กลยุทธ์การคืนสภาพได้ทางไซเบอร์: แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล

CYBER RESILIENCE STRATEGY: A KEY GUIDE TO ENTERPRISE OPERATIONS IN DIGITAL AGE

จิตสุภา ฤทธิผลิน

Jitsupa Rittipalin

สำนักเทคโนโลยีสารสนเทศ

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

กรุงเทพฯ 10400

Information Technology Bureau, Office of the National Broadcasting and Telecommunications Commission, Bangkok 10400 Thailand

Corresponding E-mail : jitsupa.r@nbtc.go.th

Received Date August 9, 2021
Revised Date September 9, 2021
Accepted Date October 12, 2021

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่กระทบต่อองค์กร และศึกษากรอบแนวทางและกลยุทธ์การคืนสภาพได้ทางไซเบอร์ โดยเป็นการศึกษาเชิงคุณภาพด้วยการทบทวนวรรณกรรมและงานวิจัยเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ และการคืนสภาพได้ทางไซเบอร์ ผลการศึกษาพบว่า ปัจจุบันองค์กรต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่หลากหลาย จำเป็นอย่างยิ่งที่องค์กรต้องมีความสามารถในการคืนสภาพได้ทางไซเบอร์ กล่าวคือ สามารถคาดการณ์ ตรวจจับ ต้านทาน กู้คืน และพัฒนาเมื่อเผชิญกับเหตุการณ์ภัยคุกคามทางไซเบอร์ได้ ข้อเสนอแนะสำหรับองค์กรของไทยในการรับมือกับภัยคุกคามทางไซเบอร์ ได้แก่ กำหนดกลยุทธ์การลงทุนด้านการคืนสภาพได้ทางไซเบอร์ที่เป็นพลวัต เน้นการรับมือการโจมตีทางไซเบอร์ในระดับนโยบายที่ต้องมีการสร้างความตระหนักรู้ในบุคลากรทุกระดับ และการพัฒนาบุคลากรในการรองรับการโจมตีทางไซเบอร์ด้วยทักษะการตอบโต้แบบ Red Team และ Blue Team ด้วยการจำลองและฝึกทักษะการโจมตีและป้องกันเป็นระยะ ๆ

คำสำคัญ: ภัยคุกคามทางไซเบอร์ การโจมตีทางไซเบอร์ การคืนสภาพได้ทางไซเบอร์

Abstract

The objectives of this academic article aimed to study and analyze cyber threats affecting the organization and study the framework and strategies for cyber resilience. This qualitative and applied research was methodology. This study is documentary research that reviews the literature and research on the subject of cyber security, cyber threats, and cyber resilience. This paper was found that organizations now have faced a variety of cyber threats and need to adopt cyber resilience, i.e. be able to anticipant, detect, withstand, recover, and evolve in the face of cyber incidents. The suggestions for Thai corporates to cope with cyber threats are to establish a dynamic strategy for investing in cyber resilience, focus on responding to cyber-attacks at the policy level which, cyber security must be aware of at all levels of personnel, and develop the cyber-attack response personnel with Red team and Blue team countermeasure skill by stimulating and practicing with an attack scenario periodically.

Keywords: Cyber Threat, Cyber Attack, Cyber Resilience

1. บทนำ

ปัจจุบันระบบเศรษฐกิจโลกเข้าสู่ภาวะเศรษฐกิจดิจิทัล นับเป็นการปฏิวัติทางดิจิทัล (Digital revolution) ส่งผลให้ทุก ๆ ระบบในโลกมีการพึ่งพิงเทคโนโลยีดิจิทัลเป็นจำนวนมากและขยายวงกว้างขึ้น ซึ่งจัดเป็นการพัฒนาอุตสาหกรรมในยุคที่ 4 โดยองค์กรส่วนใหญ่ในโลกต่างเข้าสู่การเปลี่ยนผ่านให้อยู่ในรูปขององค์กรดิจิทัล (Digital transformation) ซึ่งในปี พ.ศ. 2564 มีมูลค่าการลงทุนองค์กรดิจิทัลสูงถึง 1.54 ล้านล้านดอลลาร์สหรัฐ คิดเป็นร้อยละ 16.6 ของการลงทุนในปีก่อนหน้า (Dickson & Goodwin, 2020) ขณะที่มีการเติบโตทางเทคโนโลยีดิจิทัลอย่างต่อเนื่อง วิวัฒนาการของภัยคุกคามทางดิจิทัลก็เพิ่มขึ้นเป็นเงาตามตัว ซึ่งการขยายตัวของการโจมตีทางไซเบอร์ (Cyber attack) ทั้งในด้านความถี่และความรุนแรงมีอัตราเพิ่มสูงมากขึ้นในระยะเวลา 2 ปีที่ผ่านมา นอกจากนี้ ภาวะวิกฤตการระบาดของโรค COVID-19 ตั้งแต่ปี พ.ศ. 2563 เป็นต้นมา ทำให้ประชากรต้องมีการควบคุมการแพร่ระบาดด้วยการรักษาระยะห่างทางสังคม ส่งผลให้มีการลดจำนวนบุคลากรที่ปฏิบัติงานในองค์กรลง และส่งเสริมให้มีการทำงานจากที่บ้าน (Work from Home) ที่มีการเข้าใช้ระบบเครือข่ายขององค์กรผ่านโปรแกรมเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) เพิ่มมากขึ้น อาชญากรไซเบอร์จึงหันมาใช้วิกฤตนี้ในการโจมตีองค์กรต่าง ๆ ทางไซเบอร์ กรณีตัวอย่างในเดือนพฤษภาคม พ.ศ. 2564 ของบริษัท Colonial Pipeline ซึ่งประกอบกิจการท่อส่งน้ำมันในสหรัฐอเมริกา ได้ถูกอาชญากรไซเบอร์กลุ่ม Darkside ขโมยรหัสผ่าน (Password) เข้าระบบคอมพิวเตอร์ของบริษัท โดยมี

สาเหตุมาจากกลุ่มอาชญากรไซเบอร์พบข้อมูลของเจ้าหน้าที่ในองค์กรที่ใช้งานระบบการควบคุมทางไกล (Remote) ซึ่งมีการใช้งานด้วยซอฟต์แวร์ TeamViewer และ Microsoft Remote Desktop ในระหว่างการปฏิบัติงานช่วงการระบาดของโรค COVID-19 รั่วไหล หลังจากนั้นจึงทำการโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ส่งผลให้ระบบการขนส่งน้ำมันไปยังมลรัฐในสหรัฐอเมริกาจำนวน 18 รัฐหยุดชะงักและมีการโจรกรรมข้อมูลของบริษัทออกมามากกว่า 100 กิกะบิต (Gigabit) พร้อมทั้งเรียกค่าไถ่ (Trend Micro Research, 2021)

การโจมตีทางไซเบอร์ในวันนี้เป็นเรื่องที่ใกล้ตัวมากและยังสามารถสร้างความเสียหายที่ไม่ได้จำกัดเพียงแค่ตัวบุคคล แต่ยังกระทบต่อองค์กรทั้งในด้านของชื่อเสียงและการดำเนินงาน ในปี พ.ศ. 2563 องค์กรส่วนใหญ่ที่เคยถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ พบว่าถูกโจมตีเพิ่มสูงขึ้นจากปีก่อนหน้าร้อยละ 62 และมีการจ่ายเงินค่าไถ่เพิ่มขึ้น ร้อยละ 336 รวมมูลค่าความเสียหาย 370 ล้านดอลลาร์สหรัฐ โดยเป็นการจ่ายค่าไถ่ในรูปของบิตคอยน์ (Bitcoin) ซึ่งทำให้ยากในการติดตามแกะรอย (สำนักข่าวอินโฟเควสท์, 2564) ทั้งนี้ การโจมตีทางไซเบอร์นับวันจะมีการพัฒนารูปแบบในการโจมตีใหม่ ๆ ที่ซอฟต์แวร์ด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่อาจไม่สามารถป้องกันได้ หรือที่เรียกว่า Zero day[1]

การเตรียมความพร้อมขององค์กรในการรับมือกับภัยคุกคามทางไซเบอร์นั้นเป็นสิ่งที่องค์กรสามารถดำเนินการได้ ซึ่งควรเริ่มตั้งแต่ระดับนโยบายแล้วถ่ายทอดลงสู่ระดับปฏิบัติการ การที่องค์กรมีทักษะที่ดีในการรับมือ แก้ไข และเยียวยาจากเหตุการณ์ทางไซเบอร์ หรือที่เรียกว่าการคืนสภาพได้ทางไซเบอร์ (Cyber resilience) เป็นสภาวะที่องค์กรมีความทนทานซึ่งประกอบด้วยความคล่องตัว (Agility) และความทนทาน (Robustness) ต่อภัยคุกคามทางไซเบอร์ จะช่วยให้องค์กรสามารถป้องกัน ตรวจจับ และตอบสนองต่อการถูกโจมตีทางไซเบอร์ได้อย่างรวดเร็ว จะพบว่าหลายองค์กรเริ่มมีความตระหนักเกี่ยวกับความปลอดภัยของเทคโนโลยีสารสนเทศ และเริ่มมีการนำมาตรฐานความปลอดภัยระดับสากลมาใช้เป็นกรอบแนวทางกันมากขึ้น ผู้เขียนจึงมีความสนใจที่จะศึกษานโยบายและกลยุทธ์การคืนสภาพได้ทางไซเบอร์ที่จะสามารถช่วยให้องค์กรสามารถบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

