วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

การสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของคนไทย*

RAISING CYBER SECURITY AWARENESS AMONG THAIS

พระครูวิมลสุวรรณกร (สมพงษ์ จนฺทวโร), พระอุดมสิทธินายก (กำพล คุณงฺกโร)
Phrakhru Wimonsuwannakon (Sompong Chanthawaro),
Phraudomsitthinayok (Kumphol Kunungkaro)
วัดกู้ อำเภอปากเกร็ด จังหวัดนนทบุรี
Wat Ku, Pak Kret District, Nonthaburi Province
Corresponding Author E-mail: sakda2543210@gmail.com

บทคัดย่อ

Cybersecurity Awareness คือ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวกับภัยคุกคามทางไซเบอร์ ความเสี่ยงและแนวทางปฏิบัติที่ดีที่สุดในการปกป้องข้อมูลส่วนบุคคลและองค์กร ซึ่งการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ Cybersecurity Awareness หรือ Security Awareness นี้ เปรียบเสมือนเกราะป้องกันที่ช่วยให้องค์กรสามารถป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ทั้งในปัจจุบันและในอนาคตซึ่ง Cybersecurity Awareness ไม่ได้หมายถึงเพียงแค่การรู้จักเทคโนโลยีหรือมีความคุ้นเคยกับหลักเกณฑ์ความปลอดภัยเท่านั้น แต่ยังเน้นไปถึงการที่ทุกคนในองค์กรมีความรู้ด้านภัยคุกคามทางไซเบอร์และการตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ พูดให้เข้าใจง่าย ๆ การสร้างความตระหนักรู้ในด้านความปลอดภัย Cybersecurity Awareness หรือ Security Awareness ก็คือ การทำให้ผู้ใช้ พนักงานหรือผู้ที่เกี่ยวข้องภายในองค์กรรู้จักและมีความสามารถในการระวังและป้องกันอันตรายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ได้และยังมีกฎหมายที่ช่วยในการตระหนักรู้ความปลอดภัยด้านไซเบอร์หรือภัยคุกคามที่เกิดจากระบบของอินเทอร์เน็ตต่าง ๆ ซึ่งมีพระราชบัญญัติเกี่ยวกับและมีพระราชบัญญัติเกี่ยวกับการนำข้อมูลที่เป็นเท็จลงในคอมพิวเตอร์เป็นต้น ซึ่งเป็นประเด็นสำคัญอย่างยิ่งที่คนไทยจำเป็นจะต้องทราบและมีความรู้เกี่ยวกับเรื่องนี้จึงจะทำให้เกิดความปลอดภัยทั้งทรัพย์สินทั้งชีวิตรวมถึงทำให้สังคมน่าอยู่มากยิ่งขึ้น

คำสำคัญ: ตระหนักรู้; ความปลอดภัย; ไซเบอร์

*Received February 24, 2025; Revised March 25, 2025; Accepted April 3, 2025

Abstract

Cybersecurity Awareness is the creation of cybersecurity awareness about cyber threats, risks, and best practices for protecting personal and organizational information. Cybersecurity Awareness or Security Awareness is like a shield that helps organizations protect themselves from potential cyber threats, both current and future. Cybersecurity Awareness does not only mean knowing about technology or being familiar with security principles, but also emphasizes that everyone in the organization has knowledge of cyber threats and can effectively respond to cyber threats. Simply put, creating cybersecurity awareness or Security Awareness is making users, employees, or those involved in the organization know and have the ability to be aware of and prevent dangers related to cyber security. There are also laws that help in cybersecurity awareness or threats from various internet systems, such as the Act on and the Act on the introduction of false information into computers, etc., which are very important issues that Thai people need to know and have knowledge about in order to create safety for both property and life, as well as making society more livable.

