ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

เอกสารวิจัยส่วนบุคคล

โดย

นายพิชัย สุวรรณกิจบริหาร
ผู้อำนวยการสำนักกำกับดูแลกิจการโทรคมนาคม
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

วิทยาลัยการทัพบก
กันยายน 2561

เอกสารวิจัยเรื่อง ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

โดย นายพิชัย สุวรรณกิจบริหาร

อาจารย์ที่ปรึกษา พันเอก พิศณุ คงเมือง

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2561 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ

พลตรี **ผู้บัญชาการวิทยาลัยการทัพบก**
(ธีระพงษ์ เย็นอุทก)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก **ประธานกรรมการ**
(พิศณุ คงเมือง)

พันเอก **ผู้ทรงคุณวุฒิที่ปรึกษา**
(เศรษฐพงค์ มะลิสุวรรณ)

พันเอก **กรรมการ**
(ภรัถ เทียนทองดี)

พันเอกหญิง **กรรมการ**
(ปัทมา สมสนั่น)

บทคัดย่อ

ผู้วิจัย นายพิชัย สุวรรณกิจบริหาร
เรื่อง ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย
วันที่ กันยายน 2561 **จำนวนคำ :** 5,829 **จำนวนหน้า :** 18
คำสำคัญ ไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์ ประเทศไทย
ชั้นความลับ ไม่มีชั้นความลับ

ประเทศไทยเป็นประเทศหนึ่งในประเทศของภูมิภาคอาเซียนที่มีความเจริญก้าวหน้าทางด้านเทคโนโลยีสื่อสารโทรคมนาคม มีการใช้งานด้านการสื่อสารโทรคมนาคม และมีโครงข่ายที่มีการเชื่อมโยงไปยังประเทศต่าง ๆ อย่างแพร่หลายผ่านทางโลกไซเบอร์สเปซ (Cyber Space) ดังนั้น ระบบความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยจึงจำเป็นที่จะต้องมีการป้องกันในระดับสูงต่อความเสี่ยงจากการถูกโจมตีและถูกคุกคามจนส่งผลให้เกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจและสังคมของประเทศ โดยการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทยที่ดีและมีความเหมาะสมจึงถือเป็นปัจจัยหนึ่งที่ทำให้การใช้ระบบไซเบอร์เพื่อการขับเคลื่อนเศรษฐกิจและสังคมมีความเจริญก้าวหน้า อีกทั้ง ได้รับผลกระทบจากภัยคุกคามในระดับความเสี่ยงที่น้อยที่สุด รายงานฉบับนี้จัดทำขึ้นเพื่อศึกษาวิเคราะห์ให้เห็นถึงปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทย โดยผู้วิจัยได้ทำการศึกษาวิเคราะห์ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์จากกรณีศึกษาในประเทศต่าง ๆ และนำมาประยุกต์ใช้ให้เหมาะสมกับสถานการณ์และบริบทของประเทศไทย

ABSTRACT

AUTHOR : Mr. Pichai Suwanakijboriharn

TITLE : Critical Success Factors for Cybersecurity Strategy in Thailand

DATE : September 2018 **WORDCOUNT** : 5,829 **PAGES** : 18

KEY TERMS : Cyber, Cyber Security, Cybersecurity, Thailand

CLASSIFICATION : Unclassified

Thailand is one of the countries in ASEAN that has advanced technology in telecommunications, widespread use of telecommunications and has telecommunications networks widely connected to other countries through cyberspace. Consequently, Thailand's cybersecurity needs the high levels of risk protection from being attacked and threatened leading to damage on the economic and social stability of the country. Thailand's suitable and proper cybersecurity approach is one of the key success factors to make cyber system be a vital tool to drive economics and social development efficiently and affected from cyber threats at minimal risk level. This report is designed to analyze key factors that contribute to the successful implementation of Cybersecurity in Thailand. The researcher examines key success factors in Cybersecurity operatings from case studies in different countries and applies them to the situation and context of Thailand.

กิตติกรรมประกาศ

เอกสารการวิจัยเรื่อง “ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย” ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยความอนุเคราะห์อย่างดียิ่งจากอาจารย์ที่ปรึกษา พันเอก พิศณุ คงเมือง และผู้ทรงคุณวุฒิที่ปรึกษา พันเอก ดร.เศรษฐพงค์ มะลิสุวรรณ ที่กรุณาให้คำแนะนำช่วยเหลือ ตลอดจนให้ความรู้ ข้อคิดเห็น ข้อเสนอแนะต่าง ๆ และประสบการณ์ที่ดีอันเป็นประโยชน์ต่อการวิจัยอย่างต่อเนื่อง

ขอขอบพระคุณ เลขาธิการ กสทช. นายฐากร ตัณฑสิทธิ์ ในฐานะผู้บังคับบัญชาสูงสุดของสำนักงาน กสทช. ที่กรุณาให้ความไว้วางใจและมีส่วนในการตัดสินใจ โดยได้มอบหมายให้ผู้วิจัยได้มีโอกาสเข้ารับการศึกษาในวิทยาลัยการทัพบก สถาบันอันทรงเกียรติ ตลอดจนเพื่อนนักศึกษาที่ได้มีส่วนร่วมในการศึกษา การทำกิจกรรมร่วมกัน และเป็นกำลังใจให้กันตลอดระยะเวลาของการทำวิจัยในห้วงระยะเวลาของการศึกษาหลักสูตรหลักประจำวิทยาลัยการทัพบก ชุดที่ 63

สุดท้ายนี้ ขอกราบขอบพระคุณคณาจารย์ที่ประสิทธิ์ประสาทวิชาความรู้แก่ผู้วิจัยให้สามารถทำการวิจัยได้สำเร็จลุล่วงเป็นไปตามวัตถุประสงค์ของวิทยาลัยการทัพบกทุกประการ หากส่วนดีในการศึกษาครั้งนี้มีคุณประโยชน์อันใด ขอมอบความดีทั้งมวลให้แก่ทุกท่านที่ได้กล่าวถึงข้างต้นด้วยความเคารพ

ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

ประเทศไทยเป็นประเทศหนึ่งในประเทศของภูมิภาคอาเซียนที่มีความเจริญก้าวหน้าทางด้านเทคโนโลยีสื่อสารโทรคมนาคม และมีการใช้งานในการเชื่อมโยงประเทศต่าง ๆ ในโลกด้วยไซเบอร์สเปซ (Cyber Space) ดังนั้น ระบบไซเบอร์ของประเทศไทยจึงมีความเสี่ยงในระดับสูงที่จะถูกโจมตีและถูกคุกคามจนส่งผลให้เกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจ และสังคมของประเทศ การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทยที่ดีและมีความเหมาะสม จึงถือเป็นปัจจัยหนึ่งที่ทำให้การใช้ระบบไซเบอร์เพื่อการขับเคลื่อนเศรษฐกิจและสังคมมีความเจริญก้าวหน้า อีกทั้ง ได้รับผลกระทบจากภัยคุกคามในระดับความเสี่ยงที่น้อยที่สุด โดยการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ที่มีประสิทธิภาพและมีความเหมาะสมจะส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทย

ความเจริญก้าวหน้าทางด้านเทคโนโลยีที่อาจส่งผลต่อความปลอดภัยทางไซเบอร์

การก้าวเข้าสู่การปฏิวัติอุตสาหกรรรมครั้งที่ 4 (Industry 4.0) อันเนื่องมาจากการพลิกผันทางเทคโนโลยี (Technology Disruption) ซึ่งเป็นผลจากความเจริญก้าวหน้าทางด้านเทคโนโลยี (Technological Advancement) ในยุคปัจจุบันนั้น กำลังพัฒนาให้ประเทศไทยได้มีการนำเทคโนโลยีต่าง ๆ มาประยุกต์ใช้เพื่อยกระดับให้ประเทศไทยได้มีการพัฒนาในด้านเศรษฐกิจ สังคม และคุณภาพชีวิตของประชาชน โดยอาจกล่าวได้ว่าในทุกภาคส่วนจะมีการเปลี่ยนผ่านสู่ดิจิทัล (Digital Transformation) โดยมีนักอนาคตศาสตร์กลุ่มหนึ่งที่สามารถพยากรณ์อนาคตได้อย่างแม่นยำมาตลอด และได้พยากรณ์ในสิ่งที่จะเกิดขึ้นภายใน 10 ปีข้างหน้า[1] อาทิ

อุตสาหกรรมยานยนต์ โดยมีการคาดการณ์ว่าในอีก 10 ปีข้างหน้า ยานยนต์จะขับเคลื่อนด้วยตัวเองโดยอาศัยพลังงานไฟฟ้าและระบบที่สร้างขึ้น และรถทุกคันจะมีอุปกรณ์ต่าง ๆ

มากมายรอบคันรถ เพื่อใช้ในการเชื่อมต่อกับอินเทอร์เน็ตให้รถมีระบบบอกตำแหน่งที่แม่นยำตามเวลาจริง (Real Time) เพื่อให้รถทุกคันสามารถสื่อสารกันได้ (M2M : Machine to Machine) ซึ่งจะช่วยลดอุบัติเหตุและการจัดการระบบจราจรในภาพรวม[2]

อุตสาหกรรมอิเล็กทรอนิกส์ เช่น อากาศยานไร้คนขับ (Unmanned Aerial Vehicle : UAV) ประเภทโดรน (Drone) ในอีก 10 ปีข้างหน้า นักอนาคตศาสตร์ได้คาดการณ์ว่าโดรนจะเข้ามามีบทบาทในชีวิตประจำวันของทุกคน และเป็นเครื่องมือที่เข้ามาช่วยดำเนินการในหลายอุตสาหกรรม เช่น เครื่องมือเพื่อการส่งสินค้าในอุตสาหกรรมการขนส่ง เป็นต้น รวมถึงการนำโดรนมาใช้ในการแพร่ภาพและการรักษาความปลอดภัยของเมืองและที่พักอาศัย[3]

อุตสาหกรรมการเงินและธนาคาร ในอีก 10 ปีข้างหน้า นักอนาคตศาสตร์ได้กล่าวว่าการทำธุรกรรมทางการเงินจะมีการเปลี่ยนแปลงไปอย่างสิ้นเชิง โดยการนำเทคโนโลยีที่มีความก้าวหน้ามากกว่าการตรวจสอบของมนุษย์มาใช้ เช่น การแสดงตนด้วยระบบชีวภาพต่าง ๆ อาทิ ลายนิ้วมือ ม่านตา เสียง เป็นต้น

รวมถึงการนำสมาร์ทโฟน (Smartphone) มาใช้เป็นส่วนหนึ่งของชีวิตประจำวันแทนที่บัตรเครดิต บัตรประจำตัวประชาชน หนังสือเดินทาง กุญแจ รหัสเข้าถึง (Password) และคอมพิวเตอร์[4] ในอีก 10 ปีข้างหน้า โดยสมาร์ทโฟนจะเชื่อมต่อกับเครือข่ายอุปกรณ์ตรวจจับ (Sensor) ข้อมูลประเภทต่าง ๆ ซึ่งได้มีการคาดการณ์ว่าจะมีจำนวนอุปกรณ์ตรวจจับ (Sensor) ถึงกว่า 1 แสนล้านชิ้น ที่เชื่อมต่อกันผ่านเครือข่ายอินเตอร์เน็ต จนโลกจะถึงจุดที่เรียกระบบเศรษฐกิจว่า “A Trillion-Sensor Economy”[5]

ข้อมูลจำนวนมหาศาลซึ่งเคลื่อนย้ายอยู่บนโครงข่ายอินเทอร์เน็ตที่เชื่อมต่อกับทุกอุปกรณ์ต่าง ๆ ทั่วโลก หรือที่เรียกว่า Internet of Everythings (IoE) จนทำให้เกิดการวิเคราะห์และประมวลผลจากข้อมูลมหาศาล (Big Data Analytics) ด้วยเหตุนี้ เทคโนโลยีที่เรียกว่าปัญญาประดิษฐ์ (Artificial Intelligence : AI) จึงถูกนำมาใช้เป็นเครื่องมือที่สำคัญในการวิเคราะห์ข้อมูล[6] โดยหน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชน สามารถใช้เทคโนโลยี

AI นี้ เป็นเครื่องมือในการทำงานร่วมกันเพื่อการบริหารจัดการพลังอำนาจแห่งชาติในด้านต่าง ๆ ให้เป็นไปอย่างสอดคล้องกันและมีประสิทธิภาพมากที่สุด

ในรายงานจากมหาวิทยาลัยฮาร์วาร์ด (Harvard University) ซึ่งตีพิมพ์หัวข้อเรื่อง “Artificial Intelligence and National Security” เมื่อเดือนกรกฎาคม 2017 ได้ระบุไว้ในผลการศึกษาอย่างชัดเจนว่า AI กำลังจะส่งผลกระทบและมีบทบาทในทุก ๆ ประเทศใน 3 มิติหลัก คือ ด้านพลังอำนาจทางทหาร (Military Superiority) ด้านพลังอำนาจทางข้อมูลข่าวสาร (Information Superiority) และด้านพลังอำนาจทางเศรษฐกิจ (Economic Superiority)[7] ซึ่งความก้าวล้ำของเทคโนโลยีนี้จะทำให้เกิดความชาญฉลาดและมีการพัฒนาความรู้ใหม่ ๆ ให้กับโลกมากมาย

ในทางกลับกัน ความก้าวล้ำของเทคโนโลยีนั้นอาจส่งผลให้เกิดการโจมตีทางความมั่นคงปลอดภัยทางไซเบอร์ได้ด้วยเช่นกันเนื่องจากเทคโนโลยีทุกอย่างที่กล่าวมาข้างต้นจะทำการเชื่อมต่อข้อมูลทุกประเภทของทุกภาคส่วนผ่านเครือข่ายอินเทอร์เน็ตเข้าด้วยกัน และภายใน 10 ปีข้างหน้า การโจมตีทางไซเบอร์ (Cyber Attack) จะเป็นภัยคุกคามที่น่ากังวลและเป็นภัยคุกคามหลักของทุกประเทศทั่วโลก