โดยมีวัตถุประสงค์ดังต่อไปนี้

1) เพื่อศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อองค์กร

2) เพื่อศึกษากรอบแนวทางและกลยุทธ์การคืนสภาพได้ทางไซเบอร์สำหรับองค์กร

[1] Zero-day หมายถึง ช่องโหว่ของซอฟต์แวร์ที่เพิ่งค้นพบ เนื่องจากนักพัฒนาซอฟต์แวร์เพิ่งทราบถึงข้อบกพร่องนั่นหมายถึงแพตช์ (Patch) อย่างเป็นทางการหรือการอัปเดตเพื่อแก้ไขปัญหายังไม่ได้รับการเผยแพร่

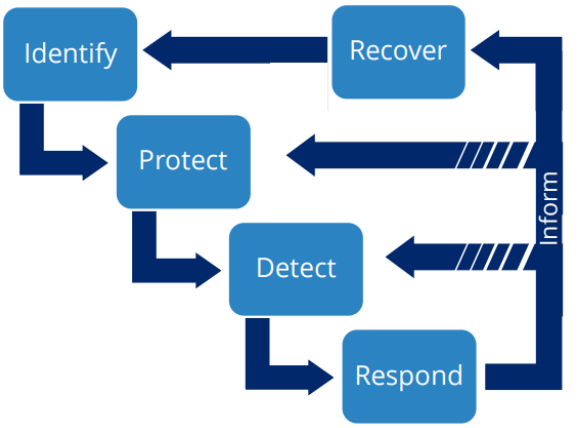
2. วิธีการศึกษา

บทความนี้เป็นการศึกษาเอกสาร (Documentary research) โดยการทบทวนวรรณกรรมและการวิเคราะห์ภัยคุกคามทางไซเบอร์ การศึกษางานวิจัยที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางไซเบอร์และศึกษาการคืนสภาพได้ทางไซเบอร์ โดยทำการวิเคราะห์รูปแบบการโจมตีทางไซเบอร์และการคืนสภาพได้ทางไซเบอร์ เพื่อกำหนดกลยุทธ์การคืนสภาพได้ทางไซเบอร์ ให้องค์กรสามารถดำเนินกิจการได้อย่างต่อเนื่องและเพิ่มศักยภาพในการแข่งขันภายใต้สภาวะเศรษฐกิจดิจิทัล อย่างไรก็ตาม บทความนี้เป็นข้อค้นพบ ข้อวิเคราะห์และการประเมินผลของผู้เขียนเป็นการวิจัยระยะสั้นในช่วงเดือนมีนาคม พ.ศ. 2564 ถึงเดือนสิงหาคม พ.ศ. 2564 จึงอาจมีประเด็นหรือปัจจัยต่าง ๆ ที่ยังไม่ได้กล่าวถึงในที่นี้ ทั้งนี้ ผู้เขียนหวังเป็นอย่างยิ่งว่าผลการศึกษาจะสามารถนำไปใช้เป็นข้อมูลเพื่อประกอบการกำหนดยุทธศาสตร์ขององค์กรให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

3. การทบทวนวรรณกรรม

3.1 กรอบแนวคิดของการคืนสภาพได้ทางไซเบอร์

การคืนสภาพได้ทางไซเบอร์ เป็นแนวคิดที่ถูกคิดค้นขึ้นในปี พ.ศ. 2554 โดย Deborah J. Bodeau และ Richard Graubart และมีการจัดทำกรอบแนวทางการคืนสภาพได้ทางไซเบอร์ (Cyber resiliency framework) ซึ่งมุ่งเน้นไปที่ “ความคงทน” หรือ “ความยืดหยุ่น” ต่อการถูกโจมตี กล่าวคือ เมื่อถูกโจมตีระบบจะต้องยังสามารถให้บริการต่อไปได้ และต้องสามารถตรวจจับการโจมตีได้อย่างรวดเร็ว สามารถหยุดการโจมตีไม่ให้แพร่กระจายสู่ระบบอื่น ๆ และจัดการกวาดล้างทำลายภัยคุกคามให้เรียบร้อย เพื่อให้ระบบกลับมาทำงานได้สมบูรณ์ดังเดิม โดยการคืนสภาพได้ทางไซเบอร์ เป็นการรวมกันของการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) การจัดการความเสี่ยง และความต่อเนื่องในการดำเนินงานขององค์กร เพื่อให้เกิดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เริ่มตั้งแต่การตรวจจับการคุกคาม การกู้คืนระบบ ไปจนถึงการปรับปรุงกระบวนการรักษาความปลอดภัยอย่างต่อเนื่อง ซึ่งการคืนสภาพได้ทางไซเบอร์เป็นกรอบการทำงานที่ออกแบบมาเพื่อช่วยให้องค์กรสามารถต้านทานการโจมตีทางไซเบอร์ได้ ไม่ใช่เพียงแค่การป้องกันชั้นเดียว แต่เป็นวิธีสำหรับองค์กรในการจัดการโครงสร้างการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบขององค์กร และเป็นกระบวนการทำซ้ำที่ทำให้การกู้คืนระบบจากการโจมตีทางไซเบอร์สามารถทำได้ดียิ่งขึ้น ช่วยให้เกิดการเฝ้าระวังอย่างต่อเนื่องตลอดเวลาทั่วทั้งองค์กร ทั้งนี้ หลักการสำคัญ 5 ประการของการคืนสภาพได้ทางไซเบอร์ ประกอบด้วย (Dickson & Goodwin, 2020)



ภาพที่ 1 กรอบแนวทางการคืนสภาพได้ทางไซเบอร์

ที่มา: Dickson and Goodwin (2020)

3.1.1 การระบุความเสี่ยง (Identification) เป็นสิ่งที่ควรทำเป็นอันดับแรก เนื่องจากเป็นการทำความเข้าใจในการบริหารจัดการภายในองค์กร ตั้งแต่เรื่องบุคลากร ขีดความสามารถ ข้อมูลและระบบภายในต่าง ๆ ตลอดจนทรัพย์สินทั้งหมดขององค์กร เพื่อนำมาประเมินความเสี่ยงและวางแผนจัดการภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อองค์กรได้อย่างเหมาะสม

3.1.2 การป้องกัน (Protect) เป็นส่วนที่มีความสำคัญมากที่สุดจากทั้ง 5 หลักการ การป้องกันจะเริ่มตั้งแต่การวางกลไกและขั้นตอนเพื่อรักษาความปลอดภัย การติดตั้งอุปกรณ์ เช่น Firewall การบำรุงรักษาอุปกรณ์ กระบวนการจัดการข้อมูล และการควบคุมการเข้าถึงและใช้งานระบบ นอกจากนี้ยังรวมถึงการฝึกอบรมและสร้างความตระหนักให้บุคลากรถึงเรื่องความสำคัญของความปลอดภัยเทคโนโลยีสารสนเทศอีกด้วย

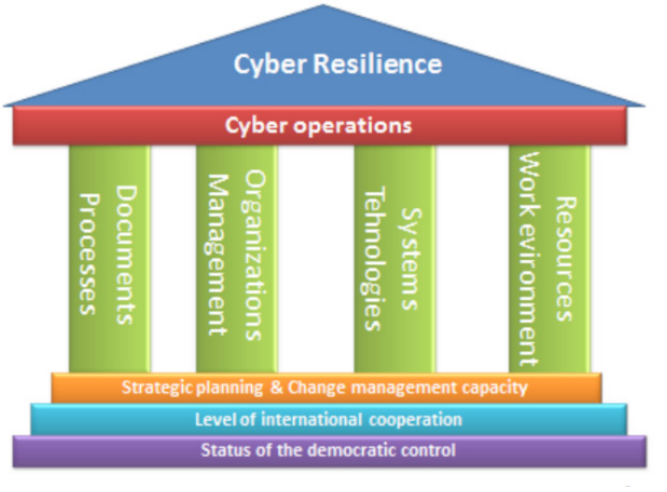
3.1.3 การตรวจจับ (Detect) จุดสำคัญของส่วนนี้คือ การเฝ้าระวังและติดตามเหตุการณ์หรือกิจกรรมน่าสงสัยที่อาจเป็นภัยคุกคามทางไซเบอร์ซึ่งกระทบต่อองค์กร รวมถึงการตรวจสอบหาช่องโหว่ของระบบ เพื่อที่จะได้พัฒนาระบบให้มีความต้านทานต่อภัยคุกคามทางไซเบอร์ได้มากยิ่งขึ้น

3.1.4 การตอบสนอง (Respond) หลังจากตรวจพบความผิดปกติที่ส่งผลต่อความปลอดภัยเทคโนโลยีสารสนเทศแล้ว ทางองค์กรจำเป็นต้องมีการตอบสนองต่อเหตุการณ์ดังกล่าวอย่างเหมาะสม โดยการวางแนวทางปฏิบัติให้ชัดเจน มีการวิเคราะห์หาสาเหตุและสื่อสารกันระหว่างองค์กรในกรณีที่อาจต้องขอความช่วยเหลือจากหน่วยงานภายนอก เพื่อหาแนวทางการป้องกันและลดโอกาสเกิดปัญหาซ้ำได้ในอนาคต

3.1.5 การกู้คืนระบบ (Recovery) เมื่อถูกโจมตีทางไซเบอร์ ทางองค์กรจำเป็นต้องทำให้ระบบกลับมาใช้งานได้เป็นปกติอย่างรวดเร็วที่สุด เพื่อให้ธุรกิจดำเนินต่อไปได้อย่างต่อเนื่อง และลดความสูญเสียทั้งด้านการเงินและด้านชื่อเสียงขององค์กร ดังนั้นจึงต้องมีการวางแผนการกู้คืนอย่างมีระบบ และมีการติดต่อสื่อสารที่ดีทั้งภายในและภายนอกองค์กร