Keywords: Awareness; Security; Cyber

บทนำ

เป็นที่ทราบกันดีว่าในปัจจุบันอินเทอร์เน็ตมีความสำคัญต่อกิจกรรมต่าง ๆ ของมนุษย์เป็นอย่างมาก ไม่ว่าจะในระดับปัจเจก ระดับองค์กร ระดับรัฐ หรือระดับระหว่างประเทศ กิจกรรมที่เคยต้องมีการเคลื่อนไหวทางกายภาพก็กลายเป็นกิจกรรมที่เกิดขึ้นผ่านระบบออนไลน์แทน เช่น การซื้อขายสินค้าต่าง ๆ การใช้บริการทางการเงินกับสถาบันการเงิน การศึกษา รวมไปถึงการติดต่อสื่อสาร ระหว่างกันก็เป็นไปอย่างง่ายดายและไร้พรมแดนต่างกับในอดีตเป็นอย่างมาก พื้นที่ในโลกไซเบอร์ (Cyberspace) เป็นโลกเสมือนจริงที่กิจกรรมมากมายเกิดขึ้นโดยไม่มีสิ่งที่จับต้องได้ แต่สามารถทำให้ กิจกรรมเหล่านั้นสำเร็จตามวัตถุประสงค์ของบุคคลต่าง ๆ ได้เช่นเดียวกับรูปแบบดั้งเดิมของกิจกรรม นั้นในอดีต นอกจากนี้อินเทอร์เน็ตยังมีส่วนสำคัญในการทำให้เกิดการพัฒนาทางเศรษฐกิจ การสื่อสาร โทรคมนาคม การควบคุมโครงสร้างพื้นฐานหรือสาธารณูปโภคที่สำคัญ รวมไปถึงการรักษาความมั่นคง ของรัฐอีกด้วย ลักษณะของโลกไซเบอร์มีความเป็นระหว่างประเทศอยู่ในตัวเอง โดยคอมพิวเตอร์ สมาร์ทโฟน หรืออุปกรณ์อื่น ๆ ที่เชื่อมต่อ

วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

อินเทอร์เน็ตได้ สามารถทำกิจกรรมทางออนไลน์ระหว่างกัน แม้จะอยู่คนละซีกโลกในเวลาอันรวดเร็วโดยไม่ต้องข้ามพรมแดนทางกายภาพไปแต่ในขณะที่มนุษย์ได้รับประโยชน์มากมายจากการใช้อินเทอร์เน็ตและการนำกิจกรรมต่าง ๆ เข้าไปอยู่ในโลกไซเบอร์ใช้อินเทอร์เน็ตเชื่อมโยงทุกสิ่งเข้าด้วยกัน (Internet of Thing: IoT) โดยสามารถเข้าถึงสิ่งเหล่านั้น ๆ ได้อย่างง่ายดาย ก็อาจเสี่ยงต่อภัยคุกคามทางไซเบอร์ (Cyber Threat) ซึ่งภัยคุกคามมีทั้งระดับที่ไม่ร้ายแรงเกิดกับบุคคลทั่วไป จนถึงภัยคุกคามที่ร้ายแรงส่งผลกระทบต่อการดำรงชีวิตของประชาชนจำนวนมากและความมั่นคงของรัฐ เช่น การทำลายระบบควบคุมโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) การจารกรรม (Espionage) ความลับที่เกี่ยวกับความมั่นคง หรือความลับทางการค้าที่สำคัญ (Trade Secret) การใช้มัลแวร์ (Malware) หรือชุดคำสั่งทำลายระบบการทำงานของคอมพิวเตอร์หรือระบบเครือข่ายที่สำคัญให้ไม่สามารถทำงานได้ อย่างปกติ โดยผู้ก่อให้เกิดภัยคุกคามเหล่านั้นอาจกระทำการจากสถานที่ใดในโลกก็ได้ ไม่จำเป็นต้อง อยู่ภายในรัฐที่ได้รับความเสียหาย ซึ่งในปัจจุบันประเทศต่าง ๆ ทั่วโลกรวมถึงองค์การระหว่างประเทศ มีความตื่นตัวในเรื่องภัยคุกคามทางไซเบอร์เป็นอย่างมาก เนื่องจากสถิติของภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็ว มีรูปแบบใหม่ ๆ ที่แตกต่างจากเดิม และมีการพัฒนารูปแบบอยู่ตลอดเวลาอีกทั้งการโจมตีทางไซเบอร์ (Cyber Attack) นั้นสามารถสร้างความเสียหายได้สูงมากเกินกว่าจะคาดการณ์ได้ ทำให้ประเทศต่าง ๆ มีการพัฒนามาตรการและบัญญัติกฎหมายเพื่อรับมือกับ ภัยคุกคามทางไซเบอร์ รวมไปถึงมีการสร้างความร่วมมือในระดับระหว่างประเทศเพื่อร่วมกันวางแนว ปฏิบัติที่เป็นมาตรฐาน ให้คำแนะนำในการเฝ้าระวังและต่อสู้กับภัยคุกคามดังกล่าว

