การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management)

กรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

เอกสารโดย
ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC- NCSA-003
ปรับปรุงล่าสุด 30 กรกฎาคม 2567

บทนำ

บทนำ

การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องสำคัญที่มีความซับซ้อนและพัฒนาอย่างต่อเนื่องในโลกยุคดิจิทัลปัจจุบัน ความท้าทายและภัยคุกคามทางไซเบอร์ที่เกิดขึ้นสามารถส่งผลกระทบอย่างรุนแรงต่อองค์กรและสังคมโดยรวม ดังนั้น การจัดการและป้องกันภัยคุกคามเหล่านี้จึงเป็นสิ่งที่ต้องให้ความสำคัญอย่างยิ่ง

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ถูกจัดทำขึ้นเพื่อเป็นแนวทางในการระบุและจัดการกับความเสี่ยงที่อาจเกิดขึ้น โดยเริ่มจากการระบุความเสี่ยงที่อาจเกิดขึ้นในระบบและข้อมูลต่างๆ ขององค์กร ซึ่งจะช่วยให้เราสามารถเข้าใจถึงลักษณะและระดับของภัยคุกคามที่อาจเกิดขึ้นได้ดียิ่งขึ้น มาตรการป้องกันความเสี่ยงจะถูกนำมาใช้เพื่อสร้างเกราะป้องกันและลดโอกาสในการเกิดเหตุการณ์ที่ไม่พึงประสงค์ นอกจากนี้ การตรวจสอบและเฝ้าระวังภัยคุกคามอย่างต่อเนื่องจะช่วยให้เราสามารถตรวจจับและตอบสนองต่อภัยคุกคามได้ทันท่วงที หากเกิดการตรวจพบภัยคุกคาม การมีมาตรการการเผชิญเหตุที่มีประสิทธิภาพจะช่วยให้การตอบสนองเป็นไปอย่างรวดเร็วและมีระบบเพื่อลดความเสียหายและผลกระทบที่อาจเกิดขึ้น

สุดท้าย มาตรการการรักษาและฟื้นฟูความเสียหายจะช่วยให้องค์กรสามารถกลับคืนสู่สภาวะปกติได้อย่างรวดเร็ว และป้องกันไม่ให้เกิดปัญหาซ้ำอีก

กรอบมาตรฐานนี้จึงเป็นเครื่องมือที่สำคัญในการสร้างความมั่นคงและความปลอดภัยในโลกไซเบอร์ ช่วยให้การบริหารจัดการภัยคุกคามและความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและครอบคลุมทุกมิติของการดำเนินงานในยุคดิจิทัล

วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

สารบัญ

บทที่ 1
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. หลักการ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวล แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

โรงงานไพ่ กรมสรรพสามิตในฐานะหน่วยงานรัฐวิสาหกิจที่มีวัตถุประสงค์เพื่อผลิตไพ่และรับจ้างพิมพ์สิ่งพิมพ์ รวมถึงดำเนินธุรกิจที่เกี่ยวข้องหรือต่อเนื่องกับหรือเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวข้างต้น ได้จัดทำประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติจึงจัดทำประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจาก พระราชบัญญัติการรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 จากสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้การรักษาความมั่นคงปลอดภัย ไซเบอร์ของหน่วยงานรัฐปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับ มาตรฐานสากล เพื่อสนับสนุนการดำาเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

2. นิยาม

1) หน่วยงาน หมายถึง โรงงานไพ่ กรมสรรพสามิต
2) คณะกรรมการ หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
3) บริการที่สำคัญ หมายถึง ภารกิจหรือบริการของหน่วยงาน
4) ