วารสารสหวิทยาการนวัตกรรมปริทรรศน์
ปีที่ 9 ฉบับที่ 1 มกราคม - กุมภาพันธ์ 2569 น.304-316.

ผลกระทบของนโยบายความปลอดภัยไซเบอร์ต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ*

IMPACT OF CYBERSECURITY POLICY ON THE DEVELOPMENT OF THE DIGITAL ECONOMY OF THE COUNTRY

โศภิษฐ์ บุญทอง
Sophit Bunthong
บริษัท คริปโตพร็อพ จำกัด
Cryptoprop Co., Ltd.
Corresponding Author E-mail: sophit.mcu@gmail.com

บทคัดย่อ

บทความวิชาการนี้มุ่งศึกษาวิเคราะห์ผลกระทบของนโยบายความปลอดภัยไซเบอร์ต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศไทย โดยใช้แนวคิดการพัฒนาเศรษฐกิจดิจิทัลร่วมกับกรอบความปลอดภัยไซเบอร์เป็นหลัก นโยบายความปลอดภัยไซเบอร์ที่มีประสิทธิภาพส่งผลต่อการเติบโตของเศรษฐกิจดิจิทัลในด้านบวก ซึ่งสามารถสร้างความเชื่อมั่นให้กับผู้ลงทุนและผู้บริโภค อย่างไรก็ตาม การบังคับใช้กฎหมายที่เข้มงวดเกินไปอาจส่งผลกระทบต่อนวัตกรรมและการแข่งขันในตลาดได้ การศึกษานี้นำเสนอแนวทางสมดุลระหว่างการรักษาความปลอดภัยไซเบอร์และการส่งเสริมการเติบโตของเศรษฐกิจดิจิทัล โดยเน้นการมีส่วนร่วมของทุกภาคส่วนในการสร้างระบบนิเวศดิจิทัลที่ปลอดภัยและยั่งยืน

คำสำคัญ: ผลกระทบ; นโยบายความปลอดภัยไซเบอร์; การพัฒนาเศรษฐกิจดิจิทัล

Abstract

This academic paper aims to examine the impact of cybersecurity policy on the development of Thailand’s digital economy, using the concept of digital economy development and cybersecurity framework as the main principles. The results of the study reveal that effective cybersecurity policies positively affect the growth of the digital economy, which can build confidence among investors and consumers. However, overly strict

*Received May 31, 2025; Revised February 9, 2026; Accepted February 19, 2026

enforcement of the law can affect innovation and market competition. This study proposes a balanced approach between cybersecurity and promoting the growth of the digital economy, emphasizing the participation of all sectors in creating a safe and sustainable digital ecosystem.

Keywords: Impact; Cybersecurity Policy; Digital Economy Development

บทนำ

ในยุคที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตและการประกอบธุรกิจ ความปลอดภัยไซเบอร์ได้กลายเป็นปัจจัยวิกฤตที่ส่งผลกระทบโดยตรงต่อเสถียรภาพทางเศรษฐกิจและความมั่นคงของชาติ อย่างไรก็ตาม สถานการณ์การรักษาข้อมูลในโลกไซเบอร์ของประเทศไทยปัจจุบันยังคงเผชิญกับความท้าทายอย่างหนัก โดยสถิติเหตุการณ์ความไม่ปลอดภัยไซเบอร์เพิ่มขึ้นอย่างมีนัยสำคัญจาก 135 เหตุการณ์ในปี พ.ศ. 2564 เป็นมากกว่า 772 เหตุการณ์ในปี 2565 (U.S. Department of Commerce, 2024) ภัยคุกคามส่วนใหญ่เป็นการละเมิดข้อมูลที่เกิดขึ้นผ่านเว็บไซต์ของสถานศึกษาและหน่วยงานภาครัฐ ซึ่งสะท้อนให้เห็นว่าข้อมูลของประชาชนยังมีความเสี่ยงสูงต่อการถูกโจรกรรมโดยองค์กรที่มุ่งแสวงหาผลประโยชน์ รัฐบาลไทยจึงได้ตราพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อเป็นกรอบกฎหมายที่ครอบคลุมในการคุ้มครองฐานข้อมูลสารสนเทศทั้งภาครัฐและเอกชน (Nishimura & Asahi, 2019)

การพัฒนาเศรษฐกิจดิจิทัลของประเทศไทยในช่วง 5 ปีที่ผ่านมามีการขยายตัวอย่างต่อเนื่องและสร้างรายได้มหาศาลให้แก่ประเทศ โดยในปี 2567 คาดการณ์ว่าเศรษฐกิจดิจิทัลจะเติบโตถึงร้อยละ 5.7 ซึ่งคิดเป็นมูลค่าประมาณ 4.44 ล้านล้านบาท (The Nation Thailand, 2024) หากพิจารณาในมิติด้านการสร้างรายได้จากการรักษาความปลอดภัยไซเบอร์ พบว่าตลาดนี้มีแนวโน้มเติบโตอย่างแข็งแกร่ง โดยคาดว่าจะมีมูลค่าสูงถึง 508.89 ล้านดอลลาร์สหรัฐในปี 2568 และจะขยับขึ้นเป็น 984.12 ล้านดอลลาร์สหรัฐภายในปี 2573 (Mordor Intelligence, 2024) ข้อมูลย้อนหลังยังระบุว่า ขนาดของเศรษฐกิจดิจิทัลไทยในปี 2566 มีมูลค่าสูงถึงร้อยละ 6 ของผลิตภัณฑ์มวลรวมในประเทศ (GDP) หรือคิดเป็น 36 พันล้านดอลลาร์สหรัฐ ซึ่งรายได้เหล่านี้ส่วนหนึ่งมาจากการขยายตัวของอุตสาหกรรมโทรคมนาคมและเนื้อหาดิจิทัลที่เติบโตอย่างรวดเร็ว

