รายงานผลการศึกษาการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี พ.ศ. 2568

THAILAND NATIONAL CYBER RISK ASSESSMENT REPORT 2025





สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)



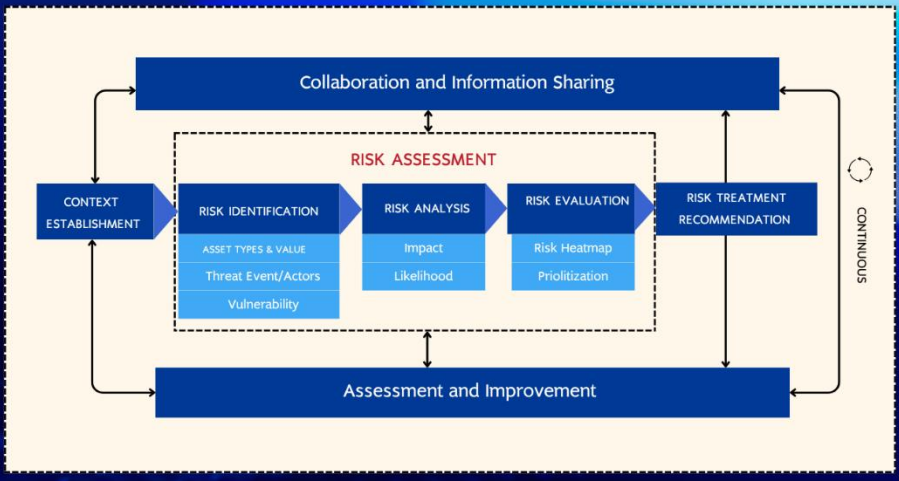
ชื่อเรื่อง รายงานผลการศึกษาการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี พ.ศ. 2568

จัดทำโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี 2568

TH-NCRAF

(Thailand National Cyber Risk Assessment Framework 2025)



สารบัญ
TABLE OF CONTENT

ภาษาไทย

บทสรุปผู้บริหาร 1

บทนำ 7

กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของระเทศไทย 9

รายงานผลการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย พ.ศ. 2568 32

ข้อเสนอแนะเชิงนโยบายเพื่อการบริหารความเสี่ยง (Risk Mitigation) 55

บทสรุปและทิศทางในอนาคต 61

ENGLISH

Executive Summary 67

Introduction 70

Thailand National Cyber Risk Assessment Framework 75

Thailand National Cyber Risk Assessment Report 2025 98

Policy Recommendations for Risk Mitigation 122

Conclusion and Future Directions 128



บทสรุปผู้บริหาร

บทสรุปผู้บริหาร

การประเมินความเสี่ยงทางไซเบอร์ระดับประเทศในปีงบประมาณ พ.ศ. 2568 จัดทำขึ้นภายใต้กรอบการประเมิน Thailand National Cyber Risk Assessment Framework (NCRAF) โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อวิเคราะห์สถานการณ์ภัยคุกคามที่ส่งผลต่อความมั่นคงปลอดภัยไซเบอร์ของประเทศ ตลอดจนเป็นข้อมูลสนับสนุนการกำหนดนโยบาย และมาตรการเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นระบบ

ผลการประเมินในภาพรวมสะท้อนให้เห็นว่า ประเทศไทยมีระดับความเสี่ยงทางไซเบอร์โดยมีความเสี่ยงสูงสุด 5 อันดับแรก ได้แก่

1. ผู้ประสงค์ร้ายจากภายนอกใช้ช่องโหว่จากซอฟต์แวร์เพื่อเข้าถึงสินทรัพย์หมวดจัดการสารสนเทศและเทคโนโลยีโดยไม่ได้รับอนุญาต
2. ผู้ประสงค์ร้ายจากภายนอกและกลุ่มผู้ประสงค์ร้ายที่รวมกลุ่มเฉพาะกิจใช้ช่องโหว่จากซอฟต์แวร์เพื่อโจมตีสินทรัพย์หมวดจัดการสารสนเทศและเทคโนโลยีด้วยโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) ที่มุ่งเป้าไปยังเป้าหมายเฉพาะ
3. ผู้ประสงค์ร้ายจากภายนอกและกลุ่มผู้ประสงค์ร้ายที่รวมกลุ่มเฉพาะกิจใช้ช่องโหว่จากซอฟต์แวร์เพื่อโจมตีสินทรัพย์หมวดจัดการสารสนเทศและเทคโนโลยีด้วยโจมตีแบบปฏิเสธการให้บริการที่ไม่ระบุเป้าหมายเฉพาะ (Simple Denial of Service: DoS)
4. ผู้ประสงค์ร้ายจากภายนอกใช้ช่องโหว่จากซอฟต์แวร์ฝังมัลแวร์เฉพาะทางลงในระบบสารสนเทศขององค์กรในหมวดข้อมูลทั่วไปของรัฐบาล เช่น Ransomware ชนิดพิเศษที่หลบเลี่ยงการตรวจจับ เป็นต้น
5. ผู้ประสงค์ร้ายจากภายนอกใช้ประโยชน์จากซอฟต์แวร์ที่ถูกค้นพบไม่นาน (Recently Discovered Vulnerabilities) เพื่อโจมตีสินทรัพย์หมวดจัดการสารสนเทศและเทคโนโลยี

จากผลการประเมิน สกมช. ได้เสนอแนวทางเชิงนโยบายเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ประกอบด้วย

1. การยกระดับความสามารถตรวจจับและตอบสนองภัยทางไซเบอร์ (Cyber Resilience) ให้ครอบคลุมทุกภาคส่วน
2. การยกระดับความสามารถตรวจจับและตอบสนองภัยทางไซเบอร์ (Cyber Resilience) ให้ครอบคลุมทุกภาคส่วน
3. การจัดตั้งกลไกการประเมินความเสี่ยงฯ ระดับชาติเป็นประจำทุกปี (National Cyber Risk Review Continues)
4. จัดทำระบบการพัฒนาแรงงานดิจิทัลด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Workforce Development System)
5. การสร้างความร่วมมือระหว่างภาครัฐ ภาคเอกชน และพันธมิตรระหว่างประเทศเพื่อแลกเปลี่ยนข้อมูลภัยคุกคาม

ผลการประเมินความมั่นคงปลอดภัยไซเบอร์ประจำปี 2568 ของประเทศไทยยังพบช่องว่างด้านการบริหารจัดการความเสี่ยงและความพร้อมรับมือ โดยเฉพาะในกลุ่มหน่วยงานภาครัฐที่มีคะแนนความพร้อมลดลงขณะที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล มีแนวโน้มพัฒนาและปรับปรุงดีขึ้น การเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไม่ใช่เรื่องที่ดำเนินการเพียงครั้งเดียว แต่ต้องมีการปรับปรุงอย่างต่อเนื่องและเป็นระบบ เพื่อรองรับภัยคุกคามที่มีความซับซ้อนและเกิดขึ้นมากขึ้นในทุกภาคส่วน

ดังนั้น การประเมินครั้งนี้จึงสะท้อนให้เห็นถึงความจำเป็นในการยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างต่อเนื่องเพื่อให้ประเทศไทยมีความพร้อมในการป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามไซเบอร์ได้อย่างมั่นคงและยั่งยืน

1. บทนำ



บทนำ

1.1 แนวโน้มสถานการณ์และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ : ภาพรวมโลกและประเทศไทย

ภาพรวมภัยคุกคาม Cyber Attack ทั่วโลกในปี 2025



ความเสียหายทางเศรษฐกิจจากอาชญากรรมไซเบอร์

คาดการณ์ว่าความเสียหายทางเศรษฐกิจจากอาชญากรรมไซเบอร์ทั่วโลกจะสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐต่อปี ภายในปี 2025 ซึ่งเพิ่มขึ้นจาก 3 ล้านล้านดอลลาร์ในปี 2015 และเติบโตเฉลี่ยปีละ 15%



การโจมตีแบบไม่ใช้มัลแวร์ (Malware-Free Attacks)

รายงานจาก CrowdStrike ระบุว่า 79% ของการตรวจจับภัยคุกคามในปี 2024 เป็นการโจมตีที่ไม่ใช้มัลแวร์ ซึ่งหมายความว่าแฮกเกอร์ใช้เทคนิคอื่นๆ เช่น การโจมตีผ่านบัญชีผู้ใช้ที่ถูกขโมย หรือการใช้เครื่องมือที่ถูกต้องในการเข้าถึงระบบ



การใช้ AI ในการโจมตี

แฮกเกอร์เริ่มนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในการโจมตี เช่น การสร้างอีเมลฟิชชิ่งที่เหมือนจริงมากขึ้น การสร้างเว็บไซต์ปลอม และการวิเคราะห์ช่องโหว่ของระบบอย่างรวดเร็ว

CYBER THREAT LANDSCAPE 2025

แหล่งที่มา Global Cybersecurity Outlook 2025, World Economic Forum

Geopolitical Tensions



ความขัดแย้งหรือความไม่ลงรอยทางการเมือง

เกือบ 60% ขององค์กรปรับแผนไซเบอร์เพราะแรงกดดันด้านภูมิรัฐศาสตร์ ที่น่ากังวลเป็นพิเศษ คือ การจารกรรมไซเบอร์ และการสูญเสียข้อมูลสำคัญ/IP ซึ่งสะท้อนว่า Cybersecurity ไม่ใช่แค่ “IT issue” แต่เป็น Strategic Business Issue

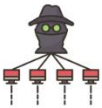
Cybercrime Sophistication



ความซับซ้อนของอาชญากรรมไซเบอร์

- การฉ้อโกงที่ใช้เทคโนโลยีไซเบอร์ (cyber-enabled fraud) มีแนวโน้มเพิ่มขึ้น
- การโจมตีแบบ phishing และ social engineering มีจำนวนมากขึ้น
- การขโมยข้อมูลส่วนบุคคล (identity theft) กลายเป็นความเสี่ยงไซเบอร์ส่วนบุคคลอันดับต้น ๆ

Supply Chain Interdependencies



การพึ่งพาอาศัยกันในห่วงโซ่อุปทาน

ความเชื่อมโยงที่ทำให้การโจมตีหรือความผิดพลาดเล็ก ๆ ในจุดหนึ่ง สามารถ “ลาม” ไปสู่ทั้งเครือข่ายธุรกิจได้

Regulatory Requirements



ข้อบังคับตามกฎหมาย/ระเบียบ

ความซับซ้อนและกฎระเบียบที่มากเกินไป คือความท้าทายใหญ่ และกลายเป็นช่องโหว่ให้เกิดการจู่โจมได้ ด้วยเพราะเกิดความสับสนจนทำให้ละเลยการทำตามกฎระเบียบ หรือความซับซ้อนยุ่งยาก จนไม่สามารถปฏิบัติตามได้หมด

AI and emerging tech



ปัญญาประดิษฐ์และเทคโนโลยีสมัยใหม่

องค์กรส่วนใหญ่ตระหนักว่า AI กำลังจะเข้ามาเปลี่ยนโฉมการโจมตีและการป้องกันไซเบอร์ แต่ยังขาดกรอบการทำงานและมาตรการกำกับดูแล

Cyber skills gap



ช่องว่างด้านทักษะไซเบอร์

ความต้องการบุคลากรไซเบอร์สูงกว่าปริมาณและคุณภาพที่มีอยู่จริง ซึ่งองค์กรส่วนใหญ่กำลังเผชิญ ความเสี่ยงเชิงโครงสร้าง หากไม่เร่งอัพสกิลหรือรีสกิลบุคลากร



สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย พ.ศ. 2568



หน่วยงานรัฐและหน่วยงานการศึกษาเป็นเป้าหมายหลักที่ถูกโจมตีในปี 2567 โดยมีรายงานเหตุการณ์ที่ได้รับการบันทึกไว้กว่า 3,100 เหตุการณ์ เหตุการณ์ภัยคุกคามอันดับต้น ๆ คือ "บัญชี/รหัสผ่านรั่วไหล" และเทคนิคการโจมตีหลัก คือ "การสร้างเว็บปลอม"



มีการบังคับใช้ระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication, MFA) ให้เป็นมาตรฐานสำหรับหน่วยงานของรัฐ เพื่อเสริมความปลอดภัย



องค์กรในประเทศไทยตกอยู่ในความเสี่ยงสูงจากการใช้ระบบที่ล้าสมัย (legacy systems) และความซับซ้อนทางเทคโนโลยีสูง ซึ่งอาจเป็นจุดอ่อนที่ผู้ไม่ประสงค์ดีใช้เจาะเข้าสู่ระบบได้



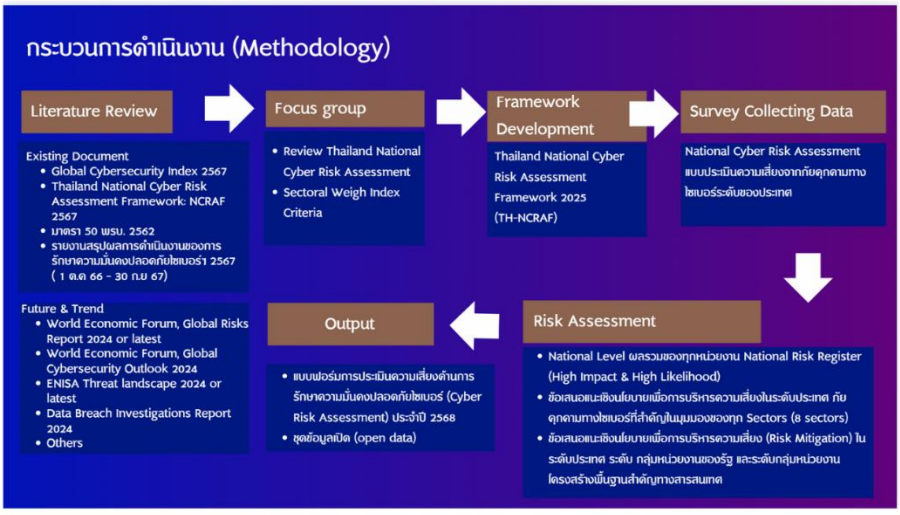
แนวโน้มการโจมตี “ห่วงโซ่อุปทาน” (Supply Chain attack) หรือการใช้ช่องโหว่ของระบบพันธมิตร ผู้ให้บริการ หรือระบบภายนอกมาเป็นจุดผ่าน (pivot) เพื่อเข้าสู่ระบบหลักขององค์กร กำลังเป็นภัยที่น่ากังวล



ระหว่างเดือนมกราคม – พฤษภาคม พ.ศ. 2568 มีรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์รวมทั้งสิ้น 1,002 เหตุการณ์ โดยลักษณะเด่นคือ การโจมตีแบบ credential stuffing, DDoS, ransomware และการรั่วไหลของข้อมูล จากปัจจัยที่เพิ่มขึ้นเมื่อผู้ประสงค์ร้ายใช้โครงสร้างพื้นฐานบนคลาวด์ และการใช้งาน AI ในรูปแบบการโจมตี

1.2 โครงสร้างกิจกรรมการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินการจัดกิจกรรมประเมินความเสี่ยงต่อภัยคุกคามทางไซเบอร์ เพื่อวิเคราะห์ประเมินความเสี่ยงด้าน ภัยคุกคามทางไซเบอร์ในภาพรวมระดับประเทศและระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจัดทำเป็นโครงการต่อเนื่องเป็นประจำทุกปีเพื่อให้สามารถทราบถึงระดับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา และเป็นไปตามแนวปฏิบัติด้านการประเมินความเสี่ยงทางไซเบอร์ตามมาตรฐานสากล ซึ่งกำหนดให้มีการประเมินความเสี่ยงทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง อีกทั้งยังสอดคล้องกับมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งกำหนดให้มีการทบทวนความเสี่ยงหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นประจำทุกปีเช่นเดียวกัน อันเป็นข้อมูลพื้นฐานนำไปสู่การวางแผนในการป้องกัน รับมือ และลดความเสี่ยงต่อภัยคุกคามทางไซเบอร์สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนด



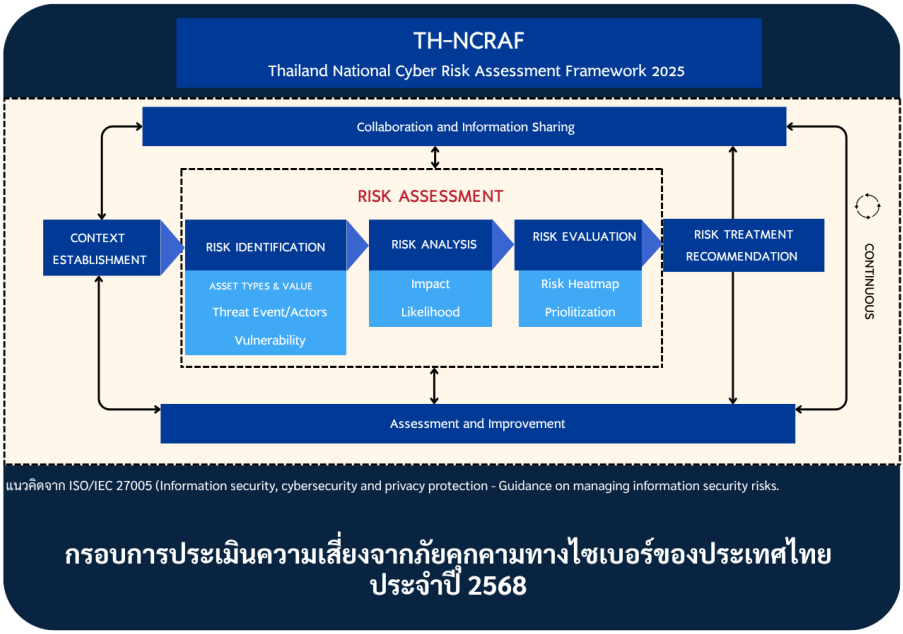
ภาพรวมการดำเนินงานโครงการ

2. กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย



กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย

กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทยประจำปี 2568 มีวัตถุประสงค์เพื่อใช้เป็นเครื่องมือในการประเมินความเสี่ยงระดับภาพรวมของประเทศโดยเป็นแนวทางให้หน่วยงานใช้ในการประเมินความเสี่ยงขององค์กรและสามารถนำผลลัพธ์จากการประเมินมาเป็นข้อมูลเทียบในระดับประเทศ (benchmark) เพื่อให้หน่วยงานได้ทราบถึงสถานะความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในระดับประเทศ อีกทั้งยังช่วยลดความซ้ำซ้อนและสร้างมาตรฐานของการรายงานข้อมูลตามมาตรา 54 แห่งพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งกำหนดให้มีการทบทวนความเสี่ยงหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นประจำทุกปี



หมายเหตุ กรอบการประเมินความเสี่ยงฯ ปรับปรุงจากกิจกรรมกิจกรรมประชุมรับฟังความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง (Focus Group) (ร่าง) กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ณ วันที่ 16 พฤษภาคม 2568

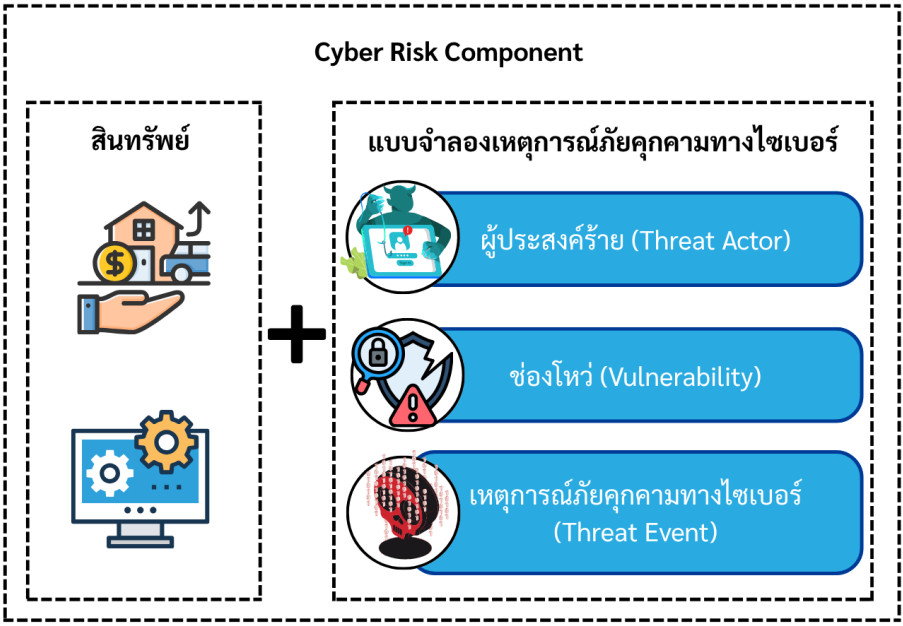
2.1 การระบุบริบทหน่วยงาน (Context Establishment)

การระบุบริบทของหน่วยงานเป็นข้อมูลสำคัญที่ระบุถึงความสำคัญของหน่วยงาน ผู้จัดทำรายงานการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์เพื่อสะท้อนถึงบทบาทสำคัญที่หน่วยงานและหน้าที่ของหน่วยงานนั้นต่อภาพรวมของประเทศซึ่งมีรายละเอียดที่ต้องระบุตามกรอบ ประกอบด้วย

ชื่อหน่วยงาน	
ประเภทหน่วยงาน	หน่วยงานควบคุมหรือกำกับดูแล
	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
	หน่วยงานของรัฐ (ที่ไม่ใช่ CII)
หมวดภารกิจ	1. ด้านความมั่นคงของรัฐ
	2. ด้านบริการภาครัฐที่สำคัญ
	3. ด้านการเงินและการธนาคาร
	4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
	5. ด้านการขนส่งและโลจิสติกส์
	6. ด้านพลังงานและสาธารณูปโภค
	7. ด้านสาธารณสุข
	8. หน่วยงานของรัฐ (ที่ไม่ใช่ CII)
ลักษณะของหน่วยงาน	อ้างอิงรายละเอียดจาก “ประกาศ กมช. เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจ หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564”
ภารกิจที่ให้บริการ	

2.2 การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยงภัยคุกคามทางไซเบอร์ ทำการพิจารณาเหตุการณ์ภัยคุกคามที่มีผู้ประสงค์ร้าย (Adversarial Threat) ที่อาจเกิดขึ้นกับองค์กร - ประเทศ ซึ่งมีองค์ประกอบความเสี่ยง แบ่งเป็น 2 ส่วน ได้แก่ สินทรัพย์องค์กร (Asset) และ แบบจำลองเหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Modeling) ซึ่งมีโครงสร้างดังภาพ



ในแต่ละปีหน่วยงานจะมีการจัดทำรายงานประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์และรายงานต่อ สกมช. ตามมาตรา 54 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งข้อมูลดังกล่าวได้ถูกรวบรวมและเรียบเรียงตามกรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยนำเข้าเฉพาะข้อมูล ที่ครบถ้วนตามองค์ประกอบของกรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ฯ ของประเทศไทย ประจำปี พ.ศ. 2568 เท่านั้น

การพิจารณาคุณภาพของข้อมูลที่หน่วยงานจัดทำขึ้น โดยต้องมีองค์ประกอบอย่างต่ำ ประกอบด้วย

- ✓ ชื่อสินทรัพย์/ประเภทสินทรัพย์
- ✓ ช่องโหว่ (Vulnerability)
- ✓ ผู้ประสงค์ร้าย/ผู้คุกคาม
- ✓ เหตุการณ์ภัยคุกคาม (Threat Event)
- ✓ การวิเคราะห์ระดับผลกระทบ - โอกาส และความเสี่ยง

เมื่อพิจารณาความครบถ้วน จึงระบุบริบทของหน่วยงานตามข้อ 2.1 ในฐานข้อมูลทะเบียนความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย พ.ศ. 2568

2.2.1 การระบุหมวดสินทรัพย์

ข้อมูลสินทรัพย์เป็นรายละเอียดเกี่ยวกับสินทรัพย์ที่หน่วยงานประเมินว่าอาจถูกโจมตีทางไซเบอร์ ทั้งนี้เนื่องจากชื่อสินทรัพย์ที่ประเมินความเสี่ยงจัดเป็นข้อมูลอ่อนไหว หากมีการเปิดเผยอาจมีความเสี่ยงให้ผู้ประสงค์ร้ายสามารถทราบถึงมาตรการรักษาความปลอดภัย ที่หน่วยงานจัดทำขึ้นต่อสินทรัพย์นั้น ๆ จึงได้พิจารณาความเกี่ยวข้องของสินทรัพย์และจัดเข้ากับหมวดข้อมูลดังที่กำหนดในประกาศ สกมช. เรื่อง “แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2567” หลีกเลี่ยงการระบุข้อมูลประเภทสินทรัพย์ที่อาจเป็นข้อมูลอ่อนไหว



2.2.2 การระบุช่องโหว่ (Vulnerability)

ช่องโหว่เป็นช่องทางที่ภัยคุกคามทางไซเบอร์จะเข้ามาสร้างความเสียหายแก่สินทรัพย์ขององค์กร โดยกรอบฯได้อ้างอิงประเภทของช่องโหว่ตามมาตรฐาน ISO/IEC 27005:2022 ซึ่งจำแนกประเภทช่องโหว่ที่อาจเป็นเหตุให้เกิดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยข้อมูลการประเมินความเสี่ยงของหน่วยงานจะถูกพิจารณาจัดเป็นหมวดหมู่ดังตาราง