ตัวอย่างเช่น UNGGE ซึ่งเป็นองค์ประชุมในด้านข้อมูลสารสนเทศที่จัดตั้งโดยสหประชาชาติ ได้ให้ ความสำคัญกับประเด็นด้านความมั่นคงไซเบอร์ โดยในปี 2015 ได้มีการลงมติและออกรายงานที่ A/70/174 ระบุว่ากฎหมายระหว่างประเทศมีความสำคัญในการสร้างความมั่นคงปลอดภัยให้แก่รัฐ ในการใช้เทคโนโลยีสารสนเทศ ดังนั้น ควรมีการนำกฎหมายระหว่างประเทศมาบังคับใช้กับโลกไซเบอร์ด้วย ปัจจุบันหลายประเทศได้นำมติและแนวทางของ UNGGE มาใช้ในการสร้างความร่วมมือระหว่างกัน ทั้งในระดับทวิภาคีและความร่วมมือในระดับภูมิภาค ทว่าการนำเอาคำแนะนำของ UNGGE มาดำเนินการบังคับใช้อย่างเท่าเทียมกันในแต่ละประเทศยังคงไม่มีความชัดเจน จึงมีความพยายามของรัฐต่าง ๆ รวมถึงเอกชน อาทิ บริษัทไมโครซอฟท์ ที่พยายามสนับสนุนให้มีการจัดทำอนุสัญญา Digital Geneva Convention เพื่อระบุให้ประเทศต่าง ๆ นำเอามาตรฐานด้านความมั่นคงไซเบอร์ ที่จะถูกพัฒนาขึ้นมาไปใช้ดำเนินการเพื่อให้โลกไซเบอร์มีความปลอดภัย เพื่อเป็นการคุ้มครองและเยียวยาพลเรือนที่ต้องได้รับผลกระทบจากการกระทำ

อันไม่พึงประสงค์ทางไซเบอร์ซึ่งได้รับการ สนับสนุนโดยรัฐ โดยมุ่งจะคุ้มครองพลเรือนตามหลักการสิทธิมนุษยชนระหว่างประเทศและกฎหมาย มนุษยธรรมระหว่างประเทศ ดังเช่นที่เคยมีอนุสัญญาเจนีวา 1949 (Geneva Convention 1949)

