# รายงานการศึกษาส่วนบุคคล
# (Individual Study)

# เรื่อง แนวทางพัฒนาการดำเนินนโยบาย การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย


จัดทำโดย นางสาวกัลยา ชินาธิวร

รหัส 93077



รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 93

วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ประจำปี 2564

# รายงานการศึกษาส่วนบุคคล
# (Individual Study)

**เรื่อง แนวทางพัฒนาการดำเนินนโยบาย**
**การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย**

**จัดทำโดย นางสาวกัลยา ชินาธิวร**
**รหัส 93077**

**หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 93**
**วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.**
**ประจำปี 2564**
**รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา**

**สำนักงาน ก.พ.**

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม ของสำนักงาน ก.พ.

นายอารักษ์ พรหมณี
อาจารย์ที่ปรึกษา

นายจุฬา สุขมานพ
อาจารย์ที่ปรึกษา

รศ.ดร. อักษรศรี พานิชสาส์น
อาจารย์ที่ปรึกษา

# บทสรุปสำหรับผู้บริหาร

ปัจจุบันทุกประเทศกำลังก้าวเข้าสู่ยุคดิจิทัล และผลักดันนโนยายเศรษฐกิจดิจิทัลด้วยการส่งเสริมให้มีการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัล และนวัตกรรมในทุกภาคส่วน ทั้งภาครัฐ ภาคอุตสาหกรรม ภาคเอกชน และประชาชน ซึ่งเทคโนโลยีดิจิทัลที่มีการใช้งานมากที่สุด คือการใช้อินเทอร์เน็ต จนอาจกล่าวได้ว่า ชีวิตในสังคมสารสนเทศทุกวันนี้เราทุกคนเกี่ยวข้องกับอินเทอร์เน็ตในทางใดทางหนึ่ง แม้จะไม่ใช่ “ผู้ใช้อินเทอร์เน็ต” โดยตรงก็ตาม

ในขณะที่อินเทอร์เน็ตจะนำมาซึ่งโอกาสในการขับเคลื่อนไปสู่เศรษฐกิจดิจิทัล ไม่ว่าจะเป็นการส่งเสริมการเรียนรู้ การศึกษา การสร้างธุรกิจใหม่ การส่งเสริมด้านสุขภาพ และการขนส่งคมนาคม แล้วอินเทอร์เน็ตยังถูกใช้เป็นเครื่องมือในการก่อให้เกิดภัยคุกคามและอาชญากรรมทางไซเบอร์ ซึ่งเป็นภัยคุกคามที่ไร้พรหมแดน ทั้งยังทวีความรุนแรงและซับซ้อน และมีผลกระทบในทุกมิติ ทั้งด้านเศรษฐกิจ สังคม และความมั่นคงของประเทศ สอดคล้องกับรายงานของ World Economic Forum ซึ่งได้จัดอันดับ 10 ความเสี่ยงระดับโลกที่เป็นอันตรายในปัจจุบัน ประจำปี ค.ศ. 2021 พบว่า ความล้มเหลวในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity failure) เป็นความเสี่ยงที่จัดอยู่ในอันดับที่ 4

รัฐบาลไทยได้ให้ความสำคัญในการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งตามยุทธศาสตร์ชาติ พ.ศ. 2561–2580 ภายใต้ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง ข้อ 4.2 การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง กำหนดให้มีการแก้ไขปัญหาเดิมที่มีอยู่อย่างตรงประเด็นจนหมดไปอย่างรวดเร็ว และป้องกันไม่ให้ปัญหาใหม่เกิดขึ้น ซึ่งรวมถึงปัญหาอาชญากรรมทางไซเบอร์ และการติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่ ซึ่งรวมถึง ภัยคุกคามทางไซเบอร์ นอกจากนี้ ประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ ได้ระบุถึงการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ ต่อเศรษฐกิจและสังคม และปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมตระหนักถึงการปรับปรุงเปลี่ยนแปลงโครงสร้างพื้นฐานสำคัญๆ ที่กำลังเกิดขึ้นตามนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัลและไทยแลนด์ 4.0 ของรัฐบาล ซึ่งเป็นการเปลี่ยนผ่านประเทศครั้งสำคัญ โดยจะละเลยไม่ได้กับภัยคุกคามทางไซเบอร์ต่างๆ ที่อาจฉุดรั้งการเปลี่ยนผ่านที่เกิดขึ้น และเมื่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 จึงได้มีการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งขณะนี้อยู่ในระหว่างการจัดตั้งองค์กรตามโครงสร้างและอัตรากำลัง โดยสำนักงานฯ จะเป็นหน่วยงานหลักในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ต่อไป

การศึกษานี้ดำเนินการวิเคราะห์ปัจจัยที่ทำให้ประเทศสิงคโปร์และมาเลเซียประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ช่วงปี ค.ศ. 2014 จนถึงปัจจุบัน แล้วนำผลการวิเคราะห์มาเปรียบเทียบกับการดำเนินงานของไทย เพื่อหาแนวทางและข้อเสนอแนะในการพัฒนาการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย โดยการศึกษาจะวิเคราะห์ตามกรอบดัชนีตัวชี้วัดตามที่สหภาพโทรคมนาคมระหว่างประเทศ (International

Telecommunication Union หรือ ITU) ซึ่งเป็นทบวงการชำนัญพิเศษภายใต้สหประชาชาติ ได้แบ่งเป็น 5 ด้าน ได้แก่ (1) ด้านกฎหมาย (2) ด้านเทคนิค (3) ด้านองค์กร (4) ด้านการเสริมสร้างศักยภาพ และ (5) ด้านความร่วมมือ ทั้งนี้ จากการศึกษาพบว่า ปัจจัยหลักที่ทำให้สิงคโปร์และมาเลเซียประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ คือรัฐบาลทั้งสองประเทศมีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วยการใช้เทคโนโลยีดิจิทัลและนวัตกรรม จึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีการดำเนินการอย่างจริงจัง ต่อเนื่องและเป็นระบบ ทั้งในด้านการออกกฎหมาย กฎระเบียบที่ครอบคลุมและเข้มงวด การส่งเสริมและสนับสนุนเงินงบประมาณจากภาครัฐในการจัดหาเทคโนโลยีชั้นสูงมารับมือกับอาชญากรรมไซเบอร์ รวมทั้งการให้ความสำคัญกับเรื่องมาตรฐานและการรับรองมาตรฐาน การมีแผนยุทธศาสตร์และการจัดตั้งองค์กรที่รับผิดชอบและการทำงานข้ามองค์อย่างครอบคลุมและเป็นระบบ การวางแผนยุทธศาสตร์และดำเนินนโยบายในการเสริมสร้างและพัฒนาศักยภาพบุคลากรทุกภาคส่วน รวมถึงการสร้างความตระหนักรู้แก่ประชาชน และการส่งเสริมความร่วมมือกับทุกภาคส่วนทั้งในประเทศและระหว่างประเทศ

จากการศึกษาวิเคราะห์ปัญหาหลักของประเทศไทย พบว่า เนื่องจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพิ่งมีผลบังคับใช้ และยังอยู่ในระหว่างการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามโครงสร้างที่กำหนด ซึ่งมีหน้าที่สำคัญในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ การจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงอาจทำให้การดำเนินนโยบายการรักษาความมั่นคงปลอดไซเบอร์ของไทยในปัจจุบันยังไม่เป็นรูปธรรม ซึ่งผู้เขียนได้เสนอแนวทางการแก้ไขปัญหาและพัฒนานโยบายในส่วนของประเทศไทยในแต่ละด้าน โดยใช้ข้อมูลจากการวิเคราะห์ปัจจัยความสำเร็จของสิงคโปร์และมาเลเซียในตัวชี้วัดทั้ง 5 ด้าน รวมทั้งข้อเสนอแนะในการพัฒนาจุดแข็งของไทย ได้แก่ 1) การกำหนดให้มีการทำงานไปในทิศทางเดียวกับกฎหมายอื่นที่เกี่ยวข้อง 2) การสนับสนุนเงินงบประมาณจากภาครัฐในการนำเทคโนโลยีที่ทันสมัยมาใช้เพื่อจัดการความเสี่ยงจากภัยคุกคามและอาชญากรรมทางไซเบอร์ 3) การศึกษา Best Practice ในการจัดตั้งองค์กรและรูปแบบการทำงานข้ามองค์กรของประเทศมาเลเซีย 4) การใช้ประโยชน์จากศูนย์ฝึกอบรมอาเซียน - ญี่ปุ่น อย่างเต็มศักยภาพ การพัฒนาหลักสูตรด้าน Cybersecurity ในสถาบันการศึกษา และการสร้างการตระหนักรู้แก่ประชาชน และ 5) ยกระดับความร่วมมือกับทุกภาคส่วนทั้งในประเทศและระหว่างประเทศ ทั้งนี้ เพื่อเป็นข้อมูลสำหรับเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้บริหารของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ใช้ประกอบการพิจารณาในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564 - 2568 ตามที่กำหนดไว้ในมาตรา 9 (1) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ต่อไป

# กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคลฉบับนี้ สำเร็จลงได้ด้วยความกรุณาของอาจารย์ที่ปรึกษาทั้ง 3 ท่าน ประกอบด้วย ท่านอารักษ์ พรหมณี ท่านจุฬา สุขมานพ และท่าน รศ.ดร. อักษรศรี พานิชสาส์น ที่ให้คำแนะนำและข้อคิดเห็นอันเป็นประโยชน์ในการปรับปรุงรายงานฉบับนี้ให้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบคุณท่านอัจฉรินทร์ พัฒนพันธ์ชัย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ให้โอกาสผู้เขียนรายงานฉบับนี้ได้เข้ารับการฝึกอบรมในหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม ของสำนักงาน ก.พ. และขอขอบคุณท่านวิทยากร เพื่อนร่วมรุ่นจากหน่วยราชการต่างๆ ตลอดจนเจ้าหน้าที่ทุกท่านจากสำนักงาน ก.พ. ที่ทำให้ผู้เขียนได้มีโอกาสเพิ่มพูนความรู้ ประสบการณ์และสร้างมิตรภาพ ตลอดระยะเวลาของการฝึกอบรมอันมีคุณค่าในครั้งนี้

สุดท้ายขอขอบคุณเจ้าหน้าที่กองการต่างประเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทุกท่านที่สนับสนุนข้อมูลและเป็นกำลังใจในการเข้าร่วมฝึกอบรมฯ และหวังว่ารายงานการศึกษาส่วนบุคคลฉบับนี้จะเป็นประโยชน์ต่องานราชการในการใช้เป็นข้อมูลอ้างอิงต่อไป

กัลยา ชินาธิวร

11 มิถุนายน 2564

# สารบัญ

# สารบัญตาราง

# สารบัญแผนภูมิ

# คำอธิบายคำศัพท์และคำย่อ

**“ดิจิทัล”** หมายความว่า เทคโนโลยีที่ใช้วิธีการนำสัญญลักษณ์ศูนย์และหนึ่งหรือสัญญลักษณ์อื่นมาทดแทนค่าสิ่งทั้งปวง เพื่อใช้สร้าง หรือก่อให้เกิดระบบต่างๆ เพื่อให้มนุษย์ใช้ประโยชน์

**“ดิจิทัลเพื่อเศรษฐกิจและสังคม”** หมายความว่า ระบบเศรษฐกิจและสังคมที่มีการติดต่อสื่อสาร การผลิต การอุปโภคบริโภค การใช้สอย การจำหน่ายจ่ายแจก การพาณิชย์อิเล็กทรอนิกส์ การทำธุรกรรมทางอิเล็กทรอนิกส์ การคมนาคมขนส่ง การโลจิสติกส์ การศึกษา การเกษตรกรรม การอุตสาหกรรม การสาธารณสุข การเงินการลงทุน การภาษีอากร การบริหารจัดการข้อมูล และเนื้อหาหรือกิจกรรมทางเศรษฐกิจและสังคมอื่นใด หรือการใดๆ ที่มีกระบวนการหรือการดำเนินงานทางดิจิทัลหรือทางอิเล็กทรอนิกส์ ทั้งในกิจการกระจายเสียง กิจการโทรทัศน์ กิจการวิทยุคมนาคม กิจการโทรคมนาคม กิจการสื่อสาร ดาวเทียม และการบริหารคลื่นความถี่ โดยอาศัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งเทคโนโลยีที่มีการหลอมรวมหรือเทคโนโลยีอื่นใดในทำนองเดียวกันหรือคล้ายคลึงกัน

