แนวทางการพัฒนาการปฏิบัติการข่าวสารของกองทัพภาคที่ 3 เพื่อเสริมสร้างความมั่นคงอย่างเป็นองค์รวม

เอกสารวิจัยส่วนบุคคล

โดย

พันเอก สืบสกุล ชมภูนุช

เสนาธิการกรมทหารราบที่ 7 กองพลทหารราบที่ 4

วิทยาลัยการทัพบก

กันยายน 2565

เอกสารวิจัยเรื่อง แนวทางการพัฒนาการปฏิบัติการข่าวสารของกองทัพภาคที่ 3 เพื่อเสริมสร้างความมั่นคงอย่างเป็นองค์รวม

โดย พันเอก สืบสกุล ชมภูนุช

อาจารย์ที่ปรึกษา พันเอกหญิง นวลสมร จรวงษ์

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2565 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ **ดีมาก**

พลตรี (วิชาติ เอี่ยมไพจิตร์) **ผู้บัญชาการวิทยาลัยการทัพบก**

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก (สินสมุทร์ จันทรเนตร) **ประธานกรรมการ**

พันเอก (เจน สุขศรีทอง) **ผู้ทรงคุณวุฒิที่ปรึกษา**

พันเอกหญิง (นวลสมร จรวงษ์) **กรรมการ**

บทคัดย่อ

ผู้วิจัย นาวาอากาศเอก สืบศิริ อ่ำสำอางค์

เรื่อง กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์
บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และ
พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ 2562

วันที่ กันยายน 2565 **จำนวนคำ:** 8,342 คำ **จำนวนหน้า:** 31 หน้า

คำสำคัญ องค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศ, เทคโนโลยีการดำเนินงาน, กรอบการปฏิบัติการความมั่นคงไซเบอร์, มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ, พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562

ชั้นความลับ ไม่มีชั้นความลับ

เครือข่ายเทคโนโลยีการดำเนินงานในองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ตและมีการป้องกันภัยคุกคามทางไซเบอร์เป็นแบบง่ายๆ อีกทั้งการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจทำให้การดำเนินงานขององค์กรต้องหยุดชะงักลงไป ประกอบกับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหลายประเภทที่ต้องการความมั่นคงปลอดภัยไซเบอร์ในที่แตกต่างกันไป ในการศึกษาเฉพาะเรื่องนี้มีวัตถุประสงค์เพื่อจัดทำกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ความสอดคล้องกับความต้องการในการดำเนินธุรกิจหลักและผู้เกี่ยวข้องทุกภาคส่วนขององค์กร และตอบสนองต่อ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยใช้ระเบียบวิธีการวิเคราะห์โครงสร้าง (Structural model) จากมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ เพื่อการวิเคราะห์วิธีการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งใช้กำหนดขอบเขตข้อมูลจากมาตรการความมั่นคงปลอดภัยไซเบอร์จากมาตรฐาน ISO/IEC 27001 และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 ในการศึกษาพบว่ากรอบแนวทางที่ใช้ในการออกแบบกระบวนการการจัดการและพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศในภาพรวมทั้งองค์กร สามารถใช้เป็นแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 44 ของ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 ซึ่งเชื่อมโยงสู่ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ABSTRACT

AUTHOR: Group Captain Seubsiri Aumsum-ang

TITLE: Strategic Cybersecurity Framework Based on Baldrige Excellency Criteria and Thai Cybersecurity Law and Regulation

DATE: September 2021 **WORD COUNT:** 8,342 **PAGES:** 31

KEY TERMS: Operational technology network, IT critical infrastructures, Strategic Cybersecurity Framework, Baldrige Excellency Criteria, Thai Cybersecurity Law and Regulation

CLASSIFICATION: Unclassified

Operational technology network is critical for IT infrastructure within organisations which are connected to the Internet with simple protection against cyber threats. It is not only the development of cybersecurity systems that may cause disruption to an organization's operations but also there are different types of critical IT infrastructure within organisations which require tailored cybersecurity solutions. The objective of this specific study is to develop a strategic cybersecurity framework for critical IT infrastructure within organisations which are consistent with the core business needs and the needs of the organization's participants which include responsibility to the Cybersecurity Act 2019. The Baldrige Cybersecurity Excellence Builder system has been deployed to analyse by Structural model and define the data boundaries of the ISO/IEC 27001 standard and the Cybersecurity Act 2019. The study found that a strategic framework to design a management system and develop a cybersecurity strategy for critical IT infrastructure within organizations in the whole enterprise and a substance can be used as a cyber-threat response plan together with a risk assessment and the criteria which follow through section 44 of the Cybersecurity Act 2019.

กิตติกรรมประกาศ

การวิจัยเชิงยุทธศาสตร์ เรื่อง “กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ 2562” ตามแนวทางการศึกษาในหลักสูตรหลักประจำ วิทยาลัยการทัพบก ซึ่งงานวิจัยฉบับนี้ ทำให้ผู้วิจัยได้รับความรู้ ทักษะ และกระบวนการความคิด

ขอขอบพระคุณ ผู้บัญชาการวิทยาลัยการทัพบก ผู้ส่งเสริมให้เกิดศักยภาพในการแสวงหาความรู้ของกองทัพบกให้มีประสิทธิภาพ บังเกิดประโยชน์ต่อหน่วย และประเทศชาติ ขอขอบพระคุณ ประธานกรรมการควบคุมเอกสารวิจัยส่วนบุคคล กรรมการควบคุมเอกสารวิจัยส่วนบุคคล อาจารย์ที่ปรึกษา และผู้ทรงคุณวุฒิที่ปรึกษา กรุณาเอื้อเฟื้อ เสียสละเวลา ให้ข้อมูล คำแนะนำ ช่วยปรับแก้ไขให้งานวิจัยให้ความกรุณาถ่ายทอดความรู้และประสบการณ์ ในการทำงานวิจัย ตลอดจนให้ข้อแนะนำและแนวคิด รวมถึงมุมมองและวิสัยทัศน์ อันทรงค่าอย่างยิ่งต่องานวิจัย

ท้ายนี้ ผู้วิจัยขอขอบพระคุณ คณะอาจารย์ วิทยาลัยการทัพบกทุกท่าน ที่ได้มอบความรู้ ทักษะในการศึกษา และเป็นกำลังใจอย่างดียิ่ง อีกทั้งขอขอบคุณเพื่อนนักศึกษา หลักสูตรหลักประจำ วิทยาลัยการทัพบก ชุดที่ 67 ที่ให้การสนับสนุนและช่วยเหลือด้วยดีและหวังว่า งานวิจัยฉบับนี้จะเป็นประโยชน์กองทัพและประเทศชาติสืบไป

สารบัญ

หน้า

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

อาชญากรไซเบอร์ใช้เทคโนโลยีสาระสนเทศและการสื่อสารข้อมูลรูปแบบต่างๆ ในการก่ออาชญากรรมทางอินเทอร์เน็ต ซึ่งไม่มีขีดจำกัดด้านขอบเขตและทางภูมิศาสตร์อันก่อให้เกิดผลกระทบมหาศาลต่อความมั่นคงโลก ผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์คาดการณ์ว่าค่าใช้จ่ายสุทธิทั้งหมดของอาชญากรรมในโลกไซเบอร์จะเพิ่มขึ้น 15% ต่อปี ในช่วง 5 ปีข้างหน้า[1]

ในอดีต อาชญากรไซเบอร์ได้กำหนดเป้าหมายไปยังอุตสาหกรรมต่างๆ โดยเฉพาะพลังงานและอีคอมเมิร์ซ ซึ่งพวกเขาได้รับผลประโยชน์ทางการเงินมหาศาล ในปี 2020 อุตสาหกรรมการดูแลสุขภาพกลายเป็นจุดสนใจหลัก โดยอาชญากรไซเบอร์มุ่งเป้าไปที่ช่องโหว่ของระบบในโรงพยาบาล ศูนย์ดูแลสุขภาพ ผู้ผลิตวัคซีน และห้องปฏิบัติการที่ต้องการเรียกค่าไถ่[1]

โดยทั่วไปองค์กรอุตสาหกรรมและองค์กรด้านโครงสร้างพื้นฐานสำคัญที่ต้องใช้ระบบควบคุมทางอุตสาหกรรม (ICS : Industrial Control Systems) เพื่อใช้ประกอบธุรกิจ เช่น บริษัท ด้านพลังงาน สาธารณูปโภค น้ำมันและก๊าซ ยา ผลิตสารเคมี อาหารเครื่องดื่ม ซึ่งเป็นแหล่งสะสมของเทคโนโลยีสารสนเทศแบบดั้งเดิมที่เชื่อมต่อกับอินเทอร์เน็ตสาธารณะและการป้องกันแบบง่ายๆ รวมถึงความเชื่อที่ว่าเครือข่ายเทคโนโลยีการดำเนินงาน (OT : Operational Technology)[2] ที่ไม่ได้รับการตรวจสอบหรือแก้ไขแต่อย่างใด เนื่องจากความเชื่อเดิมว่าอุปกรณ์หรือเทคโนโลยีดังกล่าวจะถูกแยกส่วนออกจากอินเทอร์เน็ตทั่วไป จึงเป็นเหตุให้เกิดช่องโหว่ ทั้งนี้การพัฒนาเป็นระบบดิจิทัลเป็นสิ่งสำคัญในการดำเนินงานทางธุรกิจ ซึ่งมีผลให้การที่เครือข่ายเทคโนโลยีการดำเนินงานจะเชื่อมต่อกับเครือข่ายไอทีขององค์กรเพิ่มมากขึ้น จึงเป็นการจัดเตรียมเส้นทางเพิ่มเติมสำหรับผู้เข้าโจมตี โดยเฉพาะภัยคุกคามรูปแบบใหม่เช่น บริการเกี่ยวกับอาชญากรรมไซเบอร์ (Crimeware-as-a-Service : CaaS) ที่ทำให้เครื่องมือและบริการของอาชญากรไซเบอร์อยู่ในมือของผู้ก่อเหตุที่หลากหลายยิ่งขึ้น แม้จะไม่ใช่ด้านเทคนิคก็ตาม ทุกคนสามารถกลายเป็นอาชญากรไซเบอร์ได้ด้วยการลงทุนเพียงเล็กน้อย[3]

เพื่อเกิดประสิทธิภาพและประสิทธิผลในการบรรลุวัตถุประสงค์ความมั่นคงทางไซเบอร์ และการสนับสนุนให้องค์กรประสบความสำเร็จตามเป้าหมายโดยรวมของการปฏิบัติงานหลักองค์กรนั้น องค์กรต้องมีแนวทางการออกแบบกรอบแนวทางยุทธศาสตร์ การจัดการและการพัฒนากระบวนการทำงานความมั่นคงปลอดภัยไซเบอร์เพื่อการดำเนินงานที่ต่อเนื่องและสอดคล้องกับแผนกลยุทธ์ทาง

ธุรกิจ รวมถึงมีการสร้างกระบวนการทำงาน (work processes) และการประเมินในกระบวน (in-process measure)[4] เพื่อให้เป็นไปตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ 2562 โดยเป็นข้อกำหนดการปฏิบัติตามยุทธศาสตร์ชาติ พ.ศ.2561-80 ว่าด้วยแผนแม่บทย่อย 2 การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง และแผนแม่บทย่อย 3 แผนย่อยการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคง[5] อีกทั้งยัง พ.ร.บ.ความมั่นคงไซเบอร์ฯ ยังถูกกำหนดให้เป็นแนวทางการปฏิบัติในแผนระดับ 3 และแผนเตรียมพร้อมแห่งชาติ พ.ศ. 2560-2564 ว่าด้วยยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 ที่ทุกกระทรวงต้องนำมาประยุกต์ใช้[6]