ความเชื่อมั่นในมาตรฐานความปลอดภัยไซเบอร์ยังมีส่วนสำคัญในการผลักดันรายได้จากการส่งออกสินค้าและบริการดิจิทัล ซึ่งคาดว่าจะเติบโตถึงร้อยละ 17.2 ในปี พ.ศ.2567 ซึ่งสูงกว่าอัตราการเติบโตของการส่งออกโดยรวมถึง 2.8 เท่า (The Nation Thailand, 2025) นอกจากนี้ นโยบายที่ชัดเจนยังช่วยดึงดูดการลงทุนโดยตรงจาก

ต่างประเทศ (FDI) ในโครงสร้างพื้นฐานสำคัญ เช่น ระบบคลาวด์และปัญญาประดิษฐ์ (AI) โดยมีบริษัทข้ามชาติเข้าลงทุนในไทยด้วยมูลค่ารวมกว่า 100 พันล้านบาทในช่วงต้นปี 2568 (The Nation Thailand, 2025) สิ่งนี้แสดงให้เห็นว่าการมีนโยบายความปลอดภัยไซเบอร์ที่มีประสิทธิภาพสามารถเปลี่ยนจากต้นทุนการป้องกัน ให้กลายเป็นปัจจัยหลักในการสร้างความได้เปรียบทางเศรษฐกิจและดึงดูดเม็ดเงินเข้าสู่ประเทศได้อย่างเป็นรูปธรรม อย่างไรก็ตาม แม้นโยบายความปลอดภัยไซเบอร์จะมีผลกระทบเชิงบวก แต่ผู้เขียนเล็งเห็นว่าการบังคับใช้กฎระเบียบที่เข้มงวดเกินไปอาจส่งผลกระทบย้อนกลับต่อการแข่งขันและนวัตกรรม โดยเฉพาะข้อกำหนดเรื่องการจัดเก็บข้อมูลในประเทศ (Data Localization) หรือมาตรฐานที่ซับซ้อนสำหรับการให้บริการดิจิทัล มาตรฐานเหล่านี้อาจกลายเป็นอุปสรรคสำคัญต่อสตาร์ทอัพและวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ที่มีทรัพยากรจำกัดในการปฏิบัติตามกฎหมาย ความท้าทายดังกล่าวอาจนำไปสู่ต้นทุนการดำเนินงานที่สูงขึ้นและลดขีดความสามารถในการแข่งขันในตลาดสากล (Tilleke & Gibbins, 2024) ปัญหานี้จึงเป็นประเด็นสำคัญที่ต้องได้รับการวิเคราะห์เพื่อหาจุดสมดุลที่เหมาะสม

จากความสำคัญและความท้าทายที่กล่าวมาข้างต้น จึงเป็นแรงจูงใจสำคัญที่ทำให้ผู้เขียนสนใจนำเสนอบทความวิชาการฉบับนี้ เพื่อศึกษาวิเคราะห์ความสัมพันธ์เชิงนโยบายความปลอดภัยไซเบอร์ที่มีต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศไทย ผู้เขียนมุ่งหวังที่จะนำเสนอองค์ความรู้เกี่ยวกับแนวทางการสร้างสมดุลระหว่างการกำกับดูแลและการส่งเสริมนวัตกรรม โดยเน้นการมีส่วนร่วมของทุกภาคส่วนเพื่อสร้างระบบนิเวศดิจิทัลที่ปลอดภัยและยั่งยืน การศึกษาครั้งนี้ไม่เพียงแต่จะช่วยให้เข้าใจผลกระทบในมิติต่าง ๆ อย่างรอบด้าน แต่ยังนำไปสู่ข้อเสนอแนะในการกำหนดนโยบายที่มีประสิทธิภาพ เพื่อให้ประเทศไทยบรรลุเป้าหมายการเป็นศูนย์กลางดิจิทัลของภูมิภาคอาเซียนได้อย่างมั่นคงต่อไป

แนวคิดเกี่ยวกับนโยบายความปลอดภัยไซเบอร์

1. กรอบกฎหมายและนโยบายหลัก นโยบายความปลอดภัยไซเบอร์ของประเทศไทยมีรากฐานมาจากพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 กฎหมายฉบับนี้มีวัตถุประสงค์หลักเพื่อรักษาความมั่นคงปลอดภัยแห่งชาติในพื้นที่ไซเบอร์ โดยครอบคลุมทั้งฐานข้อมูลและสารสนเทศของภาครัฐและเอกชน (Nishimura & Asahi, 2019) พระราชบัญญัติดังกล่าวกำหนดให้มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) โดยมีนายกรัฐมนตรีเป็นประธาน พร้อมด้วยผู้แทนจากกระทรวงและหน่วยงานที่เกี่ยวข้อง รวมถึงผู้เชี่ยวชาญจากภาคเอกชน คณะกรรมการนี้มีหน้าที่กำหนดนโยบายและแผนปฏิบัติการด้านความ

ปลอดภัยไซเบอร์ รวมถึงมาตรฐานขั้นต่ำสำหรับระบบคอมพิวเตอร์ที่ใช้ในหน่วยงานภาครัฐและองค์กรโครงสร้างพื้นฐานสารสนเทศสำคัญ (Asia Law Portal, 2019) ดังนั้น นโยบายความปลอดภัยไซเบอร์มีจุดเริ่มต้นจากพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมุ่งเน้นการรักษาความมั่นคงปลอดภัยในพื้นที่ไซเบอร์ทั้งภาครัฐและเอกชน โดยมีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน ทำหน้าที่กำหนดนโยบาย แผนปฏิบัติการ และมาตรฐานขั้นต่ำสำหรับระบบคอมพิวเตอร์ที่สำคัญของประเทศ