3.2 Shalamano (2019)

ได้วิเคราะห์สภาพแวดล้อมในโลกไซเบอร์ เพื่อระบุแบบจำลองสำหรับการคืนสภาพได้ทางไซเบอร์ในมุมมองขององค์กรและพนักงาน โดยมีการนำเสนอถึงสถาปัตยกรรมองค์กรที่มีการคืนสภาพได้ทางไซเบอร์ (ภาพที่ 2) ซึ่งเป็นโครงสร้างที่เป็นไปตามแนวปฏิบัติของการวิจัยด้านธรรมาภิบาลความมั่นคงปลอดภัย โดยเปลี่ยนจากการมุ่งเน้นจากความมั่นคงปลอดภัยไซเบอร์เพียงอย่างเดียวมาเป็นการทำงานร่วมกันกับการคืนสภาพได้ทางไซเบอร์



ภาพที่ 2 สถาปัตยกรรมองค์กรที่มีการคืนสภาพได้ทางไซเบอร์

ที่มา: Shalamano (2019)

3.3 Conklin et al. (2017)

กล่าวว่า การคืนสภาพได้ทางไซเบอร์ไม่ใช่การป้องกันแบบเดิม ๆ แต่ยังมุ่งเน้นไปที่การตรวจจับการบุกรุกเครือข่ายหรือตรวจจับมัลแวร์ ซึ่งแนวคิดการคืนสภาพได้ทางไซเบอร์เป็นการทำให้องค์กรสามารถดำรงอยู่ได้ในทางปฏิบัติและสามารถกู้คืนระบบเมื่อเผชิญกับเหตุการณ์โจมตีทางไซเบอร์ได้ทุกรูปแบบ การนำสถาปัตยกรรมองค์กรที่มีการคืนสภาพได้ทางไซเบอร์ไปใช้งานให้ได้อย่างมีประสิทธิภาพจำเป็นต้องมีวิสัยทัศน์เชิงกลยุทธ์ ทั้งยังต้องการการมีส่วนร่วมอย่างบูรณาการเพื่อให้มั่นใจว่าวิสัยทัศน์นั้นเหมาะสม นอกจากนี้ยังต้องมีการเปลี่ยนแปลงวัฒนธรรมองค์กรร่วมด้วย จึงจะทำให้กลยุทธ์การคืนสภาพได้ทางไซเบอร์นั้นประสบความสำเร็จ

4. นิยามศัพท์

4.1 ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

ความมั่นคงปลอดภัยไซเบอร์ที่ใช้กันในปัจจุบันมีความหมายหลากหลาย ไม่ชัดเจน ซ้ำซ้อน และอาจเปลี่ยนแปลงได้ตามการนำไปใช้งานของแต่ละองค์กร ซึ่งนิยามของ “ความมั่นคงปลอดภัยไซเบอร์” ตามมาตรฐาน ISO/IEC 27032:2012 หมายถึง การปกป้องรักษาความเป็นความลับ ความถูกต้อง และความพร้อมในการเข้าถึงของข้อมูลภายในโลกไซเบอร์

4.2 การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience)

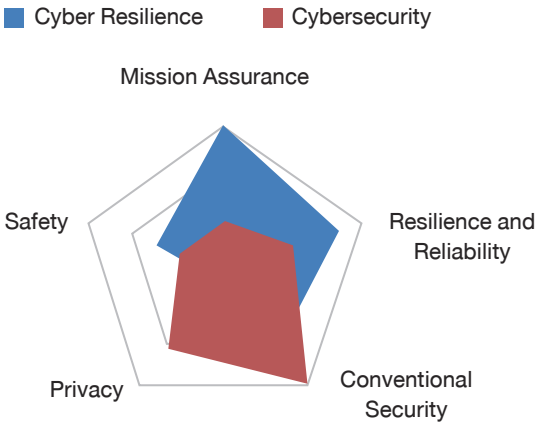
การคืนสภาพได้ทางไซเบอร์ คือ ความสามารถในการเตรียมตัวและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ จึงอาจกล่าวได้ว่า “การคืนสภาพได้ทางไซเบอร์” มุ่งเน้นไปในเรื่องของความพร้อม หรือการปรับตัวเพื่อรับมือกับสถานการณ์ที่เกี่ยวข้องกับภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้เสมอ ซึ่งแตกต่างกับคำว่า “ความมั่นคงปลอดภัยไซเบอร์” ที่เน้นไปในทางป้องกันไม่ให้เกิด (จันทกานต์ ผลพล, 2563)

คำนิยามศัพท์ในเอกสาร Presidential Policy Practice: Critical Infrastructure. Security and Resilience (PPD-21) โดยทำเนียบขาว รัฐบาลสหรัฐได้ให้คำจำกัดความ “Security” แตกต่างจากคำว่า “Resilience” ดังนี้ (ปริญญา หอมเอนก, 2561)

“Security” หมายถึง การลดความเสี่ยงให้กับโครงสร้างพื้นฐานทั้งทางกายภาพและทางไซเบอร์ มุ่งเน้นไปที่การบริหารจัดการ การบุกรุก การโจมตี รวมทั้งภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้นโดยตั้งใจและไม่ได้ตั้งใจ เช่น การก่อการร้าย การโจมตีทางไซเบอร์

“Resilience” หมายถึง ความสามารถในการเตรียมตัวและการปรับตัวต่อการเปลี่ยนแปลง รวมทั้งความสามารถในการทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้นโดยตั้งใจและไม่ได้ตั้งใจ

“การคืนสภาพได้ทางไซเบอร์” มีความหมายที่แตกต่างจาก “ความมั่นคงปลอดภัยไซเบอร์” ดังภาพที่ 3 “การคืนสภาพได้ทางไซเบอร์” ให้ความสำคัญกับการรับประกันว่าองค์กรสามารถบรรลุภารกิจได้โดยไม่ถูกขัดขวางด้วยภัยคุกคามทางไซเบอร์ ซึ่งมีทั้งความปลอดภัย ความน่าเชื่อถือ และความยืดหยุ่น ในขณะที่ “ความมั่นคงปลอดภัยไซเบอร์” เน้นไปที่ความเป็นส่วนตัว (Privacy) และความปลอดภัยทั่วไปทางเทคโนโลยีสารสนเทศและการสื่อสาร



ภาพที่ 3 ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยไซเบอร์และการคืนสภาพได้ทางไซเบอร์

ที่มา: ปริญญา หอมเอนก (2561)

5. ผลการศึกษา

5.1 รูปแบบและประเภทภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์เป็นสิ่งที่เกิดขึ้นเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมีวัตถุประสงค์ในการโจมตีใน 3 ลักษณะ ได้แก่ การนำความลับไปเปิดเผย (Data confidentiality) การเปลี่ยนแปลงข้อมูล (Data integrity) และการทำให้ระบบหยุดบริการ หรือไม่สามารถใช้งานได้ (System availability) ซึ่งการจะเข้าดำเนินการกับระบบคอมพิวเตอร์นั้นมีกลยุทธ์การโจมตี (Tactics) องค์กรตามกรอบการโจมตีของ MITRE (MITRE Attack Framework) (Mitre, n.d.) ได้แก่

1) การลาดตระเวน (Reconnaissance) เป็นการรวบรวมข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร เช่น ข้อมูลองค์กร โครงสร้างพื้นฐาน เจ้าหน้าที่/บุคลากร เป็นต้น เพื่อกำหนดขอบเขตและจัดลำดับความสำคัญของวัตถุประสงค์ในการโจมตี

2) การพัฒนาทรัพยากร (Resource development) เป็นการสร้างทรัพยากรสำหรับการโจมตีทางไซเบอร์ เช่น การขโมยทรัพยากรหรือโค้ดต่าง ๆ สำหรับการปฏิบัติการ หรือการขโมยอีเมลสำหรับการทำฟิชชิง (Phishing)[2]

[2] Phishing เป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ มักเป็นในรูปแบบอีเมลหรือเว็บไซต์เพื่อหลอกลวงให้เหยื่อเผยข้อมูลความลับต่าง ๆ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต รวมถึงการหลอกลวงให้กดลิงก์เพื่อแอบติดตั้งมัลแวร์ลงในคอมพิวเตอร์ของเหยื่อ

3) การเข้าถึงเป้าหมาย (Initial access) เป็นการเข้าถึงเครือข่ายสารสนเทศขององค์กร ได้แก่ การเจาะระบบผ่านช่องโหว่ของแอปพลิเคชัน เช่น ช่องโหว่การอัปโหลดไฟล์ขึ้นบนเว็บไซต์ ช่องโหว่ของโปรแกรมบริหารจัดการบนเว็บไซต์ หรือช่องโหว่ของโปรแกรมเครือข่ายส่วนตัวเสมือน มีการเดารหัสผ่านของบัญชีผู้ใช้หากระบบไม่ได้ถูกตั้งค่าการป้องกัน (Brute Force Attack) รวมถึง Spearphishing[3] ที่เป็นเป้าหมาย

4) การดำเนินการ (Execution) เป็นขั้นตอนการเรียกโปรแกรมหรือคำสั่งอันตราย (Malicious code) ในระบบภายใน หรือการเรียกใช้ผ่านการเข้าถึงระยะไกล (Remote access) ขึ้นมาประมวลผล เช่น เรียกใช้งานโปรแกรมผ่าน Command line หรือ PowerShell[4] ทำการเข้าถึงระบบจากระยะไกล

5) ความพยายามที่จะรักษาจุดที่ยึดครองไว้ได้ (Persistence) เป็นการทำให้มัลแวร์ยังคงทำงานอยู่ในระบบถึงแม้อุปกรณ์จะถูกปิดหรือเปลี่ยนแปลงการตั้งค่า เช่น การกำหนดค่าการเข้าถึง (Configuration) ต่าง ๆ ใหม่