**“อินเทอร์เน็ต”** หมายความว่า เครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ มีการเชื่อมต่อระหว่างเครือข่าย เครือข่ายทั่วโลก โดยใช้ภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โพร์โทคอล ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ในหลายๆ ทาง เช่น ไปรษณีย์อิเล็กทรอนิกส์ หรืออีเมล์ และสามารถสืบค้นข้อมูลและข่าวสารต่างๆ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้

**“ออนไลน์”** หมายความว่า ติดต่อสื่อสารกับคอมพิวเตอร์โดยตรง และพร้อมใช้งาน

**“แพลตฟอร์ม”** หมายความว่า สภาวะแวดล้อมที่ประกอบด้วยฮาร์ตแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ระบบหนึ่ง

**“ไซเบอร์”** หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

**“ภัยคุกคามทางไซเบอร์”** หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**“การรักษาความมั่นคงปลอดภัยไซเบอร์”** หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

**“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์”** หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่งคงปลอดภัยไซเบอร์ หรือ

ความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพวิเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

**“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”** หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

AI = Artificial Intelligence (ปัญญาประดิษฐ์)

CERT = Computer Emergency Response Team (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์)

CII = Critical Information Infrastructure (โครงสร้างพื้นฐานสำคัญทางสนสนเทศ)

CSA = Cyber Security Agency (หน่วยงานรักษาความมั่นคงปลอดภัยไซเบอร์)

GCI = Global Cybersecurity Index (ตัวชี้วัดระดับโลกว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์)

ITU = International Telecommunication Union (สหภาพโทรคมนาคมระหว่างประเทศ)

IoT = Internet of Things (อินเทอร์เน็ตทุกสรรพสิ่ง)

SMEs = Small and Medium Enterprises (วิสาหกิจขนาดกลางและขนาดย่อม)

## 1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

**(ข้อมูลส่วนบุคคลไม่เผยแพร่)**

## 2. ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

### 2.1 การกำหนดประเด็นการศึกษา

ปัจจุบันโลกกำลังเข้าสู่ยุคเปลี่ยนผ่านไปสู่เศรษฐกิจดิจิทัล ความก้าวหน้าทางเทคโนโลยีดิจิทัลและนวัตกรรมเป็นไปอย่างรวดเร็วและมีการใช้งานอย่างกว้างขว้าง ทั้งในชีวิตประจำวัน การให้บริการในทุกภาคส่วน และการดำเนินการ/ประกอบการธุรกิจ สำหรับประชาชนในทุกเพศทุกวัย จากรายงานของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU) ซึ่งเป็นทบวงการชำนัญพิเศษภายใต้สหประชาชาติ พบว่า ในปี 2562 จำนวนประชากรโลกร้อยละ 53 หรือคิดเป็นจำนวน 4.1 พันล้านคน มีการใช้งานอินเทอร์เน็ต ทั้งนี้ ITU ยังได้คาดการณ์ว่า ภายในปี 2566 จำนวนผู้ใช้งานอินเทอร์เน็ตจะเพิ่มเป็นร้อยละ 70 ของประชากรโลก สอดคล้องกับผลสำรวจของสำนักงานสถิติแห่งชาติ ปี 2563 พบว่าร้อยละ 77.8 ของประชาชนผู้มีอายุ 6 ปีขึ้นไปใช้งานอินเทอร์เน็ต เปรียบเทียบกับผลการสำรวจปี 2562 ซึ่งมีจำนวนร้อยละ 66.7 นอกจากนี้ จากผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทยปี 2563 โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ ยังพบว่าประเทศไทยขยับสู่สังคมดิจิทัลเต็มรูปแบบแล้ว เมื่อค่าเฉลี่ยการใช้งานอินเตอร์เน็ตคนไทยเพิ่มมากยิ่งขึ้น โดยผู้ตอบแบบสำรวจฯ ใช้อินเทอร์เน็ตเฉลี่ยวันละ 11 ชั่วโมง 25 นาที เมื่อเทียบกับผลสำรวจครั้งแรกในปี 2556 คนไทยใช้อินเทอร์เน็ตเฉลี่ยวันละ 4 ชั่วโมง 36 นาที เท่านั้น คิดเป็นอัตราการเติบโตเพิ่มขึ้นถึง 3 เท่าตัว

อย่างไรก็ดี ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ต มาพร้อมกับความท้าทายและภัยคุกคามทางไซเบอร์ซึ่งมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ข้อมูลที่ไม่เป็นจริง การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ การสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ และการโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ และปัจเจกบุคคล จากรายงานการศึกษาจัดทำโดย Microsoft ร่วมกับ Frost & Sullivan เรื่อง Understanding the Cybersecurity Threat Landscape in Asia Pacific : Securing the Modern Enterprise in Digital World พบว่า ในปี 2560 มีการโจมตีทางไซเบอร์ซึ่งก่อให้เกิดผลเสียหายทางเศรษฐกิจในภูมิภาคเอเชียและแปซิฟิกมากถึง 1.745 ล้านล้านเหรียญสหรัฐอเมริกา คิดเป็นมูลค่ามากกว่าร้อยละ 7 ของผลิตภัณฑ์มวลรวม (Gross Domestic Product: GDP) ในภูมิภาคฯ

ในส่วนของประเทศไทย จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย ปี 2563 รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต หรือ ThaiCERT) พบว่า ในปี 2563 มีการแจ้งเหตุภัยคุกคาม จำนวนรวม 1,474 เรื่อง โดยภัยคุกคามอันดับ 1 คือ โปรแกรมไม่พึงประสงค์ (Malicious code) จำนวน 531 เรื่อง คิดเป็นร้อยละ 38.7 ตามมาอันดับ 2 คือ การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) จำนวน 346 เรื่อง คิดเป็นร้อยละ 24.7 ดังนั้น การเฝ้าระวัง การป้องกันและรับมือกับภัยคุกคามจึงต้องอาศัยความรวดเร็ว ทันเหตุการณ์ เทคโนโลยีที่ทันสมัย และการทำงานที่มีระบบและมีประสิทธิภาพ เพราะมีผลกระทบต่อการขาดความเชื่อมั่นในการใช้งานเทคโนโลยีดิจิทัลในมิติต่างๆ รวมถึงความสูญเสียและความเสียหายที่จะเกิดขึ้น

จากสภาพปัญหาดังกล่าว ทั่วโลกต่างตระหนักถึงภัยคุกคามทางไซเบอร์ซึ่งทวีความรุนแรงขึ้นตามจำนวนผู้ใช้งานอินเทอร์เน็ต มีความซับซ้อน และมีผลกระทบในวงกว้างมากขึ้นทุกๆ ปี ทั้งยังควบคุมได้ยากเนื่องจากเป็นการสื่อสารไร้พรหมแดน ปัญหาของภัยคุกคามมีสาเหตุสำคัญมาจากการขาดระบบการบริหารจัดการเครือข่ายที่ดี ความไม่พร้อมของระบบเทคโนโลยี การขาดแคลนบุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีสื่อสารและด้านความมั่นคงปลอดภัยไซเบอร์ ทำให้แต่ละประเทศรวมทั้งสหประชาชาติและองค์การระหว่างประเทศต่างๆ ที่เกี่ยวข้องต่างหามาตรการและกำหนดแนวนโยบายในการสร้างความมั่นคงปลอดภัยไซเบอร์ รวมทั้งมีความร่วมมือในการป้องกันภัยคุกคามทางไซเบอร์ โดยสหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU ได้ทำการศึกษาและจัดทำดัชนีตัวชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) เพื่อวัดระดับความสามารถในการจัดการเรื่องดังกล่าวของประเทศสมาชิก ITU ทั้งหมด 193 ประเทศ รวมทั้งประเทศไทย และได้จัดทำแบบสอบถาม ส่งให้ประเทศสมาชิกตอบแบบสอบถาม และนำมาวิเคราะห์ร่วมกับข้อมูลอื่นๆ ประกอบ เพื่อจัดอันดับประเทศที่มีการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง ซึ่งเริ่มตั้งแต่ ปี ค.ศ. 2013 โดยรายงานฉบับล่าสุด เมื่อปี ค.ศ. 2018 พบว่า ในส่วนของกลุ่มประเทศสมาชิกอาเซียน ประเทศที่มีคะแนนสูงสุดและเป็นอันหนึ่งในอาเซียน คือ สาธารณรัฐสิงคโปร์ อันดับสอง คือ ประเทศมาเลเซีย และอันดับที่สาม คือ ประเทศไทย

ในส่วนของประเทศไทย รัฐบาลได้กำหนดนโยบายไทยแลนด์ 4.0 ซึ่งขับเคลื่อนเศรษฐกิจและสังคมด้วยนวัตกรรมและการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัลในทุกภาคส่วน โดยในส่วนของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีภารกิจในการขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคงในการป้องกันและแก้ไขปัญหาอาชกรรมและภัยคุกคามทางไซเบอร์ สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580) ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล ซึ่งมุ่งเน้นการมีกฎหมาย กฎระเบียบ กติกาและมาตรฐานที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมและทำธุรกรรมออนไลน์ต่างๆ รวมถึงสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัล

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมตระหนักถึงการปรับปรุงเปลี่ยนแปลงโครงสร้างพื้นฐานสำคัญๆ ที่กำลังเกิดขึ้นตามนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัลและไทยแลนด์ 4.0 ของรัฐบาล ซึ่งเป็นการเปลี่ยนผ่านประเทศครั้งสำคัญ อันหมายถึง การเคลื่อนย้ายจากสังคมหนึ่งไปอีกสังคมหนึ่งด้วยการเข้าถึงข้อมูลและการบริการต่างๆ ด้วยระบบดิจิทัลและนวัตกรรม โดยจะยิ่งละเลยไม่ได้กับภัยคุกคามไซเบอร์ต่างๆ ที่อาจฉุดรั้งการเปลี่ยนผ่านที่เกิดขึ้น กระทรวงฯ จึงได้ดำเนินการในการเสนอร่างกฎหมาย โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบภายในประเทศ

อย่างไรก็ดี เนื่องจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพิ่งมีผลบังคับใช้ และยังอยู่ในระหว่างการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งมีหน้าที่สำคัญในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคง

ปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ การจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงจำเป็นอย่างยิ่งที่ประเทศไทยจะต้องเร่งพัฒนาการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรุกอย่างจริงจัง รวมทั้งปรับปรุงแก้ไขประเด็นที่ต้องมีการพัฒนาอย่างทันท่วงที เพื่อป้องกันและสามารถรับมือกับภัยคุกคามและอาชญากรรมไซเบอร์ที่ทวีความรุนแรงและพัฒนารูปแบบอย่างรวดเร็ว ได้อย่างมีประสิทธิภาพและประสิทธิผล ตลอดจนสามารถป้องกันและลดผลกระทบความเสียหายจากภัยคุกคามดังกล่าว ผู้เขียนจึงเห็นควรศึกษาเรื่อง “แนวทางพัฒนาการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย” เพื่อเป็นข้อมูลสำหรับเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้บริหารกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ใช้ประกอบการพิจารณาในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564 - 2568 ตามที่กำหนดไว้ในมาตรา 9 (1) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

## 2.2 การกำหนดข้อเสนอเชิงนโยบาย

### 2.2.1 หลักการ แนวคิด ที่ใช้เป็นกรอบหรือแนวทางในการจัดทำข้อเสนอ

ในการศึกษาเพื่อจัดทำ “แนวทางการพัฒนาการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย” จะดำเนินการวิเคราะห์ปัจจัยที่ทำให้ประเทศสิงคโปร์และประเทศมาเลเซียประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ช่วงปี ค.ศ. 2014 จนถึงปัจจุบัน และวิเคราะห์ปัญหาในการดำเนินงานของไทย แล้วนำผลการวิเคราะห์มาเสนอเป็นข้อเสนอเชิงนโยบายเพื่อพัฒนาการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยจะวิเคราะห์ตามกรอบดัชนีตัวชี้วัดตามที่สหภาพโทรคมนาคมระหว่างประเทศจัดทำ ประกอบด้วย 5 ด้าน ดังนี้

1) **ด้านกฎหมาย** (legal measures) โดยวิเคราะห์จากกรอบกฎหมายที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

2) **ด้านเทคนิค** (technical measures) โดยวิเคราะห์จากกรอบงานทางเทคนิคที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

3) **ด้านองค์กร** (organizational measures) โดยวิเคราะห์จากสถาบัน องค์กรที่ประสานงานเชิงนโยบาย และวิเคราะห์จากยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ

4) **ด้านการเสริมสร้างศักยภาพ** (capacity building) โดยวิเคราะห์จากการศึกษาวิจัยและการพัฒนา (R & D) การฝึกอบรม การรับรองหน่วยงานภาครัฐและหน่วยงานระดับมืออาชีพที่ส่งเสริมการพัฒนาศักยภาพ

