การจัดการความมั่นคงปลอดภัยไซเบอร์
สำหรับอุตสาหกรรมขนาดใหญ่

โดย

นายยุทธนา เจียมตระการ
ผู้ช่วยผู้จัดการใหญ่ - การบริหารกลาง
บริษัท ปูนซิเมนต์ไทย จำกัด (มหาชน)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60
ประจำปีการศึกษา พุทธศักราช 2560 - 2561

บทคัดย่อ

เรื่อง การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย นายยุทธนา เจียมตระการ **หลักสูตร** วปอ. **รุ่นที่** 60

การนำพาประเทศไทยก้าวสู่ยุคไทยแลนด์ 4.0 โดยใช้วิทยาศาสตร์และเทคโนโลยีมายกระดับเศรษฐกิจของประเทศให้สามารถแข่งขันได้อย่างยั่งยืน จำเป็นต้องมีการจัดการความมั่นคงปลอดภัยไซเบอร์ควบคู่ไปด้วย ซึ่งไม่เพียงเฉพาะภาครัฐเท่านั้นแต่รวมถึงภาคธุรกิจด้วย

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ มีวัตถุประสงค์เพื่อหาแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ให้มีประสิทธิผลและประสิทธิภาพ และสอดรับกับนโยบายของประเทศในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ โดยทำการศึกษางานวิจัยและข้อมูลที่เกี่ยวข้อง เช่น ยุทธศาสตร์ชาติ 20 ปี นโยบายและแผนระดับชาติ มาตรฐานที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ เป็นต้น สัมภาษณ์ผู้ทรงคุณวุฒิทั้งภาครัฐและภาคธุรกิจ และศึกษาการปฏิบัติจริงขององค์กรที่อยู่ในอุตสาหกรรมขนาดใหญ่ วิเคราะห์ข้อมูล และสารสนเทศทั้งหมดข้างต้นจนสามารถกำหนดเป็นกรอบการดำเนินการที่จำเป็นในการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity 4-Core Framework) ที่สามารถนำไปขยายผลในการปฏิบัติในภาคธุรกิจอื่นๆ ต่อไปได้ เสนอกลไกการจัดการเพื่อให้เกิดการเชื่อมต่อจากระดับนโยบายของภาครัฐสู่การปฏิบัติในภาคธุรกิจ และข้อเสนอแนะการดำเนินการสำคัญสำหรับภาครัฐและอุตสาหกรรมขนาดใหญ่ในภาคธุรกิจเพื่อช่วยให้การสร้างความมั่นคงปลอดภัยไซเบอร์บรรลุความสำเร็จอย่างมีประสิทธิภาพยิ่งขึ้น เช่น การกำหนดเป้าหมายในยุทธศาสตร์ชาติ การจัดทำแผนแม่บทของประเทศ การสร้างความตระหนักกับผู้บริหารระดับสูงขององค์กร การใช้หลักการบริหารจัดการความเสี่ยงเพื่อการดำเนินการ การสร้างเครือข่ายความร่วมมือ เป็นต้น ทั้งนี้การจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ ซึ่งในที่นี้เปรียบเสมือนตัวแทนของภาคธุรกิจจะสำเร็จได้ จำเป็นต้องมีการดำเนินการร่วมกันในลักษณะ 3 ประสานของทั้ง ภาครัฐ อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ และเครือข่ายความร่วมมือ ที่สอดคล้องไปด้วยกัน อันจักนำพาประเทศไทยก้าวเข้าสู่ยุค 4.0 ที่มีความมั่นคง มั่งคั่ง และยั่งยืนตามเป้าหมายของยุทธศาสตร์ชาติต่อไป

Abstract

Title : Cybersecurity for Business in Large-scale Industry

Field : Science and Technology

Name : Mr. Yuttana Jiamtragan **Course :** NDC **Class :** 60

To lead Thailand to Industry 4.0 era by utilizing science and technology in order to raise the country's economic level for sustainable competitiveness requires the implementation of cybersecurity not only in the public sector, but also in the private sector.

This qualitative research aims to explore the effective and efficient cybersecurity approaches for the large-scale industry aligning with Thailand's cybersecurity policy by studying the relevant researches and the information such as 20-year national strategy, national cybersecurity policy and plans, cybersecurity standards, etc., interviewing the public and private cybersecurity professionals, exploring the selective organization practices, and analyzing overall data and information to create the Cybersecurity 4-core Framework which is able to apply in other sectors. This research also recommends the mechanisms to deploy policy from the government to a private sector as well as the suggestion for execution such as the national cybersecurity targets, the national cybersecurity master plan, executive top management awareness, risk management, and cooperative networking, etc., for more efficient cybersecurity implementation. Moreover, cybersecurity approaches for the large-scale industry representing the private sector, require the coordination of 3 parties; the public sector, the large-scale industry in the private sector, and the cooperative network to achieve the cybersecurity goals in order to bring Thailand stepping forward to 4.0 era with Stability, Prosperity and Sustainability as the vision of 20-year national strategy.

คำนำ

จากการที่รัฐบาลมุ่งขับเคลื่อนประเทศไปสู่ไทยแลนด์ 4.0 ผ่านการดำเนินการต่างๆ เช่น การผลักดัน PromptPay การมุ่งสู่ Cashless Payment การพัฒนา Smart Service ผ่านการใช้บัตรประชาชนใบเดียวในการติดต่อราชการ การส่งเสริมธุรกิจ E-Commerce เป็นต้น ล้วนดำเนินการบนโครงข่ายดิจิทัลที่มีความเสี่ยงต่อภัยคุกคามไซเบอร์แฝงอยู่ มีการวิเคราะห์แนวโน้มของภัยนี้ว่าจะสร้างความสูญเสียแก่เศรษฐกิจโลกอย่างมหาศาล และประเทศในกลุ่มอาเซียนเป็นเป้าหมายสำคัญของกลุ่มแฮ็กเกอร์ สำหรับประเทศไทยเองก็ได้รับการโจมตีทางไซเบอร์อย่างต่อเนื่องทุกปี ซึ่งล่าสุดเมื่อเดือนเมษายน พ.ศ.2561 ที่ผ่านมา ก็ถูกโจมตีโดยการแฮ็กเข้าสู่เซิร์ฟเวอร์ของมหาวิทยาลัยแห่งหนึ่ง เพื่อใช้เป็นฐานจารกรรมข้อมูลของประเทศอื่นๆ อีก 17 ประเทศ เห็นได้ชัดว่าภัยคุกคามไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลาหากมีช่องโหว่ในระบบ

สำหรับประเทศไทยทั้งภาครัฐและบางภาคธุรกิจมีการดำเนินการเพื่อป้องกันภัยไซเบอร์อยู่แล้วตามความเหมาะสมของแต่ละหน่วยงาน แต่การเกิดเหตุการณ์โจมตีแบบข้างต้นก็เป็นเรื่องจำเป็นที่ควรศึกษาว่าการดำเนินการที่มีอยู่แล้วยังมีประสิทธิผลเพียงพอหรือไม่ และด้วยเหตุที่ผู้วิจัยอยู่ในอุตสาหกรรมขนาดใหญ่ที่เข้าข่ายเป็น Critical Infrastructure ซึ่งมีโอกาสที่จะได้รับผลกระทบจากภัยคุกคามไซเบอร์ รวมทั้งยังสามารถส่งผลไปสู่องค์กรอื่นในวงกว้างได้ ผู้วิจัยจึงมุ่งศึกษาแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ เพื่อตอบประเด็นว่า การดำเนินการที่มีอยู่แล้วควรเพิ่มเติมเรื่องใดเพื่อเพิ่มประสิทธิผล และประสิทธิภาพในการป้องกันให้ดียิ่งขึ้น หากต้องมีการทบทวนและจัดลำดับความเร่งด่วน จะมีแนวทางอย่างไร รวมทั้งทำอย่างไรให้เกิด Alignment ระหว่างภาครัฐและอุตสาหกรรมขนาดใหญ่ในภาคธุรกิจได้

สุดท้ายนี้ ผู้วิจัยหวังว่า งานวิจัยฉบับนี้สามารถเป็นประโยชน์ทั้งต่อภาครัฐและภาคธุรกิจในการสร้างความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นรูปธรรม และสามารถใช้พัฒนาต่อยอดการดำเนินการเพื่อเพิ่มขีดความสามารถการแข่งขันด้วยเศรษฐกิจดิจิทัลให้กับประเทศชาติได้

(นายยุทธนา เจียมตระการ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 60
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

สารบัญแผนภาพ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ประเทศไทยในการก้าวสู่ยุคไทยแลนด์ 4.0 ที่รัฐมีเป้าหมายส่งเสริมให้มีการใช้วิทยาศาสตร์ เทคโนโลยี วิจัยและพัฒนา อีกทั้งนวัตกรรมในทุกสาขาของภาคการผลิต และบริการ โดยเฉพาะเทคโนโลยีดิจิทัล เพื่อยกระดับด้านเศรษฐกิจ และสังคมของประเทศ ตามที่กำหนดไว้ในร่างยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2560-2579) ยุทธศาสตร์ที่ 2 ด้านการสร้างความสามารถในการแข่งขัน อย่างไรก็ตามแนวโน้มความเสี่ยงของภัยคุกคามไซเบอร์ (Cybersecurity) ที่มีต่อเศรษฐกิจของโลกในระดับต้นๆ ก็มีการนำเสนอไว้ในหลายรายงาน เช่น รายงานของ World Economic Forum ที่มีการสำรวจตั้งแต่ปี พ.ศ. 2555-2560 พบว่าลำดับความสำคัญของภัยคุกคามไซเบอร์ที่มีต่อเศรษฐกิจของโลกอยู่ในระดับ Top 5 มาโดยตลอด[1] รายงานวิจัยในปี พ.ศ. 2555 ของบริษัท Verizon ประเทศสหรัฐอเมริกา ที่สำรวจการโจมตีด้านไซเบอร์ที่เกิดขึ้นทั่วโลก ได้รายงานการพบเหตุการณ์ภัยคุกคามไซเบอร์ที่สำคัญทั่วโลกถึง 855 ครั้ง จากการโจมตีกว่า 174 ล้านรายการ และในรายงานของบริษัท Ponemon Institute ประเทศสหรัฐอเมริกา ในปีเดียวกัน ก็มีรายงานผลการวิจัยว่า องค์กรขนาดใหญ่ 56 แห่งในสหรัฐอเมริกาถูกภัยคุกคามไซเบอร์สูงถึง 1.8 ครั้งต่อองค์กรต่อสัปดาห์ มีมูลค่าความเสียหายจากอาชญากรรมไซเบอร์สูงถึง 8.9 ล้านเหรียญสหรัฐต่อองค์กร[2] และยังมีการคาดการณ์ว่า ในปี พ.ศ. 2564 ภัยคุกคามไซเบอร์จะสร้างความสูญเสียต่อเศรษฐกิจทั่วโลกได้มากกว่า 6 ล้านล้านเหรียญสหรัฐ โดยมีสาเหตุหลักมาจากการมีช่องโหว่ของระบบไซเบอร์เพิ่มขึ้นตามการแพร่หลายของอุปกรณ์ IoT (Internet of Things) และเครื่องจักรอัตโนมัติ ปริมาณข้อมูล

---

[1] "บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก" – NIST's Framework for Improving Critical Infrastructure Cybersecurity "โอกาส ภัยคุกคาม และความเสี่ยงที่ผู้บริหารองค์กรต้องตระหนัก". (ออนไลน์). เข้าถึงได้จาก : www.acisonline.net/?p=4036&lang=th, 2560.

[2] "ความปลอดภัยทางไซเบอร์ (Cyber Security)". (ออนไลน์). เข้าถึงได้จาก : www.trendmicro.co.th/th/technology-innovation/cyber-security/, 2560.

ออนไลน์รวมถึงรหัสซอฟต์แวร์ใหม่ที่เกิดขึ้นในระดับหลายพันล้านรายการในแต่ละปี และการเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น การบุกรุกระบบ การทำลายข้อมูล การโจรกรรมทางการเงินและทรัพย์สินทางปัญญา การโจรกรรมข้อมูลส่วนบุคคลและทางการเงิน การโจมตีระบบไซเบอร์และทำให้การดำเนินงานของภาครัฐ และภาคธุรกิจหยุดชะงัก เป็นต้น[3] สำหรับประเทศไทยก็ได้รับผลกระทบจากภัยคุกคามไซเบอร์เช่นกัน จากข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. (ETDA) พบว่า มีภัยคุกคามไซเบอร์เกิดขึ้นอย่างต่อเนื่องทุกปี เฉพาะปี พ.ศ. 2560 (ตั้งแต่เดือนมกราคม - กันยายน) มีเกิดขึ้นแล้วถึง 2,624 ครั้งโดย 3 อันดับแรกที่พบอย่างสม่ำเสมอ คือ ความพยายามที่จะบุกรุกระบบ (Intrusion Attempts) การฉ้อโกง (Fraud) และการบุกรุกระบบ (Intrusions)[4]

ด้วยความเสี่ยงของภัยคุกคามไซเบอร์ต่อเศรษฐกิจของโลกข้างต้น และจากการที่สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้มีการสำรวจประเทศต่างๆ ทั่วโลก 193 ประเทศ รวมทั้งประเทศไทยด้วย ในเรื่องของความมุ่งมั่นของการจัดการความมั่นคงปลอดภัยไซเบอร์ระดับชาติ (National Cybersecurity Commitments) ใน 5 ด้านที่เกี่ยวข้อง ได้แก่

1. ด้านกฎหมาย (Legal)
2. ด้านเทคนิค (Technical)
3. ด้านโครงสร้างองค์กร (Organizational)
4. ด้านการสร้างความสามารถ (Capacity Building) และ
5. ด้านการให้ความร่วมมือ (Co-operation)

โดยผลการสำรวจในปี พ.ศ. 2560 พบว่า ประเทศไทยมีคะแนนจากการสำรวจที่เรียกว่า Global Cybersecurity Index (GCI) Score ต่ำกว่าประเทศสิงคโปร์ มาเลเซีย ออสเตรเลีย ญี่ปุ่น เกาหลีใต้ และนิวซีแลนด์ ซึ่งอยู่ในภูมิภาคเอเชียแปซิฟิกเช่นเดียวกัน โดยอยู่ในอันดับที่ 22[5]

---

[3] “การโจมตีทางไซเบอร์…ภัยคุกคามเศรษฐกิจใหม่”. (ออนไลน์). เข้าถึงได้จาก : thaitribune.org/contents/detail/312?content_id=29801&rand=1507434306, 2560.

[4] “สถิติภัยคุกคาม”. (ออนไลน์). เข้าถึงได้จาก : www.thaicert.or.th/statistics/statistics.html, เข้าถึงเมื่อ 12 ต.ค. 2560.

[5] International Telecommunication Union. “Global Cybersecurity Index (GCI) 2017”. 2017.

ซึ่งยังต่ำกว่าเป้าหมายที่กำหนดไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564) ที่กำหนดว่า อันดับความเสี่ยงจากการโจมตีด้านไซเบอร์ตามดัชนี ITU ของประเทศไทยจะต้องต่ำกว่าอันดับที่ 10 ของโลก[6] ด้วยเหตุนี้ หากประเทศไทยต้องการบรรลุเป้าหมาย ก็เป็นเรื่องจำเป็นที่จะต้องศึกษารายละเอียดหลักเกณฑ์ที่ต้องมีการดำเนินการของทั้ง 5 ด้านข้างต้น เพื่อนำมาปรับปรุงและยกระดับการดำเนินการด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศให้เป็นไปตามเป้าหมายที่กำหนดไว้ต่อไป

จะเห็นได้ว่าภาครัฐได้มีการกำหนดเป้าหมายด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 แล้ว แต่การจะบรรลุเป้าหมายดังกล่าวได้ ประเทศไทยจะต้องมีความพร้อม ซึ่งย่อมไม่ใช่เพียงหน้าที่ของภาครัฐเท่านั้น แต่เป็นหน้าที่ของทุกภาคส่วน รวมทั้งภาคธุรกิจด้วยที่ต้องร่วมมือกันอย่างเป็นองคาพยพ โดยเฉพาะธุรกิจที่อยู่ในอุตสาหกรรมโครงสร้างพื้นฐานสำคัญของประเทศ เพราะหากดำเนินการป้องกันภัยคุกคามนี้ได้ไม่เพียงพอ ไม่เพียงทำให้ยุทธศาสตร์ชาติไม่ประสบความสำเร็จตามเป้าหมาย “มั่นคง มั่งคั่ง ยั่งยืน” แต่ยังส่งผลต่อความสูญเสียทางเศรษฐกิจและกระทบต่อความมั่นคงของประเทศชาติด้วย

ทั้งนี้ การสร้างความมั่นคงปลอดภัยไซเบอร์ในองค์กรธุรกิจ นอกจากความเกี่ยวข้องกับหน่วยงานของภาครัฐในเรื่องที่เกี่ยวกับกฎหมาย ระเบียบ แนวปฏิบัติ หรือการสร้างความรู้และความตระหนักรู้ในเรื่องของไซเบอร์แล้ว องค์กรธุรกิจเอง จำเป็นที่ต้องศึกษาแนวทางที่เหมาะสมในการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรของตนเอง เช่น การกำหนดโครงสร้างองค์กร กรอบการทำงานและมาตรฐานความปลอดภัยด้านไซเบอร์ การพัฒนาบุคลากรในองค์กรให้มีทั้งความรู้ ความสามารถ และความตระหนักรู้ด้านภัยคุกคามไซเบอร์ ตลอดจนต้องทราบขีดความสามารถ ทั้งด้านการป้องกัน และการตอบสนองภัยคุกคามภายในองค์กรตนเอง เพื่อให้การบริหารและจัดการความเสี่ยงด้านไซเบอร์ทำได้อย่างเหมาะสมกับธุรกิจ นอกจากนี้กระบวนการในการดำเนินการ (Execution) ก็เป็นเรื่องที่ควรให้ความสำคัญเช่นเดียวกัน

งานวิจัยนี้เป็นการศึกษาองค์ประกอบข้างต้น เพื่อเป็นกรณีศึกษาในการจัดการ โดยเน้นวิจัยการจัดการโครงสร้างองค์กร และการสร้างความสามารถในอุตสาหกรรมขนาดใหญ่ เพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิผลและประสิทธิภาพ และสอดคล้องกับทิศทางของ

---

[6] สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. “แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่สิบสอง พ.ศ. 2560 - 2564”. 2560.

ยุทธศาสตร์ชาติ อันจะนำไปสู่การบรรลุความสำเร็จตามเป้าประสงค์เศรษฐกิจประเทศไทยยุคไทยแลนด์ 4.0 ได้อย่างเต็มภาคภูมิ

วัตถุประสงค์ของการวิจัย

1. ทบทวนสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย
2. เสนอแนะแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่
3. วิเคราะห์และสรุปปัจจัยที่มีผลต่อการจัดการความมั่นคงปลอดภัยไซเบอร์ ให้เกิดประสิทธิผลและประสิทธิภาพ

ขอบเขตของการวิจัย

ศึกษาองค์กรตัวอย่างที่เป็นอุตสาหกรรมขนาดใหญ่ในประเทศไทย และเข้าข่ายเป็น Critical Infrastructure ที่ระบุอยู่ในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology: NIST)

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยเริ่มจากการศึกษายุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายความมั่นคงแห่งชาติ กรอบการดำเนินงาน มาตรฐาน รายงานการสำรวจ และงานวิจัยที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยและการป้องกันภัยคุกคามทางไซเบอร์ของประเทศไทยและต่างประเทศ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิ และสำรวจประสิทธิผล และประสิทธิภาพการจัดการขององค์กรในอุตสาหกรรมขนาดใหญ่ที่เข้าข่ายเป็น Critical Infrastructure แล้วนำข้อมูลทั้งหมดมาวิเคราะห์ เพื่อเสนอแนะแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ในระดับนโยบายและการดำเนินการต่อไป

ประโยชน์ที่ได้รับจากการวิจัย

1. เข้าใจสถานการณ์การดำเนินการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย
2. ได้แนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิผลและประสิทธิภาพ สำหรับอุตสาหกรรมขนาดใหญ่
3. ทราบปัจจัยสำคัญในการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้เกิดประสิทธิผลและประสิทธิภาพ

คำจำกัดความ

ความมั่นคงปลอดภัยไซเบอร์	หมายถึง	กระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวล และกระจายข้อมูล ทั้งนี้รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรมและความผิดพลาดต่างๆ
Internet of Things (IoT)	หมายถึง	การที่สิ่งต่างๆ ถูกเชื่อมโยงเข้าสู่โลกอินเตอร์เน็ต ทำให้มนุษย์สามารถสั่งการ หรือ ควบคุมอุปกรณ์ต่างๆ ผ่านทางระบบเครือข่ายอินเตอร์เน็ตได้ จากทั้งระยะใกล้และไกล เช่น การปิด-เปิดอุปกรณ์ไฟฟ้า เครื่องจักรในโรงงานอุตสาหกรรม บ้านเรือน โดยผ่านเครือข่ายอินเตอร์เน็ต หากรักษาความปลอดภัยในระบบอินเตอร์เน็ตไม่ดีพอ ผู้ไม่ประสงค์ดีจะสามารถเข้ามากระทำสิ่งอันไม่พึงประสงค์ต่อตัวอุปกรณ์ เครื่องจักร สารสนเทศ และความเป็นส่วนตัวของบุคคลได้

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์

การพาประเทศไทยก้าวสู่ยุคไทยแลนด์ 4.0 โดยการส่งเสริมการใช้วิทยาศาสตร์ เทคโนโลยี วิจัยและพัฒนา และนวัตกรรมทั้งในภาคการผลิตและภาคบริการ ย่อมเกี่ยวข้องกับความก้าวหน้าของเทคโนโลยียุคใหม่โดยเฉพาะเทคโนโลยีไซเบอร์ ซึ่งมีทั้งประโยชน์ในการช่วยเพิ่มขีดความสามารถในการแข่งขันของประเทศ แต่ก็นำพาภัยคุกคามรูปแบบใหม่ที่เรียกว่าภัยคุกคามไซเบอร์เข้ามา ซึ่งสามารถสร้างผลกระทบทั้งต่อความมั่นคงและต่อเศรษฐกิจของประเทศ การสร้างความมั่นคงปลอดภัยไซเบอร์จึงเป็นเรื่องจำเป็นอย่างยิ่ง ภาครัฐเองมีการกำหนดเรื่องนี้ไว้ในยุทธศาสตร์ชาติ มีการจัดทำแผนและนโยบายรองรับ ศึกษากรอบการทำงานและมาตรฐานสากลที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ รวมทั้งวิจัยและสำรวจการดำเนินการดังกล่าวทั้งในหน่วยงานภาครัฐ และองค์กรภาคธุรกิจที่มีการใช้เทคโนโลยีไซเบอร์ เพื่อเป็นข้อมูลในการดำเนินการป้องกันภัยคุกคามดังกล่าวให้เกิดประสิทธิภาพ ประสิทธิผล และไม่เป็นอุปสรรคต่อเป้าหมายในการพัฒนาประเทศ

ยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

1. ยุทธศาสตร์ชาติ 20 ปี

ประเทศไทยได้จัดทำร่างยุทธศาสตร์ชาติระยะเวลา 20 ปี (พ.ศ. 2560-2579)[1] เพื่อให้เป็นยุทธศาสตร์ในการพัฒนาประเทศในระยะยาว ยกระดับคุณภาพของประเทศไทยในทุกภาคส่วนและนำพาประเทศให้หลุดพ้นหรือบรรเทาความรุนแรงของสภาพปัญหาที่เกิดขึ้นในปัจจุบัน ทั้งปัญหาความมั่นคง ปัญหาทางเศรษฐกิจ ปัญหาความเหลื่อมล้ำ ปัญหาการทุจริตคอร์รัปชัน

[1] สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. "(ร่าง) ยุทธศาสตร์ชาติ ระยะ 20 ปี (พ.ศ. 2560-2579)". 2560.

และปัญหาความขัดแย้งในสังคม รวมถึงสามารถรับมือกับภัยคุกคาม และบริหารจัดการกับความเสี่ยงที่จะเกิดขึ้นในอนาคต และสามารถเปลี่ยนผ่านประเทศไทยไปพร้อมกับการเปลี่ยนแปลงภูมิทัศน์ใหม่ของโลกได้ โดยยุทธศาสตร์ชาติจะเป็นกรอบในการจัดทำแผนต่างๆ ให้สอดคล้องและบูรณาการกันเพื่อไปสู่เป้าหมายของประเทศที่วางไว้

ยุทธศาสตร์ชาติฉบับนี้ประกอบด้วย 6 ยุทธศาสตร์หลัก มี 2 ยุทธศาสตร์ที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ ได้แก่ ยุทธศาสตร์ที่ 1 ยุทธศาสตร์ด้านความมั่นคง และยุทธศาสตร์ที่ 2 ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน โดยเล็งเห็นถึงภัยคุกคามไซเบอร์ที่จะมีความรุนแรงมากขึ้น จากการใช้ช่องทางไซเบอร์ในการจารกรรมข้อมูล การโจมตีระบบสาธารณูปโภค และการทำลายเสถียรภาพของรัฐบาล ประกอบกับทำเลที่ตั้งของประเทศไทยอยู่ใจกลางภูมิภาค และมีนโยบายการเปิดเสรีการค้าและการลงทุน จึงยากที่จะหลีกเลี่ยงการเผชิญกับอาชญากรรมข้ามชาติที่เกี่ยวกับไซเบอร์ได้ ทั้ง 2 ยุทธศาสตร์นี้ได้กำหนดแนวทางการพัฒนาเพื่อสร้างความมั่นคงปลอดภัยไซเบอร์ไว้ดังนี้

ตารางที่ 2-1 ยุทธศาสตร์ด้านความมั่นคงที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ / วัตถุประสงค์ / เป้าหมาย
ยุทธศาสตร์ที่ 1: ยุทธศาสตร์ด้านความมั่นคง วัตถุประสงค์: สร้างความมั่นคงในทุกระดับ ตั้งแต่ ระดับชาติ สังคม ชุมชน และความมั่นคงของมนุษย์จากภัยคุกคามทั้งที่เป็นภัยคุกคามแบบดั้งเดิม และภัยคุกคามรูปแบบใหม่ เช่น ภัยคุกคามจากการโจมตีทางไซเบอร์ เป็นต้น เป้าหมาย : ไม่ได้กำหนดเฉพาะชัดเจน
แนวทางการพัฒนา (เฉพาะที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์)
1.2 พัฒนาศักยภาพในการป้องกันประเทศ พร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่นๆ 1.2.3 พัฒนาประสิทธิภาพระบบการเตรียมพร้อมแห่งชาติ และระบบการบริหารจัดการสาธารณภัยและความมั่นคงแบบใหม่ให้มีความพร้อมเผชิญกับภาวะไม่ปกติ และภัยคุกคามทุกรูปแบบ **1.3 บูรณาการความร่วมมือกับต่างประเทศที่เอื้อให้เกิดความมั่นคง ความมั่งคั่งทางเศรษฐกิจ ป้องกันภัยคุกคามข้ามชาติ และคุณภาพชีวิตของคนในชาติ** 1.3.1 เสริมสร้างบทบาทของไทยในการพัฒนาผลประโยชน์ร่วมกัน ระหว่างผลประโยชน์ของชาติกับผลประโยชน์ของภูมิภาคและนานาประเทศ ตลอดจนพัฒนาระบบ กลไก มาตรการและความ

ตารางที่ 2-1 ยุทธศาสตร์ด้านความมั่นคงที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

แนวทางการพัฒนา (เฉพาะที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์) (ต่อ)
ร่วมมือระหว่างประเทศทุกระดับให้สอดคล้องกับกฎหมายระหว่างประเทศ 1.3.2 สร้างเสริมประสิทธิภาพการป้องกัน แก้ไข ระงับยับยั้ง ฟื้นฟู ภัยจากการก่อการร้ายและอาชญากรรมข้ามชาติทุกรูปแบบโดยบัญญัติกฎหมายที่เกี่ยวข้อง พัฒนาศักยภาพบุคลากร นำเทคโลยีที่ทันสมัยมาปรับใช้ในการดำเนินการเสริมสร้างจิตสำนึกภูมิคุ้มกันให้กับคนในสังคม 1.3.4 เสริมสร้างความมั่นคงและปกป้องโครงสร้างพื้นฐาน / สาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ให้ปลอดภัยจากการโจมตี รวมถึงส่งเสริมวัฒนธรรม สร้างความตระหนักรู้ในการใช้ไซเบอร์ในทางที่เหมาะสม ตลอดจนพัฒนาขีดความสามารถขององค์กร / บุคลากรผู้รับผิดชอบด้านไซเบอร์ให้มีความเชี่ยวชาญอย่างต่อเนื่อง

ที่มา : สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2560.

ตารางที่ 2-2 ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขันที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ / วัตถุประสงค์ / เป้าหมาย
ยุทธศาสตร์ที่ 2: ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน วัตถุประสงค์: สร้างความสามารถในการแข่งขันของประเทศคือ การเพิ่มผลิตภาพการผลิต (Productivity) โดยใช้วิทยาศาสตร์ เทคโนโลยี วิจัยและพัฒนา และนวัตกรรมในทุกสาขาของภาคการผลิตและบริการที่เป็นฐานรายได้เดิมและที่ต่อยอดเป็นฐานรายได้ใหม่ เป้าหมาย: 1. รายได้ต่อคน $\geq$ 15,000 USD / ปี หรือประมาณ $\geq$ 500,000 บาทต่อปี 2. GDP ขยายตัวเฉลี่ย 4-5% ต่อปี ในช่วงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 และเพิ่มเป็น $\geq$5% ในช่วง 15 ปี หลังจากนั้น 3. ผลิตภาพการผลิตรวม $\geq$ 3% ต่อปี 4. ประเทศไทยถูกจัดอันดับไม่ต่ำกว่า 1 ใน 10 ของการจัดอันดับความสามารถในการแข่งขันของโลกโดยองค์กรต่างๆ

ตารางที่ 2-2 ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขันที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

แนวทางการพัฒนา (เฉพาะที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์)
2.3 การพัฒนาปัจจัยสนับสนุนและการพัฒนาโครงสร้างพื้นฐานเพื่อเพิ่มขีดความสามารถในการแข่งขัน
2.3.1 แนวทางที่ 3 พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อส่งเสริมการพัฒนาเศรษฐกิจดิจิทัล และรองรับการยกระดับทางเศรษฐกิจอย่างทั่วถึงและคุณภาพชีวิตประชาชน โดยคำนึงถึงความปลอดภัยและความมั่นคงของประเทศ ขณะเดียวกันจะต้องมีการพัฒนาระบบการรักษาความปลอดภัยของระบบและเครือข่าย (Cybersecurity) ที่มีประสิทธิภาพสูง เพื่อให้เกิดความมั่นคงทางไซเบอร์

ที่มา : สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2560.

2. แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564)[2] จัดทำโดยสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักนายกรัฐมนตรี เพื่อเป็นเครื่องมือหรือกลไกสำคัญในการถ่ายทอดยุทธศาสตร์ชาติ 20 ปี ไปสู่การปฏิบัติ แผนฉบับนี้อยู่ในช่วง 5 ปีแรกของการขับเคลื่อนยุทธศาสตร์ชาติ มีการกำหนดเป้าหมายที่จะต้องบรรลุใน 5 ปีแรก ทั้งในมิติเศรษฐกิจ สังคม และสิ่งแวดล้อม โดยได้พิจารณาและวิเคราะห์การต่อยอดไปอีกใน 3 แผน จนถึงแผนพัฒนาฯ ฉบับที่ 15 คือช่วงปี พ.ศ. 2575-2579 ซึ่งเป็นช่วงสุดท้ายของยุทธศาสตร์ชาติ

หลักการสำคัญของแผนพัฒนาฯ ฉบับที่ 12 จะยึดแนวทางประกอบด้วย “หลักปรัชญาของเศรษฐกิจพอเพียง” “คนเป็นศูนย์กลางการพัฒนา” และ “วิสัยทัศน์ภายใต้ยุทธศาสตร์ชาติ 20 ปี” มาเป็นกรอบ กล่าวคือ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” ยุทธศาสตร์ในแผนพัฒนาฯ ฉบับที่ 12 มีทั้งหมด 10 ยุทธศาสตร์ โดยมี 2 ยุทธศาสตร์เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ คือ ยุทธศาสตร์ที่ 5 การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

[2] สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. “แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่สิบสอง พ.ศ. 2560 - 2564”. 2560.

และยุทธศาสตร์ที่ 7 การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ ทั้ง 2 ยุทธศาสตร์มีการกำหนดแนวทางการพัฒนาและเป้าหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ ไว้ดังนี้

ตารางที่ 2-3 แนวทางการพัฒนาและเป้าหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ของยุทธศาสตร์ที่ 5 ตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12

ยุทธศาสตร์ / เป้าหมาย
ยุทธศาสตร์ที่ 5: การเสริมสร้างความมั่นคงแห่งชาติ เพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน เป้าหมายด้านความมั่นคงปลอดภัยไซเบอร์: ตัวชี้วัด 5.3 อันดับความเสี่ยงจากการโจมตีด้านไซเบอร์ ต่ำกว่าอันดับที่ 10 ของโลก (ดัชนีความปลอดภัยไซเบอร์ของโลกของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU))
แนวทางการพัฒนา
3.2 การพัฒนาเสริมสร้างศักยภาพการป้องกันประเทศ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคามทั้งการทหาร และภัยคุกคามอื่นๆ 3.2.1 พัฒนาศักยภาพและความพร้อมของกองทัพในการป้องกันและรักษาผลประโยชน์ของประเทศ โดยพัฒนากำลังพลให้มีความรู้ความสามารถ มีอาวุธ ยุทโธปกรณ์ ยุทธภัณฑ์ และเทคโนโลยีที่ทันสมัย เหมาะสม เพียงพอ 3.2.2 พัฒนาระบบงานด้านการข่าวที่มีประสิทธิภาพ มีกลไกเสริมสร้างความร่วมมือ พัฒนาองค์ความรู้ ศึกษาวิเคราะห์แนวโน้มภัยคุกคาม รวมทั้งจัดทำฐานข้อมูลด้านการข่าวที่เชื่อมโยงระหว่างหน่วยงานภายในประเทศและต่างประเทศอย่างเป็นระบบ 3.2.3 มีระบบเตรียมพร้อมและกลไกเผชิญเหตุที่มีประสิทธิภาพทั้งในยามปกติและในสถานการณ์วิกฤติ ทั้งจากภัยคุกคามด้านความมั่นคง และจากสาธารณภัยขนาดใหญ่ 3.2.7 ดำเนินบทบาทเชิงรุก และใช้กรอบความร่วมมือระหว่างประเทศทั้งระดับภูมิภาค และพหุภาคี ตลอดจนเสริมสร้างขีดความสามารถ แลกเปลี่ยนและเรียนรู้แนวปฏิบัติที่เป็นเลิศ และร่วมมือในการรับมือภัยคุกคามด้านความมั่นคงระหว่างประเทศ **3.3 การส่งเสริมความร่วมมือกับต่างประเทศด้านความมั่นคง** 3.3.1 ดำเนินความสัมพันธ์กับต่างประเทศอย่างสมดุล โดยพัฒนาความร่วมมือกับประเทศเพื่อนบ้านอาเซียนและนานาประเทศในการแลกเปลี่ยนข้อมูลการข่าว และการร่วมกันดำเนินการเชิงรุก

ตารางที่ 2-3 แนวทางการพัฒนาและเป้าหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ของยุทธศาสตร์ที่ 5 ตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (ต่อ)

แนวทางการพัฒนา (ต่อ)
เพื่อป้องกันแก้ไขปัญหาและลดผลกระทบจากภัยคุกคาม 3.3.3 พัฒนาระบบการเก็บรักษาข้อมูลส่วนบุคคลด้านไซเบอร์ให้มีความมั่นคงปลอดภัยและกำกับดูแลระบบการส่งข้อมูลส่วนบุคคลข้ามแดนไปต่างประเทศให้เป็นไปตามมาตรฐานสากล **3.5 การบริหารจัดการความมั่นคงเพื่อการพัฒนา** 3.5.1 ปรับปรุงระบบติดตาม เฝ้าระวัง ศึกษา วิเคราะห์ และประเมินสถานการณ์ด้านความมั่นคง การเปลี่ยนแปลงของสถานการณ์ สภาวะแวดล้อมด้านความมั่นคง พิสูจน์ทราบและคาดการณ์ภัยคุกคาม 3.5.2 พัฒนากลไกด้านความมั่นคงและระบบการขับเคลื่อนแผนงานต่างๆ ให้พร้อมรับสถานการณ์ทั้งระดับชาติและระดับพื้นที่ โดยสร้างเครือข่ายการสนับสนุน ทั้งด้านนโยบาย องค์ความรู้ และการสร้างกลไกขับเคลื่อนแผนงานให้มีความเชื่อมโยงและตอบสนองต่อนโยบายรัฐบาล ควบคู่ไปกับการสนับสนุนการมีส่วนร่วมของภาคประชาชน (ประชารัฐ) ในการกำหนดและขับเคลื่อนแผนงานด้านความมั่นคง

ที่มา : สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2560.

