Cybersecurity Strategy

A Guideline and Recommendations

September 2015

Col.Settapong Malisuwan, Ph.D.

รายงานฉบับนี้เป็นเอกสารไม่มีชั้นความลับ

เนื่องจากแหล่งอ้างอิงทั้งหมด

เป็นเอกสารเปิดเผยต่อสาธารณะ

คำนำ

การเชื่อมโยงประเทศต่างๆ ในโลกด้วยไซเบอร์สเปซ (Cyber Space) มีผลกระทบในด้านความมั่นคงในระดับนานาชาติมากขึ้นเป็นลำดับ จึงทำให้ประเทศต่างๆ หันมาให้ความสนใจในการวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ให้เป็นยุทธศาสตร์ระดับชาติ เพื่อที่จะสามารถใช้ระบบไซเบอร์ในการขับเคลื่อนเศรษฐกิจและสังคมให้เจริญก้าวหน้าด้วยความเสี่ยงที่น้อยที่สุด

ประเทศไทยเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางด้านเทคโนโลยีสื่อสารโทรคมนาคม และมีการใช้งานเป็นลำดับต้นๆ ของประเทศในภูมิภาคอาเซียน จึงปฏิเสธไม่ได้ว่ามีระดับความเสี่ยงในระดับสูงที่ระบบไซเบอร์ของประเทศจะถูกโจมตีและคุกคามจนเกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจ และสังคมของประเทศ

รายงานฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) โดยผลของรายงานฉบับนี้ได้มาจากการศึกษา วิจัยและวิเคราะห์ แนวทางการพัฒนายุทธศาสตร์จากประเทศต่างๆ ทั่วโลก โดยเอกสารเหล่านั้นไม่มีชั้นความลับ เป็นเอกสารเชิงวิชาการเพื่อให้ผู้ศึกษาเอกสารฉบับนี้ได้นำไปประยุกต์ใช้ให้เหมาะสมกับสถานการณ์ของประเทศและวัฒนธรรมขององค์กรต่อไป

พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ
ประธานกรรมการกิจการโทรคมนาคม/
รองประธาน กสทช.

แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(National Cybersecurity Strategy)

พันเอก ดร.เศรษฐพงค์ มะลิสุวรรณ
ประธานกรรมการกิจการโทรคมนาคม
รองประธาน กสทช.

ปัจจุบัน ประชาคมนานาชาติมีความกังวลด้านความมั่นคงปลอดภัยด้านไซเบอร์เป็นอย่างมาก เนื่องจากมีแนวโน้มการก่อความไม่สงบ และการก่อการร้ายโดยใช้ช่องทางไซเบอร์สเปซ (Cyber Space) เป็นช่องทางการปฏิบัติการ ดังนั้น รัฐบาลในทุกประเทศจึงหันมาให้ความสำคัญในการวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น ซึ่งในปัจจุบันพบว่าการดำเนินการโดยภาครัฐฝ่ายเดียวนั้นไม่สามารถที่จะลดความเสี่ยงด้านไซเบอร์ได้อีกต่อไป ความมั่นคงปลอดภัยไซเบอร์นั้นต้องเป็นการปฏิบัติการด้วยความร่วมมือจากฝ่ายต่างๆ ทั้งองค์กรภาครัฐ และเอกชนที่มีหน้าที่รับผิดชอบควบคุม ดูแลระบบโครงสร้างพื้นฐานที่ขับเคลื่อนด้วยระบบไซเบอร์สเปซ

รายงานฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางในการดำเนินการการวางยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติจนไปถึงการบริหารจัดการในระดับองค์กรทั้งแนวคิดทางด้านบริหารจัดการและทางเทคนิค โดยได้อธิบายถึงหลักการพื้นฐาน รวมทั้งข้อเสนอแนะในการจัดทำยุทธศาสตร์ดังกล่าวต่อไป

1. โครงสร้างพื้นฐานสารสนเทศ

จากผลการศึกษาของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ระบุว่า เทคโนโลยีสารสนเทศ และการสื่อสาร (ICTs) เป็นตัวขับเคลื่อนโครงสร้างพื้นฐานที่สำคัญของประเทศต่างๆ ทั่วโลก เช่น ระบบไฟฟ้า, โทรคมนาคม, การเงินการธนาคาร เป็นต้น ซึ่งสามารถเรียกได้ว่าเป็นโครงสร้างพื้นฐานสารสนเทศสำคัญ (Critical Information Infrastructure: CII) หาก CII นั้นมีความเปราะบางในเรื่องความน่าเชื่อถือ และความมั่นใจในความปลอดภัย อาจจะทำให้เกิดผลกระทบต่อการดำเนินชีวิตประจำวันของประชาชน ความมั่นคงทางการค้า และความมั่นคงของชาติได้ จึงทำให้ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่จะต้องถูกยกเป็นประเด็นในระดับยุทธศาสตร์ของชาติในที่สุด เพราะเนื่องจากผลกระทบเป็นวงกว้างมีความซับซ้อน และมีการ

เชื่อมโยงถึงกันระหว่าง CII จึงทำให้ยากต่อการคาดการณ์ผลลัพธ์ที่จะเกิดขึ้นจากการคุกคามทางไซเบอร์ จึงมีความจำเป็นอย่างยิ่งที่รัฐบาลจะต้องมีการดำเนินการโครงการ (Project) หรือ โปรแกรม (Program) เพื่อเป็นการป้องกัน ปกป้องโครงสร้างพื้นฐานสำคัญ (CIIP) ต่อไป

2. วัตถุประสงค์ของยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

ผู้นำของประเทศทุกประเทศควรจะมีมุมมองต่อยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ไปในเชิงส่งเสริมสนับสนุนคุณค่าที่เกิดขึ้นจากการใช้ไซเบอร์สเปซ ไม่ควรคิดไปในเชิงอุปสรรค เพราะระบบเครือข่ายสารสนเทศเป็นเครื่องมือขับเคลื่อนหลักเศรษฐกิจดิจิทัลของประเทศ ดังนั้น วัตถุประสงค์ของยุทธศาสตร์ดังกล่าว จะต้องให้เกิดผลว่าจะทำอย่างไรที่ประเทศจะสามารถใช้ระบบไซเบอร์สเปซเพื่อสร้างความมั่นคงทางเศรษฐกิจและสังคมได้อย่างต่อเนื่อง ด้วยความเสี่ยงที่น้อยที่สุด และสร้างความมั่นใจต่อผู้ใช้ประโยชน์ได้มากที่สุด

ปัจจุบัน มีการเสนอแนวคิดที่สามารถช่วยผู้นำในระดับชาติเพื่อใช้ในการโน้มน้าวให้ผู้เกี่ยวข้องให้เห็นความสำคัญของยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ซึ่งรัฐบาลควรเริ่มต้นด้วยหลักฐานสนับสนุนที่ว่าผู้ที่มีส่วนเกี่ยวข้องทั้งหมดต้องเข้าใจว่าการสนับสนุนของ CII ต่อการส่งมอบบริการนั้นจำเป็นสำหรับชีวิตประจำวันของประชาชน การค้า และความมั่นคงของชาติ แต่ผู้ที่มีส่วนเกี่ยวข้อง อาจขาดทักษะความรู้เกี่ยวกับขั้นตอนที่ต้องปฏิบัติเพื่อเพิ่มความมั่นคงให้กับระบบที่ใช้งานและควบคุมอยู่ ผู้มีส่วนเกี่ยวข้องทุกภาคส่วนอาจต้องการความช่วยเหลือเพื่อให้พวกเขาเข้าใจบทบาทของตนเองในการพัฒนาความมั่นคงปลอดภัยไซเบอร์ เพื่อที่จะส่งเสริมให้ความมั่นคงของชาติโดยรวมมีความมั่นคงปลอดภัยอย่างยั่งยืนต่อไป

3. หลักพื้นฐานสำหรับโครงสร้างยุทธศาสตร์

ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นความท้าทายอย่างหนึ่งในระดับโลก ด้วยเหตุนี้การตอบรับความร่วมมือจากหลายๆ ภาคส่วน ทั้งภายในประเทศ และระหว่างประเทศ จึงเป็นหนทางปฏิบัติที่ดีที่สุด เพื่อสร้างความมั่นใจและความเชื่อมั่นจากประชาชนในการใช้ ICTs แต่เนื่องจากเราไม่มีรัฐบาลกลางของโลก ดังนั้นความพยายามจากทั่วโลกในการลดความเสี่ยงด้านไซเบอร์จึงขึ้นอยู่กับการปฏิบัติการระดับชาติ ที่จะต้องมีความร่วมมือกันทั้งในภูมิภาค และระหว่างภูมิภาคในโลก

จากการเปิดเสรีทางการค้าจึงทำให้อุตสาหกรรมโทรคมนาคมถูกกำกับดูแลด้วยองค์กรอิสระ โดยปราศจากการแทรกแซงจากรัฐบาล แต่ก็ไม่ได้หมายความว่ารัฐบาลจะไม่สามารถควบคุมดูแล และกำหนดทิศทางด้านยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ในระดับชาติได้ ในทางตรงกันข้าม รัฐจะต้องวางกลยุทธ์ กลไก และโครงการที่จะทำให้เกิดความมั่นใจ และคุ้มครองปกป้องทรัพย์สินของประชาชน รัฐต้องเป็นผู้นำในความพยายามที่จะกำหนดเป้าหมายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สร้างโครงการหรือโปรแกรมสำหรับปกป้องโครงสร้างสารสนเทศพื้นฐานสำคัญของชาติอย่างเป็นระบบ เพื่อปกป้องไซเบอร์สเปซจากการคุกคาม อีกทั้งมอบหมายหน้าที่รับผิดชอบต่อผู้ที่มีหน้าที่และผู้มีส่วนได้ส่วนเสียด้วยความเข้าใจและเต็มใจในการให้ความร่วมมือ และปฏิบัติงาน รวมทั้งต้องมีการวิเคราะห์ความเสี่ยงและให้ข้อมูลด้านความเสี่ยง มาตรการป้องกัน และการรับมืออย่างมีประสิทธิภาพ

ดังนั้น หลักพื้นฐานที่สำคัญเพื่อที่จะทำให้ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติบรรลุผล คือ ต้องได้รับความร่วมมือจากทุกส่วนที่เกี่ยวข้อง และรัฐจะต้องมีการควบคุมป้องกันระบบสื่อสารโทรคมนาคมอยู่ในระดับที่สามารถลดความเสี่ยงของความมั่นคง และยังสามารถดำเนินการการใช้งานระบบสื่อสารโทรคมนาคมได้อย่างต่อเนื่อง

4. การสร้างขีดความสามารถทรัพยากรบุคคล

ขีดความสามารถของบุคลากร และสถาบันฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์นั้นมีความสำคัญอย่างยิ่งในการพัฒนาการปกป้องไซเบอร์สเปซที่มีประสิทธิภาพ ถึงแม้ว่าการกำหนดวิสัยทัศน์ แนวทาง วิธีการ และเครื่องมือ หรือทรัพยากร มีความสำคัญมากก็ตาม แต่หากขาดบุคลากรที่มีความสามารถก็จะไม่สามารถปกป้องระบบไซเบอร์สเปซให้มีความมั่นคงได้ ส่วนความร่วมมือ และแลกเปลี่ยนข้อมูลระหว่างองค์กร และบุคคลก็เป็นสิ่งที่มีความสำคัญตามมาเมื่อเราได้ผลิตบุคลากรที่มีความรู้ ความสามารถ และมีคุณธรรม

5. ผู้มีส่วนได้ส่วนเสียด้านความมั่นคงปลอดภัยไซเบอร์

รัฐควรมีส่วนร่วมกับผู้มีส่วนได้เสียทุกภาคส่วนให้มากที่สุดเท่าที่จะทำได้ ในการวางแผนกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างละเอียด นั่นเป็นเพราะไซเบอร์สเปซเข้าถึงกิจกรรมความมั่นคงด้านสังคม เศรษฐกิจ และชาติ ในทุกรูปแบบ การเชื่อมโยงกลุ่มผู้มีส่วนร่วมอย่างกว้างขวางมีความสำคัญด้วยสาเหตุในทางปฏิบัติ อันดับแรก คือช่วยสร้างความมั่นใจให้ผู้ถือ