สำหรับในระดับประเทศนั้น ประเทศต่าง ๆ มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรม ไซเบอร์ และความมั่นคงทางไซเบอร์กันออกมาเป็นจำนวนมาก รวมไปถึงนโยบายและแผนระดับชาติ อีกด้วย แต่กฎหมาย มาตรการ และนโยบายด้านความมั่นคงไซเบอร์เหล่านั้นส่งผลกระทบโดยตรงกับ สิทธิมนุษยชน เช่น สิทธิในความเป็นส่วนตัว (Right to Privacy) เสรีภาพในการแสดงออก (Freedom of Expression) สิทธิในการเข้าถึงข้อมูลข่าวสาร (Right to Access to Information) เป็นต้น โดยผู้ มีอำนาจกำหนดนโยบายหรือผู้มีอำนาจตรากฎหมายมีวัตถุประสงค์เพื่อจะปกป้องโลกไซเบอร์ ตลอดจนระบบเทคโนโลยีสารสนเทศจากการกระทำในทางไม่พึงประสงค์ ซึ่งในปัจจุบันไม่เพียงแต่บุคคลหรือกลุ่มบุคคลที่เป็นมิจฉาชีพ หรือกระทำในลักษณะการก่อการร้าย แต่ยังอาจรวมไปถึงการกระทำภายใต้การสนับสนุนโดยรัฐใดรัฐหนึ่ง โดยมีเจตนามุ่งร้ายต่อรัฐอื่น ๆ ทำให้กฎหมายและ มาตรการต่าง ๆ ที่ออกมาให้น้ำหนักไปในเรื่องความมั่นคงเป็นหลัก แทนที่จะมุ่งไปในเรื่องการรักษา ความปลอดภัยของระบบ จนทำให้กฎเกณฑ์ในเรื่องความมั่นคงทางไซเบอร์ในประเทศต่าง ๆ มีมากมายและกว้างเกินไป ขาดความชัดเจนและปราศจากการตรวจสอบถ่วงดุล หรือกลไกความรับผิด ต่อระบอบ (Regime) อื่น ๆ การเยียวยาผู้ได้รับผลกระทบจากการบังคับใช้มาตรการต่าง ๆ เหล่านั้น ซึ่งสามารถนำไปสู่การละเมิดสิทธิมนุษยชนได้ในกรณีของประเทศไทยได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562 (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562) ซึ่งประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 และมีผลใช้บังคับ ตั้งแต่วันที่ 28 พฤษภาคม พ.ศ. 2562 ซึ่งพระราชบัญญัติฉบับนี้ถูกวิพากษ์วิจารณ์โดยภาคส่วนต่าง ๆ ในสังคมอย่างกว้างขวาง ด้วยความวิตกกังวลว่าจะก่อให้เกิดการละเมิดสิทธิมนุษยชน เพราะความไม่ ชัดเจนในการให้นิยามของคำสำคัญในบทบัญญัติต่าง ๆ รวมไปถึงการใช้ดุลพินิจของเจ้าหน้าที่ผู้มี อำนาจหน้าที่ในการบังคับใช้กฎหมายดังกล่าวการศึกษาการตระหนักรู้ความปลอดภัยทางไซเบอร์ของคนไทยจึงมีความสำคัญอย่างยิ่งที่จะทำให้ประชาชนได้มีความเข้าใจในระบบอินเตอร์เน็ตและความปลอดภัยทำให้ป้องกันภัยที่จะเกิดขึ้นต่าง ๆทำให้เป็นสิ่งที่องค์ความรู้นำมาพัฒนาเป็นแนวทางในการปฏิบัติปัจจุบันของคนไทยได้เป็นอย่างดีผู้เขียนจึงได้นำเสนอบทความวิชาการเรื่องการสร้างการตระหนักรู้ด้านการปลอดภัยไซเบอร์ของคนไทยเพื่อเป็นแนวทางทางวิชาการและนำไปสู่การปฏิบัติจริงทำให้สังคมได้อยู่และปลอดภัย

วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

ความสำคัญของความปลอดภัยทางไซเบอร์

โดยสิ่งที่สามารถช่วยในการสร้าง Cybersecurity Awareness ให้กับทุกคนภายในองค์กรได้ นั่นก็คือการจัดอบรม Security Awareness Training เสริมการเรียนรู้และทำแบบทดสอบความรู้เกี่ยวกับ Cybersecurity Awareness เพื่อให้แน่ใจได้ว่า บุคลากรภายในองค์กรจะมีความพร้อมในการค้นหา ป้องกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพนั่นเอง

เนื่องจากในปัจจุบันภัยคุกคามทางไซเบอร์มีรูปแบบที่หลากหลายและซับซ้อนค มากขึ้น องค์กรต่าง ๆ จึงจำเป็นต้องมีมาตรการ Cybersecurity เพื่อปกป้องข้อมูลและระบบสารสนเทศของตนเอง เรียกได้ว่าการทำ Cybersecurity Awareness ก็คือ หนึ่งในมาตรการที่ช่วยสร้างความตระหนักรู้ที่นำไปสู่การป้องกันภัยคุกคามทางไซเบอร์ต่าง ๆ ได้เป็นอย่างดี ซึ่ง Cybersecurity Awareness จะสำคัญกับองค์กรมากน้อยแค่ไหนนั้น? ตาม SOSECURE ดังนี้ คือ

- ลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ เนื่องจากบุคลากรในองค์กรมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ จึงสามารถสังเกตและป้องกันภัยคุกคามต่าง ๆ ได้อย่างทันท่วงที

- ป้องกันการบุกรุกการรู้และเข้าใจเกี่ยวกับเทคนิคและวิธีการที่ผู้ไม่หวังดีใช้ในการโจมตีจะช่วยลดโอกาสที่จะเกิดการบุกรุก และเสริมความสามารถในการรู้จักและป้องกันก่อนที่จะเกิดความเสียหายกับองค์กรได้

- ป้องกันการรั่วไหลข้อมูลการตระหนักรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ Cybersecurity Awareness สามารถช่วยให้บุคลากรในองค์กรระวังปัญหาที่เกี่ยวข้องกับความปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับได้ในระดับหนึ่ง

