# แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร
# Cyber Security Risk Management Guidance for Enterprise

**บทความวิชาการ**

**อนาวิล แก้วสอาด[1] และ ณัฐวี อุตกฤษฎ์[2]**
Anawin Kaewsa-ard and Nattavee Utakrit
**ภาควิชาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล**
**มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กรุงเทพฯ ประเทศไทย 10800**
Department of Information Technology Management, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand 10800
E-mail: s6307021910041@email.kmutnb.ac.th[1] and E-mail: nattavee.u@itd.kmutnb.ac.th[2]

**บทคัดย่อ**

บทความนี้มีวัตถุประสงค์เพื่อศึกษาค้นคว้าแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร และเสนอวิธีการบริหารความเสี่ยงอย่างเหมาะสมเป็นไปตามมาตรฐานสากล สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเกิดขึ้นกับระบบสารสนเทศขององค์กรได้ในอนาคตโดยการศึกษาครั้งนี้ได้อธิบายถึงกระบวนการบริหารความเสี่ยง ตั้งแต่กระบวนการเตรียมการ กระบวนการประเมินความเสี่ยง การรายงานผลการประเมินความเสี่ยง และการติดตามผลการประเมินความเสี่ยงตามวงรอบ จนถึงการกำหนดมาตรการควบคุม เพื่อตอบสนองต่อความเสี่ยงที่เกิดขึ้นจากการสังเคราะห์กรอบแนวคิด NIST Framework กฎหมาย ระเบียบข้อบังคับ ตลอดจนข้อมูลจากเอกสารทางวิชาการต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางปฏิบัติ และลำดับกระบวนการบริหารความเสี่ยงอย่างเป็นระบบที่สามารถนำไปปฏิบัติหรือประยุกต์ใช้ได้จริงในองค์กร

วันที่รับบทความ: 1 ต.ค.63 วันที่แก้ไขบทความ: 10 ก.พ.64 วันที่ตอบรับบทความ: 15 ก.พ.64

จากผลการศึกษาค้นคว้าพบว่า การบริหารความเสี่ยงที่ดีจะเป็นส่วนสำคัญอย่างยิ่งในการบริหารความมั่นคงปลอดภัยไซเบอร์ในองค์กรให้ประสบความสำเร็จ เนื่องจากองค์กรได้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้งาน เพื่อสนับสนุนภารกิจให้ขับเคลื่อนไปข้างหน้า ทั้งนี้แนวทางการบริหารความเสี่ยงยังเป็นกระบวนการที่ช่วยพิจารณาว่ามาตรการควบคุมที่ได้มีการบังคับใช้มีความเหมาะสมสอดคล้องกับบริบทขององค์กร และสามารถลดระดับความเสี่ยงได้อย่างแท้จริง อีกทั้งยังช่วยส่งเสริมให้ระบบสารสนเทศ สามารถสนับสนุนกระบวนการทางธุรกิจ และระบบงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

**คำสำคัญ**

ความมั่นคงปลอดภัยไซเบอร์, การบริหารความเสี่ยงระดับองค์กร, การประเมินความเสี่ยง

**Abstracts**

This article aims to study enterprise cyber security risk management guidance as well as to present appropriate risk management methods that meet worldwide standard so as to deal with cyber threats of information system in the future. This study explains risk management procedures, including preparation, risk assessment, risk assessment report, and follow-up on risk assessment results. The study also includes measures in order to respond to the risks. The author synthesized the National Institute of Standards and Technology Framework (NIST Framework), laws, regulations, and academic documents in implementing the risk management practices and processes that are systematic and practical for organizations.

The results of the study show that an appropriate risk management is essential to successful management of cyber security in an organization because information technology is contributed to drive enterprise mission. Risk management guidance also determines whether the measures implemented in the organization appropriately align with the context of organization and are able to effectively reduce risks. Furthermore, it also helps to improve information systems in order to support business processes and the core functions of organizations more efficiently.

**Keywords:** Cyber Security, Enterprise Risk Management, Risk Assessment

**บทนำ**

ปัจจุบันเทคโนโลยีสารสนเทศ และอินเทอร์เน็ตนับว่าเป็นเครื่องมือที่ได้เข้ามามีบทบาทสำคัญอย่างยิ่งในการขับเคลื่อนภารกิจหลักขององค์กรทั่วโลก โดยเฉพาะอย่างยิ่งองค์กรที่เป็นผู้นำในอุตสาหกรรมต่าง ๆ รวมถึงหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure) ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์, 2562, เล่ม 136) จำนวน 8 ด้าน ประกอบด้วย 1) ด้านความมั่นคงของรัฐ 2) ด้านการบริการภาครัฐที่สำคัญ 3) ด้านการเงินการธนาคาร 4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม 5) ด้านการขนส่งและโลจิสติกส์ 6) ด้านพลังงานและสาธารณูปโภค 7) ด้านสาธารณสุข และ 8) ด้านอื่นตามที่คณะกรรมการประกาศเพิ่มเติม ถึงวันนี้

ไม่สามารถปฏิเสธได้ว่า ภัยไซเบอร์ (Cyber Security Threats) เป็นเรื่องไกลตัวอีกต่อไป เพราะโลกกำลังเปลี่ยนแปลงเข้าสู่ยุคเศรษฐกิจดิจิทัล ดังนั้น ประเด็นสำคัญเรื่องความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการความเสี่ยงในระดับองค์กร (Enterprise Risk Management) จึงเป็นอีกประเด็นสำคัญที่ระดับผู้บริหารต้องคำนึงถึงภัยไซเบอร์ ไม่ได้เป็นความเสี่ยงที่เกิดขึ้นแต่กับระบบสารสนเทศ หรืออุปกรณ์คอมพิวเตอร์ขององค์กรแต่เพียงอย่างเดียวเท่านั้น แต่ยังมีความเสี่ยงที่เกิดขึ้นในรูปแบบของกระบวนการ (Process) ซึ่งประกอบไปด้วย ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงจากการให้บริการหรือฟังก์ชันงานขององค์กร (Services Risk) ความเสี่ยงที่เกิดขึ้นจากบุคลากร (Employees Risk) ความเสี่ยงที่เกิดขึ้นจากการที่ไม่ปฏิบัติตามข้อกฎหมาย (Law Risk) และความเสี่ยงที่ส่งผลต่อภาพลักษณ์และชื่อเสียงของหน่วยงาน (Reputational Risk) ซึ่งความเสี่ยงในลักษณะนี้ จะส่งผลกระทบอย่างมากต่อองค์กร (อรรคเดช ประทีปอุษานนท์ และธาราทิพย์ กัลยาณมิตร, 2560, น.15) ดังนั้น ผู้บริหารระดับสูง หรือผู้นำองค์กรจำเป็นต้องให้ความสนใจ และความสำคัญกับการป้องกันเพื่อปกป้องชื่อเสียงขององค์กร โดยเฉพาะการเสื่อมเสียชื่อเสียงใน Social Media ตลอดจนการรั่วไหลของข้อมูลที่มีชั้นความลับขององค์กร ผ่านช่องทางต่าง ๆ เช่น Shadow Data/Shadow IT ทั้งนี้ ปัญหาต่าง ๆ อาจจะเกิดจากแฮ็กเกอร์ภายนอกองค์กร หรืออาจเกิดจากบุคลากรในองค์กรเอง (Insider Threats) เนื่องจากขาดความตระหนักรู้ก็มีความเป็นไปได้ทั้งสิ้น (Coat, 2559) รวมไปถึงผู้บริหารระดับสูงส่วนใหญ่ยังคงเข้าใจว่า ภัยไซเบอร์เป็นปัญหาด้านเทคนิคแต่เพียงอย่างเดียวเท่านั้น แท้จริงแล้วภัยไซเบอร์เป็นเรื่องที่ผู้บริหารระดับสูงหรือผู้ที่มีส่วนเกี่ยวข้อง จำเป็นต้องมีความรู้ความเข้าใจถึงผลกระทบ และเป็นความเสียหายที่อาจเกิดขึ้นกับองค์กร เพื่อที่จะนำไปสู่การบริหารจัดการอย่างยั่งยืน