5) **ด้านความร่วมมือ** (cooperation) โดยวิเคราะห์จากหุ้นส่วนพันธมิตร กรอบความร่วมมือ และเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง

ทั้งนี้ ITU ได้กำหนดตัวชี้วัดย่อยรวมทั้งสิ้น 25 ตัว แบ่งตามน้ำหนักแต่ละตัวชี้วัด รายละเอียดปรากฏตามภาคผนวก 3

อย่างไรก็ดี เนื่องจากมีข้อจำกัดด้านระยะเวลาทำการศึกษา ผู้เขียนจะใช้ระเบียบวิธีศึกษาแบบพรรณาเชิงวิเคราะห์ (Descriptive Analysis) โดยการทบทวนและวิเคราะห์ข้อมูลวรรณกรรมที่เกี่ยวข้องกับขอบเขตการศึกษาในหัวข้อ ทั้งหนังสือ เว็บไซต์ พระราชบัญญัติ แผนนโยบายและยุทธศาสตร์ ข้อมูลสถิติ รายงาน และเอกสารวิชาการ ตลอดจนรวบรวมข้อมูลทุติยภูมิที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานที่เกี่ยวข้อง เช่น สหภาพโทรคมนาคมระหว่างประเทศ/ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์/ ThaiCERT/ Cyber Security Agency of Singapore/ InfoComm Media Development Authority (IMDA) ประเทศสิงคโปร์ และ Ministry of Communications and Information ประเทศมาเลเซีย

**2.2.2 การวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อประกอบการจัดทำข้อเสนอ**

จากการศึกษารายงาน Global Cybersecurity Index ปี ค.ศ. 2018 พบว่า อันดับประเทศที่มีการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ได้ผลสำเร็จสูงสุดในอาเซียน อันดับหนึ่งคือ สาธารณรัฐสิงคโปร์ โดยได้คะแนนจากตัวชี้วัดทั้ง 5 ตัว รวมเป็น 0.898 (จากจำนวนเต็ม 1) อันดับสอง คือ ประเทศมาเลเซีย ได้คะแนนรวม 0.893 และอันดับที่สาม คือ ประเทศไทย โดยได้คะแนนรวม 0.796 รายละเอียดปรากฏตามตารางที่ 1

ตารางที่ 1 ลำดับประเทศในอาเซียนในการดำเนินการทั้ง 5 ด้าน ตาม GCI ปี ค.ศ. 2018

| ประเทศ | คะแนน (เต็ม 1) | อันดับในอาเซียน | อันดับในภูมิภาคเอเชียและแปซิฟิก | อันดับในทั่วโลก |
|---|---|---|---|---|
| สิงคโปร์ | 0.898 | 1 | 1 | 6 |
| มาเลเซีย | 0.893 | 2 | 2 | 8 |
| ไทย | 0.796 | 3 | 7 | 35 |
| อินโดนีเซีย | 0.776 | 4 | 9 | 41 |
| เวียดนาม | 0.693 | 5 | 11 | 50 |
| ฟิลิปปินส์ | 0.643 | 6 | 12 | 58 |
| บรูไนดารุสซาลาม | 0.624 | 7 | 14 | 64 |
| สปป ลาว | 0.195 | 8 | 22 | 120 |
| เมียนมา | 0.172 | 9 | 26 | 128 |
| กัมพูชา | 0.161 | 10 | 27 | 131 |

ที่มา: ITU Global Cybersecurity Index (GCI) 2018

จากข้อมูลดังกล่าว อาจแบ่งความก้าวหน้าในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศในกลุ่มอาเซียนได้ 3 กลุ่ม ดังนี้

- กลุ่มที่มีความก้าวหน้าในระดับดีมาก จำนวน 2 ประเทศ ได้แก่ สิงคโปร์ และ มาเลเซีย
- กลุ่มที่มีความก้าวหน้าในระดับปานกลางถึงระดับดี จำนวน 5 ประเทศ ได้แก่ ไทย อินโดนีเซีย เวียดนาม ฟิลิปปินส์ และบรูไน ดารุสซาลาม
- กลุ่มที่ต้องการการพัฒนา จำนวน 3 ประเทศ ได้แก่ สปป ลาว เมียนมา และ กัมพูชา

**(1) การวิเคราะห์ปัจจัยที่ทำให้สิงคโปร์และมาเลเซียประสบความสำเร็จ**

จากรายงาน ITU Global Cybersecurity Index (GCI) 2018 ได้แสดงผลคะแนนในตัวชี้วัดแต่ละด้านของสิงคโปร์และมาเลเซีย ซึ่งได้อันดับที่ 1 และอันดับที่ 2 ของภูมิภาคเอเชียและแปซิฟิก ทั้งนี้ ในรายงานของ ITU เปิดเผยคะแนนในแต่ละด้านเฉพาะ 3 ประเทศแรกในแต่ละภูมิภาค ซึ่งในส่วนของภูมิภาคเอเชียและแปซิฟิก คือ ประเทศออสเตรเลีย ด้วยคะแนนรวม 0.890 ทำให้ขาดข้อมูลว่าประเทศไทยได้คะแนนในแต่ละด้านเท่าใด ผู้เขียนจึงได้สอบถามข้อมูลไปยัง ITU สำนักงานใหญ่ ณ นครเจนีวา สมาพันธรัฐสวิส และได้รับทราบผลคะแนนตัวชี้วัดของประเทศไทยในแต่ละด้าน รายละเอียดปรากฏตามตารางที่ 2

ตารางที่ 2 แสดงผลคะแนนในแต่ละด้านของสิงคโปร์ มาเลเซีย และ ไทย

| Member States | GCI Score | Legal | Technical | Organiza-tional | Capacity building | Coopera-tion |
|---|---|---|---|---|---|---|
| Singapore | 0.898 | 0.200 | 0.186 | 0.192 | 0.195 | 0.125 |
| Malaysia | 0.893 | 0.179 | 0.196 | 0.200 | 0.198 | 0.120 |
| Thailand* | 0.796 | 0.186 | 0.174 | 0.124 | 0.170 | 0.142 |

ที่มา: ITU Global Cybersecurity Index (GCI) 2018

จากตารางดังกล่าวพบว่า สิงคโปร์มีคะแนนรวมมากกว่ามาเลเซียเพียงเล็กน้อย และหากพิจารณาคะแนนในแต่ละตัวชี้วัดแต่ละด้าน พบว่า สิงคโปร์ได้คะแนนด้านกฎหมายเต็ม (0.200) อาจเนื่องจากรัฐบาลสิงคโปร์มีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนการพัฒนาเศรษฐกิจและสังคม จึงได้ให้ความสำคัญกับเรื่องการออกกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์มีการดำเนินการอย่างจริงจัง ต่อเนื่อง และเป็นระบบ เริ่มตั้งแต่ ปี ค.ศ. 2005 อย่างไรก็ดี ผลคะแนนของมาเลเซียมีคะแนนมากกว่าสิงคโปร์ถึง 3 ด้าน ได้แก่ ด้านเทคนิค ด้านองค์กร (คะแนนเต็ม 0.200) และด้านการเสริมสร้างศักยภาพ ซึ่งอาจกล่าวได้ว่า หากมาเลเซียมีการพัฒนาในด้านกฎหมายและการบังคับใช้กฎหมายที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มากขึ้น และยังคงรักษามาตรฐานในการดำเนินการด้านอื่นๆ รวมทั้งพัฒนาเพิ่มเติมในเรื่องความร่วมมือ มาเลเซียก็อาจสามารถขึ้นแซงหน้าสิงคโปร์ในอนาคตได้

ผลการวิเคราะห์ปัจจัยความสำเร็จของสิงคโปร์และมาเลเซีย ตามตัวชี้วัดหลักทั้ง 5 ตัว มีดังนี้

**1) ด้านกฎหมาย (Legal Measures)**

จากการศึกษาพบว่ารัฐบาลสิงคโปร์และมาเลเซียให้ความสำคัญกับการออกกฎหมายกฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างครอบคลุม เนื่องจากเป็นเครื่องมือสำคัญในการดำเนินการและเป็นกรอบกฎหมายที่กำหนดนโยบาย ขั้นตอนดำเนินการ

และแนวทางปฏิบัติ เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการ โดยมีแผนแม่บทและกฎหมายอื่นที่เกี่ยวข้องไม่ว่าจะเป็นกฎหมายเกี่ยวกับการแทรกแซงระบบคอมพิวเตอร์ กฎหมายเกี่ยวกับข้อมูล รวมทั้งการกำหนดกฎระเบียบหรือแนวทางปฏิบัติเกี่ยวกับการป้องกันข้อมูล การแจ้งเมื่อมีการละเมิดข้อมูล การให้ประกาศนียบัตรหรือใบรับรองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการตรวจสอบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล การโอนเงินและการทำธุรกรรมอิเล็กทรอนิกส์ โดยรัฐบาลของทั้งสองประเทศได้มีการแก้ไขและออกกฎหมายและกฎระเบียบอย่างต่อเนื่อง และโดยเฉพาะรัฐบาลสิงคโปร์ที่ให้ความสำคัญกับขั้นตอนก่อนการตรากฎหมายหรือกฎระเบียบต่างๆ โดยมีการหารือและทำการศึกษากับทุกภาคส่วนที่เกี่ยวข้อง รวมทั้งนักวิชาการ นักเทคนิค สถาบันการศึกษา และสถาบันวิจัย

แผนแม่บทและกฎหมายที่สำคัญของสิงคโปร์ ได้แก่ แผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์ ฉบับแรก คือ Infocomm Security Masterplan 2005–2007 สาระสำคัญของแผนแม่บทเพื่อประสานงานระหว่างหน่วยงานของรัฐในเรื่องความมั่นคงปลอดภัยไซเบอร์ โดยให้ความสำคัญอันดับแรกคือการเสริมสร้างความสามารถในหน่วยงานภาครัฐในการบรรเทา และรับมือกับภัยคุกคามไซเบอร์ ต่อมา ปี ค.ศ. 2008 ได้ประกาศแผนแม่บทฯ ฉบับที่ 2 สำหรับปี 2008–2012 ซึ่งเป็นแผนแม่บทที่มุ่งเน้นเรื่องการรักษาความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Infrastructure Information หรือ CII) ของสิงคโปร์ ในปี ค.ศ. 2013 ได้ประกาศใช้แผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 3 ครอบคลุมระบบนิเวศน์สารสนเทศและการสื่อสารกว้างขึ้น ทั้งภาคเอกชน และปัจเจกบุคคล ไม่เฉพาะเพียง CII เพื่อให้สิงคโปร์เป็นศูนย์กลางสารสนเทศและการสื่อสารที่มั่นใจและเข็มแข็งได้ นอกจากนี้ สิงคโปร์ยังได้ประกาศใช้แผนปฏิบัติการต่อต้านอาชญากรรมไซเบอร์แห่งชาติ (National Cybercrimes Action Plan) เมื่อเดือนกรกฎาคม ปี ค.ศ. 2016 โดยกระทรวงกิจการภายใน และในปี ค.ศ. 2017 มีการแก้ไขกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์และการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse and Cybersecurity Act) และเมื่อกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) มีผลบังคับใช้เมื่อวันที่ 2 มีนาคม ค.ศ. 2018 ซึ่งเป็นกรอบกฎหมายสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงทำให้คะแนนของสิงคโปร์ในส่วนของตัวชี้วัดด้านกฎหมาย ในปี ค.ศ. 2018 ได้คะแนนเต็ม 0.2000 โดยภายใต้กฎหมายฉบับนี้ได้มีการกำหนดนโยบาย หน้าที่หน่วยงานที่เกี่ยวข้อง ขั้นตอนปฏิบัติในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุมคามไซเบอร์ และการฟื้นตัวหลังเกิดเหตุการณ์ บทลงโทษ ไว้อย่างชัดเจน

นอกจากนี้ ตามกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์แล้ว สิงคโปร์ยังได้กำหนดให้มีการทำงานไปในทิศทางเดียวกับกฎหมายอื่นๆ ที่มีอยู่ รวมทั้งทำงานร่วมกับหน่วยงานกำกับดูแลอิสระอื่นที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012) แนวทางการจัดการการล่วงละเมิดข้อมูล (Guide to Managing Data Breaches) แนวทางการรักษาความปลอดภัยข้อมูลส่วนบุคคล แนวทางการสร้างเว็บไซต์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม (Guide to Building Websites for small and medium – sized enterprises (SMEs))

