เอกสารวิชาการ
เรื่อง

แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง (Critical Information Infrastructure หรือ CII for Logistic Industry) ระยะ 5 ปี (พ.ศ. 2566 - 2570)

โดย

นางสาว อธิตานันท์ อภิธนทวีพัฒน์

นักศึกษาหลักสูตรนักยุทธศาสตร์ รุ่นที่ 16

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

ประจำปีงบประมาณ พ.ศ. 2565

บทคัดย่อ

รายงานส่วนบุคคลฉบับนี้เป็นการจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง (Critical Information Infrastructure หรือ CII for Logistic Industry) ระยะ 5 ปี (พ.ศ. 2566-2570) มีวัตถุประสงค์เพื่อ (1) ศึกษาสภาพแวดล้อมทางยุทธศาสตร์ที่ส่งผลต่อความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง หรือ Logistic Industry ในประเทศไทย (2) การจัดทำแผนปฏิบัติการส่งเสริมและพัฒนาแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่งในระยะ 5 ปี (พ.ศ. 2566 – 2570) และ (3) จัดทำข้อเสนอแนะทางยุทธศาสตร์ในการพัฒนาและกำหนดแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่งของประเทศไทยให้มีความปลอดภัยเป็นไปตามมาตรฐานสากล และ พรบ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562 โดยผู้ศึกษาได้ทำการตรวจสอบสภาพแวดล้อมและปัจจัยที่ส่งผลกระทบต่อการดำเนินงานด้านการรักษาความมั่น คงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่งของประเทศไทย โดยใช้กรอบแนวคิดของ PASTEL ในการตรวจสอบสภาพแวดล้อมภายนอก และ McKinsey 7’s Framework เพื่อตรวจสอบสภาพแวดล้อมภายใน วิเคราะห์ออกมาเป็น SWOT ก่อนจะนำไปใช้ในการกำหนดพื้นที่ทางยุทธศาสตร์ของหน่วยงานด้านการขนส่ง โดยได้ผลลัพธ์ตกอยู่ในพื้นที่ W-O ซึ่งยังแสดงให้เห็นถึงโอกาสในการดำเนินการ แต่ต้องเร่งปรับ ปรุงภายในเพื่อให้สามารถขับเคลื่อนหน่วยงานให้นำโอกาสที่มีอยู่มาใช้อย่างมีประสิทธิภาพสูงสุดได้ ผู้ศึกษาได้นำเสนอ เป้าหมาย (END) ของหน่วยงานด้านการขนส่งโดยกำหนดวิสัยทัศน์ “เป็นหน่วยงานบูรณาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่งให้มีความปลอดภัยต่อการใช้งานต่อชีวิตและ ทรัพย์สินของประชาชน ทั้งในระดับชาติ และ ระดับสากล ในการยกระดับขีดความสามารถของหน่วยงานด้านการขนส่งในการป้องกันภัยทางไซเบอร์ ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศภายในปี พ.ศ.2570” เสนอแนะแนวทางในการดำเนินการ (WAYS) กำหนดเป็น **4 ประเด็นยุทธศาสตร์** และได้นำเสนอมาตรการและเครื่องมือ (MEANS) เป็นร่างตัวอย่างโครงการจำนวนรวมทั้งสิ้น **24** โครงการ ที่จะนำไปใช้เป็นกลไกในการขับเคลื่อนหน่วยงานด้านการขนส่งให้บรรลุเป้าหมายที่นำเสนอไว้ การศึกษานี้ มีข้อเสนอแนะในการขับเคลื่อนและการนำยุทธศาสตร์ไปใช้ใน 3 ประเด็นหลักดังนี้ (1) กำหนดระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่งในแต่ละระดับให้ชัดเจน (2) มีมาตรการรักษาความปลอดภัยเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของหน่วยงานด้านการขนส่งและโลจิสติกส์ (3) มีเครื่องมือและกลไกในการป้องกัน เฝ้าระวัง และติดตามภัยคุกคามทางไซเบอร์ และ (4) พัฒนาศักยภาพเทคโนโลยีและบุคลากรในการบริหารจัดการ เพื่อให้สามารถตอบสนอง รับมือเหตุการณ์ละเมิดความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันท่วงที

ผู้จัดทำหวังว่ารายงานฉบับนี้จะให้ความรู้ และเป็นประโยชน์แก่ผู้อ่านทุก ๆ ท่านเพื่อเป็นแนวทางตัวอย่างในการศึกษา หากรายงานฉบับนี้มีข้อผิดพลาดประการใด ผู้เขียนขออภัย ไว้ ณ ที่นี้

นางสาว อธิตานันท์ อภิธนทวีพัฒน์
นักศึกษาหลักสูตรนักยุทธศาสตร์ รุ่นที่ 16

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1 บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศเป็นส่วนสำคัญในการดำรงชีวิตไม่ว่าจะในด้านเศรษฐกิจและสังคม ด้านการเงิน ด้านการรักษาความมั่นคงปลอดภัยและการป้องกันประเทศ ด้านการสื่อสารโทรคมนาคม และการควบคุมดูแลโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) และ ป้องกันโครงสร้างพื้นฐานสาธารณูปโภคที่สำคัญ (CI) และจะเพิ่มความ สำคัญยิ่งขึ้นในอนาคต เนื่องจากความสามารถในการพัฒนาทางเทคโนโลยีสารสนเทศที่รวดเร็วทั้งของ ประเทศชั้นนำด้านเทคโนโลยีสารสนเทศและความสามารถในการพัฒนาและการเข้าถึงเทคโนโลยีสารสนเทศของประเทศที่มีความก้าวหน้าทางเทคโนโลยีในระดับรองลงมา หรือ ประเทศที่กำลังพัฒนาซึ่งความก้าวหน้าทางเทคโนโลยีสารสนเทศจะตอบสนองต่อการใช้งานเครือข่ายเทคโนโลยีสารสนเทศของประชาชนในแต่ละประเทศได้เป็นจำนวนมาก ทั้งกลุ่มที่เป็นผู้ใช้งานเครือข่ายเทคโนโลยีสารสนเทศโดยตรงหรือผู้ที่ได้รับประโยชน์จากการใช้งาน หรือ ผู้ให้บริการเครือข่ายเทคโนโลยีสารสนเทศทั้งในทางตรงและทางอ้อม เช่น การควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญทั้งในภาคการเงินการธนาคาร ภาคตลาดทุน ภาคอุตสาหกรรมการผลิตต่างๆ ภาคการขนส่งหรือคมนาคมทั้งทางน้ำ ทางบกและทางอากาศ ภาคพลังงาน ภาคการสื่อสารโทรคมนาคม ภาคการศึกษา เป็นต้น ซึ่งจะช่วยประหยัดเวลา และ ลดต้นทุนในการดำเนินการ ดังนั้น องค์กรที่มี**โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII)** ซึ่งเป็นระบบสารสนเทศที่หน่วยงานซึ่งเป็น**โครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure หรือ CI)** ใช้ในการดำเนินงานและให้บริการ ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือ องค์กรหรือส่วนงานขององค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงปลอดภัย หรือ ความสงบเรียบร้อยของประเทศ หรือของสาธารณชน หรือ ต่อสาธารณประโยชน์ของประเทศชาติที่จำเป็นต้องมีการกำหนดยุทธศาสตร์ และ แผนปฏิบัติงานที่ชัดเจนรองรับสถานการณ์ภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น และ มีผลกระทบต่อความมั่นคงของประเทศ

จากการศึกษาการใช้ประโยชน์จากเครือข่ายเทคโนโลยีสารสนเทศและระบบดิจิทัลสำหรับประเทศไทยโดย**สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** ได้จัดทำการสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือนและภาคอุตสาหกรรมต่างๆ เป็นครั้งแรกเมื่อ พ.ศ. 2544 และตั้งแต่ พ.ศ. 2546 เป็นต้นมา ได้ทำการสำรวจอย่างต่อเนื่องเป็นประจำทุกปี และในปีพ.ศ. 2564 ได้มีการปรับแผนการสำรวจจากรายปีเป็นรายไตรมาส เนื่องจากมีความต้องการใช้ข้อมูลเทคโนโลยีสารสนเทศและการสื่อสารเพิ่มมากขึ้น โดยจากสถิติของ**สำนัก งานสถิติแห่งชาติฯ** พบว่ามีการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนอายุ 6 ปีขึ้นไป ประมาณ 63.9 ล้านคน พบว่า มีผู้ใช้อินเทอร์เน็ต 52.3 ล้านคน (ร้อยละ 81.8) ใช้โทรศัพท์มือถือ 59.2 ล้านคน (ร้อยละ 92.7) และมีโทรศัพท์มือถือ 54.0 ล้านคน (ร้อยละ 84.5) สำหรับการใช้งานอินเตอร์เน็ต ในช่วงระหว่างปี 2560 – 2564 (ไตรมาส 2) พบว่า ในระยะ 5 ปีนี้ ประเทศไทยมีผู้ใช้อินเทอร์เน็ตเพิ่มขึ้น โดยผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นจากร้อยละ 52.9 ในปี 2560 เป็นร้อยละ 81.8 ในปี 2564 (ไตรมาส 2) (จาก 33.3 ล้านคน เป็น 52.3 ล้านคน) สำหรับการใช้อินเทอร์เน็ตของประชาชนที่อาศัยอยู่ในเขตเทศบาลและนอกเขตเทศบาล ระหว่างปี 2560–2564 (ไตรมาส 2) พบว่า ผู้ใช้อินเทอร์เน็ตมีแนวโน้มเพิ่มขึ้น ทั้งในเขตเทศบาลและนอกเขตเทศบาล คือ ในเขตเทศบาล จากร้อยละ 62.7 ในปี 2560 เป็นร้อยละ

86.9 ในปี 2564 (ไตรมาส 2) ส่วนนอกเขตเทศบาลจากร้อยละ 45.0 ในปี 2560 เป็นร้อยละ 77.7 ในปี 2564 (ไตรมาส 2) เมื่อพิจารณาผู้ใช้อินเทอร์เน็ตเป็นรายภาค ระหว่างปี 2560 – 2564 (ไตรมาส 2) พบว่าในระยะ 5 ปี ผู้ใช้อินเทอร์เน็ตมีแนวโน้มสูงขึ้นทุกภาค ซึ่งในปี 2564 (ไตรมาส 2) กรุงเทพมหานคร มีผู้ใช้อินเทอร์เน็ตสูงที่สุดคือ ร้อยละ 92.8 รองลงมาคือภาคกลางร้อยละ 85.4 ส่วนภาคที่ใช้ต่ำที่สุดคือ ภาคตะวันออก เฉียงเหนือ ร้อยละ 75.4

นอกจากนี้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. ได้มีการสำรวจพฤติกรรมการใช้อินเทอร์เน็ตเป็นประจำทุกปี ปัจจุบันได้เดินทางมาถึงปีที่ 10 (เริ่มสำรวจตั้งแต่ปี 2556-2565) กิจกรรมออนไลน์ที่มีแนวโน้มเติบโตอย่างต่อเนื่อง ได้แก่ การติดต่อสื่อสาร การดูหนัง/ฟังเพลง การซื้อขายของ การทำธุรกรรมทางการเงิน และการอ่านข่าว โพสต์บทความหนังสือ ส่วนกิจกรรมออนไลน์ที่มีแนวโน้มลดลงและอาจจะหายไปในอนาคตได้แก่ การค้นหาข้อมูลโดยใช้ Search Engine การรับ-ส่งอีเมล เพราะ ปัจจุบันผู้ใช้อินเทอร์เน็ตมีทางเลือกในการค้นหาข้อมูล หรือติดต่อสื่อสารมากขึ้น อีกทั้ง Social Media ยังมีการเติบโตมากเมื่อเทียบจากอดีต ทำให้พฤติกรรมค้นหาข้อมูล หรือติดต่อสื่อสารเปลี่ยนไป ตัวอย่างเช่น การค้นหาข้อมูลจากข้อมูลภายในของ Google พบว่า คน GenZ เกือบ 40% ชอบค้นหาข้อมูลบน TikTok และ Instagram มากกว่า Google Search และ Google Maps อีกทั้งในปี 2021 ได้มีการสำรวจ Gen Z และ Gen Y ในสหรัฐเอเมริกา พบว่า 56% ของ Gen Y และ 67% ของ Gen Z แทบจะไม่มีหรือไม่เคยใช้อีเมลในการติดต่อกับเพื่อนและครอบครัว 31% ของกลุ่มคนรุ่นใหม่เหล่านี้ ได้ระบุว่า มีกว่า 1,000 อีเมล ที่ไม่ได้มีการเปิดอ่าน เช่นเดียวกับกิจกรรมการดาวน์โหลดซอฟต์แวร์ เพลง ละคร เกม เพื่อเก็บไว้ดูย้อนหลัง ในอนาคตก็อาจจะไม่มีอีกแล้ว เพราะถูกแทนที่ด้วย Streaming ที่สามารถดูได้แบบ Real-Time และดูย้อนหลังได้ผ่านแพลตฟอร์มนั้น ๆ ในปี 2565 โดยภาพรวมคนไทยใช้เวลาในการเข้าถึงอินเทอร์เน็ตเฉลี่ยอยู่ที่ 7 ชั่วโมง 4 นาทีต่อวัน จากผลการสำรวจพบว่าเจนเนอเรชั่นที่ใช้อินเทอร์เน็ตมากที่สุด คือ Gen Y (ช่วงอายุ 22-41 ปี) อยู่ที่ 8 ชั่วโมง 55 นาทีต่อวัน ในขณะที่ Gen Z (อายุน้อยกว่า 22 ปี) ซึ่งเคยเป็นเจนเนอเรชั่นที่ใช้อินเทอร์เน็ตมากที่สุดในปี 2564 มาในปี 2565 Gen Z ใช้อินเทอร์เน็ตน้อยกว่า Gen Y โดยใช้เวลาในการออนไลน์อยู่ที่ 8 ชั่วโมง 24 นาทีต่อวัน เมื่อพิจารณา 5 อันดับแรกของผู้ที่ใช้เวลาในการเข้าถึงอินเทอร์เน็ตมากที่สุดรายอาชีพ พบว่า ทั้ง 5 กลุ่มอาชีพมีจำนวนชั่วโมงการใช้อินเทอร์เน็ตสูงกว่าค่าเฉลี่ยในภาพรวมแทบทั้งสิ้น โดยข้าราชการ/เจ้าหน้าที่ของรัฐมีการใช้อินเทอร์เน็ตมากที่สุดเมื่อเทียบกับอาชีพอื่น ซึ่งใช้เวลาในการออนไลน์สูงถึง 11 ชั่วโมง 37 นาทีต่อวัน ส่วนหนึ่งเกิดจากผลของสถานการณ์การแพร่ระบาดของ COVID-19 ที่เกิดขึ้นตั้งแต่เมื่อปี 2563 ที่ผ่านมา ทำให้ทุกคนต้องปรับตัวไปสู่ยุควิถีชีวิตใหม่ (New Normal) เร็วขึ้นต้องติดต่อผ่านทางออนไลน์เป็นหลักซึ่งสถานการณ์นี้เองก็ได้ส่งผลกระทบต่อหน่วยงานของรัฐเช่นกัน ทำให้รัฐบาลจำเป็นต้องเร่งปรับตัวให้ทันกับยุค New Normal อย่างรวดเร็วด้วยการเพิ่มช่องทางการให้บริการเป็นแบบออนไลน์เพื่ออำนวยความสะดวกประชาชนได้อย่างทันท่วงที ส่งผลให้ข้าราชการ/เจ้าหน้า ที่ของรัฐต้องปรับตัวด้วยการนำเอาเทคโนโลยีมาใช้ในการทำงานมากยิ่งขึ้น ไม่ว่าจะเป็นการประชุมออนไลน์ (e-Meeting) การจัดทำและส่งไฟล์เอกสารอิเล็กทรอนิกส์ (e-Document) การลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ (e-Signature) เป็นต้น รวมถึงการพัฒนาความพร้อมของบุคลากรภาครัฐที่ต้องทำงาน เพื่อรองรับบริการภาครัฐที่มีให้ บริการประชาชนในรูปแบบออนไลน์เพิ่มมากขึ้น รองลงมาคือนักเรียน/นักศึกษา ใช้เวลาเข้าถึงอินเทอร์เน็ตอยู่ที่ 8 ชั่วโมง 57 นาทีต่อวัน ฟรีแลนซ์ 7 ชั่วโมง 40 นาทีต่อวัน เจ้าของ

กิจการ-ธุรกิจส่วนตัวใช้เวลาเข้าถึงอินเทอร์เน็ต อยู่ที่ 7 ชั่วโมง 29 นาทีต่อวัน และพนักงาน/ลูกจ้างเอกชน ใช้เวลาเข้าถึงอินเทอร์เน็ตอยู่ที่ 7 ชั่วโมง 6 นาทีต่อวัน

จากข้อมูลผลการศึกษา พบว่าการใช้งานเทคโนโลยีสารสนเทศและการเข้าถึงระบบเครือข่ายสารสนเทศทำได้ง่าย และสะดวกสบายต่อการใช้ชีวิตประจำวัน แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดและเสี่ยงที่จะเกิดภัยคุกคามต่อชีวิตเพิ่มขึ้นอีกด้วย กล่าวคือ ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดีใช้ระบบเครือ ข่ายสารสนเทศในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ ภัยที่จะเกิดต่อระบบควบคุมดูแลการใช้งานระบบเครือข่ายสารสนเทศและระบบปฏิบัติการที่เกี่ยวข้องกับโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ ซึ่งก่อ ให้เกิดผลกระทบต่อการใช้ชีวิตของพลเมืองภาคธุรกิจเอกชนและหน่วยงานของรัฐ ทั้งในยามปกติ และ ยามเกิดเหตุฉุกเฉิน ภัยที่ส่งผลกระทบต่อสังคม วัฒนธรรม และธรรมเนียมประเพณีอันดีงามทั้งต่อบุคคลทั่วไป เด็ก สตรี และเยาวชน ตลอดจนผู้สูงอายุ โดยเป็นภัยที่เกิดจากกลุ่มคนที่ไม่ประสงค์ดีหรือรู้เท่าไม่ถึงการณ์ ในการใช้ไซเบอร์สเปซ (Cyber Space) ในทางที่ผิดตลอดจนการใช้ความก้าวหน้าทางเทคโนโลยีไซเบอร์เป็นเครื่องมือในการทำสงครามหรือทำให้ประเทศของตนได้เปรียบ การก่อให้เกิดความขัดแย้งทั้งในระดับประเทศและระดับโลก ดังนั้น การดูแลรักษาความมั่นคงปลอดภัยเครือข่ายเทคโนโลยีสารสนเทศและระบบเครือข่ายให้มีความมั่นคง มีการใช้งานได้อย่างต่อเนื่อง ความสามารถในการป้องกัน แก้ไขปัญหาการถูกโจมตีระบบสารสนเทศ และ การกู้คืนระบบสารสนเทศให้กลับมาใช้งานได้ตามปกติได้อย่างรวดเร็วและป้องกันไม่ให้ระบบเครือข่ายถูกนำไปใช้ในทางที่ผิด จึงเป็นสิ่งสำคัญอย่างยิ่งที่ทุกหน่วยงานจะต้องตระหนักและมีแนวทางการดำเนินงานของแต่ละหน่วยงาน **เพื่อให้การขับเคลื่อนทางเศรษฐกิจ การเมือง สังคมและการป้องกันประเทศ มีภูมิคุ้มกันทางไซเบอร์** และ มีความสามารถในการแข่งขันกับประเทศอื่น ๆ หน่วยงานรัฐบาลไทยได้เล็งเห็นถึงความสำคัญของการดูแลป้องกัน และ การเตรียมพร้อมในการรับมือ แก้ไขปัญหาที่อาจเกิดขึ้นกับระบบเครือข่ายสื่อสารและโครงสร้างพื้นฐานที่สำคัญของประเทศ จึงได้บรรจุประเด็นความมั่นคงไว้ในยุทธศาสตร์ชาติ (พ.ศ. 2561 - 2580) เพื่อเป็นแนวทางให้ประเทศมีแผนการดำเนินงานในการป้องกันปัญหาที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและข้อมูลที่ได้จากอุปกรณ์และเครื่องจักรต่าง ๆ พร้อมกำหนดให้ทุกหน่วยงาน ที่เกี่ยวข้อง ในการป้องกันดังกล่าวดำเนินการจัดทำแผนการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ซึ่งเป็นโครงการเร่งด่วน (Flagship) ที่จะต้องดำเนินการในระยะ 5 ปีแรก (พ.ศ. 2560 - 2565) โดยมอบหมายให้**กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** (ดศ.) ร่วมกับ สมช.เป็นหน่วยงานหลักในการดำเนินการซึ่ง ดศ. ได้ขอให้ทุกหน่วย งานเร่งจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์และเพื่อให้เป็นไปตามยุทธศาสตร์ชาติ

ดังนั้นหน่วยงานที่มีระบบ**โครงสร้างพื้นฐานสำคัญสารสนเทศ** (CII) ในภาคอุตสาหกรรมการขนส่ง หรือ Logistic จึงจำเป็นต้องจัดทำแผนปฏิบัติการ**ด้านความมั่นคงปลอดภัยทางไซเบอร์** เพื่อการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเป็นกรอบในการดำเนินงานของหน่วยงานในสังกัด และ แสดงถึงความพร้อมของหน่วยงานในการตอบสนองต่อการป้องกันภัยคุกคามทางไซเบอร์ในส่วนของโครงสร้างพื้นฐานสำคัญทางสารสน เทศด้านการขนส่งของประเทศ

1.2 วัตถุประสงค์ของการศึกษา

1) เพื่อวิเคราะห์สภาพแวดล้อมที่มีผลกระทบต่อการดำเนินการของ**หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)** ในภาคอุตสาหกรรมการขนส่ง หรือ Logistic ทั้งปัจจัยภายนอก โอกาสและภัยคุกคาม และปัจจัยภายในของจุดอ่อน จุดแข็ง โดยการวิเคราะห์ SWOT Analysis
2) เพื่อจัดทำแผนกลยุทธ์ในการสร้างโอกาสในการพัฒนาขีดความสามารถของ**หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)** ในภาคอุตสาหกรรมการขนส่ง หรือ Logistic. โดยการใช้ TOWS Matrix
3) เพื่อกำหนดมาตรการ นโยบาย และกลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศและตอบโต้ในภาวะวิกฤต หรือฉุกเฉินเพื่อนำไปสู่การป้องกันและการแก้ไขปัญหา
4) เพื่อเป็นแนวทางในการดำเนินงานของ**หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)** ในการพัฒนาให้ความรู้แก่ บุคลากรทางไซเบอร์และผู้ใช้งานทั่วไป ให้ได้รับการปลูกฝังให้ตระหนักในการร่วมกันป้องกันภัยไซเบอร์ทั้งในด้าน ความรับผิดชอบ จริยธรรม และมีความตระหนักรู้ในการบริโภคข้อมูล
5) เพื่อสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการ**หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)** หน่วยงานของรัฐที่เกี่ยวข้อง และ หน่วยงานกำกับดูแลที่เกี่ยวข้อง ในการได้รับการปกป้องจากภัยคุกคามทางไซเบอร์ในทุกรูปแบบต่างๆ อาทิเช่น ระบบขัดข้อง (Disruption) การขโมยข้อมูล (Hack) การเรียกค่าไถ่ข้อมูลสำคัญ (Hijack) การเปลี่ยนแปลงแก้ไขข้อมูลเพื่อการหลอกลวง เผยแพร่ข้อมูลที่ไม่เป็นจริง เป็นต้น

1.3 ขอบเขตของการศึกษา

การจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง (Critical Information Infrastructure หรือ CII for Logistic Industry) ระยะ 5 ปี (พ.ศ. 2566 – 2570) ฉบับนี้ จัดทำภายใต้ขอบเขต ดังนี้

1) ขอบเขตด้านเอกสารและประชากร
   - การวิเคราะห์เอกสาร (Documentary Analysis) ที่น่าเชื่อถือประกอบด้วยข้อมูลสถิติต่างๆ ยุทธศาสตร์ชาติ (พ.ศ. 2561 - 2580) เพื่อเป็นแนวทางให้ประเทศมีแผนการดำเนินงานในการป้องกันปัญหาที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
   - การวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ ประชากร ประกอบด้วย ผู้ใช้งานระบบ ผู้ดูแลระบบ ผู้บังคับบัญชาระดับต้น และผู้ปฏิบัติของหน่วยงาน**ที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)** ในภาคอุตสาหกรรมการขนส่ง หรือ Logistic ในระดับที่เกี่ยวข้อง
2) ขอบเขตด้านพื้นที่ศึกษาจะศึกษาเฉพาะหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) ในภาคอุตสาหกรรมการขนส่ง หรือ Logistic
3) ขอบเขตด้านระยะเวลา ระยะเวลาในการศึกษา ๒ เดือน (มีนาคม – เมษายน ๒๕๖๖)