2. การจำแนกโครงสร้างพื้นฐานสารสนเทศสำคัญ พระราชบัญญัติฯ ได้กำหนดโครงสร้างพื้นฐานสารสนเทศสำคัญ (Critical Information Infrastructure: CII) ไว้ 7 ด้าน ได้แก่ ความมั่นคงแห่งชาติ การบริการสาธารณะที่จำเป็น การธนาคารและการเงิน เทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ สาธารณูปโภค (ไฟฟ้า ปิโตรเลียมและก๊าซธรรมชาติ สาธารณูปการประปา) และสาธารณสุข (Tilleke & Gibbins, 2024) องค์กรที่ดำเนินการในด้านเหล่านี้จะต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยไซเบอร์ที่เข้มงวด โดยต้องมีแผนบริหารความเสี่ยงด้านความปลอดภัยไซเบอร์ การประเมินความเสี่ยงอย่างน้อยปีละครั้ง และแผนตอบสนองภัยคุกคามไซเบอร์ รวมถึงการรายงานเหตุการณ์ด้านความปลอดภัยไซเบอร์ต่อหน่วยงานที่เกี่ยวข้องภายใน 30 วัน ดังนั้น กฎหมายกำหนดกลุ่มเป้าหมายหลักเป็นโครงสร้างพื้นฐานสารสนเทศสำคัญ 7 ด้าน ได้แก่ ความมั่นคงแห่งชาติ บริการสาธารณะ การเงิน โทรคมนาคม การขนส่ง สาธารณูปโภค และสาธารณสุข โดยองค์กรในกลุ่มนี้มีพันธะหน้าที่ทางกฎหมายที่ต้องจัดทำแผนบริหารความเสี่ยง ประเมินความปลอดภัยประจำปี และรายงานเหตุการณ์ภัยคุกคามภายในระยะเวลาที่กำหนด

3. มาตรฐานและแนวปฏิบัติใหม่เพื่อให้เท่าทันต่อภัยคุกคามในปัจจุบันทางทีมคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ออกประกาศเพิ่มเติมในเดือนมกราคม 2567 จำนวน 3 ฉบับ เพื่อกำหนดข้อกำหนดด้านความปลอดภัยสำหรับองค์กรและสินทรัพย์สำคัญ โดยมีประกาศสำคัญ 2 ฉบับที่จะเริ่มมีผลบังคับใช้ในวันที่ 18 มกราคม 2568 ได้แก่ มาตรฐานการกำหนดประเภทความปลอดภัยสำหรับระบบข้อมูลหรือสารสนเทศ และมาตรฐานขั้นต่ำสำหรับระบบข้อมูลและสารสนเทศ (Tilleke & Gibbins, 2024) นอกจากนี้ ในเดือนกันยายน 2567 ได้มีการออกมาตรฐานการรักษาความปลอดภัยไซเบอร์ในระบบคลาวด์คอมพิวติ้ง พ.ศ. 2566 เพื่อควบคุมผู้ให้บริการคลาวด์ให้ดำเนินการตามมาตรฐานที่กำหนด โดยเฉพาะระบบสารสนเทศที่มีระดับผลกระทบสูงจะถูกบังคับให้ต้องดำเนินงานจากศูนย์ข้อมูลหลัก (Data Center) ที่ตั้งอยู่ในประเทศไทยเท่านั้น เพื่อความมั่นคงและความปลอดภัยของข้อมูลภายในประเทศ (Digital Policy Alert, 2024)

สรุปได้ว่า การปรับปรุงข้อกำหนดให้ทันสมัยนั้นต้องผ่านประกาศมาตรฐานความปลอดภัยใหม่ที่มุ่งเน้นการจำแนกประเภทความปลอดภัยข้อมูลและระบบสารสนเทศ ซึ่งจะมีผลบังคับใช้เต็มรูปแบบในปี 2568 นอกจากนี้ ยังมีการให้ความสำคัญกับระบบคลาวด์คอมพิวติ้ง โดยกำหนดมาตรฐานเฉพาะสำหรับผู้ให้บริการ และมีมาตรการจัดเก็บข้อมูลภายในประเทศ (Data Localization) สำหรับระบบที่มีความสำคัญสูง เพื่อสร้างความมั่นใจในอธิปไตยดิจิทัลและความปลอดภัยของข้อมูล

แนวคิดเกี่ยวกับการพัฒนาเศรษฐกิจดิจิทัล

1. สถานการณ์ปัจจุบันของเศรษฐกิจดิจิทัลไทย เศรษฐกิจดิจิทัลของประเทศไทยกำลังเติบโตอย่างก้าวกระโดด โดยมีการขยายตัวอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา ตามข้อมูลล่าสุดจากกระทรวงเศรษฐกิจดิจิทัลและสังคม เศรษฐกิจดิจิทัลของไทยในปี พ.ศ. 2567 คาดว่าจะเติบโต 5.7% ซึ่งเป็นการเติบโตที่สูงกว่า GDP โดยรวมของประเทศถึงสองเท่า โดย GDP ดิจิทัลโดยรวมในปี 2567 คาดว่าจะอยู่ที่ 4.44 ล้านล้านบาท (The Nation Thailand, 2025) ขนาดของเศรษฐกิจดิจิทัลไทยในปี 2566 มีมูลค่าประมาณ 6% ของ GDP แห่งชาติ หรือคิดเป็นมูลค่า 36 พันล้านดอลลาร์สหรัฐ และคาดการณ์ว่าจะเติบโตไปถึง 11% ของ GDP ในปี พ.ศ. 2570 การเติบโตนี้เกิดจากการนำเทคโนโลยีดิจิทัลมาใช้อย่างรวดเร็วในทั้งภาครัฐและเอกชน โดยได้รับการสนับสนุนจากนโยบายของรัฐบาลที่มุ่งให้ประเทศไทยเป็นศูนย์กลางเทคโนโลยีสารสนเทศและการสื่อสารของภูมิภาค (U.S. Department of Commerce, 2024)