การป้องกันภัยคุกคามทางไซเบอร์ บางองค์กรจึงจัดทำแผนและนโยบายในการปรับปรุงพัฒนา แก้ไขระบบให้เป็นรุ่นที่ทันสมัยขึ้น โดยที่ไม่ให้การดำเนินการใดๆขององค์กรต้องหยุดชะงักลงไปและเพื่อชดเชยมาตรการความมั่นคงปลอดภัยที่หายไปในเวลาปรับปรุงพัฒนาดังกล่าว ฉะนั้นองค์กรจำเป็นต้องมีแนวทางปฏิบัติสอดคล้องผสมผสาน*ระหว่างแผนกลยุทธ์หลักขององค์กร (Orgnisation Strategy) กับแผนกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Strategy)* ควรเริ่มจากผู้นำขององค์กรที่จะวางแผนกลยุทธ์หรือยุทธศาสตร์ วิสัยทัศน์และธุรกรรมต่างๆขององค์กร จนถึงการประเมินความตระหนักรู้ของผู้บริหารระดับสูงตลอดจนพนักงานและองค์กรที่มีส่วนเกี่ยวข้อง[4]

ในการพิจารณาถึงข้อกำหนดตามมาตรการความมั่นคงปลอดภัยไซเบอร์ ความคาดหวังของผู้ใช้บริการและผู้มีส่วนได้เสียต่อองค์กร ตลอดจนมาตรการและนโยบายที่มีต่อผลิตภัณฑ์และบริการขององค์กรนั้น มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ (The Baldrige Cybersecurity Excellency Builder) มีความสามารถจัดการทุกส่วนขององค์กรที่เกี่ยวข้องและที่ได้รับผลกระทบจากไซเบอร์อย่างครบวงจร ซึ่งประกอบด้วยแนวทางที่เกี่ยวข้องกับระบบรักษาความมั่นคงทางไซเบอร์ในเรื่องผู้นำ แผนกลยุทธ์ ลูกค้า แรงงาน การดำเนินงานและการจัดทำวิธีจัดการความรู้ขององค์กร ตลอดจนผลลัพธ์ที่ได้รับหลังการประเมิน ซึ่งผู้ใช้กรอบแนวทางและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ จะสามารถช่วยองค์กรให้มีรูปแบบ วิธีการและกรอบแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ การจัดการความเสี่ยงและสร้างความตระหนักรู้ถึงภัยคุกคามไซเบอร์ ในภาพรวมองค์กรได้เป็นอย่างดี[4]

คำถามวิจัย

1. กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 มีลักษณะเป็นอย่างไร

2. กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 สามารถปรับใช้ได้กับแผนยุทธศาสตร์องค์การทุกระดับได้หรือไม่

3. กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 สามารถปรับใช้ได้กับองค์กรโครงสร้างพื้นฐานสำคัญทุกรูปแบบหรือไม่

วัตถุประสงค์การวิจัย

1. เพื่อศึกษากรอบความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2. เพื่อจัดทำกรอบแนวทางความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ความสอดคล้องกับความต้องการในการดำเนินธุรกิจหลักและผู้เกี่ยวข้องทุกภาคส่วนขององค์กร และตอบสนองต่อ พ.ร.บ.ความมั่นคงทางไซเบอร์ พ.ศ. 2562 (เฉพาะส่วนการยุทธศาสตร์ความมั่นคงไซเบอร์)

3. เพื่อนำเสนอกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

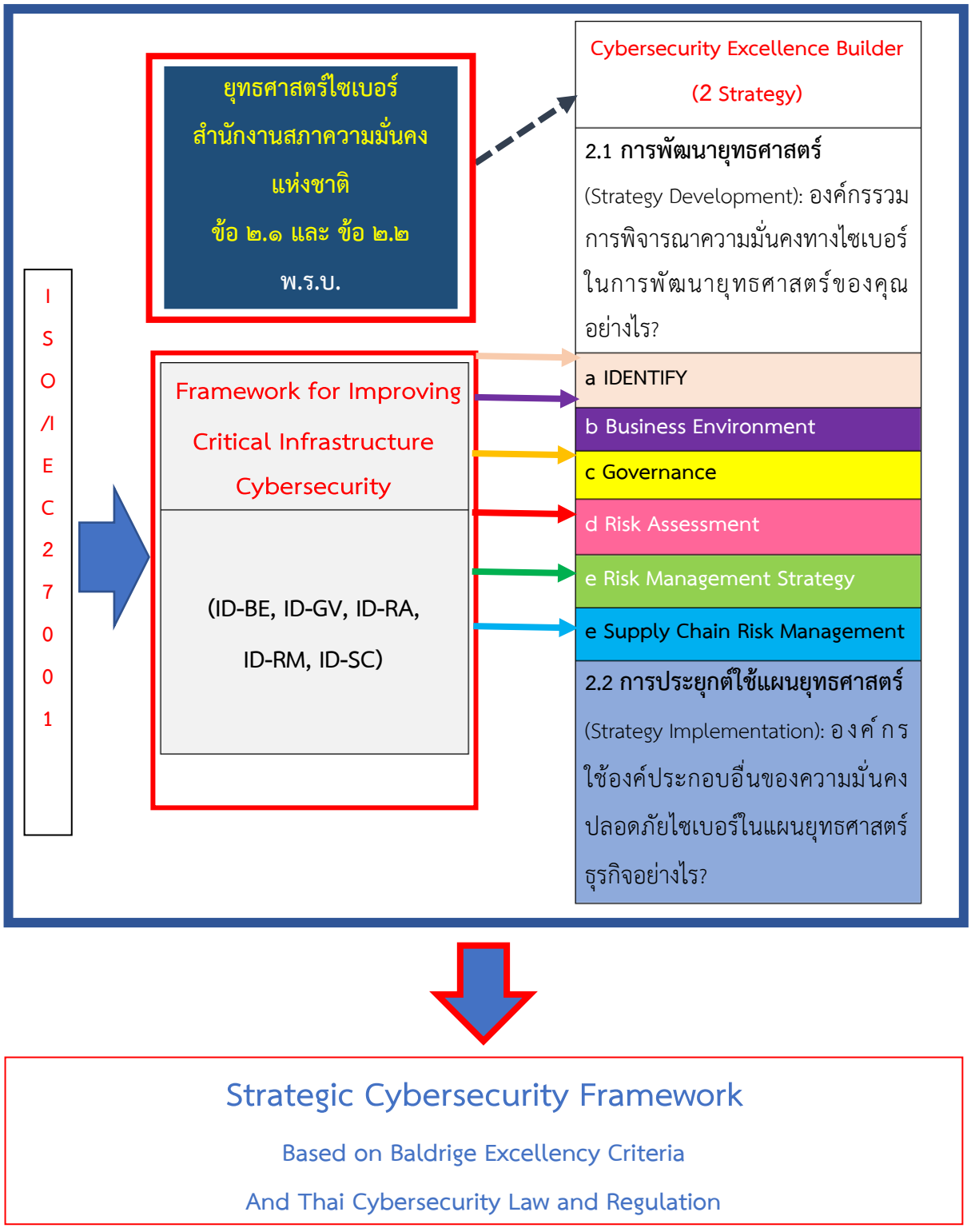
กรอบแนวคิดการวิจัย

เพื่อศึกษาความจำเป็นความมั่นคงปลอดภัยไซเบอร์ในการบริหารองค์กร นิยาม ความหมาย คำจำกัดความ ตลอดจนมาตรการในการประเมินความมั่นคงทางไซเบอร์ขององค์กรตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ รวมถึงการรวบรวมข้อมูลจากกรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์[5] ดังนี้

1. ประเภทมาตรการ (Functions) ได้แก่ และ การระบุ (Identify) การปกป้อง (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) การกู้คืน (Recover)

2. กลุ่มงานหลัก (Categories) และ กลุ่มงานย่อย (Subcategories)

3. ข้อมูลอ้างอิงการปฏิบัติ (Informative References) ตามมาตรฐาน ISO/IEC 27001 (2013)



ภาพที่ 1 แสดงกระบวนการสร้างกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

วิธีการศึกษา

1. ทบทวนวรรณกรรมที่เกี่ยวข้องกับความจำเป็นความมั่นคงปลอดภัยทางไซเบอร์และพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ 2562

2. ทบทวนวรรณกรรมที่เกี่ยวข้องวิธีการและกรอบแนวทางความมั่นคงปลอดภัยไซเบอร์

3. วิเคราะห์ข้อมูลวิธีการและนำเสนอกรอบแนวทางความมั่นคงปลอดภัยไซเบอร์

ขั้นตอนการดำเนินงาน

รายการ	2564	2565				
	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.
เสนอโครงร่างการวิจัย	←					
เก็บรวบรวมข้อมูล		←	→			
วิเคราะห์ข้อมูล				←	→	
สรุปผลและอภิปรายผล					←	→
จัดทำรูปเล่มวิจัย				←	→	

ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถประยุกต์ใช้กรอบความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง (มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ กรอบการพัฒนาโครงสร้างพื้นฐานสำคัญ ด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือ ISO/IEC 27001) และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2. สามารถวิเคราะห์และจัดทำกรอบแนวทางความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ความสอดคล้องกับความต้องการในการดำเนินธุรกิจหลักและผู้เกี่ยวข้องทุกภาคส่วนขององค์กร และตอบสนองต่อ พ.ร.บ. ความมั่นคงทางไซเบอร์ พ.ศ. 2562 (เฉพาะส่วนยุทธศาสตร์ความมั่นคงไซเบอร์)

3. สามารถประยุกต์ใช้คุณสมบัติการใช้งานของกรอบแนวฯ

บทที่ 2
บทวิเคราะห์

ในการจัดทำงานวิจัยนี้ได้นำพ.ร.บ.ไซเบอร์ ปี 2562 เป็นพื้นฐานเพื่อศึกษา นิยาม ความหมาย คำจำกัดความ ตลอดจนมาตรฐานและมาตรการสากลในการประเมินความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยใช้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของไบล์ดริจเป็นพื้นฐานในการรวบรวมและรับทราบถึงประสิทธิภาพและประสิทธิผลของมาตรการ เพื่อพัฒนาวิธีการและกรอบแนวทางความมั่นคงปลอดภัยทางไซเบอร์ใหม่ และใช้เป็นกรอบแนวทางความมั่นคงปลอดภัยทางไซเบอร์ระดับยุทธศาสตร์ขององค์กรประกอบแผนปฏิบัติราชการ ที่ตอบสนองต่อยุทธศาสตร์ไซเบอร์สำนักงานสภาความมั่นคงแห่งชาติ

2.1 การวิเคราะห์สาเหตุของปัญหาภัยคุกคามไซเบอร์

2.1.1 วิเคราะห์สิ่งแวดล้อมภายนอก (เหตุการณ์ภัยคุกคาม สถิติและวิธีโจมตีแบบใหม่)

โลกยุคโลกาภิวัตน์ที่มีเศรษฐกิจเติบโตและเทคโนโลยีที่พัฒนาอย่างรวดเร็ว ก่อให้เกิดภัยคุกคามไร้พรมแดนที่เพิ่มขึ้นต่อผู้มีบทบาทมากมายทั้งภาครัฐบาล ภาคธุรกิจ และประชาชน เป็นเหตุให้ทุกวันนี้ทุกคนอาจตกเป็นเหยื่อของอาชญากรรมไซเบอร์ โดยเฉพาะในปี 2020 การระบาดใหญ่ ของ COVID-19 บังคับให้ประเทศและธุรกิจต่างๆ ผลักดันความพยายามในการทำให้เป็นดิจิทัล และเปลี่ยนวิธีการทำงาน การเรียนรู้ การซื้อของ และการธนาคาร โดยเฉพาะอย่างยิ่ง รัฐบาลกำหนดข้อจำกัดต่างๆ ที่ระบุให้องค์กรและพนักงานต้องทำงานจากที่บ้านเป็นระยะเวลายาวนาน จึงทำให้ปริมาณและความถี่ของการทำธุรกรรมออนไลน์จึงเพิ่มขึ้น[1]