ประโยชน์ร่วมยอมรับ ผู้ได้รับผลประโยชน์ร่วมมักจะพัฒนาจิตสำนึกของการเป็นเจ้าขององค์กร การสนับสนุนเป็นสิ่งสำคัญในระหว่างการนำกลยุทธ์ไปใช้ ประการต่อมา คือรัฐบาลอาจไม่ได้อยู่ในสถานะที่เหมาะต่อการควบคุมกลยุทธ์ เนื่องจากผู้มีส่วนได้ส่วนเสีย ล้วนเป็นเจ้าของและผู้ปฏิบัติงานด้านโครงสร้างพื้นฐาน ซึ่งปกติแล้วผู้มีส่วนได้ส่วนเสีย โดยส่วนมากมักมีทักษะความสามารถนอกเหนือจากความสามารถหลักของหน่วยงานรัฐ อย่างไรก็ตาม ผู้มีบทบาทจะรู้ว่าควรปฏิบัติงานอย่างไร หน่วยงานที่มักมีบทบาทในการสร้างยุทธศาสตร์ และกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เกิดขึ้น มีดังนี้

5.1) ฝ่ายบริหารของรัฐ

รัฐบาลมีหน้าที่สร้างความเชื่อมั่นด้านความเจริญรุ่งเรืองและความมั่นคงของชาติ รับผิดชอบในการสร้างความมั่นใจให้ด้านความมั่นคงปลอดภัยของชาติทั้งหมด ตามหลักการแล้ว ฝ่ายบริหารระดับรัฐบาลควรปฏิบัติหน้าที่ ดังต่อไปนี้

- ให้คำจำกัดความของบทบาทของไซเบอร์สเปซเพื่อบรรลุเป้าหมายการพัฒนาชาติ
- มีการกำหนด การวิเคราะห์ และการลดความเสี่ยง เพื่อผลประโยชน์ของชาติ
- มีการจัดสรรทรัพยากรแก่โครงการหรือโปรแกรมเพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- มีการพัฒนาการออกกฎหมายอาชญกรรมทางคอมพิวเตอร์ ซึ่งสามารถนำไปใช้และทำงานร่วมกันกับประเทศต่างๆ ได้ทั่วโลก
- การส่งเสริมการพัฒนาเทคโนโลยีด้านความปลอดภัย เช่น เทคโนโลยีการใช้รหัสลับ เป็นต้น
- การจัดการโครงการ หรือโปรแกรมการสร้างความสามารถของบุคคลากรและองค์กร
- การลงนามความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับสัญญาและข้อตกลงระหว่างประเทศ
- การกำหนดบทบาทของความมั่นคงปลอดภัยไซเบอร์ในการประชุมระดับภูมิภาคและระดับโลก

ภาครัฐเป็นผู้ใช้อำนาจ และทำให้เกิดอำนาจนิติบัญญัติและเป็นผู้ออกแบบมาตรการกระตุ้นเศรษฐกิจดิจิทัล เพื่อช่วยสร้างความเชื่อมั่นให้ผู้ได้รับผลประโยชน์ร่วมทั้งหมดยอมรับความรับผิดชอบและใช้มาตรการเพื่อปกป้องไซเบอร์สเปซเพื่อส่วนรวม

5.2) ฝ่ายกฎหมายของรัฐ

หน่วยงานภาครัฐมีบทบาทสำคัญในด้านการสรรหาผู้บริหารที่มีความสามารถ ซึ่งเป็นทรัพยากรที่จำเป็นต่อการดำเนินการให้ไซเบอร์สเปซมีความปลอดภัย มั่นคง และขับเคลื่อนเศรษฐกิจของประเทศ สภานิติบัญญัติแห่งชาติจะต้องออกกฎหมาย เพื่อมั่นใจได้ว่าการป้องกันไซเบอร์สเปซจะไม่ละเมิดค่านิยมของชาติ เช่น สิทธิเสรีภาพในการแสดงออก เป็นต้น

5.3) ผู้ควบคุมโครงสร้างพื้นฐานสำคัญ

ผู้ควบคุมโครงสร้างพื้นฐาน ควรมีส่วนในการรับผิดชอบเพื่อลงรายละเอียดเกี่ยวกับกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เนื่องจากผลประโยชน์ทางเศรษฐกิจโดยตรงที่พวกเขาได้รับจากความสำเร็จของโครงการหรือโปรแกรมเพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รัฐอาจวางมาตรการทางกฎหมายและกฎระเบียบเพื่อให้เกิดการยอมรับ ตามข้อกำหนดของความมั่นคงปลอดภัยไซเบอร์ การเข้ามามีส่วนร่วมของผู้ควบคุมโครงสร้างพื้นฐานสำคัญ จะทำประโยชน์ให้แก่ประเทศชาติได้ในระยะยาว เจ้าของและผู้ควบคุมโครงสร้างพื้นฐานสำคัญมีบทบาทในการวางแผนรายละเอียดในระดับกลยุทธ์ ดังต่อไปนี้

- ให้รายละเอียดเชิงลึกว่าภัยคุกคาม และความไม่มั่นคงทางไซเบอร์ ส่งผลกระทบต่ออุตสาหกรรมอย่างไร
- ให้ข้อมูลว่าความไม่มั่นคงทางไซเบอร์ ส่งผลกระทบต่อระบบและซอฟต์แวร์ที่ใช้งานอยู่อย่างไร
- แลกเปลี่ยนความรู้จากการปฏิบัติงานจริง ผ่านประสบการณ์การรักษาความปลอดภัยในการปฏิบัติงาน
- แลกเปลี่ยน แบ่งปันทักษะความรู้ความเชี่ยวชาญ ด้านเครือข่าย ระบบ อุปกรณ์อำนวยความสะดวกโปรแกรมประยุกต์ และการทำงานด้านไซเบอร์
- นำเสนอวิธีรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสมดุลกันระหว่างประสิทธิภาพการควบคุมและผลประโยชน์ที่ได้รับ

- มีส่วนช่วยในด้านความเชี่ยวชาญและประสบการณ์การรับมือกับเหตุการณ์ไม่คาดคิด

5.4) การบังคับใช้กฎหมาย

คณะทำงานด้านกฎหมายที่ทำหน้าที่บังคับใช้กฎหมายอาชญากรรมคอมพิวเตอร์ ควรมีส่วนร่วมในการวางแผนรายละเอียดของยุทธศาสตร์และกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติด้วยเหตุผลหลายประการ เหตุผลประการแรกคือ การบังคับใช้กฎหมายสามารถตรวจสอบความถูกต้องของการบังคับใช้กรอบการดำเนินงานด้านอาชญกรรมคอมพิวเตอร์ตามที่วางแผนไว้ เหตุผลประการที่สองคือ คณะทำงานสามารถแนะนำเกี่ยวกับกฎเกณฑ์การตรวจสอบอาชญากรรมคอมพิวเตอร์ทั้งในปัจจุบันและอนาคต ประการที่สาม การบังคับใช้กฎหมายอาจทำให้ได้รับความคิดเห็นด้านการจัดการความร่วมมือระดับนานาชาติด้านอาชญากรรมคอมพิวเตอร์ คณะทำงานด้านการบังคับใช้กฎหมาย จะเป็นผู้มีส่วนร่วมกับองค์กรต่างๆ เช่น Interpol และ Virtual Global Taskforce (VGT)

5.5) ประชาคมด้านข่าวกรอง

เพื่อความพร้อม เราควรตระหนักไว้ว่าองค์กรด้านข่าวกรองมีบทบาทอย่างยิ่งในการวางแผนและการดำเนินการด้านกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์ โดยองค์กรด้านข่าวกรองจะต้องมีความเชี่ยวชาญในการเฝ้าระวังตรวจสอบเครือข่ายโทรคมนาคม เราควรตระหนักว่าความสัมพันธ์ขององค์กรด้านข่าวกรองต่างๆ มีการถ่วงดุลและความขัดแย้งกัน หลายประเทศมีการแบ่งแยกระหว่างเครือข่ายพลเรือนและเครือข่ายทหาร ดังนั้น การรวมองค์กรข่าวกรองไว้ในการวางแผนกลยุทธ์อาจทำให้เกิดอุปสรรคในการดำเนินการอยู่บ้าง และอาจเกิดปัญหาในการถกเถียงกันในประเด็นด้านเสรีภาพของประชาชน

5.6) ผู้จำหน่ายอุปกรณ์

ผู้จำหน่ายอุปกรณ์ หรือ vendor ควรเข้าร่วมในกระบวนการการวางแผนรายละเอียดด้านกลยุทธ์ด้วย เนื่องจากผู้จำหน่ายอุปกรณ์ทำหน้าที่ออกแบบมาตรการทางเทคนิคที่จำเป็นต่อการหลีกเลี่ยง การป้องกัน การยับยั้ง และการฟื้นฟูจากภัยคุกคามไซเบอร์ การกีดกันไม่ให้ผู้จำหน่ายอุปกรณ์เข้ามามีส่วนร่วมกับกระบวนการนี้ อาจจะทำให้ประเทศชาติสูญเสียความคิดเห็นที่เป็นส่วนสำคัญจากภายนอก ซึ่งความคิดเห็นเหล่านี้สามารถเป็นแหล่งข้อมูลหรือเป็นแนวทาง

สำหรับแก้ปัญหาภัยคุกคามและความไม่มั่นคงทางไซเบอร์ได้ โดยบทบาทของผู้จำหน่ายอุปกรณ์มีดังนี้

- ให้ข้อมูลความไม่มั่นคงทางไซเบอร์ที่ส่งผลกระทบแก่ระบบและซอฟต์แวร์ของพวกเขาอย่างไร
- ให้ข้อมูลเชิงลึกด้านความสามารถในการออกแบบ การจัดการ และปกป้องอุปกรณ์และเครื่องมือด้านความปลอดภัย
- ทำให้ความสามารถด้านการตรวจจับภัยคุกคามไซเบอร์เป็นรูปธรรมมากขึ้น
- แลกเปลี่ยนประสบการณ์ทางเทคนิค ในการรับมือกับเหตุการณ์ต่างๆ ที่เกิดขึ้น
- สร้างขีดความสามารถเพื่อกำหนดวิธีการแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์ทางด้านเทคนิค

5.7) สถาบันทางวิชาการ

สถาบันทางวิชาการ ควรมีบทบาทในการวางแผนรายละเอียดของกลยุทธ์ด้วยเหตุผลดังนี้ 1) สถาบันทางวิชาการเป็นผู้ให้ความรู้กับผู้เชี่ยวชาญทางเทคนิค การจัดการ และปกป้องข้อมูล ซึ่งเป็นที่ต้องการเพื่อการคิดค้นและดำเนินการจัดการกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์ 2) กลุ่มทางวิชาการ มีส่วนร่วมเป็นผู้จัดตั้งศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ และ 3) กลุ่มทางวิชาการ ทำให้เกิดการศึกษา วิจัย ค้นคว้า และการพัฒนาการแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์

5.8) องค์กรความร่วมมือระหว่างประเทศ

ควรมีการพิจารณาในการขอให้พันธมิตรและองค์กรความร่วมมือระหว่างประเทศ เข้ามามีส่วนร่วมในการวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยการร่วมมือกันนั้นมีความสำคัญ เนื่องจาก ทุกคนทุกส่วนพึ่งพาไซเบอร์สเปซเดียวกัน ดังนั้นความไม่มั่นคงในองค์กรหนึ่งหรือประเทศหนึ่ง อาจส่งผลกระทบต่อประเทศอื่นๆ ที่มีความเชื่อมโยงกันในด้านเศรษฐกิจและความมั่นคงของชาติด้วย อย่างไรก็ตาม ความมั่นคงด้านเศรษฐกิจ การเมือง และประเทศชาติที่เกี่ยวข้องกับความร่วมมือกันระหว่างรัฐบาลกับต่างประเทศ อาจเกิดความกังวลในเรื่องความลับและอาจจะเป็นศัตรูกันในอนาคตก็เป็นได้ รัฐบาลอาจลดความกังวลนั้นโดยลงนามข้อตกลงด้าน