- ลดค่าใช้จ่ายในการแก้ไขปัญหาการโจมตีทางไซเบอร์ เมื่อเกิดการโจมตีทางไซเบอร์ขึ้น องค์กรจำเป็นต้องมีค่าใช้จ่ายในการแก้ไขปัญหาต่าง ๆ เช่น การกู้คืนข้อมูล การแก้ไขระบบที่เสียหาย เป็นต้น การลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์จะช่วยให้องค์กรลดค่าใช้จ่ายในการแก้ไขปัญหาต่าง ๆ เหล่านี้ได้

- สร้างภาพลักษณ์ที่ดีให้กับองค์กร การที่บุคลากรภายในองค์กรมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ความเสี่ยง และแนวทางปฏิบัติที่ดีของ Cybersecurity คือสิ่งที่สามารถส่งเสริมภาพลักษณ์ให้กับองค์กรได้เป็นอย่างดี เพราะเมื่อทุกคนภายในองค์กรรู้จักกับสิ่งเหล่านั้นก็จะทำให้องค์กรมีมาตรการรักษาความปลอดภัยทางไซเบอร์ที่ดีและย่อมได้รับความไว้วางใจจากลูกค้าและคู่ค้ามากขึ้น ทั้งนี้ยังสามารถรักษาความน่าเชื่อถือจากลูกค้าได้อีกด้วย

- สะท้อนถึงความเป็นมืออาชีพ การมีความรู้และการตระหนักรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ Cybersecurity Awareness มีผลต่อภาพลักษณ์และความเป็นมืออาชีพขององค์กรเป็นอย่างมาก โดยองค์กรที่ให้ความสำคัญกับความปลอดภัยทางไซเบอร์ย่อมแสดงให้เห็นถึงความใส่ใจในการปกป้องข้อมูลและทรัพย์สินขององค์กร ซึ่งเป็นสิ่งสำคัญสำหรับการดำเนินธุรกิจขององค์กรในยุคนี้

- เป็นส่วนหนึ่งของการปรับตัวที่รวดเร็ว อีกหนึ่งความสำคัญของ Cybersecurity Awareness คือช่วยให้บุคลากรมีความรู้และความเข้าใจเกี่ยวกับเทคโนโลยีใหม่ ๆ สามารถสังเกตและป้องกันภัยคุกคามทางไซเบอร์ใหม่ ๆ ได้อย่างทันท่วงที ทั้งยังช่วยให้บุคลากรภายในองค์กรสามารถประยุกต์ใช้เทคโนโลยีใหม่ ๆ เพื่อเพิ่มประสิทธิภาพด้านความปลอดภัยได้อีกด้วย

การตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ หรือ Security Awareness ไม่ได้เป็นเพียงมาตรการเชิงรุกเท่านั้น แต่ยังเป็นองค์ประกอบพื้นฐานของกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ที่ครอบคลุมสำหรับทุกองค์กร

ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ (โสพส พินิจศักดิ์, 2526)

ความรู้พื้นฐานของความหมายของการรักษาความปลอดภัยไซเบอร์

- Confidentiality การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลาดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนของพนักงาน จัดเป็น ความลับสูงสุดผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

- Integrity การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

- Availability ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

รูปแบบภัยคุกคามของ Cyber Security

1. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทาให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึง Server ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (Worms) และโทรจัน (Trojans)

2. Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น Email SMS เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

3. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความหรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น Email SMS เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

4. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน คือ สำรองข้อมูลเป็นประจำโดยทำการแยกเก็บไฟล์สารองข้อมูล ควรติดตั้ง Anti Malware และมีการ Update อย่างสม่ำเสมอ และก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด (นวลจันทร์ ทัศนชัยกุล, 2541)