ด้วยข้อมูลที่จากประเทศสมาชิกของ INTERPOL และหน่วยงานเอกชน และการวิจัยที่จัดทำรายงานการวิเคราะห์เกี่ยวกับขอบเขตคุกคามทางไซเบอร์ในภูมิภาคอาเซียน รายงานนี้ได้ระบุถึงรูปแบบภัยคุกคามทางไซเบอร์ที่โดดเด่นมากว่าในปี 2020 และปีต่อๆ ไป: ได้แก่ การลอบเข้าควบคุมระบบโดยอีเมล์สำหรับธุรกิจ (Business E-mail Compromise (BEC)) ฟิชชิ่ง (Phishing) แรนซัมแวร์ (Ransomware) และการจรากรรมข้อมูลอีคอมเมิร์ซ (E-commerce data interception) ยังคงครองอันดับสูงสุดโดยธุรกิจที่ประสบความสูญเสียครั้งใหญ่ เนื่องจากเป็นการลงทุนที่ให้ผลตอบแทนสูงโดยมีค่าใช้จ่ายและความเสี่ยงต่ำ ซึ่งเป็นการใช้ข้อมูลที่ได้มาจากหน่วยร่วมปฏิบัติของเรา ทั้งนี้**ภัยคุกคามรูปแบบใหม่ในขณะนี้คือ บริการเกี่ยวกับอาชญากรรมไซเบอร์** (Crimeware-as-a-Service : CaaS) คือโปรแกรมคอมพิวเตอร์หรือชุดโปรแกรมที่ออกแบบมาเพื่ออำนวยความสะดวกในกิจกรรมที่ผิดกฎหมายทางออนไลน์ สปายแวร์ ชุดฟิชชิ่ง และ**การจารกรรมสกุลเงินดิจิทัล (Cryptojacking)** ยังคงถูกใช้โดยอาชญากรไซเบอร์ การเพิ่มขึ้นของราคาในสกุลเงินดิจิทัล ประกอบกับจำนวนอุปกรณ์

อินเทอร์เน็ตของสรรพสิ่ง Internet of Things (IoT) ที่เพิ่มขึ้นทุกหนทุกแห่ง ทำให้อาชญากรไซเบอร์มีรูปแบบการโจมตีที่มากขึ้น ซึ่งโปรแกรมต่างๆ[1]

2.1.2 วิเคราะห์สิ่งแวดล้อมภายใน (จุดอ่อน ช่องโหว่และความเสี่ยงขององค์กร)

จากการที่อาชญากรไซเบอร์ได้กำหนดเป้าหมายไปยังอุตสาหกรรมต่างๆ ปฏิเสธไม่ได้ว่าการโจมตีทางไซเบอร์กับโครงสร้างพื้นฐานที่สำคัญกำลังกลายเป็นรูปแบบอาชญากรรมทางไซเบอร์รูปแบบหนึ่งที่เติบโตเร็วที่สุดด้วยโครงสร้างพื้นฐานแบบโลกาภิวัตน์และจำนวนระบบควบคุมที่เชื่อมต่อและรวมศูนย์การปฏิบัติที่เพิ่มขึ้นโดยเฉพาะภาคน้ำมัน พลังงาน และอีคอมเมิร์ซ ซึ่งพวกเขาได้รับผลประโยชน์ทางการเงินมหาศาล ในปี 2020 อุตสาหกรรมการดูแลสุขภาพกลายเป็นเป้าหมายหลัก โดยอาชญากรไซเบอร์มุ่งเป้าไปที่ช่องโหว่ของระบบในโรงพยาบาล ศูนย์ดูแลสุขภาพ ผู้ผลิตวัคซีน และห้องปฏิบัติการที่ต้องการเรียกค่าไถ่ ผลกระทบของการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญไม่เพียงแต่ทำให้เกิดความสูญเสียต่อเศรษฐกิจของประเทศเท่านั้น อันที่จริงมันทำลายความเชื่อมั่นของสาธารณชนในการให้บริการที่สำคัญเช่นเดียวกับในภาครัฐบาล[1]

โดยทั่วไปองค์กรด้านโครงสร้างพื้นฐานสำคัญที่ต้องใช้ระบบควบคุมทางอุตสาหกรรม (ICS : Industrial Control Systems) ประกอบด้วย เทคโนโลยีการดำเนินงาน (OT : Operational Technology) ที่ทำงานร่วมกันกับเทคโนโลยีสารสนเทศ ซึ่งเป็นแหล่งสะสมของเทคโนโลยีสารสนเทศแบบดั้งเดิมที่เชื่อมต่อกับอินเทอร์เน็ตสาธารณะและมีการป้องกันแบบง่ายๆ ทั้งนี้ยังมีความเชื่อที่ว่าเครือข่ายเทคโนโลยีการดำเนินงาน ที่ไม่จำเป็นต้องได้รับการตรวจสอบหรือแก้ไขแต่อย่างใด เพราะจากความเชื่อเดิมว่าอุปกรณ์หรือเทคโนโลยีดังกล่าวจะถูกแยกส่วนออกจากอินเทอร์เน็ตทั่วไปหรือไม่ได้จำกัดการเข้าถึง จึงเป็นเหตุให้ช่องโหว่และเป็นการจัดเตรียมเส้นทางเพิ่มเติมสำหรับผู้เข้าโจมตี[3]โดยการวิเคราะห์เครือข่าย IoT/ICS 1,821 เครือข่ายของเราในช่วง 12 เดือนสิ้นสุดในเดือนตุลาคม 2019 ได้ผลลัพธ์ดังต่อไปนี้: [2]

- ระบบปฏิบัติการ Windows ที่ใช้งานไม่สมบูรณ์: ระบบปฏิบัติการที่ล้าสมัย 62% ของไซต์งานมีชุดระบบปฏิบัติการ Microsoft Windows ที่ล้าสมัยและไม่รองรับต่อสถานการณ์ปัจจุบัน เช่น Windows XP และ Windows 2000 ซึ่งหมายความว่าจะไม่ได้รับปรับปรุง (unpatched Windows boxes) ความมั่นคงปลอดภัยจาก Microsoft อีกต่อไป

- รหัสผ่านที่ไม่ได้เข้ารหัส (Unencrypted Passwords) 64% ของไซต์งานมีรหัสผ่านที่ไม่ได้เข้ารหัส (cleartext) ผ่านเครือข่ายของตน เหตุที่เป็นอันตรายเพราะทำให้การเข้าถึงระบบง่าย เนื่องจากรหัสผ่านเหล่านี้ถูกส่ง "โดยไม่ได้ปกปิด" และสามารถติดตาม(sniffed) ได้ง่าย อุปกรณ์รุ่นเก่าที่ไม่รองรับโปรโตคอลสมัยใหม่

- อุปกรณ์ที่สามารถเข้าถึงได้จากระยะไกลมากเกินความจำเป็น (Excessive Access: Remotely Accessible Devices) 54% ของไซต์งานมีอุปกรณ์ที่สามารถเข้าถึงได้จากระยะไกลโดยใช้โปรโตคอลมาตรฐาน เช่น RDP, SSH และ VNC หนึ่งในทิศทางการโจมตีหลักสำหรับแรนซัมแวร์คือ RDP โดยที่ผู้โจมตีจะเข้าถึงได้โดยการขโมยข้อมูลการเข้าระบบระยะไกลผ่านการโจมตีแบบฟิชชิ่ง วิศวกรรมทางสังคม (Social Engineer)

- ไม่สนใจถึงช่องว่างการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Not Minding the Gap: Direct Internet Connections) มากกว่าหนึ่งในสี่ (27%) ของไซต์ที่ถูกวิเคราะห์ว่ามีการเชื่อมต่อโดยตรงกับอินเทอร์เน็ต เช่นการใช้อินเตอร์เน็ตส่วนตัวในสถานทำงาน ทำให้เป็นเป้าหมายที่อาจเป็นเป้าหมายของมัลแวร์ การโจมตีแบบกำหนดเป้าหมาย

2.2 วิเคราะห์การนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

2.2.1 ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560–2564[5]

กรอบยุทธศาสตร์ชาติ 20 ปี นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2560–2564) แผนพัฒนาฯฉบับที่ 12 และแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม แนวคิดของนายกรัฐมนตรีที่นำเสนอในระหว่างการประชุมสุดยอดอาเซียน ประกอบกับการประเมินสถานการณ์ภัยคุกคามไซเบอร์และความพร้อมของไทย จึงได้ประมวลเป็นยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560–2564 เพื่อเป็นกรอบการดำเนินงานที่ใช้กับทุกภาคส่วน ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาชน โดยยุทธศาสตร์ไซเบอร์ สำนักงานสภาความมั่นคงแห่งชาติ มีประเด็นที่สอดคล้องกับงานวิจัย**ได้แก่ ประเด็นยุทธศาสตร์ที่ 2** ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการ ด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์ โดย**มีเป้าหมาย**ประเทศไทยมีการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้มีหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ และมีการกำหนดบทบาทและหน้าที่หน่วยงานต่าง ๆ ของรัฐอย่างชัดเจน เพื่อดูแลการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน โดยมีเนื้อหาสำคัญดังนี้[5]

ข้อ 2.1 จัดทำกรอบนโยบาย/ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560–2564 สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ และทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อปรับปรุงนโยบายให้ทันสถานการณ์ที่เปลี่ยนไป

ข้อ 2.3 จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน พร้อมจัดลำดับความสำคัญ เพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ

2.2.2 พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เพื่อกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและเอกชน ที่ต้องมีการป้องกัน รับมือ และลดความเสียงจากภัยคุกคามทางไซเบอร์ และให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ รวมถึงให้มีมาตรการป้องกัน รับมือ และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งมีเนื้อหาที่สำคัญดังนี้[6]

หมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์

สรุปในส่วนที่ 1 แผนและนโยบาย โครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศต้องได้รับการปกป้องจากภัยคุกคามทางไซเบอร์ ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมาย และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ โดย

1) มีเป้าหมายและแนวทางอย่างน้อยตาม มาตรา 42 การบูรณาการการจัดการและการประสานความร่วมมือ การสร้างมาตรการและกลไกการป้องกัน รับมือ และลดความเสี่ยง การพัฒนาบุคลากร การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ การสร้างความตระหนัก รวมถึงการพัฒนาระเบียบและกฎหมายให้ทันต่อเหตุการณ์ปัจจุบัน

2) ให้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ตาม มาตรา 44 โดยให้มีแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ แผนการรับมือภัยคุกคามทางไซเบอร์

สรุปส่วนที่ 3 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคง (1) ด้านความมั่นคงของรัฐ (2) ด้านบริการภาครัฐที่สำคัญ (3) ด้านการเงินการธนาคาร (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (5) ด้านการขนส่งและโลจิสติกส์ (6) ด้านพลังงานและสาธารณูปโภค (7) ด้านสาธารณสุข และ(8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม ซึ่งต้องมีมาตรการดังนี้

-ได้รับการตรวจสอบมาตรฐานขั้นต่ำและต้องจัดการประเมินพร้อมรายงานผลเรื่องความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานหน่วยงานที่ควบคุมและกำกับดูแล และมีการกำหนดให้มีกลไกหรือ

ขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน

2.3 การวิเคราะห์ความจำเป็นและทางเลือกการแก้ไขปัญหา

2.3.1 จากภัยคุกคามรูปแบบใหม่และช่องโหว่ของหน่วยงานที่มาจากการปฏิบัติ ทำให้เกิดความเสี่ยงทางความมั่นคงปลอดภัยไซเบอร์ เป็นผลให้หลายๆหน่วยงานมีจัดทำยุทธศาสตร์ การวางแผนพัฒนาระบบ อุปกรณ์ ซึ่งหน่วยงานต้องเผชิญกับปัญหาระหว่างการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต้องหยุดชะงักลงหรือขาดความสามารถชดเชยมาตรการความมั่นคงปลอดภัยที่หายไปในเวลาปรับปรุงพัฒนาได้ โดยมีที่มาของปัญหาคือการขาดแนวทางยุทธศาสตร์รักษาความมั่นคงปลอดภัยไซเบอร์ ตั้งแต่เริ่มทำแผนนโยบายบริหารองค์กร (โดยเฉพาะองค์กรโครงสร้างพื้นฐานสำคัญ ซึ่งมีหลายประเภทตามลักษณะงานและมีโครงสร้างองค์กรตามคุณลักษณะและภารกิจ รวมถึงทุก ๆ องค์กรจะมีปัญหาและความต้องการความมั่นคงปลอดภัยไซเบอร์ที่แตกต่าง

2.3.2 ต้นเหตุการหยุดชะงักของระบบป้องกันภัยคุกคามทางไซเบอร์และการปฏิบัติงานหลักขององค์กร ส่วนใหญ่มีสาเหตุมาจาก ปัญหาความไม่สอดคล้องของยุทธศาสตร์ขององค์กร ซึ่งต้องการกรอบแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity strategy) ที่สอดคล้องกับยุทธศาสตร์ทางธุรกิจ (Business strategy) และต้องการความสอดคล้องทั่วถึงทุกภาคส่วนที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ เช่น ผู้บริหาร หน่วยร่วมปฏิบัติ ซึ่งจะช่วยทำให้ระบบลดการหยุดชะงักลงไปและชดเชยมาตรการความมั่นคงปลอดภัยที่หายไปในเวลาปรับปรุงพัฒนา

2.3.3 ปัญหาการกำหนดขั้นตอนการดำเนินงานทางยุทธศาสตร์ หน่วยงานต้องการกรอบแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ที่อธิบายการปฏิบัติตั้งแต่เริ่มต้นการวิเคราะห์ปัญหา และต้องสามารถใช้ประเมินความสำเร็จตามที่ พ.ร.บ. ฯ กำหนดได้ ซึ่ง Cybersecurity Framework อื่นๆ เช่น CIS CSC, COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013 และ NIST SP 800-53 ไม่ได้กล่าวถึงทุกภาคส่วนนั้น

2.3.4 **การแก้ปัญหา** พ.ร.บ.ไซเบอร์ฯ ถูกจัดทำขึ้นหลังการจัดทำยุทธศาสต์ไซเบอร์ สมช. ซึ่งเป็นจุดเชื่อมโยงที่บังคับให้หน่วยงานที่เกี่ยวข้องปฏิบัติตามข้อกำหนดตามกฎหมาย ทำให้เกิดแนวทางการดำเนินงานตาม**ประเด็นยุทธศาสตร์ที่ 2** ปกป้องโครงสร้างพื้นฐานสำคัญฯ แต่ยังขาดความเชื่อมโยงไปสู่องค์กรระดับกระทรวง เพื่อกำหนดความสอดคล้องและขั้นตอนการดำเนินงานทางยุทธศาสตร์ ไปสู่การปฏิบัติองค์ประกอบที่สำคัญของปัญหาตามข้อ (2.3.1) และจะเห็นได้ว่างานวิจัยนี้สามารถใช้เป็นแนวทางดำเนินงานสำหรับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหาข้อ (2.3.2)-(2.3.3)

2.3.5 การพิจารณาทางเลือกการแก้ไขปัญหา มาตรฐานความมั่นคงปลอดภัยไซเบอร์ ความคาดหวังของผู้ใช้บริการและผู้มีส่วนได้เสียต่อองค์กร ตลอดจนมาตรการและนโยบายที่มีต่อผลิตภัณฑ์ และบริการขององค์กรนั้น มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ มีความสามารถจัดการทุกส่วนขององค์กรที่เกี่ยวข้อง และที่ได้รับผลกระทบอย่างครบวงจร ซึ่งประกอบด้วยแนวทางที่เกี่ยวข้องกับระบบรักษาความมั่นคงทางไซเบอร์ ซึ่งผู้ใช้กรอบแนวทางและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ จะสามารถช่วยองค์กรให้มีรูปแบบ แนวทางการจัดการและสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ในภาพรวมองค์กรเพื่อแก้ไขปัญหาข้อ 2.3.4 ได้เป็นอย่างดี

2.4 มาตรฐานวิธีการและกรอบแนวทางความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ

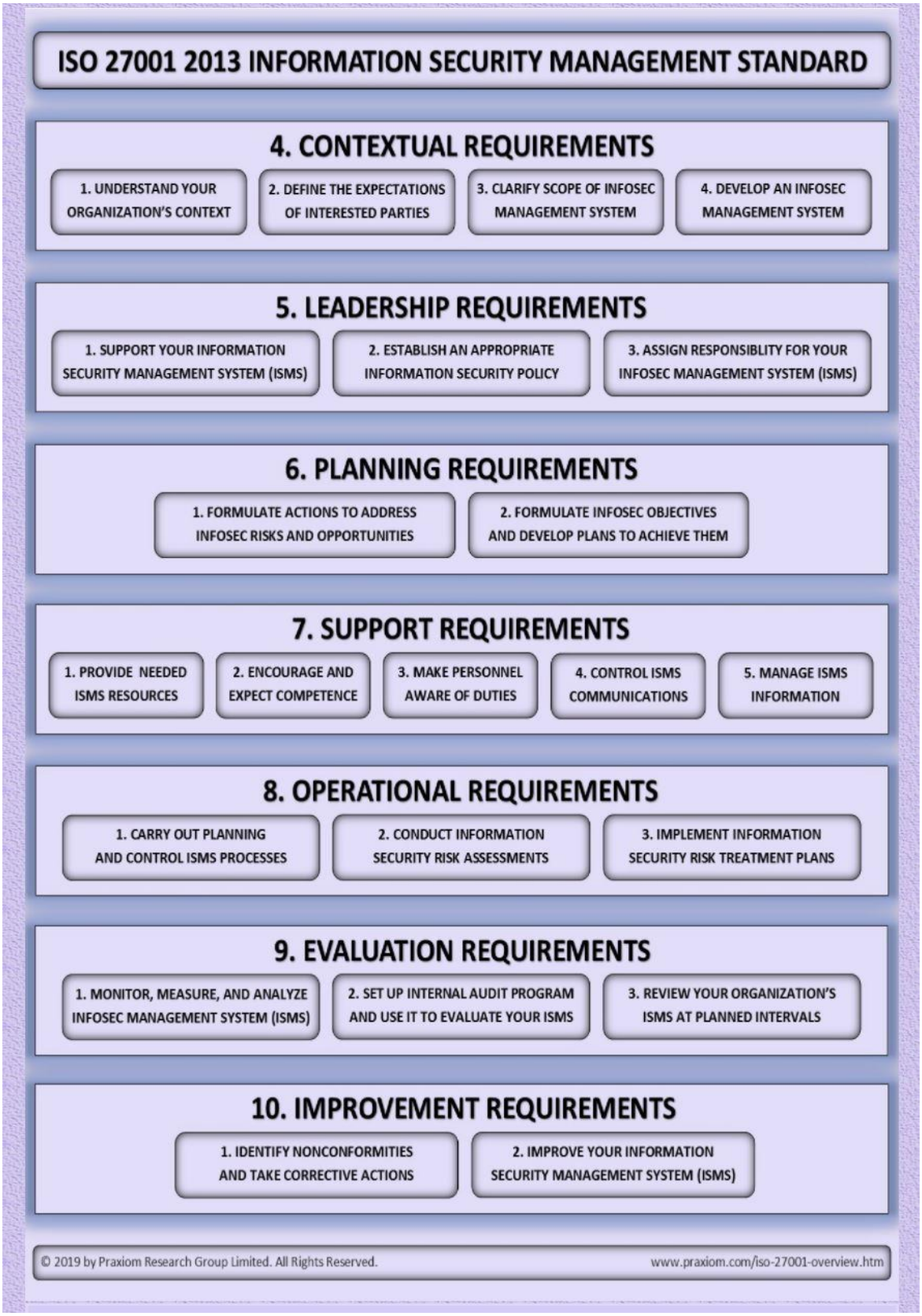
2.4.1 มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Standard) หรือ ISO/IEC 27001:2013 [7]

การจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรนั้นได้รับอิทธิพลจากความต้องการและวัตถุประสงค์ขององค์กร, ข้อกำหนดด้านความปลอดภัย, กระบวนการขององค์กร รวมถึงขนาดและโครงสร้างขององค์กร ปัจจัยเหล่านี้สามารถเปลี่ยนแปลงได้ตลอดเวลาและนำมาซึ่งจุดอ่อนและช่องโหว่แก่ความมั่นคงปลอดภัยสารสนเทศในการรักษาความลับของข้อมูล (CONFIDENTIALITY) ความสมบูรณ์ถูกต้องของข้อมูล (INTEGRITY) และการดำรงความความพร้อมใช้ของข้อมูลและระบบ (AVAILABILITY) จึงมีความจำเป็นต้องใช้กระบวนการบริหารความเสี่ยงและสร้างความมั่นใจแก่ผู้มีส่วนได้เสียว่ามีการจัดการความเสี่ยงอย่างเพียงพอในหลักการ

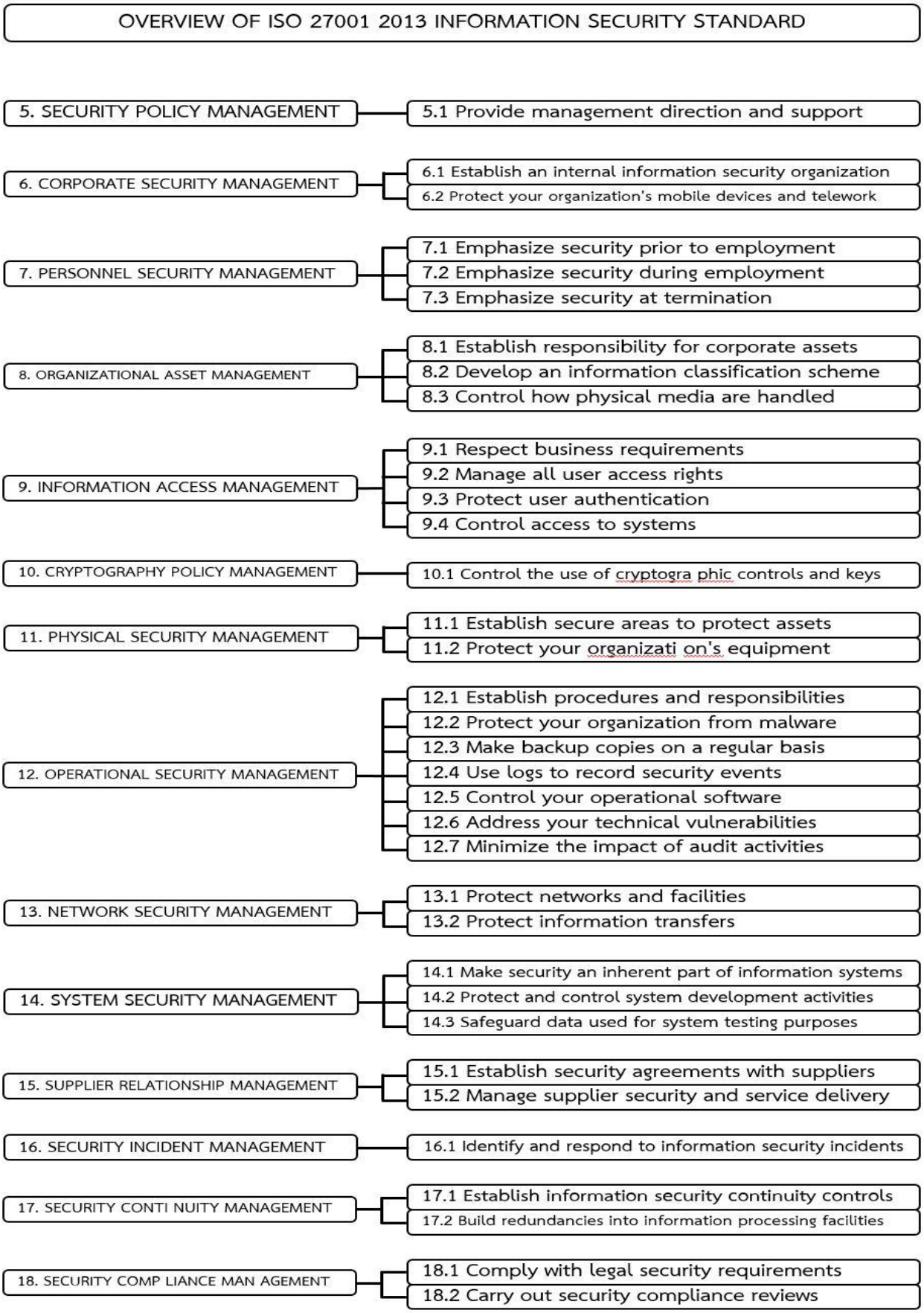
มาตรฐาน ISO/IEC 27001:จัดทำขึ้นเพื่อให้ข้อกำหนดสำหรับการดำเนิน การซ่อมบำรุงและการปรับปรุงระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ และสามารถประยุกต์ใช้ระบบการจัดการมั่นคงปลอดภัยสารสนเทศสำหรับการตัดสินใจเชิงกลยุทธ์สำหรับองค์กร ซึ่งปัจจุบันประกาศเป็น มาตรฐาน ISO/IEC 27001:2013 ซึ่งประกอบด้วย 2 ส่วน คือ (1) ข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (2) มาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ สามารถแบ่งเนื้อหาข้อกำหนดดังนี้