**นิยามศัพท์ที่เกี่ยวข้องกับการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Definition)**

**1. ความเสี่ยง (Risk)** ความไม่แน่นอนที่มีโอกาสเกิดขึ้น เนื่องจากเรามีข้อมูลไม่เพียงพอต่อการยืนยันผลลัพธ์ตามแผนการดำเนินงาน หรือวัตถุประสงค์ที่ตั้งไว้ รวมถึงปัจจัย หรือสิ่งที่อยู่นอกเหนือจากการควบคุม (Project Management Institute [PMI], 2017)

**2. การบริหารความเสี่ยง (Risk Management)** เป็นกระบวนการที่ใช้เพื่อบริหารจัดการผลกระทบ หรือความเสียหายที่มีโอกาสเกิดขึ้นต่อองค์กร หรือบุคลากรภายในองค์กร สำหรับมุมมองด้านความมั่นคงปลอดภัยไซเบอร์ หมายถึง ระบบสารสนเทศที่มีส่วนช่วยสนับสนุนภารกิจหลักของหน่วยงาน (International Organization for Standardization [ISO], 2009)

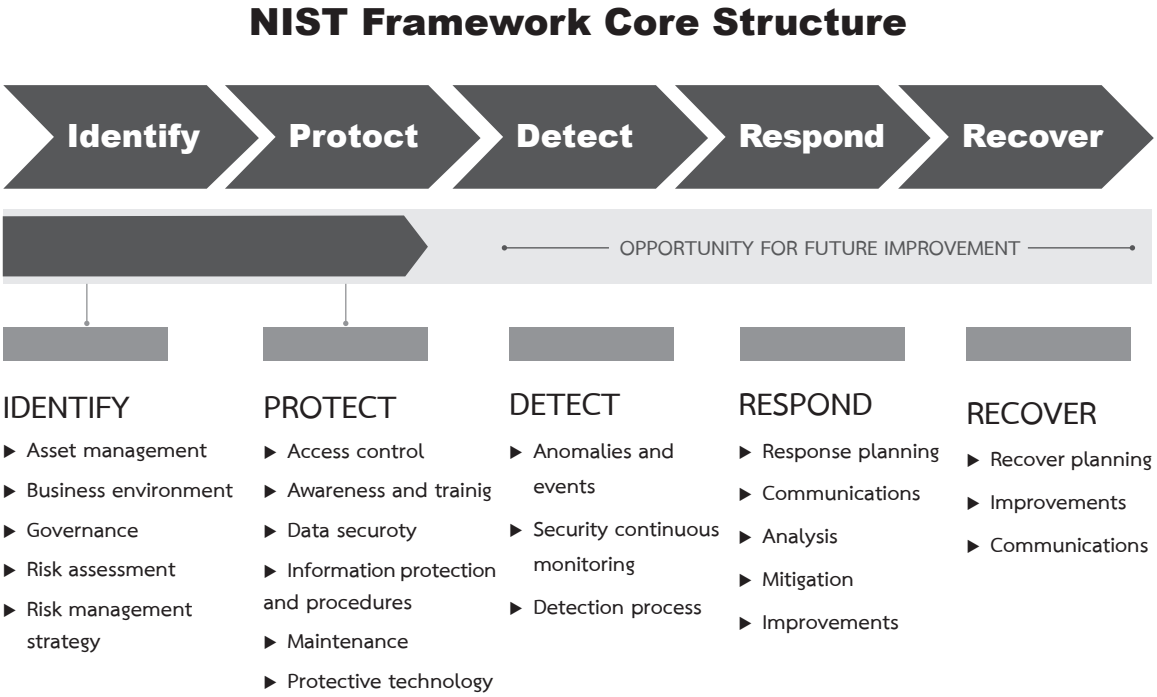
**3. การประเมินความเสี่ยง (Risk Assessment)** กระบวนการที่ทำให้ทราบว่าสินทรัพย์ขององค์กร มีระดับความเสี่ยงมากน้อยเพียงใด สินทรัพย์ใดมีความเสี่ยงมากที่สุด และยังเป็นกระบวนการที่ทำให้ทราบว่า สินทรัพย์ใดในองค์กรของเรามีความสำคัญมากที่สุด

**4. ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)** การลดความเสี่ยงให้กับโครงสร้างพื้นฐานทั้งทางกายภาพและทางไซเบอร์ มุ่งเน้นไปที่การบริหารจัดการ การบุกรุก การโจมตี รวมทั้งภัยธรรมชาติ และภัยที่มนุษย์ได้ก่อขึ้นทั้งตั้งใจ และไม่ได้ตั้งใจ เช่น การก่อการร้าย หรือการโจมตีทางไซเบอร์ (Bodeau and Graubart, 2017)

**NIST Framework กับบทบาทการบริหารความมั่นคงปลอดภัยไซเบอร์**

National Institute of Standards and Technology: NIST ได้ออก NIST Cyber Security Framework Version 1.0 ในปี พ.ศ.2557 และได้มีการปรับปรุงเป็น Version 1.1 ในปี พ.ศ.2561 (NIST, 2018)

โดยมีวัตถุประสงค์เพื่อให้หน่วยงานโครงสร้างพื้นฐานสารสนเทศที่สำคัญได้นำ 5 กระบวนการหลักของ NIST Framework Core Structure นำมาใช้ประโยชน์ในการปรับปรุงความปลอดภัยความเสี่ยงพื้นฐาน สำหรับเจ้าของผู้ประกอบการ หรือผู้สร้างโครงสร้างพื้นฐานสำคัญในองค์กรไปประยุกต์ใช้ตามบริบทของหน่วยงาน โดยไม่ได้บังคับตามกฎหมายแต่อย่างใด แต่ต้องการส่งเสริมให้องค์กรปรับกระบวนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้เข้าสู่สถานะที่เรียกว่า Cyber Resilience (เศรษฐพงศ์ มะลิสุวรรณ, 2558, น.13-17) ซึ่งจากคำนิยามศัพท์ในเอกสาร President Policy Practice: Critical Infrastructure Security and Resilience (The White House Office, 2013) หมายถึง ความสามารถในการเตรียมตัว และการปรับตัวต่อการเปลี่ยนแปลง รวมถึงขีดความสามารถในการทนทานต่อการบุกรุก โจมตี รวมทั้งภัยธรรมชาติ และภัยที่มนุษย์ได้ก่อขึ้นทั้งในรูปแบบตั้งใจ (Intention) หรือไม่ได้ตั้งใจ (Lack of Awareness) โดย 5 กระบวนการหลักของ NIST Framework Core Structure ในบทความนี้จะเน้นไปที่กระบวนการ Identify หรือกระบวนการเตรียมการบริหารความมั่นคงปลอดภัยไซเบอร์เป็นหลัก ซึ่งกระบวนการดังกล่าวจะเป็นการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญขององค์กร เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ดังภาพที่ 1