1.4 ระเบียบวิธีการศึกษา

การศึกษานี้เป็นการวิจัยเชิงบรรยาย (Descriptive Research) และเชิงคุณภาพ (Qualitative Research) มีวัตถุประสงค์เพื่อวิเคราะห์สภาพแวดล้อม ผลกระทบของเหตุการณ์และแนวโน้มที่อาจจะเกิดขึ้น รวมถึงศึกษาทางเลือกในการพัฒนาขีดความสามารถของหน่วยงานและนำเสนอแผนกลยุทธ์ในการสร้างโอกาสและการพัฒนาต่อยอดในอนาคตให้กับหน่วยงาน ซึ่งมีระเบียบวิธีการศึกษา ดังนี้

1) ประชากรและกลุ่มตัวอย่าง ประกอบด้วย ผู้ใช้งานระบบ ผู้ดูแลระบบ ผู้บังคับบัญชาระดับต้น และผู้ปฏิบัติ งานที่เกี่ยวข้อง
2) เครื่องมือในการศึกษา คือ แบบวิเคราะห์การถ่วงน้ำหนักภายในและภายนอก (SWOT Analysis) สำหรับการตรวจสอบตัวแปรสภาพแวดล้อม
3) ขั้นตอนการศึกษาและวิเคราะห์ข้อมูล
    3.1.1 ศึกษาและตรวจสอบสภาวะแวดล้อมทางยุทธศาสตร์ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง ดังนี้
        3.1.1.1 ตรวจสอบสภาวะแวดล้อมภายในของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง ตามกรอบแนวคิดของ McKinsey 7-S Framework เพื่อวิเคราะห์ปัจจัยภายในที่มีผลกระทบกับการบริหารองค์กร ซึ่งประกอบ ด้วย Structure (โครงสร้างองค์กร) Strategy (กลยุทธ์ขององค์กร) Systems (ระบบการดำเนินงานขององค์กร) Style (ลักษณะแบบแผนหรือพฤติกรรมของผู้บริหาร) Staff (บุคลากรในองค์กร) Skills (ความรู้ความสามารถของบุคลากร) และ Shared Values (ค่านิยมขององค์กร)
        3.1.1.2 การวิเคราะห์สภาวะแวดล้อมภายนอกที่มีผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง ตามกรอบ PESTEL (เชิงการเมือง - เศรษฐกิจ - สังคม - เทคโนโลยี - สิ่งแวดล้อม - กฎหมาย) และนำประเด็นจากการวิเคราะห์ตามหลัก PESTEL มาวิเคราะห์ โอกาส (Opportunities) และภัยคุกคาม (Threats) ที่มีผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง
        3.1.1.3 วิเคราะห์และประเมินสภาวะแวดล้อมภายในและภายนอก โดยการตรวจสอบสภาพแวดล้อมขององค์กร การวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ด้วยวิธี SWOT Analysis และให้กลุ่มตัวอย่างให้น้ำหนักเพื่อระบุปัจจัยหลักด้วยวิธีการให้คะแนน เพื่อจัดลำดับความสำคัญของปัจจัย โดยปัจจัยที่มีค่าคะแนนสูงจะเป็นปัจจัยหลัก และ ใช้เทคนิคการจับคู่ (SWOT matching หรือ TOWS Matrix) นำมาจัดกลุ่มกลยุทธ์และสังเคราะห์เป็นกลยุทธ์ทางเลือกเพื่อกำหนดประเด็นยุทธศาสตร์และกลยุทธ์ในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง

3.1.1.4 จัดทำแผนบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง ระยะ 5 ปี (พ.ศ. 2566-2570) และแปลงแผนไปสู่การปฏิบัติ

4) การวิเคราะห์ข้อมูล โดยพิจารณาคัดเฉพาะจุดอ่อน จุดแข็ง โอกาสและอุปสรรค ตามลำดับคะแนนการจัดลำดับความสำคัญของตัวแปร สร้างตาราง Matrix ของแต่ละประเภท

1.5 ข้อจำกัดของการศึกษา

1) การศึกษานี้เป็นการศึกษาเพื่อจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง (ระยะ 5 ปี พ.ศ.2566 – 2570) ภายในระยะเวลามีนาคม ถึง พฤษภาคม 2566 ทำให้มีข้อจำกัดด้านเวลา เนื่องจากกลุ่มตัวอย่างเป็นผู้ใช้งานระบบ ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน และผู้ปฏิบัติงานที่เกี่ยวข้อง รวมถึงหน่วยงานกำกับดูแลที่หลากหลาย และหน่วยงานด้านการขนส่งมีหลายประเภททั้งทางน้ำ ทางบก ทางอากาศ กลุ่มตัวอย่างมีค่อนข้างหลากหลาย จำเป็นต้องใช้เวลาในการนัดหมาย ซึ่งอาจต้องมีการปรับเปลี่ยนตามความเหมาะสม การรวบรวมสถิติบางประเภท จึงอาจทำให้ผลการจัดทำอาจไม่สมบูรณ์ในบางกลุ่มตัวอย่าง
2) เทคโนโลยีสารสนเทศอาจมีการเปลี่ยนแปลงอย่างรวดเร็ว รวมถึงภัยคุกคามทางไซเบอร์ ที่มีรูปแบบเปลี่ยนแปลงไปอย่างรวดเร็วอาจส่งผลต่อการจัดทำข้อมูล และ แผนปฏิบัติงานตามกรอบระยะเวลาที่กำหนด

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ข้อมูลสารสนเทศที่เกิดจากการวิเคราะห์สภาพแวดล้อมและแนวโน้มที่จะเกิดขึ้นเพื่อการวิเคราะห์ผลกระทบ ที่อาจจะเกิดขึ้นนำไปสู่การวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ (SWOT Analysis) และการทำ TOWS Matrix
2) บุคลากรของหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) ประชาชน หน่วยงานภาครัฐและเอกชนมีความเชื่อมั่นในการในการใช้บริการระบบสารสนเทศของหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII)
3) หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) และ หน่วยงานในสังกัดมีเครื่องมือและกลไกในการป้องกัน เฝ้าระวัง และติดตามภัยคุกคามทางไซเบอร์
4) หน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) มีแนวทางการดำเนินงานในการป้องกันและแก้ไขปัญหาที่อาจจะเกิดขึ้นเมื่อเกิดภัยคุกคามทางไซเบอร์
5) ได้แผนปฏิบัติการในการพัฒนาขีดความสามารถของบุคลากรของหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) เพื่อเสนอต่อผู้บริหารของหน่วยงานที่เกี่ยวข้องในปี พ.ศ.๒๕๖๖ – ๒๕๗๐

บทที่ 2 การตรวจสอบสภาวะแวดล้อมและการวิเคราะห์ทางยุทธศาสตร์

สำหรับการจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานด้านการขนส่ง ได้ศึกษายุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564) (National Cyber security Strategy 2017 – 2021) แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเพื่อเป็นกรอบแนวทางการดำเนินงานของหน่วยงานด้านการขนส่ง รวมทั้งได้กล่าวถึงสถานการณ์ด้านกฎหมายในประเทศไทยและการจัดตั้งองค์กรกำกับดูแลด้านไซเบอร์ของประเทศไทย

2.1 สภาวะแวดล้อมภายนอกด้านยุทธศาสตร์และกฎหมายที่เกี่ยวข้อง

2.1.1 ยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐)

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทยมาตรา ๖๕ กำหนดให้รัฐจัดให้มียุทธศาสตร์ชาติเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาลให้สอดคล้องและบูรณาการกันเพื่อให้เกิดพลังผลักดันร่วมกันไปสู่เป้า หมาย โดยยุทธศาสตร์ชาติ ๒๐ ปี (พ. ศ. ๒๕๖๑ – ๒๕๘๐) เป็นยุทธศาสตร์ชาติฉบับแรกของประเทศไทยตามรัฐธรรมนูญซึ่งจะต้องนำไปสู่การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” นำไปสู่การพัฒนาให้คนไทยมีความสุข และ ตอบสนองต่อการบรรลุซึ่งผลประโยชน์แห่งชาติ ในการที่จะพัฒนา คุณภาพชีวิต สร้างรายได้ระดับสูง เป็นประเทศพัฒนาแล้ว และ สร้างความสุขของคนไทย สังคมมีความมั่นคง เสมอภาค เป็นธรรม และ มีระบบเศรษฐกิจที่มีศักยภาพและสามารถแข่งขันได้ประกอบด้วย ๖ ยุทธศาสตร์ ได้แก่

1) ยุทธศาสตร์ชาติด้านความมั่นคง
2) ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน
3) ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์
4) ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม
5) ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม
6) ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

ทั้งนี้ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติได้จัดทำ แผนปฏิบัติการภายใต้ยุทธศาสตร์ชาติ จำนวน 23 ฉบับ แบ่งเป็น 98 แผนย่อย โดยยุทธศาสตร์ด้านความมั่นคง มีแผนปฏิบัติการ ภายใต้ยุทธศาสตร์จำนวน 2 แผนปฏิบัติการ ได้แก่ แผนปฏิบัติการด้านความมั่นคงและแผนปฏิบัติการด้านการต่างประเทศ ในส่วนของแผนปฏิบัติการด้านความมั่นคง ได้กำหนดให้มีการจัดทำแผนการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ เป็นแผนงานจะต้องดำเนินการเร่งด่วนในระยะ 5 ปีแรก โดยมอบหมายให้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสภาความมั่นคงแห่งชาติเป็นหน่วยงานหลักในการดำเนินงาน

2.1.2 ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564)

สำนักงานสภาความมั่นคงแห่งชาติได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) (National Cybersecurity Strategy 2017 – 2021) เพื่อเป็นแนวนโยบายระดับชาติฉบับแรกของไทย ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้รับกับสภาพสังคมที่เข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคตโดยมีเป้าหมายหลักคือการสร้างความพร้อมของประเทศไทยในการรับมือกับภัยคุกคามทางไซเบอร์ที่จะทวีความรุนแรงมากขึ้น ให้ครอบคลุมรอบด้านตามสภาวะแวดล้อม เอื้ออำนวย เสริมขีดความสามารถของไทย ให้มีความเข้มแข็งยิ่งขึ้น โดยมุ่งเน้นการมีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐานการสร้างความตระหนักในทุกภาคส่วนและสร้างความร่วมมือกับต่างประเทศโดยกำหนดกลยุทธ์เพื่อให้การดำเนินงานประสบผลสำเร็จไว้ 6 กลยุทธ์ ได้แก่

กลยุทธ์ที่ ๑ พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือนและตำรวจ และภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล

กลยุทธ์ที่ ๒ พัฒนากรอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 3 พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญ ของภัยคุกคามความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 4 ปกป้อง ป้องกัน ภัยคุกคามทางไซเบอร์สงครามไซเบอร์ และเสริมสร้างความ ปลอดภัยทางไซเบอร์โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้าง เครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ

กลยุทธ์ที่ 5 พัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์

กลยุทธ์ที่ 6 ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน/บุคลากรที่เกี่ยวข้อง ให้มีความรู้ ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

พร้อมทั้งกำหนดประเด็นยุทธศาสตร์เพื่อให้บรรลุตามเป้าหมายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ไว้ ๘ ประเด็นยุทธศาสตร์ ดังนี้

ประเด็นยุทธศาสตร์ที่ ๑ : เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

แนวทางการดำเนินการ :

๑) ระดับนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) พัฒนาโครงสร้างองค์กรในภาครัฐ เพื่อรองรับสังคมดิจิทัล และรับมือภัยคุกคามทางไซเบอร์เพื่อเสริมสร้างความไว้วางใจแก่ภาคส่วนต่าง ๆ ที่ติดต่อประสานงานกับรัฐ

๓) ส่งเสริมการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ต เพื่อการบริการประชาชน ของหน่วยงานของรัฐและการประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบและมั่นใจในการใช้บริการของหน่วยงานของรัฐ

๔) ส่งเสริมให้ภาครัฐมีความโปร่งใส โดยใช้เทคโนโลยีและดำเนิน กิจกรรมทางไซเบอร์โดยคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพ ตลอดจนความเป็นส่วนตัวของผู้ใช้บริการออนไลน์ของภาครัฐ

๕) สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่าง ๆ นอกเหนือ จากภาครัฐ โดยการเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐ ในการพัฒนา ปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์ เพื่อให้ตรงตามความต้องการและวัตถุประสงค์ของ ผู้รับบริการ

๖) ส่งเสริมให้ภาคเอกชนในธุรกิจสาขาต่าง ๆ ในทุกระดับดำเนิน ธุรกิจโดยใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ตและไซเบอร์สเปซในวงกว้างและได้มาตรฐาน โดยประชาสัมพันธ์เชิง รุกและขอความร่วมมือจากภาคเอกชน

ประเด็นยุทธศาสตร์ที่ ๒ : ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบ สารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

แนวทางการดำเนินการ :

1) จัดทำกรอบนโยบาย/ยุทธศาสตร์การรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ และ ทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อการปรับปรุงนโยบายให้ทันกับ สถานการณ์ที่เปลี่ยนไป

2) ให้มีการจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ระดับชาติเพื่อทำหน้าที่เป็นศูนย์กลางระดับนโยบายที่ขึ้นตรงต่อนายกรัฐมนตรี โดยเป็น ศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์ และประสานการปฏิบัติ ทั้งในด้านการประสานงาน เฝ้าระวัง การ ตอบสนอง บริหารจัดการภัยคุกคามทางไซเบอร์ สร้างความตระหนักตลอดจนประสานความร่วมมือทั้งในและ ต่างประเทศและส่งเสริมการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานต่าง ๆ โดย อาจพิจารณาจัดตั้งหน่วยปฏิบัติขึ้น เพื่อสนับสนุนการดำเนินงานตามความเหมาะสม

3) จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบ สารสนเทศทั้งของภาครัฐและเอกชนพร้อมจัดลำดับความสำคัญเพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ

4) กำหนดบทบาทและหน้าที่ของหน่วยงานต่าง ๆ ของรัฐ ในด้านการปกป้องโครงสร้างพื้นฐานสำคัญที่มีการบริหารจัดการด้วยระบบสารสนเทศให้มีความชัดเจน เพื่อการรับมือภัย คุกคามทางไซเบอร์ทั้งในยามปกติ ยามเกิดเหตุ การฟื้นตัวและฟื้นฟูหลังเกิดเหตุ รวมทั้งการเยียวยา แก้ไขผลกระทบรวมทั้งมีกลไกประสานความร่วมมือ กับภาคเอกชนและผู้มีส่วนเกี่ยวข้องเพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของไทยจากภัยคุกคามทางไซเบอร์

5) ส่งเสริมกำรจัดทำแผนกำรปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการ ด้วยระบบสารสนเทศ ทั้งในภาครัฐและเอกชน โดยให้แต่ละองค์กรยึดถือหลักการปกป้องโครงสร้างพื้นฐานสำคัญ ที่บริหารจัดการด้วยระบบสาร

สนเทศของหน่วยงาน โดยอาศัยศักยภาพของหน่วยงานและ ในกรณีที่สถานการณ์ยกระดับหรือเป็นเหตุฉุกเฉินที่เกินความสามารถของหน่วยงาน สามารถประสานขอความ สนับสนุนได้ทันต่อสถานการณ์

6) ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือกับสถานการณ์ทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ

7) จัดทำร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติและข้อกำหนด เพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์โดยพิจารณากำหนดบทคุ้มครองและบทลงโทษ ที่เหมาะสม

8) พัฒนาศักยภาพของบุคลากรในภาครัฐผ่านการศึกษา ฝึกอบรม ในรูปแบบต่าง ๆ และส่งเสริมการถ่ายทอดความรู้ภายในภาครัฐหรือระหว่างภาครัฐกับเอกชน ตลอดจนให้ ความสำคัญกับการพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์อย่างเหมาะสม เพื่อเป็นการรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้อยู่ในระบบราชการ

9) พัฒนาศักยภาพการวิจัยและพัฒนาด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ ตลอดจนแสวงหาความร่วมมือกับเอกชนทั้งในและต่างประเทศ เพื่อสามารถเข้าถึงแหล่ง เทคโนโลยีและแหล่งเงินทุน ตลอดจนการพัฒนาตลาดสำหรับอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศไทย เพื่อนำไปสู่การลดการพึ่งพาจากต่างประเทศ

10) ส่งเสริมการมีส่วนร่วมของภาคเอกชนอย่างจริงจังในการรักษา ความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านการพัฒนาองค์ความรู้และเทคโนโลยี การพัฒนาบุคลากร การรักษาความ มั่นคงปลอดภัยเพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม

11) พัฒนามาตรฐานและกระตุ้นให้มีกลไกการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ ในภาพรวมของประเทศ

12) ส่งเสริมให้มีการทำงานด้วยการปรับใช้มาตรการทางเทคนิคในลักษณะการทำงานแบบศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ หรือ CERT โดยเฉพาะอย่างยิ่ง ในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้มีการประสานการทำงานรับมือกับภัยคุกคามทางไซเบอร์ ในทางปฏิบัติให้มีความเข้มแข็งมากยิ่งขึ้น

ประเด็นยุทธศาสตร์ที่ ๓ : ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

แนวทางการดำเนินการ :

1) ศึกษา ติดตาม และวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งภัยคุกคามในรูปแบบเดิมและรูปแบบใหม่ เพื่อทราบถึงแนวโน้มความเป็นไปได้ที่จะเกิดภัยคุกคาม รวมถึงเป็นประโยชน์ต่อการหาทางป้องกันไม่ให้เกิดเหตุหรือลดความเสียหายให้น้อยลงมากที่สุด

2) หน่วยงานความมั่นคงที่เกี่ยวข้องพิจารณาจัดทำนโยบาย/ยุทธศาสตร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์ และบริหารจัดการการเก็บรักษาข้อมูล ป้องกันการโจมตี หรือเจาะระบบ การใช้เครื่องมือทางไซเบอร์เพื่อสร้างความขัดแย้ง รวมทั้งประเมินสถานการณ์และทบทวน นโยบาย/ยุทธศาสตร์ด้านไซเบอร์ให้ทันสมัย

3) กำหนดบทบาทให้กองทัพดูแลรับผิดชอบการป้องกันประเทศ ในมิติทางไซเบอร์และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการมอบหมายจากรัฐบาลโดยเฉพาะเมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๔ : เสริมสร้างระบบเศรษฐกิจดิจิทัล

แนวทางการดำเนินการ :

1) ส่งเสริมการพัฒนาขีดความสามารถหรือการดำเนินการที่ สนับสนุนต่อการเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลอย่างสมดุล ราบรื่น คุณภาพและนำไปสู่เศรษฐกิจดิจิทัลที่ยั่งยืน

2) สนับสนุนการมีส่วนร่วมของภาคเอกชน ในการส่งเสริม เศรษฐกิจดิจิทัลกับภาครัฐ ทั้งในกลุ่มผู้ที่ใช้เทคโนโลยีดิจิทัลเพื่อดำเนินธุรกิจอยู่แล้ว และส่งเสริมการใช้ เทคโนโลยีดิจิทัลในวงกว้าง

3) พัฒนา ปรับปรุงยุทธศาสตร์ แผนหรือแผนงานตลอดจนกฎหมาย ระเบียบปฏิบัติที่เหมาะสมสอดคล้องและเอื้ออำนวยต่อเศรษฐกิจดิจิทัล พร้อมทั้งมีการประเมินผลและทบทวน อย่างสม่ำเสมอโดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์แผนหรือแผนงานดังกล่าว

ประเด็นยุทธศาสตร์ที่ ๕ : สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางการดำเนินการ :

๑) ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วนโดยทั่วถึง ผ่านสื่อและกลไกต่าง ๆ ของภาครัฐ ภาคเอกชน และภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคาม ทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการใช้เทคโนโลยีดิจิทัลและ การดำเนินกิจกรรมทางไซเบอร์ได้อย่างปลอดภัยและเกิดประโยชน์รวมทั้งส่งเสริมความร่วมมือด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่ม ทั้งในระดับบุคคลและองค์กร

๒) ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถาบันการศึกษาต่าง ๆ ในการแลกเปลี่ยนความรู้ การวิจัยร่วมกันและ/หรือการนำเสนองานวิจัย ตลอดจนการจัดทำคู่มือเผยแพร่ ความรู้เกี่ยวข้องกับด้านไซเบอร์เช่น มหาวิทยาลัย สถาบันวิชาการ เป็นต้น

๓) ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐาน ทั้งสายสามัญและอาชีวะ โดยให้เนื้อหาของ หลักสูตร มีความแตกต่างกันไปในแต่ละระดับการศึกษา

๔) ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่ประชาชนผู้ใช้อินเทอร์เน็ตทั่วไป ผู้สูงอายุ เด็ก สตรีและเยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับ สถานศึกษา องค์การบริหารส่วนท้องถิ่นและหน่วยงานที่เกี่ยวข้อง เพื่อเผยแพร่ความรู้และสร้างความตระหนัก อย่างเป็นระบบและต่อเนื่อง

๕) ส่งเสริมและประสานความร่วมมือ ระหว่างรัฐกับเอกชนและภาคประชาสังคม เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์รวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกัน เพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชน และภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของ

ภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหา ประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุน และการเป็นผู้ร่วมรักษาความ มั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ : เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

แนวทางการดำเนินการ :

๑) ส่งเสริมค่านิยมอันดีงามของชาติบนโลกไซเบอร์ โดยส่งเสริม การใช้เทคโนโลยีสารสนเทศและการสื่อสาร ของประชาชนให้เป็นไปเพื่อการธำรงไว้ซึ่ง ชาติ ศาสนา และ พระมหากษัตริย์

๒) ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซ (Cyber Space) ด้วย ความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย

ประเด็นยุทธศาสตร์ที่ ๗ : ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

แนวทางการดำเนินการ:

1) ยกระดับและกำหนดบทบาทของผู้บังคับใช้กฎหมาย ได้แก่ เจ้าหน้าที่ตำรวจ เจ้าหน้าที่กรมสอบสวนคดีพิเศษ และเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้อง ในการสืบสวนทาง ไซเบอร์เพื่อค้นหาตัวผู้กระทำผิดมาลงโทษ

2) ส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวน และงานข่าว ตลอดจนส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยในงานสืบสวนและงานข่าว

3) ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรมเพื่อ เพิ่มประสิทธิภาพการจัดการภัยคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์

4) ส่งเสริมความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ตลอดจนประสบการณ์และแนวปฏิบัติที่ดีกับต่างประเทศ ทั้งในระดับทวิภาคีและกับองค์การระหว่างประเทศที่ เกี่ยวข้อง อาทิ ตำรวจสากล เพื่อการพัฒนาขีดความสามารถในการป้องกันและปราบปรามอาชญากรรมของไทย โดยเฉพาะประโยชน์ในการสืบสวนและการข่าว

5) ส่งเสริมและสนับสนุนการพัฒนาระเบียบและกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๘ : ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

แนวทางการดำเนินการ:

1) สนับสนุนให้มีการใช้ไซเบอร์สเปซ (Cyber Space) ในทางสันติ โดยไม่ใช้เทคโนโลยีสารสนเทศเพื่อการสร้างความขัดแย้ง ตลอดจนร่วมมือกับมิตรประเทศ ในการต่อต้านการใช้ เทคโนโลยีสารสนเทศเพื่อสนับสนุนการก่ออาชญากรรมข้ามชาติหรือการกระทำที่สร้างความเสียหาย

2) สนับสนุนการแลกเปลี่ยนองค์ความรู้ ข้อมูล แนวปฏิบัติ ที่ดีด้าน ไซเบอร์กับต่างประเทศ ทั้งในระดับทวิภาคี ระดับภูมิภาคและระดับพหุภาคี

3) มีช่องทางการสื่อสารแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ ชัดเจนในการร่วมมือกับต่างประเทศในการตอบสนองและรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

4) มีบทบาทในการส่งเสริมการหารือเกี่ยวกับบรรทัดฐาน มาตรฐาน และมาตรการสร้างความไว้วางใจหรือความเชื่อมั่นระหว่างประเทศในมิติไซเบอร์ รวมถึงการมีท่าทีร่วมกันในระดับ ภูมิภาค เพื่อให้บรรทัดฐานระหว่างประเทศเป็นที่ยอมรับและสะท้อนผลประโยชน์ของไทยและประเทศในภูมิภาค

2.1.3 แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์

ตามยุทธศาสตร์ชาติด้านความมั่นคง ได้กำหนดแผนงาน/โครงการเร่งด่วน (Flagship) ในช่วงระยะ 5 ปีแรก (พ.ศ. 2561 – 2565) ประกอบด้วย 4 แผน โดยแผนการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์เป็นหนึ่งในแผนที่จะต้องเร่งดำเนินการในระยะ 5 ปีแรก โดยมีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสภาความมั่นคงแห่งชาติเป็นหน่วยงานหลัก ในการจัดทำแผนดังกล่าว ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหา ด้านความมั่นคงปลอดภัยทางไซเบอร์ไว้เป็นแนวทางให้ทุกหน่วยงานนำไปประกอบการจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์โดยได้กำหนดกลยุทธ์ในการให้บรรลุเป้าหมายไว้ 9 กลยุทธ์ ดังนี้

กลยุทธ์ที่ 1 กำหนดแนวความคิดมาตรการมาตรฐานระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

กลยุทธ์ที่ 2 การจัดองค์กรโครงสร้างอำนาจหน้าที่ขีดความสามารถในงานความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 3 กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน

กลยุทธ์ที่ 4 ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน

กลยุทธ์ที่ 5 ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ 6 การป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

กลยุทธ์ที่ 7 การสร้างความตระหนักรู้ประชาชนและหน่วยงาน

กลยุทธ์ที่ 8 การปรับปรุงแก้ไขกฎหมาย

กลยุทธ์ที่ 9 การพัฒนาศักยภาพบุคลากรและเทคโนโลยี แต่ละกลยุทธ์ได้กำหนดแนวทางการดำเนินงานเพื่อให้หน่วยงานที่เกี่ยวข้องนำไปประกอบการ พิจารณาดำเนินการ โดยมีรายละเอียด ดังนี้

กลยุทธ์ที่ 1 กำหนดแนวความคิดมาตรการมาตรฐานระบบบริหารจัดการในการป้องกัน ความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

แนวทางการดำเนินงาน :

บริหารจัดการนโยบายมาตรการมาตรฐานและความร่วมมือทุกภาคส่วนทั้ง ภายในประเทศและต่างประเทศโดยกำหนดกรอบแนวคิดด้านไซเบอร์ทั้งระบบ โดยมีการระบุผู้รับผิดชอบ แนวทางการติดตามและประเมินผลให้ครอบคลุมการปฏิบัติงาน ๘ ด้าน ได้แก่

1) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพการตอบสนองต่อภัยคุกคามไซเบอร์

3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของประเทศ

4) การประสานความร่วมมือระหว่างภาครัฐเอกชนและประสานความ ร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ทั้ง ภาครัฐและเอกชน

7) การสร้างความตระหนักและความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

8) การพัฒนาระเบียบและกฎหมายเพื่อความมมั่นคงปลอดภัยไซเบอร์

หน่วยงานรับผิดชอบหลัก :

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม /สภาความมั่นคงแห่งชาติ/ หน่วยงานที่ตั้งใหม่

หน่วยงานสนับสนุน : สภาความมั่นคงแห่งชาติหน่วยงานด้านการขนส่ง สำนักงานพัฒนารัฐบาลดิจิทัล หน่วยงานกำกับดูแล (เช่น สำนักงานคณะกรรมการกิจการกระจาย กิจการโทรทัศน์ และกิจการโทรคมนาคม แห่งชาติ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์คณะกรรมการ กำกับและส่งเสริมการประกอบธุรกิจประกันภัย) และหน่วยงานสายความมั่นคง กระทรวงกลาโหม (กองบัญชาการกองทัพไทย) สำนักงานข่าวกรองแห่งชาติสำนักงานตำรวจแห่งชาติ(กองบังคับการปราบปราม การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี) กระทรวงยุติธรรม กระทรวงการต่างประเทศ กระทรวงศึกษาธิการ กระทรวงวิทยาศาสตร์และเทคโนโลยีกระทรวงพาณิชย์และภาคเอกชน

กลยุทธ์ที่ 2 การจัดองค์กรโครงสร้างอำนาจหน้าที่ขีดความสามารถในงานความมั่นคงปลอดภัยไซเบอร์

แนวทางการดำเนินงาน : จัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ประเทศ โดยมีรูปแบบขององค์กร เป็น 2 แนวทาง ดังนี้

1) โครงสร้างและอำนาจหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Cyber Security Agency: CSA) เป็นหน่วยงานราชการอยู่ภายใต้สำนักนายกรัฐมนตรีหรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

2) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. (National Cybersecurity Committee: NCSC) ประกอบด้วย นายกรัฐมนตรีเป็นประธานกรรมการ และมีองค์ประกอบ ๓ คณะ ได้แก่ คณะกรรมการกำกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ คณะกรรมการส่งเสริมด้านโครงสร้างพื้นฐานสำคัญทางเทคโนโลยีสารสนเทศแห่งชาติ

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / สภาความมั่นคงแห่งชาติ

หน่วยงานสนับสนุน : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สภาความมั่นคงแห่งชาติ สำนักงานคณะกรรมการพัฒนาระบบราชการ และ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

กลยุทธ์ที่ 3 กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน

แนวทางการดำเนินงาน :

กำหนดการบริหารจัดการและแนวปฏิบัติร่วมให้เป็นไปตามมาตรฐานสากล เพื่อเตรียมรับมือความเสี่ยงและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ครอบคลุมสภาวะปกติและสภาวะที่เกิด ภัยคุกคามไซเบอร์แบ่งเป็น 4 ระดับ ได้แก่

1) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับหน่วยงานบริหารจัดการ โดยหน่วยงานเองและโดยมีSector-based CERTหรือ ThaiCERT เป็นหน่วยงานสนับสนุน

2) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับกลุ่มหน่วยงาน (sector) บริหารจัดการโดยหัวหน้าหน่วยงานกำกับดูแล (Regulator) ตนเอง และ มี ThaiCERT เป็นหน่วยงานสนับสนุน เพื่อให้ปฏิบัติตามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

3) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับเกินกว่า 1 กลุ่ม (sector) ให้บริหารจัดการโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและมีหน่วยงานความมั่นคง สนับสนุนการดำเนินงาน

4) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับประเทศบริหารจัดการ โดยหน่วยงานด้านความมั่นคงจะต้องสร้างความรับรู้ความเข้าใจกับหน่วยงานภาครัฐหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ ตลอดจนภาคเอกชนที่มีความเกี่ยวข้องด้านเศรษฐกิจ หรือมีความเกี่ยวข้องหากถูก โจมตีและกระทบต่อความมั่นคงของประเทศให้รับทราบถึงแนวทางปฏิบัติและแนวทางการแก้ไขปัญหา ตลอดจนการตอบโต้หรือฟื้นฟูในกรณีที่มีเป็นปัญหารุนแรง มีการซ้อมรับมือภัยคุกคามจากการจำลอง สถานการณ์ที่อาจเกิดขึ้นจริง

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/สภาความมั่นคงแห่งชาติ/หน่วยงานที่ตั้งใหม่

หน่วยงานสนับสนุน : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สภาความมั่นคงแห่งชาติ หน่วยงานด้านการขนส่ง สำนักงานพัฒนารัฐบาลอิเล็กทรอนิกส์หน่วยงานกำกับดูแล (เช่น สำนักงานคณะกรรมการกิจการกระจาย กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์คณะกรรมการกำกับและส่งเสริมการประกอบ ธุรกิจประกันภัย) หน่วยงานความมั่นคง สถาบันการเงินภาคเอกชน และหน่วยงานสำคัญที่เกี่ยวข้อง

กลยุทธ์ที่ 4 ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน

แนวทางการดำเนินงาน :

ส่งเสริมการพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ ที่เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์ที่บูรณาการความร่วมมือ หน่วยงานทหารและพลเรือนที่เกี่ยวข้องทั้งในระดับนโยบายและระดับปฏิบัติเพื่อให้การบริหารจัดการ การสั่งการ และการรายงานรวมถึงการแจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟูปราบปรามปัญหาภัยคุกคามไซเบอร์ ในสภาวะปกติมีหน่วยงานของสำนักนายกรัฐมนตรีหรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นผู้รับผิดชอบ หลักและกรณีสภาวะไม่ปกติ(เกิดสงครามไซเบอร์) มีหน่วยงานความมั่นคง เป็นผู้รับผิดชอบหลัก เพื่อให้เกิด ความรวดเร็วมีประสิทธิภาพ และมีกลไกสนับสนุนการดำเนินงานที่ชัดเจน

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / สภาความมั่นคงแห่งชาติ/ หน่วยงานภาครัฐ/หน่วยงานที่ตั้งใหม่

หน่วยงานสนับสนุน : สภาความมั่นคงแห่งชาติหน่วยงานด้านการขนส่ง สำนักงานพัฒนารัฐบาลดิจิทัล หน่วยงานกำกับดูแล(เช่น สำนักงานคณะกรรมการกิจการกระจายกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์คณะกรรมการกำกับ และส่งเสริมการประกอบธุรกิจประกันภัย) และหน่วยงานความมั่นคง สถาบันการเงิน ภาคเอกชนและหน่วยงานสำคัญที่เกี่ยวข้อง

กลยุทธ์ที่ 5 ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

แนวทางการดำเนินงาน :

กำหนดให้หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศต้องจัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหาร จัดการด้วยระบบสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานมีความพร้อม สามารถป้องกันและตอบสนองต่อปัญหาที่เกิดขึ้นได้ ในกรณีที่สถานการณ์ยกระดับหรือมีความรุนแรงเกินความสามารถของหน่วยงาน สามารถประสานขอรับการสนับสนุนจาก หน่วยงานกำกับดูและ/หรือหน่วยงานกลางที่มีหน้าที่ดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับประเทศ นอกจากนี้จะต้องฝึกซ้อมรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ เพื่อให้มีความพร้อมทั้งในระดับ หน่วยงานและระดับภาคกลุ่ม (Sector) รวมทั้งต้องมีการตรวจสอบและประเมินระดับความพร้อมของหน่วยงาน ให้อยู่ในระดับความมั่นคงปลอดภัยที่ได้มาตรฐานสากล

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ ทุกกระทรวง

หน่วยงานสนับสนุน : กลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศสำนักงานพัฒนาธุรกรรม ทางอิเล็กทรอนิกส์ (องค์การมหาชน) สภาความมั่นคงแห่งชาติ หน่วยงานด้านการขนส่ง สำนักงานพัฒนารัฐบาลดิจิทัล หน่วยงานกำกับดูแล (เช่น สำนักงานคณะกรรมการกิจการกระจายกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์คณะกรรมการกำกับ และส่งเสริมการประกอบธุรกิจประกันภัย) และหน่วยงานความมั่นคง

กลยุทธ์ที่ 6 การป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

แนวทางการดำเนินงาน :

1) ส่งเสริมวัฒนธรรมการใช้อินเทอร์เน็ตสร้างสรรค์และรับผิดชอบทั้งในระดับ บุคคลและองค์กรมีจิตอาสานึกต่อผู้อื่นและสังคม โดยต้องเคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย
2) ส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชน เพื่อการ ธำรงไว้ซึ่งชาติศาสนาและพระมหากษัตริย์
3) ส่งเสริมการมีส่วนร่วมของภาคเอกชนและภาคประชาสังคม
4) ส่งเสริมการผลิตเผยแพร่สื่อที่ปลอดภัยและสร้างสรรค์รวมถึงการป้องกัน ตรวจสอบสื่อที่เป็นเท็จ

5) ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรม
6) ส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาสนับสนุนงานสืบสวนและงานข่าว และส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวนและงานข่าวให้มีความสามารถวิเคราะห์ สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ทันสมัยครอบคลุมรอบด้านต่อเนื่องและถูกต้องแม่นยำ
7) สร้างความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสารตลอดจนประสบการณ์ และแนวปฏิบัติที่ดีระหว่างหน่วยงานภายในประเทศ หน่วยงานต่างประเทศทั้งในระดับภูมิภาคและนานาชาติ
8) มีมาตรการการป้องปรามปราปรามจับกุมและลงโทษในกลุ่มบุคคลหรือบุคคลที่ไม่ประสงค์ดีต่อ ความมั่นคงของประเทศซึ่งจะต้องถูกดำเนินการตามกฎหมายที่โดยต้องสอดคล้องกับแนวทางปฏิบัติตามพระราช บัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐และฉบับแก้ไข เพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

   หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / หน่วยงานที่ตั้งใหม่

   หน่วยงานสนับสนุน : กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรและหน่วยงานความมั่นคง

กลยุทธ์ที่ 7 การสร้างความตระหนักรู้ประชาชนและหน่วยงาน

แนวทางการดำเนินงาน :

ส่งเสริมให้กับประชาชนและทุกหน่วยงานทั่วประเทศมีความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์ สร้างวัฒนธรรมการมีคุณธรรมและจริยธรรมในการใช้ไซเบอร์อย่างถูกต้อง และ สร้างสรรค์มีความรับผิดชอบและมีจิตสานึกต่อผู้อื่นและสังคม โดยต้องเคารพสิทธิเสรีภาพขั้นพื้นฐาน บนไซเบอร์และไม่ละเมิดกฎหมาย ดำเนินการโดยอาศัยความร่วมมือกับหน่วยงานภาครัฐ ภาคเอกชน สถาบันการศึกษา และหน่วยงานที่เกี่ยวข้องในพื้นที่ในการเผยแพร่ความรู้ประชาสัมพันธ์ข้อมูลข่าวสารและยกระดับความตระหนักรู้อย่างเป็นระบบและต่อเนื่องโดยให้ความสำคัญกับกลุ่มเป้า หมายที่เป็นกลุ่มเสี่ยงต่อภัยไซเบอร์กลุ่มที่ขาดความเข้าใจเทคโนโลยีสมัยใหม่และกลุ่มที่ไม่มีโอกาสเข้าถึงความรู้หรือได้ รับการฝึกสอนรวมถึง กลุ่มที่อยู่ห่างไกลความเจริญ

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / หน่วยงานที่ตั้งใหม่

หน่วยงานสนับสนุน : สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงมหาดไทย กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์กระทรวงศึกษาธิการ กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงสาธารณะสุข กรมประชาสัมพันธ์และภาคเอกชน

กลยุทธ์ที่ 8 การปรับปรุงแก้ไขกฎหมาย

แนวทางการดำเนินงาน : ส่งเสริมและสนับสนุนการทบทวนปรับปรุงและพัฒนากฎหมายและ มาตรการต่าง ๆ ที่เกี่ยวข้องเพื่อให้ทันต่อความก้าวหน้าและการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล และ สอดคล้องกับแนวปฏิบัติและ/หรือกฎหมายสากล โดยจัดให้มีกลไกส่งเสริมการมีส่วนร่วมของตัวแทนทุกภาค ส่วนที่เกี่ยวข้องเมื่อมีการปรับปรุง

และพัฒนากฎหมาย/มาตรฐาน/มาตรการต่าง ๆ ส่งเสริมการสร้างกลไกการ บังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น ในการป้องกันและปราบปรามการกระทำความผิดที่มีผลกระทบต่อ ความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รวมถึงงานสืบสวนและป้องกันอาชญากรรมไซเบอร์และผลักดัน ให้มีกลไกสำหรับตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / สภาความมั่นคงแห่งชาติ/หน่วยงานที่ตั้งใหม่

หน่วยงานสนับสนุน : สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานพัฒนาธุรกรรม ทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานตำรวจแห่งชาติสำนักงานข่าวกรองแห่งชาติกระทรวงยุติธรรม กลยุทธ์ที่ 9 การพัฒนาศักยภาพบุคลากรและเทคโนโลยี

แนวทางการดำเนินงาน :

พัฒนาศักยภาพขององค์กรและบุคลากรให้มีทักษะความรู้เพื่อเพิ่มขีดความสามารถในการป้องกันตนเองและหน่วยงานลดความเสี่ยงและลดความเสียหายจากการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้น พัฒนากำลังคนในทุกระดับตั้งแต่การส่งเสริมระดับสถานศึกษาเพื่อการสร้างบุคลากรรองรับความต้องการในอนาคตเพื่อยกระดับความพร้อมของประเทศในการรับมือ และ จัดการกับภาวะความเสี่ยงภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต โดยต้องเพิ่มจำนวน และคุณภาพของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความรู้และทักษะเทียบเท่ากับสากลเช่นมีใบรับรองความสามารถที่เป็นที่ยอมรับของสากลกำหนดมาตรฐานวิชาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากลสร้างแรงจูงใจและให้การสนับสนุนในการสร้างความเติบโตในสายอาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้ยั่งยืน

หน่วยงานรับผิดชอบหลัก : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม / หน่วยงานด้านความมั่นคง

หน่วยงานสนับสนุน : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงาน คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติกระทรวงศึกษาธิการ กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงมหาดไทย กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์กระทรวงยุติธรรม สำนักงานตำรวจ แห่งชาติสำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานข่าวกรองแห่งชาติ

2.1.4 กฎระเบียบที่เกี่ยวข้อง

1) กฎหมายว่าด้วยธุรกรรมการอิเล็กทรอนิกส์

ประเทศไทยได้มีการประกาศใช้กฎหมายเกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งได้กำหนดมาตรการเพื่อลดความเสี่ยงและ ทำให้เกิดความน่าเชื่อถือต่อการใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ต ในการทำธุรกรรมทางอิเล็กทรอนิกส์ และมีการกำหนดบทลงโทษสำหรับการก่ออาชญากรรมคอมพิวเตอร์นอกจากนี้ยังได้มีการกำหนดกฎกระทรวง ประกาศ ระเบียบเพื่อการบังคับใช้กฎหมายดังกล่าว อาทิ กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551 ประกาศ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องกำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2) กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์

ด้วยวิวัฒนาการเทคโนโลยีอินเทอร์เน็ตมีการเติบโตและมีพัฒนาอย่างรวดเร็ว กฎหมายที่ใช้ในการกำกับดูแลอาจจะไม่สามารถบังคับใช้หรือไม่สามารถกำกับดูแลกับสภาพปัญหาดังกล่าวได้ เช่น การใช้เงินสกุลดิจิทัล หรือการเข้ารหัสข้อมูลที่มีความซับซ้อน และ มิได้ถูกกำหนดจากกฎหมายภายในประเทศ ทำให้ภาครัฐไม่สามารถตรวจสอบการดำเนิน การภายใต้กิจกรรมดังกล่าวได้และกฎหมายอาจจะไม่เอื้ออำนวยในการดำเนินการจะเห็นได้ว่าประเทศยักษ์ใหญ่อย่างสหรัฐ อเมริกา จีน รวมทั้งประเทศในยุโรปและอาเซียน ต่างมีกฎหมายไซเบอร์เป็นกฎหมายกลาง เพื่อเป็นกลไกสำคัญในการสร้างความเชื่อมั่นให้กับระบบเศรษฐกิจและสังคมดิจิทัล และสำหรับประเทศไทยได้มีการเตรียมความพร้อมในเรื่องดังกล่าว โดยการจัดทำกฎหมายกลางเพื่อดูแลเรื่องความมั่นคงปลอดภัยไซเบอร์ของประเทศ คือ “พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. พ.ศ.2562” เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ ที่ผ่านมาประเทศไทยยังไม่มีองค์กรหรือหน่วยงานหลัก ที่ทำหน้าที่ในการกำกับดูแลด้านไซเบอร์อย่างเป็นรูปธรรม ดังนั้น “พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562” จึงได้มีการกำหนดให้มีการจัดตั้งองค์กร เพื่อรับผิดชอบในการขับเคลื่อนนโยบายความมั่นคงปลอดภัยไซเบอร์ไปสู่การปฏิบัติ การจัดทำแผนและนโยบายแห่งชาติ และ การประสานการดำเนินการระหว่างหน่วยงานที่เกี่ยวข้อง ในลักษณะองค์รวมของประเทศทั้งภาครัฐ ภาคเอกชน และภาคประชาชนในสถานการณ์ทั่วไป หรือสถานการณ์ภัยต่อความมั่นคงปลอดภัย ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงได้มีการออกกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งนี้ เพื่อเป็นการดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ จึงมีหน่วยงานที่เกี่ยวข้องในการรับผิดชอบ จำนวน ๕ หน่วย ได้แก่

๑) หน่วยงานระดับนโยบาย ได้แก่ สภาความมั่นคงแห่งชาติ และคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนเตรียมแผนปฏิบัติการและมาตรการ ตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อ ให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ และอย่างต่อเนื่อง

๒) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ในการสร้างความเชื่อมั่นทางด้านไซเบอร์ กำหนดนโยบาย แนวปฏิบัติและมาตรฐานสำหรับหน่วยงานของรัฐและเอกชน ดูแลการทำธุรกรรมทางอิเล็กทรอนิกส์ ให้มีความมั่นคงปลอดภัย มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย (ไทยเซิร์ต) ที่ช่วยดูแลภัยคุกคามไซเบอร์ ตลอด ๒๔ ชั่วโมงและมีกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญา กรรมทางเทคโนโลยี (ปอท.) เป็นผู้รักษากฎหมาย

๓) หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ได้แก่ กระทรวงพลังงาน กระทรวงสาธารณสุข กระทรวงคมนาคม กระทรวงมหาดไทย ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ที่กำกับดูแลหน่วยงานให้มีเสถียรภาพในการทำงานและการให้บริการได้อย่างต่อเนื่อง

๔) หน่วยงานรักษาความสงบเรียบร้อยภายในประเทศ เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ ตำรวจสากล เป็นหน่วยงานที่ทำหน้าที่ป้องปรามมิให้เกิดความไม่สงบ หรือมีการกระทำ ความผิดตามกฎหมาย ตลอดจนติดตามตัวผู้กระทำความผิดมาลงโทษ โดยได้มีการเตรียมพร้อมกำลังคนอย่างต่อเนื่อง เพื่อรองรับภัยคุกคามไซเบอร์ที่ทวีความรุนแรงขึ้นเรื่อย ๆ

๕) หน่วยงานด้านความมั่นคง ซึ่งได้ขยายพื้นที่การรักษาความมั่นคงแห่งรัฐ ให้ครอบคลุมพื้นที่ไซเบอร์ (Cyberspace) ในปัจจุบัน ได้แก่ กระทรวงกลาโหม กองทัพไทย และสามเหล่าทัพ โดยได้มีการตั้งหน่วยงานเฉพาะกิจสำหรับสงครามไซเบอร์ และมีการเตรียมพร้อมด้านกำลังคน กระบวนการและ เครื่องมือต่าง ๆ ไว้ด้วยแล้ว

2.2 สภาวะแวดล้อมภายนอกด้านภัยคุกคาม

สถานการณ์การเกิดภัยคุกคามในต่างประเทศ ในประเทศไทย และในระดับหน่วยงาน ที่มีการตรวจพบจากอุปกรณ์ป้องกันและตรวจจับภัยคุกคามผ่านระบบเครือข่าย ทั้งที่มีความรุนแรงมากและรุนแรงน้อยแต่ส่งผลกระทบในวงกว้าง โดยเกิดจากหลายสาเหตุ ทั้งเหตุผลทางการเมือง ความคึกคะนองของกลุ่มแฮกเกอร์ และการความต้องการเรียกร้องของกลุ่มคนบางกลุ่ม

2.2.1 สถานการณ์ภายนอกประเทศ

จากการใช้งานระบบเครือข่ายสื่อสารและอินเทอร์เน็ตมีอิทธิพลต่อการดำเนินชีวิตประจำวันของประชาชนอย่างหลีกเลี่ยงไม่ได้หลายประเทศต่างให้ความสำคัญกับการยกระดับความพร้อมและกำหนดมาตรการเพื่อรับมือกับปัญหาภัยคุกคามไซเบอร์ภายในประเทศ ทั้งนี้ สหภาพโทรคมนาคมระหว่างประเทศของสหประชาชาติหรือ International Telecommunication Union (ITU) ได้ทำการประเมินความพร้อมด้านไซเบอร์ของประเทศต่าง ๆ ทั่วโลก โดยใช้ดัชนี Global Cybersecurity Index (GCI) จำนวน ๕ หมวด ได้แก่ กฎหมาย (Legal) เทคนิค (Technical) องค์กร (Organizational) การพัฒนาศักยภาพ (Capacity building) และความร่วมมือ (Cooperation) เป็นตัวกำหนดความสามารถด้านความปลอดภัยไซเบอร์ในระดับชาติ ภูมิภาคและระดับนานาชาติ

สหภาพโทรคมนาคมระหว่างประเทศของสหประชาชาติหรือ ITU ได้เผยแพร่ข้อมูลจำนวนผู้ใช้อินเทอร์เน็ตทั่วโลกเพิ่มขึ้นถึงร้อยละ ๗๐ จากจำนวนผู้ใช้ ๑.๙๙๑ พันล้านคน (ปี ๒๕๕๓) เป็นจำนวนผู้ใช้ ๓.๓๘๕ พันล้านคน

(ปี ๒๕๕๙)[๑] และประเทศไทยมีผู้ใช้อินเทอร์เน็ตเพิ่มมากขึ้นเกือบสองเท่าจากจำนวนผู้ใช้ ๒๗.๖๕ ล้านคน (ปี ๒๕๕๗) เป็นจำนวนผู้ใช้ ๔๓.๘๗ ล้านคน (ปี ๒๕๕๙)[๒] ในขณะเดียวกันแนวโน้มจากภัยทางไซเบอร์ทวีความรุนแรงมากขึ้น สร้างความเสียหายในวงกว้างมากขึ้นเช่นเดียวกัน เมื่อเปรียบเทียบปริมาณ ข้อมูลลูกค้าบริษัทชั้นนำทั่วโลกที่ถูกแฮกเกอร์เจาะเข้าระบบได้สำเร็จในช่วงหลายปีที่ผ่านมา ได้แก่ The Home Depot (๕๖ ล้านคน ปี ๒๐๑๖) UBER (๕๗.๖ ล้านคน ปี ๒๐๑๖) Sony PlayStation (๗๗ ล้านคน ปี๒๐๑๑) Facebook (๘๗ ล้านคน ปี ๒๐๑๘) Target (๑๑๐ ล้านคน ปี ๒๐๑๓) Equifax (๑๔๓ ล้านคน ปี ๒๐๑๗) ebay (๑๔๕ ล้านคน ปี ๒๐๑๔) Under Armour (๑๕๐ ล้านคน ปี ๒๐๑๘) และ Yahoo (๓ พันล้านคน ปี๒๐๑๓ - ๒๐๑๔)[๓]

ในโลกของไซเบอร์ยังมีภัยคุกคามที่เป็นอันตรายมากมายซึ่งเกิดจากหลายสาเหตุ ไม่ว่าจะเป็นการที่แฮกเกอร์ต้องการแสดงออกทางการเมือง ทำลายชื่อเสียง เรียกร้องความสนใจเพื่อกดดันให้เกิดการเปลี่ยนแปลงโดยไม่ต้องการเปิดเผยตัวตน หรือ เป็นอาชญากรไซเบอร์ที่ต้องการโกงผลประโยชน์ทางการเงิน การล่อลวงหรือหลอกลวงที่นำไปสู่การละเมิดผู้อื่น หรืออาจจะเป็นผู้ไม่หวังดีที่ต้องการนำข้อมูลในหน่วยงานตนเองไปเผยแพร่ หรือการทำลายระบบเพื่อผลประโยชน์ทางการเงิน หรือการแก้แค้น และภัยคุกคามไซเบอร์ ประเภทที่ร้ายแรงที่สุดอันมีรัฐอยู่เบื้องหลัง เพื่อมุ่งหวังการจารกรรม บ่อนทำลาย หรือโจมตีผลประโยชน์ทางเศรษฐกิจ การเมือง หรือทางการทหาร เป็นต้น สำหรับประเทศที่พัฒนาแล้ว ได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เพื่อการบริหารจัดการองค์กรอย่างเต็มรูปแบบ มักถูกโจมตีทางไซเบอร์ โดยการโจมตีที 'สำคัญมักเกิดขึ้นกับโครงสร้างพื้นฐานสำคัญของประเทศ โดยเฉพาะโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ ซึ่งเกิดขึ้นทั่วโลก ดังตัวอย่างเหตุการณ์การโจมตีที่สำคัญๆ ได้แก่

- มิถุนายน พ.ศ. ๒๕๕๓ โรงไฟฟ้านิวเคลียร์อิหร่านถูกโจมตีโดย Stuxnet Malware ซึ่งทำลายเครื่องจักร “Centrifuges” ที่ใช้เพิ่มประสิทธิภาพของแร่ยูเรเนียม มากกว่า ๑,๐๐๐ เครื่อง และแพร่กระจายไปยังคอมพิวเตอร์จำนวนกว่า ๒๐๐,๐๐๐ เครื่อง

- กันยายน พ.ศ. ๒๕๕๕ ปฏิบัติการ “Operation Ababil” ของสถาบันการเงินสำคัญ ในสหรัฐอเมริกา เช่น New York Stock Exchange, J.P. Morgan Chase, Bank of America และอีกหลายแห่ง ถูกโจมตี DDoS โดยกลุ่ม Qassam Cyber Fighters ทำให้การบริการเว็บไซต์หยุดชะงัก

- กันยายน พ.ศ. ๒๕๕๙ แฮคเกอร์ปล่อย Mirai Malware ใช้ช่องโหว่ในอุปกรณ์ IoT โจมตีเครื่องให้บริการชื่อโดเมน ทำให้ไม่สามารถเข้าถึงเว็บไซต์ กระทบผู้ใช้งานทั่วโลก

- กันยายน พ.ศ. ๒๕๕๙ ธนาคารกลางบังคลาเทศ ถูกมิจฉาชีพลักลอบโอนเงินจากธนาคาร จำนวน ๘๑ ล้านเหรียญสหรัฐอเมริกา ทำให้ธนาคารเกิดความเสียหาย

- พฤษภาคม พ.ศ. ๒๕๖๐ WannaCry Malware โจมตีหน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยมากกว่า ๖,๙๐๐ ราย ไม่สามารถรับบริการได้ และเกิดการแพร่กระจายไปมากกว่า ๑๕๐ ประเทศ

- กรกฎาคม พ.ศ. ๒๕๖๐ ข้อมูลส่วนบุคคลของผู้บริโภคชาวสหรัฐอเมริกา ของบริษัท Equifax รั่วไหลจำนวน ๑๔๕ ล้านคน

- พฤศจิกายน พ.ศ. ๒๕๖๐ บริษัท Uber ถูกโจรกรรมข้อมูลส่วนบุคคลของคนขับรถและ ผู้ใช้บริการ จำนวน ๕๓ ล้านคน

- มกราคม พ.ศ. ๒๕๖๑ ข้อมูลผู้ใช้บริการ Florida Medicaid ของอเมริการั่วไหล จำนวน ๓๐,๐๐๐ คน

- มกราคม พ.ศ. ๒๕๖๑ ระบบฐานข้อมูลประชาชนของอินเดียพบช่องโหว่ และทำให้ ผู้ไม่ประสงค์ดีเข้าถึงข้อมูลประชาชนของอินเดียโดยไม่ได้รับอนุญาต จำนวนกว่า 1,000 คน

ภัยคุกคามทางไซเบอร์ไม่ได้จำกัดผลกระทบต่อกลุ่มโครงสร้างพื้นฐานทางสารสนเทศกลุ่มใดกลุ่มหนึ่งเป็นการเฉพาะและในหลายเหตุการณ์กลุ่มโครงสร้างพื้นฐานทางสารสนเทศมีความสัมพันธ์เชื่อมโยงอาจจะส่งผลต่อกลุ่มโครงสร้างพื้นฐานทางสารสนเทศอื่น และทำให้เกิดผลกระทบต่อความสามารถในการให้บริการในหลาย ๆ กลุ่มได้ ทั้งนี้แนวโน้มของภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แบ่งเป็น ๓ กลุ่ม ได้แก่

๑) ภัยคุกคามทางไซเบอร์จากอุปกรณ์เชื่อมต่ออินเทอร์เน็ต (Internet Connected Devices) ที่เพิ่มมากขึ้น ด้วยอัตราการเติบโตของการใช้อุปกรณ์ Internet of Things (IoT) ที่เพิ่มมากขึ้น อย่างรวดเร็วโดยสาเหตุเกิดจากผู้ผลิตอุปกรณ์เหล่านั้นไม่ได้ออกแบบให้มีมาตรการด้านการรักษาความมั่นคง ปลอดภัย เมื่อใช้งานอุปกรณ์เหล่านั้น ทำให้อุปกรณ์ IoT ที่ผลิตและติดตั้งจำนวนมากทั่วโลกไม่มีการตรวจสอบ ความมั่นคงปลอดภัย ซึ่งอาจตกเป็นเหยื่อในการโจมตีจากผู้ไม่หวังดี และนอกจากนี้ผู้ไม่ประสงค์ดียังสามารถ ควบคุมและเข้าถึงอุปกรณ์ IoT ได้ง่ายและสะวดกขึ้น ทำให้เป็นช่องทางในการโจมตีผู้อื่นโดยใช้มัลแวร์ เช่น Mirai เป็นการโจมตีแบบ Distributed Denial of Service (DDoS) ทำให้เกิดปริมาณข้อมูลจราจรที่ใช้โจมตี มากถึง ๑ Terabits ต่อวินาทีโดยใช้อุปกรณ์ IoT Botnets จากการใช้กล้อง CCTV และกล้องบันทึกวิดีโอ ส่วนตัวมากถึง ๑๕๒,๐๐๐ เครื่อง นอกจากนี้อุปกรณ์ IoT มักจะมีจุดอ่อนที่เป็นอุปกรณ์ที่ มีราคาถูก ผลิตออกมาจำหน่วยเป็นจำนวนมาก โดยไม่ได้ออกแบบและติดตั้งมาตรการรักษาความมั่นคงปลอดภัยจาก โรงงานผลิต ทำให้ไม่สามารถที่จะปรับปรุงหรือปิดช่องโหว่ด้านความมั่นคงปลอดภัยได้ในภายหลัง

๒) เครื่องมือโจมตีทางไซเบอร์มีจำนวนหลากหลาย สามารถหาได้ง่ายและใช้งานได้ง่ายขึ้น ปัจจุบันพบว่าในตลาดมืดด้านไซเบอร์ มีเครื่องมือโจมตีมากมายให้เลือกซื้อ มีบริการจ้างแฮกเกอร์โจมตีทาง ไซเบอร์ มีการให้บริการพัฒนาเครื่องมือตามความต้องการของลูกค้า และมีการให้บริการหลังการขาย เหมือนกับการให้บริการธุรกิจทั่วไป

๓) การโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของรัฐมีแนวโน้มสูงขึ้น โดยโลก ไซเบอร์มีการเชื่อมต่อถึงกันอยู่ตลอดเวลา ทำให้ประเทศต่าง ๆ ไม่สามารถตัดขาดจากอินเทอร์เน็ตได้อย่าง สมบูรณ์ การเข้าถึงกันได้ง่ายขึ้น จึงเป็นช่องทางการโจมตีต่อรัฐเพิ่มมากขึ้นด้วยที่มาจากการโจมตีของประเทศ อื่นที่ไม่ใช่พันธมิตร เกิดขึ้นได้ง่ายขึ้นด้วยไม่ว่าจะเป็นการสร้างกระแสข่าวปลอมเพื่อหลอกลวง หรือสร้างความ เข้าใจที่ผิด ดังเช่น เหตุการณ์การสร้างกระแสทาง Social Media ในสหรัฐอเมริกา ที่ส่งผลกระทบต่อผลการ เลือกตั้งประธานาธิบดีเมื่อปี พ.ศ. ๒๕๕๙ ซึ่งในปีเดียวกันนั้นในประเทศไทยก็มีกระแสกลุ่ม Hacktivist โจมตี หน่วยงานและเว็บไซต์ภาครัฐด้วยเทคนิค DDoS และเปลี่ยนข้อมูลหน้าเว็บไซต์ของหน่วยงานรัฐ เนื่องจากผลการตัดสินคดีฆาตกรรมที่เกาะเต่าของ

ไทย รวมถึงเหตุการณ์ที่กลุ่ม Anonymous ประกาศแคมเปญ SingleGateway โจมตีหน่วยงานรัฐไทยเพื่อแสดงจุดยืนของตนเอง เป็นต้น เหตุการณ์ที่กล่าวมานี้แสดงให้เห็นว่าการพัฒนาขีดความสามารถด้านไซเบอร์เป็นสิ่งจำเป็น เพื่อให้มีศักยภาพในการตอบสนอง แจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟู ปราบปราม และตอบโต้ เมื่อถูกโจมตีโดยผู้ไม่หวังดี โดยเฉพาะอย่างยิ่งโครงสร้างพื้นฐานที่สำคัญของประเทศ ต้องมีความมั่นคงปลอดภัยทั้งทางกายภาพ และความมั่นคงปลอดภัยทางไซเบอร์ด้วย

2.3 สภาวะแวดล้อมด้านภัยคุกคามภายในประเทศ

1) ระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

สหภาพโทรคมนาคมระหว่างประเทศของสหประชาชาติหรือ ITU ได้ประเมิน Global Cybersecurity Index (GCI) หรือระดับการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย พบว่าประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียน ประเทศไทยอยู่อันดับที่ ๓ รองจากสิงคโปร์ และมาเลเซีย จากการประเมินยังพบว่าประเทศไทยมีผลประเมินด้านความพร้อมในการรับมือภัยคุกคามทางเทคนิคสูงแต่ยังขาดความพร้อมด้านการจัดตั้งองค์กร และ นโยบายด้านการรักษาความมั่นคงปลอด ภัยไซเบอร์อีกทั้งยังขาดความร่วมมือระหว่างหน่วยงานทั้งในและต่างประเทศ ในการบูรณาการทำงานเพื่อต่อต้านภัยคุกคามไซเบอร์ดังนั้น ทุกหน่วยงานจะต้องเตรียม การรับมือกับเหตุการณ์ โดยการจัดทำแผนปฏิบัติการด้านการป้องกันและการแก้ไขปัญหาด้านความมั่นคงปลอดภัย ซึ่งจะต้องมีการกำหนดนโยบาย มาตรการและกลไกในการป้องกันและแก้ไขปัญหาให้เป็นไปตามมาตรฐานในการปกป้องโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ และเป็นไป ตามแนวทางการป้องกันของประเทศไทย และที่สำคัญจะต้องมีการจัดทำแผนงานโครงการ รวมทั้งการติดตามการดำเนินงานเพื่อรายงานผล ให้หน่วยงานที่เกี่ยวข้องในการกำกับดูแลรับทราบผลการดำเนินงาน

2) การคุกคามทางไซเบอร์ของประเทศไทย

ประเทศไทยประสบกับเหตุภัยคุกคามทางไซเบอร์ในลักษณะที่คล้ายกับต่างประเทศ จากข้อมูลสถิติ ไทยเซิร์ต (ThaiCERT) ที่ดำเนินการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ทำการรวบรวมปริมาณและประเภทของเหตุภัยคุกคามที่ได้รับแจ้งในช่วงครึ่งแรกของปี ๒๕๖๑ พบว่าภัยคุกคามไซเบอร์ที่เกิดขึ้น จำนวน ๑,๖๙๑ ครั้ง โดยประเภทของภัยคุกคามที่เกิดขึ้นปริมาณสูง ได้แก่ Intrusion Attempts คิดเป็นร้อยละ ๒๙ การ Fraud คิดเป็นร้อยละ ๒๖ การ Intrusions คิดเป็นร้อยละ ๑๘ Malicious code คิดเป็นร้อยละ ๘ Information security ร้อยละ ๒ โดยที่เหลือเป็นภัยคุกคามด้านอื่นๆ ทั้งนี้ปริมาณของ Intrusion Attempts และ Fraud มีปริมาณสูงเกินกว่าร้อยละ ๕๐ ของภัยคุกคามประเภท อื่นๆ เมื่อเทียบสถิติการเกิดภัยคุกคามไซเบอร์ในปี พ.ศ. ๒๕๖๐ และ พ.ศ. ๒๕๖๑ อย่างไรก็ตามภัยคุกคาม ทางไซเบอร์ยังเกิดขึ้นอยู่ตลอดเวลา โดยจากรายงานสถิติของ ECSIRT.net พบว่า ประเทศไทยยังคงติดอยู่ ในลำดับต้นๆ ของประเทศที่เกิดภัยคุกคามไซเบอร์

มีรายงานเหตุการณ์เกี่ยวกับพฤติกรรมการโจมตีทางไซเบอร์เกิดขึ้นกับหน่วยงานของรัฐและเอกชนอย่างต่อเนื่อง โดยเมื่อปี พ.ศ. ๒๕๕๕ มีการใช้วิธีการ Phishing (การหลอกเอา username และ password) บัญชีเงินฝากหรือเจาะระบบเพื่อแสดงความสามารถระหว่างกลุ ่มแฮกเกอร์ในช ่วงปี พ.ศ. ๒๕๕๖ เริ่มมีการโจมตีโดยวิธีการ Distributed Denial of Service หรือ DDoS เป็นการโจมตี จากหลายๆ ที่พร้อมๆ กัน ซึ่งเกิดขึ้นกับการโจมตีธุรกิจการเงินและการลงทุนมากขึ้น โดยมีการส่งจดหมาย อิเล็กทรอนิกส์ขู่โจมตีล่วงหน้า เพื่อเรียกเงินแลกกับการไม่ถูกโจมตี โดยช่วงที่เกิดการโจมตีแบบ DDoS เป็นช่วงระยะเวลาเดียวกันกับการขู่โจมตีสถาบันการเงินทั่วโลก และในปี พ.ศ. ๒๕๕๘ พบว่ามีการโจมตี ด้วยวิธีการ DDoS มากขึ้น นอกจากนี้ ยังพบการใช้มัลแวร์ ในรูปแบบการกระจายมัลแวร์ เพื่อเข้ารหัสลับข้อมูล ในเครื่องของเหยื่อ หรือการลอบติดตั้งมัลแวร์ ในตู้เอทีเอ็มเพื่อควบคุมการจ่ายเงิน และในปี พ.ศ. ๒๕๕๙ เกิดเหตุการณ์สำคัญที่ทำให้หน่วยงานรัฐและเอกชนของไทยตระหนักถึงผลกระทบของภัยคุกคามไซเบอร์มากขึ้น คือการขู่โจมตีธนาคารใหญ่ด้วยวิธี การ DDoS รวมทั้งการปล้นเงินจากตู้เอทีเอ็ม และการโจมตีบริการสำคัญของรัฐ ทำให้ไม่สามารถให้บริการได้เป็นระยะเวลาหลายชั่วโมง

ทั้งนี้ สาเหตุที่จูงใจให้มีการโจมตีภัยทางไซเบอร์ของประเทศไทยไม่ใช่เฉพาะผลประโยชน์ทางการเงินเท่านั้น แต่ยังใช้เป็นเครื่องมือในการแสดงออกของภาคประชาชน เช่น เหตุการณ์กลุ่ม F5 Army ที่โจมตีเว็บไซต์ของหน่วยงานภาครัฐ เนื่องจากมีความหวาดระแวงว่ารัฐบาลจะดำเนินการในเรื่อง Single gateway เพื่อดักรับข้อมูลของประชาชนบนอินเทอร์เน็ต การกระทำดังกล่าวเป็นการแสดงออกเชิงสัญลักษณ์ซึ่งส่งผลกระทบต่อความเชื่อ มั่นและความน่าเชื่อถือในการขับเคลื่อนประเทศไทยในยุคดิจิทัล

3) <u>การโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศ</u>

การกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นแนวทางที่จำเป็นเพื่อเป็นแนวทางในการบริหารจัดการ ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ โดยในแต่ละประเทศมีการกำหนดโครงสร้างพื้นฐานสำคัญแตกต่างกัน เช่น ในสหรัฐอเมริกา กำหนดกลุ่มโครงสร้างพื้นฐานสำคัญ จำนวน ๑๖ กลุ่ม ในขณะที่ประเทศอังกฤษกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญไว้ จำนวน ๙ กลุ่ม

สำหรับประเทศไทยตามพระราชกฤษฎีกาว่าด้วยวิธีการปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ได้กล่าวถึง “โครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure : CI)” ไว้ว่า บรรดาหน่วยงานหรือองค์กร หรือ ส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือ ส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องต่อความมั่นคงหรือต่อสาธารณชน หรือความสงบเรียบร้อย และร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ผ่านความเห็นชอบสภานิติบัญญัติแห่งชาติเมื่อวันที่ 28 ก.พ. 2562 ได้นิยามความหมายของ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่ เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือ โครงสร้างพื้นฐานอันเป็นประโยชน์ต่อสาธารณะ โดยในเบื้องต้นได้กำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไว้ 7 ด้านประกอบด้วย ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐ ด้านการเงิน การ

ธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและ โลจิสติกส์ ด้านพลังงานและสาธารณูปโภค และด้านสาธารณสุข เพื่อให้หน่วยงานที่เกี่ยวข้องและมีความชำนาญ เข้ามาทำหน้าที่กำหนด แนวทางการบริหารจัดการแก้ไขปัญหาด้านภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และ ได้กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือ กมช. มีอำนาจในการกำหนดโครงสร้าง พื้นฐานสำคัญทางสารสนเทศอื่นที่สำคัญเพิ่มเติมได้ หากเห็นว่ามีความจำเป็นและเหมาะสมการโจมตีต่อโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ (CII) ของประเทศไทย ได้แก่ระบบให้บริการทางการเงินการธนาคาร สาธารณูปโภค การขนส่งและ โลจิสติกส์ บริการสุขภาพ พลังงาน การสื่อสารโทรคมนาคม เป็นภัยคุกคามทางไซเบอร์ที่ก่อให้เกิดผลกระทบที่รุนแรงในวงกว้าง และสามารถสร้างความเสียหายที่ร้ายแรงต่อเสถียรภาพทางเศรษฐกิจ สังคมและความมั่นคงของประเทศ ซึ่งอาจทำให้ประเทศสูญเสียความได้เปรียบในการแข่งขันทางการค้าในตลาดโลก ทำให้ประเทศขาดความเชื่อมั่นในสายตาประชาคมโลกหรือประชาชนทั่วไป การปฏิบัติงานของประเทศต้องหยุดชะงัก รวมทั้งผลกระทบทางกฎหมายทั้งนี้ประเทศไทยเกิดเหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ หรือ (Critical Information: CI) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ดังนี้

- มิถุนายน พ.ศ. ๒๕๕๕ ผู้ให้บริการชื่อโดเมนไทย (.th) ถูกเจาะระบบและแก้ไข ข้อมูลที่อยู่เว็บไซต์ขององค์กรใหญ่หลายแห่ง
- กุมภาพันธ์ พ.ศ. ๒๕๕๖ เว็บไซต์ของตลาดหลักทรัพย์ในอเมริกา เอเชีย รวมถึงไทย ถูกโจมตีด้วย DDoS โดยกลุ่ม Anonymous ทำให้บริการขัดข้องหลายชั่วโมง ซึ่งส่งผลกระทบด้านเศรษฐกิจ
- ตุลาคม พ.ศ. ๒๕๕๘ ธนาคารพาณิชย์๕ ธนาคาร ได้รับจดหมายอิเล็กทรอนิกส์ ข่มขู่เรียกเงินเป็น Bitcoins เพื่อแลกกับการไม่ถูกโจมตี DDoS จากกลุ่ม Armada Collective
- สิงหาคม พ.ศ. ๒๕๕๙ ตู้ ATM ของธนาคารออมสิน จำนวน ๒๑ ตู้ถูกโจมตีโดย มัลแวร์และลอบขโมยเงิน ๑๒ ล้านบาท ซึ่งเป็นมัลแวร์ที่คล้ายกับที่ใช้โจมตี ATM ในไต้หวันในปีเดียวกัน
- ธันวาคม พ.ศ. ๒๕๕๙ ปรากฏการณ์ทางสังคมที่แสดงออกผ่านไซเบอร์ เมื่อกลุ่ม “พลเมืองต่อต้าน Single Gateway #opsinglegateway” รณรงค์ให้มีการโจมตี DDoS กับเว็บไซต์ของหน่วยงานของรัฐ ทำให้หลายระบบสำคัญของรัฐขัดข้อง และ พบการเจาะฐานข้อมูลเพื่อโจรกรรมข้อมูลมาเผยแพร่ รวมถึงใช้ปฏิบัติ การข่าวสาร IO ในการลดความน่าเชื่อถือของรัฐบาล

2.4 สภาวะแวดล้อมภายในของหน่วยงานด้านการขนส่ง

จากที่ประชุมคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเห็นชอบการแบ่งกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) จำนวน 7 หมวด ได้แก่ หมวด 1: ด้านความมั่นคงของรัฐ, หมวด 2: ด้านบริการภาครัฐที่สำคัญ, หมวด 3: ด้านการเงินการธนาคาร, หมวด 4: ด้านเทคโนโลยีสารสนเทศและโทร คมนาคม หมวด 5: ด้านการขนส่งและ โลจิสติกส์ หมวด 6: ด้านพลังงานและสาธารณูปโภค, หมวด 7: ด้านสาธารณสุขและยังมีการกำหนดหน่วยงานรับผิดชอบพร้อมทั้งให้หน่วยงานรับผิดชอบดำเนินการตามประกาศคณะกรรมการธุรกรรมทาง

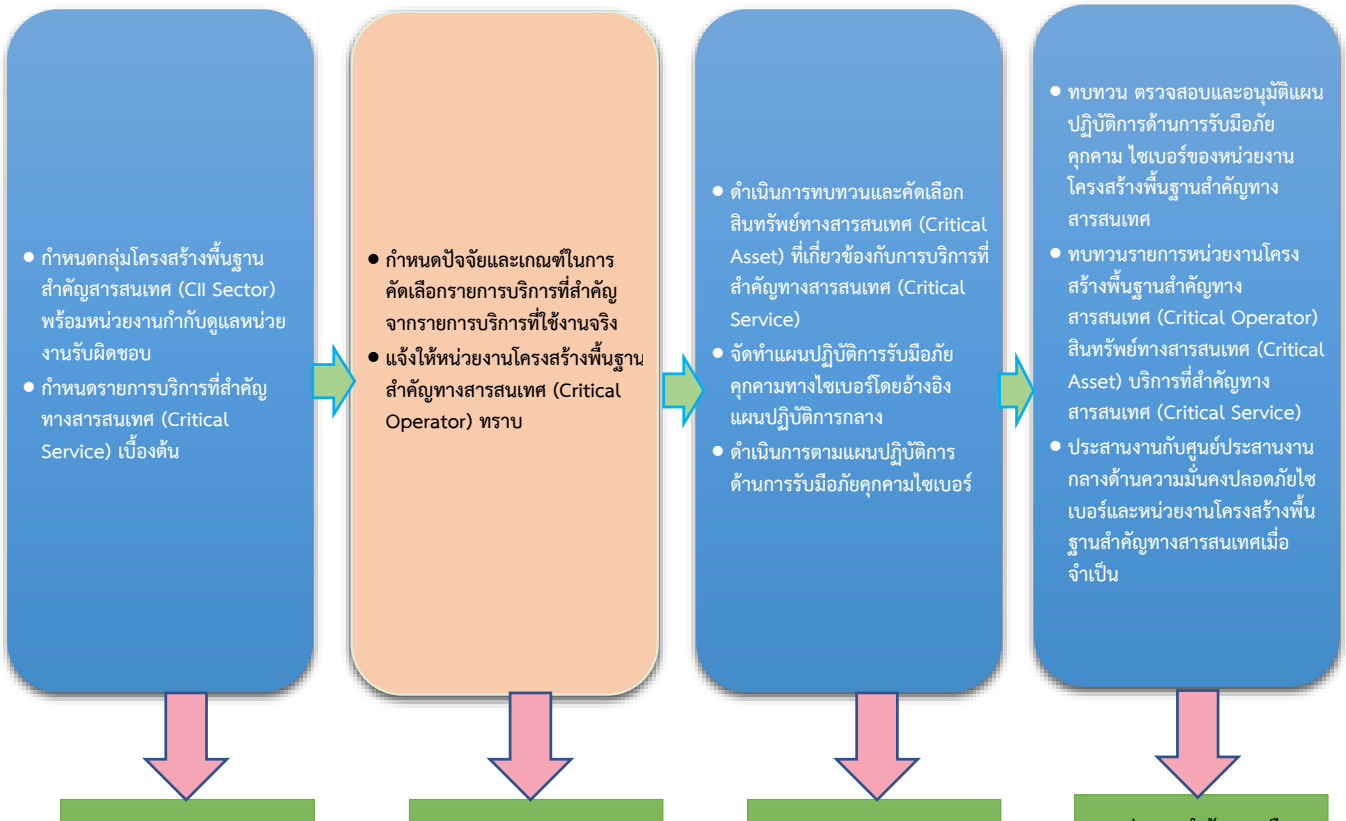
อิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ทั้งนี้ได้มีการแบ่งหน้าที่เพื่อกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศประกอบด้วยหน่วยงานประสานส่วนกลางด้านความมั่นคงปลอดภัย หน่วยงานกำกับดูและหรือประสานงานหลักและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังนี้