- ส่วนที่ 1 ข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Requirements: IMSR) โดยมี Clauses 4 to 10

- ส่วนที่ 2 มาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Information Security Controls) โดยข้อกำหนดในส่วนนี้ มุ่งเน้นไปที่การควบคุมความมั่นคง ปลอดภัยสารสนเทศ ซึ่งมีมาตรการควบคุมแบ่งออกเป็น 14 ส่วน แสดงไว้ในภาคผนวก A (Annex A)



ภาพที่ 2 แสดงส่วนที่ 1 ข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Requirements: IMSR)



ส่วนที่ 3 มาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Information Security Controls)

2.4.2 มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ (The Baldrige Cybersecurity Excellency Builder)[4]

เป็นมาตรฐานที่ได้การรรับรองจาก National Institute of Standards and Technology : NIST มีจุดเด่นในการประเมินผ่านชุดของคำถามปลายเปิด การใช้การประเมินนี้สามารถอำนวยความสะดวกในการประเมินที่สร้างความเข้าใจนโยบายและการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรโดยคำนึงถึงคุณลักษณะและสถานการณ์ทางยุทธศาสตร์การดำเนินธุรกิจหลักควบคู่กันไปและจัดการทุกพื้นที่ที่ได้รับผลกระทบจากไซเบอร์อย่างครบวงจร ดังที่แสดงในแผนภาพซึ่งระบบประกอบด้วยแนวทางที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยไซเบอร์ได้แก่

บริบทขององค์กร (Organizational Context) ความเข้าใจอย่างชัดเจนเกี่ยวกับองค์กร

ผู้นำ (Leadership) การดำเนินการของผู้นำทางปฏิบัติการและผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ มีการกำกับดูแล แสดงเป็นตัวอย่าง ให้คำแนะนำ รักษานโยบายและการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์องค์กร (Strategy) การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต้องมีการวางแผนและการประยุกต์ใช้ที่ชัดเจนและมีประสิทธิภาพ โดยเฉพาะการประยุกต์ใช้กับเหตุฉุกเฉิน และมีทรัพยากรจำกัด

ผู้ใช้บริการ/ลูกค้า (Customers) คือผู้ตัดสินคุณภาพของผลิตภัณฑ์และบริการขององค์กร ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจมีผลกระทบต่อความพึงพอใจของผู้ใช้บริการ ควบคู่กับความสะดวกสบายและรูปแบบการเข้าถึงของผู้ใช้บริการ

การประเมิน การวิเคราะห์และการจัดการความรู้ (Measurement, Analysis, and Knowledge Management) การประเมินและวิเคราะห์ ว่าองค์กรมีประสิทธิภาพในชุดมาตรการที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการคัดเลือกอย่างครบถ้วนหรือไม่ ช่วยให้คุณตัดสินใจได้อย่างไรในการปรับปรุงประสิทธิภาพความมั่นคงทางไซเบอร์

ผู้ปฏิบัติงาน (Workforce) ผู้ปฏิบัติงานในหน่วยปฏิบัติหลัก และ**ผู้ปฏิบัติงาน**ที่เกี่ยวข้องโดยตรงกับการปฏิบัติงานความมั่นคงปลอดภัยไซเบอร์ มีความเข้าใจในทิศทางขององค์กรที่ชัดเจน มีโอกาสในการเรียนรู้และความรับผิดชอบต่อผลการปฏิบัติขององค์กร

การดำเนินงาน (Operations) การออกแบบ การจัดการและการพัฒนาการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์เพื่อประสิทธิภาพและประสิทธิผล

ผลการประเมิน (Results) ผลการประเมิน ให้ข้อมูลและข้อเท็จจริง ของการประเมินความคืบหน้า ในพัฒนาการประเมินและสร้างความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง นโยบายและการดำเนินงานให้สอดคล้องกันโดยมีตัวแปรที่ใช้ในการประเมินได้แก่ วิธีการ(Approach) การประยุกต์ใช้

(Deployment) การเรียนรู้ขององค์กร (Learning) และการบูรณาการกระบวนการที่เกี่ยวข้อง (Integration)

รูปที่ 4 แสดงองค์ประกอบที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยไซเบอร์

2.4.1 ขั้นตอนการจัดทำการประเมินและปรับปรุงการจัดการความเสี่ยงทางไซเบอร์ขององค์กร ตามกรอบความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ

1 การกำหนดขอบเขต ให้กำหนดขอบเขตการประเมินให้ชัดเจน

2.บริบทขององค์กร โดยระบุข้อมูลสำคัญ ใช้เป็นแบบประเมินเบื้องต้น

3 คำถามเกี่ยวกับกระบวนการ ทั้งนี้ในการวิจัยจะใช้เฉพาะ ข้อ 2 ยุทธศาสตร์องค์กร และตาม**เครื่องมือสำหรับภาคปฏิบัติ (Crosswalk)** และข้อ 3.2 ของ กรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ V.1.1_April18 เรื่องการจัดตั้งหรือปรับปรุงโปรแกรมความปลอดภัยทางไซเบอร์ ซึ่งขั้นตอนต่อไปนี้แสดงให้เห็นว่าองค์กรสามารถใช้ Framework **<u>เพื่อสร้างรายการความปลอดภัยทางไซเบอร์ใหม่</u>**

ขั้นตอนที่ 1: การจัดลำดับความสำคัญและขอบเขต (Prioritize and Scope)

ขั้นตอนที่ 2: การทำความเข้าใจ (Orient) ระบุระบบและสินทรัพย์ ข้อกำหนดด้านกฎระเบียบ และแนวทางความเสี่ยงโดยรวม

ขั้นตอนที่ 3: การสร้างผลประเมินปัจจุบัน (Create a Current Profile)

ขั้นตอนที่ 4: การดำเนินการประเมินความเสี่ยง (Conduct a Risk Assessment)

ขั้นตอนที่ 5: สร้างโปรไฟล์เป้าหมาย (Create a Target Profile) ผลลัพธ์เป้าหมาย

ขั้นตอนที่ 6: กำหนด วิเคราะห์ และจัดลำดับความสำคัญของช่องโหว่ (Determine, Analyze, and Prioritize Gaps)

ขั้นตอนที่ 7: ดำเนินการตามแผนปฏิบัติการ (Implement Action Plan)

Crosswalk: Baldrige Cybersecurity Excellence Builder and Cybersecurity Framework

Cybersecurity Excellence Builder Categories and Items	Related Sections in the *Cybersecurity Framework*		
	2.4, Figure 2: Notional Information and Decision Flows	3.2, Establishing or Improving a Cybersecurity Program	Appendix A: Framework Core Functions and Categories[1]
C Organizational Context			
C.1 Organizational Description	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-AM, ID-BE, ID-SC
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, ID-RM
2 Strategy			
2.1 Strategy Development	Business/Process Level;Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope. Step 2: Orient. Step 4: Conduct a Risk Assessment. Step 5: Create a Target Profile; Step 6: Determine, Analyze, and Prioritize Gaps	ID-BE, ID-GV, ID-RA, ID-RM, ID-SC
2.2 Strategy Implementation	Business/Process Level;Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope. Step 2: Orient. Step 5: Create a Target Profile. Step 7: Implement Action Plan	ID-BE, ID-GV, ID-RA, ID-RM

ภาพที่ 5 แสดงวิธีการจัดทำขั้นตอนการจัดทำการประเมินและปรับปรุงการจัดการ ตามกรอบความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ (กรอบสีเหลือง)

2.4.2 ขั้นตอนการประเมินระดับการตอบสนอง โดยใช้กระบวนการและผลการประเมิน ได้กำหนดคำอธิบาย (องค์กรขั้นเริ่มต้น (Reactive), องค์กรที่มีการเตรียมตัว (Early), องค์กรกำลังพัฒนา (Developing), องค์กรแห่งความพร้อม (Mature), องค์กรชั้นนำ (Leading), องค์กรตัวอย่าง (Exemplary)) ในการตอบสนองต่อสถานการณ์ความมั่นคงทางไซเบอร์แต่ละครั้ง

2.5 วิเคราะห์ข้อมูลการสร้างกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

คำถามเกี่ยวกับกระบวนการ ทั้งนี้ในการวิจัยจะใช้เฉพาะ ข้อ 2 ยุทธศาสตร์องค์กร และตามเครื่องมือสำหรับภาคปฏิบัติ (Crosswalk) และข้อ 3.2 ของ กรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ V.1.1_April18 เรื่องการจัดตั้งหรือปรับปรุงโปรแกรมความปลอดภัยทางไซเบอร์ ซึ่งขั้นตอนต่อไปนี้แสดงให้เห็นว่าองค์กรสามารถใช้ Framework เพื่อสร้างรายการความปลอดภัยทางไซเบอร์ใหม่

<table>
<tr><th colspan="4">ขั้นตอนการวิเคราะห์</th></tr>
<tr><td>Cybersecurity Excellence Builder
Categories and Items</td><td>Framework for Improving
Critical Infrastructure Cybersecurity</td><td>พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒</td><td>ยุทธศาสตร์ไซเบอร์ สำนักงานสภาความมั่นคงแห่งชาติ</td></tr>
<tr><td>2 แผนยุทธศาสตร์ (Strategy)</td><td rowspan="2">(ID-BE, ID-GV, ID-RA, ID-RM, ID-SC)</td><td rowspan="3">ส่วนที่ 1, 3 พ.ร.บ.ฯ</td><td rowspan="2">ข้อ ๒.๑ <u>จัดทำกรอบนโยบาย/ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔</u></td></tr>
<tr><td>2.1 การพัฒนายุทธศาสตร์ (Strategy Development) : องค์กรรวมการพิจารณาความมั่นคงทางไซเบอร์ในการพัฒนายุทธศาสตร์ของคุณอย่างไร?</td></tr>
<tr><td>2.2 การใช้แผนกลยุทธ์(Strategy Implementation): องค์กรใช้องค์ประกอบอื่นของความมั่นคงปลอดภัยไซเบอร์ในแผนยุทธศาสตร์ธุรกิจอย่างไร</td><td>(ID-BE, ID-GV, ID-RA, ID-RM)</td><td>ข้อ ๒.๓ <u>จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน</u></td></tr>
</table>

ภาพที่ 6 อธิบายตัวอย่างการจัดลำดับและขั้นตอนการจัดทำกรอบแนวทางฯ

2.5.1 ขั้นตอนการตอบ**<u>คำถามการประเมินข้อที่ 2.แผนยุทธศาสตร์ แผนกลยุทธ์</u>** (Strategy) การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต้องการความชัดเจนและความเข้มแข็งในการวางแผน โดยเฉพาะอย่างยิ่งการปรับใช้แผนตามสถานการณ์อันมีทรัพยากรที่จำกัด

2.5.1.1 คำถามข้อ 2.1 การพัฒนายุทธศาสตร์ (Strategy Development): คุณจะรวมการพิจารณาความมั่นคงทางไซเบอร์ในการพัฒนา**<u>แผนยุทธศาสตร์</u>** อย่างไร?