ตารางที่ 2-4 แนวทางการพัฒนาและเป้าหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ของยุทธศาสตร์ที่ 7 ตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12

ยุทธศาสตร์ / เป้าหมาย
ยุทธศาสตร์ที่ 7: การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ เป้าหมายด้านความมั่นคงปลอดภัยไซเบอร์: ตัวชี้วัด 5.4 จำนวนหน่วยงานภาครัฐที่มีระบบความมั่นคงปลอดภัยทางไซเบอร์ เพิ่มขึ้นจากร้อยละ 47 เป็นมากกว่าร้อยละ 80 ในปี พ.ศ. 2564
แนวทางการพัฒนา
3.5 การพัฒนาเศรษฐกิจดิจิทัล 3.5.1 พัฒนาและปรับปรุงโครงสร้างพื้นฐานโทรคมนาคมของประเทศให้ทั่วถึงและมีประสิทธิภาพ

ตารางที่ 2-4 แนวทางการพัฒนาและเป้าหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ของยุทธศาสตร์ที่ 7 ตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (ต่อ)

แนวทางการพัฒนา (ต่อ)
3.5.2 ส่งเสริมการใช้เทคโนโลยีดิจิทัลในการสร้างมูลค่าเพิ่มทางธุรกิจ 3.5.3 ส่งเสริมนวัตกรรม การวิจัยและพัฒนาอุตสาหกรรมดิจิทัลและเทคโนโลยีอวกาศของไทย 3.5.4 สร้างความมั่นคงปลอดภัยไซเบอร์ โดยจัดตั้งศูนย์การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ โดยเฉพาะความมั่นคงปลอดภัยในภาคการเงิน และความปลอดภัยของข้อมูลส่วนบุคคล 3.5.5 ปรับปรุงกฎ ระเบียบ และกฎหมายที่เกี่ยวข้อง รวมทั้งการจัดตั้งองค์กรภาคเอกชนในรูปแบบสภาวิชาชีพดิจิทัล เพื่อเป็นกลไกในการพัฒนาอุตสาหกรรมดิจิทัลในส่วนของภาคเอกชนที่เชื่อมโยงกับภาครัฐ

ที่มา : สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2560.

3. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2560-2564)[3] จัดทำขึ้นโดยสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี เพื่อให้เป็นแผนหลักของชาติที่เป็นกรอบทิศทางการดำเนินการป้องกัน แจ้งเตือน แก้ไข หรือระงับยับยั้งภัยคุกคามต่างๆ ที่มีผลต่อความมั่นคงแห่งชาติ โดยใช้กระบวนการมีส่วนร่วมจากภาคส่วนต่างๆ ทั้งหน่วยงานรัฐในส่วนกลางและในพื้นที่ ภาควิชาการและผู้ทรงคุณวุฒิ และภาคประชาชน ในการให้ความเห็นและข้อเสนอ รวมถึงได้ศึกษาแนวคิดกรอบยุทธศาสตร์ชาติระยะ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 นโยบาย / ยุทธศาสตร์ของกระทรวงที่เกี่ยวข้อง และยุทธศาสตร์การจัดสรรงบประมาณร่วมด้วย นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติมีทั้งหมด 16 นโยบาย โดยมีการกำหนดการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ไว้ในนโยบายที่ 10 มีการกำหนดเป้าหมายเชิงยุทธศาสตร์ ตัวชี้วัด กลยุทธ์ และหน่วยที่รับผิดชอบหลักตามกลยุทธ์ ไว้ดังนี้

[3] สำนักงานสภาความมั่นคงแห่งชาติ. “นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2560 – 2564)”. 2560.

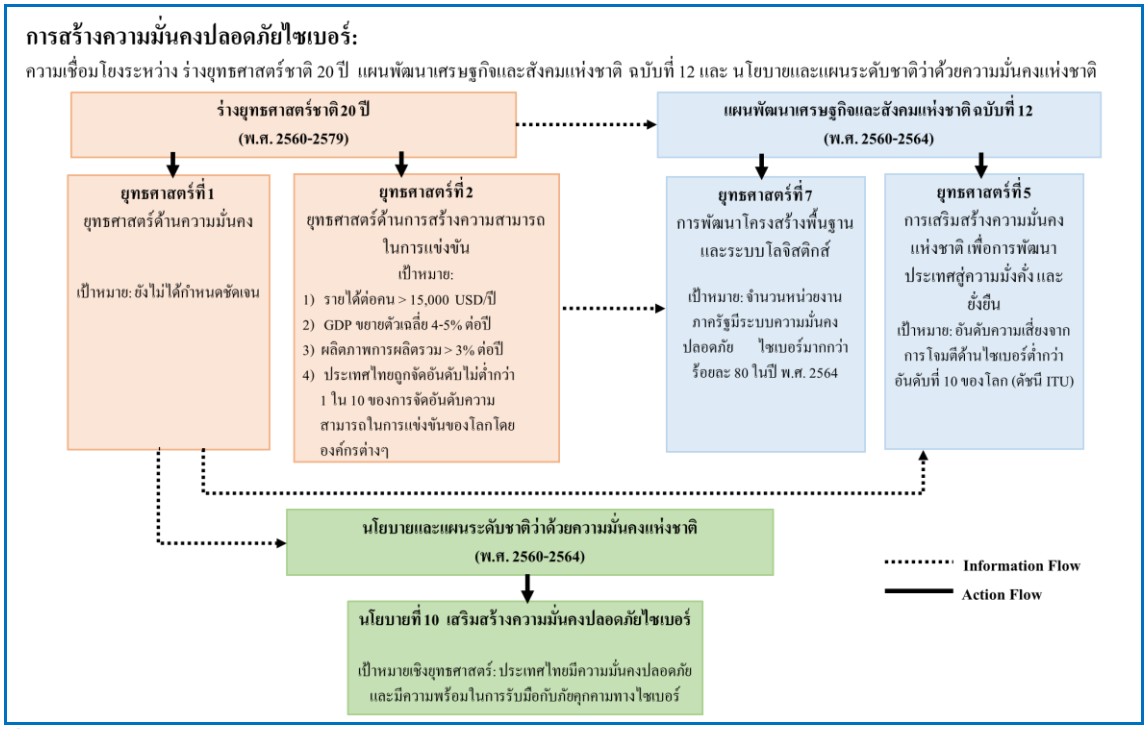
ตารางที่ 2-5 นโยบายการสร้างความมั่นคงปลอดภัยไซเบอร์ในนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

นโยบาย / เป้าหมายเชิงยุทธศาสตร์ / ตัวชี้วัด / หน่วยรับผิดชอบหลักตามกลยุทธ์
นโยบายที่ 10: เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ เป้าหมายเชิงยุทธศาสตร์: ประเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ตัวชี้วัด: 1. ระดับความพร้อมของไทยในการป้องกันความเสี่ยงจากการโจมตีด้านไซเบอร์ที่สอดคล้องกับหลักสากล 2. ระบบป้องกันทางไซเบอร์ที่มีประสิทธิภาพ สามารถปกป้องข้อมูลอิเล็กทรอนิกส์ของรัฐบาลตลอดจนโครงสร้างพื้นฐานสำคัญด้านไซเบอร์ หน่วยรับผิดชอบหลักตามกลยุทธ์: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กลยุทธ์
1. พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือน และตำรวจ และภาคส่วนต่างๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล 2. พัฒนากรอบความร่วมมือระหว่างประเทศ และอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ 3. พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญของภัยคุกคามความมั่นคงทางไซเบอร์ 4. ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ 5. พัฒนาการบังคับใช้กฎหมาย ระเบียบต่างๆ เพื่อความมั่นคงปลอดภัยไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ 6. ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน / บุคลากรที่เกี่ยวข้องให้มีความรู้ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

ที่มา : สำนักงานสภาความมั่นคงแห่งชาติ, 2560.

จะเห็นได้ว่า การสร้างความมั่นคงปลอดภัยไซเบอร์ที่ได้กำหนดไว้ในยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ นั้น มีความเชื่อมโยงและสอดรับกัน ดังแสดงในแผนภาพที่ 2-1

แผนภาพที่ 2-1 ความเชื่อมโยงของการสร้างความมั่นคงปลอดภัยไซเบอร์



ที่มา : ยุทธนา เจียมตระการ, 2561.

แนวคิด กรอบการทำงาน และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

1. แนวคิดความมั่นคงปลอดภัยไซเบอร์[4]

1.1 สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ว่าคือ ภาพรวมของเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัย การรักษาความปลอดภัย แนวทาง

[4] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). “ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security)”. 2559.

วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีปฏิบัติที่เป็นเลิศ การรับประกัน และเทคโนโลยีที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์

1.2 สำหรับประเทศไทย ยังไม่มีนิยามของคำว่า ความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศ ได้ให้นิยามคำว่า ความมั่นคงปลอดภัยไซเบอร์ คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่างๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่

C (Confidential): การรักษาความลับของข้อมูล คือ การรักษาหรือปกปิด เพื่อปกป้องข้อมูลให้เป็นความลับ โดยสามารถเข้าใช้งานได้ เฉพาะผู้ที่ได้รับอนุญาต หรือได้รับสิทธิการเข้าถึงเท่านั้น ซึ่งอาจกำหนดให้มีการเข้ารหัสข้อมูล

I (Integrity): การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล คือ การปกป้องรักษาข้อมูลไม่ให้ถูกแก้ไขเปลี่ยนแปลง หรือถูกทำลาย และเป็นการทำให้ข้อมูลมีความน่าเชื่อถือว่ามาจากแหล่งต้นฉบับจริง ไม่ได้ถูกนำไปเปลี่ยนแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต

A (Availability): ความพร้อมใช้งานของข้อมูล คือ การดูแลรักษาสภาพของข้อมูล ให้สามารถเข้าถึงและเรียกใช้งานได้ตลอดเวลาเมื่อต้องการโดยผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งระบบหรือข้อมูลสามารถหยุดให้บริการได้เมื่อไม่มีความจำเป็นในการใช้งาน หรือล่วงเลยระยะเวลาที่กำหนดให้มีการใช้งาน

1.3 นอกจากนี้ ในมาตรา 3 ของพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ให้ความหมายของ “ความมั่นคงปลอดภัยไซเบอร์” ไว้ว่า มาตรการและการดำเนินการที่กำหนดขึ้นเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้องป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเตอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

2. กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST

การสร้างความมั่นคงปลอดภัยไซเบอร์ เป็นการบริหารความเสี่ยงสำคัญที่ต้องการแนวทางการดำเนินงานอย่างเป็นระบบ เพื่อให้การบริหารจัดการเกิดประสิทธิภาพและประสิทธิผล ด้วยเหตุนี้ ในเดือนกุมภาพันธ์ พ.ศ. 2556 ประธานาธิบดีบารัค โอบามา ได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) พัฒนากรอบการทำงานเพื่อใช้ปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) ของประเทศขึ้นมา เพื่อให้เป็นแนวทางและมาตรฐาน ครอบคลุมทั้งระดับนโยบาย การจัดการองค์กร และเทคโนโลยีในการบริหารความเสี่ยงด้านไซเบอร์ ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญ 16 กลุ่มอุตสาหกรรม ประกอบด้วย

2.1 Chemical Sector

2.2 Commercial Facilities Sector

2.3 Communications Sector

2.4 Critical Manufacturing Sector

2.5 Dams Sector

2.6 Defense Industrial Base Sector

2.7 Emergency Services Sector

2.8 Energy Sector

2.9 Financial Services Sector

2.10 Food and Agriculture Sector

2.11 Government Facilities Sector

2.12 Healthcare and Public Health Sector

2.13 Information Technology Sector

2.14 Nuclear Reactors, Materials, and Waste Sector

2.15 Transportation Systems Sector และ

2.16 Water and Wastewater Systems Sector

การจัดทำกรอบการทำงานนี้ NIST ได้จัดให้มีการระดมความคิดทั้งจากหน่วยงานภาครัฐและเอกชนต่างๆ จนได้เป็นกรอบการดำเนินงานที่เรียกว่า “Framework for Improving

Critical Infrastructure Cybersecurity" โดยฉบับล่าสุดคือฉบับวันที่ 12 กุมภาพันธ์ พ.ศ. 2557[5] ประกอบด้วย 3 องค์ประกอบหลัก ดังแสดงในตารางที่ 2-6

ตารางที่ 2-6 Framework for Improving Critical Infrastructure Cybersecurity

Framework for Improving Critical Infrastructure Cybersecurity		
Framework Core	**Framework Implementation Tiers**	**Framework Profiles**
ใช้อธิบายกิจกรรมขององค์กร ประกอบด้วย **<u>หน้าที่งาน (Function)</u>** ในการสร้างความมั่นคงปลอดภัยไซเบอร์ มี 5 หน้าที่งาน ได้แก่ Identify, Protect, Detect, Response และ Recover **<u>กลุ่มงาน (Category)</u>** จำแนกตามผลลัพธ์ที่โยงกับแต่ละหน้าที่งาน **<u>กลุ่มงานย่อย (Subcategory)</u>** จำแนกตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค / กิจกรรมในการบริหารจัดการ **<u>ข้อมูลอ้างอิง (Informative References)</u>** ส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติที่นำมาใช้ในกลุ่มงานและกลุ่มงานย่อย	ใช้อธิบายบริบทขององค์กรในการมองภาพความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร และกระบวนการในการจัดการความเสี่ยงดังกล่าว แบ่งเป็น 4 ขั้น ได้แก่ ขั้นที่ 1 (Tier 1) คือ Partial เป็นขั้นที่มีพัฒนาการต่ำสุด ขั้นที่ 2 (Tier 2) คือ Risk Informed ขั้นที่ 3 (Tier 3) คือ Repeatable ขั้นที่ 4 (Tier 4) คือ Adaptive โดยแต่ละขั้น จะพิจารณาองค์กรใน 3 หมวด คือ 1. การบริหารจัดการความเสี่ยง 2. การบริหารจัดการความเสี่ยงแบบบูรณาการ 3. การร่วมมือกับหน่วยงานภายนอก	ใช้เป็นแผนภาพอธิบายโรดแม็ปขององค์กรในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดรับกับเป้าหมายขององค์กร และยังแสดงถึงลำดับการบริหารจัดการความเสี่ยงขององค์กร สามารถจัดทำเป็นหลายแผนภาพเพื่อใช้อธิบายโรดแม็ปได้ตามความซับซ้อนหรือความจำเป็นขององค์กร สามารถใช้เป็นเครื่องมือสื่อสารให้คนในองค์กรเข้าใจในภารกิจและเป้าหมายขององค์กร

ที่มา : ยุทธนา เจียมตระการ, 2561.

[5] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity". 2014.

สำหรับ Framework Core ที่เป็นกรอบการทำงานหลัก เริ่มแรกมีจุดประสงค์ที่จะใช้ระบุ ประเมิน และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานในอุตสาหกรรมโครงสร้างพื้นฐานสำคัญทั้ง 16 กลุ่มที่กล่าวมาข้างต้น แต่ต่อมาได้มีการนำไปใช้กับองค์กรทั่วไปอื่นๆ เช่นกัน ตัวอย่างของ Framework Core แสดงในตารางที่ 2-7

ตารางที่ 2-7 ตัวอย่าง Framework Core

Framework Core			
Function	**Category**	**Subcategory**	**Information References**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	**ID.AM-1:** Physical devices and systems within the organization are inventoried	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013

ตารางที่ 2-7 ตัวอย่าง Framework Core (ต่อ)

Framework Core			
Function	**Category**	**Subcategory**	**Information References**
			SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8

ที่มา : National Institute of Standards and Technology, 2014.

ในส่วนของ Framework Implementation Tiers ลักษณะของพัฒนาการการจัดการความเสี่ยงของทั้ง 4 ขั้นในแต่ละหมวด เป็นดังตารางที่ 2-8

ตารางที่ 2-8 FRAMEWORK IMPLEMENTATION TIERS

FRAMEWORK IMPLEMENTATION TIERS			
TIER	**การบริหารจัดการความเสี่ยง**	**การบริหารจัดการความเสี่ยงแบบบูรณาการ**	**การร่วมมือกับหน่วยงานภายนอก**
ขั้นที่ 1 (Partial)	ยังไม่มีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน / องค์กรอย่างเป็นทางการ เป็นเพียงแค่การแก้ไขสถานการณ์เฉพาะหน้าเท่านั้น	พนักงานส่วนใหญ่ยังไม่มีความตระหนักรู้เรื่องความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	ยังไม่มีกระบวนการทำงานร่วมกับหน่วยงานหรือองค์กรภายนอกอื่นๆ ในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
ขั้นที่ 2 (Risk Informed)	มีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	พนักงานมีความตระหนักรู้ในเรื่องความเสี่ยงด้านความมั่นคงปลอดภัย	มีกระบวนการทำงานร่วมกับหน่วยงานภายนอกและรู้บทบาท

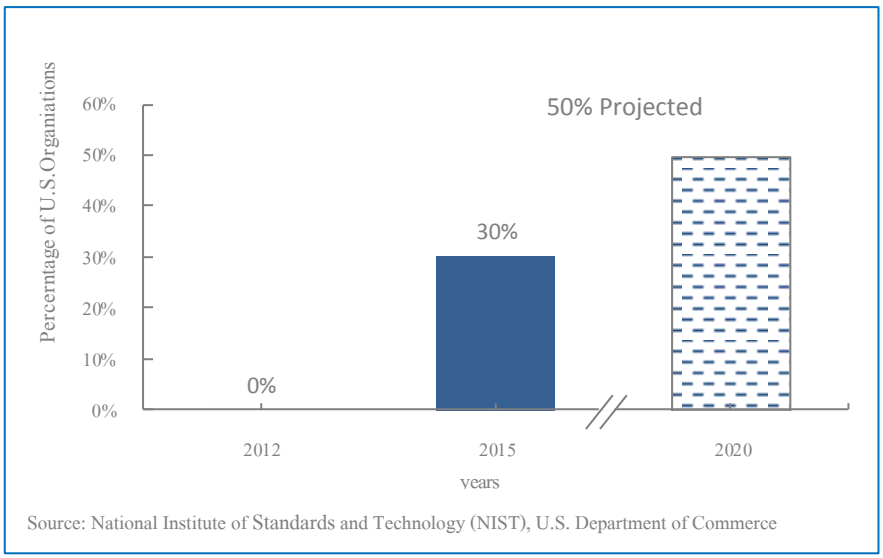
ตารางที่ 2-8 FRAMEWORK IMPLEMENTATION TIERS (ต่อ)

FRAMEWORK IMPLEMENTATION TIERS			
TIER	**การบริหารจัดการความเสี่ยง**	**การบริหารจัดการความเสี่ยงแบบบูรณาการ**	**การร่วมมือกับหน่วยงานภายนอก**
	แต่ยังไม่ได้ถูกนำมาใช้เป็นกฎทั่วไปในหน่วยงาน / องค์กร	ไซเบอร์ แต่ยังไม่ทั่วถึงทั้งหน่วยงาน / องค์กร (Organization-wide)	หน้าที่ของตน แต่ยังไม่มีการกำหนดวิธีการทำงานร่วมกับหน่วยงาน / องค์กรภายนอกอย่างเป็นรูปธรรม
ขั้นที่ 3 (Repeatable)	รูปแบบการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ได้รับการอนุมัติจากผู้บริหารอย่างเป็นทางการ และได้ถูกนำมาใช้เป็นนโยบายในหน่วยงาน / องค์กร	พนักงานมีความตระหนักรู้ในเรื่องความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงาน / องค์กรมีมาตรการบริหารจัดการความเสี่ยงครอบคลุมทุกส่วนงาน	มีกระบวนการทำงานร่วมกัน และมีการรับข้อมูลข่าวสารจากหน่วยงาน / องค์กรภายนอก เพื่อนำไปใช้ในการรับมือภัยคุกคามไซเบอร์
ขั้นที่ 4 (Adaptive)	มีการปรับปรุงนโยบายและมาตรการบริหารจัดการภัยคุกคามไซเบอร์อย่างสม่ำเสมอ และพร้อมรับมือภัยคุกคาม	การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ถือเป็นส่วนหนึ่งของวัฒนธรรมหน่วยงาน / องค์กร	มีกระบวนการทำงานร่วมกันและมีการแลกเปลี่ยนข้อมูลข่าวสารกับหน่วยงาน / องค์กรภายนอก เพื่อนำไปใช้ในการเตรียมพร้อมก่อนเกิดเหตุภัยคุกคาม

ที่มา : ยุทธนา เจียมตระการ, 2561.

ทั้งนี้ มีข้อมูลที่เผยแพร่ในเว็บไซต์ของ NIST[6] ระบุไว้ว่าในปี พ.ศ. 2560 หน่วยงานของ NIST ได้จัด Workshop ขึ้นอีกครั้งเพื่อรับข้อมูลป้อนกลับจากองค์กรและหน่วยงานในสหรัฐอเมริกาที่มีส่วนเกี่ยวข้องกับการนำกรอบการทำงานด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ที่ NIST ได้พัฒนาขึ้นไปใช้ โดยจะนำข้อมูลที่ได้มาใช้ปรับปรุงกรอบการทำงานให้มีความทันสมัยขึ้น และคาดว่าจะมีการประกาศใช้กรอบการทำงานที่ปรับปรุงใหม่เร็วๆ นี้ นอกจากนี้ เว็บไซต์ดังกล่าว ยังระบุผลสำรวจองค์กรในสหรัฐอเมริกาที่มีการนำกรอบการทำงานด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ของ NISTไปประยุกต์ใช้ โดยในปี พ.ศ. 2559 มีองค์กรที่นำไปใช้แล้ว 30% และมีการคาดการณ์ว่าจะเพิ่มขึ้นเป็น 50% ในปี พ.ศ. 2563 ดังแสดงในแผนภาพที่ 2-2

แผนภาพที่ 2-2 Cybersecurity Framework Usage



ที่มา : National Institute of Standards and Technology, 2017.

[6]"NIST Impacts: Cybersecurity". (Online). Available : www.nist.gov/industry-impacts/cybersecurity, 2017.

3. มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC27001: 2013)

มาตรฐาน ISO/IEC 27001:2013 เป็นมาตรฐานที่ถูกพัฒนาขึ้นร่วมกันระหว่างองค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (the International Organization for Standardization : ISO) และคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอเทคนิกส์ (The International Electro technical Commission: IEC) เพื่อเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศที่องค์กรทุกรูปแบบ ทุกขนาด สามารถนำไปใช้ได้ มาตรฐานนี้มีการพัฒนาต่อเนื่องเพื่อให้ทันสมัยและเข้ากับบริบทความมั่นคงปลอดภัยสารสนเทศของโลกที่เปลี่ยนแปลงไป สำหรับฉบับปัจจุบันเป็นฉบับที่ 3 ได้เริ่มใช้มาตั้งแต่วันที่ 1 ตุลาคม พ.ศ. 2556[7] โดยมีเนื้อหาแบ่งเป็น 2 ส่วน ดังแสดงในตาราง 2-9

ตารางที่ 2-9 มาตรฐานระบบความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001: 2013)

มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013)	
ส่วนที่ 1: ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	**ส่วนที่ 2: มาตรการควบคุมการดำเนินการตามระบบ**
ประกอบด้วยข้อกำหนดที่ต้องมีการดำเนินการ 7 เรื่อง คือ 1. **<u>บริบทองค์กร</u>**: ขอบเขตและกระบวนการของระบบขององค์กร ความจำเป็นและความคาดหวังจากผู้เกี่ยวข้อง 2. **<u>ภาวะผู้นำ</u>**: บทบาทผู้นำของผู้บริหาร สิ่งที่ผู้บริหารให้ความสำคัญเกี่ยวกับระบบ การกำหนดนโยบาย บทบาท ความรับผิดชอบ และอำนาจหน้าที่ของผู้รับผิดชอบต่อระบบ 3. **<u>การวางแผน</u>**: การประเมินความเสี่ยงและโอกาส การจัดการความเสี่ยง การวางแผนและกำหนดวัตถุประสงค์ในการดำเนินการ	ถูกกำหนดไว้ในภาคผนวกของมาตรฐาน มีการอธิบายวัตถุประสงค์ของการควบคุมและการดำเนินการในการควบคุมให้เป็นไปตามวัตถุประสงค์ดังกล่าว องค์กรจะต้องพิจารณามาตรการควบคุมทั้งหมด แต่จะนำมาใช้หรือไม่ก็ได้ กรณีที่จะไม่นำมาตรการควบคุมใดมาใช้ องค์กรต้องมีการระบุเหตุผลกำกับไว้ องค์กรสามารถกำหนดมาตรการควบคุมอื่นนอกเหนือจากที่กำหนดไว้ได้ โดยเป็นไปตามขอบเขตในบริบทขององค์กร

[7] International Organization for Standardization. “ISO/IEC 27001 Information technology Security techniques — Information security management systems — Requirements”. 2013.

ตารางที่ 2-9 มาตรฐานระบบความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001: 2013) (ต่อ)

มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013)	
ส่วนที่ 1: ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	**ส่วนที่ 2: มาตรการควบคุมการดำเนินการตามระบบ**
4. **<u>การให้การสนับสนุน</u>**: การจัดสรรทรัพยากรที่จำเป็น การพัฒนาความสามารถและการสร้างความตระหนักรู้ให้แก่บุคลากร การสื่อสารทั้งภายในและภายนอก การจัดการและควบคุมสารสนเทศ 5. **<u>การดำเนินการ</u>**: การจัดการความเสี่ยง ตั้งแต่ประเมิน วางแผน ลงมือปฏิบัติ และควบคุมกระบวนการ 6. **<u>การประเมินประสิทธิภาพและประสิทธิผล</u>**: การเฝ้าระวัง การวัดผล การวิเคราะห์ การประเมินผล การจัดให้มีการตรวจประเมินภายใน และการทบทวนระบบโดยผู้บริหาร 7. **<u>การปรับปรุง</u>**: การแก้ไขการดำเนินการที่ไม่สอดคล้องตามระบบ และการปรับปรุงระบบอย่างต่อเนื่อง	

ที่มา : ยุทธนา เจียมตระการ, 2561.

ทั้งนี้ เมื่อเดือนพฤษภาคม พ.ศ. 2560 ที่ผ่านมา คณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านการสื่อสารมวลชน ได้เสนอว่า การปฏิรูปโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ รัฐจะต้องกำหนดโครงสร้างพื้นฐานสำคัญของชาติ และมีนโยบายคุ้มครองโครงสร้างพื้นฐานที่สำคัญ และควรกระตุ้นให้องค์กรภาครัฐและภาคเอกชน นำมาตรฐานระบบบริหารงานคุณภาพ ISO 27001 มาใช้ในองค์กรให้มากขึ้น รวมทั้งการนำแนวทางปฏิบัติที่ใช้พิจารณาระดับความปลอดภัยทางไซเบอร์ของสหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU มา

เป็นแนวทางปฏิบัติ ตลอดจนกระตุ้นให้องค์กรทั้งภาครัฐและภาคเอกชนคำนึงถึงการรักษาความมั่นคงปลอดภัยของเครือข่ายไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญของประเทศ[8]

ผลงานวิจัย และผลสำรวจของประเทศไทยและต่างประเทศ

1. งานวิจัยของนักศึกษา วปอ. ด้านการสร้างความมั่นคงปลอดภัยไซเบอร์

1.1 งานวิจัยเรื่องการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันและการพัฒนามาตรการการรักษาความปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ

รัฐพล ภักดีภูมิ (2559) ได้ทำการวิจัยเพื่อหาแนวทางการพัฒนามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยงานวิจัยนี้กล่าวถึงรายงานของ The Information Security Forum (ISF) ที่ออกในปี พ.ศ. 2559 ซึ่งแนะนำว่า การสร้างความมั่นคงปลอดภัยไซเบอร์จะต้องใช้ทั้งแนวทางการปกป้องหรือการป้องกัน (Protect and Prevent) ร่วมกับ แนวทางการเตรียมความพร้อมและความสามารถในการตอบสนอง (Readiness and Responsiveness) โดยต้องพิจารณาให้สอดคล้องกับยุคสมัยและสถานการณ์ที่กำลังเกิดขึ้น รวมทั้งกิจกรรมด้านไซเบอร์ในอนาคตขององค์กร ทั้งส่วนที่องค์กรดำเนินการเอง และส่วนที่ผ่านผู้ให้บริการขององค์กร โดยปัจจัยสำคัญด้านการสร้างความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย คน กระบวนการ และ เทคโนโลยี (People, Process and Technology) ในส่วนของคน ต้องเตรียมให้พร้อมตลอดเวลาผ่านการอบรมและการซ้อมรับมือภัยทางไซเบอร์ (Cyber Drill) สำหรับประเทศไทย ผู้วิจัยได้ชี้ให้เห็นว่ายังมีปัญหาขาดแคลนบุคคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งควรมีการวางแผนรองรับต่อไป

1.2 งานวิจัยเรื่องยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

สุทธิศักดิ์ สลักคำ (2558) ได้ทำการวิจัยเพื่อเสริมสร้างศักยภาพด้านการป้องกันไซเบอร์ของกระทรวงกลาโหมในการรับมือภัยคุกคามจากไซเบอร์ โดยได้ศึกษาหน่วยงานด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ ของ 13 ประเทศ ได้แก่ อิสราเอล อิหร่าน สหรัฐอเมริกา เยอรมนี อังกฤษ สวีเดน จีน อินเดีย สิงคโปร์ มาเลเซีย พม่า เวียดนาม และประเทศไทย และสรุปแนวทางการป้องกันภัยไซเบอร์ที่มีการดำเนินการในประเทศต่างๆ ดังกล่าวออกมาได้รวม 9 เรื่อง คือ

---

[8] “สปท. เห็นชอบรายงานรักษาความมั่นคงปลอดภัยไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก : www.thaich8.com/news_detail/35152/สปท-เห็นชอบรายงานรักษาความมั่นคงปลอดภัยไซเบอร์, 2560.

1. มีการจัดตั้งหน่วยรับผิดชอบด้านไซเบอร์ขึ้นมาโดยเฉพาะ
2. มีการพัฒนาศักยภาพในการตอบสนองภัยจากไซเบอร์ โดยกำหนดเป็นนโยบาย และมีการพัฒนาทางเทคนิค
3. มีการประสานความร่วมมือทั้งในประเทศและต่างประเทศ
4. มีการสร้างความตระหนักรู้ในเรื่องไซเบอร์
5. มีการวิจัยและพัฒนาเทคนิค เพื่อให้พึ่งพาตนเองได้
6. ให้อำนาจรัฐในการตรวจสอบเนื้อหาหรือเข้าควบคุมเหตุฉุกเฉินทางไซเบอร์
7. กำหนดกฎหมาย ระเบียบ มาตรฐานด้านไซเบอร์
8. ปกป้องโครงสร้างพื้นฐาน โดยเฉพาะโครงสร้างพื้นฐานด้านสาธารณูปโภค
9. มีการดำเนินการเชิงรุก

ผู้วิจัยได้ชี้ให้เห็นว่า ประเทศไทยยังขาดการดำเนินการเชิงรุก และการให้อำนาจแก่รัฐในการตรวจสอบเนื้อหา หรือเข้าควบคุมเหตุฉุกเฉินทางไซเบอร์ และในส่วนของกระทรวงกลาโหมยังมีปัญหาความสามารถของบุคลากรที่รับผิดชอบงานด้านไซเบอร์ในเชิงรุกไม่เพียงพอ การขาดแคลนผู้เชี่ยวชาญ การประสานความร่วมมือกับหน่วยงานภายนอกและหน่วยงานของต่างประเทศมีความไม่ต่อเนื่อง เป็นต้น

1.3 งานวิจัยเรื่องการวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

อรัญ นำผล (2557) ได้ทำการวิจัยเพื่อหาแนวทางยกระดับขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของประเทศไทย โดยได้ชี้ให้เห็นว่าการพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ จำเป็นที่จะต้องดำเนินการทั้งด้านองค์บุคคล องค์วัตถุ และการบริหารจัดการ ร่วมกัน

ในส่วนองค์บุคคล ต้องมีการสร้างผู้เชี่ยวชาญด้านสงครามไซเบอร์ที่มีมาตรฐาน มีความสามารถในการปฏิบัติงานอย่างเพียงพอ รวมทั้งมีแผนให้ความรู้อย่างต่อเนื่องและต้องทำให้ประชาชนทั่วไปสามารถเข้าถึงองค์ความรู้นี้ได้

ในส่วนองค์วัตถุ ต้องสนับสนุนให้มีการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ได้เทคโนโลยีที่มีราคาถูกใช้อย่างเพียงพอ

ในส่วนการบริหารจัดการ หน่วยงานภาครัฐต้องบูรณาการการปฏิบัติการร่วมกันเพื่อให้สามารถทำงานประสานร่วมมือกันในการป้องกันภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ ต้องจัดให้มีหน่วยงานเฉพาะดูแลความมั่นคงด้านสงครามไซเบอร์โดยมีโครงสร้างการบริหารงาน บทบาทและหน้าที่ที่ชัดเจน ต้องปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติให้ทันสมัยสามารถบังคับใช้ได้จริง และรองรับการปฏิบัติงานของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ รวมทั้งต้องสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชนทั้งการแบ่งปันทรัพยากร การแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์ และการมีนโยบายสนับสนุนผู้ประกอบการด้านความมั่นคงปลอดภัยไซเบอร์

1.4 งานวิจัยเรื่องแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย

วิโรจน์ ธันวรักษ์กิจ (2557) ได้ทำการวิจัยเพื่อหาแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย ผู้วิจัยได้ชี้ให้เห็นว่า การจะทำให้การบริหารจัดการความมั่นคงปลอดภัยทางสารสนเทศของประเทศมีการดำเนินการอย่างเป็นรูปธรรมจากนโยบายและยุทธศาสตร์ไปสู่การปฏิบัติได้อย่างต่อเนื่องและเกิดประสิทธิผล จะต้องกำหนดหน่วยงานหลักที่มารองรับการดำเนินการของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee: NCSC) และต้องมีการบูรณาการงานของหน่วยงานภาครัฐที่เกี่ยวข้องในภาพรวม เพื่อไม่ให้เกิดการดำเนินการแบบแยกส่วนทั้งระดับนโยบายและระดับปฏิบัติการ

ผู้วิจัยยังชี้ให้เห็นว่า ประเทศไทยยังขาดแคลนบุคลากรที่เป็นผู้เชี่ยวชาญด้านไซเบอร์ที่ผ่านเกณฑ์ได้รับการรับรองด้านความสามารถเฉพาะ ทั้งของภาครัฐ และภาคเอกชน ซึ่งจำเป็นต้องมีการส่งเสริมการพัฒนาบุคลากรด้านนี้อย่างจริงจังทั้งในระดับนโยบายและระดับปฏิบัติการ และภาครัฐจะต้องกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญออกมาให้เป็นรูปธรรมและชัดเจน เพื่อลดความเสี่ยงของภัยคุกคามไซเบอร์ที่มีต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ และต้องรณรงค์ให้หน่วยงานหรือองค์กรที่เกี่ยวข้องเหล่านี้มีความตระหนักรู้ถึงความสำคัญและความเสี่ยงของตนเอง เพื่อดำเนินการปกป้ององค์กรจากภัยคุกคามดังกล่าวได้อย่างเหมาะสม

2. การสำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้สำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ของประเทศขึ้น แสดงใน Cybersecurity Survey 2016[9] เพื่อศึกษาและวิเคราะห์สถานภาพความมั่นคงปลอดภัย ปัญหา และแนวทางในการรับมือภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐและภาคเอกชน ทั้งนี้หน่วยงานภาครัฐ 370 หน่วยงาน ได้แก่ หน่วยงานของศาล กระทรวง ตั้งแต่ระดับกรมหรือเทียบเท่าขึ้นไป สำนักนายกรัฐมนตรี มหาวิทยาลัยของรัฐ รัฐวิสาหกิจ หน่วยงานอิสระของรัฐ องค์กรควบคุมการประกอบวิชาชีพ และองค์การมหาชน สำหรับหน่วยงานภาคเอกชน คัดเลือกจากประเภทของกลุ่มธุรกิจอุตสาหกรรมที่ให้มีวิธีการรักษาความปลอดภัยของธุรกรรมทางอิเล็กทรอนิกส์ในระดับเคร่งครัด ตามประกาศ

---

[9] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). “Cybersecurity survey 2016”. 2559.