6) ความพยายามในการยกระดับสิทธิการเข้าถึง (Privilege escalation) ของระบบด้วยการใช้ประโยชน์จากจุดอ่อนของระบบ เพื่อเข้าถึงข้อมูลที่จำเป็นต้องมีสิทธิเข้าถึงระดับสูง เช่น ข้อมูล ผู้บริหาร หรือข้อมูลผู้ดูแลระบบ เป็นต้น

7) การพยายามหลบหลีกการตรวจจับ (Defense Evasion) เป็นเทคนิคที่ใช้หลบเลี่ยงการตรวจจับหรือการสังเกตความผิดปกติของระบบ เช่น การปิดซอฟต์แวร์ความปลอดภัย การซ่อนหรือปลอมแปลงมัลแวร์ไม่ให้ปรากฏเมื่อเรียกดูข้อมูลด้วยวิธีปกติ การลบไฟล์ log ของระบบ เป็นต้น

8) การเข้าถึงข้อมูลประจำตัว (Credential access) เป็นการพยายามขโมยบัญชีและรหัสผ่านสำหรับเข้าสู่ระบบ

9) การค้นพบ (Discovery) เป็นการค้นพบสภาพแวดล้อมทางเครือข่ายและระบบเครือข่ายภายในโดยมีจุดประสงค์เพื่อปรับแนวทางการโจมตี หรือตรวจหาข้อมูลสำคัญว่าอยู่ที่ใด และจะใช้เพื่อประโยชน์การใด

---

[3] Spearphishing เป็นการโจมตีที่พุ่งเป้าไปยังเป้าหมายรายบุคคล โดยอาชญากรไซเบอร์จะค้นหาข้อมูลเบื้องต้นของพนักงานในองค์กรที่เป็นเป้าหมายจากช่องทางต่าง ๆ เช่น เครือข่ายสังคมออนไลน์ (Social network) จากนั้นอาชญากรไซเบอร์จะสร้างอีเมลฟิชชิง ที่ระบุเนื้อหาสอดคล้องกับเป้าหมายเพื่อให้เป้าหมายเชื่อใจกดลิงก์ที่แนบมากับอีเมล

[4] PowerShell คือ แอปพลิเคชันสำหรับรับคำสั่งและภาษาสคริปต์ที่สร้างขึ้นบน .NET ซึ่ง PowerShell ช่วยให้ผู้ดูแลระบบและผู้ใช้งานสามารถสั่งให้กระบวนการต่าง ๆ ทำงานโดยอัตโนมัติบนระบบปฏิบัติการ (Linux, macOS และ Windows)

10) การทำ Lateral movement เป็นการรวบรวมข้อมูลเครือข่ายเพื่อทำการเจาะไปยังอุปกรณ์เครื่องอื่น ๆ ต่อไป เช่น เชื่อมต่อไปยังคอมพิวเตอร์เครื่องอื่นผ่านช่องทาง Secure shell (SSH) หรือ Remote Desktop (RDP) ด้วยการโจมตีผ่าน SMB โดยอาศัยฟีเจอร์ (Feature) Windows Admin Share เพื่อขโมยข้อมูลสั่งดำเนินการ (Run) โปรแกรมปลายทาง หรืออาจเพิ่มมัลแวร์ลงในโฟลเดอร์ที่มีการแชร์ผ่านเครือข่าย โดยตั้งชื่อไฟล์ให้ดูเหมือนว่าเป็นไฟล์ทั่วไป เพื่อผู้ใช้คนอื่นในระบบหลงเชื่อและเปิดไฟล์ดังกล่าว

11) การรวบรวม (Collection) เป็นการรวบรวมข้อมูลจากแหล่งเก็บข้อมูลต่าง ๆ ขององค์กรเพื่อส่งออกไปยังภายนอก

12) การใช้เทคนิค Command and control จากภายนอกเพื่อส่งข้อมูลออกจากระบบไปยังภายนอกโดยหลีกเลี่ยงการตรวจจับ

13) การกรองข้อมูล (Exfiltration) คือ การขโมยข้อมูลออกไปด้วยวิธีการทำเป็นแพ็กเกจ (Package) บีบอัด และเข้ารหัส รวมถึงจำกัดขนาดในการส่งข้อมูล เพื่อหลีกเลี่ยงการถูกตรวจจับขณะนำข้อมูลออกจากระบบ

14) การสร้างผลกระทบ (Impact) เป็นความพยายามในการจัดการ ควบคุม ขัดขวาง หรือทำลายระบบขององค์กร ซึ่งรวมความพยายามในการทำลายและเปลี่ยนแปลงแก้ไขข้อมูลขององค์กร

Gaurav (2020) เสนอรูปแบบของภัยคุกคามในอนาคตอันใกล้ที่องค์กรต้องเผชิญ โดยมีรูปแบบภัยคุกคามใหม่ ๆ ได้แก่

1) ช่องโหว่บนคลาวด์ (Cloud vulnerability) เนื่องจากองค์กรต่าง ๆ ใช้ประโยชน์จากแอปพลิเคชันและจัดเก็บข้อมูลละเอียดอ่อนที่เกี่ยวข้องกับพนักงานและธุรกิจบนระบบคลาวด์ โดย Forbes คาดการณ์ว่าร้อยละ 83 ของปริมาณงานทั้งหมดขององค์กรจะถูกนำขึ้นมาอยู่บนระบบคลาวด์ภายในปี พ.ศ. 2563 ซึ่งการละเมิดข้อมูล การกำหนดค่าอินเตอร์เฟส (Interface) และ API (Application Programing Interface) ที่ไม่ถูกต้องปลอดภัย การลักลอบใช้บัญชีภัยคุกคามภายในที่เป็นอันตรายและการโจมตี DDoS (Distributed Denial of Service)[5] ถือเป็นภัยคุกคามด้านความปลอดภัยอันดับต้น ๆ ของแพลตฟอร์มคลาวด์

[5] DDoS (Distributed Denial of Service) เป็นการพยายามที่จะทำให้บริการออนไลน์ไม่พร้อมใช้งาน สำหรับผู้ใช้งานมักจะเป็นการทำให้ระบบหยุดชะงัก หรือระงับการบริการของเซิร์ฟเวอร์โฮสต์ (Hosting server) ชั่วคราว

2) AI-Enhanced Cyber threats เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ถูกอาชญากรไซเบอร์ใช้ประโยชน์ในการเปิดการโจมตีทางไซเบอร์ที่ซับซ้อน โดยการใช้มัลแวร์ที่ถูกควบคุมโดยปัญญาประดิษฐ์ทำให้สามารถสร้างสแปม (Spam) ที่มีความน่าเชื่อถือ ซึ่งสามารถหลีกเลี่ยงการตรวจจับความปลอดภัยและปรับให้เข้ากับแต่ละเป้าหมายได้ดีขึ้น ทั้งยังมีการใช้ปัญญาประดิษฐ์ ในการสแกนสื่อสังคมออนไลน์เพื่อค้นหาบุคคลที่เหมาะสมในการกำหนดเป็นเป้าหมายสำหรับการทำฟิชชิง แล้วสามารถสร้างสแปมที่ปรับแต่งให้เหมาะกับเหยื่อ

3) AI Fuzzing เป็นเทคนิคการค้นหาช่องโหว่ในแอปพลิเคชัน หรือในระบบที่ได้รับความนิยมมากที่สุด ด้วยการใช้ประโยชน์จากเทคโนโลยีการเรียนรู้ของเครื่อง (Machine learning) ทำให้อาชญากรไซเบอร์ยังสามารถใช้เทคนิคนี้เพื่อเริ่มการโจมตีได้อย่างอัตโนมัติ และย่นระยะเวลาของการโจมตีแบบ Zero-day

4) Machine Learning Poisoning อาชญากรไซเบอร์ใช้ประโยชน์จากข้อมูลที่ผู้ใช้สร้างขึ้น เช่น การให้คะแนนความพึงพอใจ ประวัติการซื้อ หรือการเข้าชมเว็บ เพื่อใช้หลอกลวง มีการฝังสคริปต์ (Script) ที่เป็นอันตราย หรือโทรจัน (Trojan) เพื่อใช้ทำลายระบบ

5) Smart Contract Hacking เป็นการโจมตีสัญญาดิจิทัลอัจฉริยะ (Smart contract) บนแพลตฟอร์มบล็อกเชน (Blockchain) เช่น Ethereum ซึ่งทำงานด้วยเทคโนโลยีบล็อกเชน และมีการใช้เหรียญดิจิทัล คือ Ether (ETH) ในการขับเคลื่อนการทำงานของระบบ โดย Ethereum ถูกสร้างขึ้นมาเป็นแพลตฟอร์มแบบเปิด (Open Source) เพื่อให้นักพัฒนานำเอาจุดเด่นด้านการทำ Smart Contract ไปพัฒนาและประยุกต์ใช้งานได้หลากหลาย แต่ก็เป็นการเปิดช่องโหว่ที่ให้เกิดการโจมตี Smart Contract ของ Ethereum ได้

6) Social Engineering Attacks เช่น ฟิชชิง มักถูกใช้โดยอาชญากรไซเบอร์เพื่อหลอกลวงเอาข้อมูลส่วนบุคคลจากเหยื่อ เช่น ชื่อบัญชีและรหัสผ่านในการเข้าสู่ระบบเครือข่ายขององค์กร หรือการหลอกล่อข้อมูลบัตรเครดิตและข้อมูลสำหรับการทำธุรกรรมทางการเงิน โดยการฟิชชิงสามารถทำได้หลายวิธี ได้แก่ อีเมลฟิชชิง ที่เป็นการล่อลวงเหยื่อผ่านทางอีเมล หรือ SMiShing ซึ่งเป็นการล่อลวงเหยื่อผ่านระบบข้อความ SMS (SMS Phishing) บนโทรศัพท์เคลื่อนที่