<u>หมายเหตุ</u> การพัฒนายุทธศาสตร์หมายรวมถึงแนวทางขององค์กรในการเตรียมพร้อมสำหรับอนาคต รายการคำถามชุดที่ 2 นี้ถามถึงการวางแผนยุทธศาสตร์ขององค์กรที่จะพิจารณา

ความต้องการความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้สอดคล้องกับแผนยุทธศาสตร์ธุรกิจหลักในภาพรวมขององค์กรควบคู่กัน

ในการพัฒนากลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์นั้น องค์กรควรพิจารณาระดับความเสี่ยงขององค์กรที่ยอมรับได้ ซึ่งตามความเหมาะสมแล้ว องค์กรต้องพิจารณารวมถึง ส่วนสนับสนุนต่างๆ เช่น หน่วยสับสนุนและหน่วยร่วมปฏิบัติ ที่มีส่วนร่วมในการดำเนินการความปลอดภัยทางไซเบอร์ขององค์กร ได้แก่ (1) รวมการวางแผนความมั่นคงปลอดภัยไซเบอร์กับกระบวนการวางแผนกลยุทธ์ขององค์กร (2) ทำให้มั่นใจว่า การเรียบเรียงแผนเพื่อความมั่นคงปลอดภัยไซเบอร์เข้ากับแผนยุทธศาสตร์โดยรวมขององค์กร (3) กระบวนการพัฒนายุทธศาสตร์ถูกรวมเข้ากับนโยบายใหม่และการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (4) รวบรวม วิเคราะห์ข้อมูลที่เกี่ยวข้อง และพัฒนาข้อมูลเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์สำหรับกระบวนการวางแผนยุทธศาสตร์ (5) ประเมินกระบวนการใดด้านความมั่นคงปลอดภัยไซเบอร์ที่จะสำเร็จได้โดยพนักงานและกระบวนการใดจะสำเร็จได้โดยผู้สนับสนุนหรือคู่ค้า (6) อะไรคือเป้าหมายเชิงกลยุทธ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดเวลาในการบรรลุเป้าหมายนั้น (7) วัตถุประสงค์เชิงยุทธศาสตร์ของความมั่นคงปลอดภัยไซเบอร์ที่สำคัญขององค์กรสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์โดยรวมขององค์กรอย่างไร (8) องค์กรบรรลุผลเป้าหมายแผนยุทธศาสตร์ด้านความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยสับสนุน หน่วยร่วมปฏิบัติ ผู้มีส่วนได้ส่วนเสียและวัตถุประสงค์ได้อย่างไร?

2.5.1.2 คำถามข้อ 2.2 การประยุกต์ใช้แผนกลยุทธ์ (Strategy Implementation): หมายรวมถึงการใช้องค์ประกอบอื่นของความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในแผนยุทธศาสตร์อย่างไร? เช่น (1) ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับแผนปฏิบัติการหลักในระยะสั้นและระยะยาว? (2) การประยุกต์ใช้ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับแผนปฏิบัติการอย่างไร (3) องค์กรมั่นใจได้อย่างไรว่าทรัพยากรทางการเงินและทรัพยากรอื่น ๆ พร้อมที่จะสนับสนุนให้องค์กรการบรรลุความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับแผนปฏิบัติการ ในขณะที่คุณปฏิบัติตามข้อผูกพันในปัจจุบัน? (4) กำลังพลหลักขององค์กรมีแผนสนับสนุนเป้าหมายความมั่นคงปลอดภัยไซเบอร์ระยะสั้นและระยะยาว ด้านแผนยุทธศาสตร์และแผนการปฏิบัติงานขององค์กรอย่างไร? (5) องค์กรใช้มาตรการหรือตัวชี้วัดใด ในการติดตามผลสัมฤทธิ์และประสิทธิภาพของความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับแผนปฏิบัติการ? (6) มาตรการหรือตัวชี้วัดตามข้อ 5 นั้น องค์กรคาดการณ์และประมาณการณ์ว่าจะได้ผลลัพท์ ด้านประสิทธิภาพในการวางแผนระยะสั้นและระยะยาวในรูปแบบใด? (7) องค์กรจัดทำและประยุกต์ใช้ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับแผนปฏิบัติการได้อย่างไร หากสถานการณ์ต้องการการปรับระดับแผนงาน (shift in plans) และการปฏิบัติตามแผนใหม่อย่างเร่งด่วน

2.5.2 ขั้นตอนการสร้างกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

2.5.2.1 การพัฒนายุทธศาสตร์ (Strategy Development) ตามข้อ 3.2 ของกรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ V.1.1_April18 มีการดำเนินการตามกลุ่มงานหลักคือ การระบุ (ID) และมีกลุ่มงานย่อยได้แก่ ID-BE, ID-GV,ID-RA, ID-RM, ID-SC ซึ่งจะอธิบายแต่ละขั้นตอนต่อไป

ขั้นตอนที่ 1: การจัดลำดับความสำคัญและขอบเขต (Prioritize and Scope)

- Risk Management Strategy (ID.RM): ลำดับความสำคัญขององค์กร ข้อจำกัด ความเสี่ยงที่ยอมรับได้ และข้อสมมติขององค์กรได้รับการกำหนดและใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ

- Supply Chain Risk Management (ID.SC): ลำดับความสำคัญ ข้อจำกัด การยอมรับความเสี่ยง และข้อสมมุติฐานขององค์กร เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในห่วงโซ่อุปทาน และการองค์กรได้กำหนดและประยุกต์ใช้กระบวนการเพื่อระบุ ประเมิน และจัดการความเสี่ยงในห่วงโซ่อุปทาน

ขั้นตอนที่ 2: การทำความเข้าใจ (Orient)

- Business Environment (ID.BE): การทำความเข้าใจและจัดลำดับความสำคัญ พันธกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสีย และกิจกรรมขององค์กร เพื่อแจ้งบทบาทหน้าที่ความรับผิดชอบและการตัดสินใจในการจัดการความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

- Governance (ID-GV): การทำความเข้าใจ นโยบาย ,ขั้นตอน, กระบวนการในการจัดการและติดตามข้อกำหนดขององค์กร ,กฎหมาย ความเสี่ยง, สิ่งแวดล้อม และข้อกำหนดในการดำเนินงานและแจ้งเตือนถึงการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ขั้นตอนที่ 4: การดำเนินการประเมินความเสี่ยง (Conduct a Risk Assessment)

ID-RA, Risk Assessment (ID.RA): องค์กรเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร และบุคคล (รวมถึงความเสี่ยงทาง ภารกิจ หน้าที่ ภาพลักษณ์ หรือชื่อเสียง)

ขั้นตอนที่ 5: สร้างโปรไฟล์เป้าหมาย (Create a Target Profile) องค์กรกำหนดเอง

ขั้นตอนที่ 6: กำหนด วิเคราะห์ และจัดลำดับความสำคัญของช่องโหว่ (Determine, Analyze, and Prioritize Gaps) องค์กรกำหนดเอง ตามผลการประเมิน

2.5.2.2 ขั้นตอนการการประยุกต์ใช้แผนกลยุทธ์ (Strategy Implementation): ตามข้อ 3.2 ของ กรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์

V.1.1_April18 มี การดำเนินการตามกลุ่มงานหลักคือ การระบุ (ID) และมีกลุ่มงานย่อยได้แก่ ID-BE, ID-GV, ID-RA และ ID-RM ซึ่งจะอธิบายแต่ละขั้นตอนต่อไป

ขั้นตอนที่ 1: การจัดลำดับความสำคัญและขอบเขต (Prioritize and Scope)

- Risk Management Strategy (ID.RM): ลำดับความสำคัญขององค์กร ข้อจำกัด ความเสี่ยงที่ยอมรับได้ และข้อสมมติขององค์กรได้รับการกำหนดและใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ

- Governance (ID-GV): นโยบาย ,ขั้นตอน, กระบวนการในการจัดการและติดตามข้อกำหนดขององค์กร ,กฎหมาย ความเสี่ยง, สิ่งแวดล้อม และข้อกำหนดในการดำเนินงาน เป็นที่เข้าใจและเป็นเรื่องแจ้งเตือนถึงการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ขั้นตอนที่ 2: การทำความเข้าใจ (Orient)

-Business Environment (ID.BE): การทำความเข้าใจและจัดลำดับความสำคัญ พันธกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสีย และกิจกรรมขององค์กร เพื่อแจ้งบทบาทหน้าที่ความรับผิดชอบและการตัดสินใจในการจัดการความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

-ID-RA, Risk Assessment (ID.RA): องค์กรเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร และบุคคล (รวมถึงความเสี่ยงทาง ภารกิจ หน้าที่ ภาพลักษณ์ หรือชื่อเสียง)

ขั้นตอนที่ 5: สร้างโปรไฟล์เป้าหมาย(Create a Target Profile) ตาม Assessment Rubric

ขั้นตอนที่ 7: ดำเนินการตามแผนปฏิบัติการ (Implement Action Plan)

2.6 การจัดทำกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

ประกอบด้วย 1 ฟังชั่นคือการ ระบุ (Identify : ID) มีกลุ่มงานหลักและกลุ่มงานย่อย รวมถึงการปฏิบัติตาม iso 27001 ดังนี้

1 **Business Environment (ID.BE):** การทำความเข้าใจและจัดลำดับความสำคัญ พันธกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสีย และกิจกรรมขององค์กร เพื่อแจ้งบทบาทหน้าที่ความรับผิดชอบและการตัดสินใจในการจัดการความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

ID.BE-1**:** ระบุบทบาทขององค์กรในห่วงโซ่อุปทาน และสื่อสารไปสู่ทุกส่วนที่เกี่ยวข้อง (ข้อมูลอ้างอิงตาม iso 27001 ได้แก่ A.15.1.1**,** A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

ID.BE-2: ระบุสถานที่ในโครงสร้างพื้นฐานที่สำคัญและภาคอุตสาหกรรม และทำความเข้าใจกับทุกส่วนที่เกี่ยวข้อง (ข้อมูลอ้างอิงตาม iso 27001 ได้แก่ Clause 4.1

ID.BE-3: จัดทำลำดับความสำคัญของภารกิจ วัตถุประสงค์ และกิจกรรมขององค์กรและได้รับการเผยแพร่ให้เข้าใจทั่วกัน ใช้มาตรฐาน NIST SP 800-53 Rev. 4 PM-11, SA-14 เนื่องจากไม่

