค้นวันที่ 10 เมษายน 2568, จาก https://www.senate.go.th/

Axel,T. (2015). Gaining an Edge in Cyberspace with Advanced Situational Awareness. *IBM Research, 5*(22), 419-428.

Cisco. (2021). *Cybersecurity for SMBs Asia Pacific businesses prepare for digital defense.* Retrieved on April 10, 2025, from https://www.cisco.com/

Gruner, E. (2025). 9 Common Cyber Security Threats and 4 Defensive Measures *Cybersecurity for SMBs Asia Pacific businesses prepare for digital defense.* Retrieved on April 10 2025, from https://www.cynet.com/

Herek, G.M. (1986). 'The Instrumentality of Attitudes. *Toward a Neofunctional, 4*(22), 99-114.

Kim, M. s. and Hunter, J. e. (1993). Relationships Among Attitudes, Behavioral Intentions, and Behavior A Meta-Analysis. *Past Research, 7*(2), 331-364.