7) Deepfake เป็นอีกรูปแบบหนึ่งของการปลอมแปลงเนื้อหาตั้งแต่ข้อความ ภาพ เสียง วิดีโอ หรือแม้กระทั่งบทความ คือ การปลอมแปลงอัตลักษณ์ของบุคคลด้วยปัญญาประดิษฐ์ ซึ่งในระยะเวลาอันใกล้นี้ Deepfake จะพัฒนาไปสู่วิธีการปลอมแปลงที่ซับซ้อนและดูน่าเชื่อถือมากขึ้น

5.2 อาชญากรรมไซเบอร์และผลกระทบ

จากรายงานของ Crowdstrike เรื่องดัชนีชี้วัดอาชญากรรมไซเบอร์ (eCrime) ในช่วงปลายปี พ.ศ. 2563 ถึงกุมภาพันธ์ พ.ศ. 2564 พบว่าอัตราความถี่ของอาชญากรรมไซเบอร์จากทั่วโลกเพิ่มขึ้นถึงร้อยละ 123.94 (Crowdstrike, 2021) แสดงให้เห็นว่าแนวโน้มของการก่ออาชญากรรมไซเบอร์กำลังพุ่งสูงขึ้นอย่างต่อเนื่อง ก่อให้เกิดความสูญเสียทั้งส่วนบุคคลและทางธุรกิจจากความเสียหายจากการทำลายข้อมูล การขโมยเงินดิจิทัล การสูญเสียประสิทธิภาพจากการทำงาน การโจรกรรมทรัพย์สินทางปัญญา การขโมยข้อมูลส่วนบุคคลและข้อมูลทางการเงิน การฉ้อฉล การทุจริต การหยุดชะงักทางธุรกิจภายหลังจากการถูกโจมตี การกู้ข้อมูลและฟื้นฟูระบบ และการคุกคามต่อชื่อเสียงและความไว้วางใจ

นอกจากนี้ ข้อมูลจาก Cybersecurity Venture ระบุว่ามูลค่าความเสียหายที่เกิดจากการโจมตีทางไซเบอร์ภายในปี พ.ศ. 2564 จะมีมูลค่าสูงถึง 6 ล้านล้านดอลลาร์สหรัฐ และยังคาดการณ์ว่าในช่วง 5 ปีข้างหน้าจะมีมูลค่าความเสียหายจากอาชญากรรมทางไซเบอร์ทั่วโลกขยายตัวเพิ่มขึ้นร้อยละ 15 ต่อปี ซึ่งหมายความว่าในปี พ.ศ. 2568 คาดว่าจะมีมูลค่าความเสียหายสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐ ซึ่งสูงกว่าความเสียหายจากภัยพิบัติทางธรรมชาติ โดยข้อมูลอาชญากรรมไซเบอร์ที่มีการกระทำกับองค์กรขนาดใหญ่ในปี พ.ศ. 2564 เช่น กรณีบริษัท Brenntag ซึ่งเป็นผู้จัดจำหน่ายสารเคมีของสหพันธ์สาธารณรัฐเยอรมนี ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่โดยกลุ่ม Darkside ในช่วงเวลาเดียวกันกับการโจมตีบริษัท Colonial Pipeline ของสหรัฐอเมริกา ซึ่งกลุ่มอาชญากรไซเบอร์มีการเรียกค่าไถ่สูงถึง 7.5 ล้านดอลลาร์สหรัฐ หลังจากนั้นมีการเจรจาต่อรองลดลงเหลือ 4.4 ล้านดอลลาร์สหรัฐ เพื่อแลกกับข้อมูลที่ถูกขโมยไป 150 กิกะไบต์ (สำนักข่าวอินโฟเควสท์, 2564)

Gaurav (2020) ได้รายงานผลการศึกษาของ Threat Horizon ถึงภัยคุกคามทางไซเบอร์ที่องค์กรต่าง ๆ กำลังจะต้องเผชิญ ซึ่งประกอบด้วย 3 ประเด็นหลัก ได้แก่ 1) การหยุดชะงัก (Disruption) ทำให้อินเทอร์เน็ตหยุดทำงานซึ่งส่งผลกระทบต่อการดำเนินธุรกิจ 2) การบิดเบือน (Distortion) เป็นการแพร่กระจายของข้อมูลที่ผิดโดยบอต (Bots)[6] และการบิดเบือนแหล่งข้อมูลทำให้ความน่าเชื่อถือของข้อมูลลดลงโดยอัตโนมัติ 3) การเสื่อมสภาพ (Deterioration) ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีขัดแย้งกับความต้องการในการพัฒนาความมั่นคงของชาติส่งผลเสียต่อความสามารถขององค์กรในการควบคุมข้อมูลและความปลอดภัยของระบบ

สำหรับขององค์กรในประเทศไทยนั้น มีงานวิจัยของ Microsoft และ Frost and Sullivan ในปี พ.ศ. 2561 โดยการสร้างแบบจำลองเพื่อประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นจากอาชญากรรมไซเบอร์ โดยนำปัจจัยเชิงเศรษฐกิจองค์รวมและข้อมูลเชิงลึกจากผู้เข้าร่วมการสำรวจมาพิจารณา แบบจำลองนี้

[6] บอต ย่อมาจาก Robot เป็นอุปกรณ์คอมพิวเตอร์ที่มีมัลแวร์ฝังอยู่เพื่อรับคำสั่งจากอาชญากรไซเบอร์

แบ่งผลกระทบที่สามารถเกิดขึ้นได้จากเหตุการณ์ภัยคุกคามทางไซเบอร์เป็น 3 แบบ ประกอบด้วย 1) ผลกระทบทางตรงที่ก่อให้เกิดความเสียหายทางการเงิน ลดประสิทธิภาพการทำงาน ยืดระยะเวลาในการฟื้นฟู และเกิดค่าเสียหายที่ต้องชดใช้ 2) ผลกระทบทางอ้อม ซึ่งเป็นการสูญเสียโอกาสทางธุรกิจ เช่น การสูญเสียลูกค้าเพราะขาดความเชื่อมั่น 3) ผลกระทบวงกว้าง เป็นผลกระทบมวลรวมเชิงเศรษฐกิจ เช่น สภาพคล่องทางการใช้จ่ายขององค์กรและผู้บริโภค ซึ่งการโจมตีทางไซเบอร์นั้น สามารถก่อความเสียหายได้มากมายที่อาจไม่เห็นในทันที ทั้งในทางอ้อมและในวงกว้าง จึงทำให้โดยทั่วไปแล้ว มูลค่าความเสียหายที่แท้จริงของภัยคุกคามนั้น มักถูกประเมินไว้ต่ำกว่าความเป็นจริง นอกจากนี้ ยังมีความเสียหายในการคว้าโอกาสทางธุรกิจในยุคแห่งเศรษฐกิจดิจิทัล โดยผลการสำรวจพบว่าองค์กรกว่าร้อยละ 73 ได้หยุดการนำเทคโนโลยีดิจิทัลเข้ามาปฏิรูปธุรกิจ อันเนื่องจากความกังวลในเรื่องภัยคุกคามทางไซเบอร์ (“ภัยคุกคามทางไซเบอร์สร้างความเสียหายองค์กรถึง 2 แสนกว่าล้านบาท”, 2561)

5.3 การรับมือภัยคุกคามทางไซเบอร์

5.3.1 CIA Triad คือ พื้นฐานของการรักษาความปลอดภัยด้านสารสนเทศ ซึ่งประกอบด้วย

1) การรักษาความลับ (Confidentiality) เป็นสิ่งสำคัญในโลกปัจจุบันที่ต้องปกป้องข้อมูลขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต การปกป้องความลับต้องมีการกำหนดและบังคับใช้สิทธิการเข้าถึงข้อมูลและจำเป็นต้องกำหนดการเข้าถึงข้อมูล โดยพิจารณาถึงความอ่อนไหวของข้อมูลนั้น ๆ เช่น ความเสียหายในกรณีที่ความลับขององค์กรรั่วไหลหรือถูกละเมิด ซึ่งวิธีการทั่วไปที่ใช้ในการจัดการการรักษาความลับในการเข้าถึงข้อมูล ได้แก่ รายการควบคุมการเข้าถึง (Access control list) และการเข้ารหัสไฟล์

2) การปกป้องความถูกต้องสมบูรณ์ (Integrity) ของข้อมูลเป็นการป้องกันข้อมูลจากการถูกลบหรือแก้ไขจากบุคคลที่ไม่ได้รับอนุญาต

3) การปกป้องความถูกต้องสมบูรณ์ (Availability) ของข้อมูลในองค์กร กลไกการตรวจสอบสิทธิ์ ช่องทางการเข้าถึง และระบบทั้งหมด กล่าวโดยรวมก็คือ ความพร้อมใช้งานทำให้องค์กรสามารถเข้าถึงและเข้าใช้งานทรัพยากรที่จำเป็นในระบบได้ตามความต้องการและยังคำนึงถึงความปลอดภัย โดยระบบที่มีความพร้อมใช้งานสูงมีสถาปัตยกรรมระบบที่ออกแบบมาเพื่อปรับปรุงความพร้อมใช้งานของระบบ