2. ภาคอุตสาหกรรมที่เติบโต อุตสาหกรรมที่มีการเติบโตสูงสุดในเศรษฐกิจดิจิทัลไทย คือ อุตสาหกรรมเนื้อหาดิจิทัลที่เติบโต 12.6% และอุตสาหกรรมโทรคมนาคมที่เติบโต 10% โดยประมาณ 80% ของการเติบโตของ GDP ดิจิทัลมาจากการขยายตัวของอุตสาหกรรมโทรคมนาคม (Bangkok Post, 2024) การค้าอิเล็กทรอนิกส์ของไทยก็กำลังเติบโตอย่างแข็งแกร่ง โดยเป็นตลาดที่ใหญ่เป็นอันดับสองในอาเซียน และคาดการณ์ว่าจะขยายตัวต่อเนื่องประมาณ 20% ต่อปีในช่วงห้าปีข้างหน้า ในด้านการส่งออกสินค้าและบริการดิจิทัลคาดว่าจะเติบโต 17.2% ในปี 2567 ซึ่งสูงกว่าอัตราการเติบโตของการส่งออกโดยรวมที่ 6.1% ถึง 2.8 เท่า สะท้อนให้เห็นถึงศักยภาพของอุตสาหกรรมดิจิทัลในการสร้างรายได้จากต่างประเทศ (The Nation Thailand, 2024) การเติบโตนี้ได้รับการสนับสนุนจากการลงทุนของภาคเอกชนที่เพิ่มขึ้น 10.3% และโครงการรัฐบาลคลาวด์ที่คาดว่าจะกระตุ้นความต้องการในบริการคลาวด์ ศูนย์ข้อมูล และเทคโนโลยีปัญญาประดิษฐ์

3. เป้าหมายและวิสัยทัศน์ระยะยาว รัฐบาลไทยได้กำหนดเป้าหมายให้เศรษฐกิจดิจิทัลมีส่วนร่วมใน GDP ของประเทศถึง 30% ภายในปี 2570 หากแนวโน้มการเติบโต

ในปัจจุบันยังคงดำเนินต่อไป (The Nation Thailand, 2025) ภายใต้ยุทธศาสตร์ Thailand 4.0 รัฐบาลไทยมีวิสัยทัศน์ให้ประเทศไทยเป็นศูนย์กลางดิจิทัลของอาเซียน โดยตามข้อมูลของสำนักงานคณะกรรมการกิจการกระจายเสียงและแพร่ภาพทางโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) การใช้งานแอปพลิเคชันที่ใช้เทคโนโลยี 5G อย่างแพร่หลายอาจสร้างมูลค่าเพิ่มให้กับเศรษฐกิจไทยได้ 9.3 พันล้านดอลลาร์สหรัฐ หรือ 10% ของ GDP ภายในปี 2578

สรุปได้ว่า การพัฒนาเศรษฐกิจดิจิทัลยังได้รับการสนับสนุนจากการพัฒนาโครงสร้างพื้นฐานดิจิทัล โดยเฉพาะเครือข่าย 5G ที่ครอบคลุมประชากรไทยเกือบ 90% ในปลายปี 2566 และคาดการณ์ว่าการใช้ข้อมูลต่อการสมัครสมาชิกจะเพิ่มขึ้นจาก 32.7 GB ต่อเดือนในปี 2565 เป็นเกือบ 80 GB ต่อเดือนในปี 2568

ผลกระทบของนโยบายความปลอดภัยไซเบอร์ต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ

1. ผลกระทบเชิงบวก

นโยบายความปลอดภัยไซเบอร์ที่มีประสิทธิภาพส่งผลกระทบเชิงบวกต่อการพัฒนาเศรษฐกิจดิจิทัลในหลายมิติ โดยเฉพาะการสร้างความเชื่อมั่นให้กับผู้ลงทุนและผู้บริโภคในการใช้บริการดิจิทัล ตลาดความปลอดภัยไซเบอร์ของไทยเองก็กำลังเติบโตอย่างแข็งแกร่ง โดยคาดการณ์ว่าจะมีมูลค่า 508.89 ล้านดอลลาร์สหรัฐในปี 2568 และเติบโตด้วยอัตรา CAGR 14.10% เพื่อไปถึงมูลค่า 984.12 ล้านดอลลาร์สหรัฐภายในปี 2573 (Mordor Intelligence, 2024) การเติบโตของตลาดความปลอดภัยไซเบอร์นี้เป็นผลมาจากความต้องการที่เพิ่มขึ้นของการใช้โซลูชันความปลอดภัยต่างๆ รวมถึงความปลอดภัยคลาวด์ ความปลอดภัยข้อมูล ความปลอดภัยเครือข่าย และการป้องกันโครงสร้างพื้นฐาน และการที่รัฐบาลเน้นการพัฒนากรอบการทำงานเพื่อให้เศรษฐกิจดิจิทัลของไทยมีความยืดหยุ่นต่อภัยไซเบอร์ได้กระตุ้นให้องค์กรต่างๆ ลงทุนในโซลูชันความปลอดภัยขั้นสูงมากขึ้น

1.1 การพัฒนาความปลอดภัยในภาคการเงิน ภาคการเงินซึ่งเป็นเป้าหมายหลักของภัยคุกคามไซเบอร์ ได้แสดงให้เห็นถึงการปรับตัวเชิงรุกในด้านความปลอดภัยไซเบอร์ การที่ภาคการเงินจัดการข้อมูลลูกค้าจำนวนมหาศาลและได้พัฒนาโซลูชันนวัตกรรมที่มีผลกระเพื่อมต่ออุตสาหกรรมอื่นๆ แสดงให้เห็นถึงความมุ่งมั่นในการรักษาความปลอดภัยออนไลน์ (Tech Collective, 2024)