มีระบุไว้ใน iso 27001

PM-11 ภารกิจและการกำหนดกระบวนการทางธุรกิจ โดย **a.** กำหนดภารกิจขององค์กรและกระบวนการทางธุรกิจโดยคำนึงถึงความมั่นคงปลอดภัยข้อมูลและความเป็นส่วนตัว รวมถึงความเสี่ยงที่มีผลต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร บุคคล องค์กรอื่นๆ และประเทศชาติ **b.** กำหนดการปกป้องข้อมูลและความต้องการการประมวลผลข้อมูลระบุตัวบุคคล ซึ่งเกิดจากภารกิจที่กำหนดไว้และกระบวนการทางธุรกิจ และ **c**. ทบทวนและแก้ไขภารกิจและกระบวนการทางธุรกิจเป็นระยะๆ จนกว่าจะได้รับการคุ้มครองและการประมวลผลข้อมูลระบุตัวบุคคล

SA-14 การวิเคราะห์ที่สำคัญ (**CRITICALITY ANALYSIS**) ระบุส่วนประกอบและหน้าที่ของระบบที่สำคัญโดยทำการวิเคราะห์สำคัญสำหรับ ระบบที่กำหนดโดยองค์กร ส่วนประกอบของระบบ หรือบริการของระบบ ที่การตัดสินใจที่กำหนดโดยองค์กรในวงจรชีวิตการพัฒนาระบบ

ID.BE-4: สร้างระบบสำรองและฟังก์ชั่น สำหรับการให้บริการที่สำคัญ (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.11.2.2, A.11.2.3, A.12.1.3**)

ID.BE-5: จัดทำข้อกำหนดให้ความอ่อนตัวสำหรับการปฏิบัติงานทั้งหมด เพื่อรองรับการให้บริการที่สำคัญ (เช่น ภายใต้การบังคับ/การโจมตี ระหว่างการกู้คืน การดำเนินการปกติ) (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1**)

2 **Governance:** (**ID-GV**) การทำความเข้าใจ นโยบาย **,**ขั้นตอน**,** กระบวนการในการจัดการและติดตามข้อกำหนดขององค์กร **,**กฎหมาย, ความเสี่ยง**,** สิ่งแวดล้อม และข้อกำหนดในการดำเนินงานและแจ้งเตือนถึงการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ID.GV-1: จัดตั้งและสื่อสารนโยบายความมั่นปลอดภัยทางไซเบอร์ขององค์กร (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.5.1.1**

ID.GV-2: การประสานงานบทบาทและความรับผิดชอบด้านความปลอดภัยทางไซเบอร์ ให้สอดคล้องกับบทบาทผู้มีส่วนเกี่ยวข้องทั้งภายในและภายนอก (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.6.1.1, A.7.2.1, A.15.1.1**)

ID.GV-3: ทำความเข้าใจและจัดการ ข้อกำหนดทางกฎหมายและข้อบังคับเกี่ยวกับความมั่นปลอดภัยทางไซเบอร์ รวมถึงความเป็นส่วนตัวและภาระผูกพันด้านความเสรีในการใช้งาน (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5**

ID.GV-4: กระบวนการกำกับดูแลและการจัดการความเสี่ยงจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **Clause 6** การวางแผน (**Planning)**
3 **Risk Assessment (ID.RA):** องค์กรเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กร และบุคคล (รวมถึงความเสี่ยงทาง ภารกิจ หน้าที่ ภาพลักษณ์ หรือชื่อเสียง)

ID.RA-1: ระบุถึงช่องโหว่ของสินทรัพย์ และจัดทำเป็นเอกสาร ((ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.12.6.1, A.18.2.3**)

ID.RA-2: ได้รับการกระจายข้อมูลข่าวสารภัยคุกคามทางไซเบอร์จากกลุ่มเคลื่อข่ายและแหล่งข่าว (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.6.1.4**)

ID.RA-3: ระบุและจัดทำเอกสาร ภัยคุกคามทั้งภายในและภายนอก (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **Clause 6.1.2**)

ID.RA-4: ระบุผลกระทบและโอกาสทางธุรกิจที่อาจเกิดขึ้น (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.16.1.6, Clause 6.1.2**)

ID.RA-5: ภัยคุกคาม ความเปราะบาง โอกาส และผลกระทบ ที่ต้องใช้เพื่อกำหนดความเสี่ยง (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.12.6.1**)

ID.RA-6: **Risk responses are identified and prioritized** (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **Clause 6.1.3**)

4 **ID-RM Risk Management Strategy (ID.RM):**ลำดับความสำคัญขององค์กร ข้อจำกัด ความเสี่ยงที่ยอมรับได้ และข้อสมมติขององค์กรได้รับการกำหนดและใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ

ID.RM-1: จัดทำและการจัดการกระบวนการจัดการความเสี่ยง และได้รับการยอมรับโดยผู้มีส่วนได้ส่วนเสียขององค์กร (ข้อมูลอ้างอิง **iso 27001** ได้แก่ **Clause 6.1.3, Clause 8.3, Clause 9.3**)

ID.RM-2: กำหนดและแสดงระดับความเสี่ยงที่ยอมรับได้ขององค์กรอย่างชัดเจน (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **Clause 6.1.3, Clause 8.3**)

ID.RM-3: การกำหนดระดับความเสี่ยงที่ยอมรับได้ขององค์กรนั้นได้รับแจ้งจากบทบาทในโครงสร้างพื้นฐานที่สำคัญและการวิเคราะห์ความเสี่ยงเป็นการเฉพาะแต่ละส่วน (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **Clause 6.1.3, Clause 8.3**)

5 **Supply Chain Risk Management (ID.SC):** ลำดับความสำคัญ ข้อจำกัด การยอมรับความเสี่ยง และข้อสมมุติฐานขององค์กร เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงที่เกี่ยวข้องกับการ

จัดการความเสี่ยงในห่วงโซ่อุปทาน และการองค์กรได้กำหนดและประยุกต์ใช้กระบวนการเพื่อระบุ ประเมิน และจัดการความเสี่ยงในห่วงโซ่อุปทาน

ID.SC-1: กระบวนการจัดการความเสี่ยงในห่วงโซ่อุปทานไซเบอร์ถูกระบุจัดตั้งประเมิน จัดการและตกลงโดยผู้มีส่วนได้เสียขององค์กร (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2**)

ID.SC-2: ซัพพลายเออร์และคู่ค้าบุคคลที่สามของระบบข้อมูลส่วนประกอบและบริการมีการระบุจัดลำดับความสำคัญและประเมินโดยใช้กระบวนการประเมินความเสี่ยงโซ่อุปทานไซเบอร์ (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.15.2.1, A.15.2.2**)

ID.SC-3: สัญญากับซัพพลายเออร์และพันธมิตรบุคคลที่สามถูกนำมาใช้เพื่อดำเนินการตามมาตรการที่เหมาะสมซึ่งออกแบบมาเพื่อตอบสนองวัตถุประสงค์ของโครงการรักษาความปลอดภัยทางไซเบอร์ขององค์กรและแผนการจัดการความเสี่ยงทางไซเบอร์ซัพพลายเชน (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.15.2.1, A.15.2.2**)

ID.SC-4: ซัพพลายเออร์และพันธมิตรบุคคลที่สามจะได้รับการประเมินเป็นประจำโดยใช้การตรวจสอบผลการทดสอบหรือการประเมินรูปแบบอื่น ๆ เพื่อยืนยันว่าพวกเขาปฏิบัติตามภาระผูกพันตามสัญญา (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.15.2.1, A.15.2.2**)

ID.SC-5: การวางแผนและทดสอบการตอบสนองและการกู้คืนจะดำเนินการกับซัพพลายเออร์และผู้ให้บริการบุคคลที่สาม (ข้อมูลอ้างอิงตาม **iso 27001** ได้แก่ **A.17.1.3**)

บทที่ 3

บทอภิปรายผล

3.1 กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ใหม่ ตาม พ.ร.บ ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 สามารถแสดงขั้นตอนการทำงานได้นี้

Strategic Cybersecurity Framework Based on Baldrige Excellency Criteria and Thai Cybersecurity Law and Regulation		
หัวข้อการปฏิบัติ	วิธีการ/กลุ่มงาน	<u>ส่วนเพิ่มเติม</u> -ส่วนที่ 1, 3 พ.ร.บ.ฯ -ยุทธศาสตร์ไซเบอร์ สมช.
1 การกำหนดขอบเขต 2 บริบทขององค์กร		กำหนดตามคุณลักษณะขององค์กรโครงสร้างพื้นฐานสำคัญแต่ละประเภท
3 การพัฒนายุทธศาสตร์ องค์กรรวมการพิจารณาความมั่นคงทางไซเบอร์ในการพัฒนายุทธศาสตร์อย่างไร?	(ID-BE, ID-GV, ID-RA, ID-RM, ID-SC)	การจัดทำกรอบนโยบายของหน่วยงาน
4 การประยุกต์ใช้แผนยุทธศาสตร์ องค์กรใช้องค์ประกอบอื่นของความมั่นคงปลอดภัยไซเบอร์ในแผนยุทธศาสตร์ธุรกิจอย่างไร?	(ID-BE, ID-GV, ID-RA, ID-RM)	จัดทำรายงานการเตรียมความพร้อมของหน่วยงาน
5 การประเมินผลการปฏิบัติ วิธีการ (Approach): •การประยุกต์ใช้ (Deployment): •การเรียนรู้ (Learning): •การบูรณาการ (Integration):	องค์กรขั้นเริ่มต้น (Reactive), องค์กรที่มีการเตรียมตัว (Early), องค์กรกำลังพัฒนา (Developing), องค์กรแห่งความพร้อม (Mature), องค์กรชั้นนำ (Leading), องค์กรตัวอย่าง (Exemplary))	เพื่อพัฒนาความเป็นเอกภาพและการบูรณาการในการดำเนินงานขององค์กรและต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

รูปที่ 7 ส่วนเพิ่มขยายของกรอบแนวทางปฏิบัติการความมั่นคงไซเบอร์

1 การกำหนดขอบเขต การประเมินการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ทั้งหน่วยงานย่อยหรือส่วนต่างๆ ขององค์กร

2 ทำความเข้าใจบริบทขององค์กร โดยเน้นถึงความต้องการและผลการปฏิบัติงานที่สำคัญด้านความมั่นคงปลอดภัยไซเบอร์

3 คำถามเกี่ยวกับกระบวนการ (หมวด 1-6) คำถามส่วนมากเริ่มจากคำถามว่า "อย่างไร" ในการตอบคำถามให้ข้อมูลเกี่ยวกับกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งการศึกษาเฉพาะเรื่องได้ใช้คำถาม ข้อ 6 เรื่องการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

4 การประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจได้รวมเนื้อหาส่วนเครื่องมือสำหรับภาคปฏิบัติ (**Crosswalk**) แสดงรายการในความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจสัมพันธ์กับองค์ประกอบของกรอบแนวทางการพัฒนาโครงสร้างพื้นฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งใช้ในการประเมิน ได้แก่ วิธีการ (**Approach):** องค์กรบรรลุเป้าความมั่นคงปลอดภัยไซเบอร์ โดยวิธีการหรือระบบสำคัญที่ใช้ในการแก้ปัญหาอย่างไร**?** การประยุกต์ใช้ (**Deployment):** องค์กรประยุกต์ใช้กระบวนการหลักความมั่นคงปลอดภัยขององค์กรอย่างต่อเนื่องหรือไม่ การเรียนรู้ (**Learning):** องค์กรปรับปรุงกระบวนการสำคัญทางความมั่นคงปลอดภัยไซเบอร์และถูกแบ่งปันภายในองค์กรหรือไม่ และการบูรณาการ (**Integration):** ระบบความมั่นคงปลอดภัยไซเบอร์ตอบสนองความต้องการขององค์กรในปัจจุบันและอนาคตอย่างทั่วถึงอย่างไร[4]