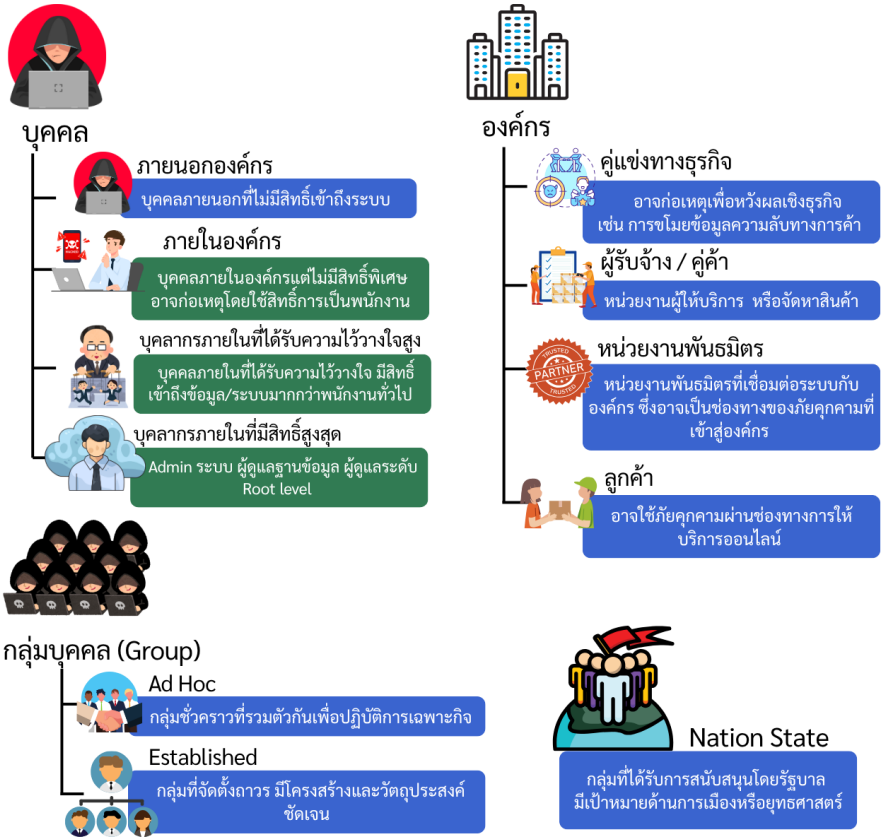
ช่องโหว่ (Vulnerability)	รายละเอียด
องค์กร	ขาดโครงสร้างกำกับดูแล ที่ทำการตรวจสอบ การผลักดันนโยบายไซเบอร์ที่ครอบคลุมด้านการใช้ซอฟต์แวร์/เครื่องมือ/บริการ
กระบวนการและระเบียบปฏิบัติ	ช่องโหว่อันเนื่องจากระเบียบปฏิบัติที่เปิดช่องโหว่ให้ผู้ประสงค์ร้ายฉวยโอกาสสร้างผลกระทบต่อองค์กร
กิจวัตรของฝ่ายบริหาร	ช่องโหว่จากกิจวัตรประจำวันของฝ่ายบริหาร หรือกำหนดการดำเนินงานที่อาจรั่วไหลสู่ภายนอก ส่งให้ผู้ประสงค์ร้าย ฉวยโอกาสโจมตี
บุคลากร / พนักงาน	ช่องโหว่เกิดจากปัจจัยของบุคลากร ทั้งด้านองค์ความรู้ ความตระหนัก/การรู้เท่าไม่ถึงการ ความประมาท อันเป็นเหตุให้ผู้ประสงค์ร้ายชักจูงและฉวยโอกาสโจมตี
สภาพแวดล้อมทางกายภาพ	จุดอ่อนในโครงสร้างพื้นฐานหรือสภาพแวดล้อมทางกายภาพขององค์กร เช่น สภาพพื้นที่ที่เปิดโอกาสให้เกิดการโจมตี
การตั้งค่าระบบสารสนเทศ	จุดอ่อนที่เกิดจากการตั้งค่าระบบผิดพลาด ไม่ถูกต้องตามหลักความมั่นคงปลอดภัยไซเบอร์
ฮาร์ดแวร์ อุปกรณ์สื่อสาร	จุดอ่อนที่เกิดจากฮาร์ดแวร์ เฟิร์มแวร์ หรืออุปกรณ์สื่อสาร ที่มีความบกพร่อง เก่า หรือ ไม่ได้รับการสนับสนุน/ดูแลจากผู้ให้บริการ
ซอฟต์แวร์	ช่องโหว่ที่เกิดในซอฟต์แวร์ หรือเขียนโค้ดมีช่องโหว่ จุดบกพร่อง หรือซอฟต์แวร์ขาดการอัพเดท
การพึ่งพาบุคคลหรือหน่วยงานภายนอก	ช่องโหว่ที่เกิดจากกิจกรรมสำคัญของบุคคลที่สาม ซึ่งอาจส่งผลให้เกิดความเสี่ยงและช่องโหว่ที่องค์กรไม่สามารถควบคุมได้โดยตรง

2.2.3 ผู้ประสงค์ร้าย (Threat Actor)

ผู้ประสงค์ร้าย หมายถึง บุคคล กลุ่มบุคคล องค์กร หรือ ประเทศที่ต้องการใช้ประโยชน์จากช่องโหว่และภัยคุกคามทางไซเบอร์โจมตีสินทรัพย์ขององค์กรโดยเจตนา

การระบุผู้ประสงค์ร้ายจึงเพิ่มโอกาสในการทราบถึงแรงจูงใจในการโจมตีระดับความเชี่ยวชาญ กลวิธีและเทคนิคในการโจมตีทางไซเบอร์ที่คาดว่าจะใช้โจมตีและโอกาสสำเร็จในการโจมตีทางไซเบอร์เพื่อกำหนดมาตรการควบคุมและเฝ้าระวังผู้ประสงค์ร้ายกลุ่มนั้น

กรอบฯได้อ้างอิงกลุ่มผู้ประสงค์ร้ายจากมาตรฐาน NIST SP 800-30 ภาคผนวก D-2 Taxonomy of Threat Sources ซึ่งมีการแบ่งกลุ่มดังนี้



2.2.4 เหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Event)

เหตุการณ์ภัยคุกคามทางไซเบอร์ หมายถึงเหตุการณ์ที่ผู้ประสงค์ร้ายกระทำความเสียหายโดยใช้กลวิธี และเทคนิคการโจมตีทางไซเบอร์ ซึ่งตามกรอบฯ ได้อ้างอิงจากมาตรฐาน NIST SP 800-30 ภาคผนวก E-2 Taxonomy of Threat Events ซึ่งมีการแบ่งกลุ่มเหตุการณ์ภัยคุกคามออกเป็น 8 กลุ่ม ได้แก่



1. หมวด P: สอดแนมและรวบรวมข้อมูล



P.1 ดำเนินการสำรวจหรือสแกนเครือข่ายรอบนอกขององค์กร
P.2 ดำเนินการดักจับข้อมูลการสื่อสารบนเครือข่ายที่เปิดเผย
P.3 รวบรวมข้อมูลขององค์กรจากแหล่งข้อมูลสาธารณะ
P.4 ดำเนินการสำรวจและสอดแนมองค์กรเป้าหมาย
P.5 ดำเนินการสืบค้นข้อมูลภายในองค์กรโดยอาศัยมัลแวร์ที่ถูกติดตั้งในระบบ

2. หมวด C: สร้างเครื่องมือโจมตี



C.1 การสร้างและออกแบบการโจมตีแบบฟิชชิง
C.2 สร้างและออกแบบการโจมตีแบบสเปียร์ฟิชชิงที่เจาะจงเป้าหมาย
C.3 สร้างหรือออกแบบการโจมตีเฉพาะตามสภาพแวดล้อมเทคโนโลยีสารสนเทศที่ใช้งานอยู่
C.4 สร้างเว็บไซต์ปลอม/เว็บไซต์เลียนแบบ
C.5 สร้างหรือปลอมแปลงใบรับรองดิจิทัล
C.6 สร้างบริษัทบังหน้าเพื่อแทรกส่วนประกอบที่เป็นอันตรายเข้าสู่ห่วงโซ่อุปทานของหน่วยงาน

3. หมวด D: ติดตั้งความสามารถที่เป็นอันตราย



D.1 ส่งมัลแวร์ที่รู้จักโดยทั่วไปเข้าสู่ระบบสารสนเทศภายในองค์กร
D.2 ส่งมัลแวร์ที่ถูกดัดแปลงไปยังระบบสารสนเทศภายในองค์กร
D.3 โจมตีด้วยมัลแวร์แบบเจาะจงเป้าหมายเพื่อยึดควบคุมระบบภายใน และดึงข้อมูลออกจากองค์กร
D.4 ส่งมัลแวร์เข้าสู่ระบบโดยการให้สื่อที่ถอดได้
D.5 การสุ่มฝังมัลแวร์ลงในซอฟต์แวร์ที่ดาวน์โหลดได้/หรือผลิตภัณฑ์เทคโนโลยีสารสนเทศเชิงพาณิชย์

3. หมวด D: ติดตั้งความสามารถที่เป็นอันตราย

D.6 ฝังมัลแวร์แบบเจาะจงเป้าหมายลงในระบบสารสนเทศและส่วนประกอบของระบบภายในองค์กร

D.7 ฝังมัลแวร์เฉพาะทางลงในระบบสารสนเทศขององค์กรตามการตั้งค่าระบบที่ใช้งานอยู่

D.8 ลักลอบแทรกอุปกรณ์ปลอมหรือถูกดัดแปลงให้เกิดช่องโหว่ในห่วงโซ่อุปทานขององค์กร

D.9 การดัดแปลง หรือแก้ไขส่วนประกอบสำคัญ โดยไม่ได้อนุญาตในอุปกรณ์ที่ส่งผลต่อห่วงโซ่อุปทาน

D.10 ติดตั้งโปรแกรมดักจับข้อมูลทั่วไปบนระบบควบคุมหรือเครือข่ายขององค์กร

D.11 ติดตั้งโปรแกรมดักจับข้อมูลแบบมุ่งเป้าเฉพาะเป้าหมายบนระบบควบคุมหรือเครือข่ายขององค์กร

D.12 ฝังมัลแวร์แสกนภายในอุปกรณ์และซอฟแวร์

D.13 การโจมตีผ่าน "บุคคล" ที่ไม่ปฏิบัติตามเจตนารมณ์ขององค์กร

D.14 โจมตีผ่าน "บุคคล" ที่ไม่ปฏิบัติตามเจตนารมย์ขององค์กร โดยบุคคลนั้นอยู่ในตำแหน่งที่สำคัญขององค์กร



4. หมวด E: ใช้ประโยชน์ช่องโหว่และการถูกบุกรุก

E.1 ใช้สิทธิ์การเข้าถึงของพนักงานที่ได้รับอนุญาต เพื่อเข้าไปยังพื้นที่หรือสิ่งอำนวยความสะดวกขององค์กร

E.2 เจาะช่องโหว่ของระบบสารสนเทศที่ตั้งค่าผิดพลาดหรือไม่ได้รับอนุญาตซึ่งเปิดเผยต่ออินเทอร์เน็ต

E.3 ใช้ช่องโหว่จากการตั้งค่า Split Tunneling เพื่อเข้าถึงระบบองค์กร

E.4 ใช้ช่องโหว่จากการแชร์ทรัพยากรของผู้ใช้หลายรายในระบบคลาวด์

E.5 ใช้ประโยชน์จากช่องโหว่ของอุปกรณ์เคลื่อนที่ เช่น แล็ปท็อป, PDA, สมาร์ทโฟน เป็นต้น

E.6 ใช้ประโยชน์จากช่องโหว่ที่เพิ่งถูกค้นพบใหม่ไม่นาน

4. หมวด E: ใช้ประโยชน์ช่องโหว่และการถูกบุกรุก

E.7 ใช้ประโยชน์จากช่องโหว่ในระบบสารสนเทศภายในองค์กร
E.8 ใช้ประโยชน์จากช่องโหว่ที่ยังไม่ถูกเปิดเผยหรือยังไม่มีแพตช์ (Zero-Day) เพื่อโจมตีระบบ
E.9 ลักลอบแทรกอุปกรณ์ปลอมหรือถูกดัดแปลงให้เกิดช่องโหว่ในห่วงโซ่อุปทานขององค์กร
E.10 การดัดแปลง หรือแก้ไขส่วนประกอบสำคัญ โดยไม่ได้อนุญาต ในอุปกรณ์ที่ส่งผลต่อห่วงโซ่อุปทาน
E.11 ละเมิดการจำกัดสิทธิ์ของผู้ใช้ในระบบคลาวด์ที่ใช้ร่วมกันหลายหน่วยงาน
E.12 บุกรุกระบบสารสนเทศที่มีความสำคัญโดยอาศัยการเข้าถึงทางกายภาพ
E.13 บุกรุกระบบสารสนเทศหรืออุปกรณ์ที่ถูกนำไปใช้นอกองค์กร แล้วถูกนำกลับเข้ามาเชื่อมต่อในระบบขององค์กรอีกครั้ง
E.14 เจาะหรือแทรกแซงซอฟต์แวร์ของระบบสารสนเทศที่มีความสำคัญขององค์กร
E.15 เจาะระบบสารสนเทศขององค์กรเพื่ออำนวยความสะดวกในการขโมยหรือนำข้อมูลออกไปภายนอก
E.16 เจาะหรือละเมิดข้อมูลที่มีความสำคัญต่อภารกิจหลักขององค์กร
E.17 เจาะหรือละเมิดกระบวนการออกแบบ การผลิต และ/หรือการจัดจำหน่ายส่วนประกอบของระบบสารสนเทศ (รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์)

5. หมวด A: ดำเนินการโจมตี



A.1 ดำเนินการโจมตีด้วยการดักจับการสื่อสาร
A.2 ดำเนินการโจมตีด้วยการรบกวนสัญญาณไร้สาย
A.3 ดำเนินการโจมตีโดยใช้พอร์ต โปรโตคอล หรือบริการที่ไม่ได้รับอนุญาต
A.4 ดำเนินการโจมตีโดยใช้ประโยชน์จากการเคลื่อนย้ายข้อมูล/การรับส่งข้อมูลที่อนุญาตให้ข้ามเขตป้องกัน

5. หมวด A: ดำเนินการโจมตี

A.5 ดำเนินการโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) แบบง่าย
A.6 ดำเนินการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed Denial of Service: DDoS)
A.7 ดำเนินการโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) ที่มุ่งเป้าไปยังเป้าหมายเฉพาะ
A.8 ก่อเหตุโจมตีทางกายภาพต่อสถานที่หรืออุปกรณ์ทางกายภาพองค์กร
A.9 ก่อเหตุโจมตีทางกายภาพต่อโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร
A.10 ก่อเหตุโจมตีระบบสารสนเทศเพื่อควบคุมหรือทำลายสถานที่ หรืออุปกรณ์ทางกายภาพขององค์กร
A.11 ดำเนินการโจมตีแบบค้นหาข้อมูลในสภาพแวดล้อมคลาวด์
A.12 ดำเนินการโจมตีการพยายามเข้าสู่ระบบแบบคาดเดารหัสผ่าน
A.13 ดำเนินการโจมตี Zero-day แบบไม่มุ่งเป้าเฉพาะ
A.14 ยึดครองการเชื่อมต่อของผู้ใช้จากภายนอกองค์กร
A.15 ยึดครองการเชื่อมต่อของผู้ใช้จากภายในองค์กร
A.16 ดำเนินการโจมตีการแก้ไขการรับส่งข้อมูลเครือข่ายจากภายนอก (Man-in-the-Middle)
A.17 ดำเนินการโจมตีการแก้ไขการรับส่งข้อมูลเครือข่ายจากภายใน (Man-in-the-Middle)
A.18 ดำเนินการทำวิศวกรรมสังคมจากภายนอกเพื่อแสวงหาข้อมูล
A.19 ดำเนินการทำวิศวกรรมสังคมจากภายในเพื่อแสวงหาข้อมูล
A.20 ดำเนินการโจมตีที่มุ่งเป้าและทำให้เครื่องมือหรืออุปกรณ์ส่วนตัวของพนักงานสำคัญถูกเจาะระบบ
A.21 ดำเนินการโจมตีห่วงโซ่อุปทานที่มุ่งเป้าและเจาะช่องโหว่ในฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ที่สำคัญ

6. หมวด R: การบรรลุผลลัพธ์ที่ไม่พึงประสงค์

R.1 ดักจับและขโมยข้อมูลอ่อนไหวผ่านการดักฟังเครือข่ายภายนอก (Network Sniffing)
R.2 ขโมยข้อมูลสำคัญออกจากระบบขององค์กร (Data Exfiltration)
R.3 ทำให้บริการหรือระบบที่ผู้โจมตีเลือกไว้ทำงานช้าลงหรือไม่สามารถให้บริการได้
R.4 ทำให้ส่วนสำคัญของระบบเสียหายหรือถูกทำลายจนไม่สามารถใช้งานได้
R.5 แก้ไขหรือลบข้อมูลบนระบบสาธารณะจนข้อมูลไม่ถูกต้อง (เช่น การเปลี่ยนหน้าเว็บไซต์ขององค์กรให้กลายเป็นเว็บไซต์การพนัน)
R.6 ทำให้ข้อมูลสำคัญผิดเพี้ยนหรือเสียหายจนไม่สามารถเชื่อถือได้
R.7 ก่อให้เกิดการสูญเสียความถูกต้องของข้อมูล โดยการแทรกข้อมูลเท็จแต่มีลักษณะน่าเชื่อถือเข้าสู่ระบบสารสนเทศขององค์กร
R.8 ก่อให้เกิดการเปิดเผยข้อมูลที่สำคัญและ/หรือข้อมูลอ่อนไหว โดยผู้ใช้ที่ได้รับอนุญาต
R.9 ทำให้ข้อมูลลับรั่วไหลหรือไม่สามารถใช้งานได้โดยไม่ได้รับอนุญาต
R.10 ดักฟังข้อมูลบนเครือข่ายไร้สายจากภายนอกองค์กร
R.11 การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต
R.12 เข้าถึงหรือรวบรวมข้อมูลที่มีความอ่อนไหวจากระบบสารสนเทศที่เปิดให้สาธารณะเข้าถึงได้
R.13 ขโมยหรือเก็บกู้ข้อมูลและอุปกรณ์จากระบบสารสนเทศเมื่อมีโอกาส





7. หมวด M: ลอบเร้นและหลบเลี่ยงระบบตรวจจับ

M.1 ทำให้การกระทำของฝ่ายผู้โจมตีถูกปกปิดหรือยากต่อการตรวจจับ
M.2 ปรับรูปแบบการโจมตีทางไซเบอร์ตามข้อมูลที่ได้จากการเฝ้าสอดแนมอย่างละเอียด

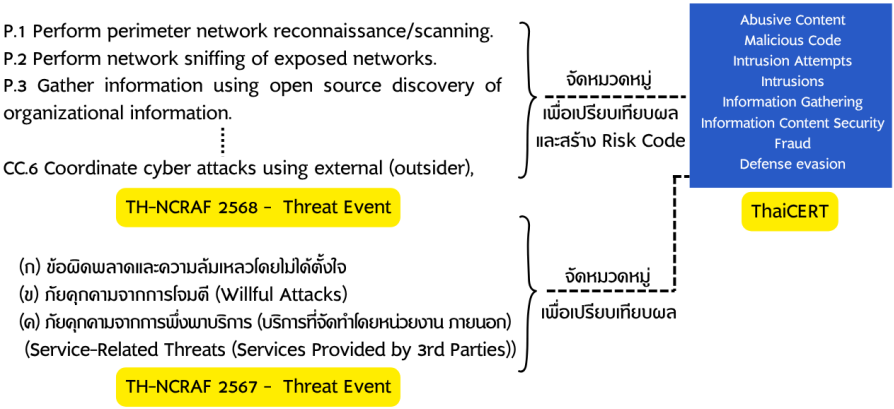
8. หมวด CC: โจมตีประสานหลายรูปแบบ/ช่องทาง

CC.1 วางแผนและดำเนินการโจมตีหลายขั้นตอนแบบต่อเนื่องและข้ามระบบ
CC.2 วางแผนโจมตีจากทั้งภายในและภายนอกพร้อมกันในหลายระบบขององค์กร
CC.3 วางแผนโจมตีหลายองค์กรพร้อมกันเพื่อขโมยข้อมูลหรือบรรลุเป้าหมายที่ตั้งไว้
CC.4 ขยายการโจมตีจากระบบที่ถูกเจาะแล้วไปยังส่วนอื่นขององค์กรอย่างเป็นขั้นตอน
CC.5 วางแผนโจมตีไซเบอร์แบบต่อเนื่องและปรับเปลี่ยนได้ โดยอาศัยข้อมูลจากการสอดแนมอย่างละเอียด
CC.6 วางแผนโจมตีไซเบอร์โดยใช้ทั้งช่องทางภายนอก ภายใน และจากคู่ค้าในห่วงโซ่อุปทาน

2.2.5 การเทียบเคียงจำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ถูกระบุในความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ปี พ.ศ. 2567-2568

เนื่องจากเหตุการณ์ภัยคุกคามทางไซเบอร์ของกรอบฯ ที่มีการทบทวนนั้นมีการพิจารณาปรับปรุงความเป็นปัจจุบันและพิจารณาเฉพาะเหตุการณ์ภัยคุกคามที่มีผู้ประสงค์ร้าย (Adversarial Threat) โดยอ้างอิงจากกลวิธีและเทคนิค ตามมาตรฐาน NIST SP 800-30 ดังที่กล่าวในหัวข้อ 2.2.4 ซึ่งมี รายละเอียดที่แตกต่างจากกรอบฯ ปี พ.ศ. 2567

ในการนี้เพื่อให้เทียบเคียงผลตามหลักสถิติได้ จึงมีการวิเคราะห์จัดหมวดเหตุการณ์ภัยคุกคามทางไซเบอร์ของกรอบฯ ปี พ.ศ. 2567-2568 กับ “หมวดเหตุการณ์ภัยคุกคามทางไซเบอร์” (Incident Class) ที่ “ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ” (ThaiCERT) อ้างอิงหมวดหมู่จาก ENISA* เพื่อจัดทำสถิติทางภัยคุกคามทางไซเบอร์ โดยมีแนวคิดแสดงดังภาพ



* – Reference Incident Classification Taxonomy - ENISA

Incident Class	Sub Categories
Abusive Content	Spam
	Harassment
Malicious Code	Virus/Worm/Trojan/Spyware
Information Gathering	Scanning
	Sniffing
	Social Engineering
Intrusion Attempts	Exploiting of known Vulnerabilities
	Login attempts
	New attack signature
Intrusion	Privileged Account Compromise
	Unprivileged Account Compromise
	Application Compromise
	Campaigns
Availability Attack	DoS
	DDoS
	Sabotage

หมวดตามมาตรฐาน Reference Incident Classification Taxonomy - ENISA

หมวดที่เพิ่มเติม เพื่อให้สอดคล้องเหตุการณ์ภัยคุกคามทางไซเบอร์ตามกรอบฯ

Incident Class	Sub Categories
Information Content Security	Unauthorises access to information
	Unauthorised modification of information
Fraud	Unauthorized use of resources
	Masquerade
	Fake Website
Other	Defense evasion

สามารถสแกน QR Code เพื่อเข้าถึงผลการจัดหมวดหมู่ตามรูปแบบภัยคุกคามทางไซเบอร์ (Incident class) ได้ดังภาพ

Scan here for access to the mapping result

นอกจากนั้น ภัยคุกคามที่ถูกจัดเป็นหมวดหมู่ตามรูปแบบภัยไซเบอร์ จะถูกใช้กำหนดรหัสความเสี่ยง (Risk Code) ซึ่งใช้อ้างอิงใน Risk Matrix ในขั้นตอนการประเมินความเสี่ยง (Risk Evaluation)

การสร้างรหัสความเสี่ยง (Risk Code) สำหรับ Risk Matrix

หมวดสินทรัพย์ (Asset Type) + แบบจำลองเหตุการณ์ภัยคุกคามทางไซเบอร์

ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk) ..... 1 รายการ

Risk Scenario	Incident Class	ตัวอย่างรหัสอ้างอิง
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Abusive Content : AC	AC.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Malicious Code : MC	MC.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Intrusion Attempts : IA	IA.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Intrusion: I	I.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Information Gathering: IG	IG.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Information Content Security : ICS	ICS.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Fraud : F	F.1 [Risk Scenario]
ความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Risk)	Defense Evasion : DE	DE.1 [Risk Scenario]

โดยผู้อ่านสามารถสแกน QR Code เพื่อเข้าถึงผลลงทะเบียนความเสี่ยงและรหัสอ้างอิงความเสี่ยงที่ถูกใช้ในการจัดทำ Risk Matrix ได้ดังภาพ

Scan here for access
TH-NCRAF Risk identification

2.3 การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงจากภัยคุกคามทางไซเบอร์ ประกอบด้วย 2 ส่วนหลัก ได้แก่ **ระดับผลกระทบ (Impact) และ ระดับโอกาสเกิดเหตุการณ์ (Likelihood)** ซึ่งสะท้อนถึงระดับความเสี่ยงที่หน่วยงานได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

2.3.1 การวิเคราะห์ระดับผลกระทบ (Impact Analysis)

ระดับผลกระทบ คือ ระดับความเสียหายที่อาจเกิดขึ้นจากกับองค์กรเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ขึ้นซึ่งผลกระทบตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ โดยแบ่งเป็น 3 ด้าน ตาม CIA Triad ได้แก่



ในการพิจารณาผลกระทบในแต่ละด้านตาม CIA Triad ต้องพิจารณาแยกตาม

- ผลกระทบต่อชื่อเสียงและความน่าเชื่อถือของหน่วยงาน
- ผลกระทบเกี่ยวกับความเสียหายทางการเงินและสินทรัพย์
- ผลกระทบต่อความสามารถในการปฏิบัติหน้าที่ – กระบวนงาน
- ผลกระทบต่อการปฏิบัติตามกฎหมายและระเบียบ

การพิจารณาระดับผลกระทบ กำหนดให้แบ่งเป็น 3 ระดับได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ โดยหลังจากพิจารณาแต่ละด้านครบถ้วน ระดับผลกระทบที่สูงสุดจะถูกใช้ในการประเมินระดับความเสี่ยงต่อไป

2.3.2 การวิเคราะห์โอกาสเกิดเหตุการณ์ภัยคุกคาม (Likelihood)

โอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ หมายถึง ระดับความน่าจะเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือ ระดับความเป็นไปได้ที่ภัยคุกคามทางไซเบอร์จะอาศัยช่องโหว่เข้าโจมตีหน่วยงานจนเกิดความเสียหายในการพิจารณาโอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์มีการแบ่งมิติการพิจารณาเป็น 4 ส่วน ได้แก่