กลุ่มโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical Information Infrastructure : CII) ซึ่งหมายถึงหน่วยงานที่มีความสำคัญและมีความจำเป็นต่อโครงสร้างพื้นฐานของประเทศและมีภารกิจอันเกี่ยวข้องกับเศรษฐกิจ ความมั่นคง ชีวิตความเป็นอยู่และทรัพย์สินของประชาชนภายในชาติ ได้แก่ กลุ่มไฟฟ้าและพลังงาน กลุ่มการเงินการธนาคารและการประกันภัย กลุ่มสื่อสารโทรคมนาคมและขนส่ง และกลุ่มความสงบสุขของสังคม จึงอาจตกเป็นเป้าหมายของการถูกโจมตีทางไซเบอร์อันส่งผลกระทบต่อความมั่นคงของประเทศชาติ ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่หน่วยงานด้านความมั่นคงแห่งชาติ (National Security Agencies : NSA) และหน่วยงานที่เกี่ยวข้องต่าง ๆ จะต้องให้ความสำคัญและมีบทบาทในการกำกับดูแลเกี่ยวกับการบริหารจัดการโครงสร้างทั้งหมด รวมถึงต้องพัฒนาขีดความสามารถของบุคลากรภายในหน่วยงานเพื่อให้สามารถตอบโต้กับภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ที่กำลังจะเกิดขึ้นได้ให้เป็นไปอย่างมีประสิทธิภาพด้วยเช่นกัน

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ซึ่งเป็นองค์กรชำนัญพิเศษขององค์การสหประชาชาติ (United Nations : UN) ที่มีหน้าที่ในการพัฒนามาตรฐาน และกฎระเบียบเกี่ยวกับการสื่อสารในกิจการวิทยุและกิจการโทรคมนาคม ได้กำหนดกรอบวาระความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก (Global Cybersecurity Agenda : GCA) ซึ่งมีตัวชี้วัดอันเป็นปัจจัยที่ส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ใช้เป็นเกณฑ์ในการจัดอันดับดัชนีความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) โดยได้จัดแบ่งกลุ่มประเทศสมาชิกในเรื่องนี้ออกเป็น 3 กลุ่มประเภท ได้แก่ กลุ่มประเทศเริ่มต้น (Initial Stage) กลุ่มประเทศระหว่างดำเนินการ (Maturing Stage) และกลุ่มประเทศชั้นนำ (Leading Stage)

ในรายงานการจัดอันดับดัชนีความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ประจำปี พ.ศ. 2560 พบว่า ประเทศไทยได้รับการจัดอันดับให้อยู่ในกลุ่มประเทศระหว่างดำเนินการ (Maturing Stage) โดยมีลำดับการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์อยู่ในอันดับที่ 22 ของโลก และอันดับที่ 7 ของประเทศในเอเชียแปซิฟิก[8] โดยปรากฏว่ามีประเทศที่พัฒนาแล้ว (Developed Country) ในภูมิภาคเอเชียแปซิฟิก อาทิ ประเทศสิงคโปร์ ประเทศออสเตรเลีย ประเทศญี่ปุ่น ประเทศสาธารณรัฐเกาหลี เป็นต้น และประเทศที่กำลังพัฒนา (Developing Country) ในภูมิภาคเอเชียแปซิฟิก ได้แก่ ประเทศมาเลเซีย ถูกจัดให้อยู่ในกลุ่มประเทศชั้นนำ (Leading Stage) และมีอันดับดัชนี GCI สูงกว่าประเทศไทย

จากข้อมูลการจัดอันดับดัชนีความมั่นคงปลอดภัยทางไซเบอร์ระดับโลกดังกล่าว จึงแสดงให้เห็นได้ว่า ประเทศไทยเป็นประเทศที่ได้มีการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์ในทุกภาคส่วนตามกรอบแนวทางของสหภาพโทรคมนาคมระหว่างประเทศแล้วในระดับหนึ่ง แต่ก็ยังคงมีอีกหลายสิ่งที่ต้องพัฒนาตามกรอบแนวทางดังกล่าวให้ดียิ่งขึ้น ทั้งนี้ เพื่อให้ประเทศไทยได้มีการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์เทียบเท่าต่างประเทศ และ

ให้ได้ถูกจัดอยู่อันดับในกลุ่มประเทศชั้นนำ (Leading Stage) ในด้านความมั่นคงปลอดภัยทางไซเบอร์

ตัวชี้วัดและปัจจัยองค์ประกอบต่างๆ ที่ส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทย

ตัวชี้วัดที่ส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์นั้น ประกอบด้วยหลากหลายปัจจัย เช่น ความร่วมมือ (Collaboration) ของทั้งภาครัฐ ภาคเอกชน และประชาชนทั่วประเทศ โดยในประเทศสหราชอาณาจักรได้ถือว่าความร่วมมือกันเป็นปัจจัยหลักที่นำไปสู่ความสำเร็จในการดำเนินงานความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ[9] เนื่องมาจากการดำเนินงานของภาครัฐนั้น สามารถก่อให้เกิดหรือนำทางการดำเนินงานผ่านทางนโยบายและการออกกฎระเบียบข้อบังคับได้ แต่ด้วยเพียงภาครัฐเองจะไม่สามารถดำเนินการสร้างความมั่นคงปลอดภัยทางไซเบอร์ได้ทั้งองค์รวม รัฐบาลจึงจำเป็นต้องได้รับการสนับสนุนจากภาคอุตสาหกรรมและภาคการศึกษาประกอบด้วย รวมถึงการสร้างพันธมิตรให้แข็งแกร่งทั่วโลก เพื่อช่วยกันรับมือกับภัยคุกคามหากเกิดขึ้น และเตรียมพร้อมในการสร้างความเชื่อมั่นในความปลอดภัย รวมถึงทำให้อุปสรรคที่อาจเกิดขึ้นได้จากการเกิดขึ้นของเทคโนโลยีใหม่ ๆ มีความเป็นไปได้น้อยที่สุด

อย่างไรก็ดี ตัวชี้วัดอันเป็นปัจจัยที่ส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ใช้เป็นเกณฑ์ในการจัดอันดับดัชนีความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก (GCI) ตามกรอบแนวทางของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ประกอบด้วยเสาหลัก (Pillar) ใน 5 ด้าน ดังนี้

1. ตัวชี้วัดด้านกฎหมาย (Legal Measure) หมายถึง การประเมินจากบทบาทการมีอยู่ของสถาบันทางกฎหมายและกรอบการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์และอาชญากรรม หรือภัยคุกคามทางไซเบอร์ โดยเพื่อที่ตัวชี้วัดจะวัดผลได้จำเป็นต้องประกอบด้วย 3 ปัจจัย ได้แก่ (1) การกำหนดกฎหมายอาชญากรรมทางไซเบอร์ (Cybercriminal Legislation) (2) การกำหนดกฎระเบียบด้านความมั่นคงปลอดภัยทาง

ไซเบอร์ (Cybersecurity Regulation) และ (3) การฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Training)

2. ตัวชี้วัดด้านเทคนิค (Technical Measure) หมายถึง การวัดดัชนีการมีอยู่ของสถาบันหรือหน่วยงานทางเทคนิค และกรอบการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ โดยเพื่อที่ตัวชี้วัดจะวัดผลได้จำเป็นต้องประกอบด้วย 6 ปัจจัย ได้แก่ (1) ทีมตอบโต้ต่อเหตุการณ์ไซเบอร์แห่งชาติ (National Cyber Incident Response Team : National CIRT) (2) ทีมตอบโต้ต่อเหตุการณ์ไซเบอร์ของภาครัฐ (Governement CIRT) (3) ทีมตอบโต้ต่อเหตุการณ์ไซเบอร์ในแต่ละภาคส่วน (Sectoral CIRT) (4) การกำหนดมาตรฐานองค์กร (Standards for Organization) (5) การกำหนดมาตรฐานและการรับรองสำหรับมืออาชีพ (Standards and Certification for Professional) และ (6) การคุ้มครองเด็กออนไลน์ (Child Online Protection)