ความร่วมมือ (MOU) เพื่อการร่วมมือกันเฉพาะด้าน เช่น มาตรการทางกฎหมาย การรับมือกับเหตุการณ์ฉุกเฉิน การวิจัย และการพัฒนา เป็นต้น

5.9) ประชาชน

ประชาชน มีความสำคัญมากสำหรับการสร้างยุทธศาสตร์และกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะต้องปรับตามเสียงของประชาชนเท่าที่ทำได้ ไซเบอร์สเปซเป็นสิ่งจำเป็นสำหรับวิถีชีวิตยุคใหม่ เช่น การติดต่อสื่อสารระหว่างบุคคล การรวมกลุ่มสังคม การทำธุรกรรมการเงิน และเรียนรู้ผ่านอินเทอร์เน็ต เป็นต้น ดังนั้นประชาชนถือเป็นผู้มีส่วนหลักในการดำเนินงาน อย่างไรก็ตามประชาชนอาจไม่สามารถส่งเสริมกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ หากกลยุทธ์นี้ได้รับการจัดให้อยู่เหนือสิทธิพื้นฐาน เช่น ความเป็นส่วนตัว อาจเป็นไปไม่ได้ที่จะได้รับการสนับสนุนจากประชาชนโดยตรง ดังนั้น ระบบรัฐสภาและองค์กรภาคประชาสังคมอาจเป็นผู้เสนอความเห็นของประชาชนในลักษณะตัวแทนของประชาชนได้

6. กระบวนการและขั้นตอนการวางแผน

เพื่อให้การวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ เป็นที่เข้าใจตรงกันของทุกฝ่ายที่เกี่ยวข้อง จึงมีความจำเป็นที่จะต้องกำหนดกระบวนการการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน เพื่อความง่ายเราจะกำหนดกระบวนการดังกล่าวเป็นขั้นๆ ดังนี้

Stage 0 - Cybersecurity Strategy Driver

Stage 1 - Direct and Coordinate Elaboration

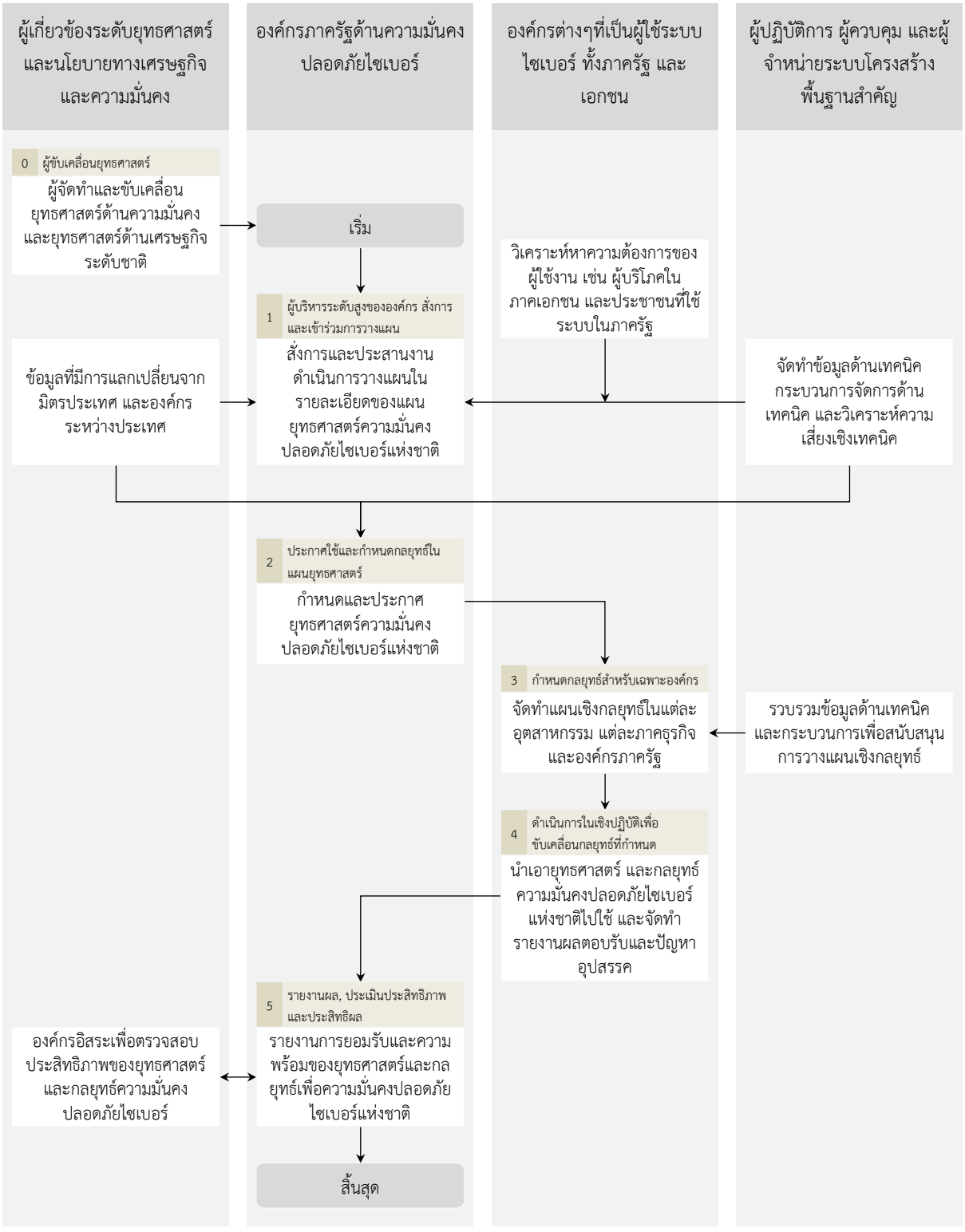
Stage 2 - Define and Issue Strategy

Stage 3 - Sector Strategies

Stage 4 - Implement Cybersecurity Strategy

Stage 5 - Report on Compliance and Efficacy

กระบวนการพัฒนายุทธศาสตร์และกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



7. กรณีศึกษากรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ของ NIST

กรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา หรือ The Nationals Institute of Standards and Technology (NIST) สามารถนำมาปรับใช้ให้เข้ากับวัฒนธรรมองค์กรและนโยบายของประเทศต่างๆ ได้ ดังนั้นในบทความนี้จึงขอยกการดำเนินการพัฒนายุทธศาสตร์เพื่อความมั่นคงปลอดภัยไซเบอร์ของ NIST เป็นกรอบตั้งต้นในการทำความเข้าใจเพื่อให้เกิดความรู้พื้นฐานที่ตรงกันต่อไป

กรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ที่ร่างโดยสถาบันมาตรฐานและเทคโนโลยี (NIST) กระทรวงพาณิชย์ สหรัฐอเมริกา นั้น เป็นการกำหนดนโยบายเกี่ยวกับความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญ ซึ่งกรอบการดำเนินงานนี้ไม่ได้เป็นการเพิ่มมาตรฐานหรือแนวคิดใหม่ ในทางตรงข้ามกลับเป็นการผลักดันและผสมผสานแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมชั้นนำที่ได้รับการพัฒนาจากองค์กรต่างๆ เช่น NIST และองค์การระหว่างประเทศว่าด้วยเรื่องมาตรฐาน (ISO)

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์นี้ เป็นผลมาจากคำสั่ง Executive Order ของประธานธิบดีสหรัฐอเมริกา ในเดือนกุมภาพันธ์ พ.ศ.2556 ที่ชื่อว่า “Improving Critical Infrastructure Cybersecurity” หรือ “การพัฒนาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ” ระยะเวลา 10 เดือนที่มีการปรึกษาหารือร่วมกันจากผู้เชี่ยวชาญด้านความปลอดภัยมากกว่า 3,000 คน รวมถึงการรวบรวมแนวทางความเสี่ยงที่อาจเกิดขึ้น จะสามารถช่วยองค์กรต่างๆ ในการระบุ จัดเตรียม และพัฒนาแนวปฏิบัติสำหรับความมั่นคงปลอดภัยไซเบอร์ให้สำเร็จ และยังสร้างภาษากลางสำหรับการสื่อสารกันทั้งภายในและระหว่างองค์กรเกี่ยวกับประเด็นความมั่นคงปลอดภัยไซเบอร์อีกด้วย

กรอบการดำเนินงานนี้เป็นกระบวนการแบบวนซ้ำ ซึ่งถูกออกแบบมาเพื่อพัฒนาแบบค่อยเป็นค่อยไป พร้อมๆ กับการเปลี่ยนแปลงรูปแบบภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ กระบวนการ และเทคโนโลยี ซึ่งจะมีการปรับปรุงเป็นระยะจากบทเรียนต่างๆ ที่ได้รับ และผลตอบรับจากภาคอุตสาหกรรม โดยที่กรอบการดำเนินงานนี้มองความมั่นคงปลอดภัยไซเบอร์ที่มีการพัฒนาอย่างมีประสิทธิภาพ จะต้องมีการพัฒนาปรับปรุงยุทธศาสตร์ และกลยุทธ์ในลักษณะวงจรพลวัตแบบต่อเนื่องที่มีทั้งการรับมือจากภัยคุมคามและมีแนวทางการแก้ปัญหาอีกด้วย

ในกรอบการดำเนินงานนี้มีกลไกในการประเมิน ซึ่งทำให้องค์กรต่างๆ ทั้งภาครัฐและเอกชนสามารถกำหนดขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในปัจจุบันได้ สามารถกำหนดจุดมุ่งหมายของอุตสาหกรรม และสร้างแผนสำหรับการปรับปรุงแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งกรอบการดำเนินงานนี้ในเบื้องต้นได้นำเสนอโดยหยิบยกมาตรฐาน NIST ซึ่งกระทรวงแห่งความมั่นคงมาตุภูมิ ของประเทศสหรัฐอเมริกานำไปใช้ ประกอบด้วย 3 องค์ประกอบหลัก ได้แก่ ข้อมูลโดยรวม (Profile), ระดับชั้นการบริหารจัดการ (Implementation Tiers) และโครงสร้างหลัก (Core)

โครงสร้างพื้นฐานสำคัญที่มีผลต่อความมั่นคงปลอดภัยไซเบอร์ ครอบคลุม 16 กลุ่มที่สำคัญ ดังนี้

1) กลุ่มอุตสาหกรรมเคมีภัณฑ์ Chemical Sector
2) ภาคการพาณิชย์ Commercial Facilities Sector
3) ภาคอุตสาหกรรมโทรคมนาคมสื่อสาร Communications Sector
4) ภาคอุตสาหกรรมการผลิตที่สำคัญ Critical Manufacturing Sector
5) เขื่อน Dams Sector
6) การป้องกันฐานอุตสาหกรรม Defense Industrial Base Sector
7) บริการช่วยเหลือในภาวะฉุกเฉิน Emergency Services Sector
8) ภาคส่วนพลังงาน Energy Sector
9) บริการทางด้านการเงิน Financial Services Sector
10) อุตสาหกรรมอาหารและการเกษตร Food and Agriculture Sector
11) การอำยวนความสะดวกภาครัฐ Government Facilities Sector
12) บริการดูแลสุขภาพและการสาธารณสุข Healthcare and Public Health Sector
13) เทคโนโลยีสารสนเทศ Information Technology Sector
14) อุตสาหกรรมเกี่ยวกับนิวเคลียร์ วัตถุดิบและปฏิกูล Nuclear Reactors, Materials, and Waste Sector
15) ระบบขนส่ง Transportation Systems Sector
16) น้ำและระบบกำจัดน้ำเสีย Water and Wastewater Systems Sector

กรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์เป็นการรวบรวมแนวทางตามความเสี่ยง ที่ได้รับการออกแบบเพื่อช่วยให้องค์กรต่างๆ สามารถประเมินขีดความสามารถในปัจจุบันและร่างแผนยุทธศาสตร์สำคัญเกี่ยวกับแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการปรับปรุงแล้ว