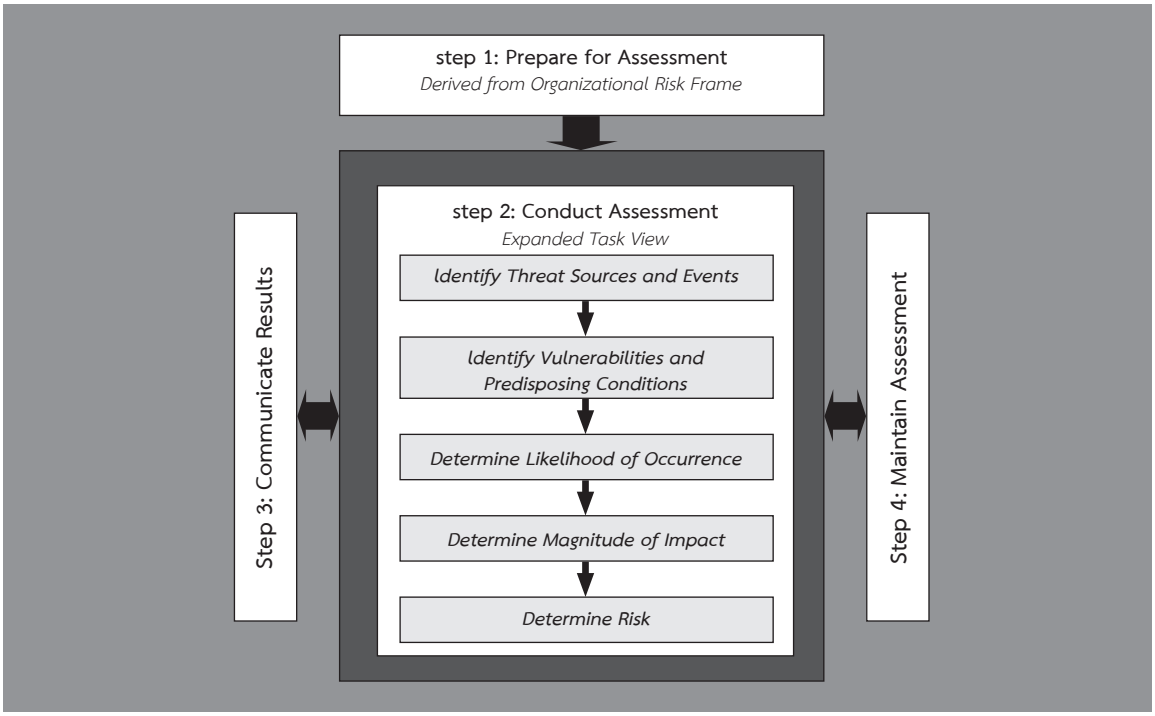

**ภาพที่ 1** ภาพรวมของ NIST Framework Core Structure

**ที่มา:** NIST Cyber Security Framework Version 1.1, 2018

**กรอบแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร**

การประเมินความเสี่ยงด้านไซเบอร์ (Cyber Risk Assessment) เป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยง (Cyber Risk Management) ทั้งนี้กระบวนการดังกล่าวถือว่าเป็นส่วนสำคัญในการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร (ปริญญา หอมเอนก, 2560) เนื่องจากว่าหน่วยงานมีการนำเทคโนโลยีสารสนเทศ และการสื่อสารเข้ามาใช้งานตามภารกิจที่หลากหลายและแตกต่างกัน ซึ่งบางภารกิจมีความสำคัญอย่างมาก จนไม่สามารถยอมให้ระบบสารสนเทศที่สนับสนุนภารกิจดังกล่าวใช้การไม่ได้ แม้จะเป็นเพียงระยะเวลาสั้น ๆ ในขณะที่บางภารกิจหากระบบสารสนเทศใช้งานไม่ได้เป็นระยะเวลาหนึ่ง ก็ยังไม่ได้รับผลกระทบมากนัก วัตถุประสงค์หลักของการประเมินความเสี่ยงด้านไซเบอร์ คือ การพิจารณาว่าจะนำมาตรการควบคุมด้านไซเบอร์มาใช้ในระดับที่เหมาะสมและสอดคล้องกับภารกิจขององค์กรเป็นสำคัญ (Gallagher, 2013)

หลักการสำคัญที่นำมาใช้ในการประเมินความเสี่ยงด้านไซเบอร์เป็นการนำมาตรฐาน NIST มาประยุกต์ใช้ เนื่องจากเป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล ประกอบกับการมีขั้นตอนในการประเมินความเสี่ยงที่ชัดเจนและไม่ซับซ้อน อีกทั้งมีความสอดคล้องกับมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอื่น ๆ ยกตัวอย่างเช่น ISO 27001:2013 Information Security Management System COBIT5 COSO เป็นต้น (Moeller, 2010) โดยการประเมินความเสี่ยงมีด้วยกันทั้งหมด 4 ขั้นตอน ดังภาพที่ 2 ดังนี้




**ภาพที่ 2** กระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment
**ที่มา:** Gallgher, 2012

จากภาพที่ 2 เป็นการอธิบายถึงภาพรวมขั้นตอนการประเมินความเสี่ยงตาม NIST 800-30R1 Guide for Conducting Risk Assessment (Gallagher, 2012) ซึ่งเป็นการปรับปรุง (Revision) จาก NIST 800-30 (Stoneburner, Goguen and Feringa, 2002) โดยประกอบไปด้วยขั้นตอนหลัก 4 ขั้นตอน ได้แก่ กระบวนการก่อนการประเมินความเสี่ยง การประเมินความเสี่ยง การรายงานผลการประเมินความเสี่ยง และการติดตามผลการประเมินความเสี่ยงตามวงรอบ ซึ่งในบทความนี้ผู้เขียนบทความจะอธิบายขั้นตอนแต่ละขั้นตอนจากการศึกษาค้นคว้าวิจัยกรอบแนวคิด NIST เพื่อให้ผู้ที่ศึกษาสามารถนำไปเป็นแนวทางในการประยุกต์ใช้ร่วมกับบริบทขององค์กรตนเองได้

**1. กระบวนการก่อนการประเมินความเสี่ยง (Prepare for Assessment)**

ขั้นตอนนี้เป็นการวิเคราะห์บริบทขององค์กร รวบรวมข้อมูลเกี่ยวกับคุณลักษณะของระบบ (System Characterization) เพื่อทำความเข้าใจว่าระบบสารสนเทศกับภารกิจหลักขององค์กรนั้นมีส่วนเกี่ยวข้องหรือขับเคลื่อนองค์กรของเราอย่างไร โดยตัวอย่างข้อมูลที่ใช้ในการประเมินความเสี่ยง ผู้เขียนบทความได้ยกตัวอย่างไว้ในตารางที่ 1 องค์ประกอบที่ใช้ในการประเมินความเสี่ยง ทั้งนี้ในการเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรสามารถดำเนินการเก็บข้อมูลอย่างเป็นระบบได้หลายรูปแบบ เช่น การทำแบบสอบถามแต่ละส่วนงาน การสัมภาษณ์ผู้ที่มีส่วนเกี่ยวข้อง การทบทวนเอกสาร หรือการใช้เครื่องมือเพื่อตรวจสอบหาช่องโหว่ เป็นต้น