หมวด ๕
ด้านการขนส่งและโลจิสติกส์

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการขนส่งทางบก	(๑) บริการที่เกี่ยวข้องกับการควบคุมการจราจรในพื้นที่กรุงเทพมหานคร	สำนักงานตำรวจแห่งชาติ
ข้อ ๒ ที่มีการให้บริการขนส่งทางราง	(๑) บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง (๒) บริการที่เกี่ยวข้องกับการส่งสัญญาณ การสื่อสาร และการส่งข้อมูล (๓) บริการขายตั๋วและสำรองที่นั่ง (๔) บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแลและเก็บข้อมูล	กรมการขนส่งทางราง

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๓ ที่มีการให้บริการขนส่งทางน้ำ	(๑) บริการที่เกี่ยวข้องกับการบริหารจัดการท่าเรือ (๒) บริการด้านเรือ สินค้า คลังสินค้า เครื่องมือทุ่นแรง และใบแจ้งหนี้ค่าภาระต่าง ๆ (๓) บริการที่เกี่ยวข้องกับการจัดการท่าเทียบเรือตู้สินค้า (๔) บริการที่เกี่ยวข้องกับการควบคุมและลากจูง	สำนักงานปลัดกระทรวงคมนาคม
ข้อ ๔ ที่มีการให้บริการขนส่งทางอากาศ	(๑) บริการจราจรทางอากาศ (๒) บริการข่าวสารการบิน (๓) บริการที่เกี่ยวข้องกับการปฏิบัติการท่าอากาศยาน (๔) บริการเครื่องอำนวยความสะดวกการเดินอากาศ (๕) บริการที่เกี่ยวข้องกับบริการสิ่งอำนวยความสะดวกและรักษาความปลอดภัยกิจการการบิน (๖) บริการที่เกี่ยวข้องกับอุตุนิยมวิทยาการบิน (๗) บริการสายการบิน (๘) บริการที่เกี่ยวข้องกับการป้องกันคลื่นวิทยุ (สนามบิน) (๙) บริการที่เกี่ยวข้องกับการขนถ่ายสินค้า (๑๐) บริการครัวการบินและสิ่งอำนวยความสะดวกสำหรับผู้โดยสารบนอากาศยาน (๑๑) บริการลานจอด ตรวจสอบและบำรุงรักษาอากาศยาน	สำนักงานการบินพลเรือนแห่งประเทศไทย

ตารางที่ 2-1 เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔



แผนภาพที่ 1: โครงสร้างการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านการขนส่ง

หน่วยงานด้านการขนส่งเป็นหน่วยงานที่ได้รับมอบหมายให้บริการโดยใช้โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการขนส่งและ โลจิสติกส์ ซึ่งเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ถูกระบุไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 โดยการดำเนินการที่ผ่านมา หน่วยงานด้านการขนส่งได้เข้าร่วมประชุมกับหน่วยงานความมั่นคงและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อรับทราบแนวทางการดำเนินงาน พร้อมรายงานความคืบหน้าการดำเนินงานตามยุทธศาสตร์ชาติด้านความมั่นคง โดยในเบื้องต้นได้มีการจัดทำแผน แผนปฏิบัติการด้านไซเบอร์ นอกจากนี้ยังมีการประชุมหารือร่วมกับหน่วยงานในสังกัด พร้อมเชิญหน่วยงานในสังกัดเพื่อซักซ้อมแนวทางการดำเนินงานและจัดทำรายละเอียดเกี่ยวกับบริการที่สำคัญ (Critical Service) รายการมาตรฐาน กฎระเบียบต่าง ๆ ที่เกี่ยวข้องเพื่อเป็นแนวทางในการกำหนดแผนงานโครงการที่จะต้องดำเนินการเร่ง ด่วน ในการป้องกันภัยคุกคามทางไซเบอร์

สำหรับการถูกคุมคามด้านไซเบอร์ของหน่วยงานด้านการขนส่งที่ผ่านมานั้นมีการตรวจพบภัยคุกคามโดยการใช้วิธีการ Phishing ซึ่งทำการปลอม IP Address เพื่อทำการแก้ไขหน้าเว็บไซต์ของหน่วยงาน การบุกรุกโดยการใช้ Malware Phishing ผ่านจดหมายอิเล็กทรอนิกส์ เพื่อแพร่กระจายไวรัสไปยังเครื่องคอมพิวเตอร์อื่นเมื่อเปิดอ่านจดหมายอิเล็กทรอนิสก์การโดยใช้ Removable Drive ที่ขาดการระมัดระวังทำให้ Malware ฝังตัวที่เครื่องคอมพิวเตอร์ลูกข่ายจนเป็น Botnets เป็นต้น

นอกจากนี้ มีบางหน่วยงานในสังกัดหน่วยงานด้านการขนส่ง มีหน่วยงานย่อยที่กระจายตามภูมิภาค แต่บุคลากรด้านไอทีของหน่วยงานจะปฏิบัติงานในส่วนกลาง ทำให้เกิดปัญหาในการถูกคุกตามทางไซเบอร์ ได้ง่าย ประกอบกับบุคลากรด้านไอทีในส่วนกลางมีการปฏิบัติงานด้านอื่น จึงทำให้ไม่สามารถตรวจติดตามการถูกโจมตีได้ตลอดเวลา จึงต้องมีการจัดทำโครงการเกี่ยวกับการจัดหาอุปกรณ์เพื่อป้องกันตรวจจับการคุกคามทางไซเบอร์และพัฒนาบุคลากรให้มีความ เชี่ยวชาญด้านความมั่นคงปลอดภัยเพิ่มขึ้น

2.5 การวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ (Strategic Analysis)

2.5.1 การวิเคราะห์สภาวะแวดล้อม (SWOT Analysis) ด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการขนส่ง

การประเมินสภาวะแวดล้อมภายในและภายนอกของหน่วยงานด้านการขนส่งเป็นการวิเคราะห์สภาวะแวดล้อมเพื่อค้นหาปัจจัยที่มีอิทธิพลต่อการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทาง

สารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง ได้แก่ จุดแข็ง (Strengths) จุดอ่อน (Weaknesses) โอกาส (Opportunities) และภัยคุกคาม (Threats) สู่การบรรลุเป้าหมายที่กำหนดไว้ตามเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) ยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2565 (National Cyber security Strategy 2023) แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งแผนอื่น ๆ ที่เกี่ยวข้อง ซึ่งการศึกษาครั้งนี้เป็นการศึกษาเชิงบรรยาย (Descriptive study) โดยผู้ศึกษาได้ใช้วิธีสัมภาษณ์ตอบแบบสอบถาม โดยนำข้อคิดเห็นของผู้ตอบแบบสอบถามมาประกอบการวิเคราะห์ สภาวะแวดล้อมที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่งที่ได้จากข้อมูลทุติยภูมิด้วย

2.5.1.1 การวิเคราะห์สภาวะแวดล้อมภายในองค์กร

การวิเคราะห์สภาวะแวดล้อมภายในของหน่วยงานด้านการขนส่งใช้กรอบแนวคิด McKinsey7’S Framework ใน 7 มิติ ได้แก่ โครงสร้างองค์กร (Structure) กลยุทธ์ขององค์กร (Strategy) ระบบในการดำเนินงานขององค์กร (System) ลักษณะแบบแผนหรือพฤติกรรมของผู้บริหารองค์กร (Style) บุคลากรในองค์กร (Staff) ความรู้ความสามารถของบุคลากร (Skills) และค่านิยมองค์กร (Shared values) ซึ่งตัวแปรหรือปัจจัยดังกล่าวมีผลต่อความสำเร็จขององค์กร ดังตารางที่ 2-1

ตารางที่ 2-2 การวิเคราะห์สภาวะแวดล้อมภายในด้วย McKinsey 7’S Framework

ประเด็นการวิเคราะห์	ผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์	
	ประเด็นที่เป็นจุดแข็ง (S)	**ประเด็นที่เป็นจุดอ่อน (W)**
1. Structure โครงสร้างองค์การ	**S1 :** หน่วยงานด้านการขนส่งมีโครงสร้างชัดเจนสำหรับภารกิจหลักและมีกฎหมายรองรับ **S2 :** หน่วยงานด้านการขนส่งมีการมอบอำนาจในการปฏิบัติงานหรือผู้รับผิดชอบในการให้บริการหลักที่สำคัญ	**W1:** ขาดความชัดเจนด้านการกำหนดหน่วยงานควบคุมกำกับสำหรับบางบริการสำคัญในด้านการขนส่ง (critical service and regulator in Logistic) **W2:** โครงสร้างองค์กรปัจจุบันยังไม่รองรับหรือมีการจัดตั้งตามโครงสร้างหน่วยงานการรักษาความปลอดภัยไซเบอร์ภายในหน่วยงานและระหว่างหน่วยงาน **W3:** การกำหนดโครงสร้างหน่วยงานกำกับและหน่วยงาน CII ภายใต้การกำกับยังมีความทับซ้อน

2. Strategy กลยุทธ์ขององค์การ	**S3**: หน่วยงานด้านการขนส่งสามารถกำหนดแผนงานและแนวทางการดำเนินงานตอบสนองนโยบายภาครัฐได้อย่างมีประสิทธิภาพ **S4**: มีเครือข่ายความร่วมมือที่หลากหลาย **S5**: มีการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ในแต่ละหน่วยงานด้านการขนส่ง	**W4**: ขาดความรู้ความเข้าใจในกลยุทธ์ด้านการรักษาความปลอดภัยไซเบอร์ของหน่วยงาน **W5**: การถ่ายทอดแผนสู่การปฏิบัติไม่ชัดเจน **W6**: ขาดการติดตามผลสัมฤทธิ์การดำเนินงาน **W7**: ขาดข้อมูลในการวางแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานและกำหนดทิศทางขององค์กรด้านไซเบอร์
3. System ระบบการปฏิบัติงาน	**S6:** มีความชัดเจนในกำหนดนโยบาย ระบบงานและขั้นตอนการบริหารจัดการด้านการรักษาความปลอด ภัยไซเบอร์ **S7:** มีระบบสารสนเทศที่สนับสนุนการทำงานการให้บริการที่สำคัญให้มีประสิทธิภาพ **S8**: มีกระบวนการจัดการด้านการให้บริการในภาวะฉุกเฉินและอย่างต่อเนื่อง ในกรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ **S9**: มีระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศที่ได้มาตรฐานระดับสากล	W8: ขาดแผนการพัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน W9: ขาดการกำหนดนโยบายด้านการพัฒนาเครื่องมือหรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII) W10: ระบบการประเมินผลยังไม่เป็นรูปธรรมที่ชัดเจน W11: ขาดการซ้อมแผนการบริหารความต่อเนื่องในการให้บริการในภาวะฉุกเฉินและในกรณีเกิดเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ W12: ขาดการสื่อสารหรือแจ้งเตือนด้านสถานการณ์ความปลอดภัยไซเบอร์ที่มีความรุนแรงมากขึ้น W13: ขาดการประสานงานร่วมมือในการปฏิบัติงานร่วมกันระหว่างหน่วยงานขนส่งด้านการรักษาความปลอดภัยไซเบอร์
4. Style ลักษณะแบบแผนหรือพฤติกรรมของผู้บริหารองค์กร	S10 : มีความพร้อมในการตอบสนองต่อนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ S11: องค์กรยอมรับการเปลี่ยนแปลงรับฟังความคิดเห็น และทันต่อเหตุการณ์	W14: การบริหารงานในองค์กร ขาดความยืดหยุ่นในการปรับปรุงโครงสร้างการบริหารงานด้านการรักษาความปลอดภัยไซเบอร์ W15: ขอบเขตอำนาจหน้าที่ความรับผิดชอบด้านการจัดการความมั่นคงปลอดภัยไซเบอร์ไม่ชัดเจน
5. Staff บุคลากร	S12: มีความรู้ ความสามารถในส่วนงานที่รับผิดชอบ S13: มีแผนงานในการฝึกอบรมการรักษาความปลอด ภัยไซเบอร์ S14: มีความชำนาญงานเฉพาะงานบริการหลักขององค์กร	W16 : บุคลากรขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ W17 : ขาดบุคลากรที่มีความรู้และประสบการณ์ในด้านการจัดการความมั่นคงปลอดภัยไซเบอร์
6. Skills ทักษะ ความรู้ความสามารถ	S15 : สามารถใช้เทคโนโลยีสารสนเทศในการให้บริการหลักด้านการขนส่งที่มีคุณภาพและประสิทธิภาพได้ดี S16: มีการพัฒนาเทคโนโลยีสารสนเทศที่ใช้ในการให้บริการหลักที่สำคัญ (CII)	W18: ขาดงบประมาณในการส่งเสริม ฝึกอบรมสร้างความชำนาญด้านการป้องกันภัยทางไซเบอร์สำหรับระบบ (CII) W19: ขาดทักษะและความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์
7. Shared Value	S17 : หน่วยงานด้านการขนส่งมีวิสัยทัศน์และค่านิยมที่ชัดเจนในการดำเนินงานอย่างมีประสิทธิภาพ S18 มีการกำหนดค่านิยมองค์กร	W20: ขาดการสร้างความรับรู้ค่านิยมองค์กร W21: ขาดการรับรู้ทิศทางด้านการจัดการและการรักษาความปลอดภัยไซเบอร์ในองค์กร

ค่านิยมร่วม	S19 มีความเชื่อมั่นในการพัฒนาองค์กร	W22: ขาดการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง

2.5.1.2 การวิเคราะห์สภาวะแวดล้อมภายนอกองค์กร

การวิเคราะห์สภาวะแวดล้อมภายนอกที่มีผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง ในการจัดทำเอกสารวิชาการนี้ ผู้ศึกษาดำเนินการผ่านการกวาดสัญญาณแนวโน้ม (Horizontal Scanning) โดยการรวบรวมข้อมูลทุติยภูมิ ผู้ศึกษาได้ใช้วิธีการ สัมภาษณ์ผู้บริหารของหน่วยงาน ผู้ดูแลระบบสารสนเทศ และผู้ใช้งานระบบสารสนเทศของหน่วยงานที่ให้บริการด้านการขนส่ง จำนวน 9 ท่าน และรวบรวมวิเคราะห์ข้อมูลจากเอกสารรายงานต่าง ๆ ของกระทรวงคมนาคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยใช้เทคนิคการวิเคราะห์ตามกรอบ PESTEL (เชิงการเมือง - เศรษฐกิจ - สังคม - เทคโนโลยี - สิ่งแวดล้อม - กฎหมาย) เมื่อนำประเด็นจากการวิเคราะห์ตามหลัก PESTEL มาวิเคราะห์โอกาส (Opportunities) และ ภัยคุกคาม (Threats) ที่มีผลกระทบต่อการบริหารจัดการความมั่นคงปลอด ภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง โดยการวิเคราะห์ตามหลัก **PESTEL Analysis** ประกอบด้วย 6 ปัจจัยดังรายละเอียดต่อไปนี้

1. **P: Politic Factor** เป็นการเป็นการพิจารณาถึงความเคลื่อนไหวต่าง ๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่งทั้งการบริหารงาน นโยบาย งบประมาณ ตลอดจนการควบคุมสถานการณ์ทางการเมือง โดยปัจจัยด้านการเมืองสามารถเป็นได้ตั้งแต่นโยบายทางการคลัง นโยบายการค้าระหว่างประเทศ นโยบายด้านแรงงาน การดูแลส่งเสริมด้านสาธารณสุข การศึกษา เทคโนโลยี สิ่งแวดล้อม และอื่น ๆ ที่อาจส่งผลกระทบต่อการดำเนินงานของหน่วยงานด้านการขนส่งได้
2. **E: Economic Factor** คือปัจจัยที่ส่งผลกระทบโดยตรงต่อประสิทธิภาพของเศรษฐกิจประชาชาติ ซึ่งสามารถส่งผลกระทบโดยตรงการลงทุน หรือการจัดซื้อจัดจ้างขององค์กร เช่น อัตราแลกเปลี่ยนระหว่างประเทศ อัตราเงินเฟ้อ ราคาต้นทุน-วัตถุดิบ เป็นต้น รวมไปถึงปัจจัยที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่งในทางอ้อม เช่น อัตราการจ้างงาน-อัตราการว่างงาน ภาวะการเติบโตทางเศรษฐกิจ รายได้ประชาชาติแนวโน้มการลงทุน ภาวะการเติบโตของอุตสาหกรรม เงินดิจิทัลความอิ่มตัวของตลาด รายได้ของเกษตรกรในแต่ละพื้นที่ ค่าครองชีพ ค่าใช้จ่ายบุคคลและครัวเรือนเป็นต้น
3. **S: Sociological Factor** คือปัจจัยใด ๆ ก็ตามที่ส่งผลกระทบต่อค่านิยม บรรทัดฐาน รวมไปถึงสภาพแวด ล้อมในสังคมที่นำมาวิเคราะห์ เช่น การเปลี่ยนแปลงโครงสร้างประชากร (Demographic change) การเติบโตของประชากร (Population Growth) การย้ายถิ่นฐาน (Geographical Migration of the Population) ความเหลื่อมล้ำทางเศรษฐกิจในแต่ละภูมิภาค (Regional Disparities) แนวโน้มของกระแสในสังคม (Trend) ทัศนคติ (Attitude) ความเชื่อ (Believe) ขนบธรรมเนียม วัฒนธรรม ประเพณี

(Cultural) คุณค่าที่เป็นที่ยอมรับในสังคม ความยุติธรรม ความสมานฉันท์การแบ่งแยกในสังคม ความขัดแย้งต่างๆ

4. T: Technological Factor เป็นปัจจัยที่ส่งผลกระทบโดยตรงต่อความสามารถในการแข่งขันขององค์กร โดยพิจารณาถึงประสิทธิภาพ แนวโน้มการเปลี่ยนแปลง และ การพัฒนาทางเทคโนโลยีที่มีผลต่อองค์กร ตั้งแต่เรื่องสิทธิบัตร อายุของเทคโนโลยี อัตราการเกิดนวัตกรรม นวัตกรรมของผลิตภัณฑ์ นวัตกรรมด้านกระบวนการ เวลาในการพัฒนา ค่าใช้จ่ายในงานวิจัยและพัฒนา ภัยคุกคามจากดิจิทัล ไวรัสคอมพิวเตอร์ การบูรณาการเทคโนโลยี อุปกรณ์จักรกลอัตโนมัติ ไปจนถึงปัญญาประดิษฐ์
5. E: Environmental Factor คือการพิจารณาถึงผลกระทบที่จะเกิดขึ้นต่อธรรมชาติทั้งหมด ตั้งแต่การเปลี่ยนแปลงของสภาพอากาศ การเพิ่มขึ้นของมลพิษ น้ำเน่าเสีย การขาดแคลนทรัพยากรธรรมชาติที่ส่งผลให้ราคาวัตถุดิบเพิ่มขึ้น ภัยธรรมชาติต่าง ๆ อย่างภัยแล้ง น้ำท่วม รวมไปถึงโรคระบาดต่าง ๆ ดังนั้นองค์กรจึงต้องคำนึงถึงการมส่วนร่วมในการรับผิดชอบต่อสังคม (Social Responsibility) การบริหารทรัพยากร การผลิตและการขนส่ง (Supply Chain Management) การลดคาร์บอนฟุตพริ้นท์ (Carbon Footprint) เพื่อมุ่งมั่นสร้างความยั่งยืนทั้งในเชิงธุรกิจและสิ่งแวดล้อม
6. L: Legal Factor เป็นการพิจารณาถึงระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น สิทธิบัตร (Patent Rights) การรับผิดชอบต่อสินค้า (Product Liability) กฎหมายคุ้มครองสิ่งแวดล้อม (Environment Protection) การคุ้มครองผู้บริโภค (Consumer Protection) รวมไปถึงการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) และกฎหมายการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ตารางที่ 2-3 สรุปผลการวิเคราะห์ PESTEL เพื่อหาโอกาสและภัยคุกคาม

ประเด็นการวิเคราะห์	ผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์	
	ประเด็นที่เป็นโอกาส (O)	ประเด็นที่ภัยคุกคาม (T)
การเมือง (Political)	O1: ภาครัฐมีความชัดเจนเชิงกฎหมาย นโยบายในการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ O2: มีการจัดตั้งหน่วยงานของรัฐสำหรับดูแลเฉพาะด้านการจัดการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ O3: มีนโยบายและแผนยุทธศาสตร์ระดับชาติ และเป้าหมายการพัฒนาประเทศในแผนฉบับต่าง ๆ ให้ความสำคัญกับการพัฒนาเทคโนโลยีดิจิทัล โดยมีเป้า หมายให้หน่วยงานของรัฐเป็นองค์กรดิจิทัล สนับสนุน การพัฒนาและการนำเทคโนโลยีดิจิทัลเข้ามาใช้ในการให้บริการ	T1: กฎหมายและกฎระเบียบที่กำหนดด้านการรักษาความปลอดภัยไซเบอร์อาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรมด้านการขนส่ง T2: การของบประมาณในการพัฒนาเทคโนโลยีดิจิทัลต้องผ่านหลายขั้นตอน หรือผันแปรไปตามนโยบายรัฐบาลแต่ละสมัยที่เปลี่ยนไป T3: มีการใช้เทคโนโลยีสารสนเทศหรือการโจมตีทางไซเบอร์เป็นเครื่องมือทางการเมือง
เศรษฐกิจ (Economic)	O4: การขยายของเมืองและระบบการขนส่ง เป็นปัจจัยส่งเสริมให้มีการพัฒนาระบบสารสนเทศในการให้บริการ เป็นโอกาสในการขยายการร่วมลงทุนระหว่างภาครัฐและเอกชน	T4 : ขาดการคำนึงถึงงบประมาณในการปรับ ปรุงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำคัญของหน่วยงาน และการป้อง กันภัยทางไซเบอร์