ส่วนประกอบด้านข้อมูลโดยรวม (Profile) มีไว้เพื่อทำให้องค์กรต่างๆ สามารถกำหนดตำแหน่งและปรับปรุงแก้ไขแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมตามความต้องการของแต่ละธุรกิจ ต้านทานต่อความเสี่ยง และสามารถจัดการทรัพยากรที่มีอยู่ได้ ซึ่งในแต่ละองค์กรจะต้องสร้างข้อมูลโดยรวม (Profile) ในปัจจุบัน โดยการประเมินโปรแกรมที่มีอยู่เดิมเทียบกับแนวปฏิบัติที่แนะนำในโครงสร้างหลักของกรอบแนวคิดนี้ (Core) โดยแนวปฏิบัตินี้ประกอบด้วยกระบวนการ วิธีดำเนินการ และเทคโนโลยี เช่น การจัดการสินทรัพย์ให้เป็นไปตามแนวทางของกลยุทธ์ทางธุรกิจ การประเมินความเสี่ยง การควบคุมการเข้าถึง การฝึกอบรมพนักงาน ความปลอดภัยของข้อมูล การบันทึกการใช้งานและวิเคราะห์เหตุการณ์ต่างๆ และแผนในการรับมือกับสถานการณ์ต่างๆ เป็นต้น

การระบุกลุ่มเป้าหมายของข้อมูลโดยรวม องค์กรจะใช้เกณฑ์ของโครงสร้างหลักเดียวกันในการกำหนดผลลัพธ์ที่จำเป็น สำหรับการพัฒนาปรับปรุงลักษณะความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยข้อกำหนดเฉพาะของอุตสาหกรรม ลูกค้า และพันธมิตรทางธุรกิจ ถือเป็นปัจจัยในการกำหนดกลุ่มเป้าหมายข้อมูลโดยรวมเช่นกัน เมื่อเตรียมกลุ่มเป้าหมายข้อมูลโดยรวมเรียบร้อยแล้ว การเปรียบเทียบระหว่างข้อมูลโดยรวมปัจจุบันและข้อมูลที่องค์กรควรจะมีไว้เพื่อความมั่นคงปลอดภัยที่พอเพียง จะทำให้เห็นช่องโหว่ที่ควรจะแก้ไข เพื่อนำมาปรับปรุงความมั่นคงปลอดภัยไซเบอร์และวางรากฐานแผนกลยุทธ์สำคัญที่ช่วยให้การพัฒนานี้ให้ประสบความสำเร็จ ซึ่งการดำเนินการนี้คล้ายกับการวิเคราะห์ Gap Analysis

ระดับการบริหารจัดการ (Implementation Tiers) ช่วยสร้างสภาพแวดล้อมที่ทำให้องค์กรเข้าใจว่าขีดความสามารถในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันขององค์กรแตกต่างกับคุณลักษณะที่อธิบายไว้ในกรอบการดำเนินการอย่างไร โดยการกำหนดขอบเขตจากระดับย่อย (ระดับ 1) สู่ระดับการปรับตัว (ระดับ 4) ดังตารางที่ 1 สถาบัน NIST ได้แนะนำให้องค์กรจัดเตรียมการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่มี

ประสิทธิภาพ และสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ และสามารถก้าวเข้าสูระดับ 3 หรือระดับ 4 ได้สำเร็จ

ตารางที่ 1 ระดับขั้นของการพัฒนาความมั่นคงปลอดภัยไซเบอร์

ระดับ 1	ระดับย่อย	การบริหารจัดการความเสี่ยงเป็นแบบเฉพาะกิจ ด้วยข้อจำกัดในการรับรู้ความเสี่ยง และยังไม่มีความร่วมมือกับภาคส่วนอื่น
ระดับ 2	รับทราบความเสี่ยง	มีขั้นตอนและแนวทางจัดการความเสี่ยง แต่ยังไม่ได้นำไปใช้ครอบคลุมทั่วทั้งองค์กร องค์กรมีความเข้าใจการประสานงานและความร่วมมือ แต่ยังขาดความสามารถในการปฏิบัติ
ระดับ 3	ทำซ้ำ	มีการใช้นโยบายการปฏิบัติสำหรับกระบวนการและแนวทางจัดการความเสี่ยงในองค์กร พร้อมกับเริ่มมีความร่วมมือกับองค์กรภายนอกแล้วในบางส่วน
ระดับ 4	ปรับตัว	กระบวนการและแนวทางจัดการความเสี่ยง เป็นพื้นฐานมาจากบทเรียนที่ได้รับ และจากการปลูกฝังทางวัฒนธรรม พร้อมกับมีการร่วมมือกันในเชิงรุก

โครงสร้างหลักของกรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) นี้ เป็นตัวกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ผลลัพธ์ที่เกิดขึ้น และเป็นกรอบอ้างอิงที่สามารถนำไปใช้งานได้ และมีกิจกรรมพื้นฐานที่ต่อเนื่องกัน สามารถแบ่งย่อยได้ 5 กิจกรรมหลัก ได้แก่ การกำหนด การป้องกัน การตรวจจับ การรับมือ และการคืนสภาพ (ตารางที่ 2) โดยโครงสร้างหลักของกรอบการดำเนินงานอธิบายวงจรต่อเนื่องของกระบวนการทางธุรกิจซึ่งทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

ตารางที่ 2 โครงสร้างหลัก 5 ประการ ของความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

ฟังก์ชั่น	ความหมาย	หมวดหมู่
การกำหนด	การศึกษา ทำความเข้าใจวิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ	การจัดการทรัพย์สิน สภาพแวดล้อมทางธุรกิจ การดำเนินงานภาครัฐ การประเมินความเสี่ยง กลยุทธ์การจัดการความเสี่ยง
การป้องกัน	ควบคุม และดำเนินงานตามมาตรการป้องกันที่เหมาะสม เพื่อป้องกันหรือจำกัดระดับของภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์	การควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล กระบวนการป้องกันข้อมูล การดูแลรักษา เทคโนโลยีที่ใช้ในป้องกัน

การตรวจจับ	การเฝ้าระวัง หรือมีการตรวจสอบติดตามอย่างต่อเนื่องเพื่อการเตือนภัยกับเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันที และสามารถควบคุมสถานการณ์ได้	ความผิดปกติและเหตุการณ์ต่างๆ การสังเกตการณ์อย่างต่อเนื่อง และกระบวนการตรวจสอบ
การรับมือ	กิจกรรมการรับมือกับเหตุการณ์ต่างๆ ที่เกิดขึ้น	การวางแผนรับมือ การสื่อการ การวิเคราะห์ การลดความเสี่ยง และปรับปรุงแก้ไข
การคืนสภาพ	แผนความต่อเนื่องทางธุรกิจเพื่อรองรับการดำเนินงานต่อเนื่อง แผนการกู้คืนขีดความสามารถภายหลังจากการโดนคุกคามทางไซเบอร์	การวางแผนฟื้นฟู การปรับปรุง การสื่อสาร

8. บทบาทและกระบวนทัศน์ของคณะกรรมการและฝ่ายบริหารระดับสูง

การสื่อสารองค์กรและการกำหนดทิศทางจากคณะกรรมการบอร์ด และฝ่ายบริหารระดับสูง เป็นจุดเริ่มต้นของการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ คณะกรรมการบอร์ดต้องมีความชัดเจนในเรื่อง ทิศทางและนโยบายต่อฝ่ายบริหารระดับสูงอย่างชัดเจนเสียก่อน ก่อนที่จะเริ่มกระบวนการในการวางยุทธศาสตร์และกลยุทธ์การสื่อสารนั้นไม่ใช่แค่เพียงมีความถี่ที่สม่ำเสมอเท่านั้น แต่ยังต้องมีการพัฒนาการสื่อสารที่มีประสิทธิภาพและเหมาะสมกับวัฒนธรรมองค์กรอีกด้วย องค์ประกอบของบทบาทและกระบวนทัศน์ของคณะกรรมการบอร์ด และฝ่ายบริหารระดับสูงมีดังนี้ (แสดงดังรูปที่ 1)

รูปที่ 1 กระบวนทัศน์ของคณะกรรมการบอร์ด และฝ่ายบริหารระดับสูง

1) ความเป็นผู้นำ (Leadership)

การแสดงถึงความเป็นผู้นำที่ชัดเจนที่จะต้องแสดงถึงเจตนาที่มุ่งมั่นในการให้ความสำคัญต่อความมั่นคงปลอดภัยไซเบอร์ และสามารถแปลงความหมายความเสี่ยงขององค์กรให้บุคลากรเข้าใจในทิศทางเดียวกัน และมีความตระหนักรู้ในการร่วมกันในการวางแผนต่อไป

2) ปัจจัยด้านบุคลากร (Human Factors)

การปรับเปลี่ยนวิธีคิดและความเชื่อ รวมทั้งวัฒนธรรมองค์กรให้สอดคล้องกับยุทธศาสตร์ โดยต้องโน้มน้าวให้บุคลากรมีความเต็มใจ และเข้าร่วมกับฝ่ายบริหารในการดำเนินการอีกทั้งต้องมีความระมัดระวังในประเด็นสิทธิเสรีภาพทางไซเบอร์ของบุคคลากรด้วย

3) การบริหารความเสี่ยงด้านข้อมูล (Information Risk Management)

มีการบริหารความเสี่ยงด้านข้อมูลอย่างมีประสิทธิภาพทั่วทั้งองค์กร และสามารถส่งผ่านข้อมูลด้วยมาตรการที่ลดและควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

4) การดำเนินการทางธุรกิจอย่างต่อเนื่องและการบริหารในสภาวะวิกฤต (Business Continuity and Crisis Management)

มีการเตรียมการในด้านความปลอดภัย และมีความสามารถในการป้องกันและลดผลกระทบ เมื่อเกิดภาวะวิกฤตให้แก่องค์กร และให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholder) ขององค์กร จึงจะทำให้องค์กรสามารถดำเนินธุรกิจได้ต่อเนื่องไม่หยุดชะงัก

5) กระบวนการดำเนินงานและเทคโนโลยี (Operations and Technology)

มีมาตรการควบคุมในระดับปฏิบัติการและมีเทคโนโลยีที่อยู่ในระดับที่ทำให้องค์กรสามารถตรวจสอบและระบุความเสี่ยงได้ และสามารถลดผลกระทบจากภัยคุกคามได้อย่างมีประสิทธิภาพ

6) กฎหมายและการกำกับดูแล (Legal and Compliance)

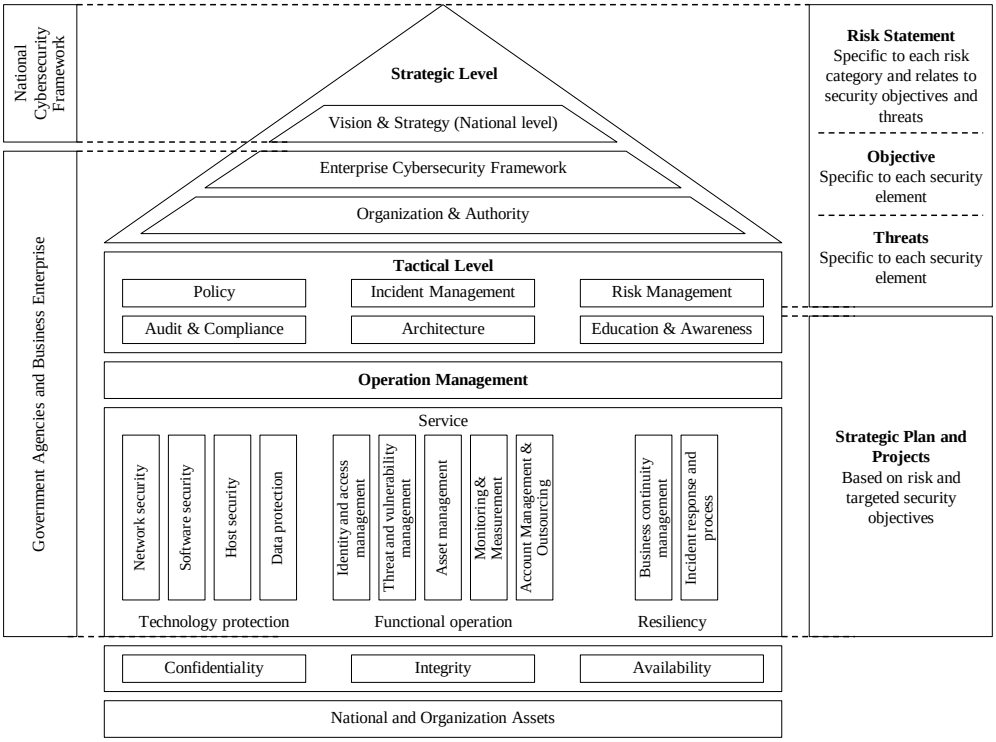
การกำกับดูแล และมาตรฐานระดับสากลเป็นสิ่งที่มีความจำเป็นเพื่อให้เกิดความมั่นใจและเกิดความเชื่อมั่นให้แก่บุคคลากร และองค์กรภายนอก

9. แนวทางการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ผลจากการศึกษาของรายงานฉบับนี้ สรุปได้ว่าควรนำกรอบการดำเนินงานการบริหารจัดการโครงการด้านไซเบอร์ (Cyber Program Management: CPM) ของ ITU มาใช้เป็นข้อมูล

อ้างอิงสำหรับการสร้างกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งพื้นฐานของกรอบการดำเนินงานของ ITU นี้ถูกนำมาใช้ในการพิจารณาบทบาทของการรักษาความปลอดภัยของข้อมูล, เทคโนโลยีสารสนเทศในธุรกิจ และกระบวนการของภาครัฐ ซึ่งอาจมีข้อมูลสำคัญรั่วไหลออกมา และมีความเสี่ยงในการจัดการโครงสร้างภายใต้การคุกคามทางไซเบอร์ ดังนั้นจึงควรมีการจัดลำดับความสำคัญเชิงยุทธศาสตร์และวัตถุประสงค์ขององค์กรอย่างชัดเจน ทั้งองค์กรธุรกิจและหน่วยงานภาครัฐ

รายงานฉบับนี้เสนอให้นำกรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework) ร่วมกับเครื่องมือที่ใช้ในการบริหารความเสี่ยงด้านข้อมูล ดังแสดงในรูปที่ 2



รูปที่ 2 Integrated Cybersecurity Framework

กรอบการดำเนินงานดังรูปที่ 2 นี้ แสดงให้เห็นถึงผู้มีส่วนได้ส่วนเสียทุกภาคส่วนไว้อย่างชัดเจน ในการสร้างแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่มีความยืดหยุ่น สามารถนำมาปรับใช้ในองค์กรทุกขนาดได้อย่างมีประสิทธิภาพ ดังนั้นผู้เขียนจึงขอสรุปประเด็นสำคัญในการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีกรอบการดำเนินงาน ที่ประกอบด้วยประเด็นต่างๆ ดังต่อไปนี้:

1) ในการบูรณาการยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ จะต้องพิจารณาบทบาทของผู้มีส่วนได้เสียทั้งหมด โดยกรอบการดำเนินงานจะต้องถูกสร้างขึ้นโดยอาศัยความร่วมมือระหว่างภาคอุตสาหกรรมและรัฐบาล ซึ่งต้องมีมาตรฐานในการดำเนินการและมาตรฐานที่เฉพาะเจาะจง แนวทางและวิธีปฏิบัติในการส่งเสริมความมั่นคงของชาติ โดยกรอบการดำเนินงานจะต้องมีการสร้างแนวทางเพื่อทำความเข้าใจถึงภัยคุกคาม และมีแนวทางสำหรับการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์โดยเฉพาะ ซึ่งเป็นการช่วยให้ทุกภาคส่วนสามารถจัดลำดับความสำคัญและดำเนินการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่สำคัญได้รวดเร็วและมีความเหมาะสมมากขึ้น

2) องค์ประกอบของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ สามารถจำแนกได้เป็น 5 ขั้นตอน ได้แก่ การระบุ (Identify), การป้องกัน (Protect), การตรวจสอบ (Detect), การตอบสนอง (Respond) และการคืนสภาพ (Recover) ซึ่งช่วยในการเรียนรู้ถึงความเสี่ยงทางไซเบอร์ที่เกิดขึ้นได้ โดยสามารถจัดระเบียบข้อมูล เพื่อช่วยในการตัดสินใจเกี่ยวกับการบริหารความเสี่ยง และการบริหารและการบรรเทาผลกระทบของภัยคุกคาม จากการเรียนรู้และการพัฒนาจากประสบการณ์ในอดีตที่ผ่านมา

3) กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ จะต้องกำหนดให้เป็นภาษากลางที่เข้าใจง่าย เพื่อให้เกิดความสอดคล้องตรงกัน ทั้งในเรื่องความเข้าใจ การจัดการ และความเสี่ยงทางไซเบอร์ทั้งภายในและภายนอกองค์กร โดยกรอบการดำเนินงานนี้สามารถช่วยกำหนดและจัดลำดับความสำคัญสำหรับการดำเนินการเพื่อลดความเสี่ยงด้านความปลอดภัยไซเบอร์ และเป็นเครื่องมือสำหรับการปรับนโยบาย กระบวนการทางธุรกิจ และวิธีการทางเทคนิคเพื่อการจัดการความเสี่ยงทางไซเบอร์

4) กรอบการดำเนินงานนี้จะเป็นแนวทางให้องค์กรธุรกิจและภาครัฐ สามารถทำความเข้าใจในการปฏิบัติงานและการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีความสอดคล้องกับความต้องการในองค์กรแต่ละองค์กร อย่างไรก็ตามกรอบการดำเนินงานอาจมีแนวปฏิบัติด้านการรักษาความปลอดภัยที่ไม่ได้เหมาะสมกับองค์กรทุกองค์กร แต่ถือเป็นจุดเริ่มต้นที่ดีในการดำเนินงานด้านความปลอดภัยไซเบอร์สำหรับทุกองค์กร โดยกรอบการดำเนินงานนี้ถูกสร้างมาเพื่อกำหนดทิศทางแก่องค์กรธุรกิจและภาครัฐ ซึ่งไม่ได้เป็นการกำหนดเพื่อให้เหมาะสมกับทุกองค์กร ซึ่งในบางองค์กรอาจมีแนวทางการปฏิบัติงานด้านการรักษาความปลอดภัยโดยเฉพาะขององค์กรที่แตกต่างจากองค์กรอื่นๆ

5) กรอบการดำเนินงานนี้ มีวิธีการคิดและการพัฒนาแนวทางดำเนินงานในการบริหารจัดการโครงการด้านไซเบอร์ภายในองค์กร ซึ่งไม่ได้เป็นการแก้ปัญหาด้านความปลอดภัยไซเบอร์ แต่เป็นการวิเคราะห์จุดแข็งจุดอ่อนของการดำเนินงาน (GAP analysis)

6) การพัฒนาของกรอบการดำเนินงานนี้ เป็นการบูรณาการหลักการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ และมาตรฐานการบริหารความเสี่ยงซึ่งรวมถึงมาตรฐาน the NIST SP 800 series, COBIT, ISO/IEC และ the Critical Security Controls (CSC) เป็นต้น อย่างไรก็ตามโดยทั่วไปภัยคุกคามทางไซเบอร์จะมีการเปลี่ยนแปลงอยู่เสมอ หรืออาจจะมีความรุนแรงเพิ่มขึ้นหรือลดลง ซึ่งในบทความนี้ ผู้เขียนได้พัฒนาและปรับปรุงกรอบการดำเนินงานภายใต้ความคิดเห็นที่ได้จากอุตสาหกรรมที่มีการนำกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์นี้ไปใช้ และในฐานะที่กรอบการดำเนินงานนี้เป็นแนวทางนำไปสู่การปฏิบัติ ดังนั้นสิ่งที่ได้รับจากการปฏิบัตินั้นจะถูกนำมาบูรณาการเข้ากับกรอบการดำเนินการใหม่ในอนาคต ทั้งนี้เพื่อให้ตอบสนองความต้องการของเจ้าของโครงสร้างพื้นฐานที่สำคัญและผู้ประกอบการ ในสภาพแวดล้อมแบบไดนามิกและมีความท้าทายของภัยคุกคาม ความเสี่ยง และการแก้ปัญหาใหม่ๆอยู่เสมอ

7) ในระหว่างขั้นตอนการออกแบบกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ออกแบบควรพิจารณาแนวทางจากคำถามที่ว่า

เราสามารถกำหนดกรอบการดำเนินงานเบื้องต้นได้อย่างไร:

(1) เพื่อให้มีการกำหนดกรอบและผลที่ได้รับอย่างเหมาะสม โดยมีความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่ง และสามารถสนับสนุนวัตถุประสงค์ทางธุรกิจ?

(2) เพื่อให้เกิดการดำเนินงานมีประสิทธิภาพ?

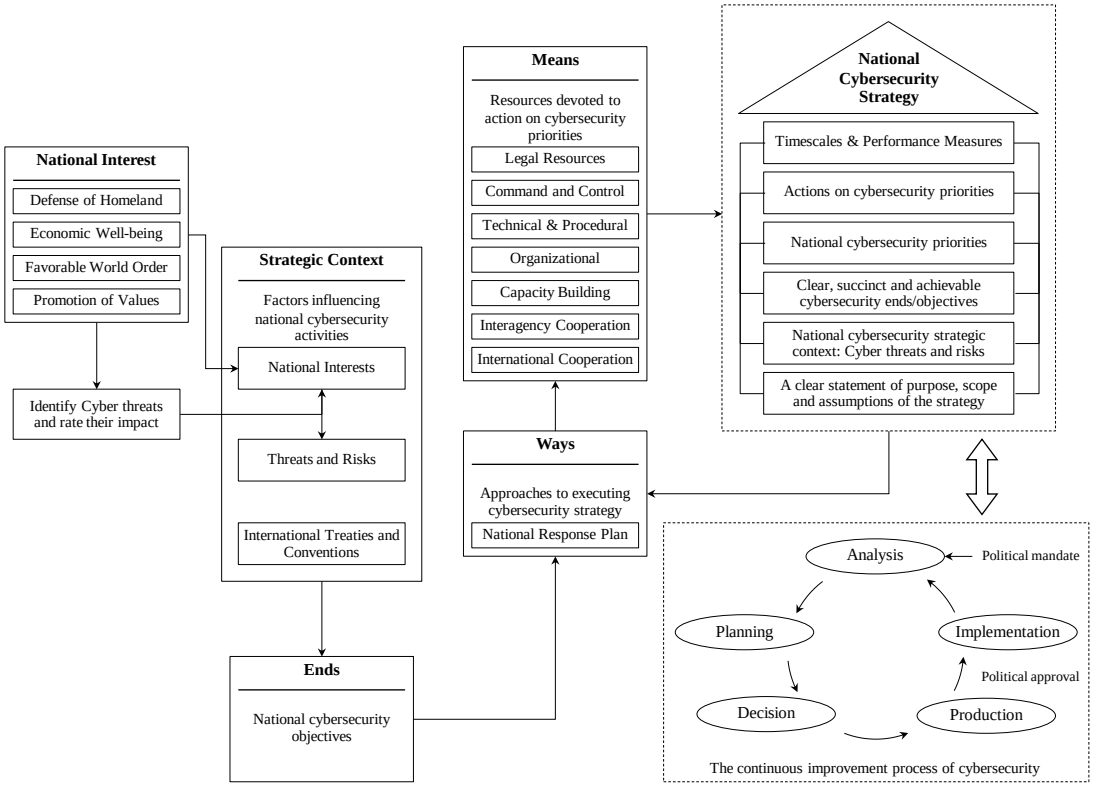
(3) เพื่อให้มีการบูรณาการความเสี่ยงทางไซเบอร์กับความเสี่ยงทางธุรกิจที่เหมาะสม?

(4) สำหรับจัดเตรียมเครื่องมือ แก่ผู้บริหารระดับสูงและคณะกรรมการบริหาร เพื่อทำความเข้าใจความเสี่ยงและวิธีการลดความเสี่ยง ในระดับที่เหมาะสม?

(5) เพื่อทำให้ผู้บริหารระดับสูงตระหนักถึงผลกระทบที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์?