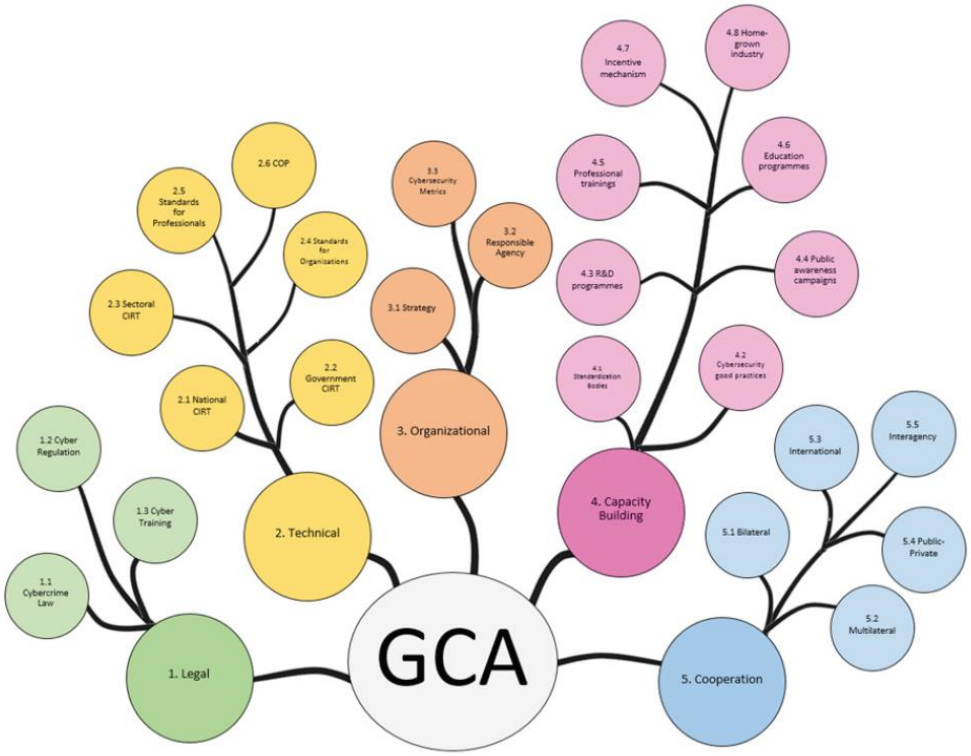
3. ตัวชี้วัดด้านองค์กร (Organizational) หมายถึง การวัดดัชนีจากบทบาทการมีอยู่ของสถาบันหรือหน่วยงานในการประสานงานด้านนโยบาย และกลยุทธ์การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในระดับชาติ โดยเพื่อที่ตัวชี้วัดจะวัดผลได้จำเป็นต้องประกอบด้วย 3 ปัจจัย ได้แก่ (1) กลยุทธ์ (Strategy) (2) หน่วยงานผู้รับผิดชอบ (Responsible Agency) และ (3) ตัวชี้วัดความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Metrics)

4. ตัวชี้วัดด้านการสร้างขีดความสามารถ (Capacity Building) หมายถึง การวัดบทบาทการมีอยู่ของกิจกรรมที่เกี่ยวข้องกับการศึกษาวิจัยและพัฒนา (Research and Development : R&D) หลักสูตรการศึกษาและการฝึกอบรมที่มีการเรียนการสอนและรับรองโดยผู้เชี่ยวชาญ ซึ่งมีหน่วยงานภาครัฐสนับสนุนการสร้างขีดความสามารถ โดยมีปัจจัยประกอบ 8 ปัจจัย ได้แก่ (1) การจัดตั้งหน่วยงานมาตรฐาน (Standardization Bodies) (2) การกำหนดแนวทางปฏิบัติที่ดี (Good Practices) (3) การจัดตั้งโครงการศึกษาวิจัยและพัฒนา (R&D Programmes) (4) การจัดตั้งโครงการรณรงค์สร้างจิตสำนึกในสาธารณะ (Public Awareness Campaigns) (5) การเสริมสร้างหลักสูตรการฝึกอบรมวิชาชีพ (Professional Training Courses) (6) การเสริมสร้างหลักสูตรการศึกษาและแผนการศึกษาแห่งชาติ

(National Education Programmes and Academic Curricula) (7) การสร้างกลไกในการจูงใจ (Incentive Mechanisms) และ (8) การมีซึ่งอุตสาหกรรมความมั่นคงปลอดภัยทางไซเบอร์ในประเทศ (Home-grown Cybersecurity Industry)

5. ตัวชี้วัดด้านความร่วมมือ (Cooperation) หมายถึง การวัดดัชนีจากบทบาทการมีอยู่ของพันธมิตรหรือคู่ค้า กรอบความร่วมมือ และเครือข่ายการแบ่งปันข้อมูล โดยมีประกอบด้วย 5 ปัจจัย ได้แก่ (1) ความร่วมมือระหว่างหน่วยงานภาครัฐ (Intra-state Cooperation) (2) ข้อตกลงพหุภาคี (Multilateral Agreements) (3) ความร่วมมือระหว่างประเทศ (International for Participation) (4) ความร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnerships) และ (5) ความร่วมมือระหว่างหน่วยงาน (Inter-agency Partnerships)

ทั้งนี้ เพื่อให้ประเทศไทยสามารถพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ไปสู่ความสำเร็จจนถูกจัดอันดับให้อยู่ในกลุ่มประเทศชั้นนำ (Leading Stage) จึงเห็นสมควรที่จะนำตัวชี้วัดและปัจจัยที่ส่งผลต่อความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ตามกรอบของสหภาพโทรคมนาคมระหว่างประเทศดังกล่าวแล้วข้างต้นมาปรับใช้และดำเนินการเพื่อให้สอดคล้องกับแนวทางดังกล่าวแล้วให้เป็นไปอย่างครบถ้วน เป็นปัจจุบันและครอบคลุมในทุกประเด็น



ภาพที่ 1 การนำปัจจัยสู่ความสำเร็จของสหภาพโทรคมนาคมระหว่างประเทศไปใช้ในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในกลุ่มประเทศชั้นนำ[10]

ในปัจจัยทางด้านกฎหมาย ปัจจัยประกอบด้านกฎหมายอาชญากรรมทางไซเบอร์นั้น ประเทศจอร์เจียได้กำหนดกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ขึ้นเพื่อให้สอดคล้องกับหลักการและกฎระเบียบของอนุสัญญาบูดาเปสต์ ทั้งในด้านเนื้อหาสาระและขั้นตอนการเข้าถึงระบบสารสนเทศแบบผิดกฎหมาย การแทรกแซงในข้อมูลและระบบ และการใช้อุปกรณ์ที่ไม่ถูกต้องจะถูกพิจารณาโดยประมวลกฎหมายอาญาของประเทศจอร์เจีย นอกจากนี้ ประเทศจอร์เจียยังมีกฎหมายในชั้นพระราชบัญญัติการปกป้องข้อมูลส่วนบุคคลที่ได้รับการรับรองโดยรัฐสภาในปี ค.ศ. 2011 โดยมีจุดมุ่งหมายเพื่อให้แน่ใจว่าได้มีการปกป้องสิทธิและเสรีภาพของมนุษย์ รวมทั้งสิทธิในความเป็นส่วนตัวในการประมวลผลข้อมูลส่วนบุคคลนี้ด้วย