สังคม (Social)	**O5:** พฤติกรรมของผู้ใช้งานระบบสารสนเทศที่มีการเปลี่ยนแปลงในยุค Covid -19 เป็นตัวเร่งให้องค์กรต้องพัฒนาระบบ Digital ทั้งด้านผลิตภัณฑ์ และรูปแบบการทำงาน การให้บริการใหม่ ๆ ให้รวดเร็วและตอบโจทย์ผู้ใช้งานระบบมากขึ้น **O6**: สังคมปัจจุบันเป็นสังคมที่ใช้สื่อด้านเทคโนโลยีดิจิทัล (Social Media) การรับรู้ การเข้าถึงข้อมูลสามารถทำได้ง่ายและรวดเร็ว **O7:** มีเครือข่ายพันธมิตรในหน่วยงานของรัฐ เอกชนรัฐวิสาหกิจ และหน่วยงานในต่างประเทศ ในการส่ง เสริมระบบสารสนเทศที่ให้บริการหลักที่สำคัญ (CII) **O8:** มีความร่วมมือ ผู้เชี่ยวชาญจากภายนอกให้คำ ปรึกษาด้านการพัฒนาระบบสารสนเทศในการให้ บริการและดำเนินงานของหน่วยงานด้านการขนส่ง	**T5:** การแพร่ระบาดของ Covid-19 ส่งผลกระทบต่อการจัดสรรงบประมาณในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการขนส่ง **T6:** การแพร่กระจายของไวรัสคอมพิวเตอร์ หรือการโจมตีทางไซเบอร์ เพิ่มมากขึ้น ในการใช้สื่อสังคมออนไลน์และการทำงานแบบ WFH **T7:** บุคลากรของหน่วยงานใช้สื่อด้านเทคโนโลยีดิจิทัลผิดวัตถุประสงค์ทำให้เกิดความเสียหายต่อระบบงานสำคัญ
เทคโนโลยี (Technology)	O9: การพัฒนาระบบสารสนเทศในการให้บริการที่สำคัญของหน่วยงานด้านการขนส่งที่เอื้อต่อการนำ มาใช้ให้บริการประชาชน และ ใช้ในการปฏิบัติงานในองค์กรให้มีความทันสมัย รวดเร็ว มีประสิทธิภาพ O10: มีการพัฒนาเครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์เพิ่มมากขึ้น	T8: ขาดทักษะความรู้ความชำนาญในการใช้งานระบบสารสนเทศของบุคลากรของหน่วยงาน T9: ขาดทักษะความรู้ความชำนาญในการใช้เครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์
สิ่งแวดล้อม (Environmental)	O11: การทำงานในรูปแบบ WFH มากขึ้นจากสภาพ แวดล้อมที่มีการแพร่ระบาดของโควิด-19 ทำให้มีการพัฒนาเทคโนโลยีเพื่อสนับสนุนการทำงานในรูปแบบ WFH ที่ทันสมัยของหน่วยงาน	**T6:** การแพร่กระจายของไวรัสคอมพิวเตอร์ หรือการโจมตีทางไซเบอร์ เพิ่มมากขึ้น ในการใช้สื่อสังคมออนไลน์ และการทำงานแบบ WFH
กฎหมาย (legal)	O12: มีการกำหนดกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล O13: มีการกำหนดกฎหมายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562	**T1:** กฎหมายและกฎระเบียบที่กำหนดด้านการรักษาความปลอดภัยไซเบอร์อาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรมด้านการขนส่ง T10: ระบบจัดซื้อจัดจ้างไม่เอื้ออำนวยในการปฏิบัติงานในการจัดหาอุปกรณ์รักษาความปลอดภัยที่ทันสมัยเข้ามาใช้งาน

2.5.2 การวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์

การวิเคราะห์ SWOT เป็นการวิเคราะห์เพื่อให้ทราบสภาวะแวดล้อมภายใน และสภาวะแวดล้อมภายนอกองค์กร โดยหลักการสำคัญของ SWOT คือการวิเคราะห์โดยการสำรวจสภาพการณ์ ๒ ด้าน ทั้งสภาพการณ์ภายในและภายนอก ดังนั้นการวิเคราะห์ SWOT จึงเรียกได้ว่าเป็นการวิเคราะห์สภาพการณ์ (Situation Analysis) ซึ่งเป็นการวิเคราะห์จุดแข็ง จุดอ่อน เพื่อให้รู้ตนเอง (รู้เรา) รู้จักสภาพแวดล้อม (รู้เขา) ชัดเจนและวิเคราะห์โอกาส–อุปสรรค ซึ่งการวิเคราะห์ปัจจัยต่าง ๆ ทั้งภายนอกและภายในองค์กรจะช่วยให้ผู้บริหารขององค์กรทราบถึงการเปลี่ยนแปลงต่าง

ๆ ที่เกิดขึ้นภายนอกองค์กรทั้งสิ่งที่ได้เกิดขึ้นแล้วและแนวโน้มการเปลี่ยนแปลงในอนาคตที่อาจจะเกิดขึ้น รวมทั้งผลกระทบของการเปลี่ยนแปลงเหล่านี้ที่มีต่อองค์กรหรือหน่วยงาน โดยข้อมูลเหล่านี้จะใช้เป็นข้อมูลสำหรับการกำหนดกรอบยุทธศาสตร์หรือทิศทาง ในการพัฒนาหน่วยงานได้อย่างเหมาะสมและมีประสิทธิภาพ โดยผลสรุปการรวบรวมจุดแข็ง จุดอ่อน โอกาสและภัยคุกคามจากทุกปัจจัย ได้ผลดังตารางที่ 2-4

การวิเคราะห์ SWOT เป็นการวิเคราะห์เพื่อให้ทราบสภาวะแวดล้อมภายในและสภาวะแวดล้อมภายนอกองค์กร เป็นการชี้ให้เห็นถึงการเปลี่ยนแปลงในปัจจุบันและแนวโน้มการเปลี่ยนแปลงใน อนาคตที่อาจจะเกิดขึ้น

ตารางที่ 2-4 การรวบรวมจุดแข็ง จุดอ่อน โอกาสและภัยคุกคามที่ได้จากการวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์

จุดแข็ง (Strengths)	จุดอ่อน (Weaknesses)
S1 : หน่วยงานด้านการขนส่งมีโครงสร้างชัดเจนสำหรับภารกิจหลักและมีกฎหมายรองรับ **S2 :** หน่วยงานด้านการขนส่งมีการมอบอำนาจในการปฏิบัติงานหรือผู้รับผิดชอบในการให้บริการหลักที่สำคัญ **S3**: หน่วยงานด้านการขนส่งสามารถกำหนดแผนงานและแนวทางการดำเนินงานตอบสนองนโยบายภาครัฐได้อย่างมีประสิทธิภาพ **S4**: มีเครือข่ายความร่วมมือที่หลากหลาย **S5**: มีการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ในแต่ละหน่วยงานด้านการขนส่ง **S6:** มีความชัดเจนในกำหนดนโยบาย ระบบงานและขั้นตอนการบริหารจัดการด้านการรักษาความปลอด ภัยไซเบอร์ **S7:** มีระบบสารสนเทศที่สนับสนุนการทำงานการให้ บริการที่สำคัญให้มีประสิทธิภาพ **S8**: มีกระบวนการจัดการด้านการให้บริการในภาวะฉุกเฉินและอย่างต่อเนื่อง ในกรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ **S9**: มีระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศที่ได้มาตรฐานระดับสากล S10 : มีความพร้อมในการตอบสนองต่อนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ S11: องค์กรยอมรับการเปลี่ยนแปลงรับฟังความคิดเห็น และทันต่อเหตุการณ์ S12: มีความรู้ ความสามารถในส่วนงานที่รับผิดชอบ S13: มีแผนงานในการฝึกอบรมการรักษาความปลอดภัยไซเบอร์ S14: มีความชำนาญงานเฉพาะงานบริการหลักขององค์กร S15: สามารถใช้เทคโนโลยีสารสนเทศในการให้บริการ หลักด้านการขนส่งที่มีคุณภาพและประสิทธิภาพได้ดี	**W1:** ขาดความชัดเจนด้านการกำหนดหน่วยงานควบคุมกำกับสำหรับบางบริการสำคัญในด้านการขนส่ง (critical service and regulator in Logistic) **W2:** โครงสร้างองค์กรปัจจุบันยังไม่รองรับหรือมีการจัดตั้งตามโครงสร้างหน่วยงานการรักษาความปลอดภัยไซเบอร์ภายในหน่วยงานและระหว่างหน่วยงาน **W3:** การกำหนดโครงสร้างหน่วยงานกำกับและหน่วยงาน CII ภายใต้การกำกับยังมีความทับซ้อน **W4**: ขาดความรู้ความเข้าใจในกลยุทธ์ด้านการรักษาความปลอดภัยไซเบอร์ของหน่วยงาน **W5**: การถ่ายทอดแผนสู่การปฏิบัติไม่ชัดเจน **W6**: ขาดการติดตามผลสัมฤทธิ์การดำเนินงาน **W7**: ขาดข้อมูลในการวางแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานและกำหนดทิศทางขององค์กรด้านไซเบอร์ W8: ขาดแผนการพัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน W9: ขาดการกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII) W10: ระบบการประเมินผลยังไม่เป็นรูปธรรมที่ชัดเจน W11: ขาดการซ้อมแผนการบริหารความต่อเนื่องในการให้บริการในภาวะฉุกเฉินและในกรณีเกิดเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ W12: ขาดการสื่อสารหรือแจ้งเตือนด้านสถานการณ์ความปลอดภัยไซเบอร์ที่มีความรุนแรงมากขึ้น W13: ขาดการประสานงานร่วมมือในการปฏิบัติงานร่วมกันระหว่างหน่วยงานขนส่งด้านการรักษาความปลอดภัยไซเบอร์

S16: มีการพัฒนาเทคโนโลยีสารสนเทศที่ใช้ในการให้บริการหลักที่สำคัญ (CII) S17 : หน่วยงานด้านการขนส่งมีวิสัยทัศน์และค่านิยมที่ชัดเจนในการดำเนินงานอย่างมีประสิทธิภาพ S18 มีการกำหนดค่านิยมองค์กร S19 มีความเชื่อมั่นในการพัฒนาองค์กร	W14: การบริหารงานในองค์กร ขาดความยืดหยุ่นในการปรับปรุงโครงสร้างการบริหารงานด้านการรักษาความปลอดภัยไซเบอร์ W15: ขอบเขตอำนาจหน้าที่ความรับผิดชอบด้านการจัดการความมั่นคงปลอดภัยไซเบอร์ไม่ชัดเจน W16 : บุคลากรขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ W17 : ขาดบุคลากรที่มีความรู้และประสบการณ์ในด้านการจัดการความมั่นคงปลอดภัยไซเบอร์ W18: ขาดงบประมาณในการส่งเสริม ฝึกอบรมสร้างความชำนาญด้านการป้องกันภัยทางไซเบอร์สำหรับระบบ (CII) W19: ขาดทักษะและความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์ W20: ขาดการสร้างความรับรู้ค่านิยมองค์กร W21: ขาดการรับรู้ทิศทางด้านการจัดการและการรักษาความปลอดภัยไซเบอร์ในองค์กร W22: ขาดการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง
โอกาส (Opportunities)	**ภัยคุกคาม (Threats)**
O1: ภาครัฐมีความชัดเจนเชิงกฎหมาย นโยบายในการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ **O2:** มีการจัดตั้งหน่วยงานของรัฐสำหรับดูแลเฉพาะด้านการจัดการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ **O3:** มีนโยบายและแผนยุทธศาสตร์ระดับชาติ และเป้าหมายการพัฒนาประเทศในแผนฉบับต่าง ๆ ให้ความสำคัญกับการพัฒนาเทคโนโลยีดิจิทัล โดยมีเป้า หมายให้หน่วยงานของรัฐเป็นองค์กรดิจิทัล สนับสนุนการพัฒนาและการนำเทคโนโลยีดิจิทัลเข้ามาใช้ในการให้บริการ **O4:** การขยายของเมืองและระบบการขนส่ง เป็นปัจจัยส่งเสริมให้มีการพัฒนาระบบสารสนเทศในการให้บริการ เป็นโอกาสในการขยายการร่วมลงทุนระหว่างภาครัฐและเอกชน **O5:** พฤติกรรมของผู้ใช้งานระบบสารสนเทศที่มีการเปลี่ยนแปลงในยุค Covid -19 เป็นตัวเร่งให้องค์กรต้องพัฒนาระบบ Digital ทั้งด้านผลิตภัณฑ์ และรูปแบบการทำงาน การให้บริการใหม่ ๆ ให้รวดเร็วและตอบโจทย์ผู้ใช้งานระบบมากขึ้น **O6**: สังคมปัจจุบันเป็นสังคมที่ใช้สื่อด้านเทคโนโลยีดิจิทัล (Social Media) การรับรู้ การเข้าถึงข้อมูลสามารถทำได้ง่ายและรวดเร็ว **O7:** มีเครือข่ายพันธมิตรในหน่วยงานของรัฐ เอกชนรัฐวิสาหกิจ และหน่วยงานในต่างประเทศ ในการส่ง เสริมระบบสารสนเทศที่ให้บริการหลักที่สำคัญ (CII)	**T1:** กฎหมายและกฎระเบียบที่กำหนดด้านการรักษาความปลอดภัยไซเบอร์อาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรมด้านการขนส่ง **T2:** การของบประมาณในการพัฒนาเทคโนโลยีดิจิทัลต้องผ่านหลายขั้นตอน หรือผันแปรไปตามนโยบายรัฐบาลแต่ละสมัยที่เปลี่ยนไป **T3:** มีการใช้เทคโนโลยีสารสนเทศหรือการโจม ตีทางไซเบอร์เป็นเครื่องมือทางการเมือง T4 : ขาดการคำนึงถึงงบประมาณในการปรับ ปรุงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำคัญของหน่วยงาน และการป้อง กันภัยทางไซเบอร์ **T5:** การแพร่ระบาดของ Covid-19 ส่งผลกระทบต่อการจัดสรรงบประมาณในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการขนส่ง **T6:** การแพร่กระจายของไวรัสคอมพิวเตอร์ หรือการโจมตีทางไซเบอร์เพิ่มมากขึ้น ในการใช้สื่อสังคมออนไลน์ **T7:** บุคลากรของหน่วยงานใช้สื่อด้านเทคโนโลยีดิจิทัลผิดวัตถุประสงค์ทำให้เกิดความเสียหายต่อระบบงานสำคัญ

O8: มีความร่วมมือ ผู้เชี่ยวชาญจากภายนอกให้คำ ปรึกษาด้านการพัฒนาระบบสารสนเทศในการให้ บริการและดำเนินงานของหน่วยงานด้านการขนส่ง O9: การพัฒนาระบบสารสนเทศในการให้บริการที่สำคัญของหน่วยงานด้านการขนส่งที่เอื้อต่อการนำ มาใช้ให้บริการประชาชน และ ใช้ในการปฏิบัติงานในองค์กรให้มีความทันสมัย รวดเร็ว มีประสิทธิภาพ O10: มีการพัฒนาเครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์เพิ่มมากขึ้น O11: การทำงานในรูปแบบ WFH มากขึ้นจากสภาพ แวดล้อมที่มีการแพร่ระบาดของโควิด-19 ทำให้มีการพัฒนาเทคโนโลยีเพื่อสนับสนุนการทำงานในรูปแบบ WFH ที่ทันสมัยของหน่วยงาน O12: มีการกำหนดกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล O13: มีการกำหนดกฎหมายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562	T8: ขาดทักษะความรู้ความชำนาญในการใช้งานระบบสารสนเทศของบุคลากรของหน่วยงาน T9: ขาดทักษะความรู้ความชำนาญในการใช้เครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์ T10: ระบบจัดซื้อจัดจ้างไม่เอื้ออำนวยในการปฏิบัติงานในการจัดหาอุปกรณ์รักษาความปลอดภัยที่ทันสมัยเข้ามาใช้งาน

2.5.3 การประเมินสภาวะแวดล้อมทางยุทธศาสตร์

2.5.3.1 การกำหนดค่าน้ำหนักและคะแนนการประเมินสภาวะแวดล้อมภายในและภายนอก

โดยผู้ศึกษาได้จัดทำแบบวิเคราะห์เพื่อหาค่าถ่วงน้ำหนักสภาวะแวดล้อมภายในและภายนอกและส่งให้กลุ่มตัวอย่าง ซึ่งเป็นผู้บริหาร ผู้ใช้งานระบบสารสนเทศ และผู้ดูแลระบบสารสนเทศของหน่วยงานด้านการขนส่งจำนวน 9 คน ให้คะแนนถ่วงน้ำหนักรายประเด็น โดยกำหนดให้คะแนนถ่วงน้ำหนักรวมทุกข้อมีค่าไม่เกิน 1 ซึ่งสรุป ค่าน้ำหนักของรายการปัจจัยสภาวะแวดล้อมภายในตาม McKinsey 7'S Framework ดังตารางที่ 2-5 และสรุปค่าน้ำหนักของรายการปัจจัยสภาวะแวดล้อมภายนอกตาม PESTEL ดังตารางที่ 2-6

ตารางที่ 2-5 สรุปค่าน้ำหนักของรายการปัจจัยสภาวะแวดล้อมภายในตาม McKinsey 7'S Framework

จำนวนคน / รายการปัจจัยสภาวะแวดล้อมภายใน	1	2	3	4	5	6	7	8	9	ค่าน้ำหนักคะแนนเฉลี่ย
S1 : Structure	0.1	0.15	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.11
S2 : Strategy	0.2	0.15	0.2	0.2	0.25	0.2	0.2	0.2	0.1	0.19
S3 : Systems	0.2	0.15	0.2	0.2	0.1	0.1	0.2	0.2	0.2	0.17
S4 : Style	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.10
S5 : Staff	0.15	0.2	0.15	0.15	0.15	0.2	0.15	0.15	0.2	0.17

S6 : Skills	0.15	0.15	0.15	0.15	0.15	0.2	0.15	0.15	0.2	0.16
S7 : Shared values	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.10
น้ำหนักคะแนนรวม	1	1	1	1	1	1	1	1	1	1

ตารางที่ 2-6 สรุปค่าน้ำหนักของรายการปัจจัยสภาวะแวดล้อมภายนอกตาม PESTEL

จำนวนคน / รายการปัจจัยสภาวะแวดล้อมภายนอก	1	2	3	4	5	6	7	8	9	**ค่าน้ำหนักคะแนนเฉลี่ย**
P: (Political)	0.15	0.1	0.15	0.15	0.1	0.15	0.15	0.15	0.15	0.14
E: (Economic)	0.15	0.1	0.15	0.1	0.2	0.1	0.1	0.15	0.1	0.13
S: (Social)	0.15	0.1	0.25	0.2	0.2	0.15	0.15	0.15	0.15	0.17
T: (Technology)	0.2	0.3	0.25	0.2	0.3	0.25	0.25	0.25	0.25	0.25
E: (Environment)	0.1	0.1	0.1	0.15	0.1	0.15	0.15	0.1	0.15	0.12
L: (Legal)	0.25	0.3	0.1	0.2	0.1	0.2	0.2	0.2	0.2	0.19
น้ำหนักคะแนนรวม	1	1	1	1	1	1	1	1	1	1

2.5.3.2 การวิเคราะห์องค์กรโดยการประเมินสภาวะแวดล้อมภายในและภายนอก

ผู้ศึกษาได้ส่งแบบประเมินสภาวะแวดล้อมภายในและภายนอก ให้พนักงานของหน่วยงานด้านการขนส่ง เพื่อให้ประเมินประเด็นที่จะมีผลกระทบต่อการดำเนินงานขององค์กร โดยให้เป็นลำดับคะแนน ดังนี้

“5” คะแนน หมายถึง ส่งผลกระทบต่อการดำเนินงานมากที่สุด

“4” คะแนน หมายถึง ส่งผลกระทบต่อการดำเนินงานมาก

“3” คะแนน หมายถึง ส่งผลกระทบต่อการดำเนินงานปานกลาง

“2” คะแนน หมายถึง ส่งผลกระทบต่อการดำเนินงานน้อย

“1”คะแนนหมายถึงส่งผลกระทบต่อการดำเนินงานน้อยที่สุด

ผลการประเมินสภาวะแวดล้อมภายในและภายนอก สามารถสรุปค่าเฉลี่ยได้ดัง ตารางที่ 2-7 และ 2-8 โดยกลุ่มตัวอย่างประเมินประเด็นสำคัญที่มีผลกระทบต่อการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่งแบ่งเป็นปัจจัยเชิงบวก ได้แก่ จุดแข็ง (Strengths) และโอกาส (Opportunities) ค่าคะแนนเฉลี่ยจะแสดงเป็นจำนวนเต็มบวก (+) ส่วนปัจจัยลบ ได้แก่ จุดอ่อน (Weaknesses) และภัยคุกคาม (Threats) ค่าคะแนนเฉลี่ยจะแสดงเป็นจำนวนเต็มลบ (-) จากการประเมินของกลุ่มตัวอย่าง พบว่าปัจจัยที่เป็นจุดแข็งได้คะแนนรวมเฉลี่ย **3.84** คะแนน และปัจจัยที่เป็นจุดอ่อนได้คะแนนรวมเฉลี่ย **4.09** คะแนนซึ่งสรุปผลได้ว่าองค์กรมีปัจจัยที่เป็นจุดแข็ง **-0.25** ในขณะที่ปัจจัยภายนอกที่เป็นโอกาสได้คะแนนรวมเฉลี่ย **4.08** คะแนนและปัจจัยที่เป็นภัยคุกคามได้คะแนน รวมเฉลี่ย **4.28** คะแนน สรุปได้ว่าปัจจัยภายนอกเป็นโอกาส **-0.20**

ตารางที่ 2-7 ค่าคะแนนเฉลี่ยสภาวะแวดล้อมภายในตาม McKinsey 7'S Framework

ประเด็นสำคัญ	จุดแข็ง (Strengths)		จุดอ่อน (Weaknesses)	
	คะแนนเฉลี่ย	Strengths	คะแนนเฉลี่ย	Weaknesses
S1 : Structure	4.11	S1	4.44	W1
	4.2	S2	3.56	W2
			4.11	W3
S2 : Strategy	3.87	S3	4.22	W4
	3.45	S4	3.89	W5
	3.8	S5	3.78	W6
			4.11	W7
S3 : Systems	3.2	S6	4	W8
	3.8	S7	4.5	W9
	3.2	S8	3.78	W10
	3.6	S9	3.7	W11
			4.11	W12
			4.22	W13
S4 : Style	3.9	S10	3.89	W14
	4.2	S11	3.9	W15
S5 : Staff	4.2	S12	4.8	W16
	3.8	S13	4.6	W17
	4.3	S14		
S6 : Skills	3.9	S15	4.3	W18
	3.8	S16	4.8	W19
S7 : Shared values	3.5	S17	3.4	W20
	3.9	S18	3.3	W21
	4.2	S19	4.5	W22
รวมคะแนนเฉลี่ย	3.84		4.09	

ตารางที่ 2-8 ค่าคะแนนเฉลี่ยสภาวะแวดล้อมภายนอกตาม PESTEL

ประเด็นสำคัญ	โอกาส (Opportunities)		ภัยคุกคาม (Threats)	
	คะแนนเฉลี่ย	(Opportunities)	คะแนนเฉลี่ย	(Threats)
P: (Political)	4	O1	4.5	T1
	4.5	O2	4.6	T2
	4.6	O3	3.9	T3
E: (Economic)	3.5	O4	4.2	T4
S: (Social)	4	O5	4.2	T5
	3.9	O6	4.5	T6
	3.85	O7	3.9	T7
	3.6	O8		
T: (Technology)	3.92	O9	4.2	T8
	4.2	O10	4.5	T9
E: (Environment)	3.92	O11	0	T6
L : (Legal)	4.5	O12	0	T1
	4.6	O13	4.3	T10
รวมคะแนนเฉลี่ย	**4.08**		**4.28**	

2.5.3.3 ค่าคะแนนถ่วงน้ำหนักและสรุปผลการวิเคราะห์สภาวะแวดล้อมภายในและภายนอก

ผู้ศึกษาได้คำนวณและกำหนดค่าน้ำหนักของคะแนนในการประเมินสภาวะแวดล้อมทั้งภายในและภายนอกแล้ว รายละเอียดปรากฏดังตารางที่ 2-9 และ 2-10 โดยค่าคะแนนถ่วง น้ำหนักจะหมายถึงระดับความรุนแรงของผลกระทบต่อความสำเร็จของการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง โดยค่าที่มากจะมีผลกระทบกว่าค่าที่น้อยกว่า ทั้งนี้ค่าถ่วงน้ำหนักจะถูกนำไปใช้ในการจัดลำดับความสำคัญของปัจจัยที่มีผลต่อไป

ตารางที่ 2-9 สรุปผลคะแนนถ่วงน้ำหนักสภาวะแวดล้อมภายในตาม McKinsey 7'S Framework

รายการปัจจัยภายใน	ค่าน้ำหนัก (1)	คะแนนเฉลี่ย		คะแนนเฉลี่ย X ค่าน้ำหนัก		สรุปผล ((4) – (5))
		จุดแข็ง (2)	จุดอ่อน (3)	จุดแข็ง (4) = (2) - (1)	จุดอ่อน (5)= (3) - (1)	
S1 : Structure	0.11	4.16	4.04	0.46	0.44	0.01
S2 : Strategy	0.19	3.71	4.00	0.70	0.76	-0.06
S3 : Systems	0.17	3.45	4.05	0.59	0.69	-0.10
S4 : Style	0.1	4.05	3.90	0.41	0.39	0.02
S5 : Staff	0.17	4.10	4.7	0.70	0.80	-0.10
S6 : Skills	0.16	3.85	4.55	0.62	0.73	-0.11
S7 : Shared values	0.1	3.87	3.73	0.39	0.37	0.01
รวมคะแนนเฉลี่ยปัจจัยภายใน และสรุปผลปัจจัยภายใน				**3.85**	**4.18**	**-0.33**

ตารางที่ 2-10 สรุปผลคะแนนถ่วงน้ำหนักสภาวะแวดล้อมภายนอกตาม PESTEL

รายการปัจจัยภายนอก	ค่าน้ำหนัก (1)	คะแนนเฉลี่ย		คะแนนเฉลี่ย X ค่าน้ำหนัก		สรุปผล ((4) – (5))
		จุดแข็ง (2)	จุดอ่อน (3)	จุดแข็ง (4) = (2) - (1)	จุดอ่อน (5)= (3) - (1)	
P: (Political)	0.14	4.37	4.33	0.61	0.61	0.00
E: (Economic)	0.13	3.50	4.20	0.46	0.55	-0.09
S: (Social)	0.17	3.84	4.20	0.65	0.71	-0.06
T: (Technology)	0.25	4.06	4.35	1.02	1.09	-0.07
E: (Environment)	0.12	3.92	0.00	0.47	0.00	0.47