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 รวม 547 หน่วยงาน ได้แก่ หน่วยงานด้านการชำระเงินอิเล็กทรอนิกส์ ด้านการเงินของธนาคารพาณิชย์ ด้านประกันภัย ด้านหลักทรัพย์ ด้านการให้บริการด้านสาธารณูปโภคและสาธารณะ หน่วยงานที่ต้องดำเนินการต่อเนื่องตลอดเวลา ที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ได้แก่ กลุ่มพลังงาน กลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร และกลุ่มขนส่งและโลจิสติกส์ และด้านการให้บริการที่จัดเก็บ รวบรวม และให้บริการข้อมูลบุคคลหรือทะเบียนต่างๆ ที่เป็นข้อมูลสาธารณะ ได้แก่ กลุ่มโรงพยาบาล-การแพทย์ (ขนาดมากกว่า 120 เตียงขึ้นไป และมีเว็บไซต์) โดยมีการจัดทำขึ้นระหว่างเดือนพฤษภาคม-สิงหาคม พ.ศ. 2559 เป็นการสำรวจวิจัยเชิงเปรียบเทียบ (Benchmarking Research) โดยใช้คำถามแบบมาตรวัดการประมาณค่า (Rating Scale) ตั้งแต่ 1-5 และมีการนำแนวคิดของ National Institute of Standards and Technology (NIST) ประเทศสหรัฐอเมริกามาประยุกต์เป็นส่วนหนึ่งของแบบสอบถาม

จากรายงานสำรวจสถานภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ อ้างถึงจากการจัดกลุ่มของ eCSIRT.net (The European Computer Security Incident Response Team Network) จำแนกเป็นประเภท 8 ประเภท ดังแสดงในตารางที่ 2-10

ตารางที่ 2-10 ประเภทเหตุภัยคุกคาม 8 ประเภท

ประเภทที่	ภัยคุกคาม	คำอธิบาย
INC 1	Abusive Content	เนื้อหาที่เป็นภัย ได้แก่ การถูกเผยแพร่ข้อมูลที่ไม่จริงและไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือ ก่อให้เกิดความเข้าใจผิด เช่น ข้อความลามกอนาจาร, Harassment Child / Sexual Violence, หมิ่นประมาท, อีเมลสแปม
INC2	Malicious Code	โปรแกรมไม่พึงประสงค์ ได้แก่ การถูกโปรแกมประสงค์ร้าย เช่น มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware, APT (Advanced Persistent Threat) และ Spyware ต่างๆ เข้าควบคุมการทำงานของระบบ เช่น ขโมยข้อมูล โจมตีระบบอื่นๆ ทำให้เกิดความขัดข้องเสียหาย
INC3	Information Gathering	ความพยายามรวบรวมข้อมูลของระบบ ได้แก่ การถูกรวบรวมข้อมูลจุดอ่อนของระบบ (Scanning) เช่น ข้อมูลปฏิบัติการ

ตารางที่ 2-10 ประเภทเหตุภัยคุกคาม 8 ประเภท (ต่อ)

ประเภทที่	ภัยคุกคาม	คำอธิบาย
		รวมถึงการดักรับข้อมูลเครือข่าย (Sniffing), Social Engineering
INC4	Information Security	ความมั่นคงปลอดภัยของระบบ ได้แก่ การเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาต (Unauthorized Access) หรือถูกเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized Modification) รวมไปถึงถูกเผยแพร่ข้อมูลที่รั่วไหล (Data Leakage)
INC5	Intrusion Attempts	ความพยายามบุกรุกเข้าระบบ เพื่อจะควบคุมหรือทำให้เกิดความขัดข้องกับบริการของระบบ เช่น การสุ่ม Login เข้าระบบ (Login Attempt), Exploiting Known Vulnerabilities, New Attack Signature, Brute Force Attempts, Firewall Authentication Command & Control, SQL Injection
INC6	Intrusions	การบุกรุกหรือเจาะระบบ ได้แก่ การถูกเข้าควบคุมหรือสั่งการระบบ จากการถูกเจาะระบบที่สำเร็จแล้ว เช่น การถูกปรับเปลี่ยนหน้าเว็บไซต์ (Web Defacement), Privilege Account Promise, Unprivileged Account Promise
INC7	Availability	ความพร้อมใช้งานของระบบ ได้แก่ การถูกโจมตีความพร้อมใช้งานของระบบ ทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้ เช่น DDoS (Denial of Service), Open DNS Resolver, Flood, Sabotage
INC8	Fraud	การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ ได้แก่ การถูกสร้างหน้าเว็บไซต์ปลอม (Web Phishing) เพื่อขโมยรหัสผ่านจากผู้ใช้, Unauthorized Use of Resources, Copyright, Masquerade

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560.

สำหรับเหตุภัยคุกคามที่สร้างความเสียหายให้แก่ภาครัฐในประเทศไทย แสดงไว้ในตารางที่ 2-11

ตารางที่ 2-11 เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดในภาครัฐ

ภาครัฐ	เหตุภัยคุกคามที่สร้างความเสียหายให้สูงสุด
หน่วยงานอิสระ	ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts)
หน่วยงานของศาล	การถูกบุกรุกหรือเจาะระบบ (Intrusions)
กระทรวง	โปรแกรมไม่พึงประสงค์ (Malicious Code)
สำนักนายกรัฐมนตรี	เนื้อหาที่เป็นภัย (Abusive Content)
องค์กรประกอบวิชาชีพ	ความพร้อมใช้งานของระบบ (Availability)
องค์การมหาชน	
รัฐวิสาหกิจ	
มหาวิทยาลัยของรัฐ	

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560.

และเหตุภัยคุกคาม ที่สร้างความเสียหายให้แก่ภาคเอกชนในประเทศไทย แสดงไว้ในตารางที่ 2-12

ตารางที่ 2-12 เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดในภาคเอกชน

ภาคเอกชน	เหตุภัยคุกคามที่สร้างความเสียหายให้สูงสุด
ธุรกิจการเงิน (Bank)	การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)
ธุรกิจหลักทรัพย์	การบุกรุกหรือเจาะระบบ (Intrusions) และ การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)
ธุรกิจการชำระเงิน (e-Payment)	ความพร้อมใช้งานของระบบ (Availability)
ธุรกิจประกันภัย	
พลังงาน	เนื้อหาที่เป็นภัย (Abusive Content)
โรงพยาบาล	โปรแกรมไม่พึงประสงค์ (Malicious Code)
เทคโนโลยีสารสนเทศและการสื่อสาร	
ขนส่งและโลจิสติกส์	

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560.

นอกจากนี้ยังได้มีการสำรวจระดับการจัดการความเสี่ยงขององค์กรภาครัฐและเอกชนดังกล่าว ใน 3 รูปแบบตามโมเดลของ NIST คือ

1. การจัดการความเสี่ยง (Risk Management)
2. การจัดการความเสี่ยงแบบบูรณาการ (Integrated Risk Management) และ
3. การร่วมมือกับหน่วยงานภายนอก (External Participation)

โดยสถานะการจัดการความเสี่ยง แบ่งเป็น 4 ระดับจากน้อยไปมาก คือ

ขั้นที่ 1. Partial

ขั้นที่ 2. Risk Informed

ขั้นที่ 3. Repeatable

ขั้นที่ 4. Adaptive

พบว่าระดับจัดการความเสี่ยงด้านความมั่นคงไซเบอร์ขององค์กรที่ได้รับการสำรวจส่วนใหญ่ อยู่ในระดับต่ำกว่า ขั้นที่ 4 ดังแสดงในตารางที่ 2-13

ตารางที่ 2-13 ผลระดับการจัดการความเสี่ยงขององค์กรภาครัฐและเอกชนด้านความมั่นคงปลอดภัยไซเบอร์

รูปแบบการจัดการ	ระดับการจัดการ
1. การจัดการความเสี่ยง	ขั้นที่ 3
2. การจัดการความเสี่ยงแบบบูรณาการ	ขั้นที่ 2
3. การร่วมมือกับหน่วยงานภายนอก	ขั้นที่ 1

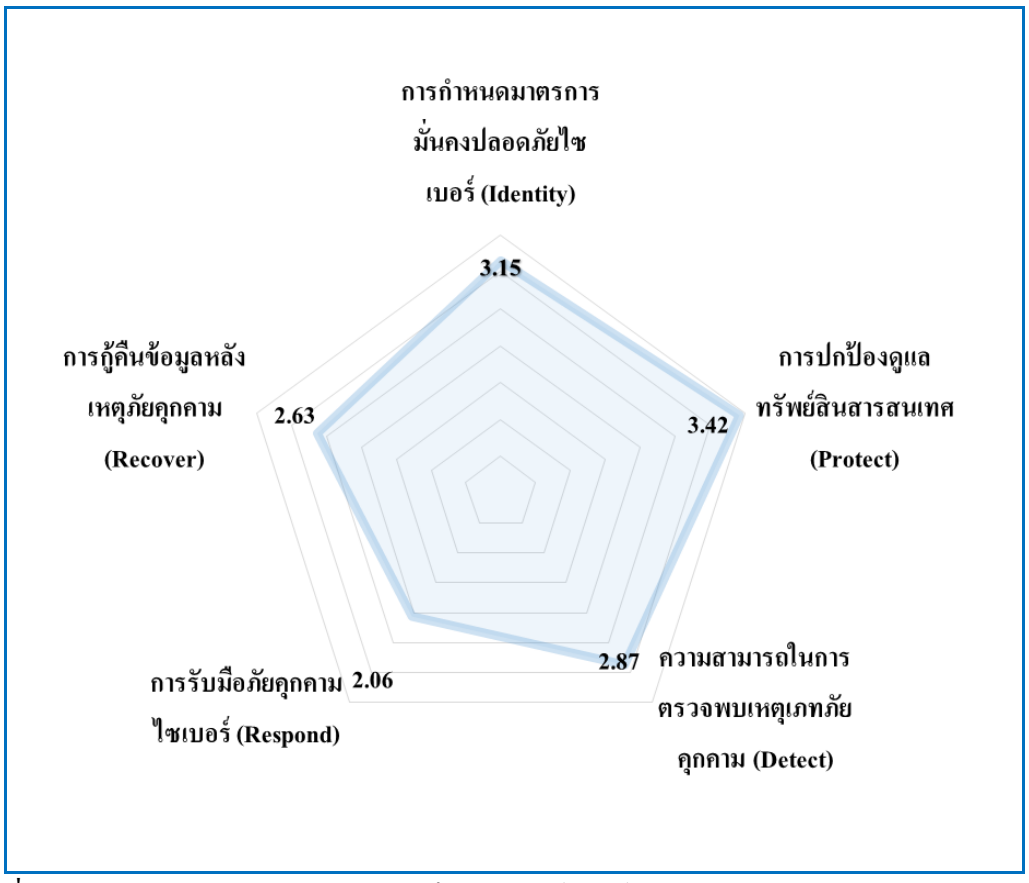
ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560.

รวมทั้งได้มีการสำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐและเอกชนดังกล่าวข้างต้น ภายใต้กรอบการทำงาน ของ NIST ได้แก่

1. การกำหนดมาตรการมั่นคงปลอดภัยไซเบอร์ (Identity)
2. การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)
3. ความสามารถในการตรวจพบเหตุเภทภัย (Detect)
4. การรับมือภัยคุกคามไซเบอร์ (Respond)
5. การกู้คืนข้อมูลหลังเหตุภัยคุกคาม (Recover)

โดยใช้ Rating Scale 1-5 ผลคะแนนเฉลี่ยที่ได้ แสดงดังแผนภาพที่ 2-3

แผนภาพที่ 2-3 คะแนนเฉลี่ย สถานภาพความมั่นคงปลอดภัยไซเบอร์ขององค์กรภาครัฐและเอกชน



ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560.

หากพิจารณาผลการสำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ขององค์กรภาครัฐและเอกชนข้างต้น จะพบว่ามีประเด็นที่ควรปรับปรุงเพื่อเพิ่มความมีประสิทธิผลและประสิทธิภาพ ในทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ดังแสดงในตารางที่ 2-14

ตารางที่ 2-14 การดำเนินงานและประเด็นควรปรับปรุงเพื่อเพิ่มความมีประสิทธิผลและประสิทธิภาพในทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์องค์กรต่างๆ ในประเทศไทย

กรอบการทำงานที่	หัวข้อ	การดำเนินงานส่วนใหญ่	ประเด็นที่ควรปรับปรุง
1.	การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)	มีการดำเนินการกระบวนการบริหารจัดการความเสี่ยง (Risk Management) ภายในองค์กร	ขาดการดำเนินการเรื่องมาตรการควบคุมดูแลด้านกฎหมาย สภาพแวดล้อม ขาดการกำหนดบทบาทและความรับผิดชอบของพนักงาน ขาดการกำหนดเป้าหมายและวัตถุประสงค์ขององค์กรด้านการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์
2.	การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)		
2.1	ด้านการควบคุมเข้าถึงข้อมูล (Access Control)	มีการควบคุมการเข้าถึงข้อมูล (Access Control)	มีการจัดการที่น้อยลงในสิ่งที่ดำเนินการได้ยากหรือซับซ้อนขึ้น เช่น การควบคุมเข้าถึงพื้นที่สำคัญ การควบคุมการใช้งานระยะไกล (Remote Access) การให้สิทธิ์การเข้างาน การแยกสิทธิ์การใช้งาน (Network Segregation)
2.2	ด้านการฝึกอบรมและการสร้างความตระหนักรู้ (Awareness and Training)	มีการให้ความสำคัญในการฝึกอบรมเพื่อสร้างความเข้าใจบทบาทและหน้าที่ความรับผิดชอบนโยบายและ	มีการให้ความสำคัญในการสื่อสารหรือฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับพนักงานหรือ

ตารางที่ 2-14 การดำเนินงานและประเด็นควรปรับปรุงเพื่อเพิ่มความมีประสิทธิผลและประสิทธิภาพในทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์องค์กรต่างๆ ในประเทศไทย (ต่อ)

กรอบการทำงานที่	หัวข้อ	การดำเนินงานส่วนใหญ่	ประเด็นที่ควรปรับปรุง
		มาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในระดับผู้บริหารสูงมากที่สุด	ผู้ใช้งานทั่วไป (All Users) น้อย
2.3	ด้านความมั่นคงปลอดภัยของข้อมูล (Data Security)	มีมาตรการป้องกันข้อมูลไม่ให้ถูกเข้าถึงโดยไม่ได้รับอนุญาตหรือถูกนำไปใช้ผิดประเภท มีการป้องกันการรั่วไหล มีกลไกในการตรวจสอบความถูกต้องของข้อมูล	ไม่ให้ความสำคัญในเรื่องการลบทิ้ง (Removal) เคลื่อนย้าย (Transfer) ทำลายข้อมูลอิเล็กทรอนิกส์ (Disposition) เท่าที่ควร
2.4	ด้านกระบวนการปกป้องข้อมูล (Information Protection Processes & Procedures)	นิยมการใช้มาตรการสำรองข้อมูล (Backups) มากที่สุด	ไม่เน้น หรือมีการดำเนินงานน้อยที่สุดในเรื่องการทำลายข้อมูลหรืออุปกรณ์บันทึกความลับที่เสี่ยงต่อความมั่นคงปลอดภัยไซเบอร์
2.5	ด้านการบำรุงทรัพย์สินสารสนเทศ (Maintenance)	ให้ความสำคัญกับการดูแลและซ่อมบำรุงทรัพย์สินสารสนเทศ (Maintenance and Repair)	ให้ความสำคัญน้อยกว่ามากในการป้องกันการเข้าถึงทรัพย์สินสารสนเทศ
2.6	ด้านการใช้เทคโนโลยีเพื่อปกป้องทรัพย์สินสารสนเทศ (Protection Technology)	เน้นการดำเนินงานในด้านการใช้เทคโนโลยีเพื่อป้องกันการโจมตีทางเครือข่ายและเรื่อง	ให้ความสำคัญกับการจำกัดและป้องกันการใช้อุปกรณ์บันทึกแบบ Removable Media น้อยมาก

ตารางที่ 2-14 การดำเนินงานและประเด็นควรปรับปรุงเพื่อเพิ่มความมีประสิทธิผลและประสิทธิภาพในทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์องค์กรต่างๆ ในประเทศไทย (ต่อ)

กรอบการทำงานที่	หัวข้อ	การดำเนินงานส่วนใหญ่	ประเด็นที่ควรปรับปรุง
		การเก็บบันทึกข้อมูล (Audit log)	อาจเนื่องจากไม่ตระหนักว่าเป็นความเสี่ยง
3.	ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ (Detect)	มีกลไกการเฝ้าระวัง (Monitor) เหตุภัยคุกคาม มีความสามารถในการตรวจพบเหตุภัยคุกคาม	ขาดความก้าวหน้าในเรื่องการทดสอบและปรับปรุงกระบวนการตรวจสอบเหตุภัยคุกคาม ขาดความสามารถในการวิเคราะห์เหตุที่เกิดขึ้นทั้งเป้าหมายและวิธีการโจมตี
4.	การรับมือภัยคุกคามไซเบอร์ (Respond)	มีการดำเนินงานบ้าง โดยส่วนใหญ่เป็นเรื่องของการจัดทำมาตรการ เช่น มาตรการและกระบวนการรับมือภัยคุกคามไซเบอร์ มาตรการป้องกันการลุกลามของภัยคุกคาม และมีการปรับปรุงแผนรับมือภัยคุกคามอยู่เสมอ	ส่วนใหญ่ยังไม่ได้มีการปฏิบัติในด้านการรับมือภัยคุกคามไซเบอร์ (No Implementation) ขาดการอบรมทีมรับมือภัยคุกคามไซเบอร์ ขาดการเพิ่มความสามารถในการวิเคราะห์สาเหตุภัยคุกคาม ขาดการจัดตั้งทีมรับมือภัยคุกคามไซเบอร์ (Incident Response Team)
5.	การกู้คืนข้อมูลและระบบหลังเหตุภัยคุกคามไซเบอร์ (Recover)	มีการดำเนินงานในด้านการมีแผนการกู้คืนข้อมูลและระบบ (Recovery Plan) ทั้ง	ขาดความร่วมมือกับส่วนงานที่เกี่ยวข้องต่างๆ ในกระบวนการฟื้นฟูข้อมูล

ตารางที่ 2-14 การดำเนินงานและประเด็นควรปรับปรุงเพื่อเพิ่มความมีประสิทธิผลและประสิทธิภาพในทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์องค์กรต่างๆ ในประเทศไทย (ต่อ)

กรอบการทำงานที่	หัวข้อ	การดำเนินงานส่วนใหญ่	ประเด็นที่ควรปรับปรุง
		ระหว่างเกิดเหตุและหลังเกิดเหตุภัยคุกคาม มีการปรับปรุงแผนการกู้คืนข้อมูลอยู่เสมอ มีการสื่อสารในองค์กรเพื่อให้ทราบถึงการกู้คืนระบบหลังเกิดเหตุภัยคุกคาม	

ที่มา : ยุทธนา เจียมตระการ, 2561.

จากผลสำรวจและข้อควรปรับปรุงเพื่อเพิ่มความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยเมื่อปี พ.ศ. 2559 ดังกล่าว ยังไม่พบว่ามีการติดตามการปฏิบัติเพื่อการยกระดับไว้ที่ใด

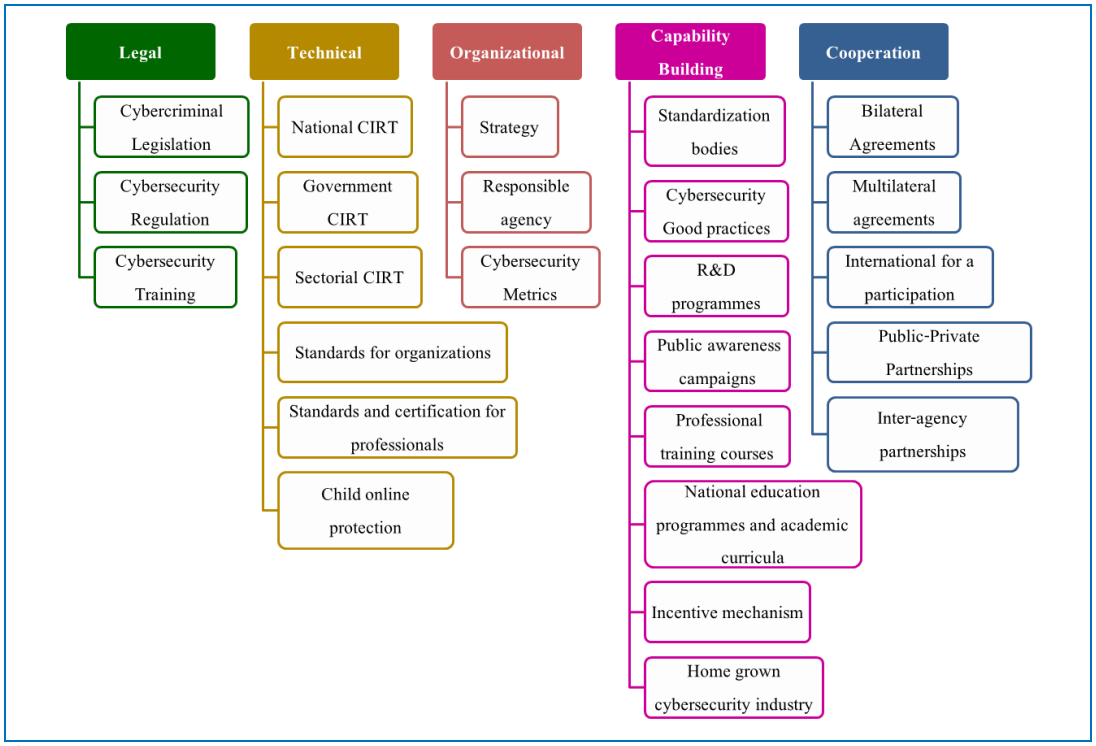
3. การสำรวจดัชนีความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ

International Telecommunication Union (ITU) ได้มีการสำรวจและจัดอันดับประเทศสมาชิก 193 ประเทศ ในเรื่องความมุ่งมั่นในการรับมือภัยคุกคามทางไซเบอร์ ภายใต้เสาหลัก (Pillar) ทั้ง 5 คือ เรื่อง

1. กฎหมาย (Legal)
2. เทคนิค (Technical)
3. องค์กร (Organization)
4. การสร้างความสามารถ (Capability Building)
5. ความร่วมมือ (Cooperation)

การสำรวจนี้ทำขึ้นครั้งแรกในปี พ.ศ. 2556-2557 และล่าสุดในปี พ.ศ. 2559-2560 โดยแสดงในรูปของ Global Cybersecurity Index (GCI)[10] ที่แสดงรูปของ GCI Pillar ทั้ง 5 และ Sub-Pillar ทั้ง 25 เพื่อนำไปใช้ในการเปรียบเทียบเพื่อการปรับปรุง ดังแสดงในแผนภาพที่ 2-4

แผนภาพที่ 2-4 GCI Pillar และ Sub-Pillar

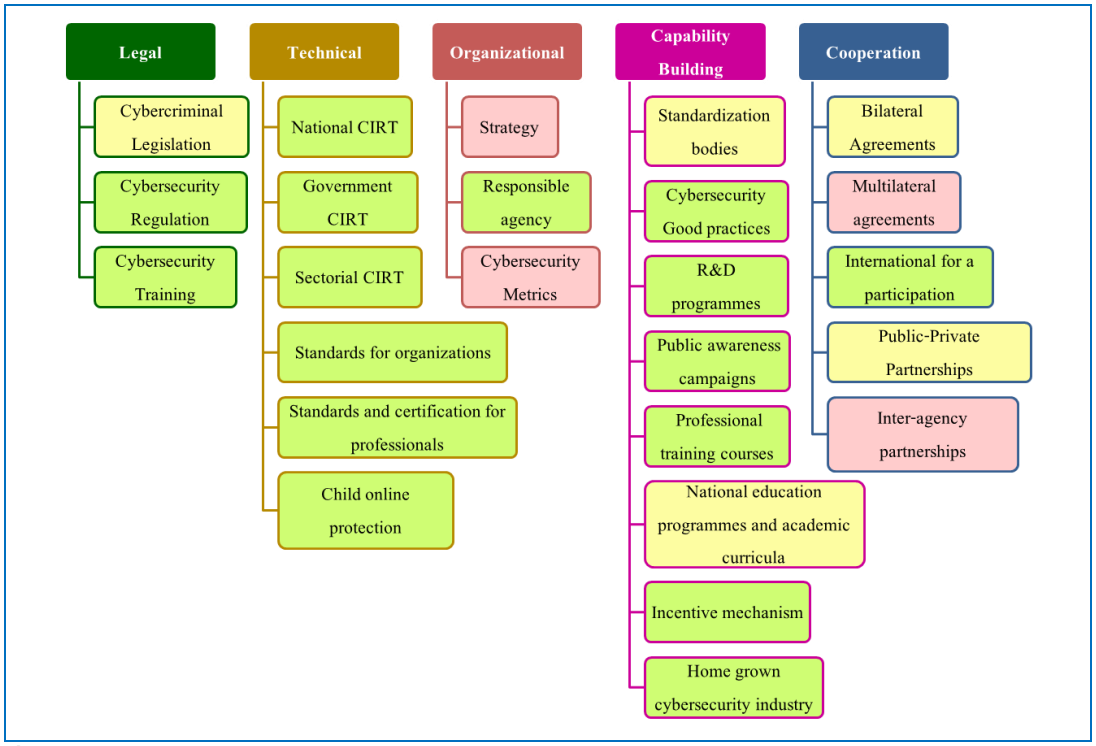


ที่มา : International Telecommunication Union, 2017.

จากผลการสำรวจดังกล่าวนำมาสู่การจัดกลุ่มประเทศสมาชิก เป็น 3 ประเภท คือ ระดับเริ่มต้น (Initiating Stage) จำนวน 96 ประเทศ ระดับกำลังเติบโต (Maturing State) จำนวน 77 ประเทศ และระดับผู้นำ (Leading Stage) จำนวน 21 ประเทศ โดยประเทศไทยได้คะแนนเป็นอันดับที่ 22 ของโลก และอยู่ในระดับกำลังเติบโต (Maturing State) และหากพิจารณาคะแนนตาม Global Cybersecurity Index (GCI) ของประเทศไทย ในระดับ Sub-Pillar จะพบว่ามีหัวข้อที่มีคะแนนอยู่ในระดับ Zone เขียว 16 รายการ ระดับ Zone เหลือง 5 รายการ และ ในระดับ Zone แดง 4 รายการ ดังแสดงใน แผนภาพที่ 2-5

[10] International Telecommunication Union. “Global Cybersecurity Index (GCI) 2017”. 2017.

แผนภาพที่ 2-5 การจำแนกกลุ่มหัวข้อ Sub-Pillar ตาม Zone เขียว-เหลือง-แดง ของประเทศไทย



ที่มา : ยุทธนา เจียมตระการ, 2561.

โดย Sub-Pillar ที่ได้คะแนนที่อยู่ในระดับ Zone สีแดง เป็นกลุ่มการดำเนินงานที่ได้คะแนนต่ำกว่า 33rd Percentile ระดับ Zone สีเหลือง เป็นกลุ่มการดำเนินงานที่ได้คะแนนในระดับ 33rd- 65th Percentile สำหรับระดับ Zone สีเขียว เป็นกลุ่มการดำเนินงานที่ได้คะแนนระดับที่สูงกว่า 65th Percentile โดยเปรียบเทียบกับทุกประเทศที่รับการสำรวจ

จากข้อมูลนี้ ประเทศไทยสามารถนำมาใช้ประโยชน์ในการพิจารณากำหนดลำดับความสำคัญเร่งด่วนในการยกระดับในเรื่อง ความมั่นคงปลอดภัยไซเบอร์ได้

กรอบแนวคิดของการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพผ่านการวิเคราะห์ข้อมูลทั้งแบบปฐมภูมิและทุติยภูมิ เพื่อสำรวจสถานภาพความมั่นคงปลอดภัยและการจัดการระบบไซเบอร์ของอุตสาหกรรมขนาดใหญ่ผ่านองค์กรตัวอย่าง และเสนอแนะแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับภาคธุรกิจ เพื่อให้การจัดการมีประสิทธิผลและประสิทธิภาพ ทั้งยังเพิ่มโอกาสในการบรรลุความสำเร็จตามยุทธศาสตร์ชาติที่เกี่ยวข้อง โดยดำเนินการดังนี้

1. ศึกษาสาระและความเชื่อมโยงของ ยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ
2. สำรวจแนวทางในการจัดการ รวมทั้งข้อพึงปฏิบัติ และข้อจำกัดต่างๆ จากกรอบการดำเนินงาน มาตรฐาน รายงานสำรวจ และงานวิจัย ที่เกี่ยวข้อง
3. สำรวจประสิทธิผลและประสิทธิภาพ การจัดการขององค์กรในอุตสาหกรรมขนาดใหญ่ รวมทั้งสัมภาษณ์ความเห็นและแนวคิดจากผู้ทรงคุณวุฒิเพิ่มเติม
4. วิเคราะห์ข้อมูลที่ได้จากข้อ 1-3 เพื่อหาแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิผลและประสิทธิภาพยิ่งขึ้น ในระดับนโยบายและการปฏิบัติสำหรับภาคธุรกิจและนโยบายระดับประเทศ โดยสะท้อนจากองค์กรตัวอย่าง

สรุป

จากการทบทวนวรรณกรรมในครั้งนี้ จะเห็นได้ว่า ประเทศไทยให้ความสำคัญกับการสร้างความมั่นคงปลอดภัยไซเบอร์ มีการกำหนดไว้ในยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ นอกจากนี้จากงานวิจัยและงานสำรวจต่างๆ ได้แสดงให้เห็นถึงความมุ่งมั่นระดับประเทศในการสร้างความมั่นคงปลอดภัยไซเบอร์เช่นกัน อย่างไรก็ตาม ภัยคุกคามไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลาและมีระดับความรุนแรงที่เพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยี ทำให้โอกาสที่ภาครัฐและภาคธุรกิจเผชิญกับภัยนี้เป็นไปได้สูง โดยเฉพาะเมื่อประเทศไทยในยุคไทยแลนด์ 4.0 ที่รัฐส่งเสริมให้ทุกภาคส่วนนำเทคโนโลยีมาใช้เพื่อเพิ่มมูลค่าของการผลิตและการบริการ อย่างไรก็ตาม ที่ผ่านมาจะเน้นศึกษาการดำเนินการของภาครัฐเป็นหลัก จึงจำเป็นต้องศึกษาการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ในภาคธุรกิจเพิ่มเติม โดยเฉพาะอย่างยิ่งในอุตสาหกรรมขนาดใหญ่ ที่สามารถส่งผลกระทบต่อเศรษฐกิจและความมั่นคงของประเทศ เพื่อหาแนวทางการจัดการให้มีประสิทธิผลและประสิทธิภาพยิ่งขึ้น

บทที่ 3
การศึกษาการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ในอุตสาหกรรมขนาดใหญ่

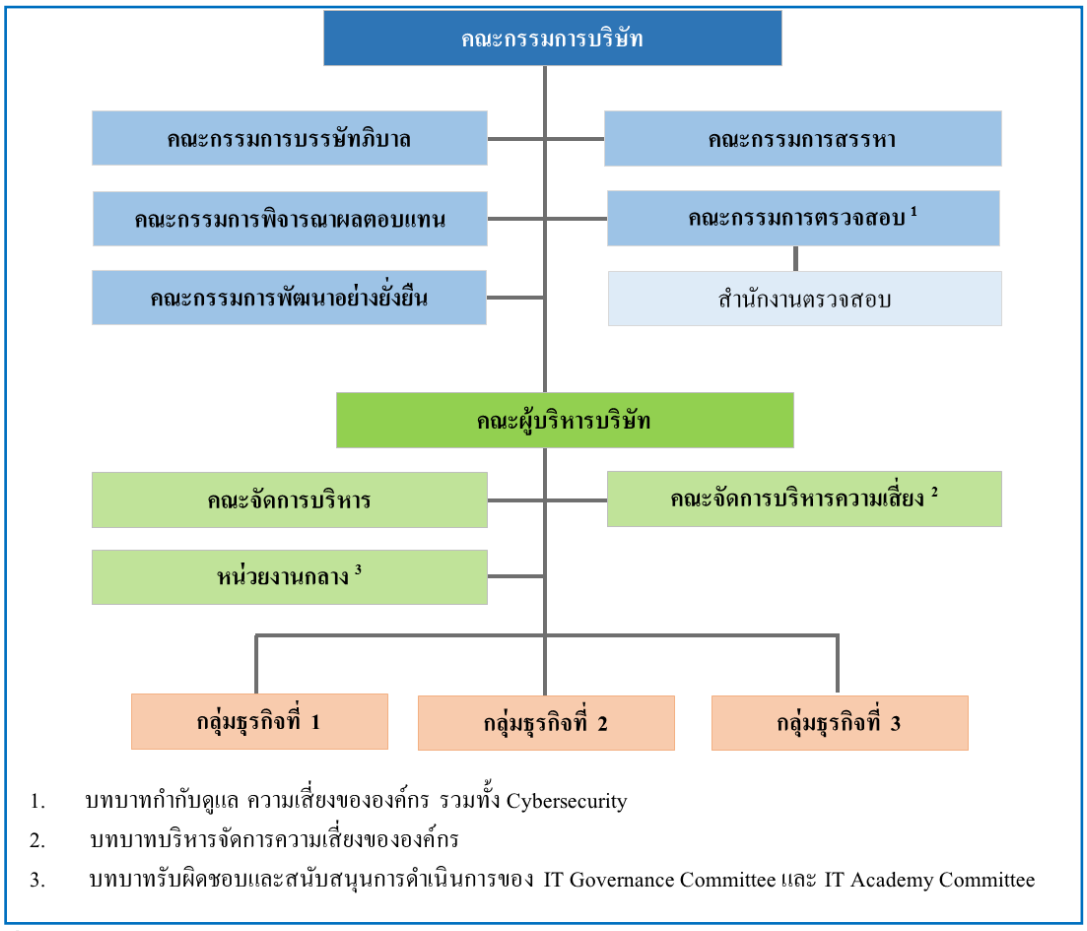
การสร้างความมั่นคงปลอดภัยไซเบอร์ขององค์กรตัวอย่าง

1. ลักษณะและโครงสร้างการบริหารขององค์กร

องค์กรตัวอย่าง (ต่อไปนี้จะแทนด้วย “องค์กร”) เป็นบริษัทไทยที่มีอายุมากกว่า 100 ปี ต่อมามีการขยายงานไปสู่ต่างประเทศ และมีการลงทุนในอาเซียน ดำเนินกิจการในหลากหลายธุรกิจ เช่น ผลิตภัณฑ์ก่อสร้าง จัดจำหน่าย เคมีภัณฑ์ บรรจุภัณฑ์และโลจิสติกส์ เป็นต้น มีบริษัทย่อยมากกว่า 200 บริษัททั้งที่อยู่ในประเทศไทยและต่างประเทศ มีสินทรัพย์รวมประมาณ 500,000 ล้านบาท มีรายได้จากการขายประมาณ 400,000 ล้านบาทต่อปี และมีพนักงานรวมประมาณ 50,000 คน

องค์กรดำเนินธุรกิจโดยยึดหลักการกำกับดูแลกิจการที่ดี มีการนำแนวปฏิบัติและการบริหารจัดการที่ดีและเป็นสากลมาใช้เพื่อเพิ่มขีดความสามารถการแข่งขันและสร้างความยั่งยืนให้แก่ธุรกิจอย่างต่อเนื่อง รวมทั้งได้เข้าร่วมเป็นสมาชิกองค์กรสากลระดับโลกด้านการบริหารจัดการและการพัฒนาเพื่อสร้างความยั่งยืน มีการจัดโครงสร้างการบริหารเพื่อให้เกิดธรรมาภิบาลในการประกอบธุรกิจ ประกอบด้วย คณะกรรมการบริษัท ทำหน้าที่กำกับดูแลการดำเนินการตามนโยบายและจริยธรรมการดำเนินธุรกิจขององค์กร และคณะผู้บริหารบริษัท ทำหน้าที่กำหนดและดำเนินการตามนโยบายเพื่อสร้างการเติบโตและความมั่นคงให้แก่ธุรกิจ โดยคณะกรรมการตรวจสอบ คณะจัดการบริหารความเสี่ยง และหน่วยงานกลาง มีบทบาทในการกำกับดูแลการบริหารความเสี่ยง และการดำเนินการปฏิบัติในเรื่องความมั่นคงปลอดภัยไซเบอร์ ดังแสดงในแผนภาพที่ 3-1 โครงสร้างการบริหารงานขององค์กร

แผนภาพที่ 3-1 โครงสร้างการบริหารงานขององค์กร



ที่มา : ยุทธนา เจียมตระการ, 2561.