(6) เพื่อให้ได้คำแนะนำที่เหมาะสม และสามารถจัดหาทรัพยากรที่เพียงพอ เพื่อช่วยให้องค์กรธุรกิจทุกขนาดยังคงรักษาความยืดหยุ่นไว้ได้?

กระบวนการที่สำคัญอย่างหนึ่งในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คือการปรับปรุงวิธีการอย่างต่อเนื่อง เพื่อสร้างมาตรการการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพมากขึ้นเท่าที่จะเป็นไปได้ กระบวนการทางยุทธศาสตร์แสดงให้เห็นอย่างชัดเจนว่า มีการดำเนินงานหลายระดับและในแต่ละระดับมีขั้นตอนที่แตกต่างกัน เป้าหมายคือการสร้างกระบวนการทางยุทธศาสตร์อย่างต่อเนื่อง และการปรับปรุงแนวทางการปฏิบัติอย่างต่อเนื่อง จากการศึกษาของผู้เขียนพบว่ากระบวนการพัฒนาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง คือ การบูรณาการโดยนำกรอบแนวคิดแบบ Ends-Ways-Means ของ ITU มาใช้ ในการปรับปรุงเชื่อมโยงยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ รูปที่ 3 แสดงตัวแบบ (Model) การวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



รูปที่ 3 National Cybersecurity Strategy Model

การดำเนินการในการจัดการความเสี่ยงในประเด็นที่สำคัญ มีดังต่อไปนี้

(1) กำหนดให้ความเสี่ยงทางไซเบอร์ เป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงและแนวทางการดำเนินงานภาครัฐ ที่ดำเนินการอยู่ในปัจจุบัน

(2) หยิบยกการอภิปรายเรื่องการบริหารความเสี่ยงด้านไซเบอร์กับผู้บริหารระดับสูงสุดและ CEO

(3) ให้ความสำคัญกับมาตรฐานอุตสาหกรรมและแนวปฏิบัติที่ดีที่สุด

(4) ประเมินผลและตอบสนองได้โดยทันที รวมทั้งมีการจัดการความเสี่ยงด้านไซเบอร์ที่เฉพาะเจาะจงขององค์กรในเชิงรุก

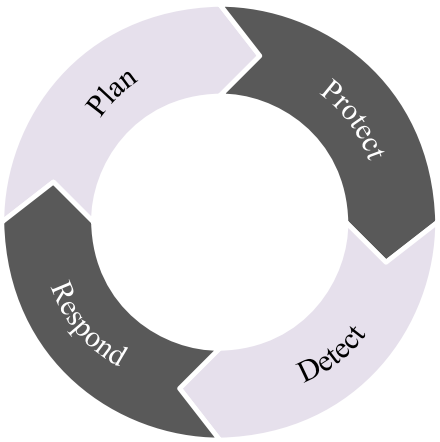
(5) มีการทดลองและทดสอบ แผนและกระบวนการในการตอบสนองการถูกคุกคามทางไซเบอร์

(6) ประสานงานการวางแผนการตอบสนองเหตุการณ์ที่เกิดขึ้นทางไซเบอร์ทั่วทั้งองค์กร

(7) ตระหนักถึงสถานการณ์ของภัยคุกคามทางไซเบอร์อยู่เสมอ

(8) มีการจัดการและตอบสนองต่ออาชญากรรมทางไซเบอร์ในเชิงรุกและมีประสิทธิภาพ จำเป็นจะต้องมีข้อกำหนดระหว่างประเทศอย่างเหมาะสม มีความร่วมมือมีความช่วยเหลือซึ่งกันและกันระหว่างประเทศมากขึ้นภายใต้กรอบของกฎหมาย

(9) จะต้องมีการบริหารจัดการอาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพ โดยการประสานงานกับองค์กรความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ นอกจากนี้จะต้องทำความเข้าใจด้านความมั่นคงปลอดภัยทางไซเบอร์ ยุทธศาสตร์ และกฎหมาย ที่มีความสอดคล้องกันในภูมิภาค และในประเทศเพื่อนบ้านอื่นๆ



รูปที่ 4 มาตรการความมั่นคงปลอดภัยไซเบอร์ในเชิงรุก

(Proactive measures of Cybersecurity)

ตารางที่ 3 มาตรการความมั่นคงปลอดภัยไซเบอร์เชิงรุก

มาตรการ	การปฏิบัติ
การวางแผน (Plan)	• ประเมินสภาพแวดล้อม • กำหนดและแก้ไขปัญหาที่เกิดขึ้น • พัฒนาแผนการรับมือเหตุการณ์ต่างๆที่เกิดขึ้น
การป้องกัน (Protect)	• มีสภาพแวดล้อมที่เข้มแข็ง • มีการปรับปรุงที่น่าเชื่อถือ • การจัดการสิทธิในการใช้งาน • จำกัดขอบเขตการสื่อสารที่ไม่จำเป็น • ลดจำนวนสิทธิของผู้ใช้งานเท่าที่จะเป็นไปได้
การตรวจหา (Detect)	• มีการโปรแกรมสำหรับตรวจสอบการรักษาความปลอดภัยเครือข่ายภายใน • มีการตรวจสอบจุดที่เชื่อมต่อไปภายนอกเครือข่าย • บันทึกและวิเคราะห์ ข้อมูลการใช้งาน • จัดเก็บรวบรวมข้อมูลที่สำคัญ
การตอบสนอง (Respond)	• เจ้าหน้าที่และการฝึกอบรมทีมงานที่รับผิดชอบเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของคอมพิวเตอร์ (Computer Incident Response Team: CIRT) • CIRT เป็นผู้มีหน้าที่ตอบสนองต่อเหตุกาณ์ที่เกิดขึ้นทางไซเบอร์ • เวลาที่ใช้การตอบสนองลดลง

(10) ภาคธุรกิจจะต้องมีมาตรการเชิงรุกในการจัดการภัยคุกคามทางไซเบอร์และมียุทธศาสตร์ในการตอบสนองได้อย่างรวดเร็วและมีประสิทธิภาพ ในรูปที่ 4 แสดงให้เห็นว่าองค์กรควรจะวางแผนสำหรับการป้องกัน การตรวจหา และการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นทางไซเบอร์ และในตารางที่ 3 ได้แสดงรายละเอียดของมาตรการความมั่นคงปลอดภัยไซเบอร์ในเชิงรุก ซึ่งการจู่โจมทางไซเบอร์ไม่สามารถมองเห็นได้ แต่สามารถเพิ่มประสิทธิภาพในการจำกัดความรุนแรงที่จะเกิดขึ้นได้อย่างมีนัยสำคัญ

10. กรอบแนวคิดการบริหารความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management Framework)

กรอบแนวคิดเพื่อขับเคลื่อนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ถือเป็นองค์ประกอบที่สำคัญของการดำเนินงานขององค์กรทั้งภาครัฐและเอกชน โดยกรอบแนวคิดดังกล่าวสามารถแบ่งออกเป็น 3 ลำดับ ดังนี้

1) ระดับกลยุทธ์ (Strategic Direction)

การกำหนดกลยุทธ์เป็นจุดเริ่มต้นในการขับเคลื่อนจากกรอบแนวคิดไปสู่การปฏิบัติการ (operation) ซึ่งต้องการบุคคลากรในการระบุถึงความต้องการด้านต่างๆ เพื่อความมั่นคงปลอดภัยไซเบอร์ทำการพิจารณาประเด็นสำคัญต่างๆ ของการขับเคลื่อนองค์กร ให้คำนิยาม จัดทำเอกสารสำคัญต่างๆ และประกาศอย่างเป็นทางการในเรื่องทิศทางในการดำเนินการขององค์กร เพื่อที่จะทำให้โครงการหรือโปรแกรมการบริหารความมั่นคงปลอดภัยไซเบอร์สามารถขับเคลื่อนได้อย่างเป็นรูปธรรม

2) การปฏิบัติการ (Operation)

ระดับปฏิบัติการจะมุ่งเน้นไปยังกิจกรรมที่เกี่ยวข้องกับโครงการหรือโปรแกรมที่จะทำให้กลยุทธ์ที่กำหนดมาแล้วแปลงให้สามารถปฏิบัติเป็นรูปโรรมได้ โดยจะต้องกำหนดวิธีการดำเนินการให้เป็นไปตามความต้องการของกลยุทธ์ที่ถูกระบุไว้ ซึ่งในระดับปฏิบัติการนี้จะต้องมีการจัดทำเอกสารที่มีการอธิบายคำนิยามหรือความหมายที่เกี่ยวข้องกับมาตรฐานขั้นตอนการดำเนินการ, กระบวนการ, ขั้นตอนในรายละเอียด โดยมีรายละเอียดอธิบายถึงใครเป็นผู้ปฏิบัติ (Who) และปฏิบัติอย่างไร (How)

3) การปฏิบัติการเชิงเทคนิคความมั่นคงปลอดภัย (Tactical Security)

ในการปฏิบัติการเชิงเทคนิค ซึ่งอาจใช้คำภาษาอังกฤษว่า ‘Tactical security’ นั้นหมายความถึง การควบคุมความมั่นคงปลอดภัยในเชิงเทคนิค มีการระบุความต้องการในการดำเนินการแบบเจาะจงในเอกสารปฏิบัติการอย่างเป็นทางการ เพื่อผู้ปฏิบัติจะได้มีความเข้าใจตรงกันไม่คลาดเคลื่อน ในระดับยุทธวิธีนี้จะเป็นการควบคุมรับผิดชอบในทุกมิติของระบบสารสนเทศขององค์กร โดยมีการตรวจสอบตรวจตราอย่างต่อเนื่อง มีการเก็บข้อมูล วิเคราะห์ข้อมูล

ตรวจจับการบุกรุก และมีการจัดทำรายงานอย่างเป็นระบบ ซึ่งรูปแบบรายงานอาจเป็นเชิง Security metrics ก็จะทำให้ง่ายต่อการรวบรวมและบูรณาการข้อมูล

แม้ว่าเราจะแบ่งระดับชั้นการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กรเป็น 3 ระดับ แต่เพื่อความเข้าใจในรายละเอียดที่ตรงกัน เราสามารถที่จะแบ่งระดับย่อยลงไปเพื่อรายละเอียดที่ชัดเจนยิ่งขึ้นเป็นองค์ประกอบ ดังนี้

- องค์ประกอบด้านผู้บริหารระดับสูง (Executive Sponsorship) ซึ่งถือว่าเป็นตัวจักรสำคัญในการขับเคลื่อนโครงการหรือโปรแกรม
- องค์ประกอบด้านการบริหารจัดการความเสี่ยงสารสนเทศ (IT Risk Management) เป็นการจัดการในการระบุ, ตรวจสอบตรวจจับ และกำหนดความเสี่ยงด้านไซเบอร์ให้แก่องค์กร
- องค์ประกอบด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ (IT and Security Audit) ซึ่งมีความจำเป็นเพื่อที่จะเกิดความมั่นใจได้ว่าระบบสารสนเทศได้รับการดูแลอย่างครบถ้วนตามมาตรฐานที่องค์กรได้กำหนดไว้ และตรวจสอบเพื่อมั่นใจได้ว่าบุคคลากรในองค์กรมีการปฏิบัติเป็นไปตามข้อกำหนดและมาตรการต่างๆ ครบถ้วน
- การข่าวกรองด้านความมั่นคงปลอดภัย (Security Intelligence)
- เป็นการวิเคราะห์ข้อมูลในอดีตและปัจจุบันเพื่อการพยากรณ์ภัยคุกคามในอนาคตที่อาจจะเกิดขึ้นทั้งภัยคุกคามจากภายในและภายนอกองค์กร และเพื่อป้องกันและลดความเสี่ยงต่อองค์กรให้น้อยที่สุด
- การปกป้องเครือข่ายและระบบ (Secure Network and Systems) องค์กรมีความจำเป็นอย่างยิ่งที่จะต้องทำการออกแบบและบริหารจัดการอุปกรณ์เครือข่ายและระบบเพื่อให้สามารถปกป้องทรัพย์สินที่จับต้องไม่ได้ เช่น ความรู้ และทรัพย์สินทางปัญญา เป็นต้น ที่เก็บไว้ในเครือข่ายคอมพิวเตอร์ขององค์กร
- การปกป้องโปรแกรมประยุกต์ (Secure Applications) องค์กรจะต้องให้ความสำคัญอย่างยิ่งในการออกแบบและบริหารจัดการระบบอัจฉริยะขององค์กร