L : (Legal)	**0.19**	4.55	4.30	0.86	0.82	0.05
รวมคะแนนเฉลี่ยปัจจัยภายนอก และสรุปผลปัจจัยภายนอก				**4.07**	**3.77**	**0.30**

จากตาราง 2-9 และ 2-10 ได้แสดงค่าคะแนนเฉลี่ยถ่วงน้ำหนักแล้ว พบว่า ปัจจัยภายในที่เป็นจุดแข็งได้คะแนนรวมเฉลี่ย **+3.85** คะแนน และปัจจัยที่เป็นจุดอ่อนได้คะแนนรวมเฉลี่ย **–4.18** คะแนน ซึ่งสรุปผลได้ว่าองค์กรมีปัจจัยที่เป็นจุดอ่อน **-0.33** ในขณะที่ปัจจัยภายนอกที่เป็นโอกาสได้คะแนนรวมเฉลี่ย **+4.07** คะแนน และปัจจัยที่เป็นภัยคุกคามได้คะแนนรวมเฉลี่ย **-3.77** คะแนน สรุปได้ว่าองค์กรมีปัจจัยที่เป็นโอกาส **+0.30**

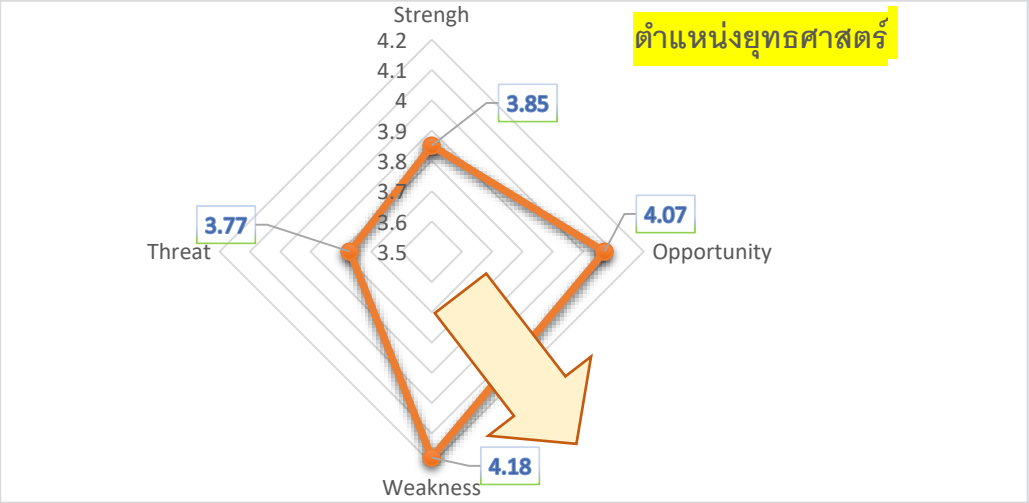
2.5.3.4 การประเมินตำแหน่งทางยุทธศาสตร์ขององค์กร

เมื่อนำเอาข้อมูลการวิเคราะห์ปัจจัยภายในและปัจจัยภายนอกที่ได้ถ่วง น้ำหนักคะแนนแล้ว มาระบุตำแหน่งในกราฟเรดาห์ ที่สร้างระหว่างปัจจัยภายในและปัจจัยภายนอกสามารถระบุตำแหน่งทางยุทธศาสตร์ (Strategic position) โดยใช้แนวคิด TOWS Matrix ซึ่งสามารถระบุตำแหน่งทางยุทธศาสตร์ได้เป็น 4 พื้นที่ที่มีความหมายต่างกัน ดังนี้

1. SO เป็นตำแหน่งที่แสดงว่า องค์กรมีจุดแข็งที่สอดคล้องกับโอกาส องค์กรประเภทนี้จึงควรกำหนดทิศทางและกลยุทธ์เชิงรุก เพื่อรักษาความได้เปรียบเชิงยุทธศาสตร์
2. WO เป็นตำแหน่งที่แสดงถึงโอกาสที่ได้เปรียบ แต่ภาพรวมภายในองค์กร มีจุดอ่อนที่ต้องการการแก้ไข ดังนั้นองค์กรประเภทนี้ควรดำเนินกลยุทธ์เชิงแก้ไข ที่มุ่งเน้นการพัฒนาองค์กร (Turnaround) เพื่อแก้ไขจุดอ่อน และสร้างจุดแข็งในการแข่งขัน
3. ST เป็นตำแหน่งที่ระบุว่าองค์กรสามารถพึ่งพาตัวเองได้ จากจุดแข็งภายใน แม้ว่าปัจจัยภายนอกจะไม่เอื้อต่อการเติบโตก็ตาม องค์กรประเภทนี้ควรดำเนินกลยุทธ์เชิงป้องกัน เพื่อใช้จุดแข็งขององค์กรในการแก้ไขวิกฤต หรือสร้างโอกาส
4. WT เป็นตำแหน่งที่แสดงให้เห็นถึงสิ่งที่อาจจะเป็นวิกฤตในอนาคต ดังนั้น องค์กรที่อยู่ในตำแหน่งทางยุทธศาสตร์นี้ ควรเร่งการดำเนินกลยุทธ์เชิงรับ โดยแก้ไขจุดอ่อน หรือ หลีกเลี่ยงภัยคุกคามที่เป็นปัญหา เพื่อหลีกเลี่ยงหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้น

จากข้อมูลการวิเคราะห์ที่ได้จากตารางสรุปผลคะแนนถ่วงน้ำหนักปัจจัย ภายในและภายนอก ผู้ศึกษาได้นำข้อมูลดังกล่าวมาจัดทำเป็นกราฟเรดาห์ เพื่อแสดงตำแหน่งทางยุทธศาสตร์ (Strategic Position) ปรากฏ**ดังภาพที่ 2**

แผนภาพที่ 2 ตำแหน่งทางยุทธศาสตร์ (Strategic Position) ของหน่วยงานด้านการขนส่ง



จากแผนภาพเราจะเห็นได้ว่า ตำแหน่งยุทธศาสตร์ด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง ตกอยู่ในพื้นที่ WO เป็นตำแหน่งที่แสดงว่า องค์กรมีจุดอ่อนที่สอดคล้องกับโอกาสและเป็นโอกาสที่ได้เปรียบแต่ภาพรวมภายในองค์กร มีจุดอ่อนที่ต้องการการแก้ไข ดังนั้นองค์กรควรดำเนินกลยุทธ์เชิงแก้ไขที่มุ่งเน้นการพัฒนาองค์กรเชิงรุก เพื่อแก้ไขจุดอ่อน และสร้างจุดแข็งในการแข่งขัน

2.5.3.5 การวิเคราะห์ TOWS Matrix

เมื่อพิจารณาผลที่ได้จากการทำ SWOT Analysis โดยเรียงลำดับของจุดแข็ง (Strengths : S) จุดอ่อน (Weaknesses : W) โอกาส (Opportunities : O) และภัยคุกคาม (Threats: T) จากคะแนนเฉลี่ยมากสุด 5 อันดับแรก ได้ผลดังนี้

1) จุดแข็ง (Strengths : S) 5 อันดับแรก

- **S14**: มีความชำนาญงานเฉพาะงานบริการหลักขององค์กร
- **S2 :** หน่วยงานด้านการขนส่งมีการมอบอำนาจในการปฏิบัติงานหรือผู้รับผิดชอบในการให้บริการหลักที่สำคัญ
- **S11**: องค์กรยอมรับการเปลี่ยนแปลงรับฟังความคิดเห็น และทันต่อเหตุการณ์
- **S12**: มีความรู้ ความสามารถในส่วนงานที่รับผิดชอบ
- **S19**: มีความเชื่อมั่นในการพัฒนาองค์กร

2) จุดอ่อน (Weakness: W)

- **W16**: บุคลากรขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
- **W19**: ขาดทักษะและความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์
- **W17**: ขาดบุคลากรที่มีความรู้และประสบการณ์ในด้านการจัดการความมั่นคงปลอดภัยไซเบอร์
- **W9**: ขาดการกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII)
- **W22**: ขาดการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง

3) โอกาส (Opportunity: O)

- **O3:** มีนโยบายและแผนยุทธศาสตร์ระดับชาติ และเป้าหมายการพัฒนาประเทศในแผนฉบับต่าง ๆ ให้ความสำคัญกับการพัฒนาเทคโนโลยีดิจิทัล โดยมีเป้าหมายให้หน่วยงานของรัฐเป็นองค์กรดิจิทัล สนับสนุน การพัฒนาและการนำเทคโนโลยีดิจิทัลเข้ามาใช้ในการให้บริการ
- **O13**: มีการกำหนดกฎหมายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562
- **O2:** มีการจัดตั้งหน่วยงานของรัฐสำหรับดูแลเฉพาะด้านการจัดการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- **O12**: มีการกำหนดกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล
- **O10**: มีการพัฒนาเครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์เพิ่มมากขึ้น

4) ภัยคุกคาม (Threat :T)

- **T2:** การของบประมาณในการพัฒนาเทคโนโลยีดิจิทัลต้องผ่านหลายขั้นตอน หรือผันแปรไปตามนโยบายรัฐบาลแต่ละสมัยที่เปลี่ยนไป
- **T1:** กฎหมายและกฎระเบียบที่กำหนดด้านการรักษาความปลอดภัยไซเบอร์อาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรมด้านการขนส่ง
- **T6:** การแพร่กระจายของไวรัสคอมพิวเตอร์ หรือการโจมตีทางไซเบอร์เพิ่มมากขึ้น ในการใช้สื่อสังคมออนไลน์
- **T9**: ขาดทักษะความรู้ความชำนาญในการใช้เครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์
- **T10:** ระบบจัดซื้อจัดจ้างไม่เอื้ออำนวยในการปฏิบัติงานในการจัดหาอุปกรณ์รักษาความปลอดภัยที่ทันสมัยเข้ามาใช้งาน

จากนั้นวิเคราะห์ความสัมพันธ์ของปัจจัยภายในและปัจจัยภายนอกที่มีความสำคัญ 5 อันดับแรกด้วยเครื่องมือ TOWS Matrix จะทำให้ได้กลยุทธ์ออกมารวม 4 รูปแบบ ซึ่งเกิดจากการจับคู่ระหว่างปัจจัยภายใน (Internal Factors) และปัจจัยภายนอก (External Factors) ที่ ได้มาจากการวิเคราะห์ SWOT และนำมาประกอบการจัดทำแผนให้เกิดทางเลือกเพื่อสามารถนำไปใช้ เป็นแนวทางในการกำหนดกลยุทธ์ ทั้งกลยุทธ์เชิงรุก (SO Strategy) กลยุทธ์เชิงป้องกัน (ST Strategy) กลยุทธ์เชิงแก้ไข (WO Strategy) และกลยุทธ์เชิงรับ (WT Strategy) โดยนำผลที่ได้จากการวิเคราะห์ ปัจจัยเชิงกลยุทธ์ (SFAS) มาจัดทำในรูปแบบของตาราง TOWS Matrix เพื่อจัดทำแผนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่ง แสดงดังตารางที่ 2-11

ตารางที่ 2-11 การวิเคราะห์แนวทางยุทธศาสตร์ด้วย TOWS Matrix

	จุดแข็ง (Strengths)	**จุดอ่อน (Weaknesses)**
ปัจจัยภายใน	■ **S14**: มีความชำนาญงานเฉพาะงานบริการหลักขององค์กร ■ **S2 :** หน่วยงานด้านการขนส่งมีการมอบอำนาจในการปฏิบัติงานหรือผู้รับผิดชอบในการให้บริการหลักที่สำคัญ	■ **W16**: บุคลากรขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ■ **W19**: ขาดทักษะและความรู้ด้านการรับมือภัยคุกคามทางไซเบอร์ ■ **W17**: ขาดบุคลากรที่มีความรู้และประสบการณ์ในด้านการจัดการความมั่นคงปลอดภัยไซเบอร์

ปัจจัยภายนอก	■ S11: องค์กรยอมรับการเปลี่ยนแปลงรับฟังความคิดเห็น และทันต่อเหตุการณ์ ■ S12: มีความรู้ ความสามารถในส่วนงานที่รับผิดชอบ ■ S19: มีความเชื่อมั่นในการพัฒนาองค์กร	■ W9: ขาดการกำหนดนโยบายด้านการพัฒนาเครื่องมือหรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII) ■ W22: ขาดการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง
โอกาส (Opportunities) ■ O3: มีนโยบายและแผนยุทธศาสตร์ระดับชาติ และเป้าหมายการพัฒนาประเทศในแผนฉบับต่าง ๆ ให้ความสำคัญกับการพัฒนาเทคโนโลยีดิจิทัล โดยมีเป้าหมายให้หน่วยงานของรัฐเป็นองค์กรดิจิทัล สนับสนุนการพัฒนาและการนำเทคโนโลยีดิจิทัลเข้ามาใช้ในการให้บริการ ■ O13: มีการกำหนดกฎหมายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ■ O2: มีการจัดตั้งหน่วยงานของรัฐสำหรับดูแลเฉพาะด้านการจัดการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ■ O12: มีการกำหนดกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล ■ O10: มีการพัฒนาเครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์เพิ่มมากขึ้น	**กลยุทธ์เชิงรุก (SO)** S11O3: ให้ความสำคัญกับการพัฒนากระบวนการ และนโยบายการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานสากลสำหรับ CII ขององค์กร	**กลยุทธ์เชิงแก้ไข (WO)** W22O2: ส่งเสริมและสนับสนุนงบประมาณด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และผู้ที่เกี่ยวข้อง W17O13: พัฒนาทักษะให้แก่บุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการรับมือภัยคุกคามทางไซเบอร์ W9O10: ส่งเสริมและกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII)
ภัยคุกคาม (Threats) ■ T2: การของบประมาณในการพัฒนาเทคโนโลยีดิจิทัลต้องผ่านหลายขั้นตอน หรือผันแปรไปตามนโยบายรัฐบาลแต่ละสมัยที่เปลี่ยนไป ■ T1: กฎหมายและกฎระเบียบที่กำหนดด้านการรักษาความปลอดภัยไซเบอร์อาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรมด้านการขนส่ง ■ T6: การแพร่กระจายของไวรัสคอมพิวเตอร์หรือการโจมตีทางไซเบอร์เพิ่มมากขึ้น ในการใช้สื่อสังคมออนไลน์ ■ T9: ขาดทักษะความรู้ความชำนาญในการใช้เครื่องมือและระบบรักษาความปลอดภัยทางไซเบอร์ ■ T10: ระบบจัดซื้อจัดจ้างไม่เอื้ออำนวยในการปฏิบัติงานในการจัดหาอุปกรณ์รักษาความปลอดภัยที่ทันสมัยเข้ามาใช้งาน	**กลยุทธ์เชิงป้องกัน (ST)** S9T6: ส่งเสริมให้มีการจัดหาหรือปรับปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ S11T6: ปรับปรุงระบบฐานข้อมูล ระบบสารสนเทศที่ให้บริการให้มีความทันสมัยและมีระบบรักษาความปลอดภัย	**กลยุทธ์เชิงรับ (WT)** W7T9: ส่งเสริมให้มีการพัฒนาเครื่องมือรักษาความปลอดภัยที่ทันสมัยและส่งเสริมบุคคลากรในองค์กรเข้ารับการอบรมด้านการรักษาความปลอดภัยไซเบอร์เชิงเทคนิค การใช้เทคโนโลยีแบบปลอดภัย W9T1: ส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานเพื่อกำหนดมาตรการเชิงรุกในด้านการเฝ้าระวัง การรับมือภัยคุกคามทางไซเบอร์ โดยมีการกำหนดแผนเผชิญเหตุและการซ้อมแผน

บทที่ 3 แผนขององค์กร

3.1 แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับหน่วยงานด้านการขนส่ง ระยะ 5 ปี (พ.ศ. 2566-2570)

การศึกษาครั้งนี้ มีวัตถุประสงค์เพื่อศึกษาสภาวะแวดล้อมทางยุทธศาสตร์ที่มีผลกระทบต่อการบริหารจัดการด้าน**ความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับ**หน่วยงานด้านการขนส่งตลอดจนการ จัดทำ**แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศ**ระยะ 5 ปี (พ.ศ. 2566-2570) เพื่อเสนอแนะแนวทางและ กลยุทธ์ในการปฏิบัติงานแก่เจ้าหน้าที่ภายในองค์กร จากการประมวลสถานการณ์ในอดีตและการ วิเคราะห์สภาวะแวดล้อมในปัจจุบัน พบว่าองค์กรในอนาคตจะมีความเสี่ยงในทุกมิติ ทั้งในด้าน เศรษฐกิจ สังคม เทคโนโลยี รวมทั้งการเมืองและกฎหมาย การศึกษานี้ จึงให้ความสำคัญต่อการกำหนดนโยบายและกลยุทธ์เชิงรุก เพื่อให้สอดรับกับเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) ยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ **ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564) แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** รวมทั้งแผนอื่น ๆ ที่เกี่ยวข้อง

3.2 เป้าหมายทางยุทธศาสตร์ (END)

วิสัยทัศน์ (Vision)

“เป็นองค์กรที่ให้บริการด้านการขนส่ง (Logistic) ที่ครบวงจร ตอบสนองความพึงพอใจให้กับลูกค้า และมุ่งมั่นในการพัฒนาเทคโนโลยีสารสนเทศเพื่อใช้ในการให้บริการที่ทันสมัยตลอดเวลา ด้วยพนักงานที่มีความรู้ความสามารถ”

พันธกิจ (Mission)

“มุ่งมั่นเป็นผู้ให้บริการด้านการขนส่ง (Logistic) ของประเทศที่มีเทคโนโลยีสารสนเทศที่ทันสมัย พร้อมใช้งาน ให้บริการอย่างถูกต้อง และ คำนึงถึงความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลของผู้ใช้งานเป็นหลัก”

ประเด็นยุทธศาสตร์ (Strategic Issues) และเป้าประสงค์ (Goals)

ประเด็นยุทธศาสตร์ที่1: กำหนดระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลในแต่ละระดับชัดเจน

เป้าประสงค์ :

1.1 มีระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศที่มีความปลอดภัยเป็นไปตามมาตรฐานสากล

1.2 มีระบบเทคโนโลยีสารสนเทศที่มีความทันสมัยและมีการพัฒนาอย่างต่อเนื่อง

<u>ประเด็นยุทธศาสตร์ที่ 2</u> : ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เป้าประสงค์ :

2.1 การปรับปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

2.2 การเพิ่มประสิทธิภาพระบบฐานข้อมูล กลางเพื่อสนับสนุนการให้บริการของหน่วยงาน

2.3 การพัฒนาขีดความสามารถของเครื่องมือที่ใช้ในการตรวจจับ เฝ้าระวังและ รับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์

<u>ประเด็นยุทธศาสตร์ที่ 3</u> : การพัฒนาบุคลากรและผู้ใช้งานระบบสารสนเทศของหน่วยงาน

เป้าประสงค์ :

3.1 การพัฒนาขีดความสามารถของบุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการป้องกัน และ รับมือภัยคุกคามทางไซเบอร์

3.2 การพัฒนาขีดความสามารถของประชาชน ผู้ใช้งานระบบ ให้มีความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์

<u>ประเด็นยุทธศาสตร์ที่ 4</u> : การพัฒนาการทำงานร่วมกันเพื่อความร่วมมือในการตอบสนองต่อสถานการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์

เป้าประสงค์ :

4.1 เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และให้การบริการสามารถดำเนินการได้อย่างต่อเนื่อง

3.3 แนวทางในการดำเนินการ (WAYS)

การกำหนดกลยุทธ์ในการดำเนินการ (WAYS) ได้มาจากการวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ภายในและภายนอกที่มีความสำคัญ 5 อันดับแรก ด้วยเครื่องมือ TOWS Matrix เพื่อนำมาวิเคราะห์ทางเลือกเชิงกลยุทธ์ที่เป็นไปได้ และจากการวิเคราะห์ตำแหน่งทางยุทธศาสตร์**ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศสำหรับ**หน่วยงานด้านการขนส่งพบว่ามีตำแหน่งทางยุทธศาสตร์ที่เอื้อต่อการดำเนินงาน ซึ่งแสดงถึงองค์กรมี**จุดอ่อนที่ต้องแก้ไขเพื่อสอดรับกับโอกาส**ดังนั้นการกำหนดกลยุทธ์ในการดำเนินงานจึงมุ่งเน้น**กลยุทธ์เชิงแก้ไข**และนำกลยุทธ์เชิงแก้ไข เชิงป้องกันและเชิงรับมาปรับใช้ในบางกรณี

สรุปประเด็นยุทธศาสตร์ เป้าประสงค์ ตัวชี้วัด และกลยุทธ์ ได้ดังตารางที่ 3-1 ถึงตารางที่ 3-4

ประเด็นยุทธศาสตร์ที่ 1 : กำหนดระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลในแต่ละระดับชัดเจน ประกอบด้วย 2 เป้าประสงค์ 2 ตัวชี้วัด และ 2 กลยุทธ์ รายละเอียดดังตารางที่ 3-1

ตารางที่ 3-1 สรุปเป้าประสงค์ ตัวชี้วัด และกลยุทธ์ ในประเด็นยุทธศาสตร์ที่ 1

ประเด็นยุทธศาสตร์	เป้าประสงค์	ตัวชี้วัด	กลยุทธ์
1. กำหนดระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลในแต่ละระดับชัดเจน	1. มีระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศที่มีความปลอดภัยเป็นไปตามมาตรฐานสากล	- ผ่านการตรวจรับรองตามมาตรฐานสากล ภายในปี 2567 โดยสถาบันผู้ตรวจสอบ	ให้ความสำคัญกับการพัฒนากระบวนการ และนโยบายการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานสากลสำหรับ CII ขององค์กร
	2. มีระบบเทคโนโลยีสารสนเทศที่มีความทันสมัยและมีการพัฒนาอย่างต่อเนื่อง	- จำนวนครั้งของการถูกโจมตีระบบสารสนเทศสำคัญไม่เกิน 1 ครั้งต่อปี	ส่งเสริมและกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII)

ประเด็นยุทธศาสตร์ที่ 2 : ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบด้วย 3 เป้าประสงค์ 3 ตัวชี้วัด และ 3 กลยุทธ์ รายละเอียดดังตารางที่ 3-2

ตารางที่ 3-2 สรุปเป้าประสงค์ ตัวชี้วัด และกลยุทธ์ ในประเด็นยุทธศาสตร์ที่ 2

ประเด็นยุทธศาสตร์	เป้าประสงค์	ตัวชี้วัด	กลยุทธ์
ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	1. การปรับปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์	ร้อยละของระบบเครือข่ายและระบบคอมพิวเตอร์มีความพร้อมใช้งาน และให้บริการ	ส่งเสริมให้มีการจัดหาหรือปรับปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์
	2. การเพิ่มประสิทธิภาพระบบฐานข้อมูล กลางเพื่อสนับสนุนการให้บริการของหน่วยงาน	ร้อยละของระบบฐานข้อมูลและระบบสารสนเทศมีความพร้อมใช้งานและพร้อมให้บริการ	ปรับปรุงระบบฐานข้อมูล ระบบสาร สนเทศที่ให้บริการให้มีความทันสมัยและมีระบบรักษาความปลอดภัย
	3. การพัฒนาขีดความสามารถของเครื่องมือที่ใช้ในการตรวจจับ เฝ้าระวังและ รับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์	ร้อยละของเหตุการณ์ละเมิดความมั่นคงปลอดภัยไวเบอร์ลดลง	ส่งเสริมให้มีการพัฒนาเครื่องมือรักษาความปลอดภัยที่ทันสมัย และส่งเสริมบุคคลากรในองค์กรเข้ารับการอบรมด้านการรักษาความปลอดภัยไซเบอร์เชิงเทคนิค การใช้เทคโนโลยีแบบปลอดภัย

ประเด็นยุทธศาสตร์ที่ 3 : การพัฒนาบุคลากรและผู้ใช้งานระบบสารสนเทศของหน่วยงาน ประกอบด้วย 2 เป้าประสงค์ 2 ตัวชี้วัด และ 2 กลยุทธ์ รายละเอียดดังตารางที่ 3-3

ตารางที่ 3-3 สรุปเป้าประสงค์ ตัวชี้วัด และกลยุทธ์ ในประเด็นยุทธศาสตร์ที่ 3

ประเด็นยุทธศาสตร์	เป้าประสงค์	ตัวชี้วัด	กลยุทธ์
การพัฒนาบุคลากรและผู้ใช้งานระบบสารสนเทศของหน่วยงาน	1. การพัฒนาขีดความสามารถของบุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการป้องกัน และ รับมือภัยคุกคามทางไซเบอร์	จำนวนบุคลากรที่ผ่านการฝึกอบรมด้านการรับมือภัยคุกคามทางไซเบอร์	พัฒนาทักษะให้แก่บุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการรับมือภัยคุกคามทางไซเบอร์
	2. การพัฒนาขีดความสามารถของประชาชน ผู้ใช้งานระบบให้มีความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์	จำนวนครั้งของการจัดอบรมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จำนวนผู้เข้ารับฟังการอบรม (ประชาชนและผู้ที่เกี่ยวข้อง)	ส่งเสริมและสนับสนุนงบประมาณด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และผู้ที่เกี่ยวข้อง