2. ขอบข่ายและการบริหารเทคโนโลยีสารสนเทศและไซเบอร์ในองค์กร

องค์กรให้ความสำคัญกับการพัฒนาและสร้างความเข้มแข็งให้แก่ธุรกิจอย่างต่อเนื่อง มีการนำเทคโนโลยีสารสนเทศและไซเบอร์มาใช้อย่างกว้างขวาง เพื่อเพิ่มประสิทธิผลและประสิทธิภาพของสินค้าและบริการ รวมถึงการปรับปรุงระบบงานภายใน ตั้งแต่โครงสร้างพื้นฐานการสื่อสารทั้งภายในและภายนอกองค์กร การเก็บ และรวบรวมข้อมูลตลอดสายโซ่ธุรกิจ การวางแผนการผลิตและการขนส่ง การเพิ่มผลผลิตในโรงงาน การควบคุมคุณภาพของกระบวนการผลิต การเพิ่มคุณภาพการให้บริการทั้งก่อนและหลังการขาย การซ่อมบำรุง เป็นต้น พนักงานจะมี User Account เฉพาะของตนเองเพื่อใช้ในการเข้าถึงระบบและบริการขององค์กร ตามสิทธิและความจำเป็นที่เกี่ยวข้องกับการปฏิบัติงาน และเพื่อให้การใช้งานเทคโนโลยีสารสนเทศและไซเบอร์เกิด

ความปลอดภัย องค์กรมีการออกนโยบายเกี่ยวกับเทคโนโลยีสารสนเทศ (e-Policy) เพื่อเป็นแนวทางในการใช้งานข้อมูล การปฏิบัติงาน การพัฒนา และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสม สอดคล้องกับกฎหมาย ตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง สำหรับทั้งพนักงาน และคู่ค้าธุรกิจ รวมทั้งได้มีการนำมาตรฐานด้านการบริหารจัดการเทคโนโลยีสารสนเทศอย่างปลอดภัย คือ ISO 27001 มาใช้เป็นกรอบในการดำเนินการ

ในส่วนของการบริหารงานด้านเทคโนโลยีสารสนเทศและไซเบอร์ (ต่อไปนี้จะแทนด้วยคำว่า ITC) องค์กรมีการจัดโครงสร้างการบริหารเพื่อให้เกิดบูรณาการจากส่วนกลางและกลุ่มธุรกิจ โดยมีหน่วยงานกลางรับผิดชอบและให้การสนับสนุนคณะทำงาน ประกอบด้วย

1. IT Governance Committee รับผิดชอบกำหนดนโยบาย และแนวทางการใช้งานระบบ การติดตามโครงการลงทุนด้าน ITC ให้เป็นไปในแนวทางเดียวกันและสอดคล้องกับกลยุทธ์ทางธุรกิจ

2. IT Academy Committee รับผิดชอบกำหนด Standard Competency และแนวทางการพัฒนาความสามารถของพนักงานด้าน ITC ให้ได้ตามมาตรฐานสากล

3. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ในองค์กร

องค์กรมีการนำหลักการการบริหารความเสี่ยงเข้ามาใช้ โดยมีคณะกรรมการตรวจสอบกำกับดูแลความเสี่ยง และคณะจัดการบริหารความเสี่ยงบริหารจัดการความเสี่ยงขององค์กร มีการแบ่งความเสี่ยงเพื่อการจัดการเป็น 8 ประเภท[1] ดังแสดงในแผนภาพที่ 3-2

[1] เอสซีจี. รายงานการพัฒนาอย่างยั่งยืน 2559 เอสซีจี. (กรุงเทพฯ : เอสซีจี, 2560). หน้า 27.

แผนภาพที่ 3-2 ประเภทการบริหารจัดการความเสี่ยงขององค์กร

ที่มา : องค์กรตัวอย่าง, 2560 : 27.

ในการบริหารจัดการความเสี่ยงด้าน ITC นอกจากการประเมินความเสี่ยงจากกิจกรรมขององค์กรแล้ว องค์กรยังได้สำรวจภัยคุกคามไซเบอร์ที่เกิดขึ้นกับองค์กรอื่นทั้งที่อยู่ในอุตสาหกรรมแบบเดียวกัน และอุตสาหกรรมที่แตกต่าง เพื่อเรียนรู้และประเมินโอกาสเสี่ยงที่สามารถเกิดกับองค์กร และยังสามารถสร้างผลเสียหายต่อลูกค้า ผู้มีส่วนได้ส่วนเสีย และคู่ธุรกิจได้ ตัวอย่างภัยคุกคามไซเบอร์ที่เกิดขึ้นกับอุตสาหกรรมขนาดใหญ่ทั่วโลกระหว่างปี พ.ศ. 2553 - 2560 ที่องค์กรได้สำรวจ แสดงในตารางที่ 3-1

ตารางที่ 3-1 ตัวอย่างภัยคุกคามไซเบอร์ต่ออุตสาหกรรมขนาดใหญ่ระหว่างปี พ.ศ. 2553 - 2560

ลำดับ	ปี พ.ศ.	เหตุการณ์	ผลกระทบ
1[2]	2553	อาชญากรไซเบอร์ได้เจาะเข้าสู่ระบบบัญชีของบริษัทผลิตซิเมนต์แห่งหนึ่งในประเทศโรมาเนีย มีการโยกบัญชีใบอนุญาตปลดปล่อยก๊าซคาร์บอน (EU Emission Allowance) ของบริษัทที่อยู่ในตลาดซื้อขายการปลดปล่อยก๊าซคาร์บอนของสหภาพยุโรปไปจำนวน 1.6 ล้านหน่วย ไปยังบัญชีที่ไม่เปิดเผยในประเทศอิตาลีและลิชเต็นสไตน์	มูลค่าความเสียหายประมาณ 17 ล้านยูโร หรือ 720 ล้านบาท
2[3]	2554	มีบริษัทจำนวน 48 แห่งในอุตสาหกรรมเคมีและอุตสาหกรรมการป้องกันประเทศ ในสหรัฐอเมริกาและสหราชอาณาจักรถูกโจรกรรมข้อมูล ในเหตุการณ์ที่เรียกว่า Nitro Attacks โดยเป็นการโจรกรรมผ่านทางอีเมล์ปลอมที่ใช้หัวเรื่องเกี่ยวกับธุรกิจหรือการปรับปรุงข้อมูลด้านความปลอดภัย ที่แนบไฟล์มัลแวร์ชื่อ PoisonIvy ไปด้วย โดยเมื่อผู้รับเปิดไฟล์ ทำให้มัลแวร์ดังกล่าวถูกติดตั้ง	ข้อมูลทรัพย์สินทางปัญญา ได้แก่ เอกสารด้านการออกแบบ สูตรและรายละเอียดกระบวนการผลิตต่างๆ ที่มีมูลค่าสูงถูกโจรกรรม

[2] "Holcim mulls next move after EU court rejects carbon theft lawsuit". (Online). Available: https://www.reuters.com/article/uk-holcim-carbon/holcim-mulls-next-move-after-eu-court-rejects-carbon-theft-lawsuit-idUKKCN0HS1E720141003, 2010.

[3] "New cyber attack targets chemical firms: Symantec". (Online). Available: https://uk.reuters.com/article/us-cyberattack-chemicals/new-cyber-attack-targets-chemical-firms-symantec-idUSTRE79U4K920111031, 2011.

ตารางที่ 3-1 ตัวอย่างภัยคุกคามไซเบอร์ต่ออุตสาหกรรมขนาดใหญ่ระหว่างปี พ.ศ. 2553 - 2560 (ต่อ)

ลำดับ	ปี พ.ศ.	เหตุการณ์	ผลกระทบ
3[4]	2555	บริษัทที่อยู่ในอุตสาหกรรมน้ำมันแห่งหนึ่งในประเทศซาอุดิอาระเบียถูกไวรัสคอมพิวเตอร์ที่ชื่อว่า Shamoon โจมตี โดยเกิดจากเจ้าหน้าที่ในทีมไอที คนหนึ่ง เปิดลิงค์ในอีเมล์ที่มีสแปม ทำให้แฮ็กเกอร์เจาะเข้าระบบได้ และเป็นผลให้คอมพิวเตอร์ 35,000 เครื่องของบริษัทหยุดการทำงานทั้งหมด บริษัทต้องปิดระบบเครือข่ายคอมพิวเตอร์ และหยุดใช้งานอินเตอร์เน็ตในสำนักงานทั่วโลก	ระบบการทำงานของบริษัท เช่น การบริหารจัดการซัพพลายเออร์ การขนส่ง ฯลฯ ถูกทำลาย บริษัทต้องหยุดจำหน่ายน้ำมันภายในประเทศนาน 17 วัน และหยุดใช้งานระบบออนไลน์นาน 5 เดือน
4[5]	2556	ระบบคอมพิวเตอร์ของโรงงานผลิตกระดาษแห่งหนึ่งในสหรัฐอเมริกาถูกโจมตี ทำให้ระบบการทำงานล้มเหลว โดยการโจมตีครั้งนี้เกิดจากอดีตพนักงานผู้เชี่ยวชาญด้านไอที และเป็นผู้ดูแลระบบของบริษัทได้ลักลอบเชื่อมเข้าระบบของโรงงานผ่าน Virtual Private Network (VPN)	พนักงานรายนี้ถูกจับได้และรับโทษจำคุกเป็นเวลา 34 เดือน และบริษัทได้รับการชดเชยค่าเสียหายเป็นเงิน 1.1 ล้านเหรียญสหรัฐ หรือประมาณ 36 ล้านบาท
5[6]	2557	บริษัทแห่งหนึ่งในอุตสาหกรรมเหล็กประเทศเยอรมนีถูกโจมตีทางไซเบอร์โดยวิธีการหลอกลวงที่เรียกว่า Spear-phishing	ระบบการทำงานทั้งหมดของโรงงานล้มเหลว ไม่สามารถควบคุมการทำงาน

[4] "The inside story of the biggest hack in history". (Online). Available: http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html, 2015.

[5] "Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System". (Online). Available: https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer, 2017.

[6] "Cyberattack on a German steel-mill". (Online). Available: https://www.sentryo.net/cyberattack-on-a-german-steel-mill/, 2016.

ตารางที่ 3-1 ตัวอย่างภัยคุกคามไซเบอร์ต่ออุตสาหกรรมขนาดใหญ่ระหว่างปี พ.ศ. 2553 - 2560 (ต่อ)

ลำดับ	ปี พ.ศ.	เหตุการณ์	ผลกระทบ
		Attack ผ่านทางอีเมล์ปลอมที่มีไฟล์มัลแวร์ ทำให้แฮ็กเกอร์สามารถเจาะเครือข่ายทั้งหมดของโรงงานและการผลิต	ของเตาหลอมเหล็กด้วยวิธีปกติได้
6[7]	2559	บริษัทผลิตน้ำประปาแห่งหนึ่ง ถูกโจมตีทางไซเบอร์ผ่านการล็อกอินเข้าสู่ระบบปฏิบัติการ AS/400 รวม 4 ครั้ง ภายใน 60 วัน เพื่อเปลี่ยนแปลงส่วนประกอบของสารเคมีที่ใช้ในการผลิตน้ำประปา ทั้งนี้การล็อกอินระบบนี้สามารถทำได้ผ่านหน้าจอ Web-server หรือผ่านระบบชำระค่าบริการของบริษัท	ไม่เกิดผลกระทบเนื่องจากระบบการแจ้งเตือนของบริษัทสามารถตรวจพบและจัดการกับปัญหาได้ทันท่วงที จึงไม่กระทบต่อการให้บริการน้ำประปา
7[8]	2560	บริษัทให้บริการขนส่งสินค้าทางเรือรายใหญ่ที่สุดแห่งหนึ่งของโลก ถูกโจมตีโดย Ransomware สายพันธุ์ใหม่ ที่ชื่อว่า NotPetya ทำให้ระบบไอที ปิดการทำงาน ไม่สามารถรับคำสั่งการขนส่งสินค้า และท่าเรือของบริษัทในหลายประเทศไม่สามารถให้บริการได้	กำไรของบริษัทในไตรมาสเดียวลดลงประมาณ 300 ล้านเหรียญสหรัฐ หรือ 10,000 ล้านบาท

ที่มา : ยุทธนา เจียมตระการ, 2561.

จากตัวอย่างภัยคุกคามไซเบอร์ที่เกิดกับองค์กรอื่นข้างต้น ประกอบกับแนวโน้มภัยดังกล่าวสามารถเกิดขึ้นได้กับทุกอุตสาหกรรมในโลกอย่างไม่จำกัด ผู้บริหารระดับสูงขององค์กรตระหนักว่าภัยคุกคามนี้เป็นความเสี่ยงต่อทุกธุรกิจ ไม่ว่าจะเป็นธุรกิจผลิตภัณฑ์ก่อสร้าง เคมีภัณฑ์

[7] "Water treatment plant hacked, chemical mix changed for tap supplies". (Online). Available: https://www.theregister.co.uk/2016/03/24/water_utility_hacked/. 2016.

[8] "Maersk Says June Cyberattack Will Cost It up to $300 Million". (Online). Available : https://www.bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack -set-to-hurt-third-quarter, 2017.

บรรจุภัณฑ์ จัดจำหน่าย และโลจิสติกส์ จึงเป็นเรื่องที่ต้องให้ความสำคัญและต้องมีการจัดการที่ดี เพื่อไม่ให้กระทบต่อทั้งองค์กรและเครือข่ายในห่วงโซ่อุปทาน ได้แก่ ลูกค้า คู่ค้า ผู้ถือหุ้น ชุมชน และรวมถึงเศรษฐกิจของประเทศชาติ ประเด็นสำคัญคือ องค์กรต้องทราบสถานะการจัดการความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันว่ายังมีช่องโหว่และข้อควรปรับปรุงอย่างไร เพื่อกำหนดแผนงานและเป้าหมายดำเนินการให้อยู่ในระดับที่มั่นใจได้

ด้วยเหตุนี้ องค์กรจึงมอบหมายให้คณะ IT Governance Committee ว่าจ้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์มาตรวจประเมินเพื่อค้นหาช่องโหว่ของระบบการทำงานภายในที่เกี่ยวข้องกับ ITC โดยเฉพาะกิจกรรมของแต่ละธุรกิจที่มีความเสี่ยงสูง

4. การค้นหาความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ในองค์กร

คณะ IT Governance Committee ขององค์กรได้ดำเนินการคัดเลือกบริษัทผู้เชี่ยวชาญด้านการประเมินระบบความมั่นคงปลอดภัยไซเบอร์ โดยมีเกณฑ์คัดเลือกสำคัญ คือ

1. เป็นบริษัท Cybersecurity Consultant ระดับโลก ที่มีชื่อเสียงน่าเชื่อถือเป็นที่ยอมรับ มีจรรยาบรรณในการทำธุรกิจและรักษาความลับของลูกค้า

2. มีประสบการณ์ในการตรวจประเมินและให้คำแนะนำในภาคธุรกิจในอุตสาหกรรมขนาดใหญ่

3. มีทีมบุคลากรที่มีความเชี่ยวชาญเรื่องการจัดการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Technology Consulting) โดยเฉพาะอย่างยิ่งในเรื่อง Industrial Control System (ICS) และ Industrial Control Technology (ICT) ซึ่งเป็นหัวใจของธุรกิจ

4. มีใบรับรองคุณวุฒิ (Certificates) ที่เป็นที่ยอมรับในระดับมาตรฐานโลก

ภายหลังจากคัดเลือกบริษัทผู้เชี่ยวชาญด้านการประเมินระบบความมั่นคงปลอดภัยไซเบอร์ได้แล้ว องค์กรและบริษัทผู้เชี่ยวชาญฯ ได้วางแผนการตรวจประเมินร่วมกัน โดยเริ่มจากการสำรวจกิจกรรมทางธุรกิจ เพื่อคัดเลือกพื้นที่ของแต่ละกลุ่มธุรกิจที่จะเป็นโมเดลศึกษา (Pilot Area) และกลุ่มผู้ที่จะรับการสัมภาษณ์

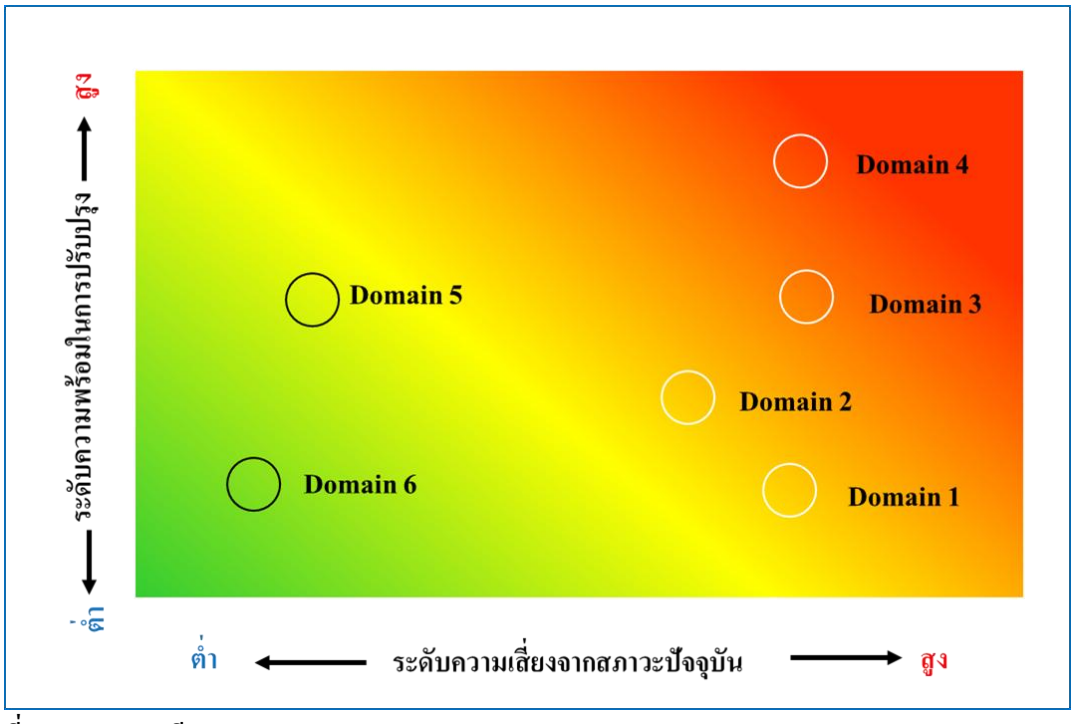
การดำเนินการเพื่อประเมินความเสี่ยงและค้นหาช่องโหว่ของระบบ ทีมงานของบริษัทผู้เชี่ยวชาญฯ มีการดำเนินกิจกรรมหลายด้าน เช่น การสัมภาษณ์ผู้เกี่ยวข้อง (ผู้บริหาร ผู้ดูแลระบบ และพนักงานหน้างาน) การจัดประชุมเชิงปฏิบัติการ การตรวจสอบเอกสาร การสำรวจหน้างานเพื่อตรวจสอบวิธีการทำงาน และการทดสอบการเข้าถึงฐานข้อมูล เป็นต้น โดยเน้นพิจารณาการปฏิบัติที่ดำเนินการจริงเปรียบเทียบกับกรอบการดำเนินงานที่เป็นมาตรฐานสากล ตั้งแต่ โครงสร้าง

การจัดการ การบริหารความเสี่ยง การป้องกัน การเฝ้าระวัง การรายงาน และการตอบสนองต่อเหตุการณ์

5. การยกระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กร

บริษัทผู้เชี่ยวชาญฯ ได้นำเสนอผลการประเมินและแผนภาพ Risk Profile Heatmap ประกอบด้วยระดับความเสี่ยงในปัจจุบันของหัวเรื่องหลัก (Domain) ที่พบ และความพร้อมในการปรับปรุงในแต่ละ Domain ดังกล่าว ดังแสดงในแผนภาพที่ 3-3

แผนภาพที่ 3-3 Risk Profile Heatmap ขององค์กร



ที่มา : ยุทธนา เจียมตระการ, 2561.

และเลือกมาดำเนินการเพียง 4 Domain ที่อยู่ในโซนสีเหลืองแดง ได้แก่ การจัดการและกำกับดูแลด้านความมั่นคงปลอดภัย (Security Governance) การบริหารความเสี่ยงไซเบอร์ (Cyber Risk Management) ปฏิบัติการด้านความมั่นคงปลอดภัย (Security Operations) และภูมิสถาปัตย์และวิศวกรรมด้านความมั่นคงปลอดภัย (Security Architecture and Engineering) โดยรายละเอียดการดำเนินการของแต่ละ Domain เป็นดังนี้

1. Domain: Security Governance กล่าวถึงการจัดการและกำกับดูแลด้านความมั่นคงปลอดภัย ตั้งแต่การกำหนดรูปแบบการทำงาน (Operating Model) โครงสร้างองค์กร ข้อกำหนดมาตรฐานต่างๆ กรอบการทำงาน การพัฒนาบุคลากร รวมถึงการประเมินระบบ

2. Domain: Cyber Risk Management กล่าวถึงการบริหารความเสี่ยงไซเบอร์ ซึ่งครอบคลุมกรอบการทำงาน การประเมินระบบโดยผู้ประเมินภายนอก การประเมิน Compliance

3. Domain: Security Operations กล่าวถึงการปฏิบัติการด้านความมั่นคงปลอดภัยที่ครอบคลุมการปรับปรุงระบบและเครื่องมือ การดูแลรักษาความลับของข้อมูล การบริหารจัดการทรัพย์สิน ICT

4. Domain: Security Architecture and Engineering กล่าวถึงภูมิสถาปัตย์และวิศวกรรมด้านความมั่นคงปลอดภัย ตั้งแต่การกำหนด Firewall การ Configure ระดับความปลอดภัยของอุปกรณ์ในเครือข่าย (Network Devices) รวมทั้งการกำหนด Architecture ระบบความปลอดภัย

ทั้งนี้องค์กรและบริษัทผู้เชี่ยวชาญฯ ได้วางแผนร่วมกันในการยกระดับความมั่นคงปลอดภัยไซเบอร์ โดยนำแผนใน 4 Domains ดังกล่าวมาออกแบบโรดแม็ป เพื่อการปรับปรุง (Roadmap for Improved Cybersecurity) ประกอบด้วยแผนใน 3 ระดับ คือ

1. ระดับที่ 1: แผนที่ดำเนินการภายใน 6 เดือน หรือเรียกว่า Quick-win Project
2. ระดับที่ 2: แผนที่ดำเนินการภายในเวลา 1 ปี
3. ระดับที่ 3: แผนที่ดำเนินการภายในเวลา 1-3 ปี

ตัวอย่างแผนงานปรับปรุงของแต่ละ Domain ดังแสดงในตารางที่ 3-2 ถึง 3-5

ตารางที่ 3-2 ตัวอย่างแผนการปรับปรุง Domain : Security Governance

แผนงาน	Domain: Security Governance
ระดับที่ 1	1. ปรับปรุงโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ระดับการกำกับจนถึงระดับปฏิบัติ 2. กำหนดดัชนีเฝ้าระวังความเสี่ยงเรื่องความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Key Risk Index) 3. เพิ่มจำนวนผู้เชี่ยวชาญดูแลเรื่องความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับส่วนกลางและระดับกลุ่มธุรกิจ
ระดับที่ 2	1. กำหนด / ทบทวน กรอบ แนวปฏิบัติ และมาตรฐานในการรับมือภัยคุกคามไซเบอร์ 1.1 Industrial Control System (ICS) Security Policy and Standards 1.2 Incident Response Framework 2. ทบทวนกลุ่มข้อมูลสำคัญขององค์กรและกลุ่มธุรกิจ เพื่อการจัดการเรื่องความปลอดภัย 3. กำหนดกลไกการพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์
ระดับที่ 3	1. พัฒนาโปรแกรมการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ตามลักษณะกลุ่มงาน (Group Security Program Management) 2. ทบทวนโครงสร้างของตำแหน่ง Chief Information Security Officer (CISO)

ที่มา : ยุทธนา เจียมตระการ, 2561.

ตารางที่ 3-3 ตัวอย่างแผนการปรับปรุง Domain: Cyber Risk Management

แผนงาน	Domain: Cyber Risk Management
ระดับที่ 1	1. พัฒนาและปรับปรุง กรอบการบริหารจัดการความเสี่ยงในเรื่องความมั่นคงปลอดภัยไซเบอร์
ระดับที่ 2	1. การให้ผู้เชี่ยวชาญจากภายนอกมาประเมินความเสี่ยงของระบบความมั่นคงปลอดภัยไซเบอร์ (Third Party Security Risk Assessment) 2. การประเมินการกำกับการปฏิบัติ (Compliance Assessment)
ระดับที่ 3	1. ทบทวนกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Re-evaluate Cybersecurity Strategy)

ที่มา : ยุทธนา เจียมตระการ, 2561.

ตารางที่ 3-4 ตัวอย่างแผนการปรับปรุง Domain: Security Operations

แผนงาน	Domain: Security Operations
ระดับที่ 1	1. ปรับปรุงระบบการบริหาร กฎเกณฑ์ และเครื่องมือเพื่อป้องกันไวรัสคอมพิวเตอร์เข้าสู่ระบบเครือข่ายขององค์กรอันเนื่องมาจากพฤติกรรมของผู้ใช้งาน (Improve Security Hygiene of Systems and Devices)
ระดับที่ 2	1. การบริหารจัดการสารสนเทศและเทคโนโลยีขององค์กร (Information and Communication Technology (ICT) Asset Management) 2. การบริหารจัดการระบบการควบคุมในโรงงาน (ICS Asset Management) 3. การซ้อมรับมือภัยคุกคามไซเบอร์ (Incident Response Simulation) 4. การทดสอบแนวป้องกันการเจาะระบบ (Penetration Testing)
ระดับที่ 3	1. ยกระดับศูนย์ปฏิบัติการเรื่องความมั่นคงปลอดภัยไซเบอร์ (Advanced Security Operation Center (SOC))

ที่มา : ยุทธนา เจียมตระการ, 2561.

ตารางที่ 3-5 ตัวอย่างแผนการปรับปรุง Domain: Security Architecture and Engineering

แผนงาน	Domain: Security Architecture and Engineering
ระดับที่ 1	1. ทบทวนและปรับชั้นป้องกันความปลอดภัย Fire Wall (Review and Clean Up Fire Wall Rule Set)
ระดับที่ 2	1. ดำเนินการตามภูมิสถาปัตย์ความมั่นคงปลอดภัยของ ICS ที่ปรับปรุงล่าสุด (Implement Updated ICS Security Architecture)
ระดับที่ 3	1. ทบทวนและกำหนดสิทธิผู้เข้าถึงข้อมูล (Privilege Access Management) 2. ดำเนินการให้เกิดการควบคุมการเข้าถึงระบบเครือข่าย (Implement Network Access Control) 3. จัดโครงสร้างอุปกรณ์ในระบบเครือข่ายเพื่อความมั่นคงปลอดภัย (Re-configure Existing Security and Network Devices)

ที่มา : ยุทธนา เจียมตระการ, 2561.

ขณะนี้องค์กรอยู่ระหว่างการปรับปรุงตามโรดแม็ปดังกล่าว และมีความก้าวหน้าตามลำดับอย่างต่อเนื่อง ดังจะเห็นได้จาก เรื่องการปรับปรุงโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตั้งแต่ระดับการกำกับจนถึงระดับปฏิบัติ (ดังแสดงในแผนภาพที่ 3-4) มีการกำหนดคณะทำงานเรื่องความมั่นคงปลอดภัยไซเบอร์ ให้มีความชัดเจนยิ่งขึ้น เพื่อให้มั่นใจว่าการบริหารงานจะมีประสิทธิผล ตั้งแต่การกำหนดทิศทาง นโยบาย ยุทธวิธี ไปจนถึงการดำเนินการในภาคปฏิบัติ ในระดับแนวดิ่ง บน-ล่าง และล่าง-บน และเกิดความร่วมมือกันอย่างบูรณาการในแนวราบระหว่างหน่วยงานกลางและธุรกิจต่างๆ ดังนี้

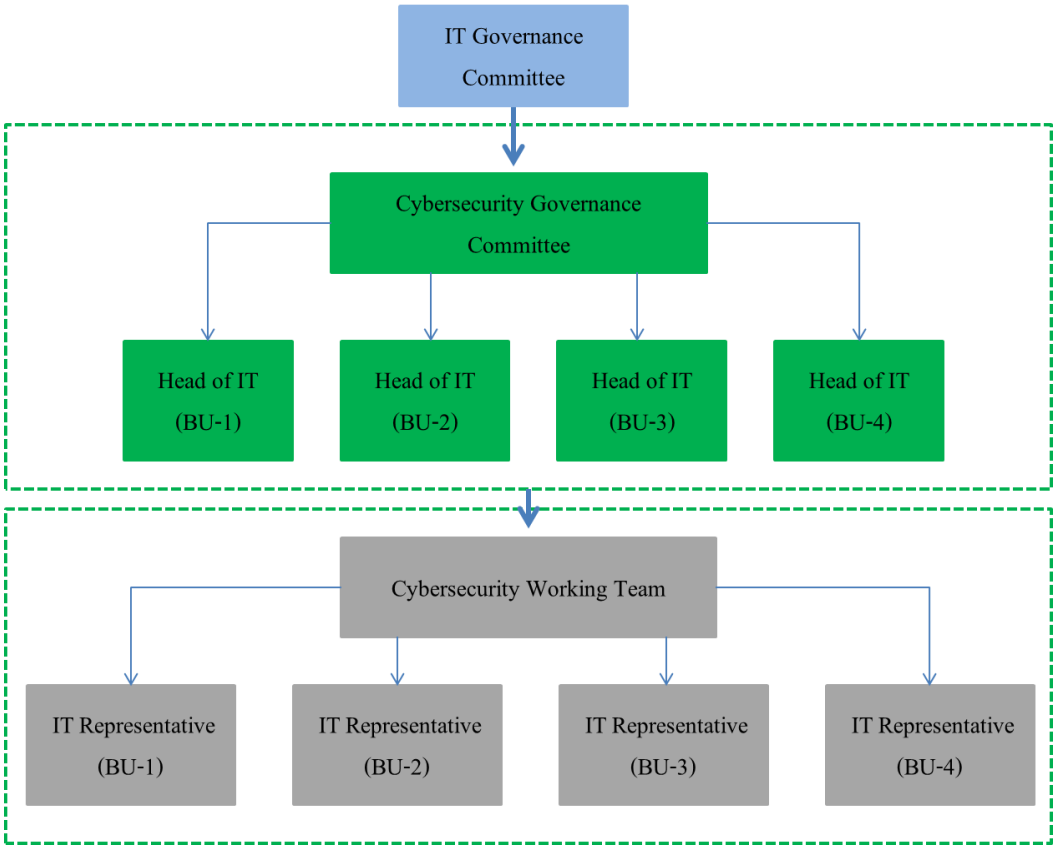
1. IT Governance Committee (ITG) มีผู้บริหารสูงสุดของหน่วยงานกลางเป็นประธาน มีคณะกรรมการประกอบด้วยผู้บริหารระดับสูง ทั้งจากแต่ละธุรกิจ และหน่วยงานกลาง ทำหน้าที่ในการกำหนดนโยบาย หลักการ และแนวทางการกำกับการปฏิบัติในเรื่อง ITC รายงานผลการดำเนินงานเรื่อง ITC ให้คณะจัดการบริหารทราบอย่างน้อยทุกไตรมาส รวมทั้งรายงานต่อคณะกรรมการตรวจสอบอย่างน้อยปีละ 2 ครั้ง

2. Cybersecurity Governance Committee (CGC) มีผู้บริหารสูงสุดของสำนักงาน Information Technology and Business Continuity Management ซึ่งเป็นเลขานุการของคณะ ITG เป็นประธาน คณะกรรมการประกอบด้วยผู้บริหารสูงสุดของหน่วยงานไอทีจากแต่ละธุรกิจ คณะ CGC

รับผิดชอบในการสร้างความเข้าใจ กำหนดกรอบและกระจายนโยบายที่ได้รับจากคณะ ITG ไปสู่แผนการปฏิบัติ ติดตามผลการดำเนินงานตามโรดแม็ป กำหนดและติดตาม IT Governance Indicators จัดการในเรื่อง Cybersecurity Network and Architecture ทั้งที่ดำเนินการโดยองค์กรเองและโดยผู้ให้บริการทั้งในและต่างประเทศ รวมทั้งผลักดันให้เกิดความตระหนักในเรื่องความมั่นคงปลอดภัยไซเบอร์ ในองค์กรมีการประชุมร่วมกันเดือนละ 1 ครั้ง และรายงานการดำเนินงานให้คณะ ITG ทราบเดือนละ 1 ครั้งเช่นกัน

3. Cybersecurity Working Team (CWT) เป็นคณะทำงานเชิงปฏิบัติการ มีเลขานุการคณะ CGC เป็นประธาน สมาชิกประกอบด้วยตัวแทนด้าน ITC จากทุกธุรกิจ ซึ่งเป็นทั้งผู้บริหารและมีความรู้ทางเทคนิคในสายวิชาชีพไอที รับผิดชอบในการกำหนดรายละเอียดของแนวปฏิบัติต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น กลไกการเฝ้าระวัง การติดตาม การตรวจสอบและรับมือภัยการโจมตี การป้องกันการรุกรานจากภายนอก และการฟื้นฟูสภาพภายหลังการโจมตี มีการประชุมเดือนละ 1 ครั้ง และรายงานผลการดำเนินการต่อคณะ CGC เดือนละ 1 ครั้งเช่นกัน

แผนภาพที่ 3-4 โครงสร้างการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร



ที่มา : ยุทธนา เจียมตระการ, 2561

การสัมภาษณ์ผู้ทรงคุณวุฒิและผู้เกี่ยวข้องขององค์กร

งานวิจัยนี้ได้มีการสัมภาษณ์ผู้ทรงคุณวุฒิด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ทั้งจากภาครัฐและภาคเอกชน รวมทั้งผู้เกี่ยวข้องขององค์กร ได้แก่ ผู้บริหารที่ดูแลด้านนโยบายการสร้างความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารที่ดูแลด้านกฎหมาย ผู้บริหารของธุรกิจที่มีการนำไซเบอร์ไปใช้ในธุรกิจ และลูกค้าของธุรกิจ เพื่อเป็นข้อมูลปฐมภูมิในมุมมองที่กว้างขึ้นทั้งในส่วนนโยบายและสถานะการปฏิบัติในระดับประเทศ ทั้งภาครัฐและธุรกิจรวมถึงความเห็นเกี่ยวกับการปฏิบัติที่ดี (Best Practice) ในต่างประเทศ เพื่อประกอบการวิเคราะห์การจัดการด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ในอุตสาหกรรมขนาดใหญ่ รายละเอียดผู้ทรงคุณวุฒิและผู้เกี่ยวข้องขององค์กรที่มีการสัมภาษณ์ แสดงในตารางที่ 3-6 ถึง 3-7

ตารางที่ 3-6 ผู้ทรงคุณวุฒิที่มีการสัมภาษณ์ และบทบาทในกระบวนการจัดการความมั่นคงปลอดภัยไซเบอร์

รายนามผู้ทรงคุณวุฒิ	บทบาทในกระบวนการจัดการความมั่นคงปลอดภัยไซเบอร์
ภาครัฐ: 1. คุณอัจฉรินทร์ พัฒนพันธ์ชัย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	ผู้ถ่ายทอดนโยบายชาติไปสู่การปฏิบัติ และผู้กำกับดูแล
ภาคเอกชน: 1. คุณปริญญา หอมเอนก President and Founder, ACIS Professional Center Co., Ltd. 2. คุณนนทวัฒน์ พุ่มชูศรี Country Managing Director, Accenture Thailand 3. คุณจิรพล ตังทัตสวัสดิ์ Director, PricewaterhouseCoopers Consulting (Thailand) Ltd.	ผู้เชี่ยวชาญและให้บริการด้านการประเมินระบบความมั่นคงปลอดภัยไซเบอร์ ผู้ให้บริการด้านการประเมินระบบความมั่นคงปลอดภัยไซเบอร์ ผู้ให้บริการด้านการประเมินระบบความมั่นคงปลอดภัยไซเบอร์

ที่มา : ยุทธนา เจียมตระการ, 2561.

ตารางที่ 3-7 ผู้เกี่ยวข้องขององค์กรตัวอย่างที่มีการสัมภาษณ์ และบทบาทในกระบวนการจัดการความมั่นคงปลอดภัยไซเบอร์

รายนามผู้เกี่ยวข้องขององค์กรตัวอย่าง	**บทบาทในกระบวนการจัดการความมั่นคงปลอดภัยไซเบอร์**
ผู้บริหาร: 1. ผู้บริหารระดับสูงของกลุ่มธุรกิจ	ผู้กำหนดวิสัยทัศน์และกลยุทธ์ของธุรกิจที่มีการใช้ ITC ในธุรกิจ
2. ตัวแทนผู้บริหารที่ดูแลด้านความมั่นคงปลอดภัยไซเบอร์	ผู้บริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์
3. ตัวแทนผู้บริหารที่ดูแลด้านกฎหมาย	ผู้ดูแลกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กร
คู่ธุรกิจ: ผู้บริหารบริษัท 5 ราย	ผู้ทำธุรกิจกับองค์กรผ่านระบบ ITC

ที่มา : ยุทธนา เจียมตระการ, 2561.