5.3.2 เสาหลักของความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

1) เทคโนโลยี (Technology) ด้านความมั่นคงปลอดภัยเปรียบเสมือนมาตรการควบคุมสำหรับปกป้องค์กรจากภัยคุกคาม ปัจจัยหลักในการเลือกใช้เทคโนโลยีให้ได้อย่างถูกต้องและเหมาะสมกับสภาวะแวดล้อมขององค์กรไม่ได้มาจากความทันสมัยหรือจำนวนฟีเจอร์ของ

เทคโนโลยี แต่มาจากการประเมินความเสี่ยง ซึ่งเทคโนโลยีที่ถูกเลือกมาเป็นมาตรการควบคุมจะต้องสามารถลดระดับความเสี่ยงด้านความมั่นคงปลอดภัยขององค์กรให้อยู่ในขอบเขตที่ยอมรับได้ โดยในปัจจุบัน เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ที่องค์กรทั้งหลายให้ความสนใจ ประกอบด้วย 1) เทคโนโลยีด้านการป้องกัน ได้แก่ Firewall ซึ่งเป็นอุปกรณ์ที่ทำหน้าที่ป้องกันการคุกคามระบบ อุปกรณ์การป้องกันการโจมตีแบบ DDoS และอุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System: IPS) เป็นต้น 2) เทคโนโลยีด้านการตรวจจับ เช่น เทคโนโลยีการวางเหยื่อล่อการโจมตีทางไซเบอร์ (Deception) อุปกรณ์ Endpoint Detection and Response (EDR) สำหรับตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัย และ 3) เทคโนโลยีจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของเครือข่าย เพื่อนำไปใช้ในการตอบโต้การโจมตี เช่น อุปกรณ์ Security Information and Event Management (SIEM)

2) กระบวนการ (Process) เพื่อรองรับการใช้งานเทคโนโลยี เช่น การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business continuity plan) เพื่อให้ระบบขององค์กรยังคงให้บริการต่อไปได้แม้เกิดภัยพิบัติ หรือมีการใช้งานจริงของภัยคุกคามและเหตุผิดปกติรูปแบบต่าง ๆ เพื่อให้ผู้ที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและเป็นระบบ นอกจากนี้ องค์กรยังสามารถนำกระบวนการที่เป็นมาตรฐาน หรือกรอบการทำงานเข้ามาใช้เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรได้ เช่น (1) ISO/IEC 27001:2013 เป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) (2) NIST Cybersecurity Framework เป็นกรอบการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะมีการระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจจับภัยคุกคาม การตอบสนองต่อภัยคุกคาม และการกู้คืนระบบ

นอกจากนี้ ยังรวมถึงการกำหนดแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมถึงการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การระบุความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ความน่าจะเป็นของภัยคุกคามและผลกระทบต่อองค์กร และความเสี่ยงที่องค์กรยอมรับได้ เช่น แผนการประเมินช่องโหว่ และแผนการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) เพื่อประเมินสถานะความมั่นคงปลอดภัยด้านสารสนเทศและเครือข่าย รวมถึงการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response Plan) ที่กำหนดขั้นตอนการกู้คืนระบบ การสอบสวนเหตุการณ์ การเก็บรักษาหลักฐาน การทบทวนมาตรการความปลอดภัยหลังการดำเนินการเพื่อให้เท่าทันต่อสภาพแวดล้อมทางไซเบอร์ ซึ่งต้องมีการกำหนดระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) การกำหนดระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective) และมาตรการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber Security Resilience and Recovery)

3) บุคลากร (People) นับเป็นปัจจัยสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ ถึงแม้องค์กรจะมีเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ที่ดีหรือมีกระบวนการที่รัดกุมมากเพียงใด แต่ถ้าพนักงานในองค์กรขาดความรู้และทักษะในการรับมือกับภัยคุกคาม ระบบขององค์กรก็ยังอาจตกเป็นเป้าหมายของอาชญากรไซเบอร์ได้ ดังนั้น องค์กรจำเป็นต้องมีการอบรมให้บุคลากรทราบถึงรูปแบบของภัยคุกคามไซเบอร์ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย นอกจากนี้ ยังควรฝึกฝนพนักงานผ่านทางการจำลองสถานการณ์จริง (Fighter pilot) เพื่อให้พนักงานมีประสบการณ์ และสามารถตอบสนองต่อการโจมตีได้อย่างรวดเร็วและถูกต้อง ทั้งนี้ ความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ที่ดีจำเป็นต้องมีการฝึกฝนและทดสอบอยู่เป็นระยะ จากการศึกษาถึงโมเดลของ Red Team และ Blue Team (Khera, 2021) โดยการจัดให้มีทั้ง Red Team และ Blue Team นี้เพื่อ 1) ระบุจุดอ่อนที่เกี่ยวข้องกับบุคคล เทคโนโลยี และระบบ 2) กำหนดขอบเขตของการปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์การป้องกันในทุก ๆ ช่วงของการโจมตี 3) สร้างประสบการณ์ขององค์กรเกี่ยวกับวิธีการตรวจจับและควบคุมการโจมตี 4) พัฒนากิจกรรมเกี่ยวกับการตอบสนองและการแก้ไขการโจมตีเพื่อกลับสู่สภาวะการทำงานปกติ โดย Red Team เป็นทีมที่ทำหน้าที่ในการโจมตี การตรวจหาจุดอ่อน การตรวจหาช่องโหว่ (Vulnerable) ซึ่งต้องใช้ทักษะขั้นสูงในการโจมตีระบบคอมพิวเตอร์ และทำลายระบบความปลอดภัยสารสนเทศขององค์กร นอกจากนี้ยังมีการทดสอบการตอบสนองของพนักงานในองค์กรผ่าน Social engineering attack โดยทุก ๆ ขั้นตอน เป็นการจำลองสถานการณ์การโจมตีทางไซเบอร์จริงที่เกิดขึ้นในโลกในปัจจุบัน ซึ่งการมี Red Team นี้เป็นการวัดความสามารถขององค์กรในการบรรเทา (Mitigate) การตรวจจับและการกู้คืนระบบจากการโจมตีทางไซเบอร์ ในส่วนของ Blue Team เป็นทีมที่ป้องกันการโจมตีในทุก ๆ ประเภทของภัยคุกคามทางไซเบอร์ (Cyber threat) และยังเป็นการทดสอบประสิทธิภาพของระบบป้องกันให้พร้อมใช้งาน ปิดช่องโหว่ (Vulnerable patch) ในระบบสารสนเทศ โดย Blue Team มักทำงานภายในศูนย์ปฏิบัติการความปลอดภัย (Security Operation Center: SOC) เพื่อยกระดับการป้องกันการโจมตีองค์กรด้วยการเฝ้าติดตามเครือข่ายตลอด 24 ชั่วโมง และตรวจจับกิจกรรมที่อาจเป็นภัยคุกคามและหยุดการโจมตี ซึ่งทั้ง 2 ทีมจะต้องทำงานร่วมกันโดยมีหน้าที่ต่างกัน เพื่อค้นหาและขจัดช่องโหว่ รวมทั้งป้องกันไม่ให้อาชญากรไซเบอร์เข้าโจมตีระบบสารสนเทศขององค์กรได้ โดยทั้งหมดนี้เป็นการทดสอบการป้องกันและความสามารถทางไซเบอร์ที่มีอยู่ในสภาพแวดล้อมที่มีความเสี่ยงต่ำ

6. สรุปผล

การพัฒนาการด้านรูปแบบการโจมตีทางไซเบอร์ทั้งในเชิงเทคนิคและเชิงกลยุทธ์นั้น มีความซับซ้อนรุนแรง พัฒนาขึ้นตามลำดับเพื่อหลีกหนีการตรวจจับจากอุปกรณ์ป้องกันการโจมตี มีกรณีตัวอย่างขององค์กรขนาดใหญ่ในโลกที่ยังคงถูกโจมตีทางไซเบอร์และได้รับความเสียหายจากอาชญากรไซเบอร์ด้วยมูลค่าความสูญเสียทั้งที่จับต้องได้และจับต้องไม่ได้ ในขณะที่องค์กรธุรกิจของประเทศไทยที่กำลังก้าวไปสู่เศรษฐกิจ

ดิจิทัลยังมีความกังวลต่อภัยคุกคามทางไซเบอร์อันเนื่องมาจากการลงทุนด้านดิจิทัลขององค์กร การรับมือกับภัยคุกคามทางไซเบอร์ในปัจจุบันมีการนำเทคโนโลยีและกระบวนการที่เป็นมาตรฐาน เพื่อตรวจสอบให้มั่นใจว่าระบบสารสนเทศขององค์กรจะมีสภาพความพร้อมใช้งานอย่างมั่นคงและปลอดภัย แต่อย่างไรก็ดี ในด้านของทรัพยากรมนุษย์ที่จะรับมือกับภัยคุกคามทางไซเบอร์นั้น มีการนำเสนอโมเดลการจัดการแบบ Red Team และ Blue Team เพื่อให้สามารถตอบสนองต่อการโจมตีได้ทุกรูปแบบ และสามารถแก้ไขให้สภาพแวดล้อมทางไซเบอร์กลับคืนสู่ปกติได้อย่างเป็นระบบ