แหล่งที่มาของภัยคุกคามทางไซเบอร์ การเกิดขึ้นของภัยคุกคามทางไซเบอร์นั้นอาจเกิดขึ้นจากกลุ่มบุคคลหรือองค์กรที่มีความชำนาญในการปฏิบัติการเพื่อเข้าถึงเครือข่ายและข้อมูล ซึ่งการเข้าถึงอาจเกิดขึ้นได้จากบุคคล ที่ได้รับความเชื่อถือภายในหน่วยงานนั้นเอง หรือการเข้าถึงระยะไกลจากบุคคลนิรนามผ่านทาง อินเทอร์เน็ต โดยศูนย์บูรณาการความมั่นคงปลอดภัยไซเบอร์และการสื่อสารแห่งชาติ (The National Cybersecurity and Communications Integration Center: NCCIC) ซึ่งเป็นหน่วยงานภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) ของสหรัฐอเมริกา ได้จำแนกกลุ่มบุคคลและองค์กรที่ทำให้เกิดภัยคุกคามไซเบอร์ออกเป็น 5 กลุ่มหลัก (NCCIC, 2019) ได้แก่

1. รัฐบาลแห่งชาติ (National Governments) การโจมตีของกลุ่มงานความมั่นคงหรือกองทัพ ด้วยจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้นกับประเทศเป้าหมาย ทั้งการ ก่อกวนเว็บไซต์ การโฆษณาชวนเชื่อและการสร้างความรำคาญให้แก่เว็บเพจ โดยมีความเสียหายระดับต่ำไปจนถึงการจารกรรมข้อมูล การโจมตีที่ร้ายแรงถึงชีวิตและแม้แต่สร้างความเสียหายให้กับโครงสร้างพื้นฐานที่สำคัญของประเทศ ซึ่งสหรัฐอเมริกาเชื่อว่า ภัยคุกคามทางไซเบอร์ที่ทรงอานุภาพเช่นนั้นเป็น การกระทำที่ได้รับการสนับสนุนจากรัฐ แน่นอนว่าประเทศที่ถูกจับตามองเป็นพิเศษ ได้แก่ จีน ซึ่งถูก ระบุว่า ผู้ที่เข้ามาโจมตีเว็บไซต์พาณิชย์ของสหรัฐอเมริกา รวมถึงจารกรรมข้อมูลสมาชิกของ ผู้ให้บริการบนระบบเครือข่ายอินเตอร์เน็ต

2. ผู้ก่อการร้าย (Terrorists) โดยทั่วไปมีจุดมุ่งหมายเพื่อที่จะทำลาย ผลประโยชน์ของชาติอยู่แล้ว กลุ่มนี้จะใช้โลกไซเบอร์สร้างแบบแผนหาเงินทุน เผยแพร่แนวความคิดและเป็นช่องทางการสื่อสาร โดยมีเป้าหมายเพื่อกระจายความหวาดกลัวไปยังพลเรือน

3. สายลับของเอกชนและองค์กรอาชญากรรม (Industrial Spies and Organized Crime Groups) มีการใช้โลกไซเบอร์ในการบุกรุกและโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลและทรัพย์สินทั้งจากภาครัฐและเอกชน อาจมีการโจมตีโครงสร้างพื้นฐานเพื่อให้เกิด ผลประโยชน์กับคู่แข่งของเอกชนที่ถูกโจมตี หรือเกิดประโยชน์กับกลุ่มอื่น ๆ โดยมีการขโมยความลับ ทางการค้าแล้วนำข้อมูลไปขาย หรือแบล็คเมล์บริษัทที่ถูกขโมยข้อมูลโดยใช้ความเสี่ยงภัยของ สาธารณะเป็นเครื่องมือในการข่มขู่

4. แฮกทิวิส (Hacktivists) คือกลุ่มแฮกเกอร์ที่ใช้แรงจูงใจทางการเมือง เพื่อรวมกลุ่มและผลักดันให้เกิดความเปลี่ยนแปลงทางความคิด หรือการต่อต้านรัฐโดยการสนับสนุน วาระทางการเมือง การสร้างมูลเหตุที่ส่งผลต่อทางการเมืองและสังคมมากกว่าการสร้างความเสียหาย ให้กับโครงสร้างพื้นฐาน

5. แฮกเกอร์ (Hackers) คือ ผู้ที่พยายามหาวิธีการหรือหาช่องโหว่ของระบบเพื่อแอบลักลอบเข้าสู่ระบบ ล้วงความลับหรือแอบดูข้อมูลข่าวสาร จนถึงทำลายข้อมูลข่าวสารและทำ ความเสียหายให้กับองค์กร ในปัจจุบันปัญหาในเรื่องอาชญากรรมทางด้านเทคโนโลยี โดยเฉพาะ ในเรื่องแฮกเกอร์ก็มีให้เห็นมากขึ้น ผู้ที่แอบลักลอบเข้าสู่ระบบจึงมาได้จากทั่วโลก ทำให้ดำเนินการ