ในปัจจัยทางด้านเทคนิค เรื่องของกรอบการใช้มาตรฐานด้านความมั่นคงปลอดภัยสำหรับองค์กรนั้น ประเทศมาเลเซียได้จัดตั้งหน่วยงานรับรองความปลอดภัยข้อมูล (Information Security Certification Body : ISCB) ภายใต้หน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศมาเลเซีย (Cybersecurity Malaysia) โดยให้เป็นหน่วยงานที่มี

หน้าที่ในการพิจารณาออกใบรับรองด้านการรักษาความปลอดภัยข้อมูล เพื่อให้สอดคล้องกับหลักเกณฑ์และมาตรฐานสากล รวมถึงการประเมินและรับรองมาตรฐาน Malaysian Common Criteria Evaluatioin and Certification (MyCC) ซึ่งรับรองการรักษาความปลอดภัยของผลิตภัณฑ์ ICT ตามมาตรฐานสากล ISO/IEC 15408 นอกจากนี้ยังมีแผน CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) ซึ่งเป็นรูปแบบสำหรับการตรวจสอบหน่วยงานด้านกฎหมาย (รัฐบาลและตัวแทนการค้า) ของระบบการจัดการความปลอดภัยข้อมูล (Information Security Management System : ISMS) ตามมาตรฐานนานาชาติ MS ISO/IEC 27001 : 2007 รวมถึง Malaysia Trustmark for Private Sector (MTPS) ซึ่งเป็นแบบจำลองสำหรับการตรวจสอบหน่วยงานด้านกฎหมาย (ภาคเอกชน) เพื่อให้ได้มาซึ่ง e-Business ที่ดีกับข้อกำหนดของ Asia-Pacific Trustmark Alliance (ATA) และขอบเขตที่ MTPS นำเสนอ[11]

ในปัจจัยทางด้านองค์กร (Organizational) ในส่วนของปัจจัยประกอบด้านกลยุทธ์นั้น สหพันธรัฐรัสเซียได้ดำเนินการตามยุทธศาสตร์ความมั่นคงแห่งชาติ ปี ค.ศ. 2000 แนวความคิดความมั่นคงแห่งชาติของสหพันธรัฐรัสเซีย และแนวคิดเรื่องนโยบายต่างประเทศของสหพันธรัฐรัสเซีย ปี ค.ศ. 2013 โดยสหพันธรัฐรัสเซียได้จัดทำแนวปฏิบัติด้านความมั่นคงสารสนเทศของสหพันธรัฐรัสเซียขึ้นในปี ค.ศ. 2000 และกำหนดให้ทุกหน่วยงานของรัฐบาลดำเนินการตรวจสอบเครือข่ายและระบบของตนเองเป็นประจำทุกปีตามแนวปฏิบัติและพื้นที่ที่ระบุไว้ในกลยุทธ์ต่าง ๆ

ในปัจจัยทางด้านการสร้างขีดความสามารถ (Capacity Building) ปัจจัยประกอบเรื่องกลไกในการจูงใจนั้น สำนักงานความปลอดภัยทางอินเทอร์เน็ตของประเทศสาธารณรัฐเกาหลี (Korea Internet & Security Agency : KISA) มุ่งมั่นที่จะสร้างรากฐานเครือข่ายสำหรับผู้ใช้อินเทอร์เน็ตและบริษัทที่เกี่ยวข้องกับอินเทอร์เน็ตโดยการปรับปรุงขีดความสามารถในการแข่งขันด้านบริการอินเทอร์เน็ตและความน่าเชื่อถือของข้อมูลและความรู้ทางอินเทอร์เน็ต โดย KISA สนับสนุนธุรกิจสตาร์ทอัพหรือธุรกิจที่เกิดขึ้นใหม่ในการทำรูปแบบธุรกิจให้สามารถทำเป็นธุรกิจเชิงพาณิชย์ได้จริง และเพิ่มขีดความสามารถในการแข่งขันในด้านเทคโนโลยีความปลอดภัยผ่านทางโปรแกรมที่มุ่งมั่น

ในการดูแล บ่มเพาะสตาร์ทอัพในอุตสาหกรรม Internet of Things (IoT) ความมั่นคง และ Fintech นอกจากนี้ KISA ยังได้จัดตั้งหน่วยบริการแบบครบวงจรเพื่อสนับสนุนสตาร์ทอัพในการเริ่มต้นสร้างรายได้ โดยไม่เพียงแต่ในตลาดภายในประเทศเท่านั้น แต่ยังมีวัตถุประสงค์เพื่อขยายธุรกิจไปยังตลาดระดับโลกอีกด้วย

ในปัจจัยทางด้านความร่วมมือ (Cooperation) ที่เกี่ยวข้องกับเรื่องของข้อตกลงทวิภาคี ประเทศฟินแลนด์เป็นสมาชิกขององค์กรหลายแห่ง เช่น สภายุโรป (Council of Europe : CoE) องค์การเพื่อความมั่นคงและความร่วมมือในยุโรป (Organization for Security and Co-operation in Europe : OSCE) องค์การสหประชาชาติ (United Nations : UN) เป็นต้น อีกทั้ง ประเทศฟินแลนด์ยังได้เข้าร่วมกับ NATO Partnership for Peace และมีส่วนร่วมกับองค์กร อาทิ การจัดการภาวะวิกฤติ เป็นต้น นอกจากนี้ยังมีการร่วมมือกับบริษัทสัญชาติฟินแลนด์ ได้แก่ บริษัท Codenomicon (ภายหลังถูกซื้อกิจการโดย Synopsys) เพื่อพัฒนาระบบตรวจสอบการบุกรุก (Intrusion Detection System : IDS) ในระดับชาติ เพื่อให้บริการรายงานเหตุการณ์ที่เป็นอัตโนมัติให้กับองค์กรกำกับดูแลของประเทศฟินแลนด์ (Finnish Communications Regulatory Authority : FICORA)

เป้าหมายในการดำเนินยุทธศาสตร์ด้านความมั่นคงปลอดภัยในสหราชอาณาจักร

ประเทศสหราชอาณาจักร รัฐบาลมีเป้าหมายในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อก่อให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ โดยประกอบด้วยจุดประสงค์หลัก 3 ข้อ[12] ดังนี้

1. การปกป้อง (Defend) : สหราชอาณาจักรจะได้รับการป้องกันจากภัยคุกคามทางไซเบอร์ และสามารถรับมือได้อย่างมีประสิทธิภาพต่อเหตุที่อาจเกิดขึ้น โดยมั่นใจได้ว่าโครงข่าย ข้อมูล และระบบทั้งหมด จะได้รับการป้องกันและสามารถกลับมาได้อย่างรวดเร็ว รวมถึงประชาชน ภาคธุรกิจ และภาครัฐทุกส่วนมีความรู้ความสามารถที่จะปกป้องตนเองได้

2. การขัดขวาง (Deter) : สหราชอาณาจักรจะเป็นเป้าหมายที่ยากต่อการจู่โจมทางความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากสหราชอาณาจักรมีการเฝ้าระวัง ทำความเข้าใจ สืบสวน และขัดขวางการจู่โจมของผู้ประสงค์ร้าย รวมถึงเมื่อเกิดเหตุการณ์โจมตีทางความมั่นคงปลอดภัยทางไซเบอร์จะติดตามและดำเนินคดีกับผู้กระทำความผิดหากจำเป็น