ข้อมูลจากการสัมภาษณ์เรื่องความมั่นคงปลอดภัยไซเบอร์ สามารถสรุปเป็นประเด็นหลักได้ดังนี้

ประเด็นที่ 1 ความตื่นตัวของภาครัฐ ภาคเอกชน และภาคประชาชน

<u>ภาครัฐ</u>

ในส่วนของกระทรวงหลักที่เกี่ยวข้องกับไซเบอร์ทั้งด้านเศรษฐกิจและความมั่นคง ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกระทรวงกลาโหมมีความตื่นตัวในเรื่องความมั่นคงปลอดภัยไซเบอร์ มาก รวมถึงรัฐวิสาหกิจที่เกี่ยวกับโครงสร้างพื้นฐานของประเทศ เช่น การไฟฟ้า การประปา เป็นต้น แต่สำหรับกระทรวงอื่นหรือหน่วยงานอื่นยังมีความตื่นตัวไม่มาก อย่างไรก็ตาม

หัวหน้าคณะรัฐบาลคือ นายกรัฐมนตรี ได้ให้ความสำคัญทั้งเรื่องเศรษฐกิจดิจิทัล และการสร้างความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก

ภาคเอกชน

ความตื่นตัวมากหรือน้อยจะขึ้นกับประเภทธุรกิจหรืออุตสาหกรรมที่รับทราบผลกระทบจากภัยคุกคามไซเบอร์ ทั้งที่มีประสบการณ์เอง หรือรับรู้จากข่าวสารต่างๆ ธุรกิจที่มีความตื่นตัวมากส่วนใหญ่เป็นธุรกิจบริการที่เกี่ยวข้องกับลูกค้าจำนวนมาก เช่น ธุรกิจธนาคารและการเงิน ธุรกิจประกันภัย ธุรกิจค้าปลีก เป็นต้น โดยธุรกิจเหล่านี้มีการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ เพิ่มขึ้นอย่างมีนัยสำคัญ แต่สำหรับอุตสาหกรรมการผลิตส่วนใหญ่ยังมีความตื่นตัวไม่มาก

ในส่วนของบริษัท พบว่าบริษัทขนาดใหญ่จะมีความตื่นตัวมากกว่าบริษัทขนาดกลางและขนาดเล็ก เนื่องจากที่ผ่านมา การแฮ็กระบบเพื่อขโมยข้อมูลมักเกิดกับบริษัทใหญ่ โดยเฉพาะในธุรกิจที่มีข้อมูลสำคัญ มีมูลค่ามากหรือสามารถสร้างความเสียหายให้กับชื่อเสียงของบริษัทได้ เช่น ข้อมูลด้านการเงิน ข้อมูลส่วนบุคคล ข้อมูลความลับทางการค้า เป็นต้น นอกจากนี้ในบริษัทที่มีการนำเทคโนโลยีดิจิทัลมาใช้ในการดำเนินธุรกิจ หรือเป็นส่วนหนึ่งของระบบปฏิบัติการในโรงงานก็ให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ มากเช่นกัน เนื่องจากถ้ามีการแฮ็กอาจทำให้ระบบไอที หรือเครือข่ายล่ม หรือทำให้โรงงานหยุดการทำงาน ทำให้เกิดความเสียหายทั้งด้านการเงิน ชื่อเสียง และความน่าเชื่อถือของบริษัทได้

ปัจจุบันมีบางกลุ่มธุรกิจได้มีการตั้งกลุ่มเพื่อแชร์ข้อมูลกัน เช่น TB-CERT ของสมาคมธนาคารไทย เป็นต้น

ภาคประชาชน

บุคคลทั่วไปยังมีความตื่นตัวในเรื่องนี้ไม่มาก โดยคนส่วนใหญ่ยังไม่รู้จักเรื่อง ความมั่นคงปลอดภัยไซเบอร์ ยกเว้นคนที่ทำงานด้านไอทีหรือดิจิทัล หรืออยู่ในธุรกิจที่มีการนำไอทีหรือดิจิทัลมาใช้และได้รับการอบรมให้ความรู้ในเรื่องนี้ นอกจากนี้คนส่วนใหญ่ยังไม่เห็นอันตรายของภัยนี้และคิดว่ามีผู้รับผิดชอบในการดูแลเรื่องนี้อยู่แล้ว และจากการสัมภาษณ์ลูกค้าขององค์กรตัวอย่างก็พบว่า ยังไม่ตื่นตัวในเรื่องนี้เช่นกัน

ประเด็นที่ 2 การบริหารจัดการ

1. รูปแบบการจัดการ

ผู้ทรงคุณวุฒิท่านหนึ่งได้ให้ข้อมูลเกี่ยวกับงานวิจัยของบริษัท Gartner, Inc. ซึ่งชี้ให้เห็นว่าการควบคุมเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์ ภาครัฐจะเป็นทั้งผู้ผลักดัน และผู้ควบคุมในเรื่องนี้ โดยทั่วโลกมีแนวโน้มที่จะเป็นการควบคุมเพื่อสร้างความปลอดภัยในระดับชาติมากขึ้น และการสร้างความมั่นคงปลอดภัยขององค์กร ส่วนใหญ่จะมีแนวโน้มเป็นแบบการคาดการณ์ (Prediction) และ การป้องกัน (Protection) มากกว่า แบบการแก้ไข (Correction) ที่ปฏิบัติกันเป็นส่วนมากในปัจจุบัน

2. องค์ประกอบการดำเนินงาน

<u>โครงสร้างการบริหารจัดการ</u>

ผู้ทรงคุณวุฒิหลายท่านชี้ให้เห็นว่า ต้องเป็นแบบ Top-Down เท่านั้น โดยผู้บริหารระดับสูงต้องเป็นผู้นำในเรื่องนี้ เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับกฎหมาย ถ้าทำได้ไม่ดีองค์กรสามารถถูกฟ้องร้อง เรียกค่าเสียหายเป็นมูลค่าสูง และเสียชื่อเสียงได้ การทำเรื่องนี้ต้องมีการกำกับที่ดี (Governance) เพราะไม่ใช่เรื่องของเทคโนโลยีเพียงอย่างเดียว แต่เป็นเรื่องการปฏิบัติของบุคลากร พฤติกรรมของคนในองค์กรซึ่งสำคัญและทำให้เกิดความเสี่ยงได้

ผู้ทรงคุณวุฒิบางท่านชี้ให้เห็นว่า การดำเนินการเรื่องนี้จำเป็นต้องมีผู้นำหลักในการกำกับให้เกิดการปฏิบัติ และไม่ควรอยู่ในหน่วยงานไอที เพราะจะทำให้พนักงานในองค์กรเกิดความตระหนักรู้ได้ยาก เพราะเห็นว่าเป็นหน้าที่ที่หน่วยงานไอที ต้องดำเนินการอยู่แล้วตามความรับผิดชอบที่มีอยู่ ทำให้ขาดการตระหนักรู้ในเรื่องความเสี่ยงและการมีส่วนร่วม ทั้งนี้ผู้นำหลักดังกล่าวจะต้องมีความเข้าใจทั้งด้านไอที ด้านความมั่นคงปลอดภัยไซเบอร์ และด้านธุรกิจไปพร้อมกัน เพื่อให้สามารถสื่อสารกับฝั่งธุรกิจได้

นอกจากนี้โครงสร้างการบริหารจัดการไม่จำเป็นต้องมีหน่วยงานที่เป็นเจ้าภาพเพียงหน่วยงานเดียว เช่น ในประเทศสหรัฐอเมริกา หน่วยงานภาครัฐมีเจ้าภาพแยกตามเรื่องด้านการทหาร มีเจ้าภาพหลักคือกระทรวงกลาโหม ด้านการเงิน คือ ธนาคารกลางสหรัฐอเมริกา เป็นต้น แต่สิ่งสำคัญคือ เจ้าภาพหลักไม่ว่าจะเป็นภาครัฐหรือเอกชน ต้องลงมือทำและรับผิดชอบการผลักดันอย่างจริงจัง รวมทั้งสามารถประสานงานกับผู้เกี่ยวข้องให้เกิดขึ้นได้

<u>นโยบายและแผน</u>

การดำเนินการตามนโยบายและแผน จำเป็นต้องมีผู้รับผิดชอบชัดเจนในการกำหนดทิศทาง และผลักดันให้เกิดการดำเนินการ เพราะถ้าขาดผู้รับผิดชอบหลักก็ยากที่ดำเนินการอย่างมีประสิทธิผลตามเป้าหมายที่วางไว้ได้

นอกจากนี้แผนงานยกระดับความมั่นคงปลอดภัยไซเบอร์ก็ต้องมีการทบทวนทุกปีหรืออย่างน้อยทุก 2 ปี เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา แผนที่วางไว้เดิมอาจไม่เหมาะสมแล้ว

<u>กฎหมาย / มาตรฐาน / กรอบการทำงาน</u>

การสร้างความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ เพื่อให้เกิดการดำเนินการอย่างจริงจังและรวดเร็ว จำเป็นต้องมีกฎหมายมารองรับ โดยขณะนี้ภาครัฐอยู่ระหว่างผลักดันกฎหมายสำคัญคือ พ.ร.บ. ความมั่นคงปลอดภัยด้านไซเบอร์ ให้ประกาศใช้ให้ได้ภายในปี พ.ศ.2561 โดยกฎหมายฉบับนี้จะมีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นหน่วยงานหลักที่ถืออำนาจ

ใน พ.ร.บ. นี้ และสาระสำคัญของกฎหมายฉบับนี้ คือ การมีคณะกรรมการ National Cybersecurity Agency หรือ NSA ซึ่งมีนายกรัฐมนตรีเป็นประธาน โดยคณะกรรมการชุดนี้มีหน้าที่ในการกำหนดแนวปฏิบัติในเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศ กำหนดหน่วยงานสำคัญของประเทศที่เรียกว่า Critical Service ที่ต้องปฏิบัติตามแนวปฏิบัติที่กำหนดขึ้นโดยมีผลในเชิงกฎหมาย กำหนดให้มีการจัดตั้งหน่วยงานหลักขึ้นมากำกับดูแลให้เกิดการปฏิบัติและการรายงานผลการปฏิบัติให้ NSA รับทราบ

สำหรับมาตรฐานและกรอบการทำงานเป็นเรื่องจำเป็นเช่นกัน ปัจจุบันมีหลายมาตรฐานและหลายกรอบการทำงานให้เลือกนำมาใช้ โดยผู้ทรงคุณวุฒิให้ความเห็นว่า แต่ละมาตรฐานจะมีจุดเด่นเฉพาะ การเลือกมาตรฐานมาใช้เป็นแนวปฏิบัติงานต้องเลือกให้เหมาะสมกับขอบข่ายของตนเอง เช่น กรอบการทำงานของ NIST จะมีจุดเด่นด้านกระบวนการที่ดำเนินการได้ครบ Loop คือ เริ่มจากการระบุขอบข่าย (Identify) การกำหนดการป้องกัน (Protect) การตรวจสอบและเฝ้าระวัง (Detect) การรับมือต่อเหตุการณ์ (Respond) และการฟื้นฟูภายหลังเหตุการณ์ (Recover) หรือมาตรฐาน ISO 27001 มีจุดเด่นคือ ทำให้เห็นภาพกว้างเชิงการจัดการ การเข้าถึงและการป้องกันข้อมูลหรือมาตรฐาน Industry Standard Architecture (ISA) เป็นมาตรฐานเฉพาะที่เกี่ยวกับระบบควบคุมและทำงานอัตโนมัติของอุตสาหกรรม (Industrial Automation and Control System) หรือ มาตรฐานด้านความปลอดภัย Payment Card Industry (PCI) เป็นมาตรฐานเฉพาะเกี่ยวกับความปลอดภัยของข้อมูลบัตรเครดิต เป็นต้น

เนื่องจากภัยคุกคามไซเบอร์สามารถเกิดได้ตลอดเวลา นอกจากการป้องกันแล้ว การซ้อมทำสงครามไซเบอร์โดยจำลองเสมือนจริง ให้มีทั้งทีมป้องกัน (White Hacker) และทีมรุกราน (Red Hacker) เพื่อทดสอบหาช่องโหว่ในระบบ ซ้อมการรับมือ และการฟื้นฟูจากการโจมตี เพื่อให้องค์กรพร้อมรับมือก็เป็นเรื่องจำเป็นเช่นกัน

<u>บุคลากร</u>

ผู้ให้สัมภาษณ์ทุกท่านมีความเห็นตรงกันว่า ความรู้ ความสามารถ และความตระหนักรู้ของบุคลากรเป็นเรื่องสำคัญมากในการสร้างความมั่นคงปลอดภัยไซเบอร์ เพราะแม้องค์กรจะมีการลงทุนเทคโนโลยีมากมายเพื่อป้องกัน แต่ถ้าคนไม่ปฏิบัติตามเนื่องจากขาดความรู้หรือความตระหนักรู้ ก็ไม่สามารถทำให้ระบบปลอดภัยได้

ประเด็นสำคัญเกี่ยวกับบุคลากรขณะนี้คือ คนที่มีความรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ในระดับผู้มีประสบการณ์ชำนาญการของประเทศไทยมีน้อยมากไม่ถึง 10 คน ส่วนระดับที่มีความรู้ได้รับใบรับรองคุณวุฒิ (Certificate) มีเพียง 200-400 คน ซึ่งถือว่าขาดแคลนมาก และเป็นเรื่องรีบด่วนลำดับต้นที่ต้องรีบดำเนินการ และเรื่องนี้จะเป็นปัญหาใหญ่เมื่อ พ.ร.บ. ความมั่นคง

ปลอดภัยไซเบอร์ มีผลบังคับใช้ตามกฎหมาย เนื่องจากองค์กรที่เป็น Critical Services ตามที่กฎหมายกำหนด จำเป็นต้องมีคนที่มีความรู้ด้านนี้เพื่อให้สามารถปฏิบัติตามที่กฎหมายกำหนดได้ ซึ่งแนวทางการแก้ไขอย่างหนึ่งที่สามารถทำได้คือ การจ้างผู้เชี่ยวชาญจากต่างประเทศ เข้ามาช่วยในการดำเนินการ ทั้งนี้ ผู้ทรงคุณวุฒิท่านหนึ่งได้ชี้ให้เห็นว่า แม้แต่บริษัทที่ปรึกษาประเมินระบบในประเทศไทยก็มีการว่าจ้างผู้เชี่ยวชาญจากต่างประเทศมาเป็นผู้ประเมินระบบให้

นอกจากเรื่องจำนวนบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยที่มีจำกัดแล้ว ในส่วนของหน่วยงานหลักของภาครัฐคือ กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมก็มีจำนวนทรัพยากรบุคคลจำกัดเช่นกัน ทำให้ไม่สามารถให้ความช่วยเหลือทั้งภาครัฐและภาคเอกชนไปพร้อมกันได้

สำหรับความตระหนักรู้ของบุคลากรในประเทศไทย พบว่า คนไทยทั่วไปยังให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์น้อย โดยผู้ให้สัมภาษณ์บางท่านมีความเห็นว่าสำหรับองค์กรแล้วความตระหนักรู้ของผู้บริหารเป็นสิ่งที่สำคัญมาก เพราะเป็นผู้กำหนดทิศทาง กลยุทธ์ และให้งบประมาณ และการสร้างความตระหนักรู้ให้แก่พนักงานที่เป็นผู้ใช้งานก็เป็นเรื่องจำเป็นเช่นกันโดยต้องปฏิบัติอย่างต่อเนื่องจนเปลี่ยนแปลงพฤติกรรมได้ ซึ่งจะใช้เพียงการอบรมเท่านั้นยังไม่เพียงพอ แต่ต้องแน่ใจว่าพนักงานมีความเข้าใจ รู้จริง และสามารถปฏิบัติได้

<u>งบประมาณ</u>

การสร้างความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ต้องมีการลงทุนทั้งด้านระบบเทคโนโลยีและบุคลากร ไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือภาคเอกชน ซึ่งการลงทุนให้งบประมาณมากหรือน้อยจะขึ้นกับมุมมองหรือวิสัยทัศน์ของผู้นำองค์กรเป็นสำคัญ ว่าเห็นความเสี่ยงของภัยคุกคามนี้มีผลต่อองค์กรอย่างไร โดยองค์กรที่อยู่ในหน่วยงานหรือกลุ่มธุรกิจที่รับทราบผลกระทบของภัยคุกคามนี้จะจัดสรรงบประมาณในส่วนนี้ไว้อย่างชัดเจน

ประเด็นที่ 3 ปัจจัยเสี่ยง

ผู้ให้สัมภาษณ์ได้ให้มุมมองเกี่ยวกับปัจจัยเสี่ยงที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยเบอร์ไซเบอร์ไว้ดังนี้

<u>บุคลากรขององค์กร</u> เป็นห่วงโซ่ที่มีความเสี่ยงมากที่สุด การลงทุนเทคโนโลยีจำนวนมาก แต่ถ้าบุคลากรไม่ปฏิบัติตามระเบียบหรือกรอบการทำงาน หรือขาดความตระหนักรู้ก็สามารถเป็นอันตรายได้ โดยเฉพาะประเทศไทยที่การดำเนินการเรื่องความมั่นคงปลอดภัยไซเบอร์เป็นแบบการแก้ไข (Correction) มากกว่าการป้องกัน (Prevention) และยังขาดการคาดการณ์ (Prediction) ด้วย

เทคโนโลยี มีเทคโนโลยีเกิดขึ้นใหม่ตลอดเวลา เช่น Data Analytics, Cloud Computing, IoT เป็นต้น หากองค์กรไม่มีการทบทวนระบบความมั่นคงปลอดภัยไซเบอร์ อย่างเพียงพอให้ทันกับการเปลี่ยนแปลงของเทคโนโลยี ก็จะเป็นความเสี่ยง นอกจากนี้ ถ้าการออกแบบเทคโนโลยี เช่น เทคโนโลยี IoT ไม่ได้นำเรื่องความมั่นคงปลอดภัยไซเบอร์ เข้ามาเป็นส่วนหนึ่งของการออกแบบตั้งแต่แรก (Primary Requirement) อุตสาหกรรมนั้นก็จะมีความเสี่ยงมาก โดยเฉพาะถ้าระบบขององค์กรดังกล่าวไม่ใช่ระบบปิดแต่เป็นระบบที่เชื่อมต่อกับเครือข่าย (Network) ความเสี่ยงก็จะยิ่งสูงมากขึ้น

กฎหมาย ขณะที่ประเทศไทยในยุคไทยแลนด์ 4.0 ส่งเสริมให้มีการนำเทคโนโลยีดิจิทัลมาใช้เพื่อยกระดับเศรษฐกิจและสังคมของประเทศไทย และแนวโน้มความเสี่ยงของภัยคุกคามไซเบอร์ก็มีมากขึ้นและเป็นปัญหาของโลกในระดับต้นๆ การที่กฎหมายสำคัญเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ และเศรษฐกิจดิจิทัล เช่น พ.ร.บ. ความมั่นคงปลอดภัยด้านไซเบอร์ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น ยังไม่ถูกประกาศใช้ จึงเป็นเรื่องที่มีความเสี่ยงอย่างยิ่ง นอกจากนี้การที่ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์มีการประกาศใช้ล่าช้า ก็ส่งผลต่อการประกาศอุตสาหกรรมโครงสร้างพื้นฐานสำคัญของประเทศล่าช้าไปด้วย ทำให้การพัฒนาบุคลากรในอุตสาหกรรมดังกล่าวอาจล่าช้า และถ้าอุตสาหกรรมนั้นขาดความตระหนักรู้ด้วย ก็ยิ่งเพิ่มความเสี่ยงในการรับมือภัยคุกคามไซเบอร์มากขึ้น

รูปแบบของการคุกคามระบบ มีแนวโน้มจะทำให้เกิดการหยุดชะงักของธุรกิจ (Digital Business Disruption) ทั้งในส่วนของภาคการผลิต และภาคบริการ มากกว่าการโจรกรรมข้อมูลบัตรเครดิต หรือข้อมูลการเงินแบบปัจจุบัน ที่เกิดกับภาคบริการเป็นส่วนใหญ่

ประเด็นที่ 4 ข้อเสนอแนะ

ผู้ให้สัมภาษณ์ได้ให้คำแนะนำเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ในด้านต่างๆ ไว้ดังนี้

แผนแม่บท (Master Plan) ภาครัฐควรจัดทำแผนแม่บทในเรื่องความมั่นคงปลอดภัยไซเบอร์ และมีองค์กรกลางทำหน้าที่ออกนโยบาย ส่งเสริม สนับสนุน และการกำกับดูแล นอกจากนี้การทำงานของภาครัฐควรเป็นเชิงรุกมากขึ้น มีการสื่อสารอย่างทั่วถึง มีระบบการเตือนภัยที่ทันท่วงที เพิ่มเติมจากการเป็นศูนย์วิชาการให้ความรู้

การพัฒนาบุคลากร จากการที่บุคลากรที่เป็นทั้งระดับผู้ชำนาญการ และระดับที่ได้รับการรับรองคุณวุฒิด้านความมั่นคงปลอดภัยไซเบอร์ มีน้อยมาก ผู้ทรงคุณวุฒิบางท่านให้คำแนะนำว่า ควรจัดสอนหลักสูตรนี้ในมหาวิทยาลัยทั้งภาคทฤษฎีและภาคปฏิบัติ และควรจัดตั้งสถาบันความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างผู้เชี่ยวชาญด้านนี้โดยเฉพาะ โดยระยะแรกอาจว่าจ้างผู้เชี่ยวชาญจากต่างประเทศเข้ามาก่อน

กลไกการออกกฎหมาย ควรมีกลไกการรับฟังตั้งแต่ยังเป็นระดับแนวคิด ที่มา หลักการ เหตุผล และเป้าประสงค์ มากกว่ามีเพียงการรับฟังในช่วงที่เป็นร่างกฎหมายแล้วอย่างในปัจจุบัน เพราะจะทำให้ผู้เกี่ยวข้องซึ่งเป็นผู้ปฏิบัติเข้าใจเจตจำนงค์ของกฎหมาย เพิ่มเติมความเห็นที่เป็นประโยชน์ต่อภาครัฐ เกิดความร่วมมือที่ดีและเกิดประสิทธิผลมากยิ่งขึ้นเมื่อกฎหมายประกาศใช้

สรุป

จากการสำรวจการจัดการในเรื่องความมั่นคงปลอดภัยไซเบอร์ขององค์กรตัวอย่างที่อยู่ในอุตสาหกรรมขนาดใหญ่ พบว่า องค์กรนี้ให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มาก เพราะมองเห็นผลกระทบว่าภัยคุกคามนี้สามารถทำให้องค์กรหยุดชะงักการผลิต ส่งผลเสียหายต่อธุรกิจขององค์กรเอง ต่อห่วงโซ่อุปทานที่เกี่ยวข้อง และต่อระบบเศรษฐกิจของประเทศได้ องค์กรจึงให้ผู้เชี่ยวชาญระดับสากลมาประเมินระบบการจัดการความมั่นคงปลอดภัยไซเบอร์ที่เป็นอยู่ เพื่อให้ทราบสถานะการจัดการของตนเอง พร้อมกับการหาช่องโหว่ที่เป็นความเสี่ยงจากภัยคุกคามไซเบอร์ และนำผลมากำหนดแผนงานปรับปรุงยกระดับในมิติต่างๆ ทั้งในด้านบริหารจัดการและด้านเทคนิคเพื่อให้เกิดประสิทธิผลและประสิทธิภาพ และเกิดความมั่นใจในความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น อาทิเช่น การจัดการ และกำกับดูแลด้านความมั่นคงปลอดภัย การบริหารความเสี่ยงไซเบอร์ ปฏิบัติการด้านความมั่นคงปลอดภัย ภูมิสถาปัตย์ และวิศวกรรมด้านความมั่นคงปลอดภัย ทั้งนี้องค์กรมีการติดตามการออกกฎหมายสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์โดยตลอด และยังได้นำกรอบแนวคิดของมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์และมาตรฐานเฉพาะที่เกี่ยวข้องกับอุตสาหกรรม ตลอดจนข้อแนะนำของผู้เชี่ยวชาญในระดับสากลมาเป็นแนวปฏิบัติในการดำเนินการด้วย

ในส่วนความเห็น แนวคิดจากผู้ทรงคุณวุฒิ และผู้เกี่ยวข้องขององค์กรตัวอย่างได้ชี้ให้เห็นความสำคัญเร่งด่วนที่ประเทศไทยต้องดำเนินการในเรื่องความมั่นคงปลอดภัยไซเบอร์ได้แก่

1. การจัดทำแผนแม่บทในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ที่ต้องกำหนดเจ้าภาพผู้รับผิดชอบให้ชัดเจนเพื่อเป็นผู้ผลักดันและประสานให้เกิดการปฏิบัติอย่างบูรณาการสัมฤทธิ์ผล ทั้งในส่วนของภาครัฐเอง และระหว่างภาครัฐกับภาคธุรกิจ

2. การผลักดันกฎหมายหลักด้านไซเบอร์ให้มีผลบังคับใช้ให้ทันกาล เพื่อช่วยให้หน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Services) ได้รับรู้ และเริ่มเตรียมการอย่างจริงจัง ลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่สามารถสร้างความเสียหายได้ตลอดเวลา

3. การพัฒนาบุคลากรระดับผู้ชำนาญการ และระดับที่ได้รับการรับรองคุณวุฒิด้านความมั่นคงปลอดภัยไซเบอร์ให้เพียงพอเพื่อสนับสนุนความแข็งแกร่งในเรื่องความมั่นคงปลอดภัยไซเบอร์ ทั้งในส่วนของภาครัฐ และภาคเอกชน ซึ่งอาจต้องใช้มาตรการด้านกฎหมายมาผลักดันให้เกิดการดำเนินการที่รวดเร็ว

4. การสร้างความตระหนักรู้ให้กับบุคลากรในองค์กร และภาคประชาชนทั่วไป เพื่อตระหนักในบทบาทของตนเอง ให้มีพฤติกรรมที่ถูกต้อง เพื่อลดความสุ่มเสี่ยงในการเป็นต้นเหตุและการเป็นเหยื่อจากภัยคุกคามไซเบอร์

ทั้งนี้แนวคิด ความเห็น และความเร่งด่วนสำคัญด้านการสร้างความมั่นคงปลอดภัยไซเบอร์จากผู้ทรงคุณวุฒิและผู้เกี่ยวข้องขององค์กรตัวอย่าง แนวทางการดำเนินการขององค์กรตัวอย่างเอง ในบทที่ 3 นี้ และข้อมูลนโยบายและแผนงานของภาครัฐที่กล่าวไว้ในบทที่ 2 จะถูกนำไปวิเคราะห์ร่วมกันในบทถัดไป เพื่อเสนอเป็นแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ที่เกิดประสิทธิผล และประสิทธิภาพมากยิ่งขึ้นสำหรับอุตสาหกรรมขนาดใหญ่

บทที่ 4
การวิเคราะห์แนวทางในการสร้างความมั่นคงปลอดภัยไซเบอร์

ประเทศไทยในการก้าวสู่ยุคไทยแลนด์ 4.0 ได้ให้ความสำคัญกับการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) มาก โดยได้กำหนดแนวทางการพัฒนาเรื่องนี้ไว้ในร่างยุทธศาสตร์ชาติ 20 ปี มีแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 และแผนปฏิบัติในระดับหน่วยงานของภาครัฐมารองรับ เช่น นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติของสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี เป็นต้น ดังแสดงความเชื่อมโยงดังกล่าวไว้ในแผนภาพที่ 2-1 ในบทที่ 2 นอกจากนี้ได้มีการร่างกฎหมายสำคัญคือ พ.ร.บ. ความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับประเทศ โดยกฎหมายฉบับนี้อยู่ระหว่างดำเนินการเพื่อให้สามารถออกมาบังคับใช้ได้ภายในปี พ.ศ. 2561 นี้

เนื่องจากภัยคุกคามไซเบอร์สามารถเกิดได้กับทุกองค์กรไม่ว่าภาครัฐหรือภาคธุรกิจ การป้องกันภัยดังกล่าวในขณะที่กฎหมายยังไม่มีผลบังคับใช้จึงขึ้นกับความตระหนักในภัยดังกล่าวของแต่ละองค์กร ในบทที่ 3 เป็นตัวอย่างขององค์กรหนึ่งที่อยู่ในอุตสาหกรรมขนาดใหญ่ที่ดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร เนื่องจากได้ตระหนักถึงภัยดังกล่าวที่มีต่อธุรกิจ แต่สำหรับบทนี้จะเป็นการวิเคราะห์เพื่อหาแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ โดยนำข้อมูลการดำเนินการขององค์กรตัวอย่างดังกล่าว มุมมองและแนวคิดของผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งของผู้เกี่ยวข้องในองค์กรตัวอย่างจากบทที่ 3 ร่วมกับข้อมูลงานวิจัยในบทที่ 2 ทั้งงานวิจัยของนักศึกษา วปอ. ข้อมูลการสำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. และข้อมูลการสำรวจดัชนีความมั่นคงปลอดภัยไซเบอร์ทั่วโลกของ ITU เพื่อหาแนวทางการดำเนินการที่มีประสิทธิผลและประสิทธิภาพ

แนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่

1. องค์ประกอบหลักในการสร้างความมั่นคงปลอดภัยไซเบอร์

จากการวิเคราะห์ข้อมูลงานวิจัยที่ศึกษามาในบทที่ 2 และข้อมูลขององค์กรตัวอย่างและผู้ทรงคุณวุฒิเกี่ยวกับแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ในบทที่ 3 สามารถสรุปองค์ประกอบหลักที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ได้ 12 เรื่อง ดังตารางที่ 4-1

ตารางที่ 4-1 องค์ประกอบหลักที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบหลัก	แหล่งข้อมูล					การอ้างอิง
	1	2	3	4	5	
1. โครงสร้างการจัดการและการกำกับ	✓		✓	✓	✓	1 = งานวิจัยนักศึกษา วปอ. 2 = ข้อมูล สพธอ. 3 = ข้อมูล ITU 4 = องค์กรตัวอย่าง 5 = ผู้ทรงคุณวุฒิและผู้เกี่ยวข้ององค์กรตัวอย่าง
2. ผู้นำ บทบาทความรับผิดชอบ	✓	✓	✓	✓	✓	
3. นโยบายและแผน	✓		✓	✓	✓	
4. กฎหมาย / มาตรฐาน / แนวปฏิบัติ	✓	✓	✓	✓	✓	
5. เทคโนโลยีและการพัฒนา	✓	✓	✓	✓	✓	
6. การบริหารความเสี่ยง		✓		✓	✓	
7. การกำกับให้เกิดการปฏิบัติ			✓	✓	✓	
8. ความสามารถบุคลากร	✓	✓	✓	✓	✓	
9. ความตระหนักรู้บุคลากร	✓	✓	✓	✓	✓	
10. การเตรียมความพร้อมและความสามารถการรับมือ	✓	✓	✓	✓	✓	
11. เครือข่ายและความร่วมมือ	✓	✓	✓	✓	✓	
12. งบประมาณ				✓	✓	

ที่มา : ยุทธนา เจียมตระการ, 2561.

จะเห็นได้ว่ามี 7 องค์ประกอบหลักที่ทุกแหล่งข้อมูลเห็นตรงกันว่ามีความสำคัญ ได้แก่ ผู้นำ บทบาทความรับผิดชอบ กฎหมาย / มาตรฐาน / แนวปฏิบัติ เทคโนโลยีและการพัฒนาความสามารถบุคลากร ความตระหนักรู้บุคลากร การเตรียมความพร้อมและความสามารถการรับมือและเครือข่ายและความร่วมมือ นอกจากนี้ ITU ซึ่งเป็นองค์กรสากลได้ให้ความสำคัญในอีก 3 องค์ประกอบหลักเพิ่มเติม ได้แก่ โครงสร้างการจัดการและการกำกับ นโยบายและแผน และการกำกับให้เกิดการปฏิบัติ

2. การสร้างความมั่นคงปลอดภัยไซเบอร์ขององค์กรตัวอย่าง

โดยทั่วไป การที่องค์กรใดจะมีการเปลี่ยนแปลงแนวปฏิบัติอย่างมีนัยสำคัญหรือสร้างแนวปฏิบัติใหม่ขึ้นมา ต้องมาจากการเล็งเห็นผลกระทบที่สามารถเกิดกับองค์กรได้หากไม่ทำการเปลี่ยนแปลง องค์กรตัวอย่างที่กล่าวไว้ในบทที่ 3 ก็เช่นกัน จากการวิเคราะห์ลำดับเหตุการณ์ที่ทำให้องค์กรตัวอย่างมีการจัดทำแผนเพื่อยกระดับการสร้างความมั่นคงปลอดภัยไซเบอร์ให้สูงขึ้น เป็นดังนี้

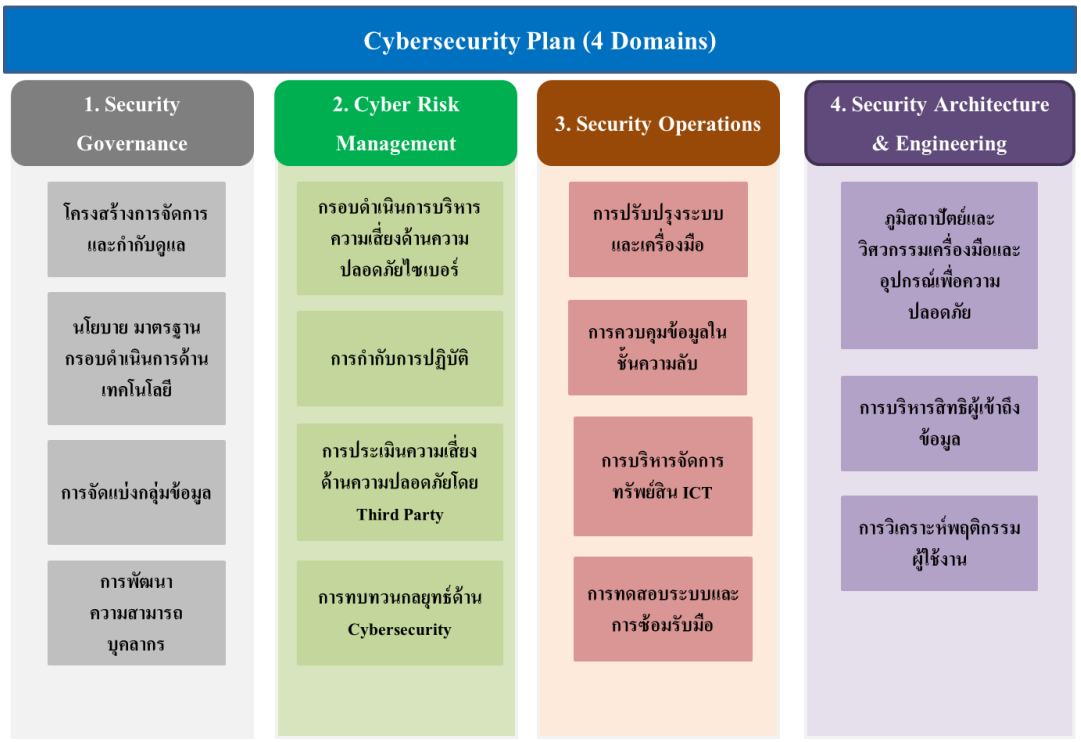
2.1 องค์กรใช้หลักการบริหารจัดการความเสี่ยง ที่มีทั้งคณะกรรมการบริษัทและคณะผู้บริหารบริษัท กำกับ ดูแลและบริหารจัดการความเสี่ยงขององค์กร ดังแผนภาพที่ 3-1 โครงสร้างการบริหารงานขององค์กร ในบทที่ 3

2.2 องค์กรมีการประเมินความเสี่ยงของภัยคุกคามไซเบอร์ผ่านการศึกษาองค์กรอื่นทั้งจากแหล่งข้อมูลที่ค้นหาได้และผู้ทรงคุณวุฒิ และนำเสนอให้ผู้บริหารระดับสูงขององค์กรทราบตามโครงสร้างการบริหารจัดการความเสี่ยงขององค์กร

2.3 ผู้บริหารระดับสูงเห็นชอบและให้การสนับสนุนงบประมาณในการจ้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์มาตรวจประเมินเพื่อค้นหาช่องโหว่ในระบบ ITC ขององค์กร

2.4 ผลการประเมินทำให้องค์กรทราบช่องโหว่ที่ยังมีอยู่ในระบบ และได้จัดทำแผนเพื่อยกระดับการสร้างความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาตามความเสี่ยงออกมาเป็น 4 Domains ดังแผนภาพที่ 4-1 และแบ่งการดำเนินการออกเป็น 3 ระดับตามระยะเวลา เพื่อให้การบริหารกำลังพลและงบประมาณเกิดประสิทธิผลและประสิทธิภาพ

แผนภาพที่ 4-1 Cybersecurity Plan (4 Domains) ขององค์กรตัวอย่าง



ที่มา : ยุทธนา เจียมตระการ, 2561.