**ตารางที่ 1** องค์ประกอบที่ใช้ในการประเมินความเสี่ยง

| **องค์ประกอบที่ใช้ในการประเมินความเสี่ยง (Risk Factors)** | | | |
|---|---|---|---|
| **1. โครงสร้างระบบสารสนเทศ (System Architect)** | **2. ข้อมูลสารสนเทศ (Information)** | **3. การกำกับดูแลกิจการ (Governance)** | **4. เจ้าหน้าที่ปฏิบัติงาน (Operation Officer)** |
| 1.1 ฮาร์ดแวร์<br>1.2 ซอฟต์แวร์<br>1.3 สถาปัตยกรรมความมั่นคงปลอดภัยระบบสารสนเทศ<br>1.4 ผังเครือข่ายคอมพิวเตอร์ | 2.1 ข้อมูลแต่ละฟังก์ชันงาน<br>2.2 รูปแบบการจัดเก็บข้อมูล<br>2.3 ความสำคัญของข้อมูล<br>2.4 ระดับชั้นความลับ<br>2.5 สิทธิ์ในการเข้าถึงระบบสารสนเทศขององค์กร | 3.1 ระบบ IT ที่ใช้ขับเคลื่อน<br>3.2 ภารกิจขององค์กร<br>3.3 นโยบายความมั่นคงปลอดภัยไซเบอร์<br>3.4 นโยบายการปฏิบัติงาน<br>3.5 มาตรการควบคุมด้านเทคนิค<br>3.6 มาตรการควบคุมด้านการบริหารจัดการ<br>3.7 มาตรการควบคุมด้านกายภาพและสภาพแวดล้อม | 4.1 เจ้าหน้าที่ดูแลระบบสารสนเทศ<br>4.2 ผู้ใช้งานระบบสารสนเทศ<br>4.3 องค์ความรู้ และขีดความสามารถ ในการใช้ระบบสารสนเทศขององค์กร |

**2. การประเมินความเสี่ยง (Conduct Risk Assessment)**

**2.1 การวิเคราะห์ภัยคุกคาม**

ขั้นตอนนี้เป็นกระบวนการประเมินความเสี่ยงโดยอันดับแรกของการเริ่มต้นประเมินความเสี่ยงได้นั้นจะต้องพิจารณาสิ่งที่เรียกว่าภัยคุกคามที่กระทำต่อระบบสารสนเทศของเราก่อนเป็นอันดับแรก ซึ่งภัยคุกคามตาม NIST 800-30 และจากงานวิจัยของ ปรัชญา เฉลิมวัฒน์ (2561) และอุดม ประตาทะยัง (2561) ได้ให้ขอบเขตนิยามของคำว่า ภัยคุกคามทางไซเบอร์ ประกอบไปด้วย ภัยคุกคามจากธรรมชาติ ภัยคุกคามจากสภาพแวดล้อม และภัยคุกคามที่เกิดขึ้นจากมนุษย์ สามารถแบ่งได้อีก 2 ประเภท ได้แก่ การโจมตีที่เกิดขึ้นอย่างตั้งใจ และการโจมตีที่เกิดขึ้นแบบไม่ตั้งใจ

**2.2 การวิเคราะห์ช่องโหว่**

ขั้นตอนนี้เป็นการปฏิบัติต่อจากขั้นตอนที่ 2.1 การวิเคราะห์ภัยคุกคาม (Threat Determination) มีวัตถุประสงค์เพื่อจัดทำรายการช่องโหว่ที่เกิดขึ้นจากระบบสารสนเทศของหน่วยงาน พิจารณาเทียบกับแหล่งที่มาของภัยคุกคาม ซึ่งขั้นตอนนี้สามารถทำได้หลายรูปแบบขึ้นอยู่กับความพร้อม และขีดความสามารถขององค์กร โดยบทความนี้ผู้เขียนได้ทำการศึกษาค้นคว้า และประยุกต์ใช้กรอบแนวคิดของ NIST 500-269 Software Assurance Tool (Black, Fong, Okun, and Gaucher, 2008) และหน่วยงาน OWASP (The Open Web Application Security Project) เข้ากระบวนการประเมินความเสี่ยง ทั้งนี้ได้ทำการสรุปประเภทของภัยคุกคามทางไซเบอร์ พร้อมยกตัวอย่างตามตารางที่ 2 ประเภทของภัยคุกคามทางไซเบอร์

**ตารางที่ 2** ประเภทของภัยคุกคามทางไซเบอร์

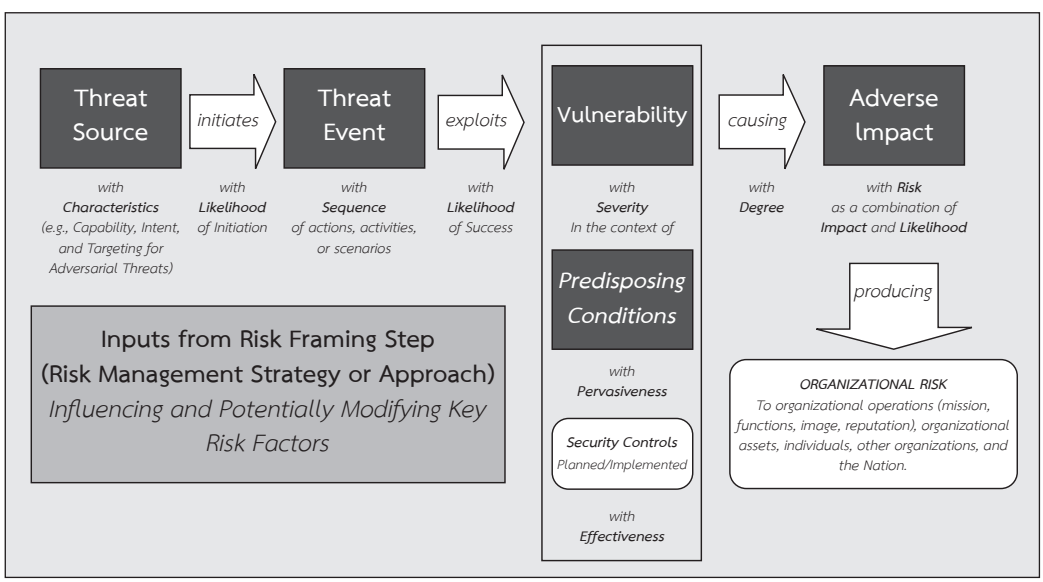
| ประเภทของภัยคุกคามทางไซเบอร์ | | | |
|---|---|---|---|
| **ธรรมชาติ** | **สภาพแวดล้อม** | **ภัยคุกคามที่มาจากมนุษย์** | |
| | | **การโจมตีแบบตั้งใจ** | **การโจมตีแบบไม่ตั้งใจ** |
| - น้ำท่วม<br>- แผ่นดินไหว<br>- พายุฟ้าคะนอง<br>- การพังทลายของอาคารพื้นที่ | - ระบบไฟฟ้าขัดข้อง<br>- อุณหภูมิไม่เหมาะสม<br>- ความชื้นจากเครื่องปรับอากาศ<br>- พื้นที่ก่อสร้างโครงสร้างพื้นฐาน | - อาชญากรรมคอมพิวเตอร์<br>- ผู้ก่อการร้ายทางไซเบอร์<br>- การจารกรรมทางไซเบอร์ | - เจ้าหน้าที่ภายในหน่วยงานที่ขาดความรู้ในการปฏิบัติงาน<br>- เจ้าหน้าที่ภายในหน่วยงานขาดความตระหนักรู้ |

**ตารางที่ 3** แนวทางการวิเคราะห์ช่องโหว่ของระบบสารสนเทศภายในองค์กร

| **แนวทางการวิเคราะห์ช่องโหว่ของระบบสารสนเทศขององค์กร** | |
|---|---|
| **การวิเคราะห์ช่องโหว่จากหลักฐานที่เป็นเอกสารหรือรายงาน** | **การทดสอบความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร** |
| - เอกสารรายงานการประเมินความเสี่ยงในห้วงที่ผ่านมา<br>- รายงานการตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ในห้วงที่ผ่านมา<br>- เอกสารความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ เช่น มาตรฐาน นโยบาย ข้อบังคับ กรอบแนวคิดที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ | - การใช้เครื่องมือสแกนหาช่องโหว่แบบอัตโนมัติ (Vulnerability Scanning Tools)<br>เช่น Acunetix, Burpsuite, Nessus, Nexpose, Nikto<br>- การใช้ระเบียบวิธีการทดสอบความมั่นคงปลอดภัยระบบ (Security Testing Methodology)<br>เช่น Black Box Testing, White Box Testing หรือกรอบแนวคิดอื่น ๆ ตามบริบทของหน่วยงาน<br>- การทดสอบเจาะระบบสารสนเทศขององค์กร (Penetration Testing) |