3. การพัฒนา (Develop) : ความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักรมีความเป็นนวัตกรรมและได้รับการพัฒนาตลอดเวลาในภายใต้หน่วยงานวิจัยและพัฒนาเชิงวิทยาศาสตร์ชั้นนำระดับโลก รวมถึงทรัพยากรบุคคลที่มีความสามารถและทักษะที่เหมาะสมกับความต้องการของประเทศเพียงพอทั้งในภาครัฐและในภาคเอกชน ด้วยทักษะและความเชี่ยวชาญที่มีความทันสมัยจะทำให้สหราชอาณาจักรสามารถก้าวข้ามภัยคุกคามและความท้าทายในอนาคตได้

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสหรัฐอเมริกา

กรอบการทำงานในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในประเทศสหรัฐอเมริกานั้น สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) มีกรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Strategy) ให้มีประสิทธิภาพ ประกอบด้วยกรอบการดำเนินงานหลัก 5 กรอบงาน[13] ซึ่งจะเป็นตัวกำหนดมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่

1. การกำหนด (Identify) : การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์เป็นขั้นตอนแรกในการศึกษา ทำความเข้าใจวิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถ โดยอยู่ในหมวดหมู่ของการจัดการทรัพย์สิน สภาพแวดล้อมทางธุรกิจ การดำเนินงานภาครัฐ การประเมินความเสี่ยงกลยุทธ์และการจัดการความเสี่ยง

2. การป้องกัน (Protect) : เป็นการปกป้องดูแลทรัพย์สินสารสนเทศโดยการควบคุม และดำเนินงานตามมาตรการป้องกันที่เหมาะสม เพื่อป้องกันหรือจำกัดระดับของภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ โดยอยู่ในหมวดหมู่ของการควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล กระบวนการป้องกันข้อมูล และการดูแลรักษาเทคโนโลยีที่ใช้ในป้องกัน

3. การตรวจจับ (Detect) : ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ โดยการเฝ้าระวัง หรือมีการตรวจสอบติดตามอย่างต่อเนื่องเพื่อการเตือนภัยกับเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันท่วงที และสามารถควบคุมสถานการณ์ได้ โดยอยู่ในหมวดหมู่ของการตรวจจับความผิดปกติและเหตุการณ์ต่าง ๆ การสังเกตการณ์อย่างต่อเนื่อง และกระบวนการตรวจสอบ

4. การรับมือ (Respond) : การรับมือภัยคุกคามทางไซเบอร์กับเหตุการณ์ต่าง ๆ ที่เกิดขึ้น โดยอยู่ในหมวดหมู่ของการวางแผนรับมือ การสื่อการ การวิเคราะห์ การลดความเสี่ยงและปรับปรุงแก้ไข

5. การคืนสภาพ (Recover) : การจัดทำแผนความต่อเนื่องทางธุรกิจเพื่อรองรับการดำเนินงานต่อเนื่อง แผนการกู้คืนข้อมูลและระบบภายหลังเกิดเหตุภัยคุกคามทางไซเบอร์ โดยอยู่ในหมวดหมู่ของการวางแผนฟื้นฟู และการปรับปรุงการสื่อสาร

ปัจจัยสู่ความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในกลุ่มประเทศชั้นนำของสหภาพโทรคมนาคมระหว่างประเทศ เป้าหมายในการดำเนินยุทธศาสตร์ด้านความมั่นคงปลอดภัยในสหราชอาณาจักร และกรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสหรัฐอเมริกาดังที่กล่าวมาข้างต้น ถือเป็นวิธีการและแนวทางปฏิบัติสากลและเป็นส่วนประกอบของปัจจัยสู่ความสำเร็จในการพัฒนายุทธศาสตร์ด้านความมั่นคงของกลุ่มประเทศชั้นนำทางด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยหน่วยงานทั้งภาครัฐ ภาคเอกชน และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในประเทศไทยจึงควรศึกษาทำความเข้าใจและนำมาปรับใช้ปฏิบัติเพื่อให้เป็นปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคง

ปลอดภัยทางไซเบอร์ของประเทศไทย อีกทั้ง ควรคำนึงถึงการปรับใช้ให้เหมาะสมกับบริบทของประเทศไทยด้วย

การพัฒนายุทธศาสตร์ด้านความมั่นคงในปัจจุบันของประเทศไทย

สถานการณ์การพัฒนายุทธศาสตร์ด้านความมั่นคงในปัจจุบันของประเทศไทยนั้น มีการจำกัดความให้ความหมาย “ความมั่นคงปลอดภัยไซเบอร์” จากระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีหน่วยงานที่ได้รับการจัดตั้งให้เป็นผู้ดูแลเป็นกิจลักษณะ รวมถึงมีขั้นตอนสู่ความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถเป็นแนวทางที่เกี่ยวข้องที่จะนำไปสู่ความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของประเทศไทย

ความหมายของคำว่า “ความมั่นคงปลอดภัยไซเบอร์”

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้คำจำกัดความของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” หมายถึง “มาตรการและการดำเนินการเพื่อปกป้อง ป้องกัน การส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ”[14]

หน่วยงานที่ได้รับการจัดตั้งให้เป็นผู้ดูแล “ความมั่นคงปลอดภัยไซเบอร์”

ปัจจุบัน ประเทศไทยมีนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยได้มีการจัดตั้ง “คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC)” ทำหน้าที่ในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามไซเบอร์ โดยหน่วยงานหลักในการขับเคลื่อน ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (Electronic Transactions Development Agency : ETDA) ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กระทรวงกลาโหม และสำนักงานตำรวจแห่งชาติ[15]

กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

จากการศึกษา พบว่ามีกฎหมายที่เกี่ยวข้องโดยตรงกับการดำเนินงานด้านความมั่นคงทางไซเบอร์ 2 ฉบับ ได้แก่ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... และระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560

ตามกรอบนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม จะต้องมีการพัฒนาและส่งเสริมพร้อมบูรณาการงาน 5 เสาสำคัญ โดยเสาที่ 2 คือ “การพัฒนา Soft Infrastructure” โดยการจัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือชุดกฎหมายเศรษฐกิจดิจิทัล โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ซึ่งขณะนี้เป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) ได้เสนอคณะรัฐมนตรีและคณะรัฐมนตรีได้พิจารณาอนุมัติเห็นชอบในหลักการร่างกฎหมายเมื่อวันที่ 16 ธันวาคม 2557 และ วันที่ 6 มกราคม 2558 ตามลำดับ โดยมีร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เป็น 1 ใน 8 ของชุดร่างกฎหมายที่ได้รับการเสนอเข้าคณะรัฐมนตรี ทั้งนี้ จากข้อมูลล่าสุดตามหน้าเว็บไซต์ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้รายงานความคืบหน้าของร่างกฎหมายชุดนี้ว่า ได้ผ่านการพิจารณาของคณะรัฐมนตรีแล้ว กล่าวคือคณะรัฐมนตรีได้รับหลักการแล้ว และขณะนี้อยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา ซึ่งหากมองในภาพรวมแล้วจะเห็นได้ว่าในขณะนี้มีเพียงร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... ที่ยังอาจมีความล้าหลังกว่าชุดกฎหมายเศรษฐกิจดิจิทัลฉบับอื่นๆ[16] สำหรับในส่วนของระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แห่งชาติ พ.ศ. 2560 นั้น ได้มีการลงประกาศในราชกิจจานุเบกษาแล้วเมื่อวันที่ 20 ตุลาคม พ.ศ. 2560

กระบวนการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสม

ในกระบวนการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมจะต้องเริ่มต้นจาก 3 ขั้นตอนเบื้องต้น ได้แก่ (1) การกำหนดและสื่อสารไปถึงคณะผู้บริหารเพื่อให้ทราบถึงความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์ (2) การสร้างนโยบายการจัดการสนับสนุนการจัดการความเสี่ยง และ (3) การระบุตัวอย่างความเสี่ยงที่อาจจะเกิดขึ้น ทั้งนี้ กระบวนการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ จึงควรมีข้อกำหนดให้มีการทบทวนเนื้อหาใหม่ในแต่ละช่วงเวลาด้วย หลังจากนั้นจึงดำเนินการในขั้นตอนสู่ความมั่นคงปลอดภัยทางไซเบอร์ 10 ขั้นตอน[17] ดังต่อไปนี้

1. การบริหารจัดการความเสี่ยง ควรดำเนินการทั่วทั้งองค์กรและได้รับการสนับสนุนอย่างจริงจังจากผู้บริหาร และแสดงถึงความชัดเจนในแนวทางของนโยบายแนวทางการปฏิบัติ และควรมีเป้าหมายเพื่อให้แน่ใจว่าผู้เกี่ยวข้องทุกคนได้ตระหนักถึงและเข้าใจในแนวทาง วิธีการตัดสินใจ และความเสี่ยงต่าง ๆ ที่สามารถเกิดขึ้นได้

2. โครงสร้างความมั่นคงปลอดภัย จะต้องมีแนวทางในการระบุเทคโนโลยีพื้นฐานที่สร้างขึ้นเพื่อให้แน่ใจว่าการจัดการสามารถช่วยปรับปรุงความมั่นคงปลอดภัยของระบบได้ดีขึ้น โดยพัฒนากลยุทธ์เพื่อตัดหรือปิดการใช้งานส่วนงานที่ไม่จำเป็นออกจากระบบ และแก้ไขช่องโหว่ที่พบอย่างรวดเร็ว

3. ความมั่นคงปลอดภัยของเครือข่าย การเชื่อมโยงเครือข่ายขององค์กรกับอินเทอร์เน็ตและเครือข่ายของพันธมิตรอาจเป็นการเปิดโอกาสให้ระบบและเทคโนโลยีขององค์กรถูกโจมตีได้ โดยองค์กรสามารถลดโอกาสที่จะทำให้เกิดการโจมตีได้ โดยการมีแผนและปรับใช้นโยบายในการตอบโต้ทางเทคนิคที่เหมาะสม

4. การจัดการสิทธิพิเศษของผู้ใช้ ถ้าผู้ใช้มีสิทธิพิเศษในการเข้าระบบโดยไม่จำเป็น อาจจะสร้างผลกระทบจากการใช้งานที่ผิดหรืออาจจะมีการละเมิดข้อมูลบัญชีผู้ใช้นั้น ๆ ดังนั้น ผู้ใช้ทุกคนควรจะได้รับสิทธิในการเข้าถึงข้อมูลที่เหมาะสมกับบทบาทในตำแหน่งงาน ควรมีการควบคุมและจัดการการให้สิทธิการเข้าถึงข้อมูลที่เหมาะสม

5. การสร้างความตระหนักและให้ความรู้แก่ผู้ใช้ ผู้ใช้มีบทบาทสำคัญในการสร้างความมั่นคงปลอดภัยให้แก่องค์กร ดังนั้น กฎระเบียบและหลักการปฏิบัติเรื่องความมั่นคงปลอดภัยในการใช้เทคโนโลยีที่มีนั้นจะช่วยให้ผู้ใช้สามารถทำงานด้วยตัวเองได้ถูกต้องและยังช่วยองค์กรในการรักษาความมั่นคงปลอดภัยด้วย ซึ่งสามารถทำให้เกิดขึ้นได้ด้วยการฝึกอบรมการสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยให้แก่บุคลากรทั่วทั้งองค์กร

6. การบริหารจัดการเหตุการณ์ไม่ปกติ ทุกองค์กรจะต้องเผชิญกับเหตุการณ์ไม่ปกติ ดังนั้น การลงทุนในการสร้างนโยบายและกระบวนการบริหารจัดการเหตุการณ์ไม่ปกติอย่างมีประสิทธิภาพจะช่วยสนับสนุนความต่อเนื่องของธุรกิจ และสร้างความเชื่อมั่นต่อผู้เกี่ยวข้องทั้งภายในและภายนอกองค์กร โดยควรจะกำหนดผู้เชี่ยวชาญเข้ามารับผิดชอบในด้านการบริหารจัดการเหตุการณ์ไม่ปกติทั้งจากภายในและภายนอกองค์กร

7. การป้องกันโปรแกรมประเภท Malicious Software หรือที่เรียกว่า มัลแวร์ (Malware) ซึ่งเป็นโปรแกรมหรือชุดคำสั่งคอมพิวเตอร์ที่ถูกสร้างขึ้นเพื่อการประสงค์ร้ายต่อเครื่องคอมพิวเตอร์หรือโครงข่ายระบบคอมพิวเตอร์ เช่น การล้วงข้อมูลความลับหรือข้อมูลสำคัญของผู้ใช้งานคอมพิวเตอร์ เป็นต้น โดยอาจจะลดความเสี่ยงได้โดยการพัฒนาและใช้นโยบายการป้องกันมัลแวร์ที่เหมาะสมและให้ถือเป็นส่วนหนึ่งของแนวทางการป้องกันโดยรวม

8. การเฝ้าติดตาม จะเป็นการสร้างขีดความสามารถในการตรวจสอบการโจมตีที่อาจเกิดขึ้นหรือมีความพยายามที่จะทำให้เกิดขึ้นต่อระบบ โดยการเฝ้าติดตามอย่างต่อเนื่องเป็นสิ่งที่จำเป็นเพื่อจะได้ตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ นอกจากนี้ การเฝ้าติดตามยังทำให้องค์กรมั่นใจได้ว่า ระบบมีการใช้งานอย่างเหมาะสม สอดคล้องกับนโยบายของ

องค์กร ซึ่งการเฝ้าติดตามมักจะเป็นการดำเนินการที่สำคัญที่ต้องทำให้สอดคล้องกับข้อกำหนดทางกฎระเบียบและทางกฎหมาย

9. การควบคุมการใช้งานอุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้ โดยอุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้สามารถเผยแพร่มัลแวร์ได้โดยไม่ได้ตั้งใจ หรืออาจจะนำข้อมูลที่สำคัญออกไปจากระบบได้ ดังนั้น ภายในองค์กรต้องมีความชัดเจน หากจะใช้อุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้ จึงควรมีการควบคุมเรื่องความปลอดภัยในการใช้ที่เหมาะสม

10. การเข้าถึงจากระยะไกล (Remote Access) จากครื่องคอมพิวเตอร์พกพา โทรศัพท์เคลื่อนที่หรืออุปกรณ์สื่อสารประเภทอื่น ๆ ไปยังระบบคอมพิวเตอร์ขององค์กร ซึ่งนับว่ามีประโยชน์ต่อการทำงานของทุกองค์กรในภาวะปัจจุบันเป็นอย่างมาก อย่างไรก็ตาม การป้องกันความเสี่ยงที่เกิดขึ้นกับการทำงานแบบทางไกลนี้จึงมีความจำเป็นต้องได้รับการพิจารณาอย่างเข้มงวด เนื่องจากอาจมีความเสี่ยงสูงจากการถูกจู่โจม (Attack) จากเข้าถึงระบบขององค์กรผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ (Public Internet) ได้ โดยองค์กรสมควรจะต้องมีนโยบายและวิธีการดำเนินการต่าง ๆ ที่สามารถสนับสนุนการทำงานจากระยะไกล หรือการทำงานบนอุปกรณ์เคลื่อนที่ประเภทอื่น ๆ ซึ่งสามารถเข้าถึง (Access) ระบบคอมพิวเตอร์ขององค์กรจากระยะไกล จากบุคลากรขององค์กร รวมทั้งองค์กรอาจสมควรต้องจัดให้มีการฝึกอบรม การสร้างความรู้ความเข้าใจ และการสร้างความตระหนักรู้ ให้แก่บุคลากรขององค์กรเกี่ยวกับความปลอดภัยในการเข้าถึงจากระยะไกล (Remote Access) ไปยังระบบคอมพิวเตอร์ขององค์กรอีกด้วย