จากลำดับเหตุการณ์ข้างต้น จะเห็นว่าการที่องค์กรตัวอย่างมีการปรับปรุงเพื่อยกระดับการสร้างความมั่นคงปลอดภัยไซเบอร์ มาจากการที่องค์กรมีการบริหารจัดการความเสี่ยง ทำให้เล็งเห็นอันตรายของภัยคุกคามไซเบอร์ และทีมผู้บริหารระดับสูงขององค์กรมีวิสัยทัศน์และภาวะผู้นำในเรื่องนี้

3. แนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่

เมื่อวิเคราะห์องค์ประกอบหลักที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ จากตารางที่ 4-1 เปรียบเทียบกับ Cybersecurity Plan (4 Domains) ขององค์กรตัวอย่างตามแผนภาพที่ 4-1 พบว่ามีบางองค์ประกอบหลักไม่ได้ถูกระบุอยู่ในแผนยกระดับขององค์กรตัวอย่างดังตารางที่ 4-2

ตารางที่ 4-2 การเปรียบเทียบองค์ประกอบหลัก (จากตารางที่ 4-1) กับ Cybersecurity Plan (4 Domains)

องค์ประกอบหลัก (จากตารางที่ 4-1)	Cybersecurity Plan (4 Domains)	
	ระบุ / ไม่ระบุ	Domain ที่เกี่ยวข้อง
1. โครงสร้างการจัดการและการกำกับ	ระบุ	Domain 1
2. ผู้นำ บทบาทความรับผิดชอบ	ไม่ระบุ	-
3. นโยบายและแผน	ระบุ	Domain 1 และ 2
4. กฎหมาย / มาตรฐาน / แนวปฏิบัติ	ระบุ	Domain 1 (แต่ขาดเรื่องกฎหมาย)
5. เทคโนโลยีและการพัฒนา	ระบุ	Domain 1 และ 4
6. การบริหารความเสี่ยง	ระบุ	Domain 2
7. การกำกับให้เกิดการปฏิบัติ	ระบุ	Domain 2
8. ความสามารถบุคลากร	ระบุ	Domain 1
9. ความตระหนักรู้บุคลากร	ไม่ระบุ	-
10. การเตรียมความพร้อมและความสามารถการรับมือ	ระบุ	Domain 3
11. เครือข่ายและความร่วมมือ	ไม่ระบุ	-
12. งบประมาณ	ไม่ระบุ	-

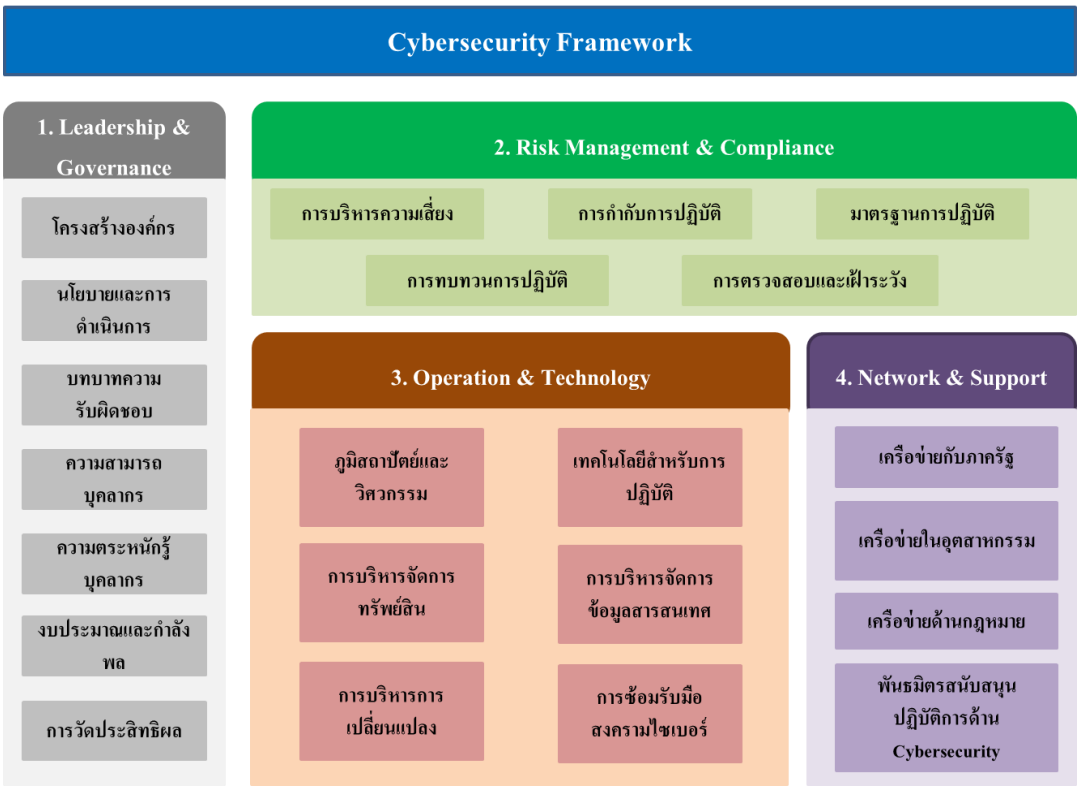
ที่มา : ยุทธนา เจียมตระการ, 2561.

จากตารางที่ 4-2 ข้างต้น จะเห็นว่าส่วนที่ไม่มีการระบุอยู่ใน Cybersecurity Plan (4 Domains) จะเป็นส่วนที่เกี่ยวกับบทบาทของผู้บริหารระดับสูง ได้แก่ ผู้นำ บทบาทความรับผิดชอบ ความตระหนักรู้บุคลากร และงบประมาณ หรือส่วนที่อยู่นอกขอบข่ายขององค์กร ได้แก่ กฎหมาย เครือข่ายและความร่วมมือ

ด้วยเหตุนี้ เพื่อให้การวิเคราะห์หาแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่มีความครบถ้วน จึงนำข้อมูลองค์ประกอบหลักในตารางที่ 4-1 มาวิเคราะห์เป็นแกนหลัก ร่วมกับตัวแปรอื่น ได้แก่ ผู้ดำเนินการ บทบาทการดำเนินการ ขอบข่ายงาน

(ภายในหรือ ภายนอกองค์กร) และได้วิเคราะห์ออกมาเป็นกรอบดำเนินการในการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ประกอบด้วย 4 กรอบย่อย ดังแผนภาพที่ 4-2 โดยกรอบย่อยที่ 1 เป็นส่วนบทบาทของผู้นำ กรอบย่อยที่ 2 เป็นส่วนการปฏิบัติที่สนับสนุนการบริหารจัดการและการกำกับ ส่วนกรอบย่อยที่ 3 และ 4 เป็นส่วนการปฏิบัติและดำเนินการทั้งภายในและภายนอกภายใต้แนวปฏิบัติของกรอบย่อยที่ 2

แผนภาพที่ 4-2 กรอบดำเนินการในการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)



ที่มา : ยุทธนา เจียมตระการ, 2561.

รายละเอียดของแต่ละกรอบย่อย เป็นดังนี้

1. ด้านการนำและกำกับดูแล (Leadership and Governance)

เป็นกรอบดำเนินการเกี่ยวกับการกำกับและบริหารจัดการด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยโครงสร้างองค์กรด้านการกำกับและการบริหารจัดการ นโยบายและการดำเนินการ บทบาทความรับผิดชอบการดำเนินการทั้งระดับคณะกรรมการ

หน่วยงาน และผู้รับผิดชอบ การพัฒนาบุคลากร การสร้างความตระหนักรู้ การจัดสรรทรัพยากรทั้งงบประมาณและกำลังพล และการวัดประสิทธิผล

สิ่งสำคัญของกรอบย่อยที่ 1 คือ วิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงเพื่อให้เกิดการสนับสนุนการดำเนินการเรื่องนี้อย่างจริงจังในองค์กร

2. ด้านการบริหารความเสี่ยงและกำกับการปฏิบัติ (Risk Management and Compliance) เป็นการดำเนินการเกี่ยวกับการบริหารความเสี่ยงและการกำกับให้เกิดการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามนโยบายและวัตถุประสงค์ขององค์กร ประกอบด้วย การบริหารความเสี่ยง การกำกับการปฏิบัติ มาตรฐานการปฏิบัติ การทบทวนการปฏิบัติ และการตรวจสอบและเฝ้าระวัง

สิ่งสำคัญของกรอบย่อยที่ 2 คือการประเมินความเสี่ยงของกิจกรรมที่เกี่ยวข้องกับไซเบอร์ได้อย่างครอบคลุมทั่วถึง และการกำกับให้เกิดการปฏิบัติตามมาตรฐานการปฏิบัติที่องค์กรได้กำหนดไว้

3. ด้านการปฏิบัติและเทคโนโลยี (Operation and Technology)

เป็นการดำเนินการด้านการปฏิบัติและเทคโนโลยีที่นำมาใช้ในองค์กรให้มีความปลอดภัยจากภัยคุกคามไซเบอร์ ประกอบด้วย ภูมิสถาปัตย์และวิศวกรรม เทคโนโลยีสำหรับการปฏิบัติ การบริหารจัดการทรัพย์สิน การบริหารจัดการข้อมูลสารสนเทศ การบริหารการเปลี่ยนแปลง การซ้อมรับมือสงครามไซเบอร์ เป็นต้น

สิ่งสำคัญสำหรับกรอบย่อยที่ 3 คือการออกแบบภูมิสถาปัตย์และวิศวกรรม และการเลือกใช้เทคโนโลยีในการป้องกันภัยไซเบอร์ได้อย่างเหมาะสม และเนื่องจากภัยไซเบอร์ไม่สามารถป้องกันได้ 100% การเตรียมความพร้อมโดยการซ้อมรับมือแบบการทำสงครามไซเบอร์รวมถึงการฟื้นฟูภายหลังเหตุการณ์จึงเป็นเรื่องจำเป็นมาก

4. ด้านเครือข่ายและการสนับสนุน (Network and Support)

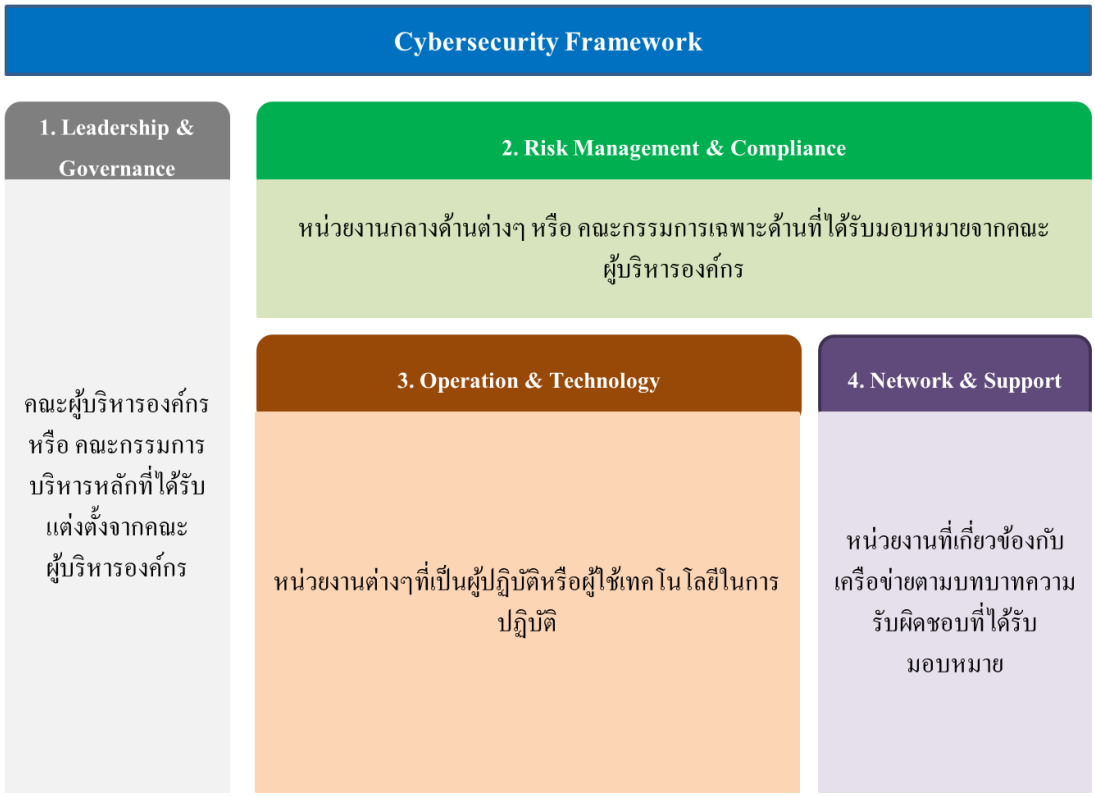
เป็นการดำเนินการด้านเครือข่ายกับภายนอก และพันธมิตรคู่ธุรกิจที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย เครือข่ายกับภาครัฐ เครือข่ายในอุตสาหกรรม เครือข่ายด้านกฎหมาย พันธมิตรสนับสนุนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

สิ่งสำคัญสำหรับกรอบย่อยที่ 4 คือ การสร้างเครือข่ายร่วมกันระหว่างภาครัฐและภาคธุรกิจ และระหว่างภาคธุรกิจที่อยู่ในอุตสาหกรรมเดียวกัน เพื่อการแบ่งปัน เรียนรู้ และช่วยเหลือกัน ทั้งการป้องกันภัยและการเตือนภัยที่เกิดประสิทธิผลและประสิทธิภาพมากขึ้น

ทั้งนี้ จากการวิเคราะห์จะเห็นว่า แต่ละกรอบย่อยมีบทบาทดำเนินการที่แตกต่างกัน ได้แก่ บทบาทการจัดการและกำกับ บทบาทการกำหนดมาตรฐานและควบคุมให้เกิดการปฏิบัติ

บทบาทการปฏิบัติและดำเนินการ และบทบาทการสร้างเครือข่ายและพันธมิตรคู่ธุรกิจกับภายนอก สามารถวิเคราะห์และสรุปผู้เกี่ยวข้องหลักในแต่ละกรอบย่อยเพื่อเป็นข้อมูลในการดำเนินการ ดังแผนภาพที่ 4-3

แผนภาพที่ 4-3 ผู้เกี่ยวข้องหลักใน Cybersecurity Framework



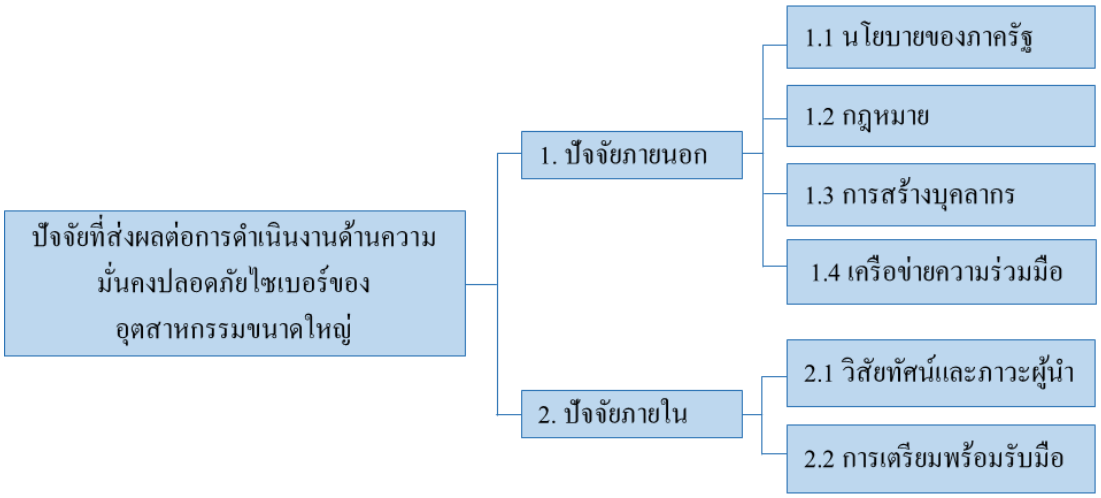
ที่มา : ยุทธนา เจียมตระการ, 2561.

ปัจจัยสำคัญในการดำเนินการ

จากองค์ประกอบหลักในการสร้างความมั่นคงปลอดภัยไซเบอร์ที่ได้กล่าวมาแล้วข้างต้น หากวิเคราะห์ต่อไปจะพบว่า มีปัจจัยสำคัญที่เป็นตัวแปรต่อการปฏิบัติ (Execution) ขององค์กรทางธุรกิจ ซึ่งจะสามารถเสริมอัตราเร่งในการเกิดประสิทธิผลและประสิทธิภาพการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ได้เป็นอย่างดี และจะไม่เพียงช่วยองค์กรในลักษณะเป็นวงแคบเท่านั้น หากจัดการกับปัจจัยสำคัญเหล่านี้ให้ดีพอ จะช่วยในการขับเคลื่อนการดำเนินการ

สร้างความมั่นคงปลอดภัยไซเบอร์ให้ขยายวงไปสู่ความมีประสิทธิผลและประสิทธิภาพในระดับประเทศได้สำเร็จด้วย ปัจจัยที่กล่าวถึงนี้แสดงในแผนภาพที่ 4-4

แผนภาพที่ 4-4 ปัจจัยที่ส่งผลต่อการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมขนาดใหญ่



ที่มา : ยุทธนา เจียมตระการ, 2561.

รายละเอียดสามารถอธิบายได้ดังนี้

1. ปัจจัยภายนอก

1.1 นโยบายของภาครัฐ

นโยบายที่ชัดเจนของภาครัฐคือปัจจัยที่สำคัญเป็นอันดับที่ 1 เพราะการตั้งโจทย์ที่ชัดเจน จึงจะทำให้สามารถถ่ายทอดจากระดับนโยบายไปสู่การปฏิบัติได้จริง ความชัดเจนจะเกิดขึ้นได้ ต้องมีการกำหนดแผนแม่บท เป้าหมาย ขอบข่ายมุ่งเน้น แนวทางปฏิบัติ ทรัพยากรสนับสนุน นอกจากนี้ต้องกำหนดดัชนีวัดความสำเร็จในระดับประเทศ เพื่อใช้เป็นตัวตรวจสอบความมีประสิทธิผลและประสิทธิภาพ และที่ขาดไม่ได้คือต้องมีหน่วยงานเจ้าภาพที่ทำหน้าที่สื่อสารผลักดันและสร้างความร่วมมือ ซึ่งจะส่งผลให้องค์กรธุรกิจและองค์กรที่เกี่ยวข้องสามารถตั้งเป้าหมายและกำหนดกิจกรรมดำเนินการได้สอดคล้องกับนโยบายและการลงทุนของภาครัฐ เกิดความเชื่อมโยงผลสัมฤทธิ์ไปสู่ผลลัพธ์โดยรวมตามเป้าประสงค์ใหญ่อย่างมีประสิทธิภาพ ตัวอย่างในการจัดการปัจจัยเรื่องนโยบายของภาครัฐ จากประเทศที่มีความพร้อมในการรับมือกับภัยคุมคาม

ไซเบอร์ที่ดีอยู่ในระดับ Top 20 ของโลก (จากการจัดอันดับของ World Economic Forum 2017)[1] แสดงได้ดังนี้

สหราชอาณาจักร[2] ได้มีการกำหนดกลยุทธ์แห่งชาติ (National Cyber Security Strategy) และแสดงเป้าหมายไว้ชัดเจนว่า "จะให้อังกฤษเป็นประเทศที่ปลอดภัยที่สุดในโลกในเรื่องธุรกิจออนไลน์ (Online Business)" โดยมีเจ้าภาพคือ Cabinet Office เป็นผู้รับผิดชอบในการขับเคลื่อนความสำเร็จ และกำหนดแผนแม่บทระยะ 6 ปี แบ่งเป็น 3 ด้าน คือ **การป้องกัน การยับยั้งและการพัฒนา** ทำให้เกิดความชัดเจนในความร่วมมือกับทุกส่วนที่เกี่ยวข้อง และเกิดความก้าวหน้าทั้งในภาคธุรกิจและภาครัฐไปทิศทางเดียวกันในการสร้างความมั่นคงปลอดภัย ดังนี้ **การป้องกัน** ทำให้เกิดความร่วมมือกับภาคเอกชนในการสร้างระบบป้องกันภัยคุกคามเพื่อป้องกันหน่วยงานโครงสร้างพื้นฐาน (Critical Infrastructures) **การยับยั้ง** ทำให้เกิดความร่วมมือกับนานาชาติในการยกระดับความสามารถของเจ้าหน้าที่รักษากฎหมาย เพื่อลดความสำเร็จในการก่ออาชญากรรมไซเบอร์ และ**การพัฒนา** ทำให้เกิดการเติบโตของกลุ่มบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเร่งพัฒนาแรงงาน เพื่อสร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น

สหรัฐอเมริกา[3] ได้กำหนดนโยบายที่ชัดเจนในการสร้างความมั่นคงปลอดภัยไซเบอร์เป็นยุทธศาสตร์ชาติ และแสดงเป้าประสงค์ "เพื่อโลกไซเบอร์ที่ปลอดภัย" มีหน่วยงานความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security: DHS) เป็นเจ้าภาพ ทั้งกำหนดแนวปฏิบัติทำให้เกิดการเข้ามามีบทบาทในการสร้างความมั่นคงปลอดภัยไซเบอร์ร่วมกันของทุกส่วนทั้งองค์กรรัฐบาล สำนักงานท้องถิ่น องค์กรเอกชน รวมถึงพลเรือน โดยเน้นความสำคัญเร่งด่วนในการปกป้องโครงสร้างพื้นฐานที่สำคัญจากการโจมตีไซเบอร์ ภาคธุรกิจที่อยู่ในกลุ่มโครงสร้างพื้นฐานที่สำคัญจึงได้รับการสนับสนุนจากทางภาครัฐและให้ความร่วมมือระหว่างกันอย่างเต็มที่ ทั้งแนวปฏิบัติที่ได้กำหนดขึ้น ก็ช่วยสร้างสิ่งแวดล้อมทางไซเบอร์ที่ปลอดภัย จากการสร้างวัฒนธรรมที่ปลอดภัยร่วมกัน

---

[1] "It's time to think differently about cyber security". (Online). Available: www.weforum.org/agenda/2017/06/how-to-win-the-cyber-war/, 2017.

[2] "UK is going to open the National Cyber Security Centre with 700 experts". (Online). Available: securityaffairs.co/wordpress/51864/cyber-crime/national-cyber-security-centre.html, 2016.

[3] "About DHS - Mission". (Online). Available: www.dhs.gov/mission, 2016.

1.2 กฎหมาย

กฎหมายที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และอาชญากรรมไซเบอร์เป็นอีกปัจจัยสำคัญต่อการเพิ่มความมีประสิทธิผลและประสิทธิภาพในการปฏิบัติขององค์กรธุรกิจ เนื่องจากหากกฎหมายไซเบอร์ที่สำคัญต่อการปฏิบัติและสอดคล้องกับนโยบายของภาครัฐออกมาได้รวดเร็วก็จะช่วยเร่งการสร้างแผนงาน กิจกรรม และการจัดสรรทรัพยากรสนับสนุน เพื่อรองรับการปฏิบัติ รวมทั้งเกิดความร่วมมือในด้านต่างๆ ขององค์กรที่เกี่ยวข้องเพื่อให้องค์กรสามารถปฏิบัติได้สอดคล้องกับข้อกำหนดตามกฎหมายอย่างทันกาล เช่น การสร้างบุคลากร องค์ความรู้ เครือข่าย ที่เกี่ยวข้องกับการจัดการไซเบอร์อย่างปลอดภัย

ตัวอย่างในการจัดการปัจจัยเรื่องกฎหมายที่ดี อาทิเช่น ประเทศสิงคโปร์[4] ซึ่งมีเป้าหมายนำประเทศไปสู่การเป็น Smart Nation ได้บังคับใช้กฎหมายความมั่นคงปลอดภัยไซเบอร์ฉบับใหม่ ในปีพ.ศ. 2560 สอดคล้องกับแผนความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ออกใหม่ในปี พ.ศ. 2559 ที่เน้นในเรื่อง การป้องกัน การตอบสนองอาชญากรรมไซเบอร์อย่างรวดเร็ว การบังคับใช้กฎหมายอย่างจริงจัง และการร่วมมือกับหน่วยงานพันธมิตร ส่งผลให้เกิดการเร่งพัฒนาบุคลากรและหามาตรการส่งเสริมเพื่อดึงดูดคนให้ทำงานด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เช่น การมีเส้นทางความก้าวหน้าในการทำงานที่ชัดเจน การเพิ่มตำแหน่งงานด้านไซเบอร์ การสร้างหลักสูตร Cyber Security Associates and Technologists เพื่อรับบุคลากรที่มีประสบการณ์ในเรื่องนี้มาก่อน 3 ปี ให้เข้าอบรมหลักสูตรความมั่นคงปลอดภัยไซเบอร์เพิ่มเติมอีก 6 เดือน และการแลกเปลี่ยนบุคลากรที่มีความเชี่ยวชาญไซเบอร์ระหว่างภาคเอกชนและภาครัฐ เป็นต้น

1.3 การสร้างบุคลากร

การมีบุคลากรที่มีความตระหนัก ความรู้ และความเชี่ยวชาญในเรื่องความมั่นคงปลอดภัยไซเบอร์ที่พร้อมต่อการเข้าปฏิบัติงาน เป็นอีกปัจจัยสำคัญที่ส่งผลต่อความมีประสิทธิผล และประสิทธิภาพในการปฏิบัติขององค์กรธุรกิจเช่นกัน ปัจจุบันได้เกิดปัญหาการขาดแคลนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ทั่วโลก แม้กระทั่งในสหรัฐอเมริกา ประเทศในยุโรป ประเทศในแถบเอเชีย รวมทั้งในประเทศไทยด้วย ซึ่งจะเป็นอุปสรรคต่อการตอบสนองนโยบายและกฎหมายในการสร้างความมั่นคงปลอดภัยไซเบอร์ได้ทันกาล แต่เรื่องนี้จะเปลี่ยนเป็นปัจจัยแห่งความสำเร็จได้ หากสามารถวางแผน สร้างความร่วมมือและจัดการได้ทันท่วงที ได้มี

---

[4] “National cybersecurity strategy aims to make Smart Nation safe: PM Lee”. (Online). Available: www.channelnewsasia.com/news/singapore/national-cybersecurity-strategy-aims-to-make-smart-nation-safe-p-7743784, 2016.

ความพยายามในการแก้ปัญหาดังกล่าวเพื่อสร้างบุคลากรไซเบอร์ให้พร้อมต่อการใช้งาน ที่น่าสนใจ อาทิเช่น

ในประเทศมาเลเซีย[5] มีความร่วมมือในการก่อตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์ UK-APAC Center of Security Excellence โดยตั้งเป้าหมายในการพัฒนาบุคลากรในด้านนี้ให้ได้ 2 ล้านคน ภายในปีพ.ศ. 2562 ทั้งในเรื่องการสร้างความตระหนัก กำหนดยุทธศาสตร์ ส่งเสริมงานวิจัย และเพิ่มโอกาสในการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ โดยหลักสูตรที่ใช้ในการเรียนการสอนจะเป็นเนื้อหาที่ได้รับการรับรองจากหน่วยงาน Government Communication Headquarters (GCHQ) ของสหราชอาณาจักร ซึ่งจะส่งผลให้มีบุคลากรด้านไซเบอร์ที่เพียงพอต่อการใช้งานในประเทศทั้งภาครัฐ และภาคธุรกิจ และยังสามารถขยายไปสู่ประเทศอื่นในเอเชียแปซิฟิกได้อีกด้วย

ในประเทศญี่ปุ่น[6] กระทรวงกิจการภายในและการสื่อสาร (The Internal Affairs and Communications Ministry) มีแผนในปี พ.ศ.2560 ในการก่อตั้งหน่วยงานใหม่ ภายใต้การดูแลของสถาบันวิจัยเทคโนโลยีสารสนเทศแห่งชาติ (National Institute of Information and Communications Technology : NICT) ทำหน้าที่วิจัยและพัฒนาเพื่อผลิต White Hat Hacker ที่มีความรู้และทักษะพร้อมรับมือการโจมตีทางไซเบอร์ให้ได้ 100 คนต่อปี และจะส่งผู้เรียนที่มีทักษะความสามารถดีเยี่ยมไปฝึกอบรมต่อในมหาวิทยาลัยชั้นนำแห่งสหรัฐอเมริกาหรือประเทศในแถบยุโรป ที่มีเทคโนโลยีและการวิจัยที่ก้าวหน้า ซึ่งจะทำให้มีเจ้าหน้าที่ของรัฐ ที่มีความรู้ความสามารถในการสนับสนุนภาคธุรกิจได้ด้วย

ในประเทศสิงคโปร์[7] มหาวิทยาลัยแห่งชาติสิงคโปร์ (National University of Singapore : NUS) ได้ร่วมมือกับ Singtel ผู้ให้บริการเครือข่ายโทรศัพท์มือถือรายใหญ่ เปิดศูนย์วิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีแผนการพัฒนาบุคลากรเพื่อรองรับความต้องการสายงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ในการสร้างนักวิจัย 100 คน และ

---

[5] "Malaysia to Establish Cybersecurity Academy". (Online). Available: www.infosecurity-magazine.com/news/malaysia-to-establish/, 2016.

[6] "ญี่ปุ่นเตรียมตั้งหน่วยงานฝึก white-hat hacker ตั้งเป้าอย่างน้อยปีละ 100 คน". (ออนไลน์). เข้าถึงได้จาก: www.thaicert.or.th/newsbite/2016-09-06-01.html, 2559.

[7] "Singapore university partners Singtel to launch $30M cybersecurity lab". (Online). Available: www.zdnet.com/article/singapore-university-partners-singtel-to-launch-30m-cybersecurity-lab/, 2016.

บุคลากรทางด้านความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ระดับปริญญาตรีจนถึงปริญญาเอก 120 คน ภายใน 5 ปี

1.4 เครือข่ายความร่วมมือ

การมีเครือข่ายความร่วมมือ หรือส่งเสริมให้เกิดเครือข่ายความร่วมมือจากภาครัฐก็เป็นอีกปัจจัยสำคัญที่จะช่วยให้การปฏิบัติขององค์กรธุรกิจ มีประสิทธิผลและประสิทธิภาพ ทั้งความร่วมมือในเรื่องการแลกเปลี่ยนข่าวสารข้อมูล องค์ความรู้ เทคโนโลยี แนวปฏิบัติ ความตระหนักและความรู้ของบุคลากร การตรวจจับ การซ้อมรับมือ การฟื้นฟูสภาพ โดยจะช่วยให้องค์กรมีความสามารถตอบสนองต่อนโยบายและกฎหมายของประเทศชาติได้อย่างรวดเร็วขึ้นด้วย ตัวอย่างการสร้างเครือข่ายความร่วมมือ ได้แก่

สหราชอาณาจักร[8] หน่วยงานความมั่นคงปลอดภัยไซเบอร์ (National Cyber Security Centre: NCSC) ซึ่งมีผู้เชี่ยวชาญไซเบอร์กว่า 70 คนได้สร้างเครือข่ายความร่วมมือกับธนาคารกลางแห่งประเทศอังกฤษ ในการสร้างความตระหนักด้านภัยคุกคามทางไซเบอร์ที่มีผลกระทบกับสถาบันการเงิน ซึ่งความร่วมมือเช่นนี้จะส่งผลต่อองค์กรทางการเงินอื่นๆ ในประเทศด้วย

ประเทศญี่ปุ่น[9] มีหน่วยงาน Industrial Cybersecurity Promotion Agency (ICPA) ที่รับมือการโจมตีทางไซเบอร์ โดยหน่วยงานนี้ได้สร้างเครือข่ายด้านงานวิจัยกับมหาวิทยาลัยทั้งในและต่างประเทศ เพื่อสร้างองค์ความรู้ และสร้างเครือข่ายร่วมกับนานาชาติ เพื่อป้องกันเชิงรุก ในรูปแบบที่ให้ผู้เชี่ยวชาญมาตรวจวิเคราะห์การโจมตีและการระวังภัยคุกคามในอุตสาหกรรมโครงสร้างสาธารณูปโภคที่มีความสำคัญ เช่น ไฟฟ้า ก๊าซ น้ำมัน โรงงานเคมี และโรงงานนิวเคลียร์

2. ปัจจัยภายในองค์กร

นอกจากปัจจัยภายนอกแล้ว ปัจจัยภายในก็เป็นเรื่องที่ต้องคำนึงถึงและเป็นหัวใจสำคัญ ในการสร้างความมั่นคงปลอดภัยไซเบอร์ ซึ่งได้พิจารณาให้ลำดับความสำคัญของปัจจัยภายในดังนี้

---

[8] “The UK Government confirms the opening of the UK first national anti-cybercrime centre, the National Cyber Security Centre (NCSC)”. (Online). Available: securityaffairs.co/wordpress/51864/cyber-crime/national-cyber-security-centre.html, 2016.

[9] “Japan to Create Cyber-Defense Government Agency to Protect SCADA Infrastructures”. (Online). Available: news.softpedia.com/news/japan-to-create-cyber-defense-government-agency-to-protect-scada-infrastructures-504293.shtml, 2016.

2.1 วิสัยทัศน์และภาวะผู้นำ

วิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูง เป็นปัจจัยสำคัญที่สุดในการนำพาองค์กรไปสู่เป้าหมาย การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรต้องเริ่มจากความตระหนักของผู้บริหารระดับสูงเพื่อเอื้อให้เกิดการสนับสนุนในด้านต่างๆ

1. ด้านงบประมาณ ตั้งแต่การลงทุนเทคโนโลยี การพัฒนาบุคลากรผู้เชี่ยวชาญ การว่าจ้างผู้เชี่ยวชาญ

2. ด้านการบริหารจัดการ ตั้งแต่การปรับโครงสร้างองค์กร กำหนดบทบาทผู้รับผิดชอบ ตลอดจนแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้อง เพื่อให้เกิดความแข็งแกร่งในเรื่องความมั่นคงปลอดภัยไซเบอร์

3. ด้านบุคลากร ทั้งในมิติบุคลากรผู้เชี่ยวชาญ ตั้งแต่การจัดสรรบุคลากรให้เพียงพอ และการพัฒนาความรู้ความสามารถให้ได้ตามมาตรฐานสากล และมิติบุคลากรทั่วไปที่ต้องได้รับการส่งเสริมให้เกิดความตระหนักรู้ และปฏิบัติได้อย่างถูกต้องตามแนวทางที่กำหนด

ดังมีตัวอย่างของกลุ่มธุรกิจธนาคารในประเทศไทย ซึ่งผู้บริหารแต่ละธนาคารตระหนักถึงภัยคุกคามไซเบอร์ ที่สร้างความเสียหายทั้งด้านการเงินและชื่อเสียง ส่งผลให้เกิดการลงทุนในเทคโนโลยีต่างๆ เพื่อรองรับภัยคุกคามมาอย่างต่อเนื่อง[10] นอกจากนี้สมาคมธนาคารไทยโดยความร่วมมือของธนาคารพาณิชย์ทั้ง 15 แห่ง ได้จัดตั้งกลุ่มความร่วมมือสถาบันการเงินภายใต้ชื่อศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector Computer Emergency Response (TB-CERT)[11] โดยมีวัตถุประสงค์ เพื่อยกระดับความร่วมมือของสถาบันการเงินในการสร้างความมั่นคงปลอดภัยไซเบอร์ ได้แก่

1. การแลกเปลี่ยนข้อมูลทั้งภัยคุกคามทางด้านไซเบอร์และแนวทางการแก้ไขตามแนวทางสากล

2. การสร้างมาตรฐานกลางด้านความมั่นคงปลอดภัยของการใช้เทคโนโลยี

---

[10] "ก่อนที่ไทยจะเป็นสังคมไร้เงินสด มารู้จัก TB-CERT ดึง 15 ธนาคารเข้าร่วม ตั้งทีมปลอดภัยไซเบอร์". (ออนไลน์). เข้าถึงได้จาก: brandinside.asia/tb-cert-security-cyber-finance/, 2560.

[11] "สมาคมธนาคารไทยจัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ภาคการธนาคารยกระดับมาตรฐานเทียบเท่าสากล". (ออนไลน์). เข้าถึงได้จาก: www.scb.co.th/th/news/2017-10-04/nws-tb-cert, 2560.