ในส่วนของมาเลเซียได้มีการออกกฎหมายเพื่อเตรียมพร้อมเข้าสู่ยุคดิจิทัลและกฎหมายที่เกี่ยวข้องกับไซเบอร์ ตั้งแต่ปี ค.ศ. 1990 หลายฉบับ ซึ่งครอบคลุมกับกฎหมายอื่นที่เกี่ยวกับแนวทางปฏิบัติด้านการป้องกันข้อมูล โดยเฉพาะอย่างยิ่งกฎหมายกฎระเบียบที่เกี่ยวกับหน่วยงาน CII ซึ่งตาม Malaysian Cyber Security Strategy 2020 – 2024 ได้กำหนด CII ไว้ 11 สาขา ได้แก่ National Defence and security, Banking and Finance, Information and Communication, Energy, Transportation, Water, Health Services, Government, Emergency Services, Agriculture and Plantation และ Trade, Industry and Economy รายชื่อกฎหมายที่เกี่ยวข้องกับไซเบอร์ของมาเลเซียปรากฏในภาคผนวก 4

**2) ด้านเทคนิค (Technical Measures)**

จากการศึกษาพบว่า ปัจจัยความสำเร็จของสิงคโปร์และมาเลเซียในด้านเทคนิคประกอบด้วย (1) รัฐบาลให้การสนับสนุนงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ (2) มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team: CERT) เพื่อซ้อมรับมือกับสถานการณ์จริง และรับมือกับเหตุเกี่ยวกับ cybersecurity (3) มีกรอบมาตรฐานการดำเนินการด้าน cybersecurity สำหรับหน่วยงานต่างๆ และการมีองค์กรที่จัดทำด้านมาตรฐาน (4) ภาครัฐและภาคเอกชนร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งการจัดหาพันธมิตรใหม่ๆ เพื่อพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์ แล (5) พัฒนาการจัดทำ Best Practice Guideline สำหรับการให้บริการรักษาความปลอดภัย เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทุกสาขา ได้ใช้เป็นแนวทางปฏิบัติ

จากการศึกษาข้อมูลทุติยภูมิ พบว่า สิงคโปร์ตระหนักและให้ความสำคัญกับการพัฒนาเทคโนโลยีการสื่อสารโทรคมนาคมและเทคโนโลยีใหม่ๆ เพื่อให้เท่าทันและสามารถป้องกันและรับมือกับภัยคุกคามไซเบอร์ โดยการจัดสรรงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ มีรายงานจาก www.fticonsultanting.com ว่า สิงคโปร์ได้ลงทุนในเรื่องความมั่นคงปลอดภัยไซเบอร์จำนวน 2.82 พันล้านเหรียญสิงคโปร์ สอดคล้องกับข้อมูลจากรายงาน Singapore Cyber Landscape 2017 ซึ่งจัดทำโดย Cyber Security Agency, Singapore พบว่า เพื่อป้องกันระบบข้อมูลของหน่วยงานภาครัฐ สิงคโปร์กำหนดจะจัดตั้ง Government Security Operations Centre ที่มีอุปกรณ์ปัญญาประดิษฐ์ (Artificial intelligence หรือ AI) และระบบการวิเคราะห์แบบก้าวหน้า ภายในปี ค.ศ. 2020 แทนศูนย์เฝ้าระวังไซเบอร์ (Cyber Watch Centre) ในปัจจุบัน นอกจากนี้ สิงคโปร์ยังกระตุ้นให้หน่วยงานภาครัฐและเอกชนจัดสรรเงินจำนวนร้อยละ 8 ของงบประมาณในส่วนเทคโนโลยีสารสนเทศ (IT) เพื่อใช้สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งถือว่าเป็นการลงทุนในการจัดการความเสี่ยง

ปัจจัยสำคัญอีกประการหนึ่งที่สิงคโปร์ประสบความสำเร็จในตัวชี้วัดเทคนิคคือ การมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT) ซึ่งมีหน้าที่ประกาศเตือน และแนะนำการปฏิบัติงานเชิงเทคนิคเมื่อเกิดเหตุ ส่งเสริมการสร้างความตระหนักรู้ผ่านการสัมมนา ประชุมปฏิบัติการ และการซ้อมรับมือกับสถานการณ์จริง (cyber drills) และร่วมมือ

กับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์อื่นๆ เพื่อรับมือกับเหตุเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดย่อยหนึ่งของตัวชี้วัดเทคนิคคือ การมีกรอบมาตรฐานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานต่างๆ และการมีองค์กรที่จัดทำด้านมาตรฐาน ในปี ค.ศ. 2013 IMDA ของสิงคโปร์ได้ร่วมมือกับวิสาหกิจและภาคอุตสาหกรรมของสิงคโปร์ในการพัฒนามาตรฐานระบบคลาวด์หลายชั้น (multi–tiered cloud computing) ครั้งแรกของโลก ที่จัดการการให้บริการ cloud ด้านความมั่นคงปลอดภัย ที่จัดหาโดยหน่วยงานภาครัฐและเอกชน มาตรฐานใหม่นี้จัดหาให้ในระดับความมั่นคงปลอดภัยที่แตกต่างกันขึ้นอยู่กับระดับความสามารถของผู้ให้บริการที่จะสามารถให้ผู้ใช้บริการ นอกจากนี้ สภามาตรฐานอุตสาหกรรมสิงคโปร์ (Singapore Standards Council) ยังได้เริ่มพัฒนามาตรฐานใหม่ๆ ที่ปัจจุบันยังไม่มีในระดับระหว่างประเทศ ซึ่งรวมถึงมาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับยานพาหนะไร้คนขับ และข้อกำหนดทั่วไปสำหรับความมั่นคงปลอดภัยใน IoT ในโครงการ Smart Nation ของสิงคโปร์ ในปี ค.ศ. 2018 สิงคโปร์ได้ออก Industrial Control Systems Cybersecurity Guidelines สำหรับผู้ประกอบการในระบบควบคุมอุตสาหกรรม ซึ่งเป็นข้อแนะนำและแนวทางปฏิบัติในการปรับปรุงกระบวนการและการควบคุมระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ในระบบแต่ละอุตสาหกรรม เช่น น้ำ พลังงาน การขนส่งทางถนนและการขนส่งทางทะเล

จากการศึกษายังพบว่า ภาครัฐและภาคเอกชนของสิงคโปร์ได้ร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งมีพันธมิตรใหม่เพิ่มขึ้นเรื่อยๆ ในการพัฒนาและนำมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์มาลดช่องว่างมาตรฐานความมั่นคงปลอดภัยไซเบอร์

ในส่วนของมาเลเซียซึ่งได้คะแนนในส่วนของด้านเทคนิคถึง 0.196 มากกว่าสิงคโปร์ที่ได้คะแนน 0.186 โดยมาเลเซียมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (MyCERT) เช่นกัน และจากรายงาน GCI 2018 พบว่า รัฐบาลมาเลเซียมีความโดดเด่นในเรื่องความร่วมมือกับภาคอุตสาหกรรมในการพัฒนาการจัดทำ Best Practice Guideline สำหรับการให้บริการรักษาความปลอดภัย รวมทั้ง Cloud Security Practice โดยการจัดเตรียมเอกสาร Cloud Security Practice เพื่อจัดทำ Cloud Security Certification Scheme นอกจากนี้ ยังได้จัดตั้ง Internet Banking Task Force ประกอบด้วย สถานบันการเงินท้องถิ่น Malaysian Communications and Information Commission ซึ่งเป็นหน่วยงานกำกับดูแล Cyber Security Malaysia และ The Royal Malaysian Police เพื่อจัดการต่อสู้กับการฉ้อโกงผ่านระบบธนาคารออนไลน์ (online banking fraud) โดยได้มีการจัดตั้งห้องทดลอง/ทดสอบ (laboratories) ปัจจัยที่มาเลเซียประสบความสำเร็จในด้านเทคนิคอีกประการคือ การที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทุกสาขาจะพบหารือในการจัดทำ Best Practices และแบ่งปันข้อมูลเทคนิคในเรื่องความมั่นคงปลอดภัยไซเบอร์

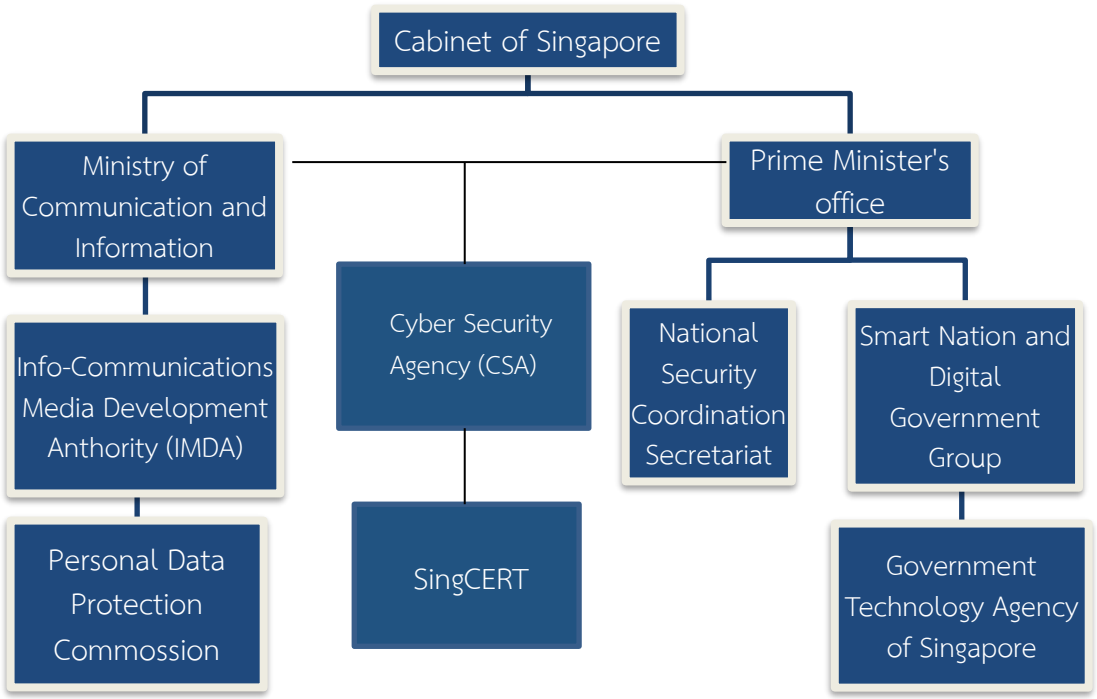
**3) ด้านองค์กร (Organizational Measure)**

ทั้งสิงคโปร์และมาเลเซียมีพัฒนาการในการจัดตั้งองค์กรหรือหน่วยงานที่กำหนดนโยบาย มีการกำหนดยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ รวมทั้งมีหน่วยงานที่รับผิดชอบการรับมือกับภัยคุกคามไซเบอร์ได้อย่างครอบคลุม และมีการ

ประสานงานข้ามองค์กรระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทำให้การดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของทั้งสองประเทศประสบความสำเร็จบรรลุตามเป้าหมายและแผนยุทธศาสตร์ระดับชาติ

จากการศึกษา พบว่า โครงสร้างองค์กรของสิงคโปร์ที่ดูแลรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะครอบคลุมหน่วยงานที่เกี่ยวข้อง ภายใต้การกำกับดูแลของคณะรัฐมนตรี และมีการยุบรวมหน่วยงานเพื่อให้เกิดการทำงานอย่างบูรณาการ รายละเอียดปรากฏตามแผนภูมิที่ 1

**แผนภูมิที่ 1** โครงสร้างองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์




ที่มา: Cybersecurity for Critical Information Infrastructure in Thailand, ThaiCERT ETDA

นอกจากหน่วยงานรัฐหลักๆ ที่ได้กล่าวมาแล้ว สิงคโปร์ยังมีหน่วยงานอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทั้งภาครัฐและเอกชน โดยเฉพาะอย่างยิ่ง หน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งตามกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ได้กำหนดไว้ ได้แก่ พลังงาน น้ำ การเงินและการธนาคาร ระบบดูแลสุขภาพ การขนส่ง (บก น้ำ อากาศ) สารสนเทศและการสื่อสาร สื่อ ความมั่นคงปลอดภัยและการให้บริการฉุกเฉิน และรัฐบาล โดยหน่วยงานที่เกี่ยวข้องต่างๆ ของสิงคโปร์ได้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด ทำให้ระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์เป็นไปอย่างมีประสิทธิภาพ แม้จะมีช่องโหว่อยู่บ้าง แต่ก็สามารถรับมือได้อย่างทันท่วงที ทำให้ลดความเสียหายที่จะเกิดขึ้น