ที่อยู่ในรูปแบบของโปรแปรมประยุกต์เพื่อปกป้องทรัพย์สินขององค์กรที่อยู่ในระบบโปรแกรมประยุกต์ดังกล่าว

กรอบแนวคิดการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ดังที่กล่าวมาแล้วสามารถแสดงดังตารางที่ 4

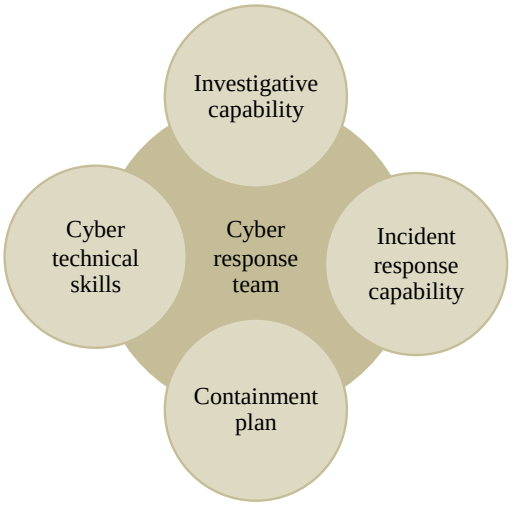
ตารางที่ 4 องค์ประกอบการบริหารความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบหลัก	องค์ประกอบย่อย
ด้านผู้บริหารระดับสูง (Executive Sponsorship)	คณะทำงานด้านกฎหมาย
	การบริหารงานบุคคล
	การศึกษาและการฝึกอบรม
	การจัดการสภาวะวิกฤต
	โครงการการจัดการด้าน Cybersecurity
	การจัดการโครงสร้าง Cybersecurity
	การสนับสนุนความมั่นคงด้านกายภาพ
ด้านการจัดการความเสี่ยงสารสนเทศ (IT Risk Management)	โครงการการจัดการด้าน Cybersecurity
	การบริหารทรัพย์สิน
	การจัดการด้านการระบุอัตลักษณ์ (Identity)
	การคัดกรองแบ่งแยกข้อมูล
	การจัดการการดำเนินการธุรกิจต่อเนื่อง (Business Continuity)
	การกู้ระบบจากภัยพิบัติ (Disaster Recovery)
	การตอบโต้สถานการณ์ฉุกเฉิน (Incident Response)
ด้านการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ (IT and Security Audit)	การบริหารการกำกับดูแลและการปฏิบัติตามกฎระเบียบ
	การบริหารจัดการผู้จำหน่ายอุปกรณ์และรับจ้างดำเนินงาน
	การบริหารจัดการทะเบียน และประวัติข้อมูลการบันทึก
	การบริหารจัดการการพัฒนาโปรแกรมประยุกต์
ด้านการข่าวกรองความมั่นคงปลอดภัย (Security Intelligence)	การบริหารจัดการการวิเคราะห์ตรวจหาช่องโหว่ของระบบ
	การวิเคราะห์ภัยคุกคามและพฤติกรรมที่มีแนวโน้มเป็นภัยคุกคาม
	การจัดการ Log file
การปกป้องเครือข่ายและ	การป้องกันไวรัสและโปรแกรมทำลายระบบ

ระบบ (Secure Network and System)	การป้องกันระบบเก็บข้อมูล
	การป้องกันการเจาะระบบ
	การออกแบบเครือข่ายเพื่อความมั่นคงปลอดภัย
	การเข้ารหัส (Encryption)
	การ Back up ข้อมูล
การปกป้องโปรแกรมประยุกต์ (Secure Applications)	ความเป็นส่วนตัวด้านข้อมูล (Data Privacy)
	การพัฒนาการเข้ารหัส (Secure Code)
	การจัดการการระบุตัวบุคคล และพิสูจน์อัตลักษณ์ (Identity)
	การจัดการระบบความปลอดภัยโปรแปรมประยุกต์

11. การพัฒนาขีดความสามารถของหน่วยงานตอบโต้สถานการณ์คุกคามด้านไซเบอร์

หน่วยงานที่ทำหน้าที่ตอบโต้ภัยคุกคามด้านไซเบอร์ (Cyber Incident Response) สามารถที่จะประยุกต์ใช้กรอบความคิดในการพัฒนาขีดความสามารถของหน่วยงานและทีมในด้านต่างๆ ดังนี้ (แสดงดังรูปที่ 5)



รูปที่ 5 กรอบความคิดในการพัฒนาขีดความสามารถ
ของหน่วยงานและทีมในด้านต่างๆ

1) ขีดความสามารถในการตอบโต้ภัยคุกคาม (Incident response capabilities)

การพัฒนาขีดความสามารถภายในหน่วยงานเพื่อการตอบโต้ภัยคุกคามด้านไซเบอร์อย่างมีประสิทธิภาพ และสามารถที่จะคาดการณ์ภัยคุกคามในอนาคตเพื่อการเตรียมการได้อย่างมีประสิทธิภาพ และทันท่วงที

2) ขีดความสามารถในการสืบสวนสอบสวน (Investigative capabilities)

ความสามารถในการระบุสาเหตุทางด้านเทคนิค และทางด้านบุคคลเพื่อตอบโต้ภัยคุกคามได้ตอบปัญหาและสาเหตุเป็นสิ่งสำคัญยิ่งในการหยุดยั้งความเสี่ยงหรือลดความเสี่ยงของภัยคุกคามและการก่ออาชญากรรมด้านไซเบอร์

3) ขีดความสามารถทางด้านเทคนิคไซเบอร์ (Cyber technical skills)

ขีดความสามารถทางด้านเทคนิคไซเบอร์ เป็นสิ่งที่ซับซ้อนและต้องใช้เวลาและความเชี่ยวชาญในการพัฒนา และหน่วยงานควรมีงบประมาณในการฝึกอบรมให้แก่บุคลากรทั้งในประเทศ และต่างประเทศ เนื่องจากการพัฒนาทางเทคโนโลยีไซเบอร์ มีการพัฒนาอย่างรวดเร็วเกินกว่าที่องค์กรจะสามารถพัฒนาได้ทันโดยปราศจากการวางแผนการพัฒนาบุคคลากรด้วยงบประมาณที่เพียงพอ

4) แผนความต่อเนื่อง (Containment plan)

การพัฒนาขีดความสามารถของหน่วยงานและทีมอย่างต่อเนื่องนั้น มีความสำคัญต่อการติดตามและคาดการณ์ภัยคุกคามในอนาคตเพื่อการเตรียมขีดความสามารถให้พร้อมตลอดเวลา หน่วยงานจึงต้องมีวิสัยทัศน์ในการดำเนินการพัฒนาขีดความสามารถอย่างต่อเนื่อง

12. การตอบโต้ภัยคุกคามด้านไซเบอร์ (Cyber Incident Response)

การตอบโต้ภัยคุกคามด้านไซเบอร์นั้นต้องมีการเตรียมการและวางแผนอยู่บนพื้นฐานจากมาตรฐานความมั่นคงปลอดภัยด้านไซเบอร์ที่อุตสาหกรรมและองค์กรยอมรับเป็นสากล อีกทั้งต้องนำเอากรณีศึกษาที่ได้จากประสบการณ์ของหลายประเทศพันธมิตรมาศึกษาเพื่อนำเอาแนวทางปฏิบัติที่ดีที่สุด (Best practices) ที่มีอยู่มาประยุกต์ใช้ เพื่อนำมาประกอบเข้ากับการจัดการความเสี่ยง (Risk Management) เพื่อปกป้องทรัพย์สินและชื่อเสียงขององค์กร

แผนตอบโต้ภัยคุกคามดังกล่าวจะต้องมีความชัดเจน โดยต้องมีกระบวนการในการทำงาน (task) และการวิเคราะห์ความเสี่ยงที่เป็นปัจจุบัน (update) อยู่เสมอ และยังต้องเอื้ออำนวยให้มีการตัดสินใจในการปฏิบัติการรวดเร็ว ทันเหตุการณ์

เพื่อการจัดการความเสี่ยงที่มีประสิทธิภาพ องค์กรมีความจำเป็นที่จะต้องเข้าใจเชิงจิตวิทยาต่อเจตนาและแรงจูงใจของแฮกเกอร์ (Hacktivists) อาชญากรไซเบอร์ และผู้ไม่หวังดีที่จะคุกคามระบบไซเบอร์ของชาติหรือขององค์กร

ความรวดเร็ว และมีประสิทธิภาพในการตอบโต้นั้นเป็นสิ่งที่จำเป็นอย่างยิ่ง การตอบโต้ภัยคุกคาม (Incident response) และขีดความสามารถในด้านนิติวิทยาศาสตร์ (Forensic capabilities) จะต้องถูกสร้างและออกแบบให้ครอบคลุมเหตุการณ์ภัยคุกคามที่จะเกิดขึ้นได้อย่างครบวงจร (Incident lifecycle) เพื่อที่จะสามารถตรวจจับ คาดการณ์ และถอนรากถอนโคนแหล่งที่มาได้ โดยกระบวนการปฏิบัติสามารถนำเสนอเป็นรูปที่ 6

รูปที่ 6 การบริหารจัดการการตอบโต้ภัยคุกคามไซเบอร์ (Cyber Incident Management)

13. ประโยชน์ที่ได้รับจากการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ถูกนำมาใช้ประโยชน์เพื่อจุดมุ่งหมายที่กำหนดไว้สำหรับการปรับปรุงความปลอดภัยความเสี่ยงพื้นฐาน สำหรับเจ้าของ ผู้ประกอบการ หรือผู้สร้างโครงสร้างพื้นฐานสำคัญในองค์กร ยิ่งไปกว่านั้น กรอบการดำเนินงานนี้ยังสามารถนำมาซึ่งประโยชน์ต่างๆ ได้แก่ ความร่วมมือและการสื่อสารที่มีประสิทธิภาพ อีกด้วย

หลักปฏิบัติของกรอบการดำเนินงานที่สำคัญยิ่ง คือการร่วมมือกันเพื่อแลกเปลี่ยนข้อมูลและพัฒนาแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไซเบอร์ และการละเมิดทรัพย์สินทางปัญญา ซึ่งในการร่วมมือกัน จะก่อให้เกิดประโยชน์อย่างแท้จริง โดยแนวทางปฏิบัติด้านความปลอดภัยที่มีประสิทธิภาพสูง มักจะมีการประสานร่วมมือกับองค์กรอื่น เพื่อยกระดับด้านความปลอดภัยและการรับรู้ถึงภัยคุกคาม โดยทั่วไปแล้วองค์กรที่มีแนวปฏิบัติด้านความปลอดภัยที่มีประสิทธิภาพสูงจะมีการร่วมมือกับองค์กรอื่นๆ เพื่อให้สามารถบรรลุเป้าหมาย ด้านความมั่นคงปลอดภัยไซเบอร์ หนึ่งในวิธีการร่วมมือที่มีประสิทธิภาพสูงสุด คือการจัดตั้งและมีส่วนร่วมในศูนย์แลกเปลี่ยนและวิเคราะห์ข้อมูล (Information Sharing and Analysis Centers : ISACs) ซึ่งสามารถจัดตั้งขึ้นเป็นองค์กรกลางเพื่อการพัฒนาความมั่นคงปลอดภัยไซเบอร์อย่างยั่งยืน