**2.3 การวิเคราะห์ความสัมพันธ์ของภัยคุกคาม รูปแบบการโจมตี และช่องโหว่**

หลังจากที่ได้ข้อมูลของภัยคุกคาม และช่องโหว่มาได้แล้ว ผู้ประเมินความเสี่ยงจะสามารถวิเคราะห์ได้ว่า รูปแบบการโจมตีที่เกิดขึ้นจากภัยคุกคามดังกล่าวโจมตีผ่านช่องโหว่ใดของระบบสารสนเทศในองค์กร และส่งผลกระทบ หรือความเสียหายมากน้อยเพียงใดกับระบบสารสนเทศที่ถูกโจมตี รายละเอียดดังภาพที่ 3 ความสัมพันธ์ของภัยคุกคาม รูปแบบการโจมตี และช่องโหว่ สามารถสรุปความสัมพันธ์ได้ว่าภัยคุกคามจะสร้างรูปแบบการโจมตี และโจมตีผ่านช่องโหว่ ทั้งนี้ ถ้าในกรณีที่เป็นช่องโหว่ร้ายแรง หรือมาตรการควบคุมปัจจุบัน (Security Controls) ไม่เพียงพอ ผลกระทบที่เกิดขึ้นจากภัยคุกคามก็จะมีความรุนแรงมากขึ้นตามไปด้วย




**ภาพที่ 3** ความสัมพันธ์ของภัยคุกคาม รูปแบบการโจมตี และช่องโหว่
**ที่มา:** Gallagher, 2012

**2.4 การพิจารณาโอกาสเกิดขึ้นของภัยคุกคาม (Likelihood Determination)**

โอกาสที่จะเกิดในทางไซเบอร์จะพิจารณาจากค่าความน่าจะเป็นที่ภัยคุกคามกระทำต่อช่องโหว่ตามสภาพแวดล้อม โดยพิจารณาจากแหล่งที่มาและขีดความสามารถของภัยคุกคาม ช่องโหว่ที่เกิดขึ้นภายในองค์กร และมาตรการควบคุมในปัจจุบัน

**2.5 วิเคราะห์ผลกระทบ (Impact Analysis)**

กระบวนการวิเคราะห์ผลกระทบ จัดทำขึ้นเพื่อกำหนดระดับความสำคัญของผลกระทบที่เกิดขึ้นกับสินทรัพย์ที่เป็นลักษณะข้อมูล หรือสารสนเทศขององค์กร (Information Assets) โดยจะพิจารณาจากหลักการประเมินผลแบบเชิงปริมาณ หรือเชิงคุณภาพ ตามบริบทของสินทรัพย์ที่ส่งผลกระทบต่อภารกิจหลักของหน่วย เช่น อุปกรณ์คอมพิวเตอร์ ระบบสารสนเทศ การให้บริการอินเทอร์เน็ต หรือสินทรัพย์อื่น ๆ ที่อยู่ภายใต้ขอบเขตของเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการสนับสนุนภารกิจหลักของหน่วยงาน ตามหลักพื้นฐานความมั่นคงปลอดภัยไซเบอร์เรื่อง ความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ทั้งนี้ การกำหนดนิยามโอกาสเกิดในทางไซเบอร์เชิงคุณภาพแบ่งออกเป็น 3 ระดับ ประกอบด้วย ต่ำ ปานกลาง และสูง ดังตารางที่ 4 และตารางที่ 5 ดังนี้

**ตารางที่ 4** ตัวอย่างการกำหนดนิยามโอกาสเกิดในทางไซเบอร์เชิงคุณภาพ

| ระดับของโอกาสเกิด | นิยามของโอกาสเกิด |
|---|---|
| **สูง** | ภัยคุกคามมีโอกาสเกิดขึ้นสูง และมาตรการควบคุมปัจจุบัน ไม่สามารถป้องกันภัยคุกคามที่เกิดขึ้นกับช่องโหว่ดังกล่าวได้ |
| **ปานกลาง** | ภัยคุกคามมีโอกาสเกิดขึ้น แต่มาตรการควบคุมปัจจุบัน สามารถป้องกันภัยคุกคามที่เกิดขึ้นกับช่องโหว่ดังกล่าวได้บางส่วน |
| **ต่ำ** | ภัยคุกคามมีโอกาสเกิดขึ้นต่ำ มีขีดความสามารถในการโจมตีผ่านช่องโหว่ต่ำ และมาตรการควบคุมปัจจุบัน สามารถป้องกันภัยคุกคามที่เกิดขึ้นกับช่องโหว่ดังกล่าวได้ |

**ที่มา:** Stoneburner, Goguen, and Feringa, 2002

**ตารางที่ 5** ตัวอย่างการกำหนดนิยามผลกระทบในทางไซเบอร์เชิงคุณภาพ

| ระดับของผลกระทบ | นิยามของผลกระทบ |
|---|---|
| **สูง** | ช่องโหว่ที่เกิดขึ้นส่งผลให้เกิดการสูญเสียงบประมาณจำนวนมากต่อสินทรัพย์ หรือทรัพยากรระบบสารสนเทศ จนส่งผลให้ภารกิจของหน่วยไม่สามารถปฏิบัติต่อไปได้ |
| **ปานกลาง** | ช่องโหว่ที่เกิดขึ้นส่งผลให้เกิดการสูญเสียงบประมาณจำนวนมากต่อสินทรัพย์ หรือทรัพยากรระบบสารสนเทศ จนส่งผลกระทบต่อภารกิจหลักของหน่วย และทำให้เกิดความล่าช้า |
| **ต่ำ** | ช่องโหว่ที่เกิดขึ้นส่งผลให้เกิดการสูญเสียงบประมาณบางส่วนต่อสินทรัพย์หรือทรัพยากรระบบสารสนเทศ โดยส่งผลกระทบต่อภารกิจรองของหน่วย และทำให้เกิดความล่าช้า |

**ที่มา:** Stoneburner, Goguen, and Feringa, 2002

**3. การพิจารณาระดับความเสี่ยง (Risk Determination)**

การพิจารณาระดับของความเสี่ยงที่เกิดขึ้นกับความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร มีประเด็นสำคัญที่ต้องพิจารณาร่วมด้วย ดังนี้

3.1 โอกาสเกิดภัยคุกคาม (Likelihood) ที่ส่งผลกระทบต่อช่องโหว่ขององค์กร

3.2 ความรุนแรงที่เกิดขึ้นของภัยคุกคาม (Impact) ที่เกิดขึ้นต่อช่องโหว่ขององค์กร

3.3 แผน หรือมาตรการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ที่ช่วยลด หรือขจัดความเสี่ยงที่เกิดขึ้นให้อยู่ในเกณฑ์ที่ยอมรับได้

ทั้งนี้ การพิจารณาระดับความเสี่ยง (Risk Level) ผู้ประเมินจะต้องให้ค่าคะแนนเทียบกับคำอธิบาย หรือนิยามระดับความเสี่ยงที่ได้มีการกำหนดขึ้น ตัวอย่างดังตารางที่ 6 และมาตรวัดระดับความเสี่ยง ดังตารางที่ 7 โดยการให้ค่าคะแนนจะประเมินจากโอกาสเกิดภัยคุกคาม (Likelihood) และความรุนแรงที่เกิดขึ้น (Impact) ในระดับสูง ปานกลาง และต่ำ ตามเกณฑ์ของกรอบแนวคิด NIST ที่ได้กำหนดไว้ดังนี้

1. ความน่าจะเป็นของโอกาสเกิดภัยคุกคามในระดับสูงที่ 1.0 คะแนน ระดับปานกลางที่ 0.5 คะแนน และระดับต่ำที่ 0.1 คะแนน

2. ระดับความรุนแรงของภัยคุกคามในระดับสูงที่ 1.0 คะแนน ระดับปานกลางที่ 0.5 คะแนน และระดับต่ำที่ 0.1 คะแนน

**ตารางที่ 6** ตัวอย่างคำอธิบายระดับความเสี่ยงและแนวทางการรับมือ (Description of Risk Level)

| ระดับความเสี่ยง | คำอธิบายระดับความเสี่ยงและแนวทางปฏิบัติ |
|---|---|
| **สูง** | ในกรณีที่ตรวจพบว่าความเสี่ยงอยู่ในระดับสูง ต้องมีการวางมาตรการควบคุมอย่างเข้มงวด เมื่อเกิดความเสี่ยงขึ้นระบบสารสนเทศต้องสามารถดำเนินต่อไปได้ และต้องมีการบังคับใช้ Corrective Action Plan ตามขีดความสามารถที่สามารถดำเนินการได้สูงสุด ณ ช่วงเวลาขณะนั้น |
| **ปานกลาง** | ในกรณีที่ตรวจพบว่าความเสี่ยงอยู่ในระดับปานกลาง ต้องมีการจัดทำ Corrective Action Plan เพื่อนำมาตรการต่าง ๆ เข้ามาใช้รับมือสถานการณ์ที่เกิดขึ้นอย่างเหมาะสม |
| **ต่ำ** | ในกรณีตรวจพบว่า ความเสี่ยงอยู่ในระดับต่ำ ให้พิจารณาว่าต้องมีการบังคับใช้มาตรการตาม Corrective Action Plan หรือไม่ และความเสี่ยงดังกล่าวอยู่ในเกณฑ์ที่สามารถยอมรับได้ หรือไม่ |

**ที่มา:** Gallgher, 2012

**ตารางที่ 7** มาตรวัดระดับความเสี่ยง (Risk Matrix)

| โอกาสเกิด (Likelihood) | ผลกระทบ (Impacts) | | |
|---|---|---|---|
| | ต่ำ (10) | กลาง (50) | สูง (100) |
| สูง (1.0) | ต่ำ<br>10 x 1.0 = 10 | ปานกลาง<br>50 x 1.0 = 50 | สูง<br>100 x 1.0 = 100 |
| ปานกลาง (0.5) | ต่ำ<br>10 x 0.5 = 5 | ปานกลาง<br>50 x 0.5 = 25 | ปานกลาง<br>100 x 0.5 = 50 |
| ต่ำ (0.1) | ต่ำ<br>10 x 0.1 = 1 | ต่ำ<br>50 x 0.1 = 5 | ต่ำ<br>100 x 0.1 = 10 |

**ที่มา:** Stoneburner, Goguen, and Feringa, 2002

**4. การกำหนดมาตรการควบคุม (Define Security Controls with Effectiveness)**

ขั้นตอนนี้จะมุ่งเน้นไปที่การกำหนดมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยงที่เกิดขึ้นต่อองค์กร ซึ่งตามกรอบแนวคิดของ NIST แนวทางการบริหารความเสี่ยงของ Antonucci (2017) และงานวิจัยของ ปานชนก สุขเจริญ (2554) ได้มีการอธิบายแนวทางในการกำหนดมาตรการควบคุมเพื่อให้สอดคล้องกับบริบทขององค์กรไว้ด้วยกัน 5 ขั้นตอน รายละเอียดตามหัวข้อที่ 4.1-4.5 แต่ทั้งนี้เพื่อเป็นการสร้างความเข้าใจในการเลือกใช้มาตรการควบคุม ผู้เขียนบทความจึงได้ทำการศึกษาค้นคว้าแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมจากงานวิจัยของ จิตตกานต์ บุญศิริทิวัตถ์ และโกวิท รพีพิศาล (2560, น.61-91) เพื่อให้การยกตัวอย่างประกอบคำอธิบายมีความชัดเจนและเห็นภาพของการเลือกใช้มาตรการควบคุมในแต่ละประเภทมากยิ่งขึ้น

**4.1 การทดสอบความเสี่ยง (Risk Assumption)**

การทดสอบความเสี่ยงเป็นการยอมรับความเสี่ยงที่เกิดขึ้นกับระบบสารสนเทศ หรือทำการพิจารณาว่าความเสี่ยงดังกล่าว จะส่งผลกระทบมากน้อยเพียงใดต่อระบบสารสนเทศขององค์กร ถ้าในกรณีที่ส่งผลกระทบเพียงเล็กน้อย จะเลือกทำการยอมรับความเสี่ยง แต่ในกรณีที่ส่งผลกระทบต่อภารกิจหลักขององค์กร จะทำการกำหนดมาตรการควบคุมที่เหมาะสมต่อไป

**4.2 การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)**

การหลีกเลี่ยงความเสี่ยงเป็นการลดขั้นตอนการดำเนินงาน หรือกระบวนการเพื่อขจัดความเสี่ยงที่มีแนวโน้มเกิดขึ้นต่อระบบสารสนเทศของหน่วยงาน ไม่ให้เกิดความเสียหายขึ้น ยกตัวอย่างเช่น แผนกทดสอบเจาะระบบตรวจพบว่า ระบบบัญชีขององค์กรมีช่องโหว่ร้ายแรง และยังไม่สามารถทำการปิดช่องโหว่ดังกล่าวได้ในปัจจุบัน เพื่อไม่ให้ความเสี่ยงดังกล่าวเกิดขึ้นกับระบบสารสนเทศขององค์กร ผู้บริหารระดับสูงจึงมีนโยบายให้แผนกบัญชีขององค์กรใช้ Microsoft Excel ที่เป็นซอฟต์แวร์ลิขสิทธิ์ทำบัญชีเป็นการชั่วคราวจนกว่าจะสามารถปิดช่องโหว่ที่เกิดขึ้นกับระบบบัญชีได้

**4.3 การวางแผนลดความเสี่ยง (Risk Mitigation Plan)**

การวางแผนลดความเสี่ยง เป็นการพิจารณาจากลำดับความสำคัญของความเสี่ยงที่เกิดขึ้น และทำการวางมาตรการควบคุมให้เหมาะสมกับความเสี่ยงดังกล่าว แต่ทั้งนี้ การกำหนดมาตรการควบคุมจะต้องพิจารณา

จากปัจจัยหลายอย่าง เช่น บริบทขององค์กร ผลกระทบและความเสียหายที่เกิดขึ้น งบประมาณ (Budget) ที่ใช้สำหรับการบริหารความเสี่ยง ผู้ที่มีส่วนเกี่ยวข้อง รวมถึงระดับผู้บริหารขององค์กรที่เป็นผู้อนุมัติให้ดำเนินการตอบสนองต่อความเสี่ยงที่เกิดขึ้น

**4.4 การศึกษาค้นคว้าวิจัยความเสี่ยงภายในองค์กร (Research and Acknowledgement)**

การศึกษาค้นคว้าวิจัยเป็นวิธีการลดความเสี่ยงโดยการยอมรับการมีอยู่ของช่องโหว่ หรือข้อบกพร่องที่เกิดขึ้นโดยหน่วยงานทำการค้นคว้าวิจัย เพื่อกำหนดมาตรการควบคุมที่เหมาะสมที่สุด ในการลดความเสียหาย ผลกระทบ โอกาสเกิด หรือขจัดช่องโหว่ที่เกิดขึ้น