สำหรับมาเลเซียมีการจัดตั้ง National Cyber Security Agency (NACSA) เพื่อรับผิดชอบงานเกี่ยวกับไซเบอร์ โดยอยู่ภายใต้ National Security Council (NSC) ซึ่งจะประกอบไปด้วยศูนย์ปฏิบัติการในแต่ละระดับความรับผิดชอบ โดยแบ่งออกเป็น 6 ระดับ ได้แก่ (1) National cyber crisis management structure (2) National cyber - threat level (3) Computer Emergency Response Team (CERT) (4) Cyber security protection mechanisms (5) Response, communication and coordination procedures และ(6) Readiness programme

นอกจากนี้ มาเลเซียยังให้ความสำคัญในการจัดทำแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีการกำหนดยุทธศาสตร์ในแต่ละด้านอย่างครอบคลุม จึงทำให้มาเลเซียได้คะแนนเต็มในส่วนของตัวชี้วัดด้านองค์กร โดยมีแผนยุทธศาสตร์ฉบับล่าสุดคือ Malaysia Cyber Security Strategy 2020 – 2024 ทั้งนี้ แผนยุทธศาสตร์ดังกล่าวได้เน้นย้ำถึงความสำคัญในการทำงานและประสานงานระหว่าง CII ทั้ง 11 สาขา รวมทั้งมีการจัด National Cyber Crisis Exercise (X – Maya) เพื่อฝึกซ้อมและทดสอบประสิทธิภาพของกระบวนการในการรับมือกับภัยคุกคามไซเบอร์ ซึ่งเป็นกิจกรรมที่กำหนดไว้ใน National Cyber Crisis Management Plan รวมทั้งการเตรียมความพร้อมรับมือกับการถูกโจมตีไซเบอร์ของหน่วยงาน CII โดยมาเลเซียได้จัดการฝึกซ้อมในระดับชาติมาแล้ว 6 ครั้ง ซึ่งมีหน่วยงานเข้าร่วมการฝึกซ้อม ทั้งภาครัฐและเอกชนจากหน่วยงาน CII มากกว่า 100 หน่วยงาน

**4) ด้านการเสริมสร้างศักยภาพ (Capacity Building)**

ตัวชี้วัดด้านการเสริมสร้างศักยภาพจะพิจารณาจากการรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่สาธารณะชน การส่งเสริมเรื่องมาตรฐาน cybersecurity และการให้ใบรับรองแก่ผู้เชี่ยวชาญ / ผู้ชำนาญการในเรื่องดังกล่าว การฝึกอบรมให้แก่ผู้เชี่ยวชาญ / ผู้ชำนาญการด้าน cybersecurity การมีหลักสูตรในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ การมีโครงการศึกษาวิจัยและการพัฒนา (R&D) การมีมาตรการส่งเสริมแรงจูงใจ และการส่งเสริมภาคอุตสาหกรรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เติบโตในประเทศ ซึ่งทั้งสิงคโปร์และมาเลเซียได้มีการดำเนินนโยบายในเรื่องนี้อย่างจริงจังและต่อเนื่อง

รัฐบาลสิงคโปร์ทำงานอย่างใกล้ชิดกับภาคอุตสาหกรรมและสถาบันการศึกษาในการริเริ่มโครงการต่างๆ ที่ส่งเสริมการเติบโตและพัฒนาสายงานอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ จากรายงาน Singapore Cyber Landscape 2017 พบว่า สิงคโปร์ได้มีการดำเนินการ เช่น การจัดทำแผนพัฒนาอาชีพสาขาการรักษาความปลอดภัยไซเบอร์ในภาคการบริการสาธารณะให้เป็นอาชีพที่ดึงดูดความสนใจ โดยมีค่าตอบแทนเป็นแรงจูงใจ และการสร้างอาชีพด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานทางทหาร

ในส่วนของการวิจัยและพัฒนา สิงคโปร์ได้ดำเนินการดังนี้

1) พัฒนาความสามารถในเรื่องความปลอดภัย Cyber–Physical Systems และเทคโนโลยี blockchain สำหรับอุตสาหกรรมโลจิสติกส์

2) จัดทำกฎเกณฑ์การประเมินผลที่ทำให้ง่ายขึ้นในการรับรองมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ IoT และผลิตภัณฑ์อื่นๆ ที่เกี่ยวข้อง

3) สนับสนุนการเติบโตและการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มผู้ประกอบการตั้งต้น (startup) ซึ่งเป็นตัวขับเคลื่อนสำคัญในเศรษฐกิจดิจิทัล

นอกจากนี้ สิงคโปร์ได้ริเริ่มดำเนินโครงการต่างๆ ที่เป็นแรงจูงใจให้มีการพัฒนาทักษะความเชี่ยวชาญด้าน cybersecurity เช่น จัดทำ Co – innovation and Development Proof – of – Concept Funding Scheme เพื่อสนับสนุนผู้ให้บริการการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity solution providers) และผู้ใช้ (cybersecurity end – users) โดยให้ทุนในการดำเนินการสูงสุดถึง 500,000 เหรียญสิงคโปร์ สำหรับระยะเวลาสูงสุดไม่เกิน 12 เดือน

ในส่วนของตัวชี้วัดย่อยในเรื่องการส่งเสริม R&D มาเลเซียให้ความสำคัญกับการส่งเสริม R&D ในภาคอุตสาหกรรมท้องถิ่น ผ่าน The National Cybersecurity Research and Development Roadmap โดยมาเลเซียได้สร้างแพลตฟอร์มความร่วมมือ R&D ระหว่างภาครัฐ สถาบันการศึกษา และภาคอุตสาหกรรม เพื่อสร้างนวัตกรรมท้องถิ่นและเพิ่มขีดความสามารถให้กับ cyber security technology solutions ที่มีอยู่ให้สามารถแข่งขันสู่ระดับโลกได้ โดยให้ความสำคัญกับ R&D ในเรื่องดังต่อไปนี้

- Privacy enhancing technology
- Digital signature
- Digital identity
- Entity authentication
- Encryption algorithm
- Cyber physical security

ปัจจัยสำคัญในการเสริมสร้างศักยภาพอีกประการคือ การสร้างความตระหนักรู้แก่ประชาชนเกี่ยวกับภัยคุกคามทางไซเบอร์ และการจัดการกับภัยคุกคามดังกล่าว สิงคโปร์และมาเลเซียได้ให้ความสำคัญอันดับแรกคือ การให้ความรู้เกี่ยวกับการปฏิบัติที่จะป้องกันข้อมูลและทำให้เครื่องมืออุปกรณ์ดิจิทัลสะอาดปลอดภัยจากไวรัสที่มาจากไซเบอร์ เช่น การตั้งรหัสผ่านให้มีความซับซ้อนยากที่จะเข้าถึง การ back up ข้อมูลอย่างสม่ำเสมอ การ update และ upgrade ซอล์ฟแวร์และฮาร์ดแวร์เป็นประจำ และจำกัดการเข้าถึงระบบที่มีความสำคัญ โดยเฉพาะมาเลเซียได้กำหนดให้มีแผนแม่บทระดับชาติว่าด้วยการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (National Cyber Security Awareness Master Plan)

นอกจากนี้ ทั้งสิงคโปร์และมาเลเซีย ยังให้ความสำคัญกับการเตรียมกำลังคนด้านไซเบอร์โดยได้จัดทำแผนระดับชาติว่าด้วยการส่งเสริมการเพิ่มศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ( National Cyber Security Capacity and Capacity Building Plan) การกำหนดให้มีหลักสูตรเกี่ยวกับ cybersecurity ทั้งในระดับโรงเรียนและสถาบันการศึกษาขั้นสูงตลอดจนการจัดให้มีการเรียนรู้ ฝึกอบรม พัฒนาทักษะ สำหรับผู้เชี่ยวชาญ และคนทั่วไป ทั้งในส่วนของภาครัฐและเอกชน โดยมาเลเซียได้กำหนดไว้ใน Malaysian Cyber Security Strategy 2020 – 2024 ว่า มาเลเซียจะจัดตั้ง Centre of Excellence ในด้านนี้ โดยร่วมมือกับมหาวิทยาลัยท้องถิ่น

**แผนภูมิที่ 2** แสดงถึงยุทธศาสตร์ด้านการเสริมสร้างศักยภาพของมาเลเซีย


ที่มา: สรุปจาก Malaysia Cyber Security Strategy 2020-2024

**5) ด้านความร่วมมือ (Cooperation)**

ITU วิเคราะห์และให้คะแนนตัวชี้วัดนี้จากหุ้นส่วนพันธมิตร กรอบความร่วมมือและเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง โดยแบ่งตัวชี้วัดย่อยเป็น 5 ตัว ประกอบด้วย การจัดทำความตกลงทวิภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำข้อตกลงและ/หรือการเข้าร่วมความตกลงพหุภาคี การเข้าร่วมในเวทีระหว่างประเทศ ความร่วมมือระหว่างภาครัฐและเอกชน ความร่วมมือกับหน่วยงานระหว่างประเทศ และการมีแบบปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity best practices)

จากการศึกษาพบว่า ทั้งสิงคโปร์และมาเลเซียมีการจัดทำความตกลงทวิภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับประเทศต่างๆ โดยเฉพาะอย่างยิ่งสิงคโปร์ รวมทั้ง มีการจัดทำข้อตกลงและ / หรือการเข้าร่วมความตกลงพหุภาคีที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ ทั้งสองประเทศได้มีการเข้าร่วมและมีบทบาทนำในเวทีระหว่างประเทศโดยเฉพาะในกรอบอาเซียน เช่น สิงคโปร์และมาเลเซียเป็นประเทศที่ยกร่างแผนแม่บทอาเซียนว่าด้วยความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งสิงคโปร์ ที่ได้เสนอการจัดทำบรรทัดฐานพฤติกรรมของรัฐในด้านไซเบอร์ (Norms of State Behavior in Cyberspace) แนวทางสำหรับกลไกเพื่อส่งเสริมการประสานงานด้านความมั่นคงปลอดภัยทางสารสนเทศของอาเซียน (Cybersecurity

Coordination Efforts in ASEAN) ตลอดจนการจัดงาน Singapore International Cyber Week (SICW) เป็นประจำทุกปี ตั้งแต่ ปี ค.ศ. 2016

ปัจจัยความสำเร็จอีกประการคือ ทั้งสองประเทศมีความร่วมมือระหว่างภาครัฐและเอกชนอย่างใกล้ชิดและเข้มแข็ง มีความร่วมมือกับหน่วยงานระหว่างประเทศ และการมีแบบปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity best practices) ตัวอย่างเช่น ข้อมูลจากเว็บไซต์ CSA สิงคโปร์ พบว่า CSA ได้จัดทำ Memorandum of Collaboration ว่าด้วยความร่วมมือในการจัดทำกรอบดำเนินงานสำหรับความมั่นคงปลอดภัยไซเบอร์กับ Cisco System นอกจากนี้ CSA ร่วมกับ GovTech ได้ร่วมมือกับ HackerOne ซึ่งเป็นชุมชนใหญ่ที่สุดในโลกที่รวมนักวิจัย Cybersecurity และแฮกเกอร์ดี (“white hat” hackers) ทั้งในและนอกประเทศ ในการจัดทำโปรแกรม Government Bug Bounty Programme (GBBP) ระหว่างเดือนธันวาคม ปี ค.ศ. 2018 – เดือนมกราคม ค.ศ. 2019 เพื่อให้แฮกเกอร์ค้นหาจุดอ่อนไหวในระบบสารสนเทศและการสื่อสารของหน่วยงานภาครัฐที่คัดเลือกมา 5 หน่วยงาน ที่มีการใช้อินเทอร์เน็ตและเว็บไซต์ปริมาณสูง โดยแฮกเกอร์จะได้รับเงินรางวัลตอบแทน ซึ่งมีจำนวนตั้งแต่ 250 – 10,000 เหรียญสหรัฐฯ ทั้งนี้ขึ้นอยู่กับความรุนแรงของตัวปัญหาหรือ “bug” ที่ค้นพบ

**(2) การวิเคราะห์ปัญหาในการดำเนินการในส่วนของประเทศไทย**

จากการวิเคราะห์บริบทของไทยในเรื่องการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ โดยวิเคราะห์จากตัวชี้วัดทั้ง 5 ด้าน ดังกล่าว ผลการศึกษาสรุปได้ดังนี้

**1) ด้านกฎหมาย** ปัจจุบัน ประเทศไทยมีพระราชบัญญัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ดังนี้ (1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (3) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 และ 4) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

สำหรับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งเป็นกฎหมายสำคัญในการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ มีสาระสำคัญดังนี้