การประเมินระดับการตอบสนอง โดยใช้กระบวนการและผลการประเมิน ได้กำหนดคำอธิบายขององค์กรขั้นเริ่มต้น(**Reactive),** องค์กรที่มีการเตรียมตัว (**Early),** องค์กรกำลังพัฒนา (**Developing),** องค์กรแห่งความพร้อม (**Mature),** องค์กรชั้นนำ (**Leading),** องค์กรตัวอย่าง (**Exemplary)**[4]

ส่วน 2.6 เป็นการดำเนินงานสร้างกรอบแนวทางความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ความสอดคล้องกับความต้องการในการดำเนินธุรกิจหลักและผู้เกี่ยวข้องทุกภาคส่วนขององค์กร และตอบสนองต่อ พ.ร.บ.ความมั่นคงทางไซเบอร์ พ.ศ. 2562 (เฉพาะส่วนยุทธศาสตร์) ตามวัตถุประสงค์ข้อ 2

3.2 การทดสอบคุณสมบัติกรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ใหม่

การทดสอบความสอดคล้องกรอบความมั่นคงปลอดภัยไซเบอร์ใหม่ กับ ยุทธศาสตร์ไซเบอร์ สมช. และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 โดยวิธี **แบบ** Desk-top analysis เริ่มจาก 1) การ

กำหนดขอบเขตและบริบทองค์กร โดยให้คำนึงถึงคุณลักษณะขององค์กรแต่ละประเภท 2) การใช้แบบประเมินผลการปฏิบัติของไบล์ดริจ เป็นแนวทางในการปฏิบัติซ้ำ เพื่อเน้นให้เกิดพัฒนาองค์กรให้มีการบรูณาการอย่างต่อเนื่อง ทั้งนี้ได้ทำการทดสอบขั้นตอนและคุณสมบัติกรอบแนวทางฯ ดังนี้

- การกำหนดขอบเขต โดยใช้แนวทางจากส่วนที่ 1 ของ พ.ร.บ.ฯ เรื่องส่วนที่ 1 แผนและนโยบายในการพิจารณา
- บริบทขององค์กร ได้ใช้แนวทางจากส่วนที่ 3 ของ พ.ร.บ.ฯ เรื่องการประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือการให้บริการในด้านต่างๆในการพิจารณาปรับความต้องการด้านความมั่นคงไซเบอร์ตามรูปแบบขององค์กร
- คำถามเกี่ยวกับกระบวนการ (หมวด 1-6) ซึ่งการศึกษาเฉพาะเรื่องได้ใช้คำถาม ข้อ 2 เรื่องแผนยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ พิจารณาควบคู่กับประเด็นยุทธศาสตร์ ข้อ ๒.๑ การจัดทำกรอบนโยบายของหน่วยงาน ที่ทำให้แผนปฏิบัติราชการขององค์กรรวมการพิจารณาความมั่นคงทางไซเบอร์ในการพัฒนายุทธศาสตร์ โดย **ID.BE-**1: ระบุบทบาทขององค์กรในห่วงโซ่อุปทาน และสื่อสารไปสู่ทุกส่วนที่เกี่ยวข้อง ข้อมูลอ้างอิงตาม **iso** 27001 ได้แก่ **A.**15.1.1**, A.**15.1.2**, A.**15.1.3**, A.**15.2.1**, A.**15.2.2 ซึ่งเป็นการจัดการ การบริการ ความสัมพันธ์กับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอก
- การประเมินผลการปฏิบัติ การพัฒนากรอบแนวทางนี้มีความเป็นเอกภาพและการบูรณาการการจัดทำแผนยุทธศาสตร์องค์กรและสอดคล้องกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 ซึ่งต้องมีผลลัพธ์ที่เน้นให้เกิดการบรูณาการและเป็นองค์กรแห่งความพร้อม และสามารถใช้เป็นเกณฑ์การประเมินขั้นต่ำตาม พ.ร.บ.ฯ รวมถึงจัดทำรายงานการเตรียมความพร้อมของหน่วยงาน

บทที่ 4

อภิปรายผล

4.1 สิ่งที่ได้รับจากงานวิจัย

กรอบแนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ใหม่ ที่สร้างขึ้นซึ่งจะสามารถตอบสนองต่อยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 ได้ดังนี้

1) องค์การจะมีแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการตรวจสอบและประเมินความเสี่ยงอย่างน้อยตาม ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. **2560-2564** ประเด็นยุทธศาสตร์ที่ 2 ข้อ 2.1 โดยมีความเชื่อมโยงกับ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ มาตรา 42 ตลอดจนทำให้องค์กรพร้อมการบูรณาการการจัดการและการประสานความร่วมมือ การสร้างมาตรการและกลไกการป้องกัน รับมือ และลดความเสี่ยง การพัฒนาบุคลากร การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ การสร้างความตระหนัก รวมถึงการพัฒนาระเบียบและกฎหมายให้ทันต่อเหตุการณ์ปัจจุบัน

2) สามารถจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประเด็นยุทธศาสตร์ที่ 2 ข้อ 2.3 โดยมีความเชื่อมโยงกับ มาตรา 44 ที่ให้มีแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ แผนการรับมือภัยคุกคามทางไซเบอร์ และใช้เป็นมาตรการควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน ตามมาตรา 55 ได้อีกด้วย

3) จากการวิเคราะห์กลุ่มงานหลักที่ข้อมูลอ้างอิงพบว่า ISO 27001 ไม่ได้กล่าวถึงและจำเป็นต้องใช้มาตรฐาน 3 NIST SP 800-53 Rev. 4 เข้าจัดการแทนได้แก่ **ID.BE-**3 ใช้ข้อมูลอ้างอิง **PM-**11**, SA-**14 และ **RS.AN-**5: ใช้ข้อมูลอ้างอิง **PM-**15 ทั้งนี้การประยุกต์ใช้มาตรฐานดังกล่าวเป็นไปตามข้อกำหนดใน **Framework Core**

4.2 สรุป

การจัดทำกรอบแนวทางยุทธศาสตร์ความมั่นคงไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ (เฉพาะยุทธศาสตร์) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 นี้สามรถประยุกต์ใช้มาตรฐานความ

มั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และ พ.ร.บ.ความมั่นคงทางไซเบอร์ พ.ศ. 2562 ซึ่งได้วิเคราะห์และทบทวนคุณสมบัติการใช้งานแบบ desk-top analysis อันมีคุณสมบัติของมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ ดังนี้

1 องค์กรสามารถสร้างสอดคล้องกับยุทธศาสต์ธุรกิจและผู้เกี่ยวข้องขององค์กร ที่ตอบสนองต่อ พ.ร.บ.ความมั่นคงทางไซเบอร์ พ.ศ. 2562

2 องค์กรสามารถใช้ออกแบบกระบวนการ การจัดการและการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรโครงสร้างพื้นฐานสาคัญแต่ละประเภท

3 องค์กรสามารถประยุกต์ใช้ข้อมูลอ้างอิงการปฏิบัติ เป็นแนวทางและการปฏิบัติส่วนเฉพาะของแต่ละองค์กร และเกิดการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคาม วิธีการและการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภายในและระหว่างองค์กร

4 องค์กรสามารถพัฒนาและจัดทำยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Strategy) ที่สอดคล้องกับยุทธศาสตร์ทางธุรกิจ (Business Strategy) และสามารถประยุกต์ใช้ในการบริหารจัดการกับความมั่นคงปลอดภัยไซเบอร์กับทุกภาคส่วนที่ได้รับผลกระทบ

5 องค์กรสามารถป้องกันการหยุดชะงักและชดเชยมาตรการความมั่นคงปลอดภัยที่หายไปในเวลาปรับปรุงพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับการดำเนินงานขององค์กรและสามารถใช้ผลการประเมินความสำเร็จในการพัฒนาต่อได้

4.3 ข้อเสนอแนะ

กรอบแนวทางยุทธศาสตร์ความมั่นคงไซเบอร์ บนพื้นฐานมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไบล์ดริจ และพ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ 2562 สามารถประยุกต์ใช้ได้กับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 จึงสมควรสร้างกรอบแนวทางความมั่นคงไซเบอร์ในภาพรวมทั้งหมดขององค์กรและในแต่ละประเภทขององค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เอกสารอ้างอิง

[1] KEY CYBERTHREAT TRENDS OUTLOOK FROM THE ASEAN CYBERCRIME OPERATIONS DESK, ASEAN CYBERTHREAT ASSESSMENT 2021, 2021[วันที่สืบค้น 2 กรกฎคม 2564]. เข้าถึงได้จาก https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

[2] CyberX [อินเทอร์เน็ต],2020 GLOBAL IoT/ICS RISK REPORT,2021[วันที่สืบค้น 2 กรกฎคม 2564]. เข้าถึงได้จาก : https://cyberx-labs.com/wp-content/uploads/2020/09/CYBX_2020_Risk-Report.pdf

[3] Cyberx [อินเทอร์เน็ต], 2019 Global ICS & IIoT Risk Report. 2020 [วันที่สืบค้น 2 กรกฎคม 2564] , เข้าถึงได้จาก: https://cyberx-labs.com/resources/risk-report-2019/

[4] National Institute of Standards and Technology (NIST), The Baldrige Cybersecurity Excellency Builder , 2017 [วันที่สืบค้น 2 กรกฎคม 2564] .เข้าถึงได้จาก : https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf

[5] Framework for Improving Critical Infrastructure Cybersecurity V.1.1_April18, 2018 [วันที่สืบค้น 2 กรกฎคม 2564] ,เข้าถึงได้จาก: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[6]มาตรฐาน ISO/IEC 27001 (2013) The International Organization for Standardization .2013,[วันที่สืบค้น 2 กรกฎคม 2564]. เข้าถึงได้จาก: www.iso.org

[7]พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ 2562 ปีที่พิมพ์ 2562

[8]ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 ปีที่พิมพ์ 2560

ประวัติย่อผู้วิจัย

ยศ ชื่อ นาวาอากาศเอก สืบศิริ อ่ำสำอางค์

วัน เดือน ปีเกิด 18 มิถุนายน 2519

ประวัติสำเร็จการศึกษา

พ.ศ. 2538	โรงเรียนเตรียมทหาร รุ่นที่ 36
พ.ศ. 2543	โรงเรียนนายเรืออากาศ รุ่นที่ 43
พ.ศ. 2552	โรงเรียนเสนาธิการทหารเรือ รุ่นที่ 90

ประวัติการทำงาน

พ.ศ. 2543 – 2545	หัวหน้าหมวดซ่อมอากาศยาน กองซ่อมอากาศยาน 1
พ.ศ. 2545 – 2548	หัวหน้าหมวดช่างประจำอากาศยาน ฝูงบิน 401
พ.ศ. 2550 – 2551	รองหัวหน้าฝ่ายการช่าง ฝูงบิน 403
พ.ศ. 2553 – 2554	หัวหน้าฝ่ายยุทธการและการข่าว กรมนักเรียนเตรียมทหาร
พ.ศ. 2554 – 2555	รองหัวหน้ากองกิจการพลเรือน กองบัญชาการโรงเรียนเตรียมทหาร
พ.ศ. 2555 – 2560	นายทหารประจำศูนย์รักษาความปลอดภัย
พ.ศ. 2560 – 2562	ผู้ช่วยผู้อำนวยการกองแผนและโครงการ ศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล
พ.ศ. 2563 - 2564	ผู้ช่วยผู้อำนวยการกองข่าว ศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล
พ.ศ. 2564 – 2565	รองผู้อำนวยการกอง 7 ศูนย์รักษาความปลอดภัย

ตำแหน่งปัจจุบัน

ปัจจุบัน	นายทหารปฏิบัติการ ประจำ ศูนย์รักษาความปลอดภัย