3. การกำหนดกระบวนการในการรับมือภัยไซเบอร์ในภาคการธนาคาร และการจัดซ้อมรับมือร่วมกันอย่างสม่ำเสมอ

4. การส่งเสริมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมทั้งการสร้างบุคลากรใหม่ และการพัฒนาบุคลากรเดิมให้มีความรู้เพิ่มขึ้นตลอดจนสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้เทียบเท่ามาตรฐานสากล

2.2 การเตรียมพร้อมรับมือ

เนื่องจากภัยคุกคามไซเบอร์มีรูปแบบใหม่เกิดขึ้นตลอดเวลา การรับมือการโจมตีที่ดีที่สุดคือการเตรียมความพร้อม ความพร้อมในที่นี้หมายรวมตั้งแต่ ความพร้อมของบุคลากรทั้งความตระหนักรู้ ความรู้ความสามารถ และความเพียงพอของผู้เชี่ยวชาญด้านการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ ความพร้อมของเทคโนโลยีในการตรวจจับ ป้องกัน และรับมือก่อนและหลังการโจมตี และความพร้อมในการบริหารจัดการที่ทำให้ธุรกิจสามารถดำเนินการได้ต่อเนื่องแม้ถูกโจมตี (Business Continuity Management) รวมทั้งการฟื้นฟูภายหลังการโจมตี

นอกจากนี้จำเป็นต้องมีการซ้อมปฏิบัติการรับมือจริงที่เรียกว่า การซ้อมหนีไฟทางไซเบอร์ (Cyber Drill) โดยเป็นการจำลองสถานการณ์โจมตีเสมือนจริง เพื่อให้ผู้เกี่ยวข้องได้เรียนรู้การปฏิบัติที่ไม่ใช่แค่ทฤษฎี และทีมผู้เชียวชาญด้านความมั่นคงปลอดภัยไซเบอร์ จะได้นำจุดอ่อนต่างๆ จากการซ้อมมาปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้ดียิ่งขึ้น โดยเฉพาะจุดอ่อนจากพฤติกรรมของกลุ่มคนที่เป็นเหยื่อการโจมตี การซ้อมนี้ควรมีแผน และดำเนินการเป็นประจำ เช่นเดียวกันกับการซ้อมหนีไฟ เพื่อกระตุ้นให้เกิดความคุ้นเคยในการปฏิบัติจริง และสร้างความตระหนักอย่างสม่ำเสมอ

สรุป

จากการใช้ข้อมูลงานวิจัยในบทที่ 2 และข้อมูลองค์กรตัวอย่างและผู้ทรงคุณวุฒิในบทที่ 3 สามารถวิเคราะห์องค์ประกอบหลัก และกรอบดำเนินการในการสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) สำหรับอุตสาหกรรมขนาดใหญ่ ซึ่งประกอบด้วย 4 กรอบย่อย ได้แก่ ด้านการนำและกำกับดูแล (Leadership and Governance) ด้านการบริหารความเสี่ยงและกำกับการปฏิบัติ (Risk Management and Compliance) ด้านการปฏิบัติและเทคโนโลยี (Operation and Technology) และด้านเครือข่ายและการสนับสนุน (Network and Support) โดยแผนภาพ Cybersecurity Framework สามารถใช้อธิบายให้ผู้เกี่ยวข้องในองค์กรเข้าใจกิจกรรมทั้งหมดด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ที่ต้องดำเนินการ เข้าใจกิจกรรมในแต่ละกรอบย่อย เห็นภาพความสัมพันธ์ของกิจกรรม

ภายในกรอบย่อยและระหว่างกรอบย่อย ทั้งนี้กิจกรรมในแผนภาพที่นำเสนอไป แต่ละองค์กรสามารถเพิ่มเติมรายละเอียดของกิจกรรมได้ตามบริบท หรือเป้าประสงค์ขององค์กรนั้นๆ ตามความเหมาะสม

ในบทนี้ยังได้วิเคราะห์ปัจจัยที่เป็นตัวแปรสำคัญในการสร้างความมั่นคงปลอดภัยไซเบอร์ในอุตสาหกรรมขนาดใหญ่ โดยปัจจัยดังกล่าวมีทั้งปัจจัยภายนอก และภายใน ถ้าสามารถบริหารจัดการได้ดีจะช่วยให้การสร้างความมั่นคงปลอดภัยไซเบอร์เกิดประสิทธิผลและประสิทธิภาพมากยิ่งขึ้น

สำหรับบทถัดไปจะเป็นการสรุปภาพรวมของงานวิจัยนี้ ตลอดจนข้อเสนอแนะเพื่อประกอบการพิจารณาเพิ่มประสิทธิผลและประสิทธิภาพการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่

บทที่ 5
สรุปและข้อเสนอแนะ

สรุป

การนำพาประเทศไทยก้าวสู่ยุคไทยแลนด์ 4.0 โดยใช้วิทยาศาสตร์และเทคโนโลยีมายกระดับเศรษฐกิจของประเทศให้สามารถแข่งขันได้อย่างยั่งยืน จำเป็นต้องมีการจัดการความมั่นคงปลอดภัยไซเบอร์ควบคู่ไปด้วย ซึ่งไม่เพียงเฉพาะภาครัฐเท่านั้นแต่รวมถึงภาคธุรกิจ ข้อมูลงานวิจัยจากหลายสถาบันแสดงให้เห็นระดับความรุนแรงและผลกระทบที่เกิดจากภัยนี้ซึ่งนับวันจะแพร่กระจายอย่างรวดเร็วไปทั่วโลกตามเทคโนโลยีที่ก้าวหน้ามากขึ้น และรูปแบบการโจมตีก็ไม่เป็นเพียงการบุกรุกระบบเพื่อขโมยข้อมูล แต่มีแนวโน้มเป็นแบบทำให้ระบบงานหยุดชะงัก ดังนั้นหากเกิดภัยนี้ในอุตสาหกรรมขนาดใหญ่ที่มีความสำคัญต่อประเทศ ไม่เพียงสร้างความเสียหายให้หน่วยงานหรือองค์กรเท่านั้น แต่สามารถส่งผลกระทบต่อเศรษฐกิจในระดับประเทศหรือระดับโลกได้ตามสายโซ่ธุรกิจของโลกาภิวัฒน์

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพเพื่อหาแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ที่มีประสิทธิผลและประสิทธิภาพ โดยทำการศึกษาข้อมูลทั้งแบบปฐมภูมิและทุติยภูมิ ได้แก่ เอกสารยุทธศาสตร์ชาติ แผน นโยบาย และการดำเนินการของภาครัฐ งานวิจัยที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยและการป้องกันภัยคุกคามทางไซเบอร์ของประเทศไทยและต่างประเทศ การจัดการขององค์กรตัวอย่างในอุตสาหกรรมขนาดใหญ่ที่เข้าข่าย Critical Infrastructure รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิทั้งที่อยู่ในภาครัฐและภาคธุรกิจ แล้วนำข้อมูลทั้งหมดมาวิเคราะห์ เพื่อหาองค์ประกอบที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์และสังเคราะห์เป็นกรอบดำเนินการ แนวทางการจัดการสำหรับอุตสาหกรรมขนาดใหญ่ รวมทั้งข้อเสนอแนะเพื่อพิจารณาทั้งสำหรับภาครัฐและอุตสาหกรรมขนาดใหญ่ที่อยู่ในภาคธุรกิจ

1. การดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในปัจจุบัน

1.1 ยุทธศาสตร์ชาติ แผน นโยบายและการดำเนินการของภาครัฐ

จากการศึกษาร่างยุทธศาสตร์ชาติ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2560-2564) พบว่าแนวทางการพัฒนาเพื่อสร้างความมั่นคงปลอดภัยไซเบอร์ มีความเชื่อมโยงกันดังแสดงในแผนภาพที่ 2-1 ในบทที่ 2 แต่สิ่งที่ขาดไปคือความเชื่อมโยงในส่วนของเป้าหมาย โดยทั้งยุทธศาสตร์ที่ 1 และยุทธศาสตร์ที่ 2 ของร่างยุทธศาสตร์ชาติ 20 ปี ไม่มีการกำหนดเป้าหมายในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ ในขณะที่แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2560-2564) มีการกำหนดเป้าหมายในระยะ 5 ปี ทำให้การจัดวางแผนของหน่วยงานภาครัฐรองรับแผนงานในระยะ 5 ปีเท่านั้น แต่ไม่ครอบคลุมถึงยุทธศาสตร์ชาติในระยะ 20 ปี ซึ่งจะส่งผลเสียต่อประเทศดังนี้

1.1.1 ขาดการเตรียมการของหน่วยงานภาครัฐที่เกี่ยวข้องซึ่งไม่ได้อยู่ในเป้าหมายระยะ 5 ปีแรก แต่ต้องรองรับในเฟสถัดไป (ปีที่ 6 ถึงปีที่ 20) เช่น การปรับเปลี่ยนโครงสร้างองค์กร กำลังพลและการพัฒนา การจัดหาแหล่งทุน เป็นต้น เพื่อรองรับเศรษฐกิจดิจิทัลอย่างเต็มรูปแบบไม่ทันกาล สูญเสียโอกาสในการแข่งขันของประเทศ และเสี่ยงที่จะได้รับผลกระทบด้านความเชื่อมั่นจากผู้ลงทุนอันเป็นผลจากภัยคุกคามไซเบอร์

1.1.2 ขาดการแสดงสมดุลและบูรณาการในระยะยาวของแผนพัฒนาด้านความมั่นคง และด้านเศรษฐกิจ ทำให้แผนพัฒนา 5 ปี ของหน่วยงานด้านความมั่นคง และหน่วยงานด้านเศรษฐกิจที่รองรับอาจมีความขัดแย้งกัน ทำให้การดำเนินการล่าช้า และเป็นอุปสรรคต่อการเข้าสู่เศรษฐกิจดิจิทัลอย่างมั่นคงและยั่งยืน

1.2 กรอบการทำงาน และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

การจัดการความมั่นคงปลอดภัยไซเบอร์ ต้องการแนวทางการทำงานที่เป็นระบบ เพื่อให้เกิดประสิทธิผล ประสิทธิภาพ สามารถต่อยอดให้เกิดการปรับปรุงอย่างต่อเนื่อง ผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยไซเบอร์บางท่านได้ชี้ให้เห็นว่า ปัจจุบันมีกรอบการทำงานและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่หลากหลาย ซึ่งองค์กรสามารถเลือกนำมาใช้ให้เหมาะกับกิจกรรมขององค์กรได้ แต่สิ่งสำคัญคือ องค์กรต้องมีความเข้าใจความเสี่ยงของภัยคุกคามไซเบอร์ในขอบข่ายงานที่มีการนำเทคโนโลยีด้านไซเบอร์มาใช้ และเข้าใจกรอบการทำงานหรือมาตรฐานที่สามารถนำมาใช้ เพื่อสร้างความมั่นคงปลอดภัยไซเบอร์ โดยไม่จำเป็นต้องเลือกใช้เพียงมาตรฐานเดียว แต่สามารถนำหลายมาตรฐานมาพัฒนาและบูรณาการกันเพื่อให้เหมาะกับขอบข่ายงานขององค์กร

อย่างไรก็ตาม สำหรับประเทศไทย การกำหนดกรอบและแนวปฏิบัติด้านการสร้างความมั่นคงปลอดภัยไซเบอร์โดยภาครัฐเป็นเรื่องจำเป็น เพราะสามารถช่วยให้ภาคธุรกิจมีแนวทางในการสร้างความมั่นคงปลอดภัยไซเบอร์ในช่วงเริ่มต้น และหากมีการปรับปรุงต่อยอดไปสู่มาตรฐานอื่นเพิ่มเติมในภายหลังก็สามารถทำได้ง่ายขึ้น

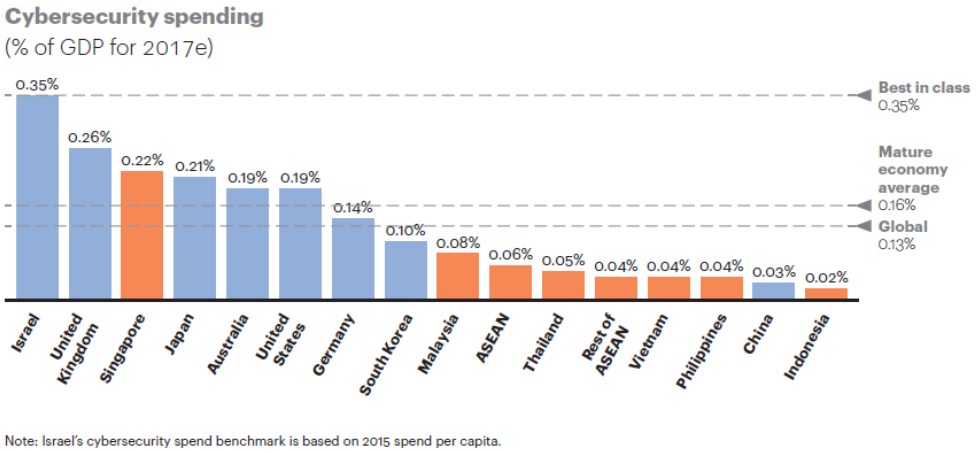
1.3 สถานภาพความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

จากการสำรวจสถานภาพความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ทั้งโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และโดย ITU พบว่า ประเทศไทยได้มีการดำเนินการเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ไปมากแล้ว ทั้งการกำหนดมาตรการควบคุมและแนวทางการป้องกันภัยคุกคามไซเบอร์ การกำหนดมาตรฐาน การจัดตั้งหน่วยงานเฝ้าระวัง และการให้ความรู้ในเรื่องความมั่นคงปลอดภัยไซเบอร์ แต่ยังขาดองค์ประกอบสำคัญที่จะทำให้เกิดการปฏิบัติอย่างแท้จริง (Execution) และมีประสิทธิผล ได้แก่ กฎหมายที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ การรับมือเมื่อเกิดภัยคุกคามและการฟื้นฟูภายหลังเหตุการณ์อย่างมีกลยุทธ์ ดัชนีวัดด้านความมั่นคงปลอดภัยไซเบอร์ สถาบันให้ความรู้และพัฒนาผู้เชี่ยวชาญ และความร่วมมือระหว่างองค์กรทั้งภาครัฐและภาคธุรกิจ

นอกจากนี้ ยังพบว่าค่าใช้จ่ายในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในปี พ.ศ.2560 อยู่ที่ 0.05% ของ GDP ซึ่งต่ำกว่าค่าเฉลี่ยของทั่วโลกเกือบ 3 เท่า ตามแผนภาพที่ 5-1 ทั้งที่ประเทศไทยมีนโยบายเรื่องไทยแลนด์ 4.0 และภัยคุกคามไซเบอร์มีแนวโน้มที่จะเกิดกับประเทศในกลุ่มอาเซียนมากขึ้น[1] ด้วยเหตุนี้ภาครัฐจำเป็นต้องพิจารณาเป้าหมายค่าใช้จ่ายในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศร่วมด้วย หากประเทศไทยต้องการเป็นผู้นำด้านเศรษฐกิจดิจิทัลในระดับต้นๆ ของโลก หรือต้องการใช้เศรษฐกิจดิจิทัลนำพาประเทศก้าวพ้นกับดักประเทศรายได้ปานกลาง ค่าใช้จ่ายด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ก็ควรอยู่ในระดับ Best in Class เพื่อสร้างความมั่นใจกับผู้ที่จะมาลงทุนและทำให้การเปลี่ยนผ่านไปสู่เศรษฐกิจดิจิทัลของประเทศเป็นจริงได้

[1] A.T.Kearney. "Cybersecurity in ASEAN: An Urgent Call to Action". 2018.

แผนภาพที่ 5-1 ค่าใช้จ่ายด้านการสร้างความมั่นคงปลอดภัยไซเบอร์



ที่มา : A.T.Kearney, 2018.

2. แนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่

งานวิจัยนี้ได้ศึกษาหาแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ขององค์กรตัวอย่างที่เป็นอุตสาหกรรมขนาดใหญ่ พบประเด็นสำคัญดังต่อไปนี้

2.1 การสร้างความมั่นคงปลอดภัยไซเบอร์เกิดจากผู้บริหารระดับสูงตระหนักถึงผลกระทบของภัยคุกคามไซเบอร์ที่สามารถทำให้องค์กรหยุดชะงักการผลิตและกระบวนการทางธุรกิจได้

2.2 องค์กรมีกลไกการบริหารจัดการความเสี่ยง และใช้กลไกดังกล่าวประเมินผลกระทบในภาพรวม นำไปสู่การกำหนดนโยบายเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ การปรับโครงสร้างการจัดการภายในองค์กร การกำหนดผู้รับผิดชอบทั้งในรูปแบบหน่วยงานหลักและในรูปแบบคณะกรรมการ เพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

2.3 องค์กรนำผู้เชี่ยวชาญระดับสากลมาตรวจประเมินการจัดการ และการดำเนินการที่เป็นอยู่ ทำให้ทราบจุดเสี่ยงจากภัยคุกคามไซเบอร์และนำไปสู่การจัดทำแผนยกระดับความมั่นคงปลอดภัยไซเบอร์ มีการพิจารณาความพร้อมและความสำคัญเร่งด่วนภายใต้ความเสี่ยงและบริบทขององค์กรควบคู่ไปด้วย

และเมื่อนำแผนงานยกระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรดังกล่าวมาวิเคราะห์ร่วมกับงานวิจัยอื่นและข้อมูลจากการสัมภาษณ์ผู้ทรงคุณวุฒิ สามารถสรุปองค์ประกอบหลักในการสร้างความมั่นคงปลอดภัยไซเบอร์ได้เป็นกรอบดำเนินการภาพใหญ่ (4-Core Framework)

ที่ประกอบด้วย 4 กรอบดำเนินการย่อยดังแสดงในแผนภาพที่ 4-2 ทั้งนี้องค์กรอื่นๆ สามารถใช้กรอบดำเนินการนี้เป็นแนวทางได้ โดยอาจเพิ่มเติมกิจกรรมลงในแต่ละกรอบย่อยได้ตามบริบทของธุรกิจ งานวิจัยนี้ยังพบปัจจัยภายนอกและภายในที่ช่วยเร่งให้เกิดประสิทธิผลและประสิทธิภาพในการจัดการได้ โดยปัจจัยภายนอกดังกล่าว ได้แก่ นโยบายของภาครัฐ กฎหมายด้านไซเบอร์ การสร้างบุคลากร เครือข่ายความร่วมมือ และปัจจัยภายใน ได้แก่ วิสัยทัศน์และภาวะผู้นำ และการเตรียมพร้อมรับมือ

ข้อเสนอแนะ

เพื่อให้การจัดการความมั่นคงปลอดภัยไซเบอร์เกิดประสิทธิผลและประสิทธิภาพในองค์รวม จึงขอเสนอแนะสิ่งที่ภาครัฐและอุตสาหกรรมขนาดใหญ่ในภาคธุรกิจจำเป็นต้องดำเนินการ ดังต่อไปนี้

1. ภาครัฐ

1.1 การกำกับดูแล

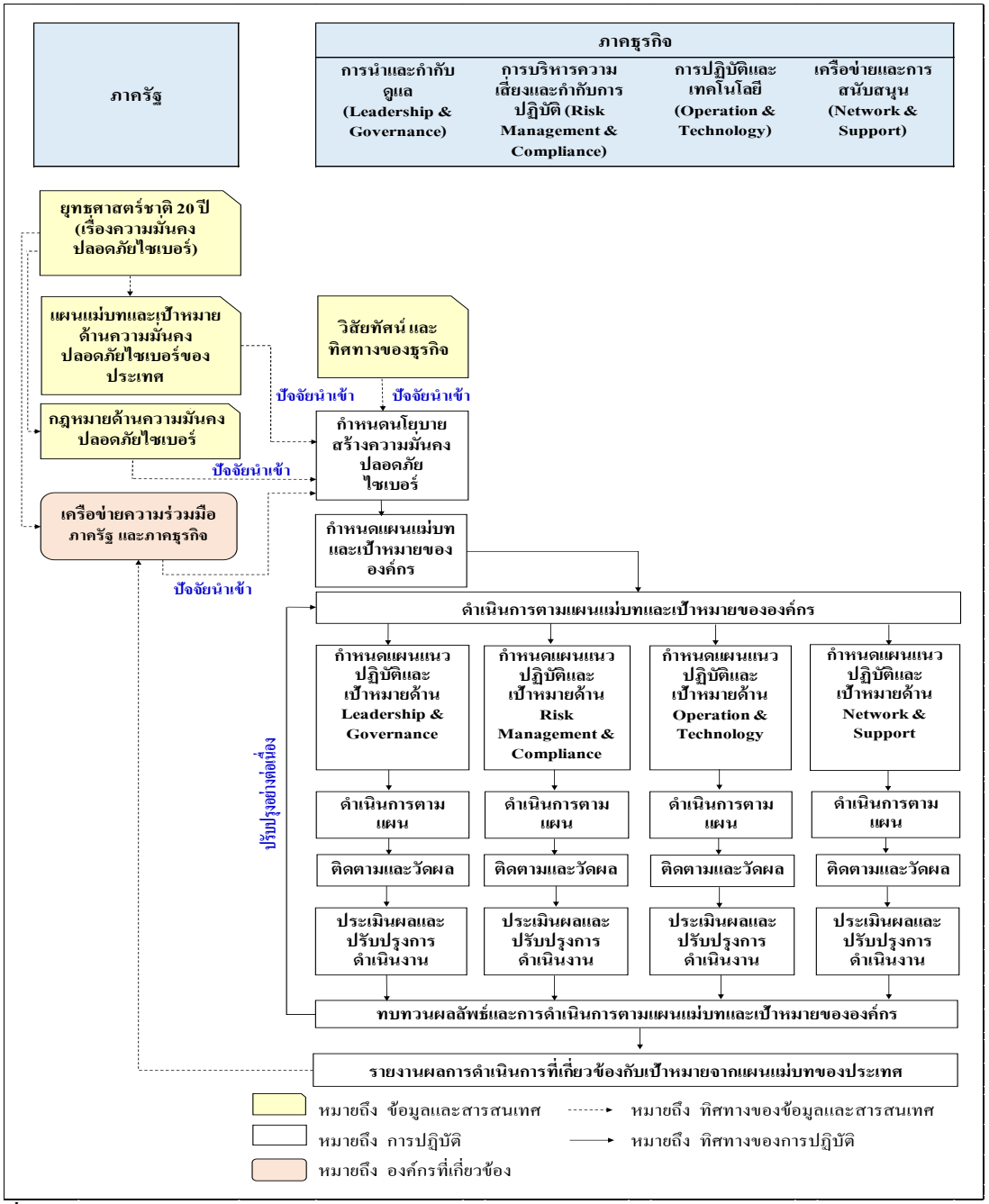
1.1.1 กำหนดเป้าหมายเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ในยุทธศาสตร์ชาติ เพื่อเป็นแนวทางให้กับหน่วยงานต่างๆ ของภาครัฐในการจัดทำแผนงานอย่างมีเป้าหมายและสอดรับกัน โดยกำหนดตำแหน่งของประเทศไทยในเรื่องความมั่นคงปลอดภัยไซเบอร์ในระยะ 20 ปีให้ชัดเจน รวมทั้งเป้าหมายการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งนี้ หากประเทศไทยต้องการให้นักลงทุนเชื่อมั่นในเศรษฐกิจดิจิทัลของประเทศว่ามีการจัดการความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับ Best in Class ก็ต้องมีเป้าหมายการลงทุนค่าใช้จ่ายด้านนี้ให้สูงกว่าหรือเทียบเท่าค่าเฉลี่ยระดับโลกเช่นกัน

1.1.2 จัดทำแผนแม่บทของประเทศในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับเป้าหมายของยุทธศาสตร์ชาติระยะ 20 ปี เพื่อส่งต่อภาพดำเนินการไปสู่การจัดทำแผนงานของหน่วยงานภาครัฐ ภาคธุรกิจ และภาคประชาชนที่เกี่ยวข้องให้สอดประสานและไปในทิศทางเดียวกัน เช่น แผนแม่บทด้านการลงทุนในการก้าวสู่ระดับ Best in Class โดยมีเป้าหมายเพิ่มสัดส่วนการลงทุนต่อ GDP ในระยะ 5, 10, 15 และ 20 ปีข้างหน้าของประเทศให้มีสัดส่วนการลงทุนจากภาครัฐ และจากภาคธุรกิจในแต่ละช่วงเวลาเป็นเท่าไร พร้อมกับกำหนดแผนงานหลักของภาครัฐที่จะผลักดันให้ภาคธุรกิจดำเนินการเรื่องความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น มาตรการส่งเสริมการลงทุนเครื่องจักร เทคโนโลยีที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ มาตรการสิทธิประโยชน์ทางภาษีสำหรับค่าใช้จ่ายด้านการจัดการในเรื่องความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

1.2 ตัวขับเคลื่อนการปฏิบัติ

1.2.1 กำหนดกลไกในการขับเคลื่อนภาคธุรกิจให้เกิดการปฏิบัติตามแผนแม่บทของประเทศ โดยเสนอดังแผนภาพที่ 5-2

แผนภาพที่ 5-2 กลไกขับเคลื่อนภาคธุรกิจให้เกิดการปฏิบัติตามแผนแม่บทของประเทศ



ที่มา : ยุทธนา เจียมตระการ, 2561.

อธิบายแผนภาพที่ 5-2 ได้ดังนี้ เมื่อภาครัฐมีการกำหนดแผนแม่บท และเป้าหมายของการสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศ จะมีการส่งต่อสู่ภาคธุรกิจ โดยผ่านการสื่อสารทางช่องทางเครือข่าย หรือในรูปกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะเป็นปัจจัยนำเข้า (Input) ให้ภาคธุรกิจนำไปพิจารณาร่วมกับ วิสัยทัศน์และทิศทางธุรกิจของตนเอง เพื่อกำหนดเป็นนโยบายสร้างความมั่นคงปลอดภัยไซเบอร์ และถ่ายทอดสู่การปฏิบัติตามกรอบดำเนินการ (4-Core Framework) ได้แก่ การนำและกำกับดูแล (Leadership and Governance) การบริหารความเสี่ยงและกำกับการปฏิบัติ (Risk Management & Compliance) การปฏิบัติ และเทคโนโลยี (Operation & Technology) และเครือข่ายและการสนับสนุน (Network & Support) โดยทั้งภาครัฐและภาคธุรกิจต้องสร้างกลไกการติดตาม วัดผล ประเมินผล และปรับปรุงการดำเนินงาน เพื่อให้บรรลุตามเป้าหมายของแผนแม่บทดังกล่าว

1.2.2 ผลักดันกฎหมาย คือ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ให้ออกมามีผลบังคับใช้โดยเร็ว เพราะการสร้างความมั่นคงปลอดภัยไซเบอร์ไม่ใช่เรื่องของความสมัครใจ แต่จำเป็นต้องเป็นภาคบังคับโดยเฉพาะอย่างยิ่งกับอุตสาหกรรมขนาดใหญ่ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญของประเทศ หรือ Critical Infrastructure ซึ่งถ้าเกิดภัยคุกคามไซเบอร์สามารถสร้างความเสียหายให้กับประเทศอย่างมากมาย การมีกฎหมายจะช่วยทำให้เกิดความชัดเจนทั้งแนวปฏิบัติ ผู้ปฏิบัติ บทบาทความรับผิดชอบทั้งของภาครัฐ และภาคธุรกิจที่เป็น Critical Infrastructure และยังช่วยเร่งการสร้างแผนงาน กิจกรรม และการจัดสรรทรัพยากรสนับสนุน เพื่อรองรับการปฏิบัติ รวมทั้งก่อให้เกิดความร่วมมือขององค์กรที่เกี่ยวข้อง เพื่อให้ปฏิบัติได้สอดคล้องกับข้อกำหนดตามกฎหมายอย่างทันกาล เช่น การสร้างบุคลากร องค์ความรู้ เครือข่าย อันจะช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์

นอกจากนี้ยังสามารถให้หน่วยงานภาครัฐ และภาคธุรกิจที่มีการนำเทคโนโลยีด้านไซเบอร์มาใช้ แต่ไม่ใช่ Critical Infrastructure ใช้เป็นแนวปฏิบัติได้ด้วย เพียงแต่ระดับความเข้มข้นและระยะเวลาการบังคับใช้อาจแตกต่างจากกลุ่มที่เป็น Critical Instructure เพราะต้องไม่ลืมว่า รูที่รั่วแม้มีขนาดเล็กมากแต่ถ้าไม่ป้องกันไว้เลยก็สามารถทำให้เรือล่มได้

1.2.3 สนับสนุนให้เกิดหน่วยงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในส่วนของภาครัฐเอง และของภาคธุรกิจในลักษณะกลุ่มอุตสาหกรรม เพื่อให้เกิดการจัดตั้งเครือข่ายความร่วมมือในการเฝ้าระวังภัย การแบ่งปันข้อมูลทั้งเรื่องภัยคุกคามไซเบอร์ และแนวปฏิบัติที่ดี (Good Practices) การพัฒนาความรู้และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากร การจัดตั้งกลุ่มผู้เชี่ยวชาญร่วม (Pool Specialist) เพื่อให้ความช่วยเหลือหรือเป็นที่ปรึกษาด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ เช่น การประเมินช่องโหว่ การตรวจสอบระบบ

การซ้อมรับมือภัยคุกคาม และการฟื้นฟูระบบภายหลังเหตุการณ์ เป็นต้น ทั้งนี้ การมีหน่วยงานกลางสามารถแบ่งเบาภาระและงบประมาณของภาครัฐในการดูแลเรื่องภัยคุกคามไซเบอร์ ทั้งการจัดการก่อนและหลังเหตุการณ์ และสามารถใช้เป็นช่องทางในการกระจายนโยบาย ข่าวสาร ความรู้จากภาครัฐสู่ภาคธุรกิจ รวมทั้งการรับข้อมูลป้อนกลับจากภาคธุรกิจสู่ภาครัฐด้วย

1.2.4 จัดตั้งศูนย์พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งระดับผู้เชี่ยวชาญในการทำสงครามไซเบอร์ ระดับตรวจสอบหรือประเมินช่องโหว่ของระบบ และระดับประกาศนียบัตรด้านมาตรฐานการจัดการ โดยหน่วยงานกลางของภาครัฐที่ดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้ดำเนินการเอง หรือร่วมกับองค์กรหรือสถาบันภาคเอกชนอื่น หรือสนับสนุนให้มหาวิทยาลัยของภาครัฐหรือเอกชนจัดสอนเป็นหลักสูตรวิชาชีพหนึ่ง และเพื่อให้การพัฒนาบุคลากรด้านไซเบอร์มีการดำเนินการอย่างจริงจัง ภาครัฐควรออกเป็นกฎหมายให้องค์กรขนาดใหญ่ที่มีการนำเทคโนโลยีด้านไซเบอร์มาใช้ในการดำเนินธุรกิจจะต้องมีเจ้าหน้าที่วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ที่มีความรู้ระดับประกาศนียบัตรเป็นอย่างน้อยอยู่ประจำในแต่ละองค์กร เฉกเช่นเดียวกับที่กฎหมายมีการกำหนดให้มีเจ้าหน้าที่วิชาชีพความปลอดภัยประจำโรงงาน

1.2.5 จัดตั้งศูนย์วิจัยและพัฒนาเครื่องมือ และ/หรือโปรแกรมการป้องกันหรือตรวจสอบภัยคุกคามไซเบอร์ เพื่อให้ความช่วยเหลือแก่องค์กรทั้งของภาครัฐ และภาคธุรกิจในราคาประหยัด หรือให้ใช้โดยไม่มีค่าใช้จ่ายแต่ผ่านการเป็นสมาชิก หรือให้การสนับสนุนมหาวิทยาลัยของภาครัฐและเอกชนหรือองค์กรธุรกิจอื่นในการวิจัยและพัฒนาเครื่องมือ และ/หรือโปรแกรมดังกล่าว ตลอดจนเทคโนโลยีด้านไซเบอร์ในรูปแบบการให้ทุนวิจัย หรือสิทธิประโยชน์ทางภาษีหรือการค้า ซึ่งจะช่วยให้มีการพัฒนาเทคโนโลยีด้านการป้องกันภัยไซเบอร์ที่ก้าวหน้า และสามารถเกิดเป็นธุรกิจใหม่ในอนาคตได้

1.2.6 จัดตั้งศูนย์กลางรวบรวมข่าวสาร หรือแหล่งความรู้ด้านภัยคุกคามไซเบอร์ทั้งของประเทศไทยและทั่วโลกที่ภาคธุรกิจหรือประชาชนทั่วไปสามารถเข้าถึงได้ตลอดเวลา รวมทั้งประชาสัมพันธ์ให้ศูนย์ดังกล่าวเป็นที่รู้จักอย่างทั่วถึง โดยปัจจุบันแม้ว่าประเทศไทยจะมีหน่วยงาน Thai-CERT ที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์อยู่แล้ว แต่การรวบรวมข้อมูลยังอยู่ในวงจำกัดและเป็นการรับข้อมูลตามความสมัครใจของผู้ให้ ทำให้ไม่ใช่ข้อมูลภาพรวมของทั้งประเทศ นอกจากนี้หน่วยงานดังกล่าวยังเป็นที่รู้จักในแวดวงจำกัดเฉพาะบางธุรกิจเท่านั้น การที่จะทำให้นโยบายไทยแลนด์ 4.0 เป็นจริงได้ จำเป็นที่หน่วยงานสำคัญของภาครัฐที่เกี่ยวข้องต้องขยายช่องทางในการประชาสัมพันธ์ให้มากขึ้น เข้าถึงได้และอย่างทั่วถึง รวมทั้งต้องสร้างกลไกที่สร้างความเชื่อมั่นแก่ทุกภาคส่วน เพื่อให้เกิดการแบ่งปันข้อมูลสู่ภาครัฐ

2. อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ

2.1 การกำกับดูแล

2.1.1 สร้างความตระหนักและเข้าใจถึงภัยคุกคามไซเบอร์ให้แก่ผู้บริหารระดับสูง ทั้งนี้วิสัยทัศน์และภาวะผู้นำต้องเริ่มจากการที่ผู้บริหารระดับสูงขององค์กรมีความตระหนักและเข้าใจถึงภัยคุกคามไซเบอร์ว่าไม่ได้เป็นความเสี่ยงเฉพาะด้านเทคโนโลยี แต่เป็นความเสี่ยงที่มีต่อธุรกิจขององค์กร ผู้มีหน้าที่ไม่ใช่เฉพาะคนทำงานด้านไอที แต่คือทุกคนที่เกี่ยวข้องกับการใช้เทคโนโลยี นำไปสู่การเกิด Tone at the Top คือ กำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และสื่อสารให้พนักงานองค์กรรับทราบทั้งในรูปเอกสารนโยบาย และการปฏิบัติจริง ทั้งเป็นผู้ลงมือปฏิบัติ และผู้สนับสนุนให้เกิดการปฏิบัติ ได้แก่ การปรับโครงสร้างองค์กร การสนับสนุนกำลังพล การกำหนดบทบาทความรับผิดชอบของผู้เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจน ทั้งการกำกับ การบริหารความเสี่ยง การควบคุมให้เกิดการปฏิบัติ การเป็นผู้ปฏิบัติ การตรวจสอบ การจัดสรรงบประมาณสนับสนุนแผนงาน และการสื่อสารกับพนักงานอย่างสม่ำเสมอ ทั้งนี้ หากผู้บริหารระดับสูงขององค์กรขาดความตระหนักถึงความจำเป็นในการสร้างความมั่นคงปลอดภัยไซเบอร์ การดำเนินการในเรื่องนี้ซึ่งต้องใช้ทั้งงบประมาณ กำลังพล และเวลา อาจไม่ได้รับการสนับสนุนอย่างต่อเนื่องตามความจำเป็น และสุดท้ายก็ไม่สามารถสร้างความมั่นคงปลอดภัยไซเบอร์ได้อย่างแท้จริง

2.1.2 จัดให้มีการบริหารความเสี่ยงด้านภัยคุกคามไซเบอร์ที่มีต่อธุรกิจ เพื่อให้เกิดการจัดลำดับความสำคัญตามผลของความเสี่ยง เนื่องจากการสร้างความมั่นคงปลอดภัยไซเบอร์ เป็นการดำเนินการที่ต้องใช้ทั้งทุน เวลา และกำลังพลจำนวนมาก จึงจำเป็นต้องพิจารณาการลงทุนเปรียบเทียบกับความเสี่ยงที่จะเกิดขึ้นกับธุรกิจ โดยแต่ละธุรกิจมีระดับความเสี่ยงที่ยอมรับได้แตกต่างกันตามต้นทุนทางธุรกิจ เช่น ขอบข่ายของธุรกิจที่มีการนำเทคโนโลยีด้านไซเบอร์มาใช้ ชื่อเสียงขององค์กร ขนาดและมูลค่าทางธุรกิจขององค์กร ผลกระทบต่อผู้มีส่วนได้เสียทางธุรกิจ เป็นต้น การตัดสินใจ (Trade-off) ว่าจะลงทุน หรือกำหนดมาตรการมากน้อยเพียงใด สามารถใช้วิธีการบริหารความเสี่ยง (Risk Management) เข้ามาช่วยในการตัดสินใจได้ อธิบายได้ดังตัวอย่างในตารางที่ 5-1

ตารางที่ 5-1 ตัวอย่างการจัดการความมั่นคงปลอดภัยไซเบอร์ตามลักษณะและความเสี่ยงของธุรกิจ

ลักษณะธุรกิจและบริบท	ระดับความเสี่ยง	มาตรการลดความเสี่ยง
กิจการธนาคาร มีการใช้เทคโนโลยีดิจิทัลในการดำเนินธุรกิจ เน้นการบริการที่ตอบโจทย์ลูกค้าในยุคดิจิทัล	มีความเสี่ยงสูง ในการถูก Hack ข้อมูล ทั้งข้อมูลทางการเงิน และข้อมูลส่วนตัวลูกค้า	1. จัดสรรงบประมาณจำนวนมากเพื่อบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ 2. กำหนดแนวทางการบริหารจัดการชั้นความลับข้อมูล 3. ลงทุนเครื่องมือและอุปกรณ์ตลอดจนผู้เชี่ยวชาญเพื่อบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ 4. กำหนดแนวปฏิบัติให้กับพนักงาน เช่น การกำหนดสิทธิ์ในการเข้าถึงชั้นข้อมูลตามระดับและความสำคัญของงานที่ได้รับมอบหมาย การใช้อุปกรณ์ใน Network 5. ร่วมกลุ่มเครือข่าย เพื่อแลกเปลี่ยนข้อมูล สร้างมาตรฐานการบริหารจัดการ และการพัฒนาบุคลากรร่วมกัน
กิจการผลิตอาหาร มีโรงงานหลายแห่ง ใช้ระบบคอมพิวเตอร์ในการดำเนินธุรกิจ รวมทั้งการควบคุมการผลิต มีเครือข่ายเชื่อมระหว่างโรงงาน และสำนักงาน เน้นการผลิตเพื่อขายเป็นหลัก มีข้อจำกัดในการจัดสรรเงินทุนและกำลังพล สำหรับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์	มีความเสี่ยงกลางถึงสูง ในการถูก Hack ข้อมูล ทั้งข้อมูลบริษัท และข้อมูลส่วนตัวลูกค้า ตลอดจนทำให้การผลิตหยุดชะงัก	1. พิจารณาลงทุนเครื่องมือและอุปกรณ์ ตลอดจนผู้เชี่ยวชาญเพื่อบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ตามความจำเป็น 2. กำหนดแนวปฏิบัติให้กับพนักงานและฝึกอบรม การใช้อุปกรณ์ใน Network

ตารางที่ 5-1 ตัวอย่างการจัดการความมั่นคงปลอดภัยไซเบอร์ตามลักษณะและความเสี่ยงของธุรกิจ (ต่อ)

ลักษณะธุรกิจและบริบท	ระดับความเสี่ยง	มาตรการลดความเสี่ยง
ร้านสะดวกซื้อ แบบดั้งเดิม ใช้ระบบคอมพิวเตอร์ในการบริหารสต็อคสินค้า และทำบัญชี แต่ไม่ได้เชื่อมต่อกับระบบ Internet เน้นขายของได้ มีกำไร	มีความเสี่ยงในการติดไวรัสจากอุปกรณ์ของผู้ใช้งาน	1. Update โปรแกรมป้องกันไวรัสในเครื่องคอมพิวเตอร์อยู่เสมอ

ที่มา : ยุทธนา เจียมตระการ, 2561.