ประเด็นยุทธศาสตร์ที่ 4 : การพัฒนาบุคลากรและผู้ใช้งานระบบสารสนเทศของหน่วยงาน ประกอบด้วย 1 เป้าประสงค์ 1 ตัวชี้วัด และ 1 กลยุทธ์ รายละเอียดดังตารางที่ 3-4

ตารางที่ 3-4 สรุปเป้าประสงค์ ตัวชี้วัด และกลยุทธ์ ในประเด็นยุทธศาสตร์ที่ 4

ประเด็นยุทธศาสตร์	เป้าประสงค์	ตัวชี้วัด	กลยุทธ์
การพัฒนาการทำงานร่วมกันเพื่อความร่วมมือในการตอบสนองต่อสถานการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์	เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันที และให้การบริการสามารถดำเนินการได้อย่างต่อเนื่อง	จำนวนครั้งของการเข้าร่วมซ้อมแผนเผชิญเหตุร่วมกัน จำนวนครั้งของความสำเร็จของการซ้อมแผน	ส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานเพื่อกำหนดมาตรการเชิงรุกในด้านการเฝ้าระวัง การรับมือภัยคุกคามทางไซเบอร์ โดยมีการกำหนดแผนเผชิญเหตุและการซ้อมแผน

3.4 มาตรการ/เครื่องมือ/ปัจจัยที่เกี่ยวข้อง (MEANS)

จากประเด็นยุทธศาสตร์ เป้าประสงค์ ตัวชี้วัดและกลยุทธ์ที่ได้จากข้อ 3.3 สามารถนำมาจัดทำแผนงาน/โครงการในแต่ละประเด็นยุทธศาสตร์ โดยมีรายละเอียดดังนี้

- ประเด็นยุทธศาสตร์ที่ 1 มีจำนวน 5 แผนงาน /โครงการ/กิจกรรม
- ประเด็นยุทธศาสตร์ที่ 2 มีจำนวน 9 แผนงาน / โครงการ/กิจกรรม

- ประเด็นยุทธศาสตร์ที่ 3 มีจำนวน 6 แผนงาน /โครงการ/กิจกรรม
- ประเด็นยุทธศาสตร์ที่ 4 มีจำนวน 4 แผนงาน /โครงการ/กิจกรรม ตามตารางที่ 3–5

ตารางที่ 3–5 แผนงาน/โครงการในแต่ละประเด็นยุทธศาสตร์มีรายละเอียดดังต่อไปนี้

ประเด็นยุทธศาสตร์ที่ 1: กำหนดระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลในแต่ละระดับให้ชัดเจน							
เป้าประสงค์ที่ 1.1: . มีระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศที่มีความปลอดภัยเป็นไปตามมาตรฐานสากล							
กลยุทธ์ 1: ให้ความสำคัญกับการพัฒนากระบวนการ และนโยบายการบริหารจัดการความมั่นคงปลอด ภัยไซเบอร์ ตามมาตรฐานสากลสำหรับ CII ขององค์กร							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
1	การพัฒนากระบวนการ และนโยบายการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล ISO27001:2022	5	3	3	3	3	ทุกหน่วยงานด้านการขนส่ง

ประเด็นยุทธศาสตร์ที่ 1: กำหนดระบบบริหารจัดการความปลอดภัยของข้อมูลสารสนเทศและข้อมูลส่วนบุคคลในแต่ละระดับให้ชัดเจน							
เป้าประสงค์ที่ 1.2: มีระบบเทคโนโลยีสารสนเทศที่มีความทันสมัยและมีการพัฒนาอย่างต่อเนื่อง							
กลยุทธ์ 2: ส่งเสริมและกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกันระบบงานที่สำคัญ (CII)							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
3	การปรับปรุงและเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยทางไซเบอร์	50	50	50	50	50	สำนักงานนโยบายและแผนการขนส่งและจราจร
4	การศึกษาทบทวนระบบคอมพิวเตอร์และระบบเครือข่ายและการรักษาความมั่นคงปลอดภัยทางไซเบอร์	10	10	10	10	10	สำนักงานนโยบาย และแผนการขนส่งและจราจร
5	ตรวจสอบ จัดซื้อและติดตั้ง Software Antivirus หรือ ระบบ Sandbox เพื่อตรวจสอบไวรัสสำหรับเครื่องลูกข่ายตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและดิจิทัลในภาวะฉุกเฉิน	15	15	15	15	15	สถาบันการบินพลเรือน
ประเด็นยุทธศาสตร์ที่ 2 : ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ							
เป้าประสงค์ 2.1: การปรับปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์							
กลยุทธ์ 1: ส่งเสริมให้มีการจัดหาหรือปรับ ปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
1	โครงการปรับปรุงระบบรักษาความปลอดภัย และ เครือข่ายคอมพิวเตอร์	30	30	30	30	30	ทุกหน่วยงานด้านการขนส่ง

2	โครงการปรับปรุงประสิทธิภาพระบบการรักษาความปลอดภัยระบบเครือข่ายและการใช้งานเครือข่ายอินเตอร์เน็ต	40	40	40	40	40	กรมทางอากาศยาน
<u>เป้าประสงค์ 2.2:</u> การเพิ่มประสิทธิภาพระบบฐานข้อมูล กลางเพื่อสนับสนุนการให้บริการของหน่วยงาน							
<u>กลยุทธ์ 2:</u> ปรับปรุงระบบฐานข้อมูล ระบบสาร สนเทศที่ให้บริการให้มีความทันสมัยและมีระบบรักษาความปลอดภัย							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
3	โครงการเพิ่มประสิทธิภาพระบบฐานข้อมูลกลางเพื่อสนับสนุนการให้บริการ	25	25	25	25	25	กรมการขนส่งทางบก
4	โครงการปรับปรุงและเพิ่มประสิทธิภาพระบบสารสนเทศ	50	50	50	50	50	ทุกหน่วยงานด้านการขนส่ง
5	โครงการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ของท่าเรือกรุงเทพ	15	15	15	15	15	การท่าเรือแห่งประเทศไทย
6	โครงการซื้อพร้อมติดตั้งอุปกรณ์รักษาความปลอดภัยบนเครือข่ายทดแทนของเดิม	30	30	30	30	30	ทุกหน่วยงานด้านการขนส่ง
7	โครงการจัดหาระบบป้องกันข้อมูลรั่วไหล	25	25	25	25	25	ทุทุกหน่วยงานด้านการขนส่ง
8	โครงการปรับปรุงศูนย์สำรองและศูนย์เทคโนโลยีสารสนเทศ	30	30	30	30	30	กรมการขนส่งทางบก
<u>เป้าประสงค์ 2.3:</u> การพัฒนาขีดความสามารถของเครื่องมือที่ใช้ในการตรวจจับ เฝ้าระวังและ รับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์							
<u>กลยุทธ์ 3:</u> ส่งเสริมให้มีการพัฒนาเครื่องมือรักษาความปลอดภัยที่ทันสมัยและส่งเสริมบุคคลากรในองค์กรเข้ารับการอบรมด้านการรักษาความปลอดภัยไซเบอร์เชิงเทคนิค การใช้เทคโนโลยีแบบปลอดภัย							
9	โครงการพัฒนาระบบบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและฝึกอบรมการใช้งานอุปกรณ์รักษาความปลอดภัย	20	20	20	20	20	ทุกหน่วยงานด้านการขนส่ง
<u>ประเด็นยุทธศาสตร์ที่ 3</u> : การพัฒนาบุคลากรและผู้ใช้งานระบบสารสนเทศของหน่วยงาน							
<u>เป้าประสงค์ 3.1</u>: การพัฒนาขีดความสามารถของบุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการป้องกัน และ รับมือภัยคุกคามทางไซเบอร์							
<u>กลยุทธ์ 1:</u> พัฒนาทักษะให้แก่บุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการรับมือภัยคุกคามทางไซเบอร์							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
1	โครงการพัฒนาทักษะและสร้างความตระหนักแก่บุคลากรด้านเทคโนโลยีสารสนเทศ	5	5	5	5	5	ทุกหน่วยงานด้านการขนส่ง
2	โครงการฝึกอบรม เรื่องความปลอดภัยด้านไซเบอร์ (Cyber Security)	5	5	5	5	5	สำนักงานนโยบาย และแผนการขนส่ง และจราจร
<u>เป้าประสงค์ 3.2:</u> การพัฒนาขีดความสามารถของประชาชน ผู้ใช้งานระบบ ให้มีความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์							

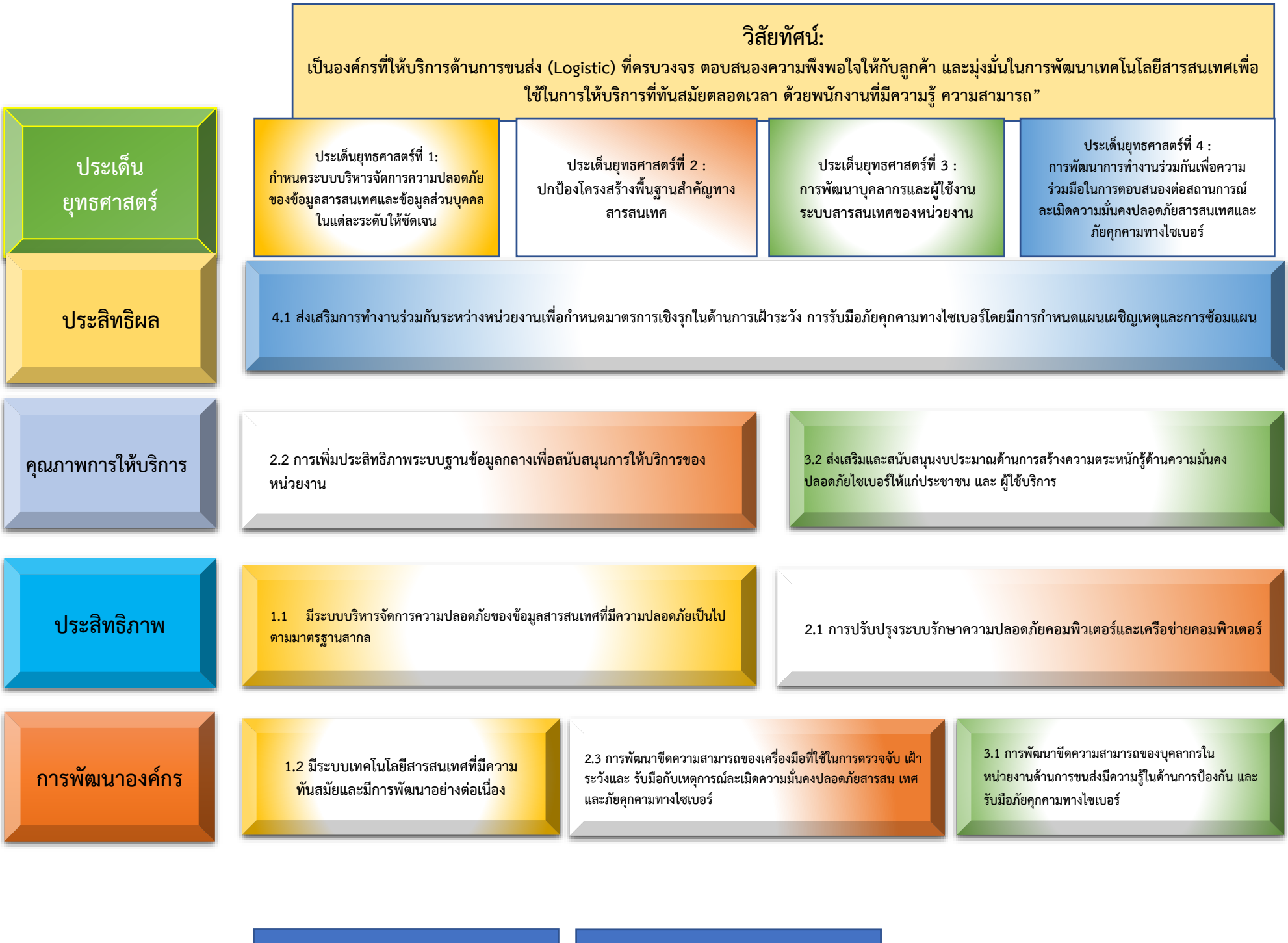
<u>กลยุทธ์ 2:</u> ส่งเสริมและสนับสนุนงบประมาณด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และผู้ที่เกี่ยวข้อง							
3	โครงการสร้างความตระหนักรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรด้าน IT ที่สังกัดกระทรวงคมนาคม	3	2	2	2	2	สำนักงานปลัดกระทรวงคมนาคม
4	โครงการเสริมสร้างความรู้ความเข้าใจเรื่องความมั่นคงปลอดภัยข้อมูล ให้แก่ผู้ใช้งานระบบ	2	2	2	2	2	การรถไฟแห่ง ประเทศไทย
5	แผนการสร้างความตระหนักรู้ (Awareness) สำหรับพนักงานภายในการท่าเรือฯ	2	2	2	2	2	การท่าเรือแห่งประเทศไทย
6	โครงการพัฒนาความรู้ความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรด้านดิจิทัล	5	5	5	5	5	สำนักงานการบิน พลเรือนแห่ง ประเทศไทย
<u>ประเด็นยุทธศาสตร์ที่ 4</u> : การพัฒนาการทำงานร่วมกันเพื่อความร่วมมือในการตอบสนองต่อสถานการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์							
<u>เป้าประสงค์ 4.1</u>: เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันทีและให้การบริการสามารถดำเนินการได้อย่างต่อเนื่อง							
<u>กลยุทธ์ 1:</u> ส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานเพื่อกำหนดมาตรการเชิงรุกในด้านการเฝ้าระวัง การรับมือภัยคุกคามทางไซเบอร์ โดยมีการกำหนดแผนเผชิญเหตุและการซ้อมแผน							
ลำดับที่	**แผนงาน/โครงการ/กิจกรรม**	**เป้าหมายปี พ.ศ. และวงเงิน (ล้านบาท)**					**หน่วยงานที่เกี่ยวข้อง**
		66	**67**	**68**	**69**	**70**	
1	โครงการเพิ่มประสิทธิภาพการรับมือภัยคุกคามไซเบอร์และจัดตั้งศูนย์ประสานงานเฝ้าระวังภัยคุกคามทางไซเบอร์	40	10	10	10	10	ทุกหน่วยงานด้านการขนส่ง
2	โครงการเช่าบริการดาต้าเซ็นเตอร์สำรองเพื่อการกู้คืนข้อมูลกรณีเกิดภัยพิบัติ (DR site)	20	20	20	20	20	กรมทางหลวง
3	การวิเคราะห์และประเมินผลการดำเนินงานด้าน Cybersecurity	-	15	5	5	5	สำนักงานนโยบาย และแผนการขนส่ง และจราจร
4	แผนพัฒนาความมั่นคงด้าน Cyber Security	30	15	15	15	15	การรถไฟแห่งประเทศไทย

3.5 แผนที่ยุทธศาสตร์ (Strategic Map)

ผู้ศึกษาได้จัดทำแผนที่ยุทธศาสตร์ (Strategic Map) โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการขนส่งและโลจิสติกส์ โดยกำหนดเป้าประสงค์ในแต่ละมิติ จากการวิเคราะห์กลยุทธ์ตามแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม พบว่า หน่วยงานด้านการขนส่ง มีกลยุทธ์ที่สอดคล้องและเป็นกลยุทธ์หลักที่จะต้องดำเนินการจำนวน 8 กลยุทธ์ ได้แก่

กลยุทธ์ที่ 1	การพัฒนากระบวนการ และนโยบายการบริหารจัดการความมั่นคงปลอด ภัยไซเบอร์ ตามมาตรฐานสากลสำหรับ CII ขององค์กร
กลยุทธ์ที่ 2	ส่งเสริมและกำหนดนโยบายด้านการพัฒนาเครื่องมือ หรือ ระบบการรักษาความปลอดภัยไซเบอร์เพื่อป้องกัน ระบบงานที่สำคัญ (CII)
กลยุทธ์ที่ 3	ส่งเสริมให้มีการจัดหาหรือปรับ ปรุงระบบรักษาความปลอดภัยคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์
กลยุทธ์ที่ 4	ปรับปรุงระบบฐานข้อมูล ระบบสาร สนเทศที่ให้บริการให้มีความทันสมัยและมีระบบรักษาความปลอดภัย
กลยุทธ์ที่ 5	ส่งเสริมให้มีการพัฒนาเครื่องมือรักษาความปลอดภัยที่ทันสมัยและส่งเสริมบุคคลากรในองค์กรเข้ารับการอบรมด้าน การรักษาความปลอดภัยไซเบอร์เชิงเทคนิค การใช้เทคโนโลยีแบบปลอดภัย
กลยุทธ์ที่ 6	พัฒนาทักษะให้แก่บุคลากรในหน่วยงานด้านการขนส่งมีความรู้ในด้านการรับมือภัยคุกคามทางไซเบอร์
กลยุทธ์ที่ 7	ส่งเสริมและสนับสนุนงบประมาณด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และผู้ที่เกี่ยวข้อง
กลยุทธ์ที่ 8	ส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานเพื่อกำหนดมาตรการเชิงรุกในด้านการเฝ้าระวัง การรับมือภัยคุกคาม ทางไซเบอร์ โดยมีการกำหนดแผนเผชิญเหตุและการซ้อมแผน

3.5.1Strategy Mapping



บทที่ 4 ข้อเสนอแนะทางยุทธศาสตร์

4.1 ข้อเสนอแนะในการขับเคลื่อนและการนำยุทธศาสตร์ไปใช้

ผลจากการศึกษาและจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศระยะ 5 ปี (พ.ศ. 2566-2570) ในครั้งนี้ ผู้ศึกษามีข้อเสนอแนะในการขับเคลื่อนและการนำยุทธศาสตร์ไปประยุกต์ใช้ เพื่อให้เกิดประโยชน์สูงสุด ดังนี้

1) ในการบูรณาการยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์จะต้องพิจารณาบทบาท ของผู้มีส่วนได้เสียทั้งหมด โดยกรอบการดำเนินงานจะต้องถูกสร้างขึ้นโดยอาศัยความร่วมมือ ระหว่างภาคอุตสาหกรรมการขนส่งและรัฐบาล ซึ่งต้องมีมาตรฐานในการดำเนินการและมาตรฐานที่ เฉพาะเจาะจง แนวทางและวิธีปฏิบัติในการส่งเสริมความมั่นคงของชาติ โดยกรอบการดำเนินงาน จะต้องมีการสร้างแนวทางเพื่อทำความเข้าใจถึงภัยคุกคาม และมีแนวทางสำหรับการลดความเสี่ยง จากภัยคุกคามทางไซเบอร์โดยเฉพาะ ซึ่งเป็นการช่วยให้ทุกภาคส่วนสามารถจัดลำดับความสำคัญ และดำเนินการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่สำคัญได้รวดเร็วและมีความเหมาะสมมากขึ้น
2) องค์ประกอบของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สามารถจำแนก ได้เป็น 5 ขั้นตอน ได้แก่ การ **ระบุ (Identify), การป้องกัน (Protect), การตรวจสอบ (Detect), การตอบสนอง (Respond) และการคืนสภาพ (Recover)** (อ้างอิง “NIST Cyber Security Framework”) ซึ่งช่วยในการเรียนรู้ถึงความเสี่ยงทางไซเบอร์ที่เกิดขึ้นได้โดยสามารถจัดระเบียบข้อมูล เพื่อช่วยในการตัดสินใจเกี่ยวกับการบริหารความเสี่ยง และการบริหารและการบรรเทาผลกระทบของภัยคุกคาม จากการเรียนรู้และการพัฒนาจาก ประสบการณ์ในอดีตที่ผ่านมา
3) กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์จะต้องกำหนดให้เป็นภาษาที่เข้าใจง่าย เพื่อให้เกิดความสอดคล้องตรงกัน ทั้งในเรื่องความเข้าใจ การจัดการ และความเสี่ยงทางไซเบอร์ทั้งภายในและภายนอกองค์กร โดยกรอบการดำเนินงานนี้สามารถช่วยกำหนดและจัดลำดับ ความสำคัญสำหรับการดำเนินการเพื่อลดความเสี่ยงด้านความปลอดภัยไซเบอร์และเป็นเครื่องมือ สำหรับการปรับนโยบาย กระบวนการทางธุรกิจ และวิธีการทางเทคนิคเพื่อการจัดการความเสี่ยงทางไซเบอร์
4) กรอบการดำเนินงานนี้จะเป็นแนวทางให้องค์กรธุรกิจและภาครัฐ สามารถทำความเข้าใจ ในการปฏิบัติงานและการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีความสอดคล้องกับความต้องการในองค์กรแต่ละองค์กร อย่างไรก็ตามกรอบการดำเนินงานอาจมีแนวปฏิบัติด้านการรักษาความปลอดภัยที่ไม่ได้เหมาะสมกับองค์กรทุกองค์กร แต่ถือเป็นจุดเริ่มต้น ในการดำเนินงานด้านความปลอดภัยไซเบอร์สำหรับทุกองค์กรโดยกรอบการดำเนินงานนี้ถูกสร้างมาเพื่อกำหนดทิศทาง แก่องค์กรธุรกิจและภาครัฐ ซึ่งไม่ได้เป็นการกำหนดเพื่อให้เหมาะสมกับทุกองค์กร ซึ่งในบางองค์กรอาจมีแนวทางการปฏิบัติงานด้านการรักษาความปลอดภัยไซเบอร์โดยเฉพาะของตนเองที่แตกต่างจาก องค์กรอื่นๆ

นอกจากนี้ผลจากการศึกษาตามหลักยุทธศาสตร์รวมถึงการจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศระยะ 5 ปี (พ.ศ. 2566-2570) ในครั้งนี้มีข้อมูลการวิเคราะห์จุดอ่อน จุดแข็ง โอกาสและอุปสรรคที่ทำให้หน่วยงานด้านการขนส่งและโลจิสติกส์ได้เข้าใจตำแหน่งยุทธศาสตร์ด้าน

การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้บริการสำคัญในกลุ่มอุตสาหกรรมด้านการขนส่งว่าอยู่จุดใด และสามารถนำข้อมูลนี้ไปกำหนดแผนงานของหน่วยงานตนเองในการปรับปรุงกลยุทธ์หรือแผนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างละเอียดและเหมาะสมกับหน่วยงานนั้น ๆ ต่อไป

บรรณานุกรม

1. ข้อมูลภัยคุกคามทางไซเบอร์ ที่มาจาก https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
2. ข้อมูลรายงานข้อมูลการใช้อินเตอร์เน็ตที่มาจาก https://www.nbtc.go.th/News/Information/ รายงานข้อมูลการใช้อินเตอร์เน็ตของประเทศไทย-ปี- 2559.aspx
3. ข้อมูลภัยคุกคามทางไซเบอร์ ที่มาจาก https://www.thesslstore.com/blog/2018-cybercrime-statistics
4. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. 2561. **ยุทธศาสตร์ชาติ**. สืบค้น 21 กุมภาพันธ์ 2566, จาก http://www.nesdc.go.th/download/document/SAC/NS_PlanOct2018.pdf
5. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. 2565. **แผนพัฒนาเศรษฐกิจและสังคม แห่งชาติ ฉบับที่ 13 (พ.ศ.2566 – 2570)** สืบค้น 21 กุมภาพันธ์ 2566, จาก http://www.nesdc.go.th/download/Plan13/Doc/Plan13_Final.pdf
6. สานักงานสภาความมั่นคงแห่งชาติ ได้จัดทายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์. แห่งชาติ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) (National Cybersecurity Strategy 2017 – 2021)

ประวัติย่อผู้วิจัย

ชื่อ-สกุล:	**นางสาว อธิตานันท์ อภิธนทวีพัฒน์**
วัน เดือน ปีเกิด:	**22 พฤษภาคม 2511**
การศึกษา:	**ปริญญาโท การบริหารจัดการระบบสารสนเทศ (Master of Information Technology) University of Wollongong, Australia** **ปริญญาตรีบริหารธุรกิจ ด้านการวิเคราะห์ระบบสารสนเทศ (Bachelor of Commerce in Business System Analysis) University of Wollongong, Australia** **ปริญญาตรีบริหารธุรกิจ ด้านการเงินการธนาคาร (Bachelor of Business Administration, in Finance and Banking, Assumption University)** **หลักสูตรการบริหารงานตำรวจในยุคดิจิทัล (Police Administration in Digital/PADA 3)** **หลักสูตรผู้นำพอเพียงเพื่อความมั่นคง (นพม.) รุ่นที่ 14** **หลักสูตรพัฒนาสัมพันธ์ระดับผู้บริหาร กองทัพอากาศ (พสบ.ทอ.) รุ่นที่ 16** **หลักสูตรวิทยาการการจัดการสำหรับนักบริหารระดับสูง (วบส.) รุ่นที่ 9**
ประวัติการทำงาน:	**Head Of IT Department, TUV Nord, Essen, Germany**
ตำแหน่งปัจจุบัน:	**กรรมการผู้จัดการ** **บริษัท เอเชี่ยนอินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด ประเทศไทย**