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เสนอร่างพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 มีทั้งหมด 83 มาตรา แบ่งเป็นบททั่วไป ได้แก่ วันบังคับใช้ นิยาม และผู้รักษาการ ประกอบด้วย 4 หมวด ดังนี้ หมวดที่ 1 คณะกรรมการ หมวดที่ 2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หมวดที่ 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ หมวดที่ 4 บทกำหนดโทษ และมีบทเฉพาะกาล หลักการสำคัญของพระราชบัญญัติคือ มุ่งที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ
- พระราชบัญญัตินี้ได้กำหนดให้มีคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security

Committee” เรียกโดยย่อว่า “NCSC” โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ และได้กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) รวมทั้ง กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีเลขาธิการคณะกรรมการ

- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการทั้ง 3 คณะ และมีหน้าที่สำคัญดังนี้

  - ส่งเสริม สนับสนุน งานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - ปฏิบัติการ ประสานงานเฝ้าระวัง แจ้งเตือน ให้ความช่วยเหลือ
  - จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน
  - ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ
  - ฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
  - รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

ตามมาตรา 41 - 44 ได้กำหนดเกี่ยวกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

(1) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(4) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน

(7) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ ตามตารางที่ 2 พบว่า คะแนนตัวชี้วัดของไทยด้านกฎหมาย ในปี ค.ศ. 2018 ได้ 0.186 มากกว่ามาเลเซียซึ่งได้ 0.179 อย่างไรก็ดี กฎหมายสำคัญคือพระราชบัญญัติการรักษาความ

มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ยังอยู่ในช่วงการจัดตั้งสำนักงานฯ และจัดทำร่างกฎหมายลำดับรอง รวมทั้งการจัดทำแนวทางในการปฏิบัติสำหรับหน่วยงานที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งแนวทางปฏิบัติสำหรับหน่วยงานที่เกี่ยวข้องกับ CII ทุกสาขา จึงอาจจะทำให้ยังไม่สามารถดำเนินนโยบายไปสู่การปฏิบัติได้ในขณะนี้ นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ยังไม่มีผลบังคับใช้ในทางปฏิบัติอย่างเต็มที่ เนื่องจากสถานะการณ์การแพร่ระบาดของโรคโควิด -19 ทำให้ภาคเอกชนยังไม่มีความพร้อมในการปฏิบัติตามแนวทางที่กฎหมายกำหนด จึงมีประกาศเลื่อนการบังคับใช้บางมาตราออกไปก่อน

**2) ด้านเทคนิค** พบว่า ประเทศไทยมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ซึ่งเป็นหน่วยงานภายใต้สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (ซึ่งเป็นองค์การมหาชน ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) ที่ทำหน้าที่เพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

ปัญหาที่พบคือ ThaiCERT เป็นเพียงหน่วยงานหนึ่งในสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งมีงบประมาณและบุคลากรทางเทคนิคจำกัด และแม้ว่าประเทศไทยจะมีหลายหน่วยงานที่มีภารกิจเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทั้งหน่วยงานภาครัฐ หน่วยงานกำกับดูแล สถาบันการศึกษา และเอกชน แต่ยังขาดการบูรณาการความร่วมมือทางเทคนิคกับหน่วยงานต่างๆ ที่เกี่ยวข้อง ประกอบกับ เนื่องจากอยู่ระหว่างการจัดตั้งสำนักงานคณะกรรมการการรักษาความปลอดภัยไซเบอร์แห่งชาติ จึงยังไม่สามารถดำเนินการสู่การปฏิบัติอย่างเป็นรูปธรรม โดยเฉพาะอย่างยิ่ง การกำหนดมาตรฐานและใบรับรองมาตรฐานต่างๆ

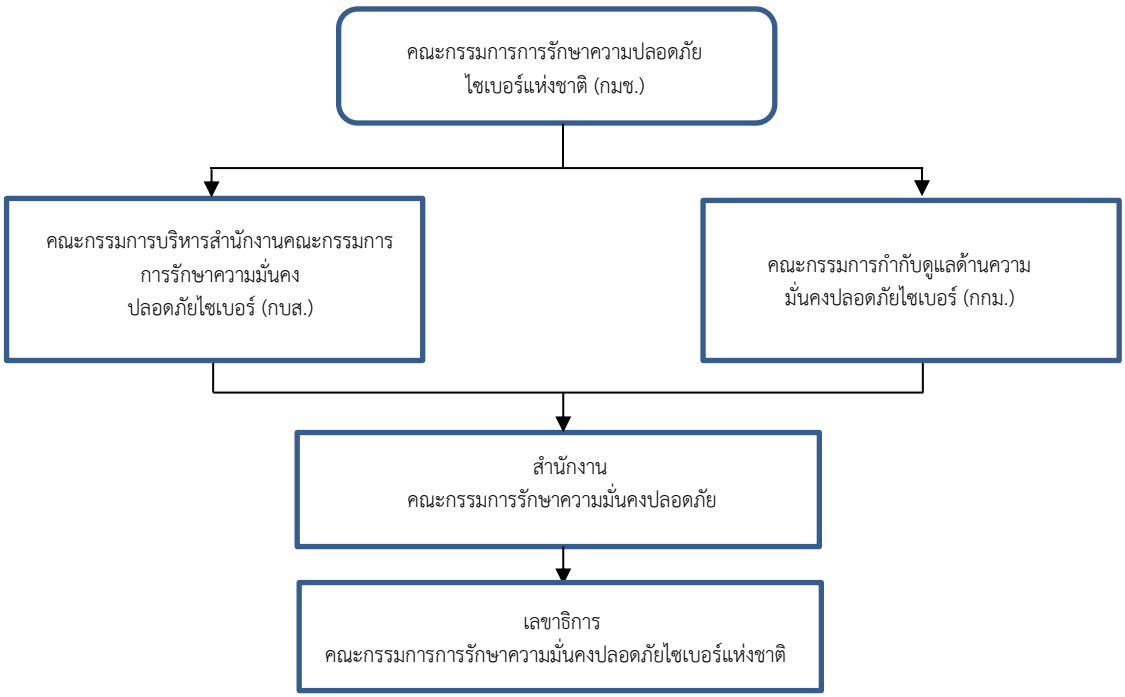
นอกจากนี้ เนื่องจากไทยอยู่ระหว่างการจัดตั้งสำนักงานคณะกรรมการการรักษาความปลอดภัยไซเบอร์แห่งชาติ จึงยังไม่สามารถดำเนินการสู่การปฏิบัติอย่างเป็นรูปธรรม โดยเฉพาะการเตรียมการด้านเทคนิคที่รับมือกับการโจมตีระบบ CII ของประเทศ

**3) ด้านองค์กร** พบว่า หลังจากพระราชพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 โดยในบทเฉพาะการได้กำหนดให้ดำเนินการจัดตั้ง สกมช. ให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และในระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการ จนกว่าจะมีการแต่งตั้งเลขาธิการ ทั้งนี้ ปัจจุบัน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ได้มีสถานะเป็นหน่วยงานของรัฐ นับตั้งแต่วันที่ 1 มกราคม 2564 โดยขึ้นตรงกับนายกรัฐมนตรี อย่างไรก็ดี ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ซึ่งเป็นหน่วยงานภายใต้สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (ซึ่งเป็นหน่วยงานภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) ยังคงปฏิบัติหน้าที่ต่อไปก่อน ในขณะที่ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อ

เศรษฐกิจและสังคมทำหน้าที่ประธานคณะกรรมการย่อยทั้ง 2 คณะ ซึ่งเป็นคณะกรรมการภายใต้คณะกรรมการการรักษาความปลอดภัยไซเบอร์แห่งชาติ จากโครงสร้างองค์กรดังกล่าว จึงอาจจะยังมีความไม่ชัดเจนสำหรับหน่วยงานปฏิบัติ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติงาน

ทั้งนี้ ตามมาตรา 49 ของพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ได้แก่ (1) ด้านความมั่นคงของรัฐ (2) ด้านบริการภาครัฐที่สำคัญ (3) ด้านการเงินการธนาคาร (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (5) ด้านการขนส่งและโลจิสติกส์ (6) ด้านพลังงานและสาธารณูปโภค (7) ด้านสาธารณสุข และ (8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม โดย สกมช. มีหน้าที่ในการประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน CII ทุกสาขา ซึ่งผลสำเร็จในกการทำงานในลักษณะข้ามองค์กรจะเป็นคะแนนตัวชี้วัดย่อยในด้านองค์กร นอกจากนี้ ตัวชี้วัดย่อยด้านองค์กรที่สำคัญคือการมีแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่ง สกมช. ยังอยู่ในระหว่างการดำเนินการ และเนื่องจากไทยยังไม่ได้มีการจัดตั้งองค์กรและยังไม่มีการดำเนินการที่เป็นรูปธรรมที่ชัดเจน จึงทำให้ไทยได้คะแนนในด้านองค์กรในปี ค.ศ. 2018 น้อยกว่าทุกด้าน โครงสร้างของหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดไว้ในพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ปรากฏตามแผนภูมิที่ 4

แผนภูมิที่ 4 โครงสร้างของหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย




ที่มา: กองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

**4) ด้านการเสริมสร้างศักยภาพ** ประเทศไทยโดยหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และสภาความมั่นคงแห่งชาติได้ตระหนักถึงความสำคัญในการเตรียมบุคลากรที่มีทักษะและความเชี่ยวชาญดังกล่าวโดยมีการจัดหลักสูตรฝึกอบรมด้านนี้

นอกจากนี้ ประเทศไทยยังมีบทบาทสำคัญในอาเซียนด้านการเสริมสร้างศักยภาพ โดยประเทศไทยได้รับเลือกให้เป็นที่ตั้งศูนย์ความร่วมมืออาเซียน – ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN – Japan Cybersecurity Capacity Building Centre) โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้จัดหาพื้นที่จัดตั้งศูนย์ และโครงการได้รับงบประมาณสนับสนุนจากกองทุน Japan ASEAN Integration Fund (JAIF) จำนวน 5 ล้านเหรียญสหรัฐ เป็นระยะเวลา 4 ปี โดยโครงการ AJCCBC ระยะที่ 1 ช่วงปี ค.ศ. 2018 – 2020 ได้รับงบประมาณ รวมทั้งสิ้น 2,907,667.86 เหรียญสหรัฐฯ โดยมีวัตถุประสงค์ในการจัดตั้งศูนย์ ดังนี้

- จัดกิจกรรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่มีหลักสูตรการฝึกอบรมสอดคล้องกับความต้องการของประเทศสมาชิกอาเซียน
- ให้ความรู้และยกระดับความสามารถในการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียน
- สร้างความเชื่อมั่นและส่งเสริมความร่วมมือระหว่างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

โดยมีเป้าหมายสำคัญ คือ การอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่กลุ่มเป้าหมายในประเทศสมาชิกอาเซียน 2 กลุ่มได้แก่ (1) ข้าราชการและ (2) เจ้าหน้าที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 700 คน โดยจะมีการจัดฝึกอบรม ปีละ 6 ครั้ง ครั้งละ 24 คน ตลอดระยะเวลา 4 ปี รวมทั้งบุคลากรที่จะเข้าร่วมการแข่งขัน Cyber SEA Game ซึ่งเป็นการแข่งขันทางเทคนิคด้านความมั่นคงปลอดภัยไซเบอร์ระดับอาเซียน โดยจะมีผู้เข้าร่วมปีละ 40 คนจาก 10 ประเทศอาเซียนติดต่อกัน 4 ปี

อย่างไรก็ดี พบว่า ประเทศไทยยังขาดการประสานงานระหว่างหน่วยงานต่างๆ ที่มีส่วนเกี่ยวข้องกับการพัฒนาบุคลากรด้าน cybersecurity โดยเฉพาะอย่างยิ่งการประสานงานกับสถาบันการศึกษา ภาคธุรกิจและภาคอุตสาหกรรมในการจัดเตรียมบุคลากรสายงานอาชีพในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ ภาคธุรกิจและประชาชนยังขาดความตระหนักรู้และทักษะพื้นฐานในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การตั้งรหัสผ่าน การตั้งโปรแกรมฆ่าไวรัส การไม่เข้าถึงเว็ปไซต์ที่ไม่ถูกกฎหมาย

**5) ด้านความร่วมมือ** ประเทศไทยโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้มีความคืบหน้าในเรื่องนี้อย่างต่อเนื่อง โดยกระทรวงฯ ได้มีการลงนามบันทึกความเข้าใจกับกระทรวงที่รับผิดชอบเทคโนโลยีสารสนเทศและการสื่อสารของประเทศต่างๆ โดยขอบเขตความร่วมมือจะครอบคลุมไปถึงด้านความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ ในส่วนของ ThaiCERT ในฐานะที่เป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/ Forum of Incident Response and Security Teams) มีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่