1.2 การกระตุ้นนวัตกรรมและการลงทุน นโยบายความปลอดภัยไซเบอร์ได้กระตุ้นให้เกิดการพัฒนานวัตกรรมใหม่ๆ โดยเฉพาะการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในระบบความปลอดภัยไซเบอร์ AI กำลังปฏิวัติตลาดความปลอดภัยไซเบอร์ด้วย

คุณสมบัติการตรวจจับการบุกรุกที่สามารถระบุและตอบสนองภัยคุกคามได้ทันที พร้อมด้วยเครื่องมือการเรียนรู้ของเครื่องที่สามารถค้นพบภัยคุกคามที่ซ่อนอยู่ได้ การใช้โครงสร้างความปลอดภัยแบบ Zero-trust ก็เป็นอีกหนึ่งนวัตกรรมที่ได้รับความนิยมเพิ่มขึ้น โดยเป็นกรอบความปลอดภัยที่ผู้ใช้ต้องได้รับการอนุญาตและการรับรองความถูกต้องก่อนเข้าถึงข้อมูลที่เป็นความลับ สถาปัตยกรรมนี้ทำการตรวจสอบผู้ใช้อย่างต่อเนื่องและจำกัดความเสียหายที่เกิดจากการบุกรุกจากภายนอก (Tech Collective, 2024) การลงทุนขนาดใหญ่ในโครงสร้างพื้นฐานดิจิทัลและความปลอดภัยไซเบอร์ก็เป็นอีกหนึ่งผลกระทบเชิงบวก โดยรัฐบาลได้รับการสนับสนุนให้บริษัทข้ามชาติสองแห่งลงทุนใน AI และศูนย์ข้อมูลในไทยต้นปี 2568 ด้วยมูลค่าการลงทุนรวมประมาณ 100 พันล้านบาท (The Nation Thailand, 2025)

1.3 การสร้างความเชื่อมั่นและการยอมรับในตลาด นโยบายความปลอดภัยไซเบอร์ที่มีประสิทธิภาพช่วยสร้างความเชื่อมั่นให้กับผู้บริโภคในการใช้บริการดิจิทัล และการที่ประเทศไทยมีกรอบกฎหมายและมาตรฐานความปลอดภัยที่ชัดเจนช่วยเพิ่มความน่าเชื่อถือในสายตาของนักลงทุนต่างชาติ ซึ่งเป็นปัจจัยสำคัญในการดึงดูดการลงทุนด้านเทคโนโลยีและนวัตกรรม การเติบโตของการใช้บริการดิจิทัลในกลุ่มผู้บริโภคไทยก็เป็นอีกหนึ่งผลกระทบเชิงบวก โดยการบริโภคดิจิทัลของภาคเอกชนเติบโต 5.6% ซึ่งสูงกว่าอัตราการเติบโตของการบริโภคโดยรวมที่ 4.8% (The Nation Thailand, 2025) สิ่งนี้แสดงให้เห็นว่าผู้บริโภคมีความเชื่อมั่นเพิ่มขึ้นในการใช้บริการดิจิทัลเมื่อมีระบบความปลอดภัยที่เหมาะสม

2. ผลกระทบเชิงลบ

2.1 ภาระต้นทุนต่อธุรกิจขนาดเล็กและกลาง การบังคับใช้กฎระเบียบความปลอดภัยไซเบอร์ที่เข้มงวดอาจสร้างอุปสรรคต่อสตาร์ทอัพและบริษัทขนาดเล็กที่มีทรัพยากรจำกัดในการปฏิบัติตามข้อกำหนดที่ซับซ้อน ค่าใช้จ่ายในการปฏิบัติตามกฎระเบียบ (Compliance Cost) รวมถึงการจ้างผู้เชี่ยวชาญ การลงทุนในระบบรักษาความปลอดภัยและการตรวจสอบอย่างสม่ำเสมอ อาจส่งผลกระทบต่อความสามารถในการแข่งขันของธุรกิจขนาดเล็กและกลาง โดยเฉพาะผู้ประกอบการรายใหม่ที่ยังไม่มีฐานรายได้ที่มั่นคง

2.2 ข้อกำหนด Data Localization และอุปสรรคต่อการลงทุน ข้อกำหนดเรื่องการจัดเก็บข้อมูลในประเทศ (Data Localization) สำหรับระบบสารสนเทศที่มีผลกระทบสูงอาจเป็นอุปสรรคต่อการลงทุนจากต่างประเทศ (Digital Policy Alert, 2024) การบังคับให้ข้อมูลบางประเภทต้องจัดเก็บภายในประเทศอาจส่งผลให้ ต้นทุนการดำเนินงานของบริษัทที่ต้องการใช้บริการคลาวด์จากผู้ให้บริการต่างประเทศเพิ่มสูงขึ้น บริษัทต่างชาติ

อาจลดความสนใจในการลงทุนเนื่องจากข้อจำกัดในการจัดการข้อมูลแบบรวมศูนย์ การเข้าถึงเทคโนโลยีและบริการคลาวด์ที่ทันสมัยอาจถูกจำกัด

2.3 ผลกระทบต่อนวัตกรรมและความคล่องตัว กฎระเบียบที่เข้มงวดเกินไปอาจชะลอการทดลองและพัฒนานวัตกรรมใหม่ ๆ โดยเฉพาะในกลุ่มเทคโนโลยีที่เกิดใหม่ เช่น Blockchain, AI, และ IoT ซึ่งต้องการความยืดหยุ่นในการทดลองและปรับเปลี่ยน ผู้ประกอบการอาจต้องใช้เวลาและทรัพยากรมากในการทำความเข้าใจและปฏิบัติตามกฎระเบียบ แทนที่จะโฟกัสไปที่การพัฒนาผลิตภัณฑ์และบริการ