ภัยคุกคามทางไซเบอร์ที่ได้กล่าวถึงไปข้างต้นนั้น สามารถทำให้เกิดความเสียหายได้ หลายระดับ แต่ภัยคุกคามที่จะทำให้เกิดความเสียหายในระดับร้ายแรงมักเป็นภัยคุกคามที่มุ่งโจมตี โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งจะกระทบต่อการดำรงชีวิตของประชาชนจำนวนมาก และอาจร้ายแรงถึงขั้นบาดเจ็บและเสียชีวิตได้ เช่น โรงไฟฟ้านิวเคลียร์ระบบผลิตและจ่ายกระแสไฟฟ้า กิจการขนส่งมวลชน การจราจรทาง

วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

อากาศ บริการสาธารณสุข บริการทางการเงิน เป็นต้น ซึ่งจะส่งผลกระทบไปยังความมั่นคงของรัฐในด้านเศรษฐกิจ สังคม และด้านอื่น ๆ อย่างไม่อาจหลีกเลี่ยงได้ การเฝ้าระวังการโจมตีต่อโครงสร้างพื้นฐานที่สำคัญนี้เองทำให้รัฐต่าง ๆ ออกแบบนโยบายและมาตรการเพื่อรับมืออย่างเข้มงวด สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ให้นิยามไว้ (Wamala, 2012) สรุปได้ว่า โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) เป็นระบบที่เป็นหัวใจของการให้บริการหรือการทำงาน ซึ่งหากถูกทำให้หยุดชะงักหรือถูกทำลายจะส่งผลกระทบให้เกิดความอ่อนแอลงของการสาธารณสุขความปลอดภัย การพาณิชย์ และความมั่นคงของชาติ หรือ หลายประการข้างต้นรวมกัน

การกำหนดว่า สิ่งใดเป็นโครงสร้างพื้นฐานที่สำคัญก็มีความแตกต่างกันไปในแต่ละประเทศ ซึ่งมีทั้งส่วนที่อยู่ในภาครัฐและภาคเอกชน เช่น ประเทศไทยได้มีประกาศคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร ที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับ เคร่งครัด พ.ศ. 2559 ซึ่งระบุชื่อหน่วยงาน จำนวน 121 หน่วยงาน โดยธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน นอกจากนี้ยังมีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งหมายถึง ระบบสารสนเทศที่หน่วยงานซึ่งเป็นโครงสร้างพื้นฐานสำคัญของประเทศใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อ เศรษฐกิจและสังคม ได้แบ่ง CII ออกเป็นกลุ่มใหญ่ ๆ 6 กลุ่ม (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2561) ได้แก่ 1. กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ 2. กลุ่มการเงิน 3. กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม 4. กลุ่มการขนส่ง และโลจิสติกส์ 5. กลุ่มพลังงานและสาธารณูปโภค และ 6. กลุ่มสาธารณสุข

พ.ร.บ.ไซเบอร์ พ.ศ. 2562 (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562) เป็นกฎหมายที่สำคัญในการปรับปรุงและควบคุมความปลอดภัยทางไซเบอร์ในประเทศไทย โดยมีเนื้อหาสำคัญดังนี้

1. กำหนดหน้าที่และอำนาจของหน่วยงานด้านความปลอดภัยทางไซเบอร์: กำหนดหน้าที่และอำนาจของหน่วยงานที่เกี่ยวข้องเพื่อดูแลและควบคุมความปลอดภัยทางไซเบอร์ในระดับประเทศ

2. ความรับผิดชอบของผู้ประกอบการ: กำหนดความรับผิดชอบของผู้ประกอบการในการรักษาความปลอดภัยทางไซเบอร์ของข้อมูลลูกค้าและลูกค้า

3. ความลับและความเป็นส่วนตัว: การรักษาความลับและความเป็นส่วนตัวของข้อมูลที่เกี่ยวข้องกับการทำธุรกิจทางอิเล็กทรอนิกส์