การประสานร่วมมือกันอย่างมีประสิทธิภาพขึ้นอยู่กับการแลกเปลี่ยนความคิดเห็นที่เปิดกว้างและมีเป้าหมาย ซึ่งสุดท้ายแล้วกรอบการดำเนินงานควรจะมีภาษากลางเพื่ออำนวยความสะดวกในการสื่อสาร เกี่ยวกับแนวทางปฏิบัติ นโยบาย และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งภายในและภายนอกองค์กร เช่น ผู้ให้บริการภายนอกและพันธมิตรทางการค้า เป็นต้น รัฐบาลควรสนับสนุนองค์กรต่างๆ เพื่อแบ่งปันข้อมูลด้านความไม่มั่นคง ภัยคุกคามต่อข้อมูล และกลยุทธ์ในการรับมือ ผลประโยชน์ที่ได้จากการใช้สื่อกลางในการสื่อสาร และความร่วมมือที่มีมากขึ้น คือ ความเข้มแข็ง ยกตัวอย่างเช่น ถ้าในห่วงโซ่อุปทานทั้งหมดขององค์กรหนึ่ง สามารถใช้คำศัพท์หรือภาษาของกรอบการดำเนินงานเหมือนกัน จะสามารถสื่อสาร ทำความเข้าใจ และสามารถลดความเสี่ยงลงได้อย่างมีประสิทธิภาพ

สิ่งสำคัญที่ควรรู้ก็คือ กรอบการดำเนินการนี้มีการแลกเปลี่ยนความคิดเห็นมีการสื่อสารเรื่องความมั่นคงปลอดภัยไซเบอร์ ด้วยคำศัพท์ด้านการจัดการความเสี่ยง ด้วยเหตุผลที่ว่า ผู้นำฝ่ายบริหารและคณะกรรมการขององค์กรต่างมีความรอบรู้ เกี่ยวกับการจัดการความเสี่ยงอยู่แล้ว และการวางกรอบเพื่อความมั่นคงปลอดภัยไซเบอร์ จะทำให้ผู้นำด้านความมั่นคงปลอดภัยนี้สามารถเชื่อมโยงความสำคัญและเป้าหมายของความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้ยังสามารถช่วยให้องค์กรต่างๆ สามารถจัดลำดับความสำคัญและตรวจสอบความสมเหตุสมผลด้านการลงทุนบนพื้นฐานการจัดการความเสี่ยงได้อีกด้วย

14. ข้อเสนอแนะ

รายงานฉบับนี้มีข้อเสนอแนะในการดำเนินการพัฒนายุทธศาสตร์และกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดังต่อไปนี้

1) เพื่อให้มีระบบการรักษาความปลอดภัยที่แข็งแกร่ง รัฐบาลควรจัดตั้งศูนย์อาชญากรรมทางไซเบอร์โดยเฉพาะ ซึ่งในระหว่างนั้นรัฐบาลจะต้องดำเนินการเพื่อแสวงหาโอกาสใหม่สำหรับการดำเนินงานร่วมกันระหว่างประเทศ

2) หน่วยงานด้านความปลอดภัยของข้อมูล ต้องมีการทำงานร่วมกับผู้กำหนดนโยบาย เพื่อให้ได้มุมมองที่กว้างขึ้น และการเยียวยาการถูกโจมตีบนคอมพิวเตอร์และโครงสร้างพื้นฐาน ในขณะเดียวกัน รัฐบาลไม่ควรแยกการป้องกันโครงสร้างพื้นฐานออกจากการป้องกันแอพพลิเคชั่น

3) รัฐบาลควรร่วมมือกับภาคส่วนโทรคมนาคม, การเงินการธนาคาร, การคมนาคมขนส่ง และภาคประชาชน เพื่อนำมาตรการบริหารความเสี่ยงมาใช้ และเพื่อรายงานเหตุการณ์ที่เกิดขึ้นต่อเจ้าหน้าที่ผู้มีอำนาจตามกฎหมาย

4) อาชญากรรมทางไซเบอร์ อาจถูกสร้างขึ้นมาเป็นแอพพลิเคชั่น ที่สามารถเข้าถึงการใช้งานแอพพลิเคชั่นอื่นๆ ของผู้ใช้ได้ ซึ่งเป็นการเข้าโจมตีโดยไม่มีสิ่งปิดกั้น ทำให้การตรวจสอบอาชญากรรมทางไซเบอร์มีความซับซ้อนมากขึ้น ดังนั้นเพื่อให้สามารถรับมือกับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ จึงมีความจำเป็นที่จะต้องเตรียมวิธีการป้องกันอย่างเหมาะสม และมีความร่วมมือและความช่วยเหลือกันระหว่างประเทศภายใต้ข้อบังคับของกฎหมาย หรือความร่วมมือกันในภูมิภาค

5) รัฐบาลต้องเข้าใจว่ากรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นแนวทางที่สามารถเปลี่ยนแปลงได้ตลอดเวลา ช่วยให้รัฐสามารถกำหนดสถานการณ์ด้านไซเบอร์ในปัจจุบันและอนาคต และลักษณะความมั่นคงปลอดภัยไซเบอร์ที่ต้องการ ตลอดจนวิธีการในการดำเนินงานไปในทิศทางที่กำหนดได้ เช่น คำแนะนำเกี่ยวกับวิธีการสื่อสารกับผู้มีส่วนได้เสียทั้งภายในและภายนอก ในเรื่องความเสี่ยงที่เป็นภัยคุกคาม

6) ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ถือเป็นปัญหาที่เกิดขึ้นทั่วโลก ไม่ได้เกิดขึ้นในธุรกิจใดธุรกิจหนึ่ง หรือประเทศใดประเทศหนึ่งเท่านั้น ดังนั้นจึงต้องมีความร่วมมือจากรัฐบาลและภาคอุตสาหกรรม ดังนั้นรัฐบาลจะต้องส่งเสริมให้ผู้มีส่วนได้เสียทุกภาคส่วน มีการดำเนินการดังต่อไปนี้

(1) ปรับปรุงเอกสารเกี่ยวกับนโยบายความปลอดภัย โดยมีการสื่อสารภาษากลางที่เข้าใจตรงกัน เพื่ออำนวยความสะดวกในการสื่อสาร

(2) กำหนดขั้นตอนการดำเนินงานสำหรับภัยคุกคามใหม่ๆ กระบวนการทดสอบความมั่นคงปลอดภัย และการปรับปรุงกระบวนการต่างๆ เพื่อรับมือกับภัยคุกคามใหม่ๆเหล่านั้น ด้วยการสร้างโปรแกรมด้านความมั่นคงปลอดภัยไซเบอร์ (cybersecurity program) ที่ทันสมัยสอดคล้องกับการเปลี่ยนแปลง

(3) มีการสร้างยุทธศาสตร์ และกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร และมีการตรวจสอบการดำเนินงานของยุทธศาสตร์และกลยุทธ์นั้นอย่างต่อเนื่อง

สรุป

ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาตินั้นไม่มีคำตอบสุดท้าย และคำตอบที่ชัดเจน สำหรับรูปแบบที่ถูกต้องสำหรับทุกองค์กร เพราะแต่ละองค์กรมีระดับความเสี่ยงที่แตกต่างกัน อีกทั้งวัฒนธรรมองค์กรแต่ละองค์กรก็มีความแตกต่างกัน ในแต่ละประเทศมีกฎหมายและระดับสิทธิเสรีภาพของประชาชนที่แตกต่างกัน อำนาจการต่อรองของแต่ละประเทศก็มีระดับที่แตกต่างกัน รายงานฉบับนี้มีวัตถุประสงค์เพียงเพื่อเป็นแนวทางพื้นฐานในการทำความเข้าใจต่อการวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อการนำไปประยุกต์ใช้ต่อไป

บรรณานุกรม

[1] เอกสารของ Carnegie Mellon ชื่อว่า “Best Practice for National Cybersecurity. Building a National Computer Security Incident Management Capability” นำเสนอรายชื่อผู้ได้รับผลประโยชน์ร่วมของความมั่นคงปลอดภัยไซเบอร์แห่งชาติทั้งหมด เรานำรายชื่อจากรายการนี้ไปใช้

[2] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

[3] InternetWorldStats. (2015). Internet Users in the World Distribution - 2014 Q4. Available: http://www.internetworldstats.com/stats.htm

[4] WorldPopulationStatistics. (2014). Asia Population 2014. Available: http://www.worldpopulationstatistics.com/asia-population-2013/

[5] UN, "Comprehensive Study on Cybercrime," UNODC, Vienna2013.

[6] Cisco, "The Internet of Everything and the Connected Athlete: This Changes... Everything," 2013.

[7] F. Wamala, "ITU National Cybersecurity Strategy Guide," ed, 2011.

[8] Ernst&Young, "Get ahead of cybercrime," 2014.

[9] TheWhiteHouseWashington, "THE NATIONAL STRATEGY TO SECURE CYBERSPACE 2003," ed, 2003.

[10] ITU, "Guidelines for the preparation of national wireless broadband masterplans for the Asia Pacific region," 2012.

[11] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[12] HomelandSecurity, "Cybersecurity Questions for CEOs," 2014.

[13] EuRActiv. (2012). Cybersecurity: Protecting the digital economy. Available: http://www.euractiv.com/infosociety/cybersecurity-protecting-oil-internet-linksdossier-508217#group_positions

พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ

ประธานกรรมการกิจการโทรคมนาคม และรองประธานกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

การศึกษา

ปริญญาเอก: วิศวกรรมศาสตรดุษฎีบัณฑิต (Ph.D. in EE) (วิศวกรรมโทรคมนาคม) จาก Florida Atlantic University สหรัฐอเมริกา

ปริญญาโท: วิศวกรรมศาสตรมหาบัณฑิต (MS in EE) (วิศวกรรมโทรคมนาคม) The George Washington University สหรัฐอเมริกา

ปริญญาโท: วิศวกรรมศาสตรมหาบัณฑิต (MS in EE) (วิศวกรรมไฟฟ้า) Georgia Institute of Technology สหรัฐอเมริกา

ปริญญาตรี: วิทยาศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร (เกียรตินิยมเหรียญทอง) โรงเรียนนายร้อยพระจุลจอมเกล้า (นักเรียนเตรียมทหารรุ่น 26, จปร. รุ่น 37)

มัธยมปลายจากโรงเรียนเตรียมอุดมศึกษา

เกียรติประวัติ

- เกียรตินิยมอันดับ 1 เหรียญทอง ปริญญาตรีสาขาวิศวกรรมไฟฟ้าสื่อสารโทรคมนาคมจากโรงเรียนนายร้อยพระจุลจอมเกล้า
- โล่ห์เกียรติยศจากโรงเรียนนายร้อยพระจุลจอมเกล้า คะแนนสูงสุดในวิชาผู้นำทหาร
- เกียรตินิยมปริญญาเอก Outstanding Academic Achievement จาก Tau Beta Pi Engineering Honor Society และ Phi Kappa Phi Honor Society
- รางวัลเกียรติยศจักรดาว ประจำปี พ.ศ.2556 จากมูลนิธิศิษย์เก่าโรงเรียนเตรียมทหาร
- ได้รับการจัดอันดับ 1 ใน 25 Young Executives ที่ประสบความสำเร็จสูงสุดในปี 2555 จากนิตยสาร GM
- ประกาศเกียรติคุณ “โครงการวิทยาศาสตร์สู่ความเป็นเลิศ” พ.ศ. 2556 จากคณะกรรมาธิการวิทยาศาสตร์ เทคโนโลยีการสื่อสาร และโทรคมนาคม วุฒิสภา
- ได้รับการจัดอันดับ 1 ใน 30 นักยุทธศาสตร์แห่งปีที่อยู่ในระดับผู้นำองค์กร ปี พ.ศ. 2556 จากนิตยสาร Strategy+Marketing Magazine
- รับพระราชทานรางวัลเทพทอง ครั้งที่ 16 ในฐานะองค์กรดีเด่น ประจำปี 2557
- ได้รับรางวัล “ผู้นำเสนองานวิจัยดีเด่น” จากสถาบันวิชาการป้องกันประเทศ ประจำปีงบประมาณ 2558
- ประกาศเกียรติคุณรางวัล ″คนดี ความดี แทนคุณแผ่นดิน″ พ.ศ.2558 สาขาการสื่อสารโทรคมนาคม จากคณะกรรมการรางวัลไทย
- ได้รับโล่เกียรติยศ “ผู้นำและผู้ทำคุณประโยชน์เพื่อผู้ด้อยโอกาส” ประจำปี พ.ศ.2558 จากสมาคมโทรคมนาคมเพื่อสิทธิเสรีภาพของผู้ด้อยโอกาส

WE'RE SMARTER
WHEN WE'RE CONNECTED