การคืนสภาพได้ทางไซเบอร์มีผลโดยตรงต่อการดำเนินธุรกิจขององค์กร และช่วยสร้างความเชื่อมั่นในธุรกิจ พร้อมสร้างความได้เปรียบในการแข่งขันได้ เนื่องจากลูกค้าจะพบว่าองค์กรมีความพร้อมในการปรับตัวและฟื้นตัวจากการโจมตีได้อย่างรวดเร็ว โดยกรอบแนวทางการคืนสภาพได้ทางไซเบอร์มุ่งเน้นไปที่ความคงทนและความยืดหยุ่นต่อการถูกโจมตี ซึ่งมีการให้ความสำคัญในการตรวจสอบและทำซ้ำในทุก ๆ กระบวนการ ตั้งแต่การระบุความเสี่ยง การป้องกันระบบ การตรวจจับภัยคุกคาม การตอบสนองต่อเหตุการณ์ทางไซเบอร์ และการกู้คืนระบบ ทั้งนี้ การคืนสภาพได้ทางไซเบอร์ไม่สามารถกระทำได้โดยปราศจากการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ โดยทั้งสองส่วนจะมีความเกี่ยวข้องกันในด้านของความปลอดภัย (Safety) ความยืดหยุ่นและความน่าเชื่อถือ (Resilience and Reliability) ซึ่งการคืนสภาพได้ทางไซเบอร์ให้ความสำคัญกับการคงสภาพการดำเนินการขององค์กรให้ทนทานต่อการบุกรุก การโจมตี และดำเนินการได้อย่างปกติขณะทำการคืนสภาพได้ของระบบ ในขณะที่ความมั่นคงปลอดภัยไซเบอร์มุ่งเน้นไปที่ความเป็นส่วนตัวและความปลอดภัยทั่วไปทางเทคโนโลยีสารสนเทศ ดังนั้น องค์กรจึงควรมีการดำเนินกลยุทธ์การคืนสภาพได้ทางไซเบอร์โดยเชื่อมโยงกับพื้นฐานแนวคิดที่ว่าไม่มีระบบป้องกันภัยคุกคามใดมีความปลอดภัยได้ทั้งหมด องค์กรควรให้ความสำคัญกับเสาหลักด้านความมั่นคงปลอดภัยไซเบอร์ในด้านเทคโนโลยี กระบวนการ และบุคคล

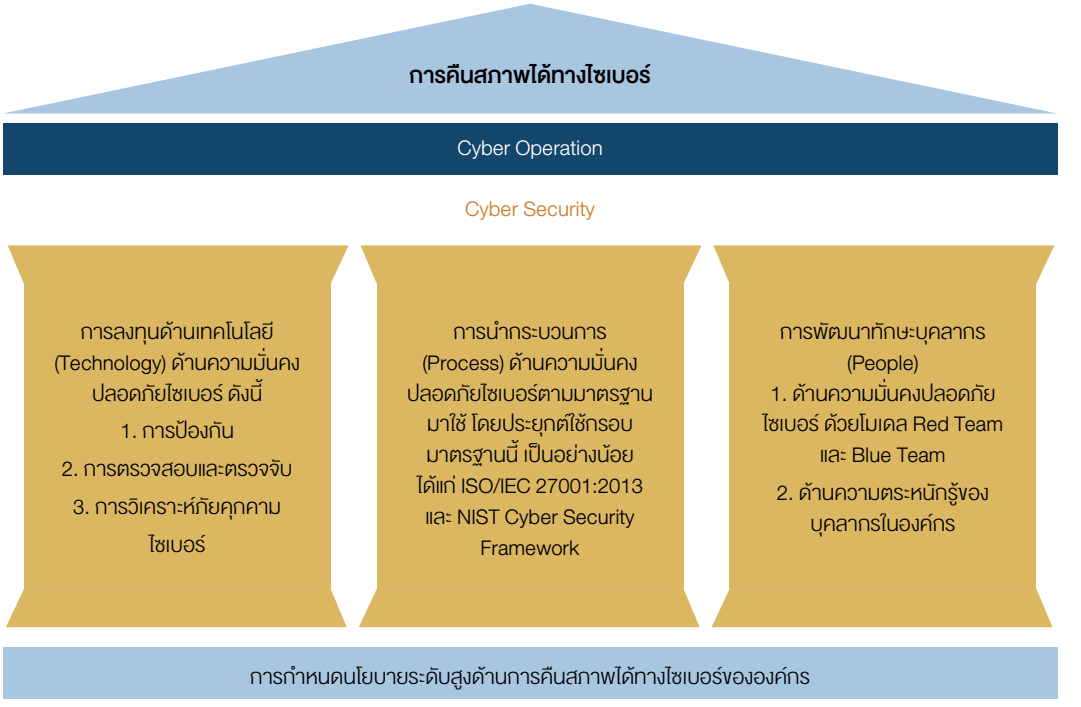
7. การอภิปรายผล

โอกาสและความท้าทายของการดำเนินกลยุทธ์การคืนสภาพได้ทางไซเบอร์ สำหรับการรับมือกับภัยคุกคามทางไซเบอร์ ได้แก่ 1) ความพยายามขององค์กรในการยกระดับความสามารถในการแข่งขันในการเข้าสู่เศรษฐกิจดิจิทัล 2) การกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นสากลสำหรับการตรวจสอบกระบวนการ ขั้นตอน และความพร้อมของเครื่องมืออุปกรณ์ทางดิจิทัลต่าง ๆ 3) การครอบครองอุปกรณ์ด้านความมั่นคงปลอดภัยไซเบอร์ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่จะช่วยให้องค์กรสามารถวิเคราะห์ภัยคุกคามตรวจสอบและดำเนินการได้ครบถ้วนตามวัฏจักรของการดำเนินการตามกลยุทธ์การคืนสภาพได้ทางไซเบอร์ 4) การศึกษาวิเคราะห์กลยุทธ์ พฤติกรรม รูปแบบและวิธีการโจมตีของอาชญากรไซเบอร์ตามขั้นตอนมาตรฐานซึ่งอ้างอิงการเฝ้าระวังและการตรวจจับภัยคุกคาม และการกู้คืนระบบ

สำหรับปัญหาอุปสรรคสำคัญที่องค์กรต้องประเมินเพื่อให้การรับมือกับภัยคุกคามทางไซเบอร์สามารถกระทำได้อย่างมีประสิทธิภาพ คือ 1) แนวคิดและทัศนคติในการรับมือกับภัยคุกคามทางไซเบอร์ที่สร้างความกังวลในการลงทุน 2) ความพร้อมของปัจจัยด้านบุคลากรที่มีศักยภาพในการรองรับการโจมตีทางไซเบอร์ 3) ความพยายามของอาชญากรไซเบอร์ในการพัฒนาเทคโนโลยี ขั้นตอน กระบวนการ และรูปแบบการโจมตีใหม่ๆ

และการสร้างมัลแวร์ด้วยเทคโนโลยีปัญญาประดิษฐ์ ที่มีความน่าเชื่อถือซึ่งทำให้หลุดรอดจากการตรวจจับของอุปกรณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้ 4) การวิเคราะห์พฤติกรรมบุคคลด้วยเทคโนโลยีปัญญาประดิษฐ์ เพื่อให้อาชญากรทางไซเบอร์สามารถเข้าถึงตัวบุคคลและหลอกลวงได้ง่าย เนื่องจากในมุมมองของผู้โจมตียังคงมองว่าการโจมตีผ่านบุคลากรในองค์กรเป็นวิธีที่ทำให้เข้าถึงระบบขององค์กรได้ง่ายที่สุด

ในยุคที่องค์กรเปลี่ยนผ่านไปสู่การเป็นองค์กรดิจิทัลเพื่อดำเนินธุรกิจบนพื้นฐานเศรษฐกิจดิจิทัลนั้น การลงทุนทางเทคโนโลยีดิจิทัลเป็นสิ่งจำเป็นอย่างมากต่อองค์กร เพื่อยกระดับความสามารถในการแข่งขัน อย่างไรก็ดี การลงทุนนั้นจำเป็นอย่างยิ่งที่จะต้องมีการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ด้วย ด้วยเหตุผลด้านความท้าทายในการยกระดับความสามารถในการแข่งขันสำหรับการนำองค์กรเข้าสู่เศรษฐกิจดิจิทัล รวมถึงภาพลักษณ์และความน่าเชื่อถือของลูกค้าและคู่ค้า (Stakeholder) ในส่วนที่องค์กรสามารถรักษาความปลอดภัยข้อมูลลูกค้า และการทำธุรกรรมการค้าระหว่างกัน เป็นต้น หากแม้องค์กรมีความวิตกกังวลต่อการลงทุนความปลอดภัยดิจิทัล องค์กรเองก็จะไม่สามารถเข้าสู่ภาวการณ์แข่งขันบนพื้นฐานเศรษฐกิจดิจิทัล อาจส่งผลต่อองค์กรในด้านการแข่งขัน ปัจจุบันการเอาผิดกับกลุ่มอาชญากรไซเบอร์ยังอยู่ในขั้นตอนที่ไม่สามารถกระทำได้อย่างสมบูรณ์ ในขณะที่อาชญากรทางไซเบอร์พยายามเลือกเส้นทางการโจมตีเพื่อเอาชนะกลยุทธ์การป้องกันที่อาจเกิดขึ้น การหลบเลี่ยงการตรวจสอบการเงินด้วยการเรียกค่าไถ่ผ่านบล็อกเชน ดังนั้น องค์กรจึงควรดำเนินกลยุทธ์การคืนสภาพได้ทางไซเบอร์ มีการปรับวิสัยทัศน์สอดคล้องกับแนวทางตามทฤษฎีเกม (Game theory) สำหรับเกมความมั่นคงปลอดภัยไซเบอร์ที่ต้องมีการกระทำซ้ำ ๆ เป็นวงรอบ เพื่อให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างยั่งยืน โดยมีกรอบแนวคิดทางกลยุทธ์ดังภาพที่ 4