สรุป

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ที่มีประสิทธิภาพและมีความเหมาะสม จะต้องคำนึงถึงปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย โดยประเทศไทยควรดำเนินงานตามปัจจัยสู่ความสำเร็จทางด้านความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพโทรคมนาคมระหว่างประเทศทั้ง 5 ปัจจัย ได้แก่ ปัจจัยทางด้านกฎหมาย (Legal) ปัจจัยทางด้านเทคนิค (Technical) ปัจจัยทางด้านองค์กร (Organizational) ปัจจัยทางด้านการสร้างขีดความสามารถ (Capacity Building) และปัจจัยที่สำคัญที่สุดคือ ปัจจัยทางด้านความร่วมมือ (Cooperation) ตามรายละเอียดปัจจัยประกอบที่ได้กล่าวไป เพื่อให้ประเทศไทยได้มีดัชนีทางความมั่นคงปลอดภัยทางไซเบอร์เพิ่มมากขึ้น ได้รับการจัดอันดับให้เข้าสู่กลุ่มประเทศชั้นนำของโลกที่มีความมั่นคงปลอดภัยทางไซเบอร์และประสบความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ นอกจากนี้ยังเห็นว่า ความล่าช้าของกระบวนการออกกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย อาจเป็นอุปสรรคอันส่งผลให้ประเทศไทยยังไม่อาจสามารถบังคับใช้กฎหมายที่เกี่ยวข้องได้ทันต่อสถานการณ์ความเปลี่ยนแปลงของโลกไซเบอร์ในปัจจุบัน ทั้งนี้กรณีดังกล่าวนี้ยังไม่รวมถึงความไม่ทันสมัยและเป็นปัจจุบันของกฎหมายที่คณะรัฐมนตรีได้เคยมีมติรับหลักการไว้ และกำลังอยู่ในระหว่างขั้นตอนกระบวนการตรากฎหมายเพื่อให้มีผลใช้บังคับด้วย

เอกสารอ้างอิง

[1] Malisuwan S. (2017). Digital Transformation [Internet]. [cited 2018 January 1]. Available from : https://www.nbtc.go.th/getattachment/News/Information/28909/Digital-Transformation.pdf.aspx

[2] Todd Jaquith & The Futurism Team, “CAR TECH FORCAST: The Next 10 Years,” The Futurism, 2017 [Internet]. [cited 2018 January 3]. Available from : https://futurism.com/images/car-tech-forecastthe-next-10-years/

[3] Marcelo Ballve, “Here's How Drones Will Become A Reality In Our Daily Lives - With Huge Implications For A Variety Of Industries,” Business Insider, Apr 16, 2014 [Internet]. [cited 2018 January 3]. Available from : http://www.businessinsider.com/drones-will-become-areality-in-our-daily-lives-2014-4

[4] Nigel Danzelman, “Top 10 things your smartphone will replace in the next 10years,” RL360° [Internet]. [cited 2018 January 4]. Available from : http://www.rl360.com/row/aboutus/technologyarticles/top10_smartphone_replace.htm

[5] Peter Diamandis, “The World in 2025: 8 Predictions for the Next 10 Years,” SingularityHub, May 11, 2015 [Internet]. [cited 2018 January 4]. Available from : https://singularityhub.com/2015/05/11/the-world-in-2025-8-predictions-for-the-next-10-years/#sm.0001voptyyd0xd68u602nk78urtal

[6] Malisuwan S. (2017). Big Data Analytics.

[7] HARVARD Kennedy School. Artificial Intelligence and National Security. (July, 2017) [Internet]. [cited 2018 January 4]. Available from : https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

[8] International Telecommunication Union. (2017). Global Cybersecurity Index (GCI) [Internet]. [cited 2018 January 7]. Available from : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[9] Warwick Ashford. (May, 2017). UK government sees collaboration as key to cyber security success [Internet]. [cited 2018 January 7]. Available from : http://www.computerweekly.com/news/450418890/UK-government-sees-collaboration-as-key-to-cyber-security-success

[10] International Telecommunication Union. (2017). Global Cybersecurity Index (GCI) 2017 [Internet]. [cited 2018 January 7]. Available from : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[11] Information Security Certification Body (ISCB) [Internet]. [cited 2018 January 7]. Available from : http://www.cybersecurity.my/en/services/security_assurance/mycb/main/detail/1765/

[12] National Cybersecurity Strategy 2016 to 2021, Cabinet office, National Security and Intelligence, Nov 1, 2016.

[13] National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity.

[14] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560

[15] การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม, 2558

[16] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 10 มกราคม 2561]. เข้าถึงได้จาก : https://ictlawcenter.etda.or.th/de_laws

[17] Malisuwan S. (2017). National Cybersecurity Strategy

ประวัติย่อผู้วิจัย

ยศ ชื่อ นามสกุล นาย พิชัย สุวรรณกิจบริหาร

วัน เดือน ปี เกิด 7 มิถุนายน 2506

ประวัติสำเร็จการศึกษา

พ.ศ. 2527	ประกาศนียบัตรวิชาชีพชั้นสูง (อิเลคทรอนิคส์) วิทยาลัยเอเซียอาคเนย์
พ.ศ. 2529	ครุศาสตร์อุตสาหกรรมบัณฑิต (วิศวกรรมโทรคมนาคม) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง
พ.ศ. 2542	รัฐประศาสนศาสตรมหาบัณฑิต (นโยบายสาธารณะและการบริหารงานบุคคล) (หลักสูตรสำหรับนักบริหาร รุ่นที่ 4) มหาวิทยาลัยศรีปทุม

ประวัติการทำงาน

พ.ศ. 2529	วิศวกรไฟฟ้าสื่อสาร 3	กรมไปรษณีย์โทรเลข
พ.ศ. 2547	วิศวกรไฟฟ้าสื่อสาร 8 วช.	กรมไปรษณีย์โทรเลข
พ.ศ. 2548	ผู้บริหาร ระดับต้น	สำนักงาน กทช.
พ.ศ. 2553	ผู้บริหาร ระดับต้น	สำนักงาน กสทช.
พ.ศ. 2556	ผู้บริหาร ระดับกลาง	สำนักงาน กสทช.

ใบอนุญาตประกอบวิชาชีพ

ใบอนุญาตประกอบวิชาชีพวิศวกรรมควบคุม ประเภทสามัญวิศวกร
สาขาวิศวกรรมไฟฟ้าสื่อสาร แขนงไฟฟ้าสื่อสาร เลขทะเบียน สฟส.302

ตำแหน่งปัจจุบัน

พ.ศ. 2556 - ปัจจุบัน ผู้อำนวยการสำนักกำกับดูแลกิจการโทรคมนาคม
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคมแห่งชาติ