เป็นสมาชิกขององค์กรเหล่านี้ กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง สอดคล้องกับคะแนนที่ไทยได้รับถึง 0.142 มากกว่าสิงคโปร์ (0.125) และมาเลเซีย (0.120)

อย่างไรก็ดี พบว่า ปัญหาสำคัญของไทย คือ การขาดการบูรณาการการทำงานระหว่างหน่วยงานที่เกี่ยวข้อง ซึ่งมีหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์หลายหน่วยงานทั้งในมิติด้านความมั่นคง เศรษฐกิจ และสังคม นอกจากนี้ ปัญหาในส่วนของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีการจัดทำความตกลงหรือบันทึกความเข้าใจ (MoU) กับประเทศอื่นด้าน Cybersecurity เช่น สิงคโปร์ และออสเตรเลีย แต่ไม่มีการดำเนินการต่ออย่างเป็นรูปธรรม รวมทั้ง บทบาทความร่วมมือของไทยในเวทีระหว่างประเทศยังไม่โดดเด่นเท่าที่ควร อาจเนื่องจากบุคลากรที่มีความรู้และทักษะในเรื่องความมั่นคงปลอดภัยไซเบอร์มีจำกัด ทำให้ไม่สามารถให้ความเห็น หรือจัดทำข้อเสนอในเวทีอาเซียนได้อย่างมีประสิทธิผลเท่าที่ควร ประกอบกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติซึ่งเป็นหน่วยงานที่ต้องรับผิดชอบและประสานงานโดยตรงในการรักษาความมั่นคงปลอดภัยไซเบอร์ยังอยู่ในระหว่างการจัดตั้งสำนักงาน

**(3) แนวทางการแก้ไขปัญหาและพัฒนานโยบาย**

จากการวิเคราะห์ข้อมูลปัจจัยความสำเร็จของสิงคโปร์และมาเลเซียในการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาจากตัวชี้วัดทั้ง 5 ตัว และจากข้อมูลการวิเคราะห์ปัญหาอุปสรรคในการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เห็นควรเสนอแนวทางการแก้ไขปัญหาและพัฒนานโยบายในส่วนของประเทศไทย ดังนี้

**<u>ด้านกฎหมาย</u>**

- เร่งดำเนินการจัดทำกฎหมายลำดับรอง และแนวทางปฏิบัติ ร่วมกับหน่วยงานที่เกี่ยวข้องทุกภาคส่วน โดยเฉพาะหน่วงานของ CII ทุกสาขา
- กำหนดให้มีการทำงานไปในทิศทางเดียวกับกฎหมายอื่นๆ ที่มีอยู่ รวมทั้งทำงานร่วมกับหน่วยงานกำกับดูแลอิสระอื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 และกฎหมายอื่นๆ ที่เกี่ยวข้องกับ CII ทุกสาขา
- ศึกษา Best Practices ในการจัดทำกฎระเบียบ และแนวทางการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์จากประเทศที่ประสบความสำเร็จทั้งในและนอกภูมิภาคเอเชียและแปซิฟิก

**<u>ด้านเทคนิค</u>**

- รัฐบาลควรให้ความสำคัญในการจัดสรรงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้เพื่อป้องกันและจัดการ ตลอดจนลดผลกระทบจากอาชญากรรมไซเบอร์ เช่น ระบบ AI การวิเคราะห์ข้อมูลแบบก้าวหน้า ซึ่งถือว่าเป็นการลงทุนในการจัดการความเสี่ยง

- จัดตั้งหน่วยงานหรือศูนย์ข้อมูลสำคัญของภาครัฐ เพื่อปกป้องรักษาข้อมูลที่สำคัญโดยเฉพาะข้อมูลเกี่ยวกับความมั่นคง มีการจัดทำการสำรองข้อมูลขนาดใหญ่ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ โดยมีเครื่องมือและบุคลากรทางเทคนิคที่มีมาตรฐานสูง
- เร่งดำเนินการจัดทำกรอบมาตรฐานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานต่างๆ และควรมีองค์กรที่จัดทำด้านมาตรฐาน รวมทั้งการออกใบรับรองมาตรฐาน
- พัฒนางานและขยายเครือข่ายความร่วมมือทางเทคนิคของ ThaiCERT กับ CERT อื่นๆ ในภูมิภาค

**ด้านองค์กร**

- ศึกษา Best Practice ในการจัดตั้งองค์กร รูปแบบการประสานงานข้ามองค์กรและหน่วยงานที่เกี่ยวข้อง ทั้งในและนอกประเทศ โดยเฉพาะของมาเลเซียซึ่งได้คะแนนตัวชี้วัดด้านองค์กรเต็ม เพื่อนำมาเป็นข้อมูลประกอบการพิจารณาการจัดตั้งองค์กรและหน่วยงานต่างๆ ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมทั้งการจัดทำแผนยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยอย่างครอบคลุม เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถปฏิบัติงานไปในทิศทางเดียวกันได้อย่างมีประสิทธิผล

**ด้านการเสริมสร้างศักยภาพ**

- การใช้ประโยชน์จากศูนย์ฝึกอบรม อาเซียน – ญี่ปุ่น อย่างเต็มศักยภาพ และพิจารณาความเป็นไปได้ในการขยายหรือยกระดับให้เป็นศูนย์ฝึกอบรมกับประเทศคู่เจรจาอาเซียน (จีน เกาหลี และอินเดีย)
- หน่วยงานที่เกี่ยวข้อง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สกมช. กระทรวงศึกษาธิการ กระทรวงแรงงาน กระทรวงอุดมศึกษา วิทยาศาตร์ วิจัยและนวัตกรรม สถาบันการศึกษาของรัฐและเอกชน ทั้งในระดับโรงเรียน อาชีวศึกษา และมหาวิทยาลัย ร่วมกันกำหนดหลักสูตร หรือพัฒนาหลักสูตรด้าน cybersecurity ในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ โดยเฉพาะการเรียนรู้ผ่านระบบออนไลน์ เพื่อผลิตบุคลากรด้าน cybersecurity รองรับตลาดแรงงานและผลกระทบที่เกิดจากเทคโนโลยีดิจิทัลซึ่งมีพลวัตรสูง
- ส่งเสริมการสร้างการตระหนักรู้ในเรื่อง cybersecurity ให้แก่ประชาชนอย่างต่อเนื่อง ผ่านรูปแบบต่างๆ อาทิ สื่อออนไลน์ สื่อดิจิทัล social media และกิจกรรมโครงการต่างๆ โดยร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคอุตสาหกรรม ทั้งนี้ อาจมอบหมายให้หน่วยงาน CII แต่ละสาขาดำเนินการในการสร้างการตระหนักรู้ให้กับหน่วยงานและภาคประชาชนด้วย
- ศึกษาการจัดทำแผนแม่บทระดับชาติในว่าด้วยการเพิ่มศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ทั้งระบบให้ครอบคลุมในทุกมิติ

**ด้านความร่วมมือ**

- ยกระดับความร่วมมือระหว่างภาครัฐ เอกชน สถาบันการศึกษา และภาคประชาคม อย่างใกล้ชิดและเข้มแข็ง
- ดำเนินการตามกรอบความร่วมมือในอาเซียนให้เกิดเป็นรูปธรรม

- การดำเนินการภายใต้บันทึกความเข้าใจ (MoU) กับสิงคโปร์ ว่าด้วย Digital Economy ที่อยู่ระหว่างการจัดทำให้เกิดเป็นรูปธรรม รวมทั้ง MoU กับประเทศอื่น ๆ
- ส่งเสริมและยกระดับบทบาทของไทยในเวทีอาเซียนด้านดิจิทัล จัดทำตัวชี้วัดบุคลากรในสำนักงานปลัดกระทรวงฯ กำหนดตัวชี้วัดตามจำนวนข้อเสนอ /โครงการ หรือการทำหน้าที่ในคณะทำงานต่างๆ ภายใต้กรอบอาเซียนด้านดิจิทัล
- จัดทำฐานข้อมูลดิจิทัลความร่วมมือระหว่างประเทศด้านดิจิทัลในกรอบอาเซียนและคู่เจรจา

**(4) ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จ**

เนื่องจากนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นนโยบายระดับชาติ และเกี่ยวข้องกับหลายหน่วยงานทั้งภาครัฐ เอกชน และประชาชน ประกอบกับเป็นเรื่องที่มีความซับซ้อนทั้งในเชิงเทคนิคและนโยบาย การผลักดันข้อเสนอเชิงนโยบายดังกล่าวอาจมีข้อจำกัด ทำให้ไม่สามารถดำเนินการได้ตามที่คาดหวัง อย่างไรก็ดี ในฐานะผู้บริหารกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สามารถร่วมผลักดันข้อเสนอในการดำเนินนโยบายดังกล่าวผ่านคณะกรรมการ คณะอนุกรรมการ หรือคณะทำงานต่างๆ ที่เกี่ยวข้องได้ ทั้งนี้ ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของประเทศไทยในแต่ละตัวชี้วัด มีดังนี้

**<u>ด้านกฎหมาย</u>** ความล่าช้าในการจัดทำกฎหมายลำดับรอง โดยมีแนวทางบริหารจัดการคือ การจัดตั้งคณะทำงานด้านกฎหมายภายใต้คณะคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่ประธานคณะกรรมการฯ เพื่อทำการศึกษาและเตรียมการในการจัดทำร่างกฎหมายลำดับรองโดยเฉพาะอย่างยิ่งการจัดทำร่างประกาศคณะกรรมการภายใต้คณะกรรมการการรักษาความปลอดภัยไซเบอร์แห่งชาติ เรื่อง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. .... ซึ่งเกี่ยวข้องกับหน้าที่และอำนาจของหน่วยงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (NationalCERT) ตลอดจนหารือหน่วยงานที่เกี่ยวข้อง เพื่อรายงานและเสนอความเห็นต่อรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

**<u>ด้านเทคนิค</u>** ขาดการสนับสนุนงบประมาณจากภาครัฐในการนำเทคโนโลยีชั้นสูงที่มีราคาสูงมาใช้ในการรับมือกับภัยคุกคามและอาชญากรรมทางไซเบอร์ โดยมีแนวทางบริหารจัดการคือ มอบหมายให้หน่วยงานที่เกี่ยวข้องทำการศึกษาเครื่องมือที่จะนำมาใช้ให้ละเอียดรอบด้าน จัดทำข้อมูลวิเคราะห์ประมาณการค่าใช้จ่ายและผลเสียหายที่อาจจะเกิดขึ้นหากไม่มีการนำเทคโนโลยีนั้นมาใช้ และวิเคราะห์ข้อมูลความพร้อมในด้านบุคลากรที่ต้องรองรับกับการใช้เทคโนโลยีนั้น รวมทั้งให้เสนอแนะแนวทางสำรองหรือเครื่องมือเทคโนโลยีอื่นที่สามารถนำมาใช้ทดแทน ทั้งนี้ เพื่อให้หน่วยงานงบประมาณและผู้บริหารระดับสูงเห็นถึงความสำคัญและจำเป็นในการลงทุนเพื่อจัดการกับความเสี่ยงจากภัยคุกคามและอาชญากรรมทางไซเบอร์ที่นับวันจะทวีความรุนแรง ซับซ้อน และปรับเปลี่ยนรูปแบบอย่างรวดเร็ว นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะต้องมีการบูรณาการข้อมูล รวมถึงการใช้ทรัพยากรร่วมกันกับหน่วยงานภาครัฐ หน่วยงานกำกับดูแลเอกชน สถาบันการศึกษา และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ CII

**<u>ด้านองค์กร</u>** เนื่องจากมีหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์จำนวนมาก ทั้งในส่วนของภาครัฐ เอกชน และสถาบันการศึกษา อาจขาดความร่วมมือจากหน่วยงาน

ที่เกี่ยวข้อง ทำให้การประสานงานระหว่างหน่วยงานและการทำงานในลักษณะข้ามองค์กรไม่มีประสิทธิภาพเท่าที่ควร ผู้เขียนเห็นว่า แนวทางบริหารจัดการคือ การกำหนดอำนาจหน้าที่แต่ละหน่วยงานให้มีความชัดเจน