ภาพที่ 4 แนวคิดกลยุทธ์การคืนสภาพได้ทางไซเบอร์

ผลการศึกษาข้างต้นสามารถวิเคราะห์ได้เป็นกรอบแนวคิดกลยุทธ์การคืนสภาพได้ทางไซเบอร์ โดยเริ่มต้นที่การกำหนดนโยบายระดับสูงขององค์กรในการคืนสภาพได้ทางไซเบอร์ มีการนำหลักแนวคิดในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ด้วยการกำหนดเทคโนโลยีในการสนับสนุน ประกอบด้วย 1) เทคโนโลยีด้านการป้องกันภัยคุกคาม เทคโนโลยีด้านการตรวจสอบและตรวจจับภัยคุกคาม และเทคโนโลยีด้านการวิเคราะห์ภัยคุกคามทางไซเบอร์สำหรับการดำเนินงานเชิงรุกของระบบให้มีการวิเคราะห์พฤติกรรม เทคนิค รูปแบบ และลักษณะการคุกคามทางไซเบอร์ของอาชญากรไซเบอร์ให้ระบบปฏิเสธการเข้าถึง หรือหยุดยั้งภัยคุกคามได้ 2) กระบวนการด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถนำมาตรฐานต่าง ๆ ระดับโลกมาประยุกต์ใช้ร่วมกันเพื่อให้ครอบคลุมมิติ ได้แก่ ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานสำหรับระบบความปลอดภัยของข้อมูล มีการประเมินความเสี่ยง การออกแบบด้านการรักษาความมั่นคงปลอดภัยและการนำไปปฏิบัติ รวมถึงความปลอดภัยทางกายภาพในการเข้าถึงระบบสารสนเทศขององค์กร นำมาประยุกต์ร่วมกับ NIST Cybersecurity Framework ที่เป็นกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่จะช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว 3) การพัฒนาทักษะของบุคลากรในองค์กรด้วยกรอบแนวคิด Red Team และ Blue Team บนสภาพแวดล้อมความมั่นคงปลอดภัยสารสนเทศขององค์กร ให้พร้อมกับการปฏิบัติงานเชิงรับของระบบและภัยคุกคาม รวมถึงการปฏิบัติงานเชิงรุกในการตรวจหาและหยุดยั้งภัยคุกคาม ซึ่งในทุกๆ มิติของเทคโนโลยี กระบวนการ และบุคลากรขององค์กรนั้นควรบรรจุไว้ในกรอบของการคืนสภาพได้ทางไซเบอร์ที่ประกอบด้วย การระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจจับภัยคุกคาม การตอบสนองต่อภัยคุกคาม และการกู้คืน พร้อมทั้งมีการเรียนรู้จากกรณีภัยคุกคามต่าง ๆ ที่เกิดขึ้นกับองค์กรด้วย เพื่อให้องค์กรมีความสามารถในการคืนสภาพได้ทางไซเบอร์ที่รวดเร็ว ลดผลกระทบและความเสียหายที่จะเกิดขึ้นจากองค์กร

8. ข้อเสนอแนะ

8.1 ข้อเสนอแนะต่องานวิจัย

องค์กรควรมีการกำหนดกลยุทธ์การลงทุนเพื่อการคืนสภาพได้ทางไซเบอร์ควรเป็นแบบพลวัต (Dynamic) โดยทุก ๆ วัฏจักรของการคืนสภาพได้ทางไซเบอร์จะต้องดำเนินการภายใต้กรอบแนวทางดังภาพที่ 4 เพื่อให้มีเครื่องมือและตัวช่วย ทั้งในด้านปฏิบัติการด้านไซเบอร์ (Cyber Operation) ขององค์กรพื้นฐานสำคัญของความมั่นคงปลอดภัยไซเบอร์ ทั้งในส่วนของเทคโนโลยี กระบวนการ และบุคลากรที่ต้องดำเนินการแบบสอดประสานกันอย่างเป็นรูปแบบ และมีการกำหนดนโยบายระดับสูงองค์กรสำหรับมาตรการการคืนสภาพได้ทางไซเบอร์ เพื่อให้ทุก ๆ ส่วนที่เกี่ยวข้องได้ดำเนินการโดยมีเป้าหมายร่วมกัน

องค์กรควรให้ความสำคัญในการตอบสนองต่อการโจมตีทางไซเบอร์ ตั้งแต่ระดับนโยบายที่มิใช่เพียงแค่การสนับสนุนทางด้านเงินทุนสำหรับการสร้างระบบรักษาความปลอดภัย แต่ต้องรวมถึงการตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ในบุคลากรทุกระดับ

การสร้างทักษะการตอบสนองต่อการโจมตีให้แก่บุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ด้วยการทำ Red Teaming และ Blue Teaming โดยเป็นการปรับแนวคิดในเรื่องการรักษาความปลอดภัยไซเบอร์ขององค์กรที่ไม่ควรจำกัดเพียงแค่การป้องกันการโจมตีเท่านั้น และไม่มีเทคโนโลยีใดที่จะสามารถป้องกันภัยคุกคามทางไซเบอร์ได้อย่างสมบูรณ์แบบ ดังนั้น องค์กรควรมีการจำลองการโจมตีจากอาชญากรไซเบอร์ และฝึกฝนทีมรุกและทีมรับเป็นระยะ ๆ

8.2 ข้อเสนอแนะเชิงนโยบายสำหรับกิจการสื่อสาร

กิจการสื่อสาร สารสนเทศ และโทรคมนาคมจัดเป็นหนึ่งในเสาหลักของโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) เป็นหนึ่งในหน่วยงานกำกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งมีหน้าที่ในการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยควรมีการกำหนดนโยบายดังนี้

8.2.1 การกำหนดยุทธศาสตร์ “การคืนสภาพได้ทางไซเบอร์” ของสำนักงาน กสทช. โดยเป็นการดำเนินงานแบบบูรณาการ (Integrate) ร่วมกันกับระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ในปัจจุบัน มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ พร้อมทั้งบูรณาการด้านทักษะของบุคลากรด้านกิจการสื่อสาร สารสนเทศ และโทรคมนาคมให้มีศักยภาพ ก่อให้เกิดการคืนสภาพได้ทางไซเบอร์

8.2.2 การกำหนดหลักเกณฑ์และแนวปฏิบัติสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ “ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม” ให้ดำเนินการด้านการคืนสภาพได้ทางไซเบอร์ของระบบการสื่อสารและโทรคมนาคม เพื่อให้ระบบการสื่อสารมีความมั่นคงปลอดภัยและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

บรรณานุกรม

จันทกานต์ ผลพล. (2563, 13 ธันวาคม). *ทำความรู้จักกับ Cyber Resilience สิ่งที่ทำให้ไปต่อได้ในทุกสถานการณ์.* ntcyfence. https://www.catcyfence.com/it-security/article/what-is-cyber-resilience/

ปริญญา หอมเอนก. (2561, 5 กันยายน). Cyber Resilience คืออะไร. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/blog/detail/645457

ภัยคุกคามทางไซเบอร์สร้างความเสียหายองค์กรถึง 2 แสนกว่าล้านบาท. (2561). thumbsup. https://www.thumbsup.in.th/cyber-security-microsoft

วริยา คำชนะ. (2562, 22 ตุลาคม). ธุรกิจ: *ภัยไซเบอร์ระบาดหนัก "ธุรกิจไทย"*. *กรุงเทพธุรกิจ*. https://www.bangkokbiznews.com/news/detail/851637.

สำนักข่าวอินโฟเควสท์. (2564, 9 มิถุนายน). *Cyber Attack-คลื่นใต้น้ำแห่งยุคดิจิทัลที่ต้องจับตามอง*. https://www.infoquest.co.th/2021/94874

Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). *Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture. 12th International Conference on Cyber Warfare and Security* (pp. 105-111). https://books.google.co.th/books?hl=en&lr=&id=iXWQDgAAQBAJ&oi=fnd&pg=PA105&dq=cyber+resilience+strategy&ots=HW6fnMSQw0&sig=4Red10ZTrhiJ908kba_ibRUnn60&redir_esc=y#v=onepage&q=cyber%20resilience%20strategy&f=false

Crowdstrike. (2021). *The 2021 Crowdstrike global Threat Report.* https://go.crowdstrike.com/crowdstrike-global-threat-report-2021.html

Dickson, F., & Goodwin, P., (2020). *Five Key Technologies for Enabling a Cyber-Resilience Framework.* IBM. https://www.ibm.com/services/business-continuity/cyber-resilience?p1=Search&p4=43700064924790111&p5=p&gclid=CjwKCAjwjJmIBhA4EiwAQdCbxhd9Ar_m8BXqz1W314hjnvzu2K-jQpMG4IJR5joQzNgXHqiPAeexyxoCCtoQAvD _BwE&gclsrc=aw.ds

Gaurav, B. (2020). *5 Cybersecurity Threats to Be Aware of in 2020*. IEEE. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020

ISO/IEC. (2012), *ISO/IEC/27043:2012 Information technology – Security techniques Guidelines for cybersecurity*. (n.p.)

Khera, V. (2021, March 24). *Red Team VS Blue Team*. Linkedin. https://www.linkedin.com/pulse/red-team-vs-blue-dr-varin-khera/?trackingId=yUCDstClsMUBW29dovQTWg%3D%3D

Mitre. (n.d.). *Enterprise Matrix*. https://attack.mitre.org/matrices/enterprise/

Shalamano, V. (2019). Organising for IT Effectiveness, Efficiency and Cyber Resilience in Academic Sector: National and Region Dimension. *Information & Security, 21*(42), 49-66. http://connections-qj.org/system/files/4203_it_academic_sector.pdf

Trend Micro Research. (2021). *What We Know About the Darkside Ransomware and the US Pipeline Attack.* https://www.trendmicro.com/en_th/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html