อย่างไรก็ตาม สิ่งสำคัญที่ต้องไม่ลืมคือ แม้จะมีแนวทางในการสร้างความมั่นคงปลอดภัยไซเบอร์ตามการบริหารจัดการความเสี่ยงแล้ว แต่เนื่องจากสภาพแวดล้อมหรือเทคโนโลยีด้านไซเบอร์ที่เกี่ยวข้องกับธุรกิจอาจมีการเปลี่ยนแปลง องค์กรยังจำเป็นต้องมีการทบทวนความเสี่ยงของภัยคุกคามไซเบอร์ใหม่ในทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ หรืออย่างน้อยปีละ 1 ครั้ง เพราะมาตรการที่มีอยู่อาจใช้ไม่ได้แล้ว และเป็นช่องโหว่ให้ภัยคุกคามไซเบอร์เข้ามาโจมตีได้

2.2 ตัวขับเคลื่อนการปฏิบัติ

2.2.1 สร้างความพร้อมให้กับบุคลากรขององค์กร ทั้งความรู้ ความสามารถ ความตระหนักรู้ เนื่องจากคนเป็นส่วนสำคัญที่สุดในการสร้างความมั่นคงปลอดภัยไซเบอร์ เพราะแม้มีกรอบการทำงานและ/หรือมาตรฐานการทำงานที่ดี ใช้เทคโนโลยีการป้องกันที่ทันสมัยและดี แต่หากคนในองค์กรไม่ปฏิบัติแล้ว ก็ไม่สามารถทำให้เกิดความปลอดภัยตามเป้าหมายได้ แต่ขณะเดียวกันหากคนในองค์กรมีความตั้งใจที่จะปฏิบัติแต่ขาดความรู้ความสามารถก็ไม่สามารถป้องกันภัยได้ตามที่หวังเช่นกัน ดังนั้นความพร้อมของบุคลากรจึงต้องประกอบด้วย ความรู้ ความสามารถ ความตระหนักรู้ และจิตใจที่พร้อมปฏิบัติ (Mindset) โดยการเตรียมความพร้อมของคนที่เกี่ยวข้องจะมาก/น้อย ก็ขึ้นกับบทบาทหน้าที่ที่รับผิดชอบ เช่น คนที่มีหน้าที่ป้องกันภัยคุกคามไซเบอร์ นอกจากการมีความตระหนักรู้และมีจิตใจที่พร้อมปฏิบัติแล้ว ก็ต้องมีความรู้ ความสามารถเกี่ยวกับเทคนิคการป้องกันภัยไซเบอร์ด้วย ในขณะที่คนที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไป อาจมีความรู้ด้านการใช้งานคอมพิวเตอร์อย่างปลอดภัย มีความตระหนักรู้ และจิตใจที่พร้อมปฏิบัติก็เพียงพอ ด้วยเหตุนี้ องค์กรจำเป็นต้องมีความชัดเจนเรื่องบทบาทของคนในแต่ละหน่วยงาน เพื่อเตรียมความพร้อมให้คนเหล่านั้นอย่างเหมาะสมไม่มากหรือน้อยไป

2.2.2 สร้างความพร้อมในการปฏิบัติ ได้แก่ การซ้อมรับมือภัยคุกคามไซเบอร์และการบริหารการเปลี่ยนแปลง เนื่องจากภัยคุกคามไซเบอร์สามารถเกิดได้ตลอดเวลา เมื่อมีช่องโหว่ในระบบ การป้องกันเพียงอย่างเดียวจึงไม่เพียงพอ แต่ต้องพร้อมรับมือและจัดการได้อย่างเหมาะสมและเร็วที่สุดเมื่อภัยเข้าสู่ระบบ เพื่อให้มีผลกระทบต่อธุรกิจน้อยที่สุด ดังนั้น หากมีการซ้อมรับมืออย่างสม่ำเสมอแบบเดียวกับการซ้อมดับไฟของโรงงาน ก็จะช่วยให้เกิดการตื่นตัว คุ้นชิน และพร้อมดำเนินการได้ทันทีเมื่อเหตุการณ์จริงเกิดขึ้น

2.2.3 ให้ความร่วมมือกับภาครัฐ และภาคธุรกิจในอุตสาหกรรมเดียวกันเพื่อสร้างเครือข่ายความร่วมมือในการเฝ้าระวัง แบ่งปันข้อมูล และช่วยเหลือกันด้านการสร้างความมั่นคงปลอดภัยไซเบอร์

2.2.4 กำหนดดัชนีวัดความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้ประเมินความสามารถการบริหารจัดการ และใช้เป็นข้อมูลเพื่อการทบทวนการจัดการและการยกระดับจุดเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรให้เกิดการปรับปรุงที่เหมาะสมและต่อเนื่อง โดยดัชนีวัดควรมีทั้งดัชนีวัดผลลัพธ์ และดัชนีวัดกระบวนการควบคู่กันด้วย เช่น ดัชนีวัดจำนวนครั้งที่ถูกโจมตีสำเร็จ และดัชนีวัดการไม่ปฏิบัติของพนักงาน เป็นต้น

2.2.5 จัดให้มีผู้เชี่ยวชาญด้านภัยคุกคามไซเบอร์มาประเมินระบบของธุรกิจที่มีการนำไซเบอร์มาใช้ในงาน เพื่อค้นหาช่องโหว่ที่เสี่ยงต่อการถูกโจมตี อย่างไรก็ตาม เนื่องจากการใช้ผู้เชี่ยวชาญจากภายนอกมีค่าใช้จ่ายที่สูง องค์กรจำเป็นต้องประเมินความคุ้มค่าของการใช้ผู้เชี่ยวชาญ กับผลกระทบความเสี่ยงที่มีต่อธุรกิจประกอบด้วย ซึ่งถ้าไม่คุ้มค่าอาจเปลี่ยนใช้วิธีอื่นที่มีค่าใช้จ่ายน้อยกว่าแต่องค์กรยังสามารถค้นหาช่องโหว่ได้ เช่น การใช้ประโยชน์จากเครือข่าย เป็นต้น

จากข้อเสนอแนะทั้งหมดที่กล่าวมาข้างต้น จะเห็นได้ว่า การจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ให้เกิดประสิทธิผลและประสิทธิภาพ ต้องเกิดจาก 3 ประสานคือ ภาครัฐ อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจและเครือข่ายความร่วมมือ ดังนี้

1. ภาครัฐ เป็นผู้กำหนดนโยบาย ออกกฎหมาย ดำเนินการ และส่งเสริม
2. อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ ร่วมมือ ปฏิบัติ และสนับสนุน
3. เครือข่ายความร่วมมือ ประสานประโยชน์ แบ่งปัน และช่วยเหลือ

ทั้งนี้ เพียงลำพังภาคธุรกิจสามารถทำได้ในระดับหนึ่ง เช่น การมีกรอบการดำเนินการและการกำหนดมาตรฐานการปฏิบัติของกิจกรรมในกรอบดำเนินการ การจัดโครงสร้างองค์กรและกำหนดบทบาทผู้รับผิดชอบให้ชัดเจน การจัดหาเทคโนโลยีที่จำเป็นมาใช้เพื่อการป้องกัน การอบรมและพัฒนาบุคลากรขององค์กรให้มีความรู้ ความเข้าใจ และตระหนักรู้ รวมทั้งการซ้อมรับมือต่างๆ เป็นต้น แต่เรื่องของภัยคุกคามไซเบอร์มีผู้เกี่ยวข้องมากมาย ไม่ใช่เฉพาะคนขององค์กรเท่านั้น

ยกเว้นเป็นองค์กรปิดที่ไม่เกี่ยวข้องกับภายนอกเลย ซึ่งไม่สามารถเป็นไปได้ในยุคเศรษฐกิจดิจิทัลและโลกาภิวัฒน์ ความร่วมมือและความช่วยเหลือจากภาครัฐและองค์กรเครือข่ายจึงเป็นเรื่องจำเป็นและหลีกเลี่ยงไม่ได้ นอกจากนี้ ทั้งภาครัฐและภาคธุรกิจเองก็มีทรัพยากรจำกัด โดยเฉพาะธุรกิจขนาดเล็ก ความร่วมมือและการมองเห็นภาพแผนแม่บทร่วมกันของประเทศจึงสำคัญมาก เพราะนอกจากการเห็นเป้าหมายร่วมกันแล้ว ยังช่วยให้การบริหารทรัพยากรประเทศมีทิศทางชัดเจน เกิดการใช้ทรัพยากรทั้งเงินทุน กำลังพล และเครื่องมือการป้องกันที่ได้ทั้งประสิทธิผลและประสิทธิภาพ สิ่งสำคัญยิ่งคือทำให้เกิดกระบวนการติดตาม และทราบความก้าวหน้าการดำเนินการอันทำให้เกิดความเชื่อมั่นว่า ความมั่นคงปลอดภัยไซเบอร์ของประเทศมีความมั่นคง สามารถทำให้เศรษฐกิจดิจิทัลของประเทศแข่งขันได้อย่างยั่งยืน และนำไปสู่ความมั่นคง มั่งคั่ง และยั่งยืนของประเทศได้ตามเป้าหมายของยุทธศาสตร์ชาตินั่นเอง

บรรณานุกรม

ภาษาไทย

หนังสือ

เอสซีจี. รายงานการพัฒนาอย่างยั่งยืน 2559 เอสซีจี. กรุงเทพฯ : เอสซีจี, 2560.

เอกสารวิจัย

รัฐพล ภักดีภูมิ. “การรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันและการพัฒนามาตรการรักษาความปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2559.

วิโรจน์ ธันวรักษ์กิจ, พลเรือตรี. “แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557.

สุทธิศักดิ์ สลักคำ, พลตรี. “ยุทธศาสตร์การป้องกันไซเบอร์ กระทรวงกลาโหม”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2558.

อรัญ นำผล, พลเรือตรี. “การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557.

สัมภาษณ์

จิรพล ตังทัตสวัสดิ์, Director, PricewaterhouseCoopers Consulting (Thailand) Ltd. สัมภาษณ์. 14 กุมภาพันธ์ 2561.

นนทวัฒน์ พุ่มชูศรี, Country Managing Director, Accenture Thailand. สัมภาษณ์. 21 กุมภาพันธ์ 2561.

ปริญญา หอมเอนก, President and Founder, ACIS Professional Center Co., Ltd. สัมภาษณ์. 12 กุมภาพันธ์ 2561.

อัจฉรินทร์ พัฒนพันธ์ชัย, ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. สัมภาษณ์. 2 มีนาคม 2561.

เอกสารไม่ตีพิมพ์

คณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, สำนักงาน. “แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่สิบสอง พ.ศ. 2560 - 2564”. 2560.

คณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, สำนักงาน. “(ร่าง) ยุทธศาสตร์ชาติ ระยะ 20 ปี (พ.ศ. 2560-2579)”. 2560.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “Cybersecurity survey 2016”. 2559.

รัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security)”. 2559.

สภาความมั่นคงแห่งชาติ, สำนักงาน. “นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2560 – 2564)”. 2560.

ฐานข้อมูลอิเล็กทรอนิกส์

"ก่อนที่ไทยจะเป็นสังคมไร้เงินสด มารู้จัก TB-CERT ดึง 15 ธนาคารเข้าร่วม ตั้งทีมปลอดภัยไซเบอร์". (ออนไลน์). เข้าถึงได้จาก : brandinside.asia/tb-cert-security-cyber-finance/, 2560.

“การโจมตีทางไซเบอร์…ภัยคุกคามเศรษฐกิจใหม่”. (ออนไลน์). เข้าถึงได้จาก : thaitribune.org/contents/detail/312?content_id=29801&rand=1507434306, 2560.

“ความปลอดภัยทางไซเบอร์ (Cyber Security)”. (ออนไลน์). เข้าถึงได้จาก : www.trendmicro.co.th/th/technology-innovation/cyber-security/, 2560.

“ญี่ปุ่นเตรียมตั้งหน่วยงานฝึก white-hat hacker ตั้งเป้าอย่างน้อยปีละ 100 คน”. (ออนไลน์). เข้าถึงได้จาก: www.thaicert.or.th/newsbite/2016-09-06-01.html, 2559.

“บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก” – NIST’s Framework for Improving Critical Infrastructure Cybersecurity “โอกาส ภัยคุกคาม และความเสี่ยงที่ผู้บริหารองค์กรต้องตระหนัก”. (ออนไลน์). เข้าถึงได้จาก : www.acisonline.net/?p=4036&lang=th, 2560.

“สถิติภัยคุกคาม”. (ออนไลน์). เข้าถึงได้จาก : www.thaicert.or.th/statistics/statistics.html, เข้าถึงเมื่อ 12 ต.ค. 2560.

“สปท. เห็นชอบรายงานรักษาความมั่นคงปลอดภัยไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก : www.thaich8.com/news_detail/35152/สปท-เห็นชอบรายงานรักษาความมั่นคงปลอดภัยไซเบอร์, 2560.

"สมาคมธนาคารไทยจัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคารยกระดับมาตรฐานเทียบเท่าสากล". (ออนไลน์). เข้าถึงได้จาก : www.scb.co.th/th/news/2017-10-04/nws-tb-cert, 2560.

ภาษาต่างประเทศ

Non-Published Document

A.T.Kearney. "Cybersecurity in ASEAN: An Urgent Call to Action". 2018.

International Organization for Standardization. “ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements”. 2013.

International Telecommunication Union. “Global Cybersecurity Index (GCI) 2017”. 2017.

National Institute of Standards and Technology. “Framework for Improving Critical Infrastructure Cybersecurity”. 2014.

Electronic Data Base

"About DHS - Mission". (Online). Available: www.dhs.gov/mission, 2016.

"Cyberattack on a German steel-mill". (Online). Available: www.sentryo.net/cyberattack-on-a-german-steel-mill/, 2016.

"Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System". (Online). Available: www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer, 2017.

"Holcim mulls next move after EU court rejects carbon theft lawsuit". (Online). Available: www.reuters.com/article/uk-holcim-carbon/holcim-mulls-next-move-after-eu-court-rejects-carbon-theft-lawsuit-idUKKCN0HS1E720141003, 2010.

“It’s time to think differently about cyber security”. (Online). Available: www.weforum.org/agenda/2017/06/how-to-win-the-cyber-war/, 2017.

“Japan to Create Cyber-Defense Government Agency to Protect SCADA Infrastructures”. (Online). Available: news.softpedia.com/news/japan-to-create-cyber-defense-government-agency-to-protect-scada-infrastructures-504293.shtml, 2016.

"Maersk Says June Cyberattack Will Cost It up to $300 Million". (Online). Available: www.bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter, 2017

“Malaysia to Establish Cybersecurity Academy”. (Online). Available: www.infosecurity-magazine.com/news/malaysia-to-establish/, 2016.

“National cybersecurity strategy aims to make Smart Nation safe: PM Lee”. (Online). Available: www.channelnewsasia.com/news/singapore/national-cybersecurity-strategy-aims-to-make-smart-nation-safe-p-7743784, 2016.

"New cyber attack targets chemical firms: Symantec". (Online). Available: uk.reuters.com/article/us-cyberattack-chemicals/new-cyber-attack-targets-chemical-firms-symantec-idUSTRE79U4K920111031, 2011.

“NIST Impacts: Cybersecurity”. (Online). Available: www.nist.gov/industry-impacts/cybersecurity, 2017.

“Singapore university partners Singtel to launch $30M cybersecurity lab”. (Online). Available: www.zdnet.com/article/singapore-university-partners-singtel-to-launch-30m-cybersecurity-lab/, 2016.

"The inside story of the biggest hack in history". (Online). Available: money.cnn.com/2015/08/05/technology/aramco-hack/index.html, 2015.

“The UK Government confirms the opening of the UK first national anti-cybercrime centre, the National Cyber Security Centre (NCSC)”. (Online). Available: securityaffairs.co/wordpress/51864/cyber-crime/national-cyber-security-centre.html, 2016.

"UK is going to open the National Cyber Security Centre with 700 experts". (Online). Available: securityaffairs.co/wordpress/51864/cyber-crime/national-cyber-security-centre.html, 2016.

"Water treatment plant hacked, chemical mix changed for tap supplies". (Online). Available: www.theregister.co.uk/2016/03/24/water_utility_hacked/. 2016.

ภาคผนวก

ผนวก ก

Framework Core ภายใต้ Framework for Improving Critical Infrastructure Cybersecurity ของ National Institute of Standards and Technology (NIST)

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Function	Category	Subcategory	Informative References
		including privacy and civil liberties obligations, are understood and managed	• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and	• **COBIT 5** APO12.05, APO13.02

Function	Category	Subcategory	Informative References
		prioritized	• **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03

Function	Category	Subcategory	Informative References
			• **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-3, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Data-in-transit is protected	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-

Function	Category	Subcategory	Informative References
			8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,

Function	Category	Subcategory	Informative References
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is	• **ISA 62443-2-1:2009** 4.3.3.3.8

Function	Category	Subcategory	Informative References
		monitored to detect potential cybersecurity events	• **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Unauthorized mobile code is detected	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
	adequate awareness of anomalous events.		• **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-

Function	Category	Subcategory	Informative References
			5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5

Function	Category	Subcategory	Informative References
	restoration of systems or assets affected by cybersecurity events.		• **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information*

Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

ผนวก ข
ประเด็นคำถามสัมภาษณ์

1. ที่ผ่านมา 3-5 ปี ในประเทศไทย ความตื่นตัวในการบริหารจัดการ Cybersecurity ของภาครัฐและภาคเอกชน เป็นอย่างไร

2. แนวโน้มการบริหารจัดการ Cybersecurity ใน 3-5 ปีข้างหน้า เป็นอย่างไรบ้าง

3. ปัจจัยที่มีความสำคัญในการสร้างและบริหารจัดการ Cybersecurity ของประเทศไทย มีอะไรบ้าง

4. มุมมองความเสี่ยงในเรื่องภัยคุกคามไซเบอร์ของประเทศไทยจากนโยบาย Thailand 4.0 เป็นอย่างไร

5. ขอบข่ายความรับผิดชอบของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในด้าน Cybersecurity คืออะไรบ้าง

6. การถ่ายทอดนโยบายด้าน Cybersecurity การบูรณาการงานนโยบายและแผนกับหน่วยงานภาครัฐ ภาคธุรกิจ ภาคประชาชน เป็นอย่างไร

7. โครงสร้างและกลไกการทำงานด้าน Cybersecurity การติดตามแผนและการทบทวนแผน ตลอดจนการรับ Feedback เป็นอย่างไร

8. กระบวนการออกกฎหมาย และการปฏิบัติตามกฎหมายด้าน Cybersecurity เป็นอย่างไร

9. ความพร้อมของภาครัฐ ในการการบริหารจัดการ Cybersecurity เพื่อรองรับภัยคุกคามไซเบอร์ ทั้งในด้านนโยบาย กรอบการทำงาน/มาตรฐาน การบังคับใช้กฎหมายต่างๆ รวมถึงหน่วยงานผู้รับผิดชอบ เป็นอย่างไร

10. ความพร้อมของภาคเอกชน ในการการบริหารจัดการ Cybersecurity เพื่อรองรับภัยคุกคามไซเบอร์ ทั้งมุมของผู้ประกอบการ และผู้ประเมินระบบ Cybersecurity เป็นอย่างไร

11. ความพร้อมของบุคลากรด้าน Cybersecurity ของประเทศไทยเป็นอย่างไร และแผนการพัฒนาความสามารถบุคลากรที่เกี่ยวกับ Cybersecurity ของประเทศไทย เป็นอย่างไร

12. หากเทียบกับกรอบการทำงาน/มาตรฐานสากล นั้น การบริหารจัดการด้าน Cybersecurity ของประเทศไทย เป็นอย่างไร มีด้านใดที่ต้องดำเนินการเพิ่มบ้าง

12.1. การกำหนดนโยบาย มาตรฐาน กฎหมายของภาครัฐ

12.2. การบริหารจัดการขององค์กรภาครัฐและเอกชน

12.3. การประเมินระบบ Cybersecurity ทั้งมาตรฐานการประเมิน และผู้ประเมิน

13. มุมมองในเรื่องความสมดุลของการสร้างการเติบโตทางเศรษฐกิจด้วยเศรษฐกิจดิจิทัล กับเรื่อง Cybersecurity เพื่อให้เกิดความมั่นคง มั่งคั่ง และยั่งยืน เป็นอย่างไรบ้าง

14. มุมมองในเรื่องการกำหนดอุตสาหกรรม โครงสร้างพื้นฐานของไทย ตลอดจนแนวทางการบริหารจัดการด้าน Cybersecurity ที่เกี่ยวข้องเป็นอย่างไรบ้าง

15. เครือข่ายความร่วมมือระหว่างภาครัฐ และภาคเอกชน ในเรื่อง Cybersecurity เป็นอย่างไร

16. สิ่งที่อยากให้ภาครัฐดำเนินการให้ หรือให้การสนับสนุนเกี่ยวกับ Cybersecurity มีอะไรบ้าง

17. เรื่องที่ภาครัฐ และภาคเอกชนที่เป็นอุตสาหกรรมโครงสร้างพื้นฐาน ควรพิจารณาดำเนินการเป็นลำดับต้นๆ (Top 3) ในเรื่อง Cybersecurity คือเรื่องใด

ประวัติย่อผู้วิจัย

ชื่อ

นายยุทธนา เจียมตระการ

วัน เดือน ปีเกิด

27 กรกฎาคม 2506

การศึกษา

Advance Management Program (AMP) Harvard Business School
ประเทศสหรัฐอเมริกา
ปริญญาโท บริหารธุรกิจ มหาวิทยาลัยอัสสัมชัญ
ปริญญาตรี วิทยาศาสตร์ สาขาวิชาเคมี จุฬาลงกรณ์มหาวิทยาลัย

ประวัติการทำงานโดยย่อ

2532 - 2551	ผู้จัดการฝ่ายขายในประเทศ ผู้จัดการฝ่ายสินค้าพิเศษ กลุ่มธุรกิจเอสซีจี เคมิคอลส์
2551 - 2558	กรรมการผู้จัดการ บริษัท เอสซีจี เพอร์ฟอร์มานซ์ เคมิคอลส์ จำกัด
2553 - 2556	กรรมการผู้จัดการ บริษัท เอสซีจี โพลิโอเลฟินส์ จำกัด
2554 - 2558	หัวหน้ากลุ่มธุรกิจ Compound and Formulation SCG Chemicals
2558 - ปัจจุบัน	ผู้ช่วยผู้จัดการใหญ่ – การบริหารกลาง บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน)

ตำแหน่งปัจจุบัน

ผู้ช่วยผู้จัดการใหญ่ - การบริหารกลาง บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน)

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่

ผู้วิจัย นายยุทธนา เจียมตระการ หลักสูตร วปอ. รุ่นที่ 60

ตำแหน่ง ผู้ช่วยผู้จัดการใหญ่ – การบริหารกลาง บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน)

ความเป็นมาและความสำคัญของปัญหา

การพาประเทศไทยก้าวสู่ยุคไทยแลนด์ 4.0 โดยการสร้างความสามารถการแข่งขันด้วยเศรษฐกิจดิจิทัลย่อมหลีกไม่พ้นที่จะเผชิญกับภัยคุกคามไซเบอร์ ซึ่งปัจจุบันเป็นภัยสำคัญลำดับต้นๆ ของโลก เนื่องจากสามารถแพร่กระจายได้รวดเร็วผ่านเครือข่ายอินเตอร์เน็ต และเทคโนโลยีดิจิทัลต่างๆ ที่ก้าวหน้า โดยมีการคาดการณ์ว่าในปี พ.ศ. 2564 ภัยคุกคามดังกล่าวจะสร้างความสูญเสียให้แก่เศรษฐกิจโลกมากกว่า 6 ล้านล้านเหรียญสหรัฐ สำหรับประเทศไทยก็มีการเก็บข้อมูลการถูกโจมตีทางไซเบอร์โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ ThaiCERT ซึ่งเป็นหน่วยงานภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. โดยพบการโจมตีต่อเนื่องทุกปีและมีจำนวนมากขึ้น นอกจากนี้ จากการสำรวจของสหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU พบว่าคะแนน Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ 22 ของโลก ซึ่งต่ำกว่าหลายประเทศในภูมิภาคเอเชียแปซิฟิก และต่ำกว่าประเทศในอาซียนคือ ประเทศสิงคโปร์และมาเลเซีย ด้วยเหตุนี้ การเพิ่มขีดความสามารถในการจัดการความมั่นคงปลอดภัยไซเบอร์ จึงเป็นเรื่องจำเป็นที่ประเทศไทยต้องดำเนินการโดยเร็ว เพื่อสร้างความเชื่อมั่นให้กับประเทศคู่ค้า โดยในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564) ได้กำหนดเป้าหมายให้อันดับของประเทศไทยตามดัชนี ITU ต่ำกว่าอันดับที่ 10 ของโลก ทั้งนี้การที่ประเทศไทยจะบรรลุเป้าหมายดังกล่าวได้ การดำเนินการเฉพาะเพียงภาครัฐไม่เพียงพอที่จะป้องกันภัยดังกล่าวได้ จำเป็นที่จะต้องให้ภาคธุรกิจมีการดำเนินการในเรื่องนี้ร่วมกับภาครัฐด้วย โดยที่ผ่านมางานวิจัยเกือบทั้งหมดจะเน้นศึกษาการสร้างความมั่นคงปลอดภัยในส่วนของภาครัฐเป็นหลัก ดังนั้น การวิจัยการสร้างความมั่นคงปลอดภัยไซเบอร์ในส่วนของภาคธุรกิจ โดยเฉพาะกระบวนการดำเนินการจึงเป็นเรื่องที่ควรให้สำคัญและสามารถ

เป็นประโยชน์ต่อประเทศไทยในการยกระดับสถานะการสร้างความมั่นคงปลอดภัยไซเบอร์ไปสู่เป้าหมายที่วางไว้

วัตถุประสงค์ของการวิจัย

1. ทบทวนสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย
2. เสนอแนะแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่
3. วิเคราะห์และสรุปปัจจัยที่มีผลต่อการจัดการความมั่นคงปลอดภัยไซเบอร์ ให้เกิดประสิทธิผลและประสิทธิภาพ

ขอบเขตของการวิจัย

เป็นการวิจัยผ่านองค์กรตัวอย่างที่เป็นอุตสาหกรรมขนาดใหญ่ในประเทศไทย และเข้าข่ายเป็น Critical Infrastructure ที่ระบุอยู่ในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST)

วิธีดำเนินการวิจัย

เป็นการวิจัยเชิงคุณภาพโดยใช้ทั้งข้อมูลปฐมภูมิและทุติยภูมิ ทั้งนี้ข้อมูลปฐมภูมิมาจากการสำรวจและสัมภาษณ์ผู้บริหารและผู้เกี่ยวข้องขององค์กรตัวอย่าง และการสัมภาษณ์ผู้ทรงคุณวุฒิที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยไซเบอร์ สำหรับข้อมูลทุติยภูมิได้จากการศึกษาเอกสารต่างๆ ได้แก่ ร่างยุทธศาสตร์ชาติ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับล่าสุด กรอบการดำเนินงานและมาตรฐานที่เกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ รายงานการสำรวจและงานวิจัยที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยทั้งของประเทศไทยและต่างประเทศ แล้วนำข้อมูลดังกล่าวมาวิเคราะห์ร่วมกัน สรุปออกมาเป็นแนวทางในการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่พร้อมกับข้อเสนอแนะประกอบการพิจารณาดำเนินการสำหรับทั้งภาครัฐและอุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ

ผลการวิจัย

1. เข้าใจสถานการณ์การดำเนินการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

2. ได้กรอบดำเนินการสร้างความมั่นคงปลอดภัยสำหรับอุตสาหกรรมขนาดใหญ่ที่เรียกว่า Cybersecurity 4-Core Framework ประกอบด้วย 4 ด้าน ได้แก่ การนำและกำกับดูแล (Leadership and Governance) การบริหารความเสี่ยงและกำกับการปฏิบัติ (Risk Management & Compliance) การปฏิบัติและเทคโนโลยี (Operation & Technology) และ เครือข่ายและการสนับสนุน (Network & Support) พร้อมรายละเอียดขององค์ประกอบที่ต้องดำเนินการและผู้เกี่ยวข้องในการดำเนินการในแต่ละด้านดังกล่าว

3. ทราบองค์ประกอบหลัก ตลอดจนปัจจัยสำคัญทั้งภายในและภายนอกในการดำเนินการการสร้างความมั่นคงปลอดภัยไซเบอร์ ให้เกิดประสิทธิผลและประสิทธิภาพ

ข้อเสนอแนะ

1. สิ่งที่ภาครัฐต้องดำเนินการ

1.1 การกำกับดูแล

1.1.1 กำหนดเป้าหมายเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ไว้ในยุทธศาสตร์ชาติ 20 ปี เพื่อให้หน่วยงานต่างๆ ของภาครัฐที่เกี่ยวข้องใช้วางแผนและดำเนินการอย่างเป็นเอกภาพและบูรณาการกัน

1.1.2 จัดทำแผนแม่บทของประเทศให้สอดรับกับยุทธศาสตร์ชาติ 20 ปี เพื่อส่งต่อภาพดำเนินการไปสู่การจัดทำแผนงานของหน่วยงานภาครัฐ ภาคธุรกิจ และภาคประชาชนให้สอดประสานและไปในทิศทางเดียวกัน

1.2 ตัวขับเคลื่อนการปฏิบัติ

1.2.1 กำหนดกลไกการขับเคลื่อนภาคธุรกิจไปสู่การปฏิบัติตามแผนแม่บท

1.2.2 ผลักดันกฎหมาย คือ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ให้ออกมาโดยเร็ว เพื่อให้อุตสาหกรรมขนาดใหญ่ที่เข้าข่ายเป็น Critical Infrastructure รวมทั้งหน่วยงานภาครัฐ และภาคธุรกิจที่เกี่ยวข้อง มีการดำเนินการด้านนี้อย่างจริงจัง ทั้งนี้การมีกฎหมายช่วยทำให้เกิดความชัดเจนทั้งแนวปฏิบัติ ผู้ปฏิบัติ บทบาทความรับผิดชอบ แผนงานและการจัดสรรทรัพยากร รวมทั้งความร่วมมือขององค์กรที่เกี่ยวข้อง เพื่อให้องค์กรปฏิบัติได้สอดคล้องกับข้อกำหนดตามกฎหมายอย่างทันกาล เช่น การสร้างบุคลากร องค์ความรู้ เครือข่าย เป็นต้น

1.2.3 สนับสนุนให้เกิดการจัดตั้งหน่วยงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในส่วนของภาครัฐเอง และของภาคธุรกิจในลักษณะกลุ่มอุตสาหกรรม

1.2.4 จัดตั้งศูนย์พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งระดับผู้เชี่ยวชาญในการทำสงครามไซเบอร์ ระดับตรวจสอบหรือประเมินช่องโหว่ของระบบ และระดับประกาศนียบัตรด้านมาตรฐานการจัดการ อย่างเป็นระบบ

1.2.5 จัดตั้งศูนย์วิจัยและพัฒนาเครื่องมือ และ/หรือโปรแกรมการป้องกันหรือ ตรวจสอบภัยคุกคามไซเบอร์ เพื่อให้ความช่วยเหลือทั้งภาครัฐและภาคธุรกิจ

1.2.6 ดำเนินการให้หน่วยงานของรัฐคือ สพธอ. (ETDA) ซึ่งเป็นศูนย์กลางรวบรวมข่าวสาร หรือแหล่งความรู้ด้านภัยคุกคามไซเบอร์ทั้งของประเทศไทยและทั่วโลกเป็นที่รับรู้อย่างทั่วถึงทั้งภาคธุรกิจและประชาชนทั่วไป

2. สิ่งที่อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจต้องดำเนินการ

2.1 การกำกับดูแล

2.1.1 สร้างความตระหนักและความเข้าใจเรื่องภัยคุกคามไซเบอร์ให้กับผู้บริหารระดับสูง เพื่อนำไปสู่การกำหนดนโยบาย และการให้การสนับสนุน

2.1.2 นำการบริหารจัดการความเสี่ยงในธุรกิจเข้ามาใช้กับการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ เพื่อให้เกิดการจัดการและการลงทุนอย่างเหมาะสมกับขอบข่ายและบริบททางธุรกิจ

2.2 ตัวขับเคลื่อนการปฏิบัติ

2.2.1 สร้างความพร้อมให้กับบุคลากรขององค์กร ทั้งความรู้ ความสามารถ ความตระหนักรู้ เนื่องจากคนเป็นส่วนสำคัญที่สุดในการสร้างความมั่นคงปลอดภัยไซเบอร์ เพราะแม้มีมาตรฐานการทำงานที่ดี ใช้เทคโนโลยีการป้องกันที่ทันสมัยและดี แต่หากคนในองค์กรไม่ปฏิบัติหรือปฏิบัติแต่ขาดความรู้ความสามารถก็ไม่สามารถทำให้เกิดความปลอดภัยตามเป้าหมายได้

2.2.2 สร้างความพร้อมการปฏิบัติทั้งด้านการตรวจจับการจู่โจม การซ้อมรับมือ การฟื้นฟูภายหลังเหตุการณ์ และให้มีการซ้อมปฏิบัติจริงอย่างสม่ำเสมอ

2.2.3 ให้ความร่วมมือกับภาครัฐในการจัดตั้งเครือข่ายความร่วมมือ

2.2.4 กำหนดดัชนีวัดประสิทธิผล และประสิทธิภาพการจัดการความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้ประเมินการจัดการและทำให้เกิดการปรับปรุงอย่างต่อเนื่อง

2.2.5 จัดให้มีผู้เชี่ยวชาญด้านภัยคุกคามไซเบอร์มาประเมินระบบที่มีการนำไซเบอร์มาใช้ ทั้งนี้องค์กรจำเป็นต้องประเมินความคุ้มค่าเนื่องจากการใช้ผู้เชี่ยวชาญมีค่าใช้จ่ายที่สูง

ทั้งนี้การจัดการความมั่นคงปลอดภัยไซเบอร์ให้เกิดประสิทธิผลและประสิทธิภาพสำหรับอุตสาหกรรมขนาดใหญ่ ควรดำเนินการในลักษณะ 3 ประสาน คือ ภาครัฐ อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ และเครือข่ายความร่วมมือ โดย

ภาครัฐ เป็นผู้กำหนดนโยบาย ออกกฎหมาย ดำเนินการ และส่งเสริม

อุตสาหกรรมขนาดใหญ่ในภาคธุรกิจ ร่วมมือ ปฏิบัติ และสนับสนุน

เครือข่ายความร่วมมือ ประสานประโยชน์ แบ่งปัน และช่วยเหลือ