**<u>ด้านการเสริมสร้างศักยภาพ</u>** ประชาชนขาดแรงจูงใจและไม่เห็นความสำคัญในการเรียนหลักสูตรเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ แนวทางบริหารจัดการคือ สร้างแรงจูงใจให้ประชาชน เช่น จัดการประกวด application เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ชนะการประกวดจะได้รับเงินรางวัล หรือมีโอกาสเข้าร่วมกิจกรรมกับบริษัท IT ที่มีชื่อเสียง หรือให้โอกาสในการต่อยอดผลิตภัณฑ์ที่ชนะการประกวด หรือการสอบเข้าเรียนหลักสูตรความมั่นคงปลอดภัยไซเบอร์ หากได้คะแนนสูงสุด จะได้เรียนฟรีตลอดหลักสูตร และเมื่อสำเร็จการศึกษาจะมีงานรองรับ ทั้งนี้ หลักสูตรที่ไทยควรให้ความสำคัญในเบื้องต้นอาจเป็นหลักสูตรฝึกอบรมที่ศูนย์ฝึกอบรม อาเซียน – ญี่ปุ่น ได้มีการดำเนินการ ได้แก่

- การฝึกรับมือภัยคุกคามไซเบอร์ด้วยระบบจำลองคอมพิวเตอร์ (CYber Defense Exercise with Recurrence: CYDER)
- การตรวจวิเคราะห์มัลแวร์ (Malware Analysis)
- การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics)

**<u>ด้านความร่วมมือ</u>** ขาดความสนใจจากภาคเอกชนในการร่วมมือกับภาครัฐในการจัดกิจกรรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ แนวทางบริหารจัดการคือ ในการหารือการจัดกิจกรรมร่วมกับภาคเอกชน ภาครัฐควรเน้นให้ภาคเอกชนเห็นถึงความสำคัญและประโยชน์จากความร่วมมือกับภาครัฐ เช่น เป็นการส่งเสริมภาพลักษณ์ขององค์กรในด้านการรับผิดชอบต่อสังคม (Corporate Social Responsibility: CSR)

### 2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

- **การกำหนดวิสัยทัศน์และกลยุทธ์** สามารถคาดการณ์ผลกระทบระยะยาวของทิศทางของประเทศและของโลก รวมถึงนัยยะทางการเมือง เศรษฐกิจ สังคม เทคโนโลยี และสิ่งแวดล้อมที่มีผลต่อทิศทางและภารกิจขององค์กร ตลอดจนสามารถสร้างการมีส่วนร่วมของผู้อื่นในทุกระดับ ในการกำหนดกลยุทธ์ เพื่อรักษาความมุ่งมั่นในการขับเคลื่อนเป้าหมายขององค์กร
- **การพัฒนาตนเองและผู้อื่น และสร้างการมีส่วนร่วมในองค์กร** เพื่อรักษาความมุ่งมั่นในการขับเคลื่อนเป้าหมายขององค์กร เนื่องจากต้องมีการประสานงานกับหน่วยงานอื่นในลักษณะข้ามองค์กร
- **การผลักดันให้เกิดนวัตกรรมและการเปลี่ยนแปลง** แสวงหาโอกาสในการสร้างนวัตกรรมและกล้าที่จะเปลี่ยนแปลงกระบวนการทำงาน เพื่อแสวงหาวิธีการที่จะพัฒนานโยบายและภารกิจให้เข้ากับสภาวะการเปลี่ยนแปลงที่รวดเร็ว โดยเฉพาะอย่างยิ่ง แนวโน้มอาชญากรรมทางไซเบอร์ที่มีการปรับเปลี่ยนรูปแบบรวดเร็วและมีความซับซ้อน

## 3. แผนพัฒนาตนเอง

**(ข้อมูลส่วนบุคคลไม่เผยแพร่)**

# บรรณานุกรม


**หนังสือ**

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ยุทธศาสตร์ชาติ พ.ศ. 2561–2580

แผนปฏิบัติราชการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ระยะ 3 ปี พ.ศ. 2563 – 2565 (ฉบับปรับปรุง พ.ศ. 2564)

แผนปฏิบัติราชการสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ประจำปีงบประมาณ พ.ศ. 2564

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2559.

Cyber Security Agency of Singapore. Singapore Cyber Landscape 2016. Singapore: Cyber Security Agency of Singapore, 2017.

_____. Singapore Cyber Landscape 2017. Singapore: Cyber Security Agency of Singapore, 2018.

_____. Singapore's Cybersecurity Strategy. Singapore: Cyber Security Agency of Singapore, 2016.

International Telecommunication Union. Global Cybersecurity Index & Cyberwellness Profiles. Geneva: International Telecommunication Union, 2015.

_____. Global Cybersecurity Index (GCI) 2017. Geneva: International Telecommunication Union, 2017.

_____. Global Cybersecurity Index (GCI) 2018. Geneva: International Telecommunication Union, 2018.

National Security Council, Prime Minister's Department. Malaysia Cyber Security Strategy 2020 – 2024. Malaysia: Federal Government Administrative Centre.

ThaiCERT, Electronic Transactions Development Agency (Public Organization). Cybersecurity for Critical Information Infrastructure in Thailand. 1st Edition. Bangkok: Thailand Computer Emergency Response Team (ThaiCERT), 2018.

**สื่ออิเล็กทรอนิกส์**

สำนักงานสถิติแห่งชาติ. สรุปผลที่สำคัญ การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2563. [ออนไลน์]. 2564. แหล่งที่มา: www.nso.go.th

ThaiCERT ETDA. สถิติภัยคุกคาม. [ออนไลน์]. 2020. แหล่งที่มา: https://www.thaicert.or.th/.

Committee on the Future Economy. Report of the Committee on the Future Economy: Pioneers of the Next Generation. [Online]. 1997. Available from: https://www.gov.sg/~/media/cfe/downloads/cfe%20report.pdf?la=en.

Cyber Security Agency of Singapore. CSA and Cisco Systems Sign Memorandum of Collaboration to Establish a Framework for Cybersecurity Cooperation. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press-releases/csa-and-cisco-systems-sign-memorandum-of-collaboration-to-establish-a-framework-for-cybersecurity-cooperation.

_____. Cybersecurity Act. [Online]. 2019. Available from: https://www.csa.gov.sg/legislation/cybersecurity-act

_____. Cyber Threats in Singapore Grew in 2017, Mirroring Global Trends. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press-releases/cyber-threats-in-singaporegrew-in-2017-mirooing-global-trends.

_____. GovTech and CSA Partner Cybersecurity Community on Government Bug Bounty Programme. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press–releases/govtech-and-csa-partner-cybersecurity-community-on-government-bug-bounty-programme.

Drew & Napier LLC. Cybersecurity in Singapore. [Online]. 2019. Available from: https://www.todayonline.com/. [29 April 2019].

FTI Consulting. Singapore's Approach to Cyber Security. [Online]. 2016. Available from: www.fticonsulting.com.

Microsoft and Frost & Sullivan. Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in Digital World. [Online]. 2021. Available from https://news.microsoft.com/apac/features/cybersecurity-in-asia.

World Economic Forum. The Global Risks Report 2021. 16th Edition. [Online]. 2021. Available from: www.weforum.org.

Yu Eileen. Singapore now able to certify products under global cybersecurity Standard. [Online]. 2019. Available from: https://www.zdnet.com/article/singapore-now-able-to-certify-global-cybersecurity-standard/.

# ภาคผนวก

**ภาคผนวก 1** ภูมิทัศน์ดิจิทัลของไทยในระยะเวลา 20 ปี

**ภาคผนวก 2** แผนภูมิการเชื่อมโยงยุทธศาสตร์สำนักงานปลัดกระทวงดิจิทัลเพื่อเศรษฐกิจและสังคม

**ภาคผนวก 3** ตัวชี้วัด GCI ของ ITU

| No. | Indicators | Weighing |
|---|---|---|
| 1. | Legal Measures | 0.2 |
| 1.1 | Cybercriminal Legislation | 0.079 |
| 1.2 | Cybersecurity Regulation | 0.079 |
| 1.3 | Containment/curbing of spam legislation | 0.042 |
| 2. | Technical Measures | 0.2 |
| 2.1 | National, Government, Sectorial of CERT/CIRT/CSIRT | 0.065 |
| 2.2 | Cybersecurity Standards Implementation Framework for Organizations | 0.035 |
| 2.3 | Standardization Body | 0.030 |
| 2.4 | Technical mechanisms and capabilities deployed to address spam | 0.024 |
| 2.5 | Use of cloud for cybersecurity purpose | 0.019 |
| 2.6 | Child Online Protection mechanisms | 0.027 |
| 3. | Organizational Measures | 0.2 |
| 3.1 | Strategy | 0.092 |
| 3.2 | Responsible Agency | 0.063 |
| 3.3 | Cybersecurity Metrics | 0.045 |
| 4. | Capacity Building | 0.2 |
| 4.1 | Public Awareness Campaigns | 0.036 |
| 4.2 | Cybersecurity Standards and Certification for Professionals | 0.027 |
| 4.3 | Cybersecurity Professional Training Courses | 0.032 |
| 4.4 | National Education Programs and Academic Curriculums | 0.032 |
| 4.5 | Cybersecurity Research & Development Programs | 0.026 |
| 4.6 | Incentive Mechanisms | 0.024 |
| 4.7 | Home Grown Cybersecurity Industry | 0.023 |
| 5. | Cooperation | 0.2 |
| 5.1 | Bilateral Agreements | 0.038 |
| 5.2 | Multilateral Agreements | 0.038 |
| 5.3 | Participation of international fora/associations | 0.036 |
| 5.4 | Public–private partnership | 0.034 |
| 5.5 | Interagency/intra–agency partnerships | 0.026 |
| 5.6 | Cybersecurity best practices | 0.028 |
| | **Total** | **1** |

ที่มา: Global Cybersecurity Index (GCI) 2018

**ภาคผนวก 4** รายชื่อกฎหมายที่เกี่ยวข้องกับไซเบอร์ของมาเลเซีย

- Criminal Procedure Code
- Sedition Act 1948
- Defamation Act 1957
- Official Secrets Act 1972
- Patents Act 1983
- Direct Sales and Anti-Pyramid Scheme Act 1993
- Digital Signature Act 1997
- Communications and Multimedia Act 1998
- Optical Discs Act 2000
- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001
- Mutual Assistance in Criminal Mattes Act 2002
- Capital Market and Services Act 2007
- Personal Data Protection Act 2010
- Financial Services Act 2013
- Prevention of Terrorism Act 2015
- Penal Code
- Evidence Act 1950
- Prevention of Crime Act 1959
- Trade Marks Act 1976
- Copyright Act 1987
- Computer Crimes Act 1997
- Telemedicine Act 1997
- Consumer Protection Act 1999
- Child Act 2001
- Film Censorship Act 2002
- Electronic Commerce Act 2006
- Electronic Government Activities Act 2007
- Security Offences (Special Measures) Act 2012
- Islamic Financial Services Act 2013
- National Security Council Act 2016
- Sexual Offences Against Children Act 2017

ที่มา: Malaysia Cyber Security Strategy 2020 - 2024

**ประวัติผู้เขียนเอกสารรายงานการศึกษาส่วนบุคคล**

**ชื่อ – สกุล** .....**นางสาวกัลยา ชินาธิวร**.....

**ประวัติการศึกษา**

ปริญญาตรี ศิลปศาสตร์บันทิต (เอกภาษาอังกฤษ)/ มหาวิทยาลัยเชียงใหม่ / สำเร็จการศึกษา ปี พ.ศ. 2532

ปริญญาโท Master of Business (Public Sector Management/ Victoria University of Technology ประเทศออสเตรเลีย / สำเร็จการศึกษา ปี พ.ศ. 2540**)**

**ประสบการณ์การรับราชการ**

| **ประวัติการทำงานและการรับราชการ** | | | |
|---|---|---|---|
| **ชื่อตำแหน่ง** | **สังกัด** | **ช่วงเวลาที่ดำรงตำแหน่ง** | **รวมเวลาดำรงตำแหน่ง** |
| 1. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 3–6) | สำนักงานปลัดกระทรวงคมนาคม (กองกิจการระหว่างประเทศ) | 17 มิ.ย. 34–30 พ.ย. 47 | 13 ปี 5 เดือน |
| 2. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 6) | สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ) | 30 พ.ย. 47–8 พ.ค. 48 | 5 เดือน |
| 3. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 7) | สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ) | 9 พ.ค 48–19 ก.ย. 50 | 2 ปี 3 เดือน |
| 4. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 8 และระดับชำนาญการพิเศษ) | สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ)<br>ปัจจุบันคือกองการต่างประเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | 20 ก.ย. 50–27 ม.ค. 62 | 11 ปี 4 เดือน |

**รางวัลหรือทุนการศึกษา (เฉพาะที่สำคัญ)**

ทุนศึกษาระดับปริญญาโท ทุนรัฐบาลออสเตรเลีย

**ตำแหน่งหน้าที่ปัจจุบันและสถานที่ทำงาน**

ผู้อำนวยการกองการต่างประเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ศูนย์ราชการเฉลิมพระเกียรติ์ 80 พรรษาฯ
อาคารรัฐประศาสนภักดี (อาคารบี) ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210