4. การเสริมสร้างความตระหนักรู้และการศึกษา: ส่งเสริมความตระหนักรู้และการศึกษาในเรื่องความปลอดภัยทางไซเบอร์ให้กับผู้ประกอบการและประชาชนทั่วไป

5. มาตรการความปลอดภัยทางไซเบอร์: กำหนดมาตรการความปลอดภัยที่ผู้ประกอบการต้องปฏิบัติเพื่อรักษาความปลอดภัยทางไซเบอร์ เช่น การรักษาความมั่นคงของระบบเทคโนโลยีสารสนเทศ การเข้ารหัสข้อมูล และการสร้างระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย

6. การประกาศเกี่ยวกับความเสียหายและการเสียชีวิตจากการกระทำที่ผิดกฎหมายทางไซเบอร์: กำหนดการประกาศความเสียหายและการเสียชีวิตที่เกิดจากการกระทำที่ผิดกฎหมายทางไซเบอร์

7. มาตรการโดยสารสนเทศ: กำหนดมาตรการเพื่อรักษาความปลอดภัยทางไซเบอร์ในการส่งสัญญาณทางโทรคมนาคมและเนื้อหาทางอิเล็กทรอนิกส์

ส่วนที่ 4 การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา 58 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

หมวด 4 บทกำหนดโทษ

มาตรา 70 ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูล คอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูล ของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ ในการดำเนินคดีกับผู้กระทำ

วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 8 ฉบับที่ 2 มีนาคม - เมษายน 2568 น.294-305

ความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือ เพื่อประโยชน์ในการดำเนินคดี กับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

มาตรา 72 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562)

สรุป

การรักษาความปลอดภัยไซเบอร์ของประเทศไทยเป็นสิ่งจำเป็น ปัจจุบันภัยคุกคามทางไซเบอร์ในโลกออนไลน์ ได้มีวิวัฒนาการหลากหลายรูปแบบ แต่ทุกการหลอกลวงและโจมตีนั้น ไม่ได้มีลักษณะตายตัว แม้ว่าจะมีความคล้ายคลึงกันบ้าง แต่ก็จะมีวิธีรับมือที่แตกต่างกันออกไป อย่างไรก็ตาม ภัยคุกคามทางไซเบอร์ที่พบมากที่สุดในปัจจุบันมี 5 ประเภท สร้างความเสียหายที่ประชาชนถูกมิจฉาชีพหลอกลวงมากที่สุด เรามาเรียนรู้รูปแบบของภัยคุกคามทางไซเบอร์ในโลกออนไลน์ที่พบได้บ่อย พร้อมวิธีการป้องกันเพิ่มความระมัดระวัง และเตรียมตัวรับมือ เพื่อไม่ให้ตกเป็นเหยื่อมิจฉาชีพ 1. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์การหลอกลวงซื้อขายสินค้าและบริการ 2. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์การหลอกให้โอนเงินหารายได้เสริม (ทำภารกิจ) 3. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์การหลอกให้กู้เงินแต่ไม่ได้เงิน 4. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์การหลอกให้ลงทุนผ่านคอมพิวเตอร์ 5. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์การข่มขู่ทางโทรศัพท์ Call Center (อัณณพ ชูบำรุง, 2532)

เอกสารอ้างอิง

นวลจันทร์ ทัศนชัยกุล. (2541). *อาชญากรรม*. กรุงเทพฯ: พรทิพย์การพิมพ์.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 20.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).(2561). *‘Critical Infrastructures (CI) และ Critical Information Infrastructures (CII) ความจำเป็นที่ต้องให้ความสำคัญและต้อง ทบทวน การประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานที่สำคัญของประเทศ*. กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

โสพส พินิจศักดิ์. (2526). *การยอมรับบทบาทของบุคลากรด้านอาชญาวิทยาในการบัญชาการตำรวจนครบาล* (วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม). นครปฐม: มหาวิทยาลัยมหิดล.

อัณณพ ชูบำรุง. (2532). *ทฤษฎีอาชญาวิทยา*. กรุงเทพฯ: มหาวิทยาลัยเกษตรศาสตร์.

Wamala, F. (2012). *The ITU National Cybersecurity Strategy Guide*. Geneva: International Telecommunication Union.

NCCIC. (2019). *Department of Homeland Security, 'Cyber Threat Source Description'*. Retrieved May 15, 2024, from https://shorturl.asia/plOZy