- ระดับความยาก-ง่ายในการโจมตีซ้ำ (Reproducibility)
- ระดับความเชี่ยวชาญของผู้โจมตีที่ต้องใช้ (Exploitability) ดำเนินการตามกลวิธีและเทคนิค ในกรณีเป็นผู้โจมตีที่เกิดจากการรวมกลุ่ม หรือ หน่วยผู้ได้รับสนับสนุนจากรัฐบาล จะทำให้โอกาสเกิดความเสี่ยงเพิ่มขึ้น
- ระดับความยาก-ง่ายที่ผู้โจมตีจะตรวจพบช่องโหว่ (Discoverability)
- เหตุการณ์ภัยคุกคามทางไซเบอร์ในอดีต (Past Incident)

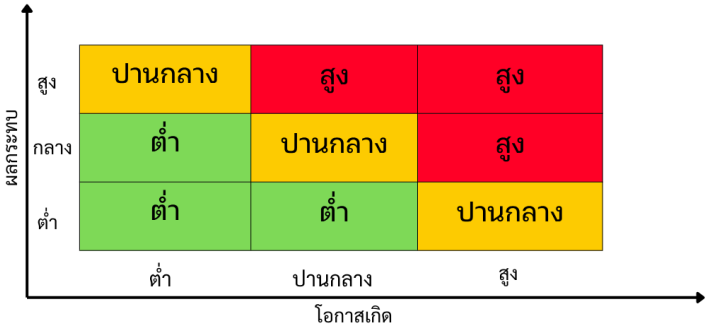
การพิจารณาระดับโอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ กำหนดให้แบ่งเป็น 3 ระดับได้แก่ ระดับสูง ระดับปานกลาง และระดับต่ำ โดยหลังจากพิจารณาแต่ละด้านครบถ้วน ระดับโอกาสเกิดที่สูงสุด จะถูกใช้ในการประเมินระดับความเสี่ยงต่อไป

2.3.3 การวิเคราะห์ระดับความเสี่ยง (Risk Analysis)

ระดับความเสี่ยงจากภัยคุกคามทางไซเบอร์ เป็นตัวบ่งชี้ระดับที่หน่วยงานได้รับ ผลกระทบจากเหตุการณ์ภัยคุกคามทางไซเบอร์ซึ่งถูกกำหนดโดยโอกาสที่จะเกิดเหตุการณ์ ภัยคุกคามที่เกิดขึ้นและระดับผลกระทบ ซึ่งระดับความเสี่ยงภายใต้กรอบฯมีวิธีการคำนวนแสดงดังสมการ

ระดับความเสี่ยง = (ระดับผลกระทบ) x (ระดับโอกาสเกิดความเสี่ยง)

ระดับความเสี่ยงจะถูกแสดงใน เมทริกซ์ความเสี่ยง (Risk Matrix) ที่จัดทำเป็น ตาราง 3x3 ดังภาพ ซึ่งจะถูกใช้แสดงภาพรวมความเสี่ยงที่เกิดขึ้นเพื่อกำหนดมาตรการบรรเทาความเสี่ยงต่อไป



2.3.4 การปรับค่าระดับให้เป็นระดับเดียวกัน

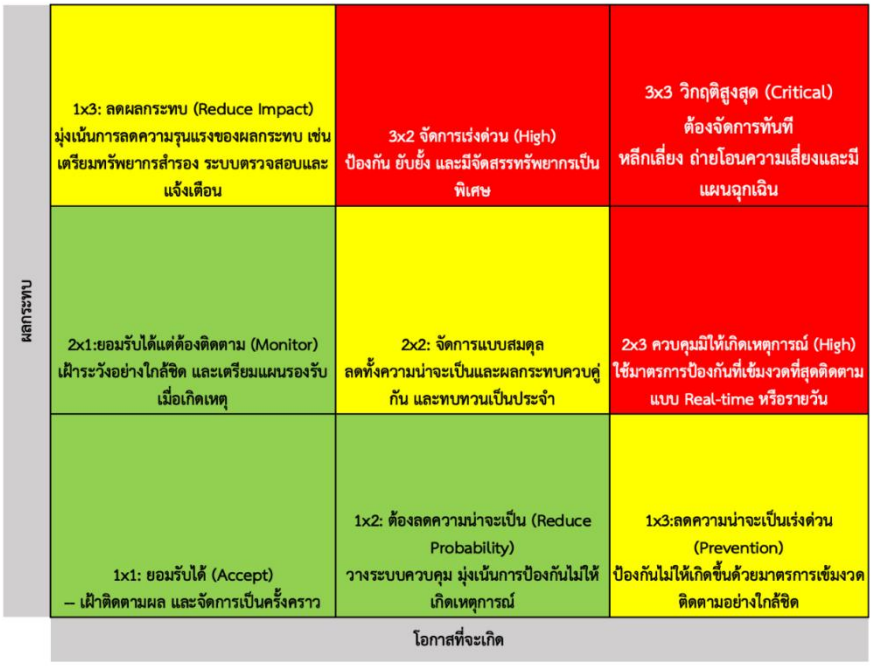
ข้อมูลจากการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ฯ ของแต่ละหน่วยงาน อาจมีเกณฑ์การพิจารณาและจัดระดับผลกระทบ - โอกาสที่จะเกิด - ระดับความเสี่ยง ที่แตกต่างกัน เพื่อให้ผลการประเมินแต่ละหน่วยงานสามารถเทียบเคียงกันได้ จึงมีการจัดระดับให้เป็นระดับเดียวกัน (Normalization) กับกรอบฯ โดยใช้เกณฑ์อ้างอิงดังตาราง

ระดับตามกรอบฯ	หน่วยงานที่ใช้เกณฑ์ 3 ระดับ	หน่วยงานที่ใช้เกณฑ์ 4 ระดับ	หน่วยงานที่ใช้เกณฑ์ 5 ระดับ
สูง	สูง	สูงมาก	สูงมาก
		สูง	สูง
ปานกลาง	ปานกลาง	ปานกลาง	ปานกลาง
ต่ำ	ต่ำ	ต่ำ	ต่ำ
			ต่ำมาก

2.4 การประเมินค่าความเสี่ยง (Risk Evaluation)

2.4.1 แนวทางการจัดลำดับความสำคัญ (Risk Prioritization)

เมื่อได้รับผลการวิเคราะห์ระดับความเสี่ยงและแสดงผลในเมทริกซ์ความเสี่ยงแล้ว จึงนำมาพิจารณาจัดลำดับความสำคัญ (Priority) ความเสี่ยงที่ควรเร่งจัดการให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ หรือ ลดผลกระทบลง ในการนี้จึงได้จัดทำแนวทางตอบสนองกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีแนวทางจัดการดังเมทริกซ์ความเสี่ยงดังภาพ



แนวทางการจัดลำดับความเสี่ยงด้วย Risk Matrix แบบ 3x3

2.4.2 แนวทางการตอบสนองกับความเสี่ยง (Risk Respond)

แนวทางตอบสนองความเสี่ยงจากภัยคุกคามระดับชาติต่อไป โดยมี 4 แนวทาง

- **การยอมรับความเสี่ยง** [Risk Acceptance (Accept)]
  สำหรับความเสี่ยงที่มีผลกระทบต่ำและไม่คุ้มค่าในการจัดการ/ป้องกัน แต่ต้องมีการเฝ้าระวังอย่างสม่ำเสมอ
- **การลด/การควบคุมความเสี่ยง** [Risk Reduction (Control)]
  ปรับปรุงระบบการทำงาน และช่องโหว่ที่เกิดขึ้น เพื่อลดโอกาสที่จะเกิดความเสียหายหรือลดผลกระทบที่อาจจะเกิดขึ้นจากความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ เช่น การจัดอบรมพนักงาน การปิดช่องโหว่ทางไซเบอร์ การพัฒนาระบบคัดกรองผู้ใช้งาน เป็นต้น
- **กระจายความเสี่ยง หรือโอนความเสี่ยง** [Risk Transfer (Transfer)]
  ถ่ายโอนความเสี่ยงให้ หน่วยงานอื่นช่วยแบ่งความรับผิดชอบ เช่น การทำประกันภัยกับบริษัทภายนอก หรือการจ้างบุคคลภายนอกดำเนินการแทน (Outsource)
- **การหลีกเลี่ยงความเสี่ยง/จำกัดความเสี่ยง** [Risk Avoidance (Avoid)]
  การจัดการกับความเสี่ยงที่อยู่ในระดับสูงมาก และไม่อาจยอมรับได้ จึงตัดสินใจยกเลิกโครงการ/กิจกรรมที่จะก่อให้เกิดความเสี่ยงนั้น รวมถึงดำเนินการกำหนดเหตุแห่งความเสี่ยง เหล่านั้น





3. รายงานผลการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย พ.ศ. 2568

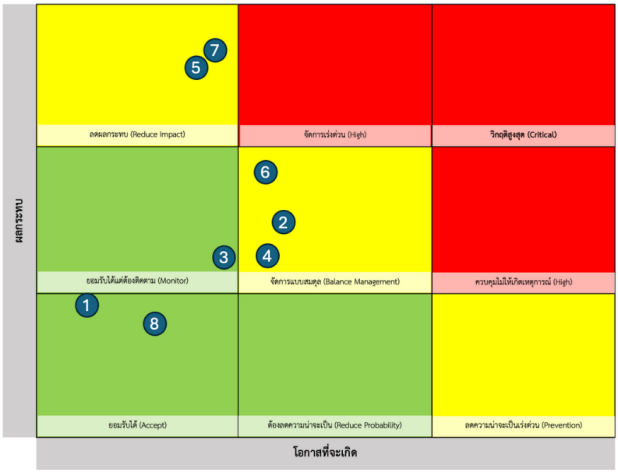


รายงานผลการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย พ.ศ. 2568

3.1 ผลการประเมินความเสี่ยงในระดับประเทศ

3.1.1 ภาพรวมความเสี่ยงในระดับประเทศ

เมื่อได้รับผลการวิเคราะห์ระดับความเสี่ยงและแสดงผลในเมทริกซ์ความเสี่ยงแล้ว จึงนำมาพิจารณาจัดลำดับความสำคัญ (Priority) ความเสี่ยงที่ควรเร่งจัดการให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ หรือ ลดผลกระทบลง ในการนี้จึงได้จัดทำแนวทางตอบสนองกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีแนวทางจัดการดังเมทริกซ์ความเสี่ยง ดังภาพ



1. ความมั่นคงของรัฐ	4. เทคโนโลยีสารสนเทศและโทรคมนาคม	7. สาธารณสุข
2. บริการภาครัฐที่สำคัญ	5. การขนส่งและโลจิสติกส์	8. หน่วยงานของรัฐ (ที่ไม่ใช่ CII)
3. การเงินและธนาคาร	6. พลังงานและสาธารณูปโภค	



ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงของประเทศไทย มีบ่งชี้ถึงรายละเอียดต่อไปนี้

(1) การเข้าถึงโดยไม่ได้รับอนุญาต หรือการพยายามเข้ามาโดยมิชอบ กับการใช้ประโยชน์จากช่องโหว่ที่มีอยู่ในระบบสารสนเทศภายในองค์กร หรือการที่ระบบเคยถูกบุกรุกเป็นความเสี่ยงที่พบมากที่สุดซึ่งระดับความเสี่ยงขึ้นอยู่กับความสำคัญของสินทรัพย์นั้น ๆ

(2) การโจมตีแบบ DoS ทั้งแบบสุ่ม แบบมุ่งเป้า และแบบกระจาย (DDoS) ยังคงเป็นภัยคุกคามทางไซเบอร์ที่ทุกหน่วยงานพบและสร้างความเสียหายแก่องค์กรได้เสมอ

(3) มีความเสี่ยงที่ข้อมูลอ่อนไหว ข้อมูลลับขององค์กรอาจรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจากการใช้บัญชีผู้มีสิทธิ์เข้าถึงระบบ (Authorized User) ที่ถูกยึดโดยผู้ประสงค์ร้าย

(4) การที่ข้อมูลสำคัญหรือองค์ประกอบระบบสำคัญของระบบสารสนเทศถูกทำลาย โดยวิธีการต่าง ๆ เช่น ถูก Ransomware โจมตี เป็นต้น นั้นถูกกล่าวถึงในรายงานความเสี่ยงในทุกภาคส่วน แต่มีสัดส่วนความเสี่ยงระดับต่ำและระดับปานกลางโดยส่วนใหญ่

(5) มีความเสี่ยงที่มัลแวร์จะถูกใส่มาในอุปกรณ์แบบถอดได้ เช่น USB, SD, Card เป็นต้น รวมถึงอาจมีการฝังมาในไฟล์ข้อมูล ที่มีการส่งมอบแก่หน่วยงาน

(6) ผู้ประสงค์ร้ายจากภายในและภายนอกองค์กรอาศัยช่องโหว่จากบุคคลที่ขาดความตระหนักรู้หรืออาศัยความไว้วางใจเพื่อหลอกล่อให้เปิดเผยข้อมูลสำคัญ (Social Engineering)



(7) ภาพรวมความเสี่ยงโดยภาพรวมของประเทศจับกลุ่มใน “ยอมรับได้แต่ต้องลดความน่าจะเป็น” และกลุ่มอื่น ๆ ในส่วนที่มีระดับต่ำเป็นส่วนใหญ่

แต่อย่างไรก็ดีจากผลการประเมินความเสี่ยงเปรียบเทียบกับผลการศึกษาแนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ พบประเด็นที่น่าสนใจคือ

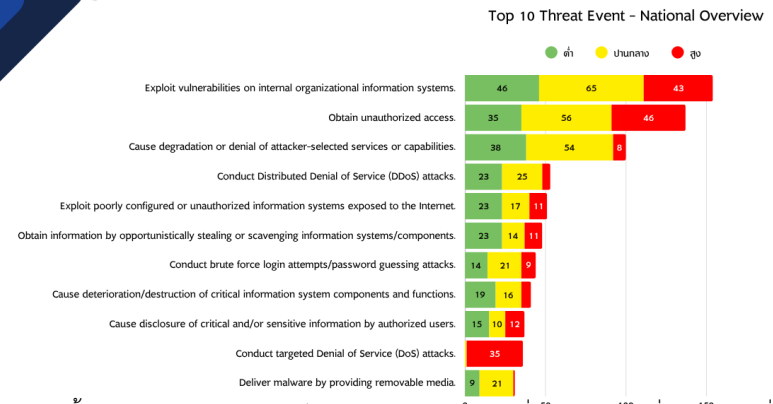
- การประเมินความเสี่ยงที่เกี่ยวกับห่วงโซ่อุปทานทั้งเหตุการณ์ภัยคุกคามทางไซเบอร์และการพึ่งพาผู้ให้บริการ ยังมีจำนวนไม่มากและรวมกลุ่มอยู่เฉพาะภาคส่วนหนึ่ง
- การคำนึงถึงความเสี่ยงต่อสินทรัพย์ที่เป็น AI ของหน่วยงาน และภัยคุกคามที่เกี่ยวกับข้อมูลของที่ใช้ฝึก AI นั้นแทบไม่มีการกล่าวถึงในการประเมินความเสี่ยง
- ความเสี่ยงจากภัยคุกคามที่มีความสามารถในการหลบเลี่ยงระบบตรวจจับภัยคุกคามทางไซเบอร์ แทบไม่ถูกกล่าวถึงในการประเมิน
- ความเสี่ยงที่เกี่ยวกับการสร้างเว็บไซต์ปลอม ใบรับรองปลอม เพื่อหลอกระบบตรวจจับภัยคุกคามแล้วส่งมัลแวร์ขโมยข้อมูลยังถูกกล่าวถึงน้อย แม้ สกมช. ได้รับรายงาน
- การประเมินความเสี่ยงเกี่ยวกับการให้บริการคลาวด์ หรือเกี่ยวกับช่องโหว่จากการพึ่งพาบริษัท/ผู้ให้บริการภายนอก ยังถูกกล่าวถึงน้อย โดยเฉพาะอย่างยิ่งการผลักดันนโยบายการใช้คลาวด์เป็นหลักส่งให้ระบบถูกโอนย้ายเข้าสู่บริการคลาวด์ที่มีพื้นที่การโจมตี (Attack Surface) สูงกว่า

3.1.2 ผลการสถิติจากการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี พ.ศ. 2568

จากการรวบรวมข้อมูลการประเมินความเสี่ยงและจัดเรียงให้อยู่ในรูปแบบข้อมูลทางสถิติ ได้ค้นพบประเด็นทางสถิติที่น่าสนใจ และมีนัยสำคัญต่อการจัดทำข้อเสนอแนะในการบรรเทาความเสี่ยง ดังต่อไปนี้

1) จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ถูกกล่าวถึงในความเสี่ยงฯ

จากข้อมูลการประเมินความเสี่ยงฯ บ่งชี้เหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Event) ที่หน่วยงานกล่าวถึงและถูกประเมินว่าอาจเกิดความเสี่ยงมากที่สุดและมีการแสดงผลเป็นข้อมูล เป็นแถบ 3 สี ประกอบด้วย สีเขียว สีเหลือง และสีแดง ซึ่งหมายถึงระดับความเสี่ยงที่หน่วยงานประเมินตนเองว่ามีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ในเรื่องนั้น ๆ ว่าทำให้เกิดความเสี่ยงระดับต่ำ ระดับปานกลาง และระดับสูงตามลำดับ ผลการรวบรวมข้อมูลทางสถิติจากรายงานผลการประเมินความเสี่ยง ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานของรัฐ รวมจำนวน 54 หน่วยงาน



มีการบ่งชี้ถึงเหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Event) ที่อาจเกิดความเสี่ยงบ่อยมากที่สุด ได้แก่

(1) การใช้ประโยชน์จากช่องโหว่ในระบบสารสนเทศภายในองค์กร (Exploit vulnerabilities on internal organizational information systems) คิดเป็นร้อยละ 12.9 ส่งผลให้เกิดความเสี่ยงระดับปานกลางเป็นส่วนใหญ่ แต่หากเป้าหมายโจมตีเป็นข้อมูลสำคัญขององค์กรจะส่งผลกระทบในระดับสูง

(2) การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต (Obtain unauthorized access) คิดเป็นร้อยละ 11.5 ส่งผลให้เกิดความเสี่ยงระดับปานกลางโดยส่วนใหญ่ หากเป็นสินทรัพย์ส่วนที่ไม่ส่งผลร้ายแรงต่อหน่วยงาน จะถูกจัดอยู่ในระดับต่ำ แต่อาจมีความน่าจะเป็นเพิ่มสูงขึ้น

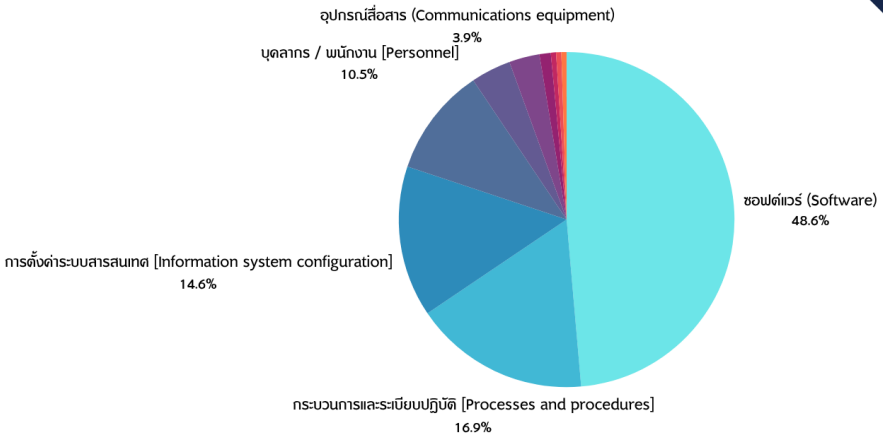
(3) ทำให้บริการหรือระบบที่ผู้โจมตีเลือกไว้ทำงานช้าลงหรือไม่สามารถให้บริการได้ (Cause degradation or denial of attacker-selected services or capabilities) คิดเป็นร้อยละ 8.4 ส่งผลให้เกิดความเสี่ยงในระดับปานกลางเป็นส่วนใหญ่

(4) การโจมตีแบบ DDoS (Conduct Distributed Denial of Service (DDoS) attacks) คิดเป็นร้อยละ 4.4 ซึ่งข้อมูลส่วนมากบ่งชี้เป็นความเสี่ยงระดับต่ำ

(5) เจาะช่องโหว่ของระบบสารสนเทศที่ตั้งค่าผิดพลาดหรือไม่ได้รับอนุญาตซึ่งเปิดเผยต่ออินเทอร์เน็ต (Exploit poorly configured or unauthorized information systems exposed to the Internet.) คิดเป็นร้อยละ 4.3 โดยส่วนใหญ่เป็นความเสี่ยงที่มีผลกระทบต่ำ

(6) การขโมยข้อมูลสำคัญขององค์กรโดยการฉวยโอกาสจากช่องโหว่ของระบบ (Obtain information by opportunistically stealing or scavenging information systems/components) คิดเป็นร้อยละ 4.0 ส่วนใหญ่จัดเป็นความเสี่ยงระดับต่ำ

2) ช่องโหว่ที่ถูกกล่าวถึงมากที่สุด



ช่องโหว่ ที่เกิดขึ้นนั้นเปิดโอกาสให้ผู้ประสงค์ร้ายเข้ามาโจมตีสินทรัพย์ขององค์กร และส่งผล กระทบต่อสินทรัพย์อื่น ที่เป็นเป้าหมายการโจมตีหลักของผู้ประสงค์ร้าย จากข้อมูลบ่งชี้ถึงช่องโหว่ที่เป็นสาเหตุให้สินทรัพย์ขององค์กรเกิดความเสียหาย ถูกละเมิด หรือถูกโจรกรรม ซึ่งช่องโหว่ที่ถูกกล่าวถึงมากที่สุด คือ

(1) **ช่องโหว่จากซอฟต์แวร์** – ทั้งจากการเขียนโค้ดของระบบสารสนเทศในองค์กรไม่ปลอดภัย เวอร์ชันของซอฟต์แวร์ โปรแกรมต่าง ๆ ซอฟต์แวร์ตัวกลางที่เชื่อมการทำงานเชิงเทคนิค ต้องได้รับการสนับสนุนจากผู้ให้บริการเพื่อปิดช่องโหว่ดังกล่าว

(2) **กระบวนการและระเบียบปฏิบัติ** – ระเบียบปฏิบัติที่มีช่องโหว่ให้ผู้ประสงค์ร้ายฉวยโอกาส หรือขาดการบังคับใช้ – ซักซ้อมจนเกิดความชำนาญ หรือขาดมาตรการตอบสนองกับเหตุการณ์ในเรื่องนั้น ๆ

(3) **การตั้งค่าระบบสารสนเทศ** – เกิดจากการตั้งค่าระบบไม่ถูกต้อง ขาดความเข้มงวดตามมาตรการรักษาความมั่นคงปลอดภัย

(4) **บุคลากร/เจ้าหน้าที่** – ขาดความตระหนักรู้ ประมาท หรือถูกชักจูง – บังคับให้ร่วมกระทำการโจมตีทางไซเบอร์ ซึ่งในบุคลากรในแต่ละกลุ่มมีความตระหนักรู้ในด้านไซเบอร์ที่แตกต่างกัน

จากข้อมูลที่ได้รับ บ่งชี้ว่าเหตุการณ์โจมตีทางไซเบอร์ทั้งหมด ผู้ประสงค์ร้ายมีเจตนาหลักทั้งหมด 3 ส่วน ได้แก่ มุ่งหวังข้อมูลลับ – อ่อนไหว มุ่งทำลายหรือทำให้ประสิทธิภาพของระบบลดลง และมุ่งหวังข้อมูลส่วนบุคคลโดยเฉพาะบัญชีผู้ใช้งานระบบ เพื่อใช้ในการโจมตีทางไซเบอร์ต่อไป โดยช่องโหว่เหล่านี้ควรได้รับการควบคุม แก้ไข เพื่อบรรเทาความเสี่ยงลง

3) ความเสี่ยงจากภัยคุกคามภายในหน่วยงาน (Insider Threat)

ผู้ประสงค์ร้ายอาจมาจากภายนอก หรือแฝงตัวเข้ามาภายในองค์กร เพื่อโจมตีทรัพย์สินขององค์กรและบรรลุวัตถุประสงค์ของบุคคลนั้น ๆ แต่ในบางกรณีก็มีโอกาสที่บุคลากรของหน่วยงานกลายเป็นผู้ประสงค์ร้ายที่ทำการโจมตีเสียเอง จากผลการศึกษาของ ENISA Threat Landscape 2024 บ่งชี้ถึงแรงจูงใจทางการเงินที่เป็นเหตุผลหลักในการโจมตีทางไซเบอร์ซึ่งอาจทำให้บุคลากรภายในหน่วยงานทั้งระดับบุคลากรระดับปฏิบัติการ (Insider) ระดับที่มีสิทธิ์เข้าถึงข้อมูลระดับสูง (Trusted Insider) และบุคลากรที่มีสิทธิ์เข้าถึงระบบจัดการขั้นสูงสุด (Privilege Insider) สามารถเปลี่ยนเป็นผู้โจมตีทางไซเบอร์เพื่อผลประโยชน์บางอย่างแก่ตนเอง

จากข้อมูลที่ได้รับ พบความเสี่ยงจากภัยคุกคามภายในดังนี้



ผู้คุกคามภายในองค์กร



อันดับ 1
ใช้ประโยชน์จากช่องโหว่ในระบบสารสนเทศภายในองค์กร



อันดับ 2
ส่งมัลแวร์เข้าสู่ระบบโดยการให้สื่อที่ถอดได้



อันดับ 3
ทำให้ข้อมูลลับรั่วไหลหรือไม่สามารถใช้งานได้โดยไม่ได้รับอนุญาต



บุคลากรภายในที่ได้รับความไว้วางใจสูง

อันดับ 1
ก่อให้เกิดการเปิดเผยข้อมูลที่สำคัญและ/หรือข้อมูลอ่อนไหวโดยผู้ใช้ที่ได้รับอนุญาต



อันดับ 2
เจาะหรือแทรกแซงซอฟต์แวร์ของระบบสารสนเทศที่มีความสำคัญขององค์กร



อันดับ 3
โจมตีด้วยมัลแวร์แบบเจาะจงเป้าหมายเพื่อยึดควบคุมระบบภายในและดึงข้อมูลออกจากองค์กร