**4.5 การถ่ายโอนความเสี่ยง (Risk Transference)**

การถ่ายโอนความเสี่ยงเป็นการกำหนดผู้รับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากหน่วยงานภายนอก และให้มีบทบาทในการจัดการความเสี่ยงแทนเจ้าของความเสี่ยง เช่น การซื้อประกันอุปกรณ์คอมพิวเตอร์ การทำประกันภัยพิบัติทางธรรมชาติ หรือการทำสัญญาในรูปแบบอื่น ๆ ที่เกี่ยวข้อง

**5. การรายงานผลการประเมินความเสี่ยง (Communicating and Sharing Risk Assessment Information)**

การรายงานผลการประเมินความเสี่ยงเป็นกระบวนการที่ใช้สำหรับสื่อสาร และอธิบายผลการประเมินความเสี่ยงที่ ณ ปัจจุบัน โดยมีวัตถุประสงค์เพื่อให้ผู้ที่มีส่วนเกี่ยวข้อง และระดับผู้บริหารใช้เป็นข้อมูลประกอบกับแนวทางในการตัดสินใจ เพื่อดำเนินการบริหารความเสี่ยงที่ส่งผลกระทบในระดับองค์กรได้อย่างเหมาะสม อีกทั้งยังช่วยให้พิจารณาเพิ่มเติมได้ว่าความเสี่ยงด้านระบบสารสนเทศนั้น ส่งผลต่อความเสี่ยง หรือภารกิจในด้านอื่น ๆ ขององค์กรอย่างไร

**6. การติดตามและเฝ้าระวังภายหลังจากประเมินความเสี่ยง (Maintain Risk Assessment)**

การติดตามและเฝ้าระวังภายหลังจากประเมินความเสี่ยง มีวัตถุประสงค์เพื่อติดตามความเสี่ยงที่มีแนวโน้มที่จะเกิดขึ้นสูง และส่งผลกระทบต่อกระบวนการ หรือภารกิจหลักขององค์กร (Core Business Function) ทั้งนี้ยังเป็นกระบวนการที่ใช้ติดตามผลของการวางมาตรการควบคุม (Security Controls) ว่ามาตรการควบคุมดังกล่าวมีส่วนช่วยลดผลกระทบ โอกาสเกิด และระดับความเสี่ยงขององค์กรหรือไม่ โดยกระบวนการนี้ผู้ประเมินควรมีการจัดทำเป็นบันทึก หรือรายงานประจำปีไว้ เนื่องจากรายงานดังกล่าวสามารถใช้เป็นข้อมูลในการอ้างอิงการประเมินความเสี่ยง และการกำหนดมาตรการควบคุมในวงรอบปีถัดไปได้ (Gallagher, 2010)

**ข้อเสนอแนะ**

องค์กรต้องเปลี่ยนแนวคิดจากการมุ่งเน้นมาตรการควบคุมไปที่การป้องกันเพียงอย่างเดียว เป็นการเตรียมความพร้อมเพื่อรับมือเหตุการณ์ไม่คาดคิด หรือเหตุการณ์ทางไซเบอร์ ตามแนวคิดของ Cyber Resilience เพราะว่าบนโลกนี้ไม่มีระบบ หรือเทคโนโลยี รวมถึงมาตรการควบคุมใด ๆ ที่สามารถป้องกันความเสี่ยงทางไซเบอร์ได้ทั้งหมด ทางองค์กรจึงจำเป็นต้องมีการนำหลักการดังกล่าวเข้ามาใช้ในการเตรียมรับมือกับภัยไซเบอร์ขององค์กรตั้งแต่วันนี้เป็นต้นไป เพื่อรับกับสภาวะที่กำลังจะเกิดขึ้นในปัจจุบันและอนาคต เนื่องจากในภายภาคหน้า ภัยไซเบอร์จะมีความรุนแรงในวงกว้างมากยิ่งขึ้น และยังจะส่งผลกระทบไปยังทุกภาคส่วน ตั้งแต่ระดับประเทศชาติ ระดับองค์กร ไปจนถึงระดับบุคคลอย่างหลีกเลี่ยงไม่ได้

**บทสรุป**

ภัยไซเบอร์ไม่ใช่เรื่องใหม่ แต่ในปัจจุบันมีความซับซ้อนมากยิ่งขึ้น อีกทั้งยังเป็นความเสี่ยงที่ส่งผลต่อภาพลักษณ์ และชื่อเสียงขององค์กร (Reputation Risk) ผู้บริหารระดับสูง และกรรมการบริหารองค์กรจำเป็นต้องให้ความสนใจ และให้ความสำคัญกับการป้องกัน เพื่อปกป้องชื่อเสียงขององค์กร ตลอดจนการรั่วไหลของข้อมูลที่มีชั้นความลับ ปัญหาต่าง ๆ อาจเกิดจากแฮ็กเกอร์ภายในองค์กรหรือจากพนักงานภายในองค์กร ก็ล้วนแต่มีความเป็นไปได้ทั้งสิ้น ดังนั้น การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงจำเป็นต้องมีการปรับปรุงวิธีการกระบวนการตลอดจนการยกระดับไปสู่การเชื่อมโยงและบูรณาการไปยังการบริหารความเสี่ยงระดับองค์กร (Gallagher, 2011) ซึ่งในบทความนี้ได้อธิบายถึงแนวทางการบริหารความเสี่ยง โดยอ้างอิงมาจากกรอบแนวคิด NIST ไว้ด้วยกัน 4 ขั้นตอน ประกอบด้วย ขั้นตอนเตรียมการ ขั้นตอนการประเมินความเสี่ยง ขั้นตอนการรายงานผลการประเมินความเสี่ยง และการติดตามและเฝ้าระวังภายหลังจากประเมินความเสี่ยง

จากผลการศึกษาค้นคว้าพบว่า การประเมินความเสี่ยงด้านไซเบอร์ถือว่าเป็นส่วนสำคัญในการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร เนื่องจากว่าองค์กรได้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้งานเพื่อสนับสนุนภารกิจขององค์กร ทั้งนี้การประเมินความเสี่ยงจะเป็นการพิจารณาการนำมาตรการควบคุมมาใช้อย่างเหมาะสมและสอดคล้องกับภารกิจขององค์กรเป็นสำคัญ เพื่อให้เกิดประสิทธิภาพสูงสุด สุดท้ายนี้จากการศึกษาค้นคว้างานวิจัยของ สุธาเทพ รุณเรศ (2561) และแนวทางการสร้างความตระหนักรู้ของ Willson (2016) ทำให้ผู้เขียนบทความได้ตระหนักว่ากลยุทธ์ที่ดีที่สุดไม่ใช่การลงทุนด้านเทคโนโลยีเพื่อใช้รับมือกับภัยคุกคามทางไซเบอร์ แต่เป็นสิ่งที่เรียกว่าการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรในองค์กรต่างหาก ที่เป็นกลยุทธ์ที่สามารถใช้รับมือภัยคุกคามดังกล่าวได้อย่างแท้จริง

## เอกสารอ้างอิง

จิตตกานต์ บุญศิริทิวัตถ์ และโกวิท รพีพิศาล. (2560). การพัฒนาแนวทางในการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร. *วารสารรังสิตสารสนเทศ, 23*(1), 61-91.

ปรัชญา เฉลิมวัฒน์. (2561). *แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ* (รายงานผลการวิจัย). กรุงเทพฯ: สถาบันวิชาการป้องกันประเทศ.