สรุปได้ว่า นโยบายความปลอดภัยไซเบอร์มีผลกระทบต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศทั้งในเชิงบวกและเชิงลบ ในขณะที่นโยบายดังกล่าวช่วยสร้างความเชื่อมั่น กระตุ้นการลงทุน และส่งเสริมนวัตกรรม แต่ก็อาจสร้างภาระต้นทุนและอุปสรรคต่อธุรกิจขนาดเล็กและการลงทุนจากต่างประเทศ การออกแบบนโยบายควรมีความสมดุลระหว่างการรักษาความปลอดภัยกับการส่งเสริมนวัตกรรมและการแข่งขัน โดยคำนึงถึงความสามารถในการปฏิบัติตามของธุรกิจทุกขนาด และควรมีมาตรการสนับสนุนเพื่อช่วยเหลือธุรกิจขนาดเล็กในการปรับตัว รวมทั้งการพัฒนากำลังคนด้านความปลอดภัยไซเบอร์เพื่อรองรับการเติบโตของตลาดในอนาคต

แนวทางนโยบายความปลอดภัยไซเบอร์ต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ

1. การสร้างสมดุลระหว่างความปลอดภัยและนวัตกรรม แนวทางที่สำคัญในการพัฒนานโยบายความปลอดภัยไซเบอร์คือการสร้างสมดุลระหว่างการรักษาความปลอดภัยและการส่งเสริมนวัตกรรม นโยบายควรมีความยืดหยุ่นเพียงพอที่จะรองรับเทคโนโลยีใหม่ๆ ที่เกิดขึ้น โดยไม่สร้างอุปสรรคต่อการพัฒนาและการแข่งขัน การใช้แนวคิด Regulatory Sandbox หรือกระบะทรายทางกฎหมายอาจเป็นทางออกที่ดี โดยอนุญาตให้บริษัทเทคโนโลยีทดลองใช้นวัตกรรมใหม่ภายใต้การควบคุมที่ผ่อนคลายเป็นการชั่วคราว การพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์เป็นอีกหนึ่งแนวทางสำคัญ ปัจจุบันความต้องการบุคลากรด้านดิจิทัลอยู่ที่ประมาณ 100,000 คนต่อปี ในขณะที่อุปทานปัจจุบันอยู่ที่ 30,000 คนเท่านั้น (The Nation Thailand, 2025) การลงทุนในการศึกษาและการฝึกอบรมจึงเป็นสิ่งจำเป็นเพื่อสร้างกำลังคนที่มีคุณภาพในการรองรับการเติบโตของเศรษฐกิจดิจิทัล

2. การส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชน ความร่วมมือระหว่างภาครัฐและเอกชนเป็นกุญแจสำคัญในการสร้างระบบความปลอดภัยไซเบอร์ที่มีประสิทธิภาพ รัฐบาลควรทำงานร่วมกับภาคเอกชนในการพัฒนามาตรฐานและแนวปฏิบัติที่ดี โดยการแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามและการสร้างกลไกการตอบสนองร่วมกัน การสร้างระบบแจ้งเตือนและการแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์แบบเรียลไทม์จะช่วยเพิ่ม

ประสิทธิภาพในการป้องกันและตอบสนองภัยคุกคาม การจัดตั้งศูนย์ปฏิบัติการความปลอดภัยไซเบอร์ร่วมระหว่างหน่วยงานต่างๆ อาจเป็นแนวทางที่มีประสิทธิภาพ

3. การพัฒนามาตรฐานสากลและการรับรองระหว่างประเทศ การพัฒนามาตรฐานความปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานสากลจะช่วยเพิ่มความน่าเชื่อถือและอำนวยความสะดวกในการค้าระหว่างประเทศ การทำงานร่วมกับองค์กรระหว่างประเทศและการมีส่วนร่วมในกรอบความร่วมมือระดับภูมิภาค เช่น ASEAN Cybersecurity Framework จะช่วยเสริมสร้างความแข็งแกร่งของระบบความปลอดภัยไซเบอร์ การพัฒนาความสามารถในการรับรองและการตรวจสอบมาตรฐานความปลอดภัยไซเบอร์ในประเทศจะช่วยลดต้นทุนและเพิ่มความสะดวกในการปฏิบัติตามกฎระเบียบสำหรับธุรกิจ นอกจากนี้ การสร้างกลไกการยอมรับร่วมกันในมาตรฐานความปลอดภัยไซเบอร์ระหว่างประเทศจะช่วยส่งเสริมการค้าและการลงทุนข้ามชาติ

4. การส่งเสริมนวัตกรรมเพื่อความปลอดภัยไซเบอร์ รัฐบาลควรส่งเสริมการวิจัยและพัฒนานวัตกรรมด้านความปลอดภัยไซเบอร์ โดยการให้การสนับสนุนทางการเงินและการสร้างแรงจูงใจสำหรับบริษัทที่พัฒนาเทคโนโลยีความปลอดภัยไซเบอร์ การจัดตั้งกองทุนนวัตกรรมความปลอดภัยไซเบอร์หรือการให้สิทธิประโยชน์ทางภาษีสำหรับการลงทุนในด้านนี้อาจเป็นมาตรการที่มีประสิทธิภาพ การส่งเสริมให้เกิดระบบนิเวศนวัตกรรมด้านความปลอดภัยไซเบอร์ รวมถึงการสนับสนุนสตาร์ทอัพและบริษัทเทคโนโลยีขนาดเล็กในการพัฒนาโซลูชันความปลอดภัยไซเบอร์ที่สร้างสรรค์ จะช่วยสร้างความแข็งแกร่งให้กับอุตสาหกรรมและเศรษฐกิจโดยรวม