บุคลากรภายในที่มีสิทธิ์สูงสุด

อันดับ 1
ก่อให้เกิดการเปิดเผยข้อมูลที่สำคัญและ/หรือข้อมูลอ่อนไหวโดยผู้ใช้ที่ได้รับอนุญาต

อันดับ 2
ยึดครองการเชื่อมต่อของผู้ใช้จากภายในองค์กร

อันดับ 3
วางแผนโจมตีไซเบอร์โดยใช้ทั้งช่องทางภายนอก ภายในและจากคู่ค้าในห่วงโซ่อุปทาน

นอกจากความเสี่ยงที่มีการกล่าวถึงจำนวนมากดังที่กล่าวไปข้างต้น ยังมีภัยคุกคามอื่น ๆ ที่มีระดับผลกระทบสูงและควรเฝ้าระวัง เช่น การละเมิดยึดครองข้อมูลสำคัญที่จำเป็นต่อการปฏิบัติภารกิจขององค์กร (Compromise mission-critical information) การแฝงบุคลากรที่มีเป้าหมายบ่อนทำลายเข้าไปในองค์กรหรือตำแหน่งที่ต้องการตลอดจนให้ความร่วมมือกับผู้ประสงค์ร้ายภายนอกเพื่อโจมตีองค์กร

เมื่อพิจารณาแรงจูงใจจากภัยคุกคามที่เกิดจากผู้ประสงค์ร้ายภายในหน่วยงาน ข้อมูลการประเมินความเสี่ยงของหน่วยงานบ่งบอกถึงเป้าหมายการโจมตีที่มุ่งเป้าไปยัง ข้อมูลสำคัญของหน่วยงานเป็นอันดับหนึ่งซอฟต์แวร์/ระบบสารสนเทศของหน่วยงานและสินทรัพย์ทางการเงินที่อาจได้เป็นค่าตอบแทนหลังจากดำเนินการโจมตีทางไซเบอร์ ตามลำดับ

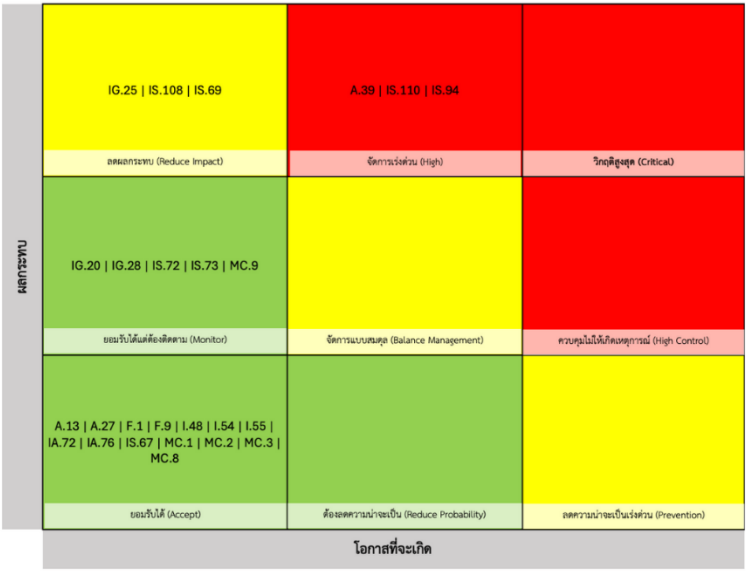
รายงานผลการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย พ.ศ. 2568

3.2 ผลการประเมินความเสี่ยงในระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3.2.1 ด้านความมั่นคงของรัฐ



หน่วยงานที่จัดเป็นด้านความมั่นคงปลอดภัยของรัฐ เป็นหน่วยงานที่ให้ความสำคัญต่อมิติความลับ (Confidential) เนื่องจากข้อมูลสารสนเทศของหน่วยงานสังกัดนี้อาจส่งผลกระทบโดยตรงต่อความเชื่อมั่น และอธิปไตยของประเทศ



ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

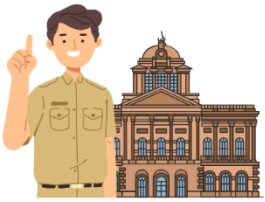
(1) ความเสี่ยงโดยส่วนใหญ่กล่าวถึงภัยคุกคามทางไซเบอร์ที่มุ่งพยายามเจาะระบบดักจับหรือพยายามโจรกรรมข้อมูลสำคัญ

(2) ความเสี่ยงที่ระบุโดยส่วนใหญ่จัดเป็นความเสี่ยงระดับต่ำและอยู่ในเกณฑ์ที่สามารถยอมรับได้

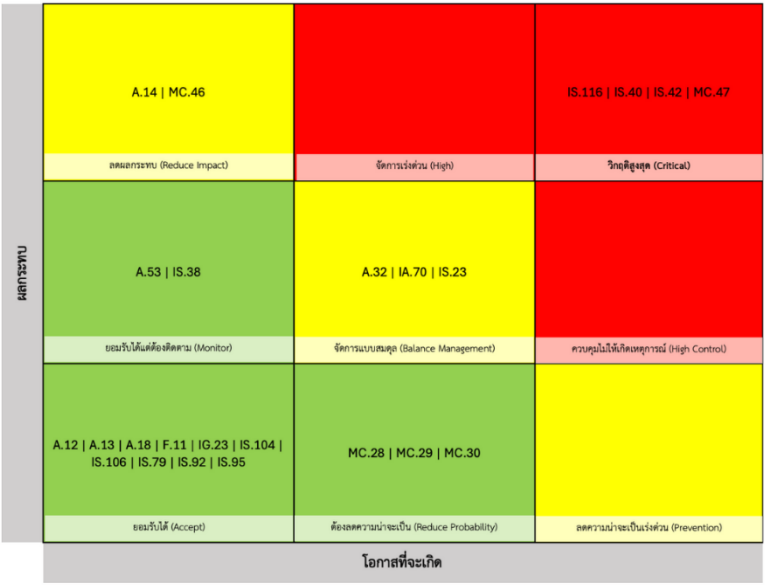
(3) ความเสี่ยงที่จัดเป็นระดับสูงและควรจัดการโดยเร็ว ประกอบด้วย

- การที่ผู้ประสงค์ร้ายจากภายนอกใช้ช่องโหว่จากการตั้งค่าระบบอ่อนแอเข้ามาทำลายข้อมูลสำคัญ หรือระบบสารสนเทศที่เกี่ยวกับสินทรัพย์ด้านการจัดการสารสนเทศและเทคโนโลยี
- การบุกรุกเข้ามาในระบบหรือเครือข่ายโดยไม่ได้รับอนุญาตโดยใช้ช่องโหว่จากซอฟต์แวร์และอุปกรณ์เครือข่ายเพื่อเข้าถึงสินทรัพย์ที่เกี่ยวกับการจัดการสารสนเทศและเทคโนโลยี และการบริหารจัดการเชิงบริหาร เพื่อโจรกรรมข้อมูลที่มีการส่งระหว่างระบบหรือในระบบเครือข่ายนั้น ๆ
- ผู้ประสงค์ร้ายจากภายนอกพยายามฉวยโอกาสโจรกรรมข้อมูลที่เกี่ยวกับการดำเนินการด้านข่าวกรองจากระบบสารสนเทศ หรือการทำลายข้อมูลที่ไม่สมบูรณ์ โดยอาศัยช่องโหว่จากซอฟต์แวร์และบุคคลที่ขาดความระมัดระวังหรือประมาท
- ผู้ประสงค์ร้ายจากภายนอกส่งมัลแวร์ที่มุ่งเป้าโจมตีระบบที่เกี่ยวข้องกับทรัพยากรโดยอาศัยช่องโหว่จากซอฟต์แวร์

3.2.2 ด้านบริการภาครัฐที่สำคัญ



หน่วยงานที่จัดเป็นด้านบริการภาครัฐที่สำคัญเป็นหน่วยงานที่มีความใกล้ชิดกับประชาชน และครอบครองข้อมูลเกี่ยวกับประชาชนมากที่สุดซึ่งเป็นข้อมูลที่มีความจำเป็นในหลายภาคส่วนในการให้บริการประชาชน จึงมุ่งเน้นความพร้อมใช้ความถูกต้องของข้อมูลและต้องรักษาความลับของข้อมูลที่มีประเด็นอ่อนไหวไม่ให้รั่วไหล



ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงจากภัยคุกคามทางไซเบอร์พบว่าโดยส่วนใหญ่ เป็นการพยายามโจรกรรมข้อมูล เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการโจมตีความพร้อมใช้ของระบบด้วยวิธีต่าง ๆ

(2) ความเสี่ยงโดยส่วนใหญ่จัดอยู่ในเกณฑ์ที่ยอมรับได้ โดยเกิดจาก การโจมตีแบบ DDoS การบุกรุก/เข้าถึงโดยมิชอบ ไปยังสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(3) ความพยายามเจาะระบบ กับการส่งมัลแวร์แบบมุ่งเป้าไปยังระบบภายในองค์กร โดยใช้วิธีการโจมตีหรือแทรกผ่านไฟล์/โปรแกรม มีโอกาสเกิดบ่อยแต่ไม่ส่งผลกระทบอย่างมีนัยสำคัญ

(4) ความเสี่ยงฯ ที่สำคัญที่หน่วยงานประเมินแล้วว่าควรต้องจัดการทันที ได้แก่

- ผู้ประสงค์ร้ายจากภายนอกบุกรุกเข้าระบบและเปิดเผยข้อมูลอ่อนไหวที่เกี่ยวกับการจัดการข้อมูลสารสนเทศและเทคโนโลยีกับข้อมูลทั่วไปของรัฐบาลโดยใช้ช่องโหว่จากซอฟต์แวร์
- ผู้ประสงค์ร้ายจากภายนอกฝังมัลแวร์ชนิดพิเศษที่ออกแบบมาเพื่อโจมตีระบบภายในองค์กรที่เกี่ยวกับข้อมูลทั่วไปของรัฐบาล โดยอาศัยช่องโหว่จากซอฟต์แวร์ของระบบนั้น
- ผู้ประสงค์ร้ายจากภายนอกส่งมัลแวร์แบบมุ่งเป้าหมายเพื่อควบคุมระบบสารสนเทศและสกัดข้อมูลเกี่ยวกับข้อมูลทั่วไปของรัฐบาล โดยอาศัยช่องโหว่จากซอฟต์แวร์ของระบบ
- ช่องโหว่จากการขาดระเบียบปฏิบัติในการแก้ไขช่องโหว่อาจเปิดโอกาสให้ผู้ประสงค์ร้ายจากภายนอกองค์กรใช้ประโยชน์จากช่องโหว่ของระบบที่เกี่ยวกับการจัดการสารสนเทศและเทคโนโลยี เพื่อโจมตี บุกรุก หรือละเมิดความปลอดภัยได้ในภายหลัง

(5) ความเสี่ยงในระดับปานกลางที่ควรเฝ้าระวังไม่ให้ขยายผลไปสู่ความเสี่ยงสูงส่วนใหญ่มีสาเหตุเกิดจากช่องโหว่ด้านกระบวนการและระเบียบปฏิบัติ หรือ ขาดความชำนาญในการปฏิบัติตามระเบียบปฏิบัติของหน่วยงานในการตอบสนองกับเหตุการณ์ภัยคุกคามทางไซเบอร์

3.2.3 ด้านการเงินการธนาคาร

หน่วยงานที่จัดเป็นหน่วยงานด้านการเงินการธนาคารเป็นหน่วยงานที่มีความใกล้ชิดกับสินทรัพย์ทางการเงินจึงให้ความสำคัญต่อมิติความพร้อมใช้งาน (Availability) และความถูกต้องครบถ้วน (Integrity) เนื่องจากระบบสารสนเทศของหน่วยงานสังกัดนี้ต้องสามารถให้บริการได้อย่างต่อเนื่องตลอดเวลา และข้อมูลทางการเงินต้องมีความแม่นยำถูกต้อง หากเกิดการหยุดชะงักหรือข้อมูลผิดพลาดอาจส่งผลกระทบโดยตรงต่อความเชื่อมั่นของระบบเศรษฐกิจและการเงินของประเทศ





ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงจากภัยคุกคามทางไซเบอร์โดยภาพรวมจับกลุ่มอยู่ในระดับผลกระทบปานกลาง-สูง โดยที่โอกาสเกิดอยู่ในระดับต่ำ ซึ่งโดยส่วนใหญ่เป็นการโจมตีความพร้อมใช้ของระบบการพยายามโจมตีเพื่อเข้าถึงข้อมูลและใช้มัลแวร์ลักษณะต่าง ๆ

(2) ความเสี่ยงฯ ทั้งหมดถูกควบคุมให้อยู่ไม่เกินในระดับปานกลาง และไม่มีความเสี่ยงระดับสูงปรากฏในทะเบียนความเสี่ยง ดังนั้นแนวทางดำเนินการสำคัญคือการควบคุมระดับผลกระทบของความเสี่ยงเหล่านั้นลง

(3) เนื่องจากเป็นภาคส่วนที่มีการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสูงจึงมีความเสี่ยงจากการฉ้อโกง มุ่งเป้าไปที่ช่องโหว่จากบุคคลเพื่อหลอกล่อหรือเข้าถึงข้อมูลโดยมิชอบ รวมถึงอาจฉวยโอกาสจากช่องโหว่ของระบบที่ไม่สามารถคัดกรองการโจมตีฟิชชิ่ง เพื่อขโมยข้อมูลลับ

(4) มีการกล่าวถึงความเสี่ยงที่เกี่ยวกับการแฝงตัวเป็นผู้ให้บริการ (Supplier) เพื่อโจมตีหน่วยงานทั้งการดัดแปลง/ฝังมัลแวร์เข้ามาในอุปกรณ์ หรือ เปิดหน่วยงานปลอมเพื่อปฏิบัติการโจมตีทางไซเบอร์

(5) การโจมตีโดยการเจาะเข้าเว็บไซต์ / เว็บแอป ที่เปิดเผยข้อมูลสาธารณะและเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ถูกประเมินระดับผลกระทบในระดับสูงเนื่องจากส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของภาคส่วนที่มีขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยในระดับสูง

(6) ความเสี่ยงฯ ที่สำคัญที่หน่วยงานประเมินแล้วว่าควรต้องเฝ้าระวังและลดผลกระทบ ได้แก่

- การแพร่กระจายของมัลแวร์ผ่านการใช้สื่อแบบถอดประกอบได้ เช่น USB โดยบุคลากรภายในองค์กรทั้งในระดับทั่วไปและตำแหน่งบริหาร ที่อาศัยช่องโหว่จากบุคลากรที่ขาดการระมัดระวังภัย – ความตระหนักด้านไซเบอร์
- การโจมตีโดยใช้มัลแวร์ที่ถูกดัดแปลง หรือ ชนิดพิเศษที่ถูกสร้างขึ้นเพื่อโจมตีระบบควบคุมทางไซเบอร์และสินทรัพย์ที่เกี่ยวกับการจัดการทางการเงิน โดยเฉพาะการใช้ช่องโหว่จากซอฟต์แวร์ที่ยังไม่สามารถตรวจจับมัลแวร์ประเภทนั้น ๆ ได้
- การโจมตี DDoS เพื่อทำลายสินทรัพย์ที่เกี่ยวกับการจัดการทางการเงินและการจัดการสารสนเทศและเทคโนโลยี โดยใช้ช่องโหว่ที่ไม่สามารถจำแนกคำขอใช้งานระบบจากการโจมตีหรือผู้ใช้งานจริงได้
- การที่บุคลากรภายในหน่วยงานถูกขู่กรรโชก ชักจูง หรือกระทำให้ความสามารถของระบบ/ฟังก์ชันถูกแทรกแซงจนประสิทธิภาพต่ำลง - ถูกทำลาย
- บุคคลและกลุ่มบุคคลภายนอกเจาะเว็บไซต์และเปลี่ยนเนื้อหาโดยใช้ช่องโหว่จากซอฟต์แวร์
- การโจมตีสินทรัพย์ที่เกี่ยวกับการจัดการทางการเงินโดยใช้ Zero-Day
- ผู้ประสงค์ร้ายจากภายนอกสามารถเข้าถึงสินทรัพย์และระบบสำคัญผ่านการเข้าถึงทางกายภาพ โดยใช้ข้อมูลส่วนบุคคล

3.2.4 ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม



หน่วยงานที่จัดเป็นด้านเทคโนโลยีสารสนเทศและโทรคมนาคม มีความสำคัญเนื่องจากโครงสร้างพื้นฐานด้านดิจิทัลและเครือข่ายสื่อสารของหน่วยงานสังกัดนี้เป็นกลไกเชื่อมโยงระบบสารสนเทศและบริการทั้งหมดของประเทศหากเกิดการหยุดชะงักหรือไม่สามารถให้บริการได้ อาจส่งผลกระทบอย่างกว้างขวางต่อการดำเนินงานของทุกภาคส่วน (Sector) และชีวิตประจำวันของประชาชน

ผลกระทบ \ โอกาสที่จะเกิด	ต้องลดความน่าจะเป็น (Reduce Probability)	ลดความน่าจะเป็นเร่งด่วน (Prevention)
ลดผลกระทบ (Reduce Impact)	จัดการเร่งด่วน (High)	วิกฤติสูงสุด (Critical)
A.21 | A.59 | F.5 | IA.61		I.60 | IS.66
ยอมรับได้แต่ต้องติดตาม (Monitor)	จัดการแบบสมดุล (Balance Management)	ควบคุมไม่ให้เกิดเหตุการณ์ (High Control)
A.23 | A.45 | A.67 | IA.29 | IA.30 | IG.10 | IG.11 | IS.1	IS.10	AC.6 | I.12 | IS.13 | IS.49 | IS.6 | MC.33
ยอมรับได้ (Accept)	ต้องลดความน่าจะเป็น (Reduce Probability)	ลดความน่าจะเป็นเร่งด่วน (Prevention)
A.24 | A.30 | A.46 | F.15 | IA.12 | IA.15 | IA.40 | IA.41 | IA.52 | IA.53 | IA.54 | IG.13 | IG.3 | IS.2 | IS.91 | IS.93 | MC.22 | MC.37	IA.16	

ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงจากภัยคุกคามทางไซเบอร์โดยภาพรวมจับกลุ่มอยู่ในระดับต่ำที่ยอมรับได้ ซึ่งโดยส่วนใหญ่เป็นการพยายามเจาะระบบโจมตีความพร้อมด้วยมัลแวร์ และการโจมตีเพื่อโจรกรรมข้อมูล

(2) ผู้ประสงค์ร้ายทั้งแบบบุคคลหรือรวมกลุ่มอาจดำเนินการหลอกลวง สร้างสถานการณ์เพื่อเข้าถึงข้อมูลสำคัญ (Social Engineer) โดยอาศัยช่องโหว่จากบุคคล หรือระบบที่ขาดคำสั่งคัดกรองผู้ใช้งานผิดปกติ

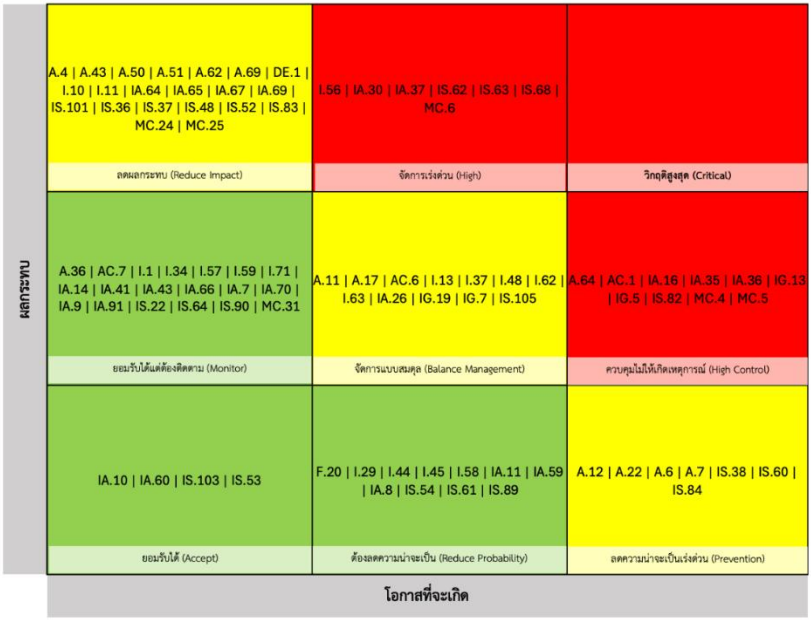
(3) ความเสี่ยงที่ต้องเร่งจัดการในทันที ประกอบด้วย

- กลุ่มผู้ประสงค์ร้ายใช้ช่องจากเฟิร์มแวร์ และบัญชีของผู้มีสิทธิ์เข้าถึงระบบเพื่อเข้าถึงสิ่งปลูกสร้างและสาธารณูปโภคของหน่วยงานในพื้นที่สำคัญได้
- ผู้ประสงค์ร้ายภายนอกขโมยหรือเก็บกู้ข้อมูลและอุปกรณ์จากระบบสารสนเทศเมื่อมีโอกาส
- การใช้มัลแวร์ที่ดัดแปลงเข้าไปในระบบภายในขององค์กร เช่น การเข้ารหัสข้อมูล ระบบควบคุมเครือข่ายหลัก เรียกค่าไถ่ และทำให้บริการชะงัก เป็นต้น

3.2.5 ด้านการขนส่งและโลจิสติกส์



หน่วยงานที่จัดเป็นด้านการขนส่งและโลจิสติกส์ ถือครองสินทรัพย์ด้านระบบสารสนเทศที่เป็นกลไกสำคัญในการควบคุมและประสานงานการเคลื่อนย้ายสินค้าและบริการทั่วประเทศ หากเกิดการหยุดชะงักหรือข้อมูลผิดพลาดอาจส่งผลกระทบโดยตรงต่อห่วงโซ่อุปทานและความปลอดภัยในการสัญจร



ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงโดยภายพรวมอยู่ในโอกาสเกิดต่ำ แต่มีผลกระทบปานกลาง - สูง ซึ่งโดยภาพรวมเป็นพยายามบุกรุกระบบ การมุ่งเป้าหมายที่ข้อมูลสำคัญ และการโจมตีความพร้อมใช้

(2) ความเสี่ยงฯ ประเภทการพยายามเข้าถึงระบบนั้นมีจำนวนมากที่สุด ซึ่งเกิดจากการใช้ประโยชน์จากการตั้งค่าอ่อนแอทำให้ข้อมูลรั่วไหลสู่อินเทอร์เน็ตและการใช้ประโยชน์จากช่องโหว่ที่มีอยู่ในระบบภายในองค์กร รวมถึงช่องโหว่แบบ Zero-Day เพื่อโจมตีสินทรัพย์ที่เกี่ยวกับการจัดการเทคโนโลยี

(1) มีการกล่าวถึงความเสี่ยงที่บุคลากรภายในจะเป็นส่วนหนึ่งของการโจมตีแบบแคมเพน (Campaign) ร่วมกับผู้ประสงค์ร้ายภายนอก โดยใช้ช่องโหว่จากกิจวัตรของฝ่ายบริหารเปิดโอกาสให้โจมตีร่วมกับผู้ประสงค์ร้ายภายนอก หรือใช้ประโยชน์จากสิทธิ์การเข้าถึงพื้นที่ทางกายภาพเพื่อให้กลุ่มผู้ประสงค์ร้ายเข้าสู่พื้นที่ขององค์กรได้

(2) ความเสี่ยงจากการที่ผู้ประสงค์ร้ายจากภายในและภายนอกประเทศเข้าถึงสินทรัพย์ที่เกี่ยวกับการจัดการเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต เป็นความเสี่ยงที่ถูกระบุมากที่สุด

(3) เนื่องจากสินทรัพย์และระบบของหน่วยงานสังกัดโลจิสติกส์ ต้องมีการเชื่อมโยงกับระบบภายนอกเพื่อให้บริการแบบ End-to-End จึงมีความเสี่ยงที่ผู้ประสงค์ร้ายจะดักจับข้อมูลอ่อนไหวระหว่างการส่งข้อมูล (Man-in-the-middle) และอาจฉวยโอกาสขโมยข้อมูลจากองค์ประกอบของระบบ/อุปกรณ์ เพื่อใช้ประโยชน์ในการโจมตี หรือเปิดเผยข้อมูลโดยมิชอบ

(4) สืบเนื่องจากการเชื่อมโยงการให้บริการภายนอกเพื่อเสริมประสิทธิภาพการให้บริการ ส่งให้พื้นที่การโจมตีเพิ่มขึ้น อาจมีความเสี่ยงที่ผู้ประสงค์ร้ายจะโจมตีสินทรัพย์ที่เกี่ยวกับการขนส่งและเทคโนโลยีสารสนเทศให้ไม่สามารถใช้งานหรือให้บริการ จนเกิดความเสียหายได้

(5) ความเสี่ยงฯ ที่ต้องจัดการอย่างเร่งด่วน มีรายละเอียดดังนี้

- ผู้ประสงค์ร้ายจากภายนอกใช้ช่องโหว่จากบุคคลเพื่อแทรกแซงความสามารถการให้บริการที่เกี่ยวข้องกับการขนส่ง
- ผู้ประสงค์ร้ายภายนอกใช้ช่องโหว่จากบุคคลเพื่อโจมตีแบบฟิชชิ่งเพื่อเข้าถึงข้อมูลเกี่ยวกับการขนส่ง
- ผู้ประสงค์ร้ายภายในองค์กรเปิดช่องโหว่ที่เกี่ยวกับกิจวัตรของฝ่ายบริหารเพื่อให้ผู้ประสงค์ร้าย โจมตีร่วมกับผู้ประสงค์ร้ายภายนอก
- ผู้ประสงค์ร้ายภายในองค์กรอาศัยความไว้วางใจกับเพื่อนร่วมงานเพื่อเข้าถึงข้อมูลสำคัญที่เกี่ยวกับการขนส่ง (Social Engineering)
- ผู้ประสงค์ร้ายฉวยโอกาสขโมยข้อมูลสำคัญที่เกี่ยวกับการเงิน หรือขนส่ง หรือการจัดการระบบสารสนเทศ จากระบบ หรือ องค์ประกอบของระบบสารสนเทศ