ปริญญา หอมเอนก. (2560). *Strategy to Cybersecurity 4.0* (พิมพ์ครั้งที่ 1). กรุงเทพฯ: บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด.

ปานชนก สุขเจริญ. (2554). *การบริหารความเสี่ยง และสร้างความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศขององค์กร กรณีศึกษาประเภทสถานศึกษาระดับพื้นฐาน* (สารนิพนธ์หลักสูตรวิทยาศาสตรมหาบัณฑิต). มหาวิทยาลัยเทคโนโลยีมหานคร. สืบค้นเมื่อ 23 กันยายน 2563, จาก http://gg.gg/mamad

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562” (2562, 27 พฤษภาคม) *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 39.

เศรษฐพงศ์ มะลิสุวรรณ. (2558). *แนวทางการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ*. สืบค้นเมื่อ 20 กรกฎาคม 2563, จาก http://www.rtna.ac.th/download/cyber/nationalcybersecurity.pdf

สุธาเทพ รุณเรศ. (2561). *ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร* (การค้นคว้าอิสระหลักสูตรวิทยาศาสตรมหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์. สืบค้นเมื่อ 23 กันยายน 2563, จาก http://ethesisarchive.library.tu.ac.th/thesis/2018/TU_2018_5923036155_7502_9460.pdf

อรรคเดช ประทีปอุษานนท์ และธาราทิพย์ กัลยาณมิตร. (2560). แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์. *วารสารสถาบันวิชาการป้องกันประเทศ, 8*(3), 11-23.

อุดม ประตาทะยัง. (2561). *แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์* (รายงานผลการวิจัย). กรุงเทพฯ: สถาบันวิชาการป้องกันประเทศ.

Antonucci, D. (2017). *The Cyber Risk Handbook*. Hoboken: John Wiley & Sons, lnc.,.

Black, P.E., Fong, E., Okun, V., and Gaucher, R. (2018). Software Assurance Tools: Web Application Security Scanner Functional Specification Version 1.0. *NIST Special Publication 500-269*. January.

Bodeau, D. and Graubart, R., (2017). *Cyber Resiliency Design Principles*. January.

Coat, B. (2559). *Shadow IT/Data ภัยคุกคามเบื้องหลังของการใช้ Cloud Applications*. สืบค้นเมื่อ 20 กรกฎาคม พ.ศ.2563, จาก https://www.techtalkthai.com/what-is-shadow-it-and-shadowdata/

Gallagher, P.D. (2010). Guide for Applying the Risk Management Framework for Federal Systems. A Security Life Cycle Approach. *NIST Special Publication 800-37*. February.

_____. (2011). Managing Information Security Risk, Organization Mission and Information System View. *NIST Special Publication 800-39*. March.

_____. (2012). Guide for Conducting Risk Assessments. *NIST Special Publication 800-30 R1*. September.

_____. (2013). R4 Security and Privacy Controls for Federal Information Systems and Organization. *NIST Special Publication 800-53*. April.

International Organization for Standardization [ISO]. (2009). *ISO 31000:2009 Risk Management Principles and Guidelines*. November.

Moeller, R.R. (2010). *IT Audit, Control and Security*. Hoboken: John Wiley & Sons, lnc.,.

National Institute of Standards and Technology [NIST]. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. April. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Project Management Institute. (2017). *Project Management Body of Knowledge (PMBOK)* (6th ed.). Pennsylvania: Project Management Institute.

Stoneburner, G., Goguen, A. and Feringa, A. (2002). Guide for Information Technology Systems. *NIST Special Publication 800-30 Risk Management*. July.

THE WHITE HOUSE Office of the Press Secretary. (2013). *President Policy Practice: Critical Infrastructure Security and Resilience (PPD-21)*. February. Retrieved from https://fas.org/irp/offdocs/ppd/ppd-21.pdf

Willson, D. (2016). *Cyber Security Awareness for CEOs and Management*. USA: Sygresss.

## ภาคผนวก (Appendix)

### ตัวอย่างแนวทางการบริหารความเสี่ยงเบื้องต้น โดยใช้กรอบแนวคิด NIST Framework

| เหตุการณ์ | จากภัยคุกคาม | ช่องโหว่ที่ตรวจพบ | มาตรการในปัจจุบัน | โอกาสเกิด | ผลกระทบ | ความเสี่ยง | ข้อเสนอแนะ |
|---|---|---|---|---|---|---|---|
| เครื่องคอมพิวเตอร์ติดมัลแวร์ประกอบไปด้วย<br>- Trojan<br>- Generic Crack,<br>- Exploit<br>- Hack Tools | แฮ็กเกอร์ (Hacker) | **<u>ช่องโหว่ด้านกระบวนการ</u>**<br>- ขาดกระบวนการทำ Change Management<br><br>- ไม่มีการจัดฝึกอบรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Awareness Training)<br><br>- หน่วยไม่มีการบังคับใช้มาตรการควบคุมในการดาวน์โหลดข้อมูลจากเครือข่ายอินเทอร์เน็ต<br><br>- ซอฟท์แวร์ที่มีการใช้งาน เพื่อปฏิบัติภารกิจในปัจจุบัน มิได้มีการระบุอยู่ในบัญชี รายการทรัพย์สินซอฟต์แวร์ของหน่วยงาน (Undocumented Software)<br><br>- ซอฟต์แวร์ละเมิดลิขสิทธิ์<br><br>- ขาดนโยบายการใช้อุปกรณ์พกพา (Removable Media) | - มี Antivirus Mcafee Endpoint Security ติดตั้งอยู่ที่เครื่องลูกข่าย<br><br>- มี Site Recovery อยู่ที่ Anywhere โดยตั้งระยะเวลาไว้ทุก 4 ชม. ในกรณีที่ Data Center หลักมีปัญหาสามารถเรียกใช้ได้ทันที<br><br>- มีการเข้ารหัสข้อมูลด้วย HASH Function ประเภท MD 5<br><br>- กำหนดให้ผู้ใช้งานระบบสารสนเทศขององค์กรจะต้องมีการยืนยันตัวตนก่อนใช้งานระบบดังกล่าว | **ปานกลาง (0.5)** | **ปานกลาง (50)** | **ปานกลาง (25)** | - ปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับภัยคุกคามที่เกิดขึ้นในปัจจุบัน<br><br>- จัดทำแนวทางปฏิบัติในการติดตั้ง/ใช้งานระบบปฏิบัติการ โปรแกรมประยุกต์ และโปรแกรมป้องกันมัลแวร์<br><br>- จัดทำแนวปฏิบัติทะเบียนสินทรัพย์สารสนเทศ โดยกำหนดให้บันทึกรายละเอียดจนถึงระดับเวอร์ชัน หรือเฟิร์มแวร์ที่ใช้<br><br>- จัดให้มีการทบทวนสิทธิ์ (Account Review) และเพิกถอนสิทธิ์ ทั้งในส่วนของผู้ใช้ทั่วไป และผู้ที่มีสิทธิ์สูงอย่างเหมาะสม |
| เครื่องคอมพิวเตอร์ติดมัลแวร์ ประกอบด้วย<br>- Botnet<br>- Hack Tools<br>- Adware<br>- Trojan | อาชญากรทางไซเบอร์ (Cyber Criminal) | | | **ต่ำ (0.1)** | **ปานกลาง (50)** | **ต่ำ (5)** | |
| เครื่องคอมพิวเตอร์ติดมัลแวร์ ประกอบไปด้วย<br>- Wannacry<br>- Ransomware | แฮ็กเกอร์ที่สนับสนุนโดยรัฐ (Stated-Sponsored Hacker) | | | **ปานกลาง (0.5)** | **สูง (100)** | **ปานกลาง (50)** | |