องค์ความรู้ใหม่

เป้าหมายหลัก เศรษฐกิจดิจิทัลที่มั่นคงปลอดภัย การสร้างสภาพแวดล้อมทางเศรษฐกิจดิจิทัลที่มีความน่าเชื่อถือ มั่นคง และปลอดภัยจากการโจมตีทางไซเบอร์ ซึ่งเป็นรากฐานสำคัญในการพัฒนาประเทศในยุคปัจจุบัน

ยุทธศาสตร์ที่ 1 สร้างสมดุล ความปลอดภัยและนวัตกรรม แนวทางนี้เน้นการหาจุดลงตัวระหว่างการป้องกันความเสี่ยงกับการส่งเสริมให้เกิดการพัฒนาสิ่งใหม่ ๆ ไม่ให้กฎระเบียบด้านความปลอดภัยเข้มงวดจนกลายเป็นอุปสรรคต่อการเติบโต ดังนี้

1. นโยบายยืดหยุ่น รองรับเทคโนโลยีใหม่ ภาครัฐต้องมีนโยบายที่ไม่ตายตัว ปรับเปลี่ยนได้ทันตามเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

2. เปิดพื้นที่หรือโครงการทดลอง (Sandbox) ให้ธุรกิจสามารถทดสอบนวัตกรรมใหม่ ๆ ในสภาพแวดล้อมที่จำกัดภายใต้การดูแลของหน่วยงานกำกับดูแล เพื่อเรียนรู้ความเสี่ยงและผลกระทบก่อนนำไปใช้จริงในวงกว้าง

3. พัฒนาบุคลากรดิจิทัล (ลดช่องว่างอุปสงค์/อุปทาน) แก้ปัญหาการขาดแคลนแรงงานด้านดิจิทัล โดยภาพกราฟแสดงให้เห็นชัดเจนว่ามีความต้องการบุคลากรสูงถึง 100k (แสนคน) แต่มีกำลังคนเพียง 30k (สามหมื่นคน) จึงจำเป็นต้องเร่งผลิตและพัฒนาคนให้ทันต่อความต้องการ

ยุทธศาสตร์ที่ 2 ความร่วมมือภาครัฐและภาคเอกชน เน้นการทำงานร่วมกันอย่างใกล้ชิดระหว่างหน่วยงานของรัฐและภาคธุรกิจ เพราะภัยคุกคามไซเบอร์ส่งผลกระทบต่อทั้งสองภาคส่วน ดังนี้

1. แบ่งปันข้อมูลภัยคุกคาม Real-time สร้างกลไกการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในทันที เพื่อให้ทุกฝ่ายเตรียมรับมือได้ทันท่วงที

2. พัฒนามาตรฐานและแนวปฏิบัติร่วมกัน รัฐและเอกชนควรร่วมมือกำหนดกฎเกณฑ์และวิธีการทำงานด้านความปลอดภัยให้เป็นไปในทิศทางเดียวกัน เพื่อให้เกิดประสิทธิภาพสูงสุด

3. ศูนย์ปฏิบัติการความปลอดภัยร่วม จัดตั้งศูนย์กลางในการเฝ้าระวัง ป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ที่ทำงานร่วมกันระหว่างหน่วยงานต่าง ๆ

ยุทธศาสตร์ที่ 3 มาตรฐานสากลและการรับรอง มุ่งเน้นการยกระดับความปลอดภัยของไทยให้ทัดเทียมกับนานาประเทศ เพื่อสร้างความเชื่อมั่นในเวทีโลก ดังนี้

1. สอดคล้องมาตรฐานโลก (เพิ่มความน่าเชื่อถือ) นำมาตรฐานความปลอดภัยไซเบอร์ที่เป็นที่ยอมรับในระดับสากล (เช่น ISO) มาปรับใช้ เพื่อสร้างความมั่นใจให้กับนักลงทุนและคู่ค้าต่างชาติ

2. ร่วมมือระดับภูมิภาคอาเซียน ทำงานร่วมกับประเทศเพื่อนบ้านในกลุ่มอาเซียนภายใต้กรอบความร่วมมือเดียวกัน เพื่อสร้างความเข้มแข็งในระดับภูมิภาค

3. กลไกการยอมรับร่วมกัน (ส่งเสริมการค้า) สร้างระบบที่ทำให้การรับรองมาตรฐานความปลอดภัยของไทยเป็นที่ยอมรับในต่างประเทศ ซึ่งจะช่วยอำนวยความสะดวกและส่งเสริมการค้าระหว่างประเทศ

ยุทธศาสตร์ที่ 4 ส่งเสริมนวัตกรรมความปลอดภัย สนับสนุนให้เกิดการคิดค้นและพัฒนาเทคโนโลยีด้านความปลอดภัยไซเบอร์ขึ้นใช้เองภายในประเทศ ไม่พึ่งพาแต่การนำเข้า ดังนี้

1. สนับสนุนทางการเงิน & กองทุน R&D ภาครัฐจัดสรรงบประมาณหรือตั้งกองทุนเพื่อสนับสนุนการวิจัยและพัฒนา (Research & Development) ด้านเทคโนโลยีความปลอดภัย

2. สิทธิประโยชน์ทางภาษี ให้แรงจูงใจทางภาษีแก่บริษัทที่มีการลงทุนหรือพัฒนานวัตกรรมด้านความปลอดภัยไซเบอร์

3. สร้างระบบนิเวศสตาร์ทอัพ สร้างสภาพแวดล้อมที่เอื้อต่อการเติบโตของธุรกิจสตาร์ทอัพ (Startup) ด้านความปลอดภัยไซเบอร์ เพื่อให้เกิดผู้เล่นหน้าใหม่และนวัตกรรมใหม่ ๆ ในตลาด