3.2.6 ด้านพลังงานและสาธารณูปโภค



หน่วยงานที่จัดเป็นด้านพลังงานและสาธารณูปโภค มีการควบคุมโครงสร้างพื้นฐานสำคัญและมีความเชื่อมโยงในทุกภาคส่วน จำเป็นต่อการดำรงชีวิตและการดำเนินงานของประเทศ เช่น ระบบไฟฟ้า น้ำประปา และพลังงาน หากเกิดการหยุดชะงักอาจส่งผลกระทบอย่างรุนแรงต่อความปลอดภัยและคุณภาพชีวิตของประชาชนทั้งประเทศ

ผลกระทบ	โอกาสที่จะเกิด		
	ยอมรับได้ (Accept)	ต้องลดความน่าจะเป็น (Reduce Probability)	ลดความน่าจะเป็นเร่งด่วน (Prevention)
ยอมรับได้แต่ต้องติดตาม (Monitor)	A.16 | A.33 | F.17 | I.43 | I.51 | IA.19 | IA.20 | IA.22 | IA.81 | IA.82 | IG.12 | IG.14 | IS.118 | IS.119 | IS.19 | IS.28 | IS.55 | IS.56 | IS.75 | MC.50 | MC.51 | MC.54 | MC.56 | MC.58 | MC.60		
จัดการแบบสมดุล (Balance Management)	A.28 | A.31 | A.34 | A.40 | A.70 | AC.10 | F.22 | I.16 | I.17 | I.18 | I.42 | I.5 | I.6 | IA.46 | IA.5 | IA.83 | IS.124 | IS.125 | IS.26 | IS.43 | IS.74 | IS.76 | MC.48 | MC.49 | MC.52 | MC.53 | MC.55 | MC.57	IS.120	
ควบคุมไม่ให้เกิดเหตุการณ์ (High Control)			
ลดผลกระทบ (Reduce Impact)	IG.15		
จัดการเร่งด่วน (High)			
วิกฤติสูงสุด (Critical)	A.1 | A.2 | A.4 | A.44 | AC.6 | F.15 | F.7 | I.23 | I.26 | I.27 | I.39 | I.7 | IA.34 | IA.41 | IA.51 | IA.53 | IA.55 | IA.72 | IA.74 | IG.2 | IG.22 | IG.24 | IG.26 | IG.27 | IS.106 | IS.13 | IS.14 | IS.37 | IS.40 | IS.53 | IS.59 | IS.80 | IS.84 | IS.85 | MC.21 | MC.32 | MC.33 | MC.34 | MC.40		

ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงฯ โดยภาพรวมรวมกลุ่มในระดับที่ยอมรับได้ และระดับวิกฤติซึ่งต้องเร่งดำเนินการแก้ไขทันที ซึ่งความเสี่ยงในกลุ่มนี้มุ่งโจมตีสินทรัพย์ที่เกี่ยวกับการจัดการเทคโนโลยีสารสนเทศทั้งหมด

(2) การใช้ประโยชน์จากช่องโหว่ของระบบภายในหน่วยงาน และการเข้าถึงโดยไม่ได้รับอนุญาต เป็นความเสี่ยงที่ถูกกล่าวถึงมากที่สุด ซึ่งมีระดับความเสี่ยงจัดเป็นระดับวิกฤติ

(3) มีความเสี่ยงที่ผู้ประสงค์ร้ายที่มีสิทธิ์ขั้นสูงและสูงสุดอาจทำการเปิดเผยข้อมูลความลับหรืออ่อนไหวโดยใช้บัญชีผู้ใช้งานซึ่งผ่านกลไกการตรวจสอบของระบบได้โดยง่าย

(4) มีความเสี่ยงที่ผู้ประสงค์ร้ายและภายในทำการแทรกแซง แก้ไขข้อมูลสำคัญเกี่ยวกับพลังงาน ให้เกิดความเสียหาย ในกรณีที่มีการใช้งานข้อมูลเพื่อฝึกฝน Machine Learning อาจทำให้ผลการวิเคราะห์จำแนก หรือทำนายผลมีความแม่นยำลดลง

(6) ผู้ประสงค์ร้ายภายนอกหรือผู้ประสงค์ร้ายภายในอาจฝังมัลแวร์ในสื่อแบบถอดได้ เพื่อแพร่กระจายในระบบเครือข่ายของหน่วยงานเพื่อโจมตีสินทรัพย์ที่เกี่ยวกับพลังงานโดยใช้ช่องโหว่จากซอฟต์แวร์

(7) ผู้ประสงค์ร้ายจากภายนอกอาจโจมตีสินทรัพย์ที่เกี่ยวกับระบบบริหารพลังงาน ผ่านการโจมตีผู้ให้บริการหน่วยงานและแฝงเข้าในเครือข่ายภายในซึ่งถูกจัดเป็นระดับต่ำ

(8) ความเสี่ยงระดับสูงที่หน่วยงานควรต้องเร่งจัดการโดยทันที มีรายละเอียดดังนี้

- บุคคลภายนอกและกลุ่มผู้ประสงค์ร้ายที่รวมตัวกันชั่วคราวดำเนินการการโจมตีแบบปฏิเสธการให้บริการ (Denial of Service) ทั้งแบบง่ายและแบบมุ่งเป้าทำให้สินทรัพย์ที่เกี่ยวกับการจัดการเทคโนโลยีสารสนเทศลดประสิทธิภาพหรือถูกทำลาย
- กลุ่มผู้ประสงค์ร้ายจากภายนอก ใช้ประโยชน์จากช่องโหว่ด้านซอฟต์แวร์ทำให้บริการหรือระบบที่ผู้โจมตีเลือกไว้ทำงานช้าลงหรือไม่สามารถให้บริการได้
- ผู้ประสงค์ร้ายโจมตีแบบฟิชชิ่งหลอกล่อบุคคลที่ขาดความตระหนักด้านความปลอดภัยเพื่อโจรกรรมข้อมูลลับ - ข้อมูลอ่อนไหว
- ผู้ประสงค์ร้ายทั้งจากภายนอกและภายในหน่วยงานอาจใช้ช่องโหว่จากซอฟต์แวร์ที่มีมาตรการคัดกรองไม่เพียงพอ บุกรุกเข้ายึดครองซอฟต์แวร์ของระบบสารสนเทศที่สำคัญ
- ผู้ประสงค์ร้ายใช้ประโยชน์การตั้งค่าระบบบกพร่องทำให้ข้อมูลสำคัญถูกเปิดเผยสู่อินเทอร์เน็ตโดยมิชอบ
- บุคคลผู้ประสงค์ร้ายทั้งจากภายนอก หรือที่รวมกลุ่มกันชั่วคราวใช้ช่องโหว่ของซอฟต์แวร์ที่ถูกค้นพบไม่นานเพื่อโจมตีสินทรัพย์ที่เกี่ยวกับการจัดการเทคโนโลยีสารสนเทศ และอาจทำให้ผู้ประสงค์ร้ายเข้าถึงโดยไม่ได้รับอนุญาต

3.2.7 ด้านสาธารณสุข



หน่วยงานที่จัดเป็นด้านสาธารณสุขเป็นหน่วยงานที่ให้ความสำคัญต่อมิติความลับ ความพร้อมใช้งาน และความถูกต้องครบถ้วน เนื่องจากสังกัดนี้เกี่ยวข้องกับข้อมูลส่วนบุคคลด้านสุขภาพที่ละเอียดอ่อน ต้องสามารถให้บริการรักษาพยาบาลได้อย่างต่อเนื่อง และข้อมูลทางการแพทย์ต้องมีความแม่นยำ หากเกิดการรั่วไหล หยุดชะงัก หรือข้อมูลผิดพลาดอาจส่งผล กระทบโดยตรงต่อชีวิตและความปลอดภัยของผู้ป่วย

ผลกระทบ			
	A.10 | A.39 | I.24 | I.25 | I.3 | I.69 | I.70 | IA.50 | IA.70 | IA.71 | IA.84 | IG.1 | IS.104 | IS.30 | IS.38 | IS.41 | IS.77 | MC.61	IS.29 | IS.44 | IS.58 | IS.87	A.49 | A.8 | F.18 | F.19 | I.72 | IA.49 | IA.88 | IA.90 | IG.16 | IS.46 | IS.47 | MC.63
	ลดผลกระทบ (Reduce Impact)	จัดการเร่งด่วน (High)	วิกฤติสูงสุด (Critical)
	A.58 | A.73 | I.36 | I.52 | IA.13 | IA.68 | IS.20 | IS.88 | MC.62	A.72 | IS.21	A.71 | IA.56 | IA.57
	ยอมรับได้แต่ต้องติดตาม (Monitor)	จัดการแบบสมดุล (Balance Management)	ควบคุมไม่ให้เกิดเหตุการณ์ (High Control)
	A.47 | DE.2 | I.19 | I.4 | IA.48 | IA.87 | IG.4 | IS.45 | IS.57	IA.32 | IS.127	I.20 | I.53
	ยอมรับได้ (Accept)	ต้องลดความน่าจะเป็น (Reduce Probability)	ลดความน่าจะเป็นเร่งด่วน (Prevention)
		โอกาสที่จะเกิด	

ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงฯ โดยภาพรวมมีการรวมกลุ่มในระดับที่ปานกลาง และระดับวิกฤติซึ่งต้องเร่งดำเนินการแก้ไขทันที ซึ่งความเสี่ยงในกลุ่มนี้มุ่งโจมตีสินทรัพย์ที่เกี่ยวกับสุขภาพทั้งหมด

(2) การใช้ประโยชน์จากช่องโหว่ของระบบภายในหน่วยงาน และพยายามขโมยข้อมูลเกี่ยวกับสุขภาพเป็นความเสี่ยงที่ถูกกล่าวถึงมากที่สุด

(3) ความเสี่ยงฯ ที่ผู้ประสงค์ร้ายภายนอกจะเข้าโจมตีทำให้บริการหรือระบบที่ผู้โจมตีเลือกไว้ทำงานช้าลงหรือไม่สามารถให้บริการได้โดยใช้ช่องโหว่จากซอฟต์แวร์ การตั้งค่า กระบวนปฏิบัติและฮาร์ดแวร์

(4) ผู้ประสงค์ร้ายดำเนินการโจมตีแบบฟิชชิ่ง หรือ วิศวกรรมทางสังคม (Social Engineer) โดยใช้ช่องโหว่จากความบกพร่องของระเบียบปฏิบัติและการขาดความตระหนักรู้ด้านไซเบอร์เพื่อเข้าถึงสินทรัพย์ด้านสุขภาพ

(5) ช่องโหว่จากระบบสารสนเทศภายในองค์กรอาจถูกใช้ประโยชน์ในการโจมตีทางไซเบอร์เพื่อถึงข้อมูลด้านสุขภาพและการจัดการระบบสารสนเทศ รวมถึงการลักลอบปรับปรุงข้อมูลเหล่านั้นให้เกิดความเสียหาย

(6) ความเสี่ยงที่ต้องจัดการโดยทันที มีรายละเอียดดังต่อไปนี้

- ผู้ประสงค์ร้ายจากภายนอกอาศัยความบกพร่องของในกระบวนการและระเบียบปฏิบัติเพื่อทำให้บริการหรือระบบสุขภาพที่ผู้โจมตีเลือกไว้ทำงานช้าลงหรือไม่สามารถให้บริการได้
- ผู้ประสงค์ร้ายภายนอกใช้ประโยชน์จากช่องโหว่ของเฟิร์มแวร์ดำเนินการโจมตีแบบ DoS
- ผู้ประสงค์ร้ายภายนอกใช้ช่องโหว่จากระบบสารสนเทศภายในองค์กรที่อาจเกิดจากการตั้งค่าระบบผิดพลาดเพื่อโจมตีสินทรัพย์ที่เกี่ยวกับสุขภาพ
- ผู้ประสงค์ร้ายภายนอกองค์กรอาศัยช่องโหว่จากระเบียบปฏิบัติและความตระหนักรู้ของบุคลากร เข้าถึงข้อมูลสำคัญและเปิดเผยข้อมูลเกี่ยวกับสุขภาพ
- ผู้ประสงค์ร้ายจากภายนอกอาจส่งมัลแวร์ที่เป็นที่รู้จัก เช่น Ransomware เข้ามาในระบบภายในที่เกี่ยวกับสุขภาพ โดยอาศัยช่องโหว่จากบุคลากร

3.3 ผลการประเมินความเสี่ยงระดับกลุ่มหน่วยงานของรัฐ



หน่วยงานที่จัดเป็นหน่วยงานของรัฐ (ที่ไม่ใช่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เป็นหน่วยงานที่ให้บริการสาธารณะและจัดเก็บข้อมูลราชการที่ต้องมีความน่าเชื่อถือและสามารถเข้าถึงได้ตามสิทธิของประชาชน หากเกิดข้อมูลผิดพลาดหรือการหยุดชะงักอาจส่งผลกระทบต่อความเชื่อมั่นในการบริหารราชการ การควบคุมกำกับดูแลและสิทธิประโยชน์ของประชาชน

ผลกระทบ			
		IA.41 | IA.53 | IS.17	
	ลดผลกระทบ (Reduce Impact)	จัดการเร่งด่วน (High)	วิกฤติสูงสุด (Critical)
	A.29 | F.4 | I.15 | I.3 | I.32 | I.33 | I.50 | I.68 | IA.4 | IA.58 | IA.62 | IA.77 | IA.78 | IS.107 | IS.114 | IS.117 | IS.25 | MC.43 | MC.44	IS.113 | IS.115 | MC.35 | MC.39 | MC.45	IS.108 | MC.34
	ยอมรับได้แต่ต้องติดตาม (Monitor)	จัดการแบบสมดุล (Balance Management)	ควบคุมไม่ให้เกิดเหตุการณ์ (High Control)
	A.48 | A.9 | AC.4 | I.30 | I.31 | I.61 | I.66 | IS.18 | IS.23 | IS.70 | IS.9 | MC.36	A.18 | AC.10 | IA.18 | IS.119	A.26 | F.16 | IS.106 | IS.111 | IS.50 | MC.42
	ยอมรับได้ (Accept)	ต้องลดความน่าจะเป็น (Reduce Probability)	ลดความน่าจะเป็นเร่งด่วน (Prevention)
		โอกาสที่จะเกิด	

ประเด็นโดยสรุปจากเมทริกซ์ความเสี่ยงข้างต้น มีรายละเอียดดังต่อไปนี้

(1) ความเสี่ยงฯ โดยภาพรวม รวมกลุ่มอยู่ในระดับที่ยอมรับได้ โดยส่วนใหญ่เป็นความพยายามโจมตีข้อมูลและการพยายามบุกรุกระบบ

(2) ด้วยช่องโหว่ที่อาจเกิดขึ้นในการพัฒนาระบบสารสนเทศและเว็บไซต์ ทำให้ระบบถูกโจมตีหรือบุกรุกเข้าไปแก้ไขเว็บไซต์แสดงผลโดยไม่ได้รับอนุญาต

(3) เนื่องจากแนวโน้มการทำงานผ่านระบบดิจิทัล ในอุปกรณ์พกพา เช่น คอมพิวเตอร์พกพาและสมาร์ทโฟน เป็นต้น ทำให้ผู้ประสงค์ร้ายจากภายนอกอาจโจมตีอุปกรณ์เหล่านั้นเพื่อใช้บุกรุกหรือเข้าถึงข้อมูลสำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่งบุคคลที่มีสิทธิ์เข้าถึงระบบในขั้นสูงที่เกี่ยวกับสินทรัพย์ด้านการจัดการระบบสารสนเทศ

(4) จากรายการความเสี่ยงพบว่ามีการกล่าวถึงการใช้ประโยชน์จากช่องโหว่ในระบบสารสนเทศภายในองค์กรและมีการบุกรุก/เข้าถึงสินทรัพยโดยไม่ได้รับอนุญาต ซึ่งมีความเสี่ยงอาจทำให้ข้อมูลสำคัญของหน่วยงานถูกแก้ไข - เปิดเผยสู่ภายนอกโดยไม่ได้รับอนุญาต

(5) ความเสี่ยงจากการโจมตีด้วยมัลแวร์ มีความเสี่ยงระดับต่ำ - ปานกลาง ทั้งมัลแวร์ที่เป็นที่รู้จักโดยทั่วไป มัลแวร์ชนิดพิเศษ มัลแวร์ที่ดัดแปลงแล้ว ผ่านช่องโหว่จากซอฟต์แวร์

(6) ความเสี่ยงฯ ที่มีระดับสูงและต้องจัดการโดยเร่งด่วน มีรายละเอียดดังนี้

- ผู้ประสงค์ร้ายจากภายนอกองค์กรเข้าถึงสินทรัพย์โดยมิชอบโดยใช้ช่องโหว่จากอุปกรณ์สื่อสารของหน่วยงานที่ขาดคุณสมบัติการตรวจจับและคัดกรองผู้บุกรุก
- ผู้ประสงค์ร้ายจากภายนอกองค์กรเข้าถึงอาจใช้ช่องโหว่ที่เพิ่งค้นพบเข้าโจมตีระบบ/บุกรุกระบบที่เกี่ยวข้องกับสินทรัพย์ด้านเทคโนโลยีดิจิทัล
- ผู้ประสงค์ร้ายภายนอกองค์กรใช้ประโยชน์จากการตั้งค่าอ่อนแอ ไม่สอดคล้องตามมาตรฐานทางไซเบอร์ เป็นเหตุให้ข้อมูลอาจเปิดเผยสู่อินเทอร์เน็ต

4. ข้อเสนอแนะเชิงนโยบายเพื่อการบริหารความเสี่ยง (Risk Mitigation)



ข้อเสนอแนะเชิงนโยบาย เพื่อการบริหารความเสี่ยง (Risk Mitigation)

4.1 ข้อเสนอแนะเชิงนโยบายเพื่อบริหารความเสี่ยง (Risk Mitigation) ในระดับประเทศ



การพัฒนามาตรฐานคำนิยาม

พัฒนามาตรฐานคำนิยามองค์ประกอบของความเสี่ยง พร้อมกำหนดรหัสอ้างอิงสำหรับเทียบองค์ประกอบที่เหมือนกันในทุกหน่วยงาน

กฎหมาย/นโยบาย

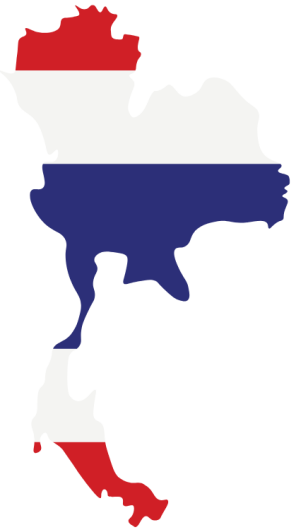
- แผนแม่บทและยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับชาติที่สอดคล้องกับสถานการณ์ภัยคุกคามปัจจุบัน
- ส่งเสริมให้มีการกำหนดตัวชี้วัดความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ เพื่อใช้ในการประเมินความก้าวหน้าและการปรับปรุงนโยบาย
- บังคับใช้กฎหมายอย่างเคร่งครัด
- ปรับปรุงมาตรการ/นโยบายป้องกันความเสี่ยงในเทคโนโลยีที่กำลังจะมา อาทิเช่น ควอนตัม, AI safety, 3rd party, cyber risk co-operation

การลงทุนโครงสร้างพื้นฐานและเทคโนโลยีที่จำเป็น

- ส่งเสริมให้มีการพัฒนาซอฟต์แวร์และเทคโนโลยีสัญชาติไทย
- จัดให้มีการพัฒนา “National Threat Intelligence Platform”
- จัดสรรงบประมาณพัฒนาโครงสร้างพื้นฐานด้านการตรวจจับและตอบสนองต่อเหตุการณ์ภัยคุกคาม (SOC, CERT) ให้มีประสิทธิภาพสูงขึ้น

ข้อเสนอแนะเชิงนโยบาย เพื่อการบริหารความเสี่ยง (Risk Mitigation)

4.1 ข้อเสนอแนะเชิงนโยบายเพื่อบริหารความเสี่ยง (Risk Mitigation) ในระดับประเทศ



การพัฒนาศักยภาพและทรัพยากรบุคคลด้านความมั่นคงไซเบอร์

- ส่งเสริมการฝึกเฝ้าระวังภัยไซเบอร์ในกลุ่มประชาชน บริษัท Startup และ SMEs
- ส่งเสริมความร่วมมือและเครือข่ายทั้งในประเทศ และต่างประเทศในการอบรม เกี่ยวกับภัยคุกคามความเสี่ยง โดยเฉพาะในด้านของ การรู้เท่าทันภัยไซเบอร์ (Cyber Awareness) ให้เข้าใจลักษณะการโจมตีที่พบบ่อย เช่น Phishing, DDoS, Brute Force, Malware การรับมือกับช่องโหว่ระบบ (System Vulnerability Management) การป้องกันการรั่วไหลของข้อมูล (Data Protection & Handling) เป็นต้น
- ควรจัดให้มีการฝึกเชิงปฏิบัติ / Road show เกี่ยวกับ ฝึกซ้อมจำลองเหตุการณ์โจมตี เช่น การโจมตี DDoS หรือ Malware แพร่ผ่าน USB สอนขั้นตอนการแจ้งเหตุ การเก็บหลักฐาน และการตอบสนองเบื้องต้น





ข้อเสนอแนะเชิงนโยบาย เพื่อการบริหารความเสี่ยง (Risk Mitigation)

4.2 ข้อเสนอแนะเชิงนโยบายเพื่อบริหารความเสี่ยง (Risk Mitigation) ในระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



เสริมสร้างมาตรฐานการจัดการช่องโหว่ (Vulnerability Management)

- จัดให้มีการสแกนและอุดช่องโหว่อย่างสม่ำเสมอ
- กำหนดมาตรฐานการ Patch และ Secure Configuration ที่เข้มงวด

สร้างระบบ Early Warning และ Threat Intelligence Sharing

- พัฒนา National Threat Intelligence Platform เชื่อมโยงทุกภาคส่วน
- จัดให้มีการแบ่งปันข้อมูล (IOC/Threat Feed) แบบ Real-time

เสริมสร้างบุคลากรและการพัฒนาศักยภาพ (Capacity Building)

- จัดอบรมและสร้างทักษะด้าน Cybersecurity ให้บุคลากรทุกระดับ
- ส่งเสริมการสอบใบรับรองมาตรฐานสากล (เช่น CISSP, CISM, CEH)

ข้อเสนอแนะเชิงนโยบาย เพื่อการบริหารความเสี่ยง (Risk Mitigation)

4.3 ข้อเสนอแนะเชิงนโยบายเพื่อบริหารความเสี่ยง (Risk Mitigation) ในระดับกลุ่มหน่วยงานของรัฐ

กำหนดมาตรฐานกลางด้านความมั่นคงไซเบอร์ภาครัฐ



- ส่งเสริมให้ทุกหน่วยงานประเมินความเสี่ยงตามมาตรฐานที่ สกมช. กำหนด
- จัดทำ Baseline Security Standard สำหรับทุกหน่วยงาน
- ใช้กรอบสากล (NIST CSF, ISO 27001) ร่วมกับ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- บังคับใช้มาตรการบริหารจัดการช่องโหว่และอุดช่องโหว่อย่างทันท่วงที
- ทุกหน่วยงานต้องมีแผน IR และ DR ที่สอดคล้องกับมาตรฐานเดียวกัน

พัฒนาศักยภาพบุคลากรภาครัฐด้าน Cybersecurity

- จัดอบรมพื้นฐานไซเบอร์สำหรับข้าราชการทุกระดับ
- พัฒนาผู้เชี่ยวชาญด้านเทคนิคเชิงลึก และสนับสนุนการสอบใบรับรอง

บูรณาการการทำงานระหว่างหน่วยงาน

- ร่วมมือกับ Cloud Provider, Telecom, Energy Sector เพื่อรับมือภัยไซเบอร์ที่ซับซ้อน

NCSA สกมช

การป้องกันโจรกรรมทางไซเบอร์ ฉบับพื้นฐาน

คิด-ก่อน Click

ระวัง link หรือ ไฟล์แนบที่ไม่น่าเชื่อถือ / ไม่มั่นใจ

พาสเวิร์ดคือสิ่งที่สำคัญในยุคดิจิทัล

ใช้พาสเวิร์ดที่ซับซ้อน และระมัดระวังให้เป็น “ความลับ” เสมอในทุกแพลตฟอร์ม

หมั่นอัพเดตซอฟแวร์อย่างสม่ำเสมอ

พยายามอัพเดต software และ security ในระบบเป็นประจำ

ระวัง Phishing

อย่าแชร์ข้อมูลส่วนตัวหรือข้อมูลสำคัญผ่านข้อความ/อีเมลที่ไม่น่าเชื่อถือ



5. บทสรุปและทิศทางในอนาคต



บทสรุปและทิศทางในอนาคต

รายงานการประเมินความเสี่ยงทางไซเบอร์ระดับประเทศ ภายใต้กรอบ Thailand National Cyber Risk Assessment Framework (TH-NCRAF) ประจำปีงบประมาณ พ.ศ. 2568 ได้สะท้อนให้เห็นภาพรวมของภูมิทัศน์ภัยคุกคามที่มีความเปลี่ยนแปลงอย่างรวดเร็วและซับซ้อนมากขึ้นโดยมีแนวโน้มการโจมตีที่พุ่งเป้าไปยังหน่วยงานของรัฐ, โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และภาคบริการดิจิทัลที่มีความเชื่อมโยงกันอย่างกว้างขวาง ทั้งในรูปแบบของการใช้ช่องโหว่ภายใน การเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีแบบ DDoS และ Ransomware ซึ่งล้วนสร้างผลกระทบในเชิงระบบต่อเศรษฐกิจและความมั่นคงของประเทศ

เมื่อเปรียบเทียบกับมาตรฐานสากลและดัชนีระดับโลก เช่น Global Cybersecurity Index (GCI) และ ENISA Threat Landscape 2024 พบว่า ประเทศไทยมีความก้าวหน้าในด้านกฎหมาย นโยบาย และกลไกบริหารจัดการ แต่ยังคงมีช่องว่าง (Gap) ที่ต้องได้รับการพัฒนาในสามประเด็นหลัก คือ

01



ด้านขีดความสามารถเชิงเทคนิค (Technical Capability)