ดังนั้น การจะพัฒนาเศรษฐกิจดิจิทัลให้มั่นคงปลอดภัยนั้น ไม่สามารถทำได้ด้วยการออกกฎบังคับเพียงอย่างเดียว แต่ต้องอาศัยความสมดุลระหว่างความปลอดภัยกับนวัตกรรม ความร่วมมือที่เข้มแข็งของรัฐและเอกชน การยึดตามมาตรฐานสากลและการส่งเสริมให้เกิดการสร้างสรรค์เทคโนโลยีป้องกันขึ้นเองภายในประเทศ

ภาพที่ 1 องค์ความรู้ใหม่

สรุป

การศึกษาเรื่องผลกระทบของนโยบายความปลอดภัยไซเบอร์ต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศไทยนี้ได้ให้ข้อมูลเชิงลึกที่มีประโยชน์หลายประการ ผลการศึกษาพบว่านโยบายความปลอดภัยไซเบอร์ที่ออกแบบและดำเนินการอย่างเหมาะสมสามารถเป็นตัวขับเคลื่อนการเติบโตของเศรษฐกิจดิจิทัลได้อย่างมีนัยสำคัญ

ผลกระทบเชิงบวกหลัก ที่พบจากการศึกษารวมถึงการสร้างความเชื่อมั่นให้กับผู้บริโภคและนักลงทุน การกระตุ้นการพัฒนานวัตกรรมและเทคโนโลยีใหม่ และการเพิ่มขึ้นของการลงทุนในภาคเทคโนโลยี ตลาดความปลอดภัยไซเบอร์ของไทยเองก็กำลังเติบโตอย่างแข็งแกร่ง โดยคาดการณ์ว่าจะเติบโตด้วยอัตรา CAGR 14.10% และมีมูลค่าเกือบ 1 พันล้านดอลลาร์สหรัฐภายในปี 2573 และความท้าทายที่สำคัญ ได้แก่ การสร้างสมดุล

ระหว่างการรักษาความปลอดภัยกับการไม่สร้างอุปสรรคต่อนวัตกรรม การจัดการต้นทุนการปฏิบัติตามกฎระเบียบสำหรับธุรกิจขนาดเล็กและกลาง และการพัฒนาบุคลากรที่มีความเชี่ยวชาญเพียงพอเพื่อรองรับการเติบโตของอุตสาหกรรม

แนวทางนโยบายที่แนะนำ ประกอบด้วยการสร้างความร่วมมือระหว่างภาครัฐและเอกชน การพัฒนามาตรฐานสากลและการรับรองระหว่างประเทศ การส่งเสริมการวิจัยและพัฒนานวัตกรรม และการลงทุนในการพัฒนาบุคลากร การใช้แนวคิด Regulatory Sandbox อาจเป็นเครื่องมือที่มีประสิทธิภาพในการทดลองนโยบายและมาตรการใหม่และข้อเสนอแนะสำหรับอนาคต รวมถึงการพัฒนาระบบการติดตามและประเมินผลกระทบของนโยบายอย่างต่อเนื่อง การสร้างกลไกการแบ่งปันข้อมูลและการประสานงานระหว่างหน่วยงาน และการเตรียมพร้อมสำหรับเทคโนโลยีอุบัติใหม่ที่อาจส่งผลกระทบต่อภูมิทัศน์ความปลอดภัยไซเบอร์ การศึกษานี้แสดงให้เห็นว่า ความปลอดภัยไซเบอร์และการพัฒนาเศรษฐกิจดิจิทัลไม่ใช่เป้าหมายที่ขัดแย้งกัน แต่สามารถสร้างผลประโยชน์ร่วมกันได้เมื่อมีการกำหนดนโยบายที่เหมาะสมและมีการดำเนินการอย่างมีประสิทธิภาพ ความสำเร็จในการสร้างสมดุลนี้จะเป็นปัจจัยสำคัญในการทำให้ประเทศไทยสามารถบรรลุเป้าหมายในการเป็นศูนย์กลางดิจิทัลของภูมิภาคได้อย่างยั่งยืน

เอกสารอ้างอิง

Asia Law Portal. (2019). *Cybersecurity Law: Thailand*. Retrieved August 20, 2025, from https://shorturl.asia/7xHFY

Bangkok Post. (2024). *Ministry eyes digital GDP growth of 5.7%*. Retrieved August 20, 2025, from https://shorturl.asia/fKqZw

Digital Policy Alert. (2024). *Thailand implemented NCSC standards for the maintenance of cybersecurity in cloud computing systems B.E. 2566 (2023) including data localisation requirements*. Retrieved August 25, 2025, from https://digitalpolicyalert.org/change/11180

Mordor Intelligence. (2024). *Thailand Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)*. Retrieved August 20, 2025, from https://shorturl.asia/yAjdq

Nishimura & Asahi. (2019). *Thailand's cybersecurity act finally comes into force*. Retrieved August 20, 2025, from https://shorturl.asia/tQKu1

Tech Collective. (2024). *Cybersecurity trends and its impact on the Thailand economy*. Retrieved August 20, 2025, from https://shorturl.asia/6YlTU

The Nation Thailand. (2024). *Thailand's digital economy expands 5.7% in 2024*. Retrieved August 20, 2025, from https://shorturl.asia/EC9xk

_____. (2025). *Thailand's digital economy booms amid surge in foreign investment*. Retrieved August 20, 2025, from https://shorturl.asia/dyMwL

Tilleke & Gibbins. (2024). Thailand Lays Out New Cybersecurity Standards. Retrieved August 20, 2025, from https://shorturl.asia/43MQR

U.S. Department of Commerce. (2024). *Thailand – Digital economy. U.S. Trade Administration*. Retrieved August 20, 2025, from https://shorturl.asia/cFw34