ประเทศชั้นนำมีการพัฒนาแพลตฟอร์มตรวจจับและตอบสนองภัยไซเบอร์แบบเรียลไทม์ (SOC / SOAR) ที่เชื่อมโยงข้อมูลจากหลายแหล่ง ขณะที่ประเทศไทยยังอยู่ในช่วงเริ่มต้นของการบูรณาการข้อมูลภัยคุกคามในระดับประเทศ

02



ด้านทรัพยากรบุคคล (Cyber Workforce)

การขาดแคลนผู้เชี่ยวชาญเฉพาะทางยังเป็นข้อจำกัดสำคัญ โดยเฉพาะในหน่วยงานของรัฐและภาคโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทำให้การตอบสนองต่อเหตุการณ์ยังขาดความคล่องตัว

03



ด้านความร่วมมือและการแบ่งปันข้อมูล (Collaboration & Intelligence)

ประเทศไทยยังไม่มีระบบกลางสำหรับแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างหน่วยงานอย่างมีประสิทธิภาพ ทำให้การรับรู้และการตอบสนองยังไม่ทันต่อสถานการณ์

บทสรุปและทิศทางในอนาคต

จากการวิเคราะห์ดังกล่าว สามารถสรุป “ทิศทางในอนาคต” เพื่อพัฒนาความมั่นคงปลอดภัยไซเบอร์ของประเทศได้ดังนี้

1. พัฒนาแพลตฟอร์มข้อมูลภัยคุกคามระดับชาติ (National Threat Intelligence Platform) เพื่อเชื่อมโยงข้อมูลระหว่างภาครัฐ เอกชน และพันธมิตรระหว่างประเทศ พร้อมระบบวิเคราะห์ด้วย AI เพื่อคาดการณ์และป้องกันภัยล่วงหน้า
2. ยกระดับขีดความสามารถในการตอบสนองเหตุการณ์ (Incident Response) สร้างศูนย์ตอบสนองเฉพาะภาคส่วน (Sectoral CERT) ที่มีความพร้อมในการปฏิบัติงานตลอด 24 ชั่วโมง พร้อมระบบจำลองเหตุการณ์ไซเบอร์ (Cyber Range) สำหรับการฝึกซ้อม
3. สร้างระบบพัฒนากำลังคนด้านไซเบอร์อย่างยั่งยืน (Cyber Workforce Framework) จัดทำมาตรฐานสมรรถนะและเส้นทางอาชีพ เพื่อยกระดับทักษะของบุคลากรทุกระดับ โดยเฉพาะในหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
4. บูรณาการกฎหมายและมาตรฐานสากล (Legal & Policy Integration) ปรับปรุงกฎหมายและกรอบนโยบายให้สอดคล้องกับมาตรฐานโลก เช่น NIST CSF 2.0, ISO/IEC 27001:2022 เป็นต้น เพื่อให้เกิดความเชื่อมโยงในระดับภูมิภาค
5. ส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์ระดับสังคม (Cyber Awareness & Resilience Culture) พัฒนาโครงการสร้างความตระหนักรู้ในทุกระดับ เพื่อให้บุคลากรและประชาชนมีพฤติกรรมดิจิทัลที่ปลอดภัย

ทิศทางเหล่านี้จะช่วยลดช่องว่างระหว่างประเทศไทยกับประเทศชั้นนำ และผลักดันให้เกิด “ระบบนิเวศความมั่นคงไซเบอร์ที่ยั่งยืน (Sustainable Cybersecurity Ecosystem)” ที่ขับเคลื่อนด้วยความร่วมมือจากทุกภาคส่วน ทั้งภาครัฐ เอกชน สถาบันการศึกษา และนานาชาติ เพื่อเสริมความพร้อมของประเทศในการเผชิญกับภัยคุกคามดิจิทัลยุคใหม่ได้อย่างมั่นคง มั่งคั่ง และยั่งยืน



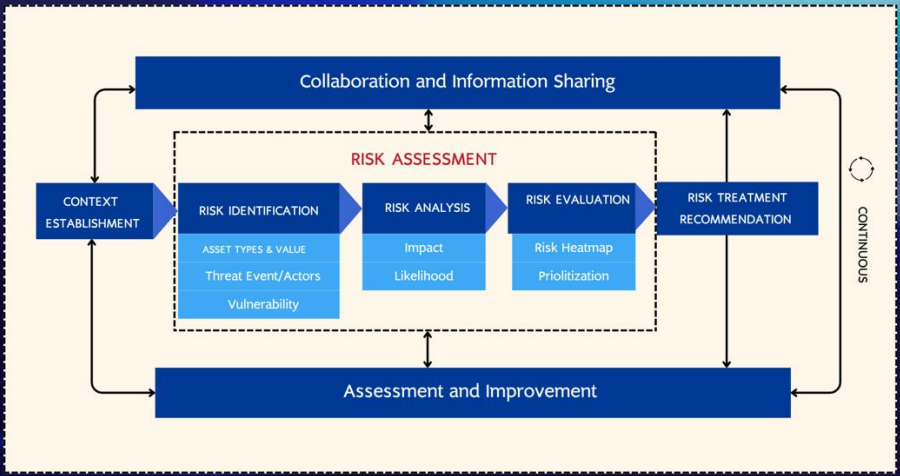
Study Report : Thailand National Cyber Risk Assessment Report 2025





Thailand National Cyber Risk Assessment Framework 2025

TH-NCRAF



Executive Summary

Executive Summary

The national cyber risk assessment for fiscal year 2025 was prepared under the Thailand National Cyber Risk Assessment Framework (NCRAF), by the Office of the National Cyber Security Committee (NCSC). Its aim is to analyze threat situations affecting the nation's cybersecurity and to provide information that supports systematic policy and strategic cyber security measures.

The overall assessment results indicate that Thailand's national cyber risk level is defined by the following top five highest-risk categories:

1. Outsiders exploiting software vulnerabilities to gain unauthorized access to information and technology management assets.
2. Outsiders and Ad hoc groups exploiting software vulnerabilities to conduct targeted Denial-of-Service (DoS) attacks on information and technology management assets.
3. Outsiders and Ad hoc groups exploiting software vulnerabilities to conduct non-targeted (simple) DoS attacks on information and technology management assets.
4. Outsiders insert specialized malware—such as evasive ransomware—into government information systems using software vulnerabilities.
5. Outsiders exploiting recently discovered software vulnerabilities to attack information and technology management assets.

Executive Summary

Based on the assessment, the National Cyber Security Committee (NCSC) has proposed several policy directions to strengthen Thailand's cybersecurity capability. These include:

1. Enhancing cyber detection & response systems and Cyber Resilience capability to comprehensively all sectors
2. Establishing a regular annual national cyber risk assessment mechanism (National Cyber Risk Review Continues).
3. Establish Cyber Workforce Framework Development System.
4. Building collaboration between government, private sector, and international partners for threat intelligence sharing.
5. Establish centralized platform for Real-Time threat information sharing.

The results of Thailand's 2025 national cybersecurity assessment revealed persistent gaps in risk management and incident response readiness, particularly among government agencies whose preparedness scores have declined. In contrast, critical information infrastructure organizations and regulatory bodies demonstrated improvements and positive development trends. Enhancing the nation's cybersecurity capabilities is not a one-time endeavor but a continuous and systematic process that requires ongoing improvement to effectively address increasingly complex and pervasive threats across all sectors.

Therefore, the assessment underscores the necessity of continuously enhancing the nation's cybersecurity capabilities to ensure Thailand's preparedness in preventing, responding to, and recovering from cyber threats in a resilient and sustainable manner.

1. Introduction



Introduction

1.1 Trends and Risks in the Cyber Threat Landscape : Global and Thailand Overview

Overall Global Cyber Attack in 2025



Economic Impact of Cybercrime

It is estimated that the global economic damage caused by cybercrime will reach USD 10.5 trillion per year by 2025, up from USD 3 trillion in 2015, representing an average annual growth rate of 15%.



Malware-Free Attacks

A report from CrowdStrike indicated that 79% of threat detections in 2024 were non-malware attacks, meaning that hackers employed alternative techniques such as attacks through compromised user accounts or the use of legitimate tools to gain access to systems.



AI Attacks

Hackers have begun leveraging artificial intelligence (AI) in their attacks — such as generating more convincing phishing emails, creating realistic fake websites, and rapidly analyzing system vulnerabilities to exploit weaknesses more effectively.

CYBER THREAT LANDSCAPE 2025

Source: Global Cybersecurity Outlook 2025, World Economic Forum

Geopolitical tensions



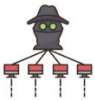
Nearly 60% of organizations have adjusted their cybersecurity strategies due to geopolitical pressures. Of particular concern are cyber espionage and the loss of sensitive information or intellectual property (IP) highlighting that cybersecurity is no longer merely an IT issue, but a strategic business issue.

Cybercrime sophistication



- Cyber-enabled fraud is showing an upward trend.
- Phishing and social engineering attacks are increasing in frequency.
- Identity theft has become one of the top personal cybersecurity risks.

Supply chain interdependencies



A cyberattack on one organization within the supply chain can trigger a chain reaction of impacts, disrupting other connected organizations and potentially affecting the entire operational ecosystem.

Regulatory requirements



Excessive complexity and overregulation have become major challenges and potential vulnerabilities as they create confusion and compliance fatigue, leading organizations to overlook or fail to fully implement required security measures.

AI and emerging tech



Most organizations recognize that AI is transforming both cyberattacks and cyber defense, yet they still lack clear frameworks and regulatory measures to effectively govern its use.

Cyber skills gap



The demand for cybersecurity professionals far exceeds the current supply in both quantity and quality, leaving most organizations exposed to structural risks if they fail to upskill or reskill their workforce promptly.



Introduction

Overall Cyber Threat Situation in Thailand 2025



The government and education sectors were among the top targets, with over 3,100 incidents recorded last year. The most common attack types were “fake websites” and “compromised or leaked accounts/passwords.”



The implementation of Multi-Factor Authentication (MFA) has been mandated as a standard requirement for government agencies to enhance overall system protection.



Organizations in Thailand face heightened cyber risks due to the continued use of outdated legacy systems and high technological complexity, which create vulnerabilities that can be exploited by malicious actors to infiltrate their networks.



The rising trend of supply chain attacks that adversaries exploit vulnerabilities in partner networks, service providers, or external systems as pivot points to infiltrate an organization’s core systems—has become an increasingly serious cybersecurity concern.



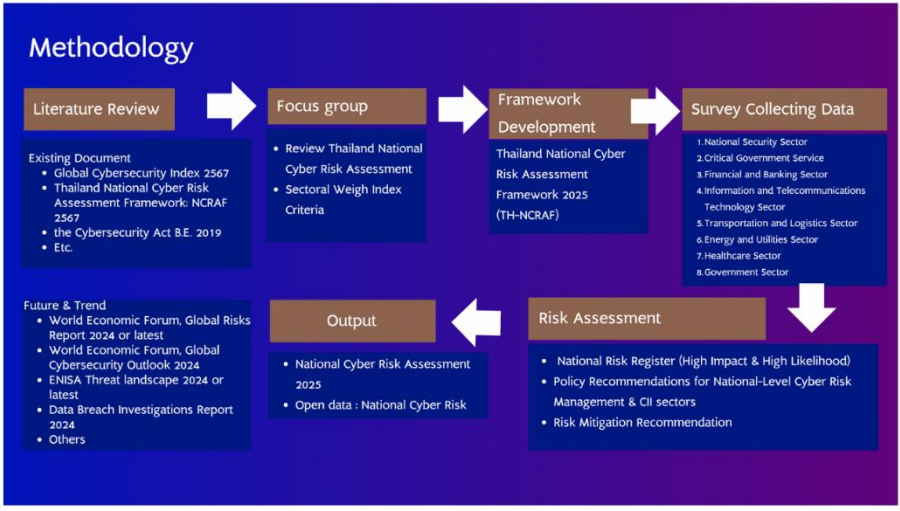
Between January and May 2025, a total of 1,002 cybersecurity incidents were reported in Thailand. The most common attack types included credential stuffing, DDoS attacks, ransomware, and data leaks. These incidents were largely driven by the increased adoption of cloud infrastructure among organizations and the growing use of AI tools by malicious actors to enhance the sophistication of their attacks.

Introduction

1.2 National Cyber Threat Risk Assessment Activities Project

The National Cyber Security Agency (NCSA) has conducted cyber threat risk assessment activities to analyze and evaluate cyber threat risks at both the national level and within groups of Critical Information Infrastructure (CII) agencies.

These activities are organized as annual projects to monitor the changing levels of cyber risk and to ensure compliance with international cybersecurity risk assessment standards, which require such assessments at least once a year. The program also aligns with Section 54 of the Cybersecurity Act B.E. 2562 (2019), which mandates annual reviews of cyber risks for CII organizations. The resulting assessments serve as a foundation for planning prevention, response, and risk mitigation measures in accordance with the provisions of the Cybersecurity Act B.E. 2562 (2019).



Project Methodology

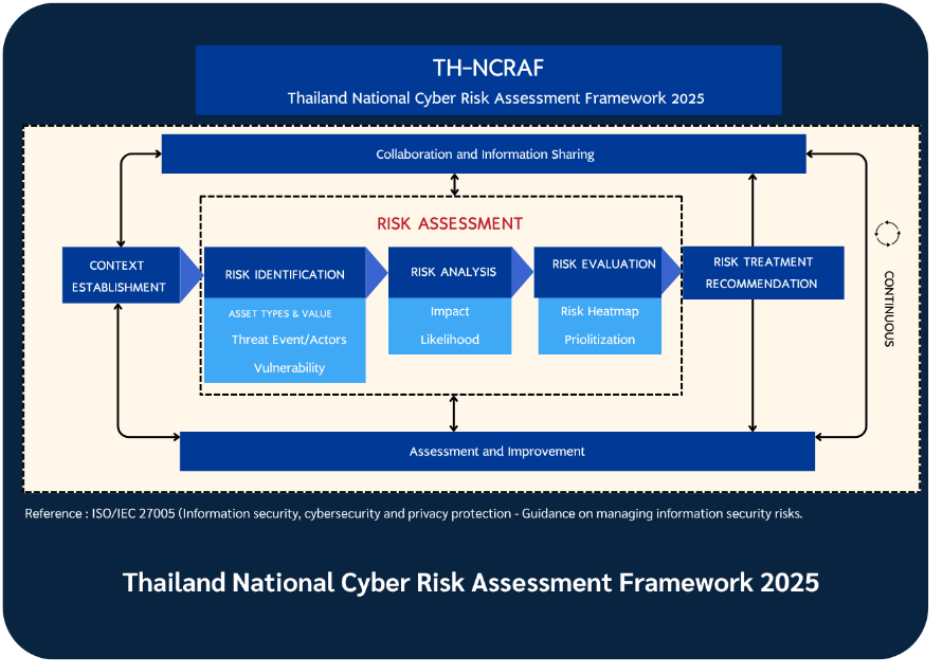
2. Thailand National Cyber Risk Assessment Framework



Thailand National Cyber Risk Assessment 2025

The Cyber Threat Risk Assessment Framework of Thailand for the Year 2025 is designed to serve as a national-level tool for assessing overall cyber risk. It provides a guideline framework for government and related agencies to evaluate organizational cyber risks and to utilize the results as a national benchmark, thereby enabling each agency to understand its cybersecurity posture in the context of the country's overall landscape.

Furthermore, the framework helps reduce redundancy and standardize reporting procedures in accordance with Section 54 of the Cybersecurity Act B.E. 2562 (2019), which mandates that cyber risk assessments of Critical Information Infrastructure (CII) agencies be reviewed annually.



Reference : ISO/IEC 27005 (Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

Thailand National Cyber Risk Assessment Framework 2025

Remark : TH-NCRAF 2025 based on the Focus Group Consultation with Relevant Stakeholders on the Draft Cyber Threat Risk Assessment Framework of Thailand, held on 16 May 2025.

2.1 Context Establishment

The identification of an agency's context serves as essential information in defining the significance of the agency preparing the Cyber Threat Risk Assessment Report. It reflects the agency's critical role in the national landscape, and must be specified in accordance with the established framework, which includes the following elements:

Organization Name	
Category	Regulators
	Critical Information Infrastructure (CII) Agency
	Government (non-CII)
Mission Category	1. National Security Sector
	2. Critical Government Service
	3. Financial and Banking Sector
	4. Information and Telecommunications Technology Sector
	5. Transportation and Logistics Sector
	6. Energy and Utilities Sector
	7. Healthcare Sector
	8. Government Sector (non-CII)
Institutional Profile	Based on the "Announcement of the National Cyber Security Agency (NCSA) on the Criteria and Characteristics of Agencies Performing Missions or Providing Services as Critical Information Infrastructure Agencies, and the Assignment of Supervisory and Regulatory Responsibilities, B.E. 2564 (2021)".
Mission Services	

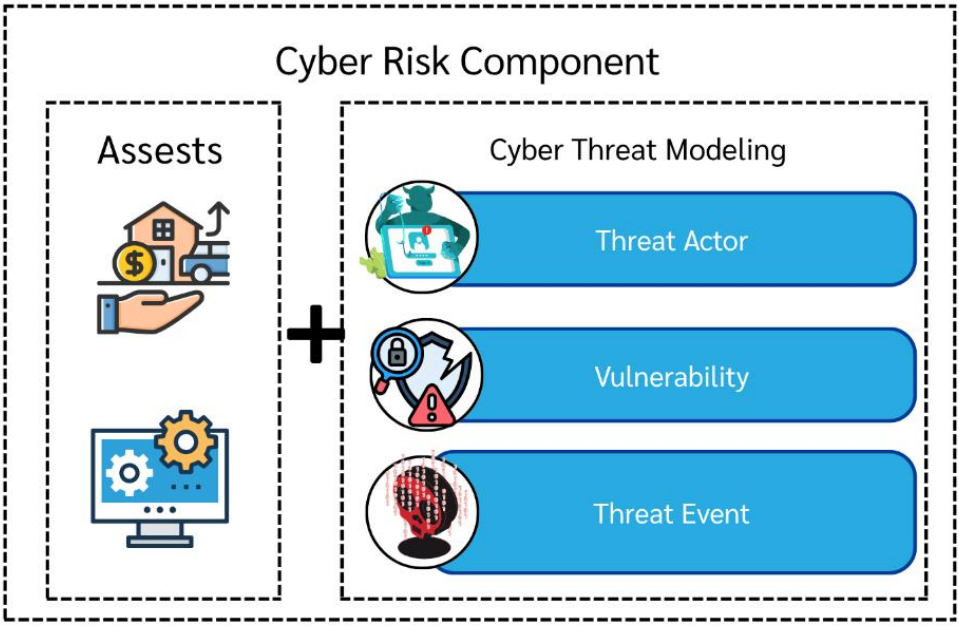
2.2 Risk Identification

The identification of cyber threat risks involves analyzing potential adversarial threats that may affect the organization or the nation. The risk components are divided into two main parts:

(1) Organizational Assets, and

(2) Cyber Threat Modeling,

the structure of which illustrated in the following diagram.



Under Section 54 of the Cybersecurity Act B.E. 2562 (2019), each agency is obligated to prepare and submit an annual Cyber Threat Risk Assessment Report to the National Cyber Security Agency (NCSA). The submitted information has been systematically aggregated and structured based on the Cyber Threat Risk Assessment Framework, ensuring that only data meeting the required completeness and alignment with the 2025 national framework are incorporated for analysis and reporting.

The minimum required data for assessment are as follows:

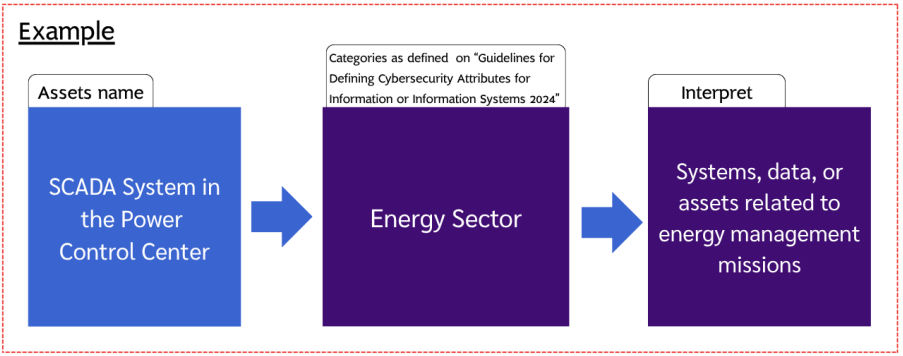
- Assets name/Type
- Vulnerability
- Adversary / Threat Actor
- Threat Event
- Impact–Likelihood–Risk Analysis

Following the completeness review, the agency's contextual information was defined in accordance with Section 2.1 of the Thailand Cyber Threat Risk Register Database (2025).

2.2.1 Asset Category Identification

Asset information refers to the details of assets that an agency has identified as potentially vulnerable to cyberattacks. As the specific names of assets included in the risk assessment are considered sensitive information, their disclosure could enable adversaries to infer the agency's security measures associated with those assets.

Therefore, the assets were categorized based on their relevance and aligned with the classifications specified in the Announcement of the National Cyber Security Agency (NCSA) on "Guidelines for Defining Cybersecurity Attributes for Information or Information Systems 2024". The identification of asset types that may constitute sensitive data was intentionally avoided.



2.2.2 Vulnerability Identification

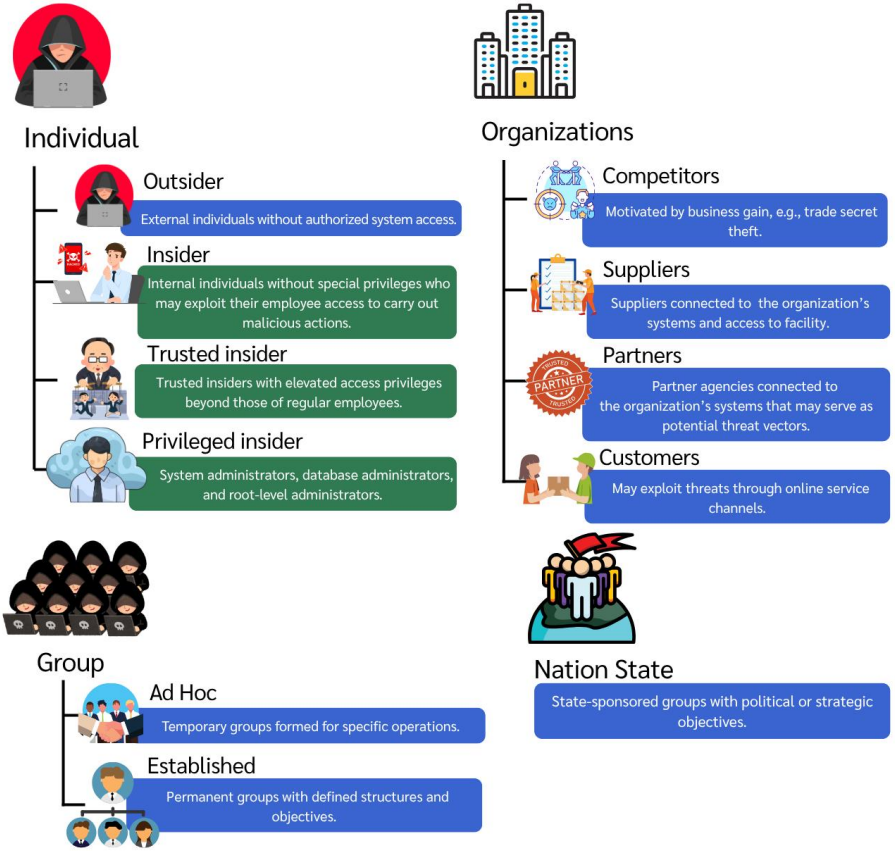
A vulnerability serves as a potential pathway through which a cyber threat can compromise an organization's assets. The framework references vulnerability classifications based on ISO/IEC 27005:2022, which categorizes types of weaknesses that may lead to cyber risks. The risk assessment data provided by each agency are reviewed and organized into categories as shown in the table below.

Vulnerability	Description
Organization	There is a lack of a governance structure to oversee and audit the implementation of cybersecurity policies, particularly those encompassing the use of software, tools, and digital services.
Processes and procedures	Vulnerabilities arising from procedural weaknesses that allow adversaries to exploit and cause harm to the organization.
Management Routines	Vulnerabilities stemming from the management routines or from operational schedules that may be inadvertently exposed to external parties can be exploited by malicious actors to launch targeted attacks against the organization
Personnel / Employees	Vulnerabilities arising from human factors—such as insufficient knowledge, lack of awareness, or negligence—can be exploited by malicious actors, who may manipulate or deceive personnel to initiate or facilitate cyberattacks.
Physical environment	Weaknesses in an organization's infrastructure or physical environment (e.g., site conditions) may create opportunities for adversaries to carry out attacks.
Information System Configuration	Weaknesses arising from misconfigured systems that do not comply with cybersecurity standards
Hardware and Communication Devices	Weaknesses in hardware, firmware, or communication devices that are outdated, defective, or no longer supported by vendors
Software	Vulnerabilities in software or code due to defects, insecure coding, or lack of updates
Dependence on external parties	Vulnerabilities arising from third-party activities that may create risks beyond the organization's direct control

2.2.3 Threat Actor

Adversaries refer to individuals, groups, organizations, or nations that intentionally exploit vulnerabilities and cyber threats to attack an organization's assets. Identifying adversaries enhances understanding of their motives, capabilities, tactics, and techniques, as well as the likelihood of a successful cyberattack, thereby enabling the development of targeted control measures and monitoring strategies.

The framework references the classification of adversary groups from NIST SP 800-30, Appendix D-2: Taxonomy of Threat Sources, which categorizes adversaries as follows:



2.2.4 Threat Event

A cyber threat event refers to an incident in which an adversary causes harm by employing various cyberattack tactics and techniques. The framework references the NIST SP 800-30, Appendix E-2: Taxonomy of Threat Events, which categorizes cyber threat events into 8 groups as follows:



1. Group P: Perform reconnaissance and gather information.



2. Group C: Craft or create attack tools.



3. Group D: Deliver/insert/install malicious capabilities.



4. Group E: Exploit and compromise.



5. Group A: Conduct an attack.



6. Group R: Achieve results.



7. Group M: Maintain a presence or set of capabilities.



8. Group CC: Coordinate a campaign.



1. Group P: Perform reconnaissance and gather information.

P.1 Perform perimeter network reconnaissance/scanning.
P.2 Perform network sniffing of exposed networks.
P.3 Gather information using open source discovery of organizational information.
P.4 Perform reconnaissance and surveillance of targeted organizations.
P.5 Perform malware-directed internal reconnaissance.



2. Group C: Craft or create attack tools.

C.1 Craft phishing attacks.
C.2 Craft spear phishing attacks.
C.3 Craft attacks specifically based on deployed information technology environment.
C.4 Create counterfeit/spoof website.
C.5 Craft counterfeit certificates.
C.6 Create and operate false front organizations to inject malicious components into the supply chain.



3. Group D: Deliver/insert/install malicious capabilities.

D.1 Deliver known malware to internal organizational information systems (e.g., virus via email).
D.2 Deliver modified malware to internal organizational information systems.
D.3 Targeted malware attacks to seize control of internal systems and exfiltration data from the organization.
D.4 Deliver malware by providing removable media.
D.5 Insert untargeted malware into downloadable software and/or into commercial information technology products.

3. Group D: Deliver/insert/install malicious capabilities.

D.6 Insert targeted malware into organizational information systems and information system components.
D.7 Insert specialized malware into organizational information systems based on system configurations.
D.8 Insert counterfeit or tampered hardware into the supply chain.
D.9 Insert tampered critical components into organizational systems.
D.10 Install general-purpose sniffers on organization-controlled information systems or networks.
D.11 Install persistent and targeted sniffers on organizational information systems and networks.
D.12 Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.
D.13 Insert subverted individuals into organizations.
D.14 Insert subverted individuals into privileged positions in organizations.



4. Group E: Exploit and compromise.

E.1 Exploit physical access of authorized staff to gain access to organizational facilities.
E.2 Exploit poorly configured or unauthorized information systems exposed to the Internet.
E.3 Exploit split tunneling.
E.4 Exploit multi-tenancy in a cloud environment.
E.5 Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).
E.6 Exploit recently discovered vulnerabilities.
E.7 Exploit vulnerabilities on internal organizational information systems.
E.8 Exploit vulnerabilities using zero-day attacks

4. Group E: Exploit and compromise.

E.9 Insertion of counterfeit or tampered devices into the organization's supply chain, resulting in exploitable vulnerabilities.
E.10 Exploit insecure or incomplete data deletion in multi-tenant environment.
E.11 Violate isolation in multi-tenant environment.
E.12 Compromise critical information systems via physical access.
E.13 Compromise information systems or devices used externally and reintroduced into the enterprise.
E.14 Compromise software of organizational critical information systems.
E.15 Compromise organizational information systems to facilitate exfiltration of data/information.
E.16 Compromise mission-critical information.
E.17 Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).



5. Group A: Conduct an attack

A.1 Conduct communications interception attacks.
A.2 Conduct wireless jamming attacks.
A.3 Conduct attacks using unauthorized ports, protocols and services.
A.4 Conduct attacks leveraging traffic/data movement allowed across perimeter.

5. Group A: Conduct an attack

A.5 Conduct simple Denial of Service (DoS) attack.
A.6 Conduct Distributed Denial of Service (DDoS) attacks.
A.7 Conduct targeted Denial of Service (DoS) attacks.
A.8 Conduct physical attacks on organizational facilities.
A.9 Conduct physical attacks on infrastructures supporting organizational facilities.
A.10 Conduct cyber-physical attacks on organizational facilities.
A.11 Conducting an information searching attack on a cloud environment.
A.12 Conduct brute force login attempts/password guessing attacks.
A.13 Conduct nontargeted zero-day attacks.
A.14 Conduct externally-based session hijacking.
A.15 Conduct internally-based session hijacking.
A.16 Conduct externally-based network traffic modification (man in the middle) attacks.
A.17 Conduct internally-based network traffic modification (man in the middle) attacks.
A.18 Conduct outsider-based social engineering to obtain information.
A.19 Conduct insider-based social engineering to obtain information.
A.20 Conduct attacks targeting and compromising personal devices of critical employees.
A.21 Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.



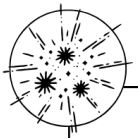
6. Group R: Achieve results

R.1 Obtain sensitive information through network sniffing of external networks.
R.2 Obtain sensitive information via exfiltration.
R.3 Cause degradation or denial of attacker-selected services or capabilities.
R.4 Cause deterioration/destruction of critical information system components and functions.
R.5 Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).
R.6 Cause integrity loss by polluting or corrupting critical data.
R.7 Cause integrity loss by injecting false but believable data into organizational information systems.
R.8 Cause disclosure of critical and/or sensitive information by authorized users.
R.9 Cause unauthorized disclosure and/or unavailability by spilling sensitive information.
R.10 Intercepting wireless network communications from outside the organization.
R.11 Obtain system or unauthorized information access.
R.12 Obtain sensitive data/information from publicly accessible information systems.
R.13 Obtain information by opportunistically stealing or scavenging information systems/components.



7. Group M: Maintain a presence or set of capabilities.

M.1 Obfuscate adversary actions.
M.2 Adapt cyber attacks based on detailed surveillance.



8. Group CC: Coordinate a campaign.

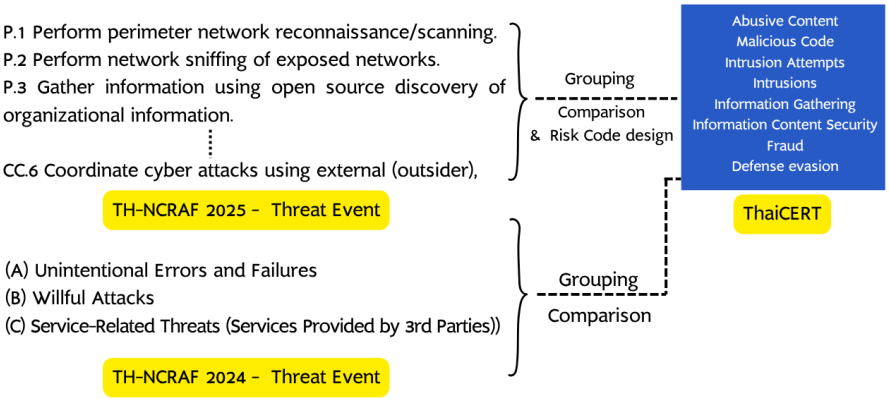
CC.1 Coordinate a campaign of multi-staged attacks (e.g., hopping).
CC.2 Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.
CC.3 Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.
CC.4 Coordinate a campaign that spreads attacks across organizational systems from existing presence.
CC.5 Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.
CC.6 Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.

To achieve consistency and comparability within the National Cyber Risk Register, cyber threat events reported by agencies under Section 54 of the Cybersecurity Act B.E. 2562 (2019) were aligned with the relevant tactics and techniques outlined in the framework. The alignment was conducted by matching the reported event descriptions to the most corresponding definitions of cyber threat events.

2.2.5 Comparison of the Number of Cyber Threat Events Identified in Thailand's Cyber Threat Risk Assessment, 2024–2025

As the cyber threat events in the current framework have been reviewed and updated to reflect only adversarial threats, based on tactics and techniques referenced in NIST SP 800-30 (as outlined in Section 2.2.4), the structure differs from that of the 2024 framework.

To enable statistical comparison and alignment, an analysis and categorization were conducted to map the cyber threat events from the 2024–2025 frameworks to the "Incident Classes" defined by the National Computer Security Coordination Center (ThaiCERT), which adopts categories from ENISA for compiling cybersecurity statistics. The conceptual approach is illustrated in the following diagram.



* – Reference Incident Classification Taxonomy - ENISA

Incident Class	Sub Categories
Abusive Content	Spam [1]
	Harassment [1]
Malicious Code	Virus/Worm/Trojan/Spyware [1]
Information Gathering	Scanning [1]
	Sniffing [1]
	Social Engineering [1]
Intrusion Attempts	Exploiting of known Vulnerabilities [1]
	Login attempts [1]
	New attack signature [1]
Intrusion	Privileged Account Compromise [1]
	Unprivileged Account Compromise [1]
	Application Compromise [1]
	Campaigns [2]
Availability Attack	DoS [1]
	DDoS [1]
	Sabotage [1]

[1] Reference Incident Classification Taxonomy - ENISA

[2] Additional Categories

Incident Class	Sub Categories
Information Content Security	Unauthorises access to information
	Unauthorised modification of information
Fraud	Unauthorized use of resources
	Masquerade
	Fake Website
Other	Defense evasion

Scan the QR code to view the cyber threat incident classification results.

Additionally, the categorized cyber threats are assigned risk codes, which are used as references in the Risk Matrix during the Risk Evaluation process.

TH-NCRAF Risk identification



Risk Scenario	Incident Class	Risk Code
Cyber Risk	Abusive Content : AC	AC.1 [Risk Scenario]
Cyber Risk	Malicious Code : MC	MC.1 [Risk Scenario]
Cyber Risk	Intrusion Attempts : IA	IA.1 [Risk Scenario]
Cyber Risk	Intrusion: I	I.1 [Risk Scenario]
Cyber Risk	Information Gathering: IG	IG.1 [Risk Scenario]
Cyber Risk	Information Content Security : ICS	ICS.1 [Risk Scenario]
Cyber Risk	Fraud : F	F.1 [Risk Scenario]
Cyber Risk	Defense Evasion : DE	DE.1 [Risk Scenario]

Scan here for access
TH-NCRAF Risk identification

2.3 Risk Analysis

The cyber threat risk analysis consists of two main components: the impact level and the likelihood level. Together, these factors reflect the overall level of risk to which an agency may be exposed from cyber threats.

2.3.1 Impact Analysis

Impact level refers to the degree of potential damage an organization may experience in the event of a cyber threat incident. The impacts are defined in accordance with the objectives of cybersecurity and are categorized into three dimensions under the CIA Triad, as follows:



When assessing impacts under each dimension of the CIA Triad, the evaluation must be conducted separately based on:

- The agency's reputation impact.
- Financial impact
- Operational processes impact
- Legal and regulatory compliance impact

The impact level is classified into three tiers: high, medium, and low. After all dimensions have been assessed, the highest impact level identified shall be used to determine the organization's overall risk level in subsequent evaluations.

2.3.2 Likelihood Analysis

The likelihood of a cyber threat event refers to the probability or possibility that a cyber threat may exploit a vulnerability and cause damage to the organization. The assessment of likelihood is conducted across 4 key dimensions, as follows:

- **Reproducibility** – the ease or difficulty of repeating the attack.
- **Exploitability** – the level of attacker expertise required to execute the tactics and techniques; the likelihood increases when attackers are organized groups or state-sponsored actors.
- **Discoverability** – the ease with which attackers can identify existing vulnerabilities.
- **Past Incidents** – the history and frequency of similar cyber threat events in the past.

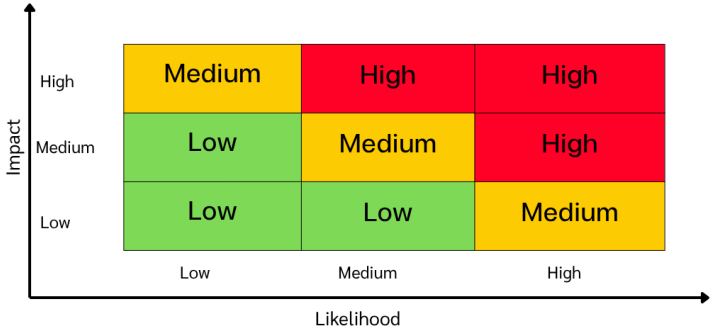
The likelihood level of a cyber threat event is categorized into three levels: high, medium, and low. After all dimensions have been evaluated, the highest likelihood level identified shall be applied to determine the organization's overall risk level in the subsequent assessment.

2.3.3 Risk Analysis

The cyber threat risk level serves as an indicator of the extent to which an organization may be affected by a cyber threat incident. It is determined by combining the likelihood of occurrence and the impact level of the threat. The method for calculating the risk level under the framework is illustrated by the following equation.

Risk Level = (Impact) x (Likelihood)

The risk level is presented in a 3x3 Risk Matrix, as illustrated in the figure. This matrix provides an overview of the identified risks and serves as a basis for determining appropriate risk mitigation measures.



2.3.4 Normalization of Risk Levels

The cyber threat risk assessment data from each agency may differ in terms of impact, likelihood, and risk level criteria. To ensure comparability across agencies, the results were normalized to align with the framework's standardized levels, using the reference criteria shown in the table.

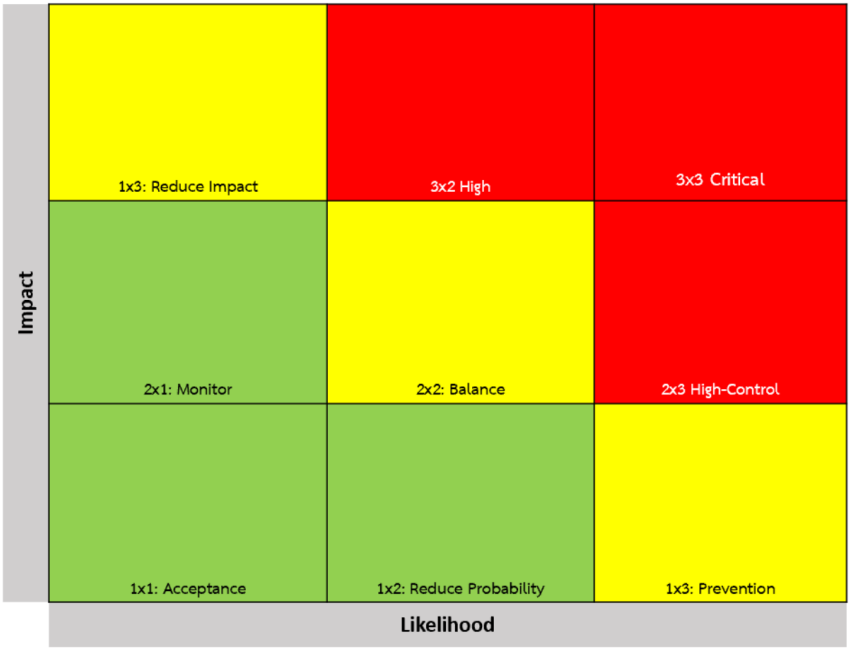
Risk Level	3 Level Assessment Scale	4 Level Assessment Scale	5 Level Assessment Scale
High	High	Very High	Very High
		High	High
Medium	Medium	Medium	Medium
Low	Low	Low	Low
			Very Low

2.4 Risk Evaluation

2.4.1 Risk Prioritization

Once the risk analysis results are obtained and presented in the Risk Matrix, they are used to determine the priority of risks that require immediate action to bring them to an acceptable level or to mitigate their potential impact.

Accordingly, guidelines for responding to cyber threat risks have been established, with management approaches illustrated in the corresponding risk response matrix.



Risk Prioritization Approach Using a 3x3 Risk Matrix

2.4.2 Risk Respond

National-Level Cyber Threat Risk Response Framework, consisting of 4 key response strategies

- **Risk Acceptance (Accept)** For low-impact risks where mitigation or prevention is not cost-effective, but continuous monitoring is still required.
- **Risk Reduction (Control)** Enhance operational systems and remediate existing vulnerabilities to minimize the likelihood or impact of potential risks to an acceptable level, such as through staff training and cyber vulnerability mitigation.
- **Risk Transfer (Transfer)** Transfer the risk by sharing responsibility with external entities for example, through cyber insurance or outsourcing specific operations to third parties.
- **Risk Avoidance (Avoid)** For unacceptable high-level risks, management may decide to terminate or discontinue projects or activities that generate such risks and identify and address their root causes.





3. Thailand National Cyber Risk Assessment Report 2025

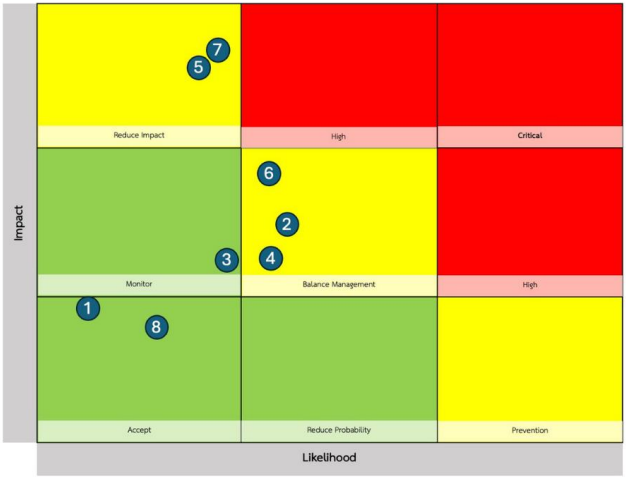


Thailand National Cyber Risk Assessment Report 2025

3.1 National Cyber Risk Assessment Results

3.1.1 Overview of National Cyber Risks

Based on the national cyber risk assessment, which utilizes data from 1,193 risk reports submitted by agencies across seven critical sectors and non-CII government entities, the results summarize the average impact and likelihood scores, presented as risk metrix that reflect the overall risk assessment of each sector, as illustrated in the figure below.



1. National Security Sector
2. Critical Government Service
3. Financial and Banking Sector
4. Information and Telecommunications Technology Sector
5. Transportation and Logistics Sector
6. Energy and Utilities Sector
7. Healthcare Sector
8. Government Sector (non-CII)



The key insights derived from Thailand's national risk metrix indicate the following details:

- Unauthorized access or attempts to gain illicit entry, along with exploitation of existing vulnerabilities within internal information systems or previously compromised systems, represent the most common risks, with the severity depending on the criticality of the affected assets.
- Denial of Service (DoS) attacks—whether random, targeted, or distributed (DDoS)—remain persistent cyber threats encountered by nearly all organizations, with the potential to cause significant operational disruption.
- There is a risk of sensitive or confidential information leakage resulting from compromised authorized user accounts, allowing malicious actors to access or disclose protected data without permission.
- The destruction of critical data or information system components, such as through ransomware attacks, is mentioned across all sectors' risk reports, though it is generally categorized within low to medium risk levels.



- There exists a risk of malware infection through removable devices (e.g., USB drives, SD cards) or embedded within data files exchanged between organizations.
- Malicious actors, both internal and external, exploit human vulnerabilities such as a lack of cybersecurity awareness or misplaced trust, to deceive individuals into revealing critical information—commonly through social engineering tactics.
- The overall national cyber risk landscape is predominantly clustered within the category of “acceptable but requires likelihood reduction,” while the remaining risks are mostly concentrated in the low-risk range.

However, when comparing the national risk assessment results with studies on emerging cyber threat trends, several noteworthy observations emerge:

- Supply chain–related risks, including cyber incidents and dependency on third-party service providers, are still limited in number and concentrated within a single sector.
- Risks associated with AI assets and threats targeting AI training data are rarely addressed in current risk assessments.
- Threats capable of evading cybersecurity detection systems are almost entirely absent from existing risk evaluations.
- Risks involving fake websites, forged certificates, or spoofed domains designed to bypass detection systems and deliver malware for data theft are infrequently mentioned, despite such incidents being reported to the NCSA.
- Cloud service–related risks and vulnerabilities from reliance on external vendors or service providers are underrepresented in the assessments — even as cloud-first policies accelerate the migration of systems to cloud environments, thereby expanding the attack surface.

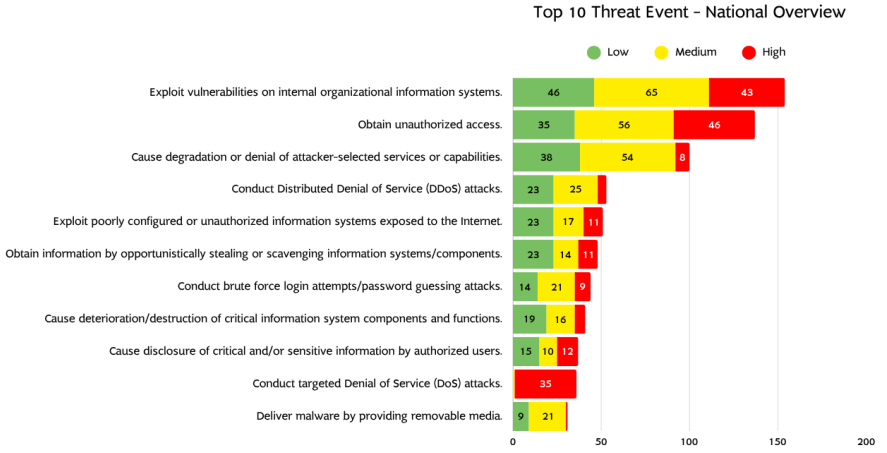


3.1.2 Statistical Results from Thailand's Cyber Threat Risk Assessment 2025

From the compilation and statistical analysis of the national cyber risk assessment data, several noteworthy statistical findings have emerged, providing significant insights that inform the development of recommendations for risk mitigation, as outlined below.

1) The frequency of cyber threat incidents identified within the risk assessment reports

Data from the national cyber risk assessments identify cyber threat events (Threat Events) most frequently cited by agencies as posing significant potential risks. The results are visually represented using three color-coded risk levels: green, yellow, and red corresponding respectively to low, medium, and high levels of self-assessed cyber risk. Statistical data were compiled from the risk assessment reports of 54 organizations, including Critical Information Infrastructure (CII) operators, regulatory and supervisory bodies, and government agencies.



Top 10 Threat Event - National Overview

The assessment identifies the most frequently occurring cyber threat events (Threat Events) that pose potential risks, including:

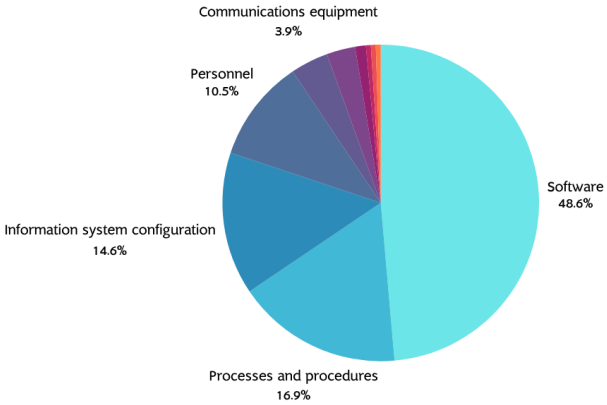
- Exploitation of internal information system vulnerabilities accounts for 12.9% of reported incidents. This threat generally results in a moderate level of risk, but if the targeted assets involve critical organizational data, the impact level increases significantly.
- Unauthorized system or data access represents 11.5% of incidents, typically resulting in a medium-to-high level of risk. For less critical assets, it is categorized as low risk, though the likelihood of occurrence remains high.
- Service degradation or denial of attacker-selected systems or functions constitutes 8.4% of cases and is mostly associated with a moderate level of risk.
- Distributed Denial of Service (DDoS) attacks make up 4.4% of identified incidents, with most being assessed as low-risk events.
- Exploitation of poorly configured or unauthorized systems exposed to the Internet accounts for 4.3%, and is largely considered a low-impact risk.
- Opportunistic data theft or scavenging of information system components represents 4.0%, generally classified within the low-risk category.







2) The most commonly identified system vulnerabilities



The identified vulnerabilities provide opportunities for malicious actors to exploit organizational assets, potentially compromising or damaging other critical systems that serve as primary attack targets. The data highlights several vulnerability types that have led to asset compromise, data breaches, or theft, with the most frequently identified categories being:

1. Software vulnerabilities – arising from insecure coding practices, outdated software versions, and technical middleware weaknesses, which require regular vendor updates and patching to prevent exploitation.
2. Regulation and process weaknesses – involving inadequate or poorly enforced operational procedures, lack of routine drills, or insufficient incident response mechanisms, creating exploitable gaps for attackers.
3. System configuration issues – resulting from improper or lax configuration of information systems that fail to meet required security standards.
4. Human factors – including lack of cybersecurity awareness, negligence, or cases where individuals are manipulated or coerced into facilitating cyberattacks. Awareness levels among personnel vary significantly across different groups.

The analysis further reveals that cyberattacks are generally driven by three primary motives: (1) stealing confidential or sensitive information, (2) disrupting or degrading system performance, and (3) obtaining personal or user account information for subsequent attacks. These vulnerabilities must therefore be monitored, controlled, and remediated to effectively reduce overall cyber risk exposure.

3) Insider Threat Risks within Organizations

Malicious actors may originate from outside the organization or infiltrate it with the intent to compromise organizational assets and achieve their objectives. However, in some cases, insiders themselves can become the threat actors. According to the ENISA Threat Landscape 2024, financial motivation remains the primary driver behind most cyberattacks. This suggests that internal personnel ranging from regular employees (Insider) to those with access to sensitive data (Trusted Insider) and even individuals with administrative or privileged system access (Privileged Insider) may potentially turn into cyber attackers to pursue personal gain or other interests.

Based on the collected data, the following insider threat risks have been identified:



Insider Threat

1st
Exploitation of vulnerabilities within the organization's internal information systems.

2 nd
Introducing malware into the system through removable media such as USB drives or external storage devices.

3 rd
Causing confidential information to be leaked or rendered inaccessible without proper authorization.

1st
Disclosure of critical and/or sensitive information by authorized users within the organization.

2 nd
Hacking or tampering with critical organizational information system software.

3 rd
Targeted malware attacks aimed at gaining control over internal systems and exfiltrating data from the organization.



Trusted Insider



Privillege Insider

1st
Disclosure of critical and/or sensitive information by authorized users within the organization.

2 nd
Hijacking user connections from within the organization.

3 rd
Coordinating cyberattacks through combined vectors leveraging external, internal, and supply chain partner channels.

In addition to the frequently mentioned risks outlined above, there are other high-impact threats that warrant close monitoring. These include the compromise or takeover of mission-critical information essential to an organization's operations, infiltration by individuals placed within the organization or in strategic positions with the intent to cause harm, and collaboration between insiders and external threat actors to conduct coordinated cyberattacks.

When examining the motives behind insider threats, agency risk assessments indicate that the primary targets of such attacks are sensitive organizational information, followed by the organization's software or information systems, and finally, financial assets that may serve as a form of monetary gain or reward resulting from the cyberattack.

Thailand National Cyber Risk Assessment Report 2025

3.2 Critical Information Infrastructure (CII) Agency Risk Assessment Results

3.2.1 National Security Sector



Government agencies responsible for national security prioritize information confidentiality, recognizing that any compromise of their data could directly affect the nation's sovereignty, credibility, and overall stability.

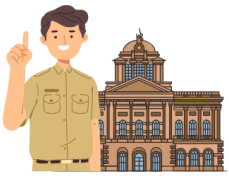


The key takeaways from the above risk metrics can be summarized as follows:

1) The majority of identified risks pertain to cyber threats aimed at system intrusion, interception, or theft of critical information.
2) Most risks are categorized as low-level and within acceptable tolerance thresholds.
3) High-level risks requiring immediate mitigation include the following:

- External threat actors exploiting weak system configurations to destroy critical data or compromise information systems related to information and technology asset management.
- Unauthorized intrusions into systems or networks through vulnerabilities in software and network devices, targeting assets associated with information and technology management or executive operations, with the intent to steal data transmitted within or across networks.
- External attackers attempting to steal intelligence-related information or corrupt incomplete data by exploiting software vulnerabilities and human negligence or carelessness.
- Delivery of targeted malware by external threat actors to compromise systems associated with key organizational resources, exploiting weaknesses in software security.

3.2.2 Critical Government Service



Agencies classified as key public service providers maintain close engagement with citizens and hold the largest volume of citizen-related data, which is essential across multiple sectors for public service delivery. Consequently, this sector prioritizes data availability, accuracy, and the protection of sensitive information to prevent unauthorized disclosure or leakage.



The key takeaways from the above risk metrix can be summarized as follows:

- The majority of cyber threats identified involve attempts to steal or disclose information without authorization, as well as attacks targeting system availability through various methods.
- Most risks are considered within acceptable levels, commonly stemming from DDoS attacks or unauthorized access to information technology assets.
- System intrusion attempts and targeted malware infections—often delivered through files or software—occur frequently but generally do not cause significant impact.

The critical risks identified by agencies as requiring immediate mitigation include the following:

- External attackers infiltrating systems and disclosing sensitive information related to information and technology management, as well as general government data, by exploiting software vulnerabilities.
- External threat actors embedding specialized malware designed to target internal systems that handle general government information, leveraging existing software weaknesses.
- Targeted malware attacks launched by external actors to gain control of information systems and extract government-related data, exploiting system software vulnerabilities.
- Lack of standardized procedures for patch management may allow external attackers to exploit unaddressed vulnerabilities in systems related to information and technology management, enabling future intrusions or security breaches.

3.2.3 Financial and Banking Sector



Agencies classified under the financial and banking sector maintain close association with financial assets and therefore place strong emphasis on the dimensions of availability and integrity. Their information systems must ensure continuous service operations and accurate, reliable financial data at all times. Any service disruption or data inaccuracy could directly undermine confidence in the nation's financial and economic systems.



The key takeaways from the above risk matrix can be summarized as follows:

- The overall cyber threat risks in this sector are concentrated within the medium to high impact range, though their likelihood of occurrence remains low. Most incidents involve attacks on system availability, attempts to gain unauthorized data access, and the use of various types of malware.
- All identified risks have been effectively maintained within the medium level, with no high-risk items recorded in the risk register. Consequently, the key strategic approach is to further mitigate and reduce the potential impact of these existing risks.

- As this sector maintains strict cybersecurity controls, the primary risks involve fraud attempts exploiting human vulnerabilities, such as social engineering or phishing, to deceive personnel and gain unauthorized access to sensitive information. Attackers may also exploit system weaknesses that fail to effectively filter phishing-based intrusions aimed at data theft.
- Risks were also identified concerning threat actors impersonating suppliers to infiltrate organizations—either by embedding malware into hardware or software components or by establishing fake entities to conduct cyberattacks.
- Website or web application defacement attacks, which alter publicly available content without authorization, are assessed as high-impact risks due to their potential to damage the reputation and trust of a sector known for its strong cybersecurity posture.
- The key risks that agencies have identified as requiring continuous monitoring and mitigation include the following:

  - Malware spread via removable media (e.g., USB) due to low cyber awareness among staff.
  - Specialized malware attacks targeting financial systems through undetected software flaws.
  - DDoS attacks disrupting financial and IT assets by exploiting weak traffic filtering.
  - Insider coercion or manipulation causing system disruption or degradation.
  - Website hacking and defacement through software vulnerabilities.
  - Zero-Day attacks on financial management assets.
  - Physical access breaches using stolen personal data.
  - Privileged insider colluding with external actors in multi-stage attacks.
  - External control and data theft from financial systems via software vulnerabilities.

3.2.4 Information and Telecommunications Technology Sector



Agencies classified under the information technology and telecommunications sector play a critical role, as their digital infrastructure and communication networks serve as the backbone connecting the nation's entire information systems and services. Any service disruption or outage could therefore have widespread impacts on the operations of all sectors and the daily lives of citizens.



The key takeaways from the above risk matrix can be summarized as follows:

(1) Overall cyber threat risks in this sector are generally at an acceptable low level, primarily involving system intrusion attempts, attacks on service availability, and data theft incidents.

(2) Malicious actors, whether individuals or organized groups, may conduct social engineering schemes—manipulating situations to access critical information by exploiting (3) human vulnerabilities or insufficient system screening mechanisms.

The immediate risks requiring prompt mitigation include the following:

- Firmware and privileged account exploits used to access critical facilities.
- External data and device theft from information systems.
- Modified malware/ransomware attacks disrupting core network operations.

3.2.5 Transportation and Logistics Sector



Agencies classified under the transportation and logistics sector manage information systems that are vital for coordinating and controlling the movement of goods and services nationwide. Any disruption or data inaccuracy could directly impact the supply chain and transportation safety.

Impact			
	A.4 | A.43 | A.50 | A.51 | A.62 | A.69 | DE.1 | I.10 | I.11 | IA.64 | IA.65 | IA.67 | IA.69 | IS.101 | IS.36 | IS.37 | IS.48 | IS.52 | IS.83 | MC.24 | MC.25	I.56 | IA.30 | IA.37 | IS.62 | IS.63 | IS.68 | MC.6	
	Reduce Impact	High	Critical
	A.36 | AC.7 | I.1 | I.34 | I.57 | I.59 | I.71 | IA.14 | IA.41 | IA.43 | IA.66 | IA.7 | IA.70 | IA.9 | IA.91 | IS.22 | IS.64 | IS.90 | MC.31	A.11 | A.17 | AC.6 | I.13 | I.37 | I.48 | I.62 | I.63 | IA.26 | IG.19 | IG.7 | IS.105	A.64 | AC.1 | IA.16 | IA.35 | IA.36 | IG.13 | IG.5 | IS.82 | MC.4 | MC.5
	Monitor	Balance	High-Control
	IA.10 | IA.60 | IS.103 | IS.53	F.20 | I.29 | I.44 | I.45 | I.58 | IA.11 | IA.59 | IA.8 | IS.54 | IS.61 | IS.89	A.12 | A.22 | A.6 | A.7 | IS.38 | IS.60 | IS.84
	Acceptance	Reduce	Prevention
		Likelihood	

The key takeaways from the above risk matrix can be summarized as follows:

(1) Overall cyber threat risks in this sector have a low likelihood of occurrence but a moderate to high impact, primarily involving system intrusions, Information Content Security, and Availability attack.

(2) The most frequent risk type involves unauthorized access, typically exploiting weak configurations that cause data leakage to the internet, as well as internal system vulnerabilities—including Zero-Day exploits targeting technology management assets.

(3) There are identified risks of insiders collaborating with outsider in coordinated campaigns, exploiting management routines to facilitate attacks, or using physical access of authorized staff to allow external intruders into organizational premises.

(4) Unauthorized access by both domestic and foreign threat actors to IT management assets is among the most frequently reported risks.

(5) Since logistics systems must connect with external platforms to enable end-to-end services, there is a risk of man-in-the-middle (MITM) attacks that intercept sensitive data transmissions, as well as data theft from system components or devices for further exploitation or unauthorized disclosure.

(6) The expansion of external service integrations—aimed at enhancing operational efficiency—has increased the attack surface, creating risks of attacks that disable transportation and IT systems, potentially causing significant service disruption.

(7) The critical risks requiring immediate mitigation are as follows:

- Outsider exploiting human vulnerabilities to degradation or denial of attacker-selected services or capabilities.
- Outsider conducting phishing attacks by leveraging human weaknesses to gain access to transportation data.
- Insiders exposing administrative routine vulnerabilities, enabling coordinate a campaign of multi-staged attacks.
- Internal personnel exploiting trust relationships with colleagues to obtain sensitive transportation information (social engineering).
- Threat actors opportunistically stealing critical financial, transportation, or IT management data from systems or system components.

3.2.6 Energy and Utilities Sector



Agencies classified under the energy and utilities sector oversee critical national infrastructure that is interconnected with all other sectors and essential for daily life and national operations—such as electricity, water supply, and energy systems. Any disruption or failure in these services could have severe consequences for public safety and the quality of life across the country.

Impact			
	IG.15		A.1 | A.2 | A.4 | A.44 | AC.6 | F.15 | F.7 | I.23 | I.26 | I.27 | I.39 | I.7 | IA.34 | IA.41 | IA.51 | IA.53 | IA.55 | IA.72 | IA.74 | IG.2 | IG.22 | IG.24 | IG.26 | IG.27 | IS.106 | IS.13 | IS.14 | IS.37 | IS.40 | IS.53 | IS.59 | IS.80 | IS.84 | IS.85 | MC.21 | MC.32 | MC.33 | MC.34 | MC.40
	Reduce Impact	High	Critical
	A.28 | A.31 | A.34 | A.40 | A.70 | AC.10 | F.22 | I.16 | I.17 | I.18 | I.42 | I.5 | I.6 | IA.46 | IA.5 | IA.83 | IS.124 | IS.125 | IS.26 | IS.43 | IS.74 | IS.76 | MC.48 | MC.49 | MC.52 | MC.53 | MC.55 | MC.57	IS.120	
	Monitor	Balance	High-Control
	A.16 | A.33 | F.17 | I.43 | I.51 | IA.19 | IA.20 | IA.22 | IA.81 | IA.82 | IG.12 | IG.14 | IS.118 | IS.119 | IS.19 | IS.28 | IS.55 | IS.56 | IS.75 | MC.50 | MC.51 | MC.54 | MC.56 | MC.58 | MC.60		
	Acceptance	Reduce Probability	Prevention
	Likelihood		

The key takeaways from the above risk matrix can be summarized as follows:

(1) Overall, the risks are concentrated within acceptable and critical levels, with the latter requiring immediate remediation, primarily targeting IT management assets.

(2) Exploitation of internal system vulnerabilities and unauthorized access are the most frequently cited risks, both classified as critical-level threats.

(3) There is also a risk that privileged or highly authorized insiders may disclose confidential or sensitive informationusing accounts that can easily bypass system verification mechanisms.

(4) There is a risk that external or internal threat actors may tamper with or alter critical energy-related data, causing damage. In cases where such data are used to train machine learning models, the interference could result in reduced accuracy in analysis process, classification, or prediction outcomes.

(5) External or internal attackers may embed malware into removable media to spread within the agency's network, targeting energy-related assets by exploiting software vulnerabilities.

(6) External threat actors may attack energy management systems through third-party service providers, infiltrating internal networks — these risks are currently categorized as low-level.

(7) The high-level risks that agencies should immediately threatment are as follows:

- Outsider or Ac-hoc groups launching Denial-of-Service (DoS) attacks, both simple and targeted, causing degradation or destruction of IT management assets.
- Outsider exploiting software vulnerabilities to degradation or denial of attacker-selected services or capabilities.
- Outsider conduct phishing attacks to deceive individuals with low security awareness, aiming to steal confidential or sensitive information.
- Both outsider and insider attackers exploiting software vulnerability that inadequate screening controls to compromise or take control of critical information system software.
- Outsider exploiting misconfigured systems, resulting in unauthorized exposure of critical data to the Internet.
- Outsider or ad hoc groups exploiting recently discovered software vulnerabilities to attack IT management assets, potentially gaining unauthorized system access.

3.2.7 Healthcare Sector



Agencies classified under the public health sector place strong emphasis on the dimensions of confidentiality, availability, and integrity, as they manage sensitive personal health information. Their systems must ensure continuous delivery of medical services and maintain highly accurate medical data. Any data breach, service disruption, or information inaccuracy could directly impact patients' lives and safety.

Impact			
	A.10 | A.39 | I.24 | I.25 | I.3 | I.69 | I.70 | IA.50 | IA.70 | IA.71 | IA.84 | IG.1 | IS.104 | IS.30 | IS.38 | IS.41 | IS.77 | MC.61	IS.29 | IS.44 | IS.58 | IS.87	A.49 | A.8 | F.18 | F.19 | I.72 | IA.49 | IA.88 | IA.90 | IG.16 | IS.46 | IS.47 | MC.63
	Reduce Impact	High	Critical
	A.58 | A.73 | I.36 | I.52 | IA.13 | IA.68 | IS.20 | IS.88 | MC.62	A.72 | IS.21	A.71 | IA.56 | IA.57
	Monitor	Balance	High-Control
	A.47 | DE.2 | I.19 | I.4 | IA.48 | IA.87 | IG.4 | IS.45 | IS.57	IA.32 | IS.127	I.20 | I.53
	Acceptance	Reduce Probability	Prevention
		Likelihood	

The key takeaways from the above risk matrix can be summarized as follows:

(1) Overall, the risks are concentrated within the medium and critical levels, the latter requiring immediate mitigation, as these threats primarily target health-related assets.

(2) Exploitation of internal system vulnerabilities and attempts to steal health-related data are the most frequently identified risks in this sector.

(3) Outsiders may exploit software, configuration, procedural, or hardware vulnerabilities to disrupt or degrade the performance of selected healthcare systems or services.

(4) Outsiders conduct phishing or social engineering attacks, leveraging procedural weaknesses and low cybersecurity awareness among staff to gain access to health-related assets.

(5) Internal information system vulnerabilities may be exploited in cyberattacks to access or manipulate health and information management data, potentially causing data loss or corruption.

(6) The high-priority risks requiring immediate mitigation are outlined as follows:

- Outsiders exploiting procedural weaknesses to slow down or disable selected healthcare systems or services.
- Outsiders leveraging firmware vulnerabilities to launch Denial-of-Service (DoS) attacks.
- Outsiders exploiting misconfigured internal information systems to attack health-related assets.
- Outsiders using procedural gaps and low staff awareness to gain access to and disclose sensitive health information.
- Outsiders deploying known malware, such as ransomware, into internal healthcare systems by exploiting human vulnerabilities.

3.3 Government Sector (non-CII)



Government agencies not classified as Critical Information Infrastructure (CII) provide public services and maintain official government data that must be reliable and accessible in accordance with citizens' rights. Any data errors or service disruptions could undermine public trust in governance, regulatory oversight, and citizens' entitlements and benefits.



The key takeaways from the above risk matrix can be summarized as follows:

(1) Overall, the risks are concentrated within the medium and critical levels, the latter requiring immediate mitigation, as these threats primarily target health-related assets.

(2) Exploitation of internal system vulnerabilities and attempts to steal health-related data are the most frequently identified risks in this sector.

(3) With the growing trend of digital operations via portable devices such as laptop and smartphones, Outsiders may target these devices to infiltrate or access critical organizational data, particularly from individuals with high-level access privileges to information management assets.

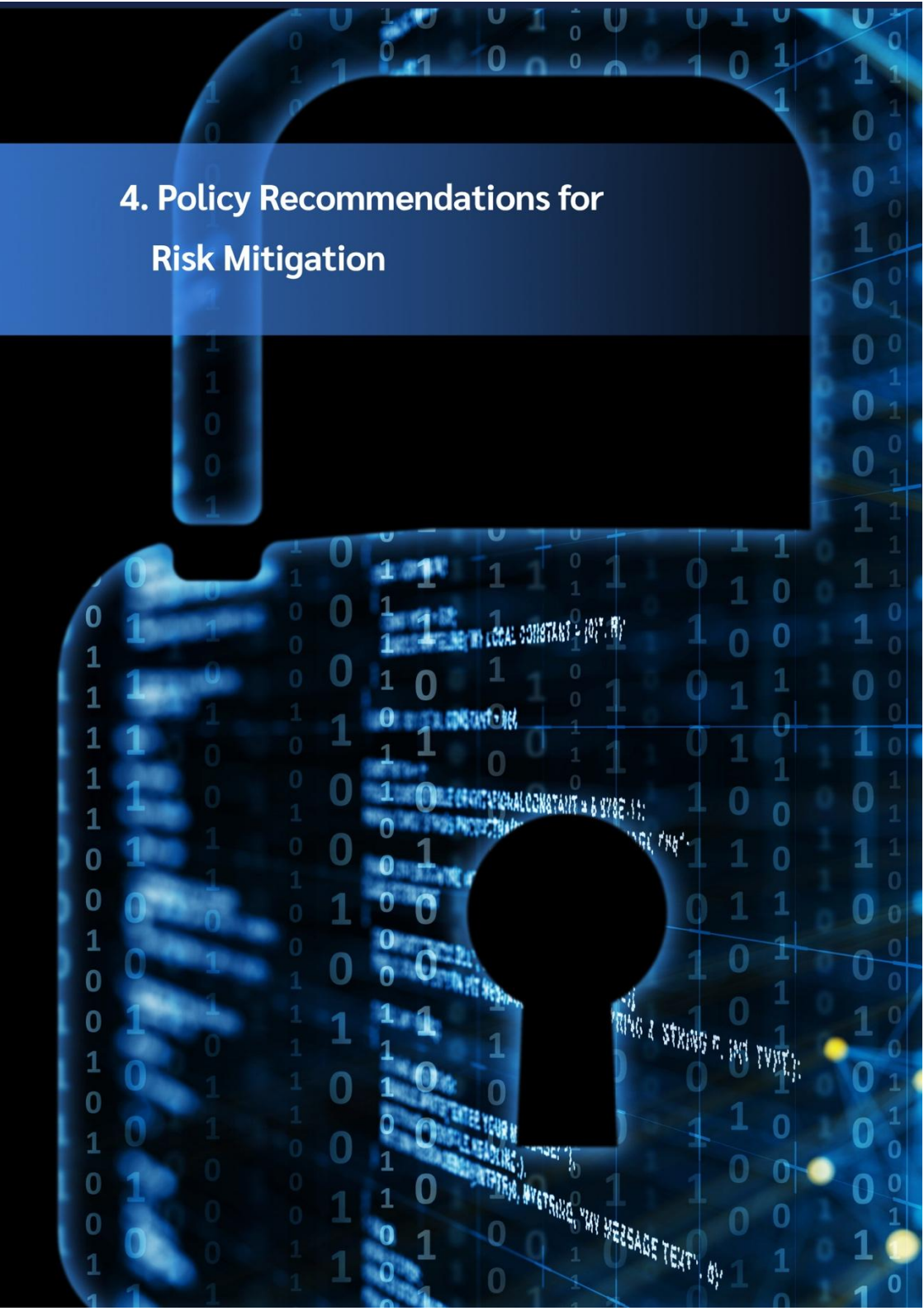
(4) Risk assessments reveal instances of internal system vulnerabilities being exploited, leading to unauthorized intrusions or access that could result in the modification or disclosure of critical organizational data.

(5) Malware-related risks range from low to medium severity, including common, specialized, and modified malware exploiting software vulnerabilities.

(6) The high-level risks requiring immediate mitigation are as follows:

- Outsiders gaining unauthorized access to assets by exploiting vulnerabilities in communication devices lacking proper intrusion detection and filtering capabilities.
- Outsiders exploiting recently discovered vulnerabilities to attack or infiltrate systems related to digital technology assets.
- Outsiders taking advantage of poorly configured information systems, resulting in the unauthorized exposure of information to the Internet.

4. Policy Recommendations for Risk Mitigation



Policy Recommendations for Risk Mitigation

4.1 Policy Recommendations for Risk Mitigation in National



Definition Standard

Establish standardized definitions for risk elements and assign reference codes to enable uniform identification and comparison of equivalent components across agencies.

Laws/Regulations

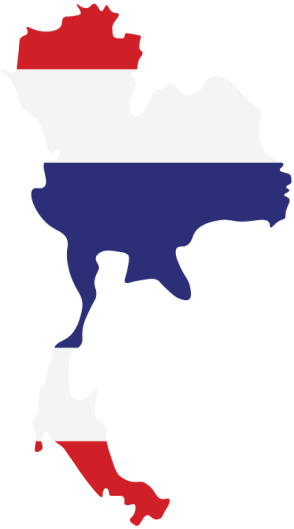
- Develop a national cybersecurity master plan and strategy aligned with current threat landscapes.
- Promote the establishment of national cybersecurity performance indicators to assess progress and guide policy enhancement.
- Enforce cybersecurity laws and regulations strictly.
- Update preventive measures and policies to address emerging technologies such as quantum computing, AI safety, third-party risks, and cyber risk cooperation.

Investment in Essential Infrastructure and Technologies

- Promote the development of Thai-origin software and technologies.
- Establish a “National Threat Intelligence Platform.”
- Allocate budgets to enhance infrastructure for threat detection and incident response (SOC, CERT) to improve operational efficiency.

Policy Recommendations for Risk Mitigation

4.1 Policy Recommendations for Risk Mitigation in National



Development of Cybersecurity Capabilities and Human Resources

- Promote cyber threat monitoring training for the public, corporations, startups, and SMEs.
- Foster domestic and international cooperation and networks for training on cyber risk awareness, focusing on Cyber Awareness — understanding common attack types such as phishing, DDoS, brute-force attacks, and malware, as well as system vulnerability management and data protection and handling.
- Organize practical training and roadshows featuring simulated cyberattack exercises (e.g., DDoS or malware spread via USB), including procedures for incident reporting, evidence collection, and initial response.





Policy Recommendations for Risk Mitigation

4.2 Policy Recommendations for Risk Mitigation in Critical Information Infrastructure (CII) Agency



Enhancement of Vulnerability Management Standards

- Conduct regular vulnerability scanning and remediation.
- Establish strict standards for patch management and secure configuration.

Establish an Early Warning and Threat Intelligence Sharing System

- Develop a National Threat Intelligence Platform connecting all sectors.
- Enable real-time sharing of threat information (IOC/Threat Feed).

Strengthening Human Resources and Capacity Building

- Provide cybersecurity training and skill development for personnel at all levels.
- Promote international certification programs (e.g., CISSP, CISM, CEH).

Policy Recommendations for Risk Mitigation

4.3 Policy Recommendations for Risk Mitigation in Government

Establish National Cybersecurity Standards for Government Agencies



- Encourage all agencies to conduct risk assessments in accordance with NCSA standards.
- Develop a Baseline Security Standard for all agencies based on NIST CSF and ISO 27001, aligned with the Cybersecurity Act B.E. 2562 (2019).
- Enforce timely vulnerability management and remediation measures.
- Require all agencies to maintain IR and DR plans consistent with national standards.

Empower Government Personnel with Advanced Cybersecurity Competencies

- Provide foundational cybersecurity training for government officials at all levels.
- Develop deep technical experts and support professional certification programs.

Integrate Interagency Cybersecurity Collaboration

- Collaborate with cloud providers, telecom operators, and the energy sector to strengthen collective defenses against complex cyber threats.

NCSA anus

CYBERCRIME AWARENESS

Think Before You Click
Avoid suspicious links and unknown attachments.

Protect Your Passwords
Use strong, unique passwords for every account.

Update Regularly
Keep your software and antivirus up to date.

Beware of Phishing
Don’t share personal info via email or messages.



5. Conclusion and Future Directions



Conclusion and Future Directions

The National Cyber Risk Assessment Report, conducted under the Thailand National Cyber Risk Assessment Framework (NCRAF) for Fiscal Year 2025, reveals a rapidly evolving and increasingly complex cyber threat landscape. The assessment highlights a growing trend of targeted attacks against government agencies, Critical Information Infrastructure (CII) sectors, and interconnected digital service ecosystems. These threats manifest through various forms such as the exploitation of internal system vulnerabilities, unauthorized access, Distributed Denial of Service (DDoS) attacks, and ransomware incidents, all of which have systemic impacts on Thailand's economy and national security.

When compared with international standards and global indices such as the Global Cybersecurity Index (GCI) and the ENISA Threat Landscape 2024, Thailand has made notable progress in terms of legal frameworks, policies, and governance mechanisms. However, there remain several gaps that require further development in three key areas:

01



TECHNICAL CAPABILITY

Leading countries have developed real-time cyber threat detection and response platforms (SOC / SOAR) that integrate data from multiple sources. In contrast, Thailand is still in the early stages of integrating cyber threat intelligence at the national level.

02



Cyber Workforce

The shortage of specialized cybersecurity professionals remains a major limitation, particularly within government agencies and critical infrastructure sectors, resulting in a lack of agility and responsiveness when addressing cyber incidents.

03



Collaboration & Intelligence

Thailand currently lacks a centralized system for efficient cyber threat information sharing among agencies, which limits situational awareness and timely response to emerging threats.

Conclusion and Future Directions

Based on this analysis, the following “future directions” are proposed to enhance the nation’s cybersecurity resilience and capability:

1. Develop a National Threat Intelligence Platform to connect data across government agencies, the private sector, and international partners, supported by AI-driven analytics for proactive threat prediction and prevention.
2. Enhance national incident response capability by establishing Sectoral CERTs operating 24/7, along with cyber range environments for simulation and hands-on training.
3. Establish a sustainable Cyber Workforce Framework by defining competency standards and career pathways to strengthen skills at all levels, particularly within government and critical infrastructure sectors.
4. Integrate legal and policy frameworks with international standards, such as NIST CSF 2.0 and ISO/IEC 27001:2022, to ensure regulatory coherence and regional interoperability.
5. Promote a nationwide culture of cyber awareness and resilience through continuous education and outreach programs that encourage safe and responsible digital behavior among personnel and the public.

These directions will help narrow the gap between Thailand and leading nations while fostering a Sustainable Cybersecurity Ecosystem driven by collaboration across all sectors government, private industry, academia, and international partners. This collective effort will strengthen the nation’s preparedness to effectively confront and adapt to emerging digital threats, ensuring Thailand’s security, prosperity, and long-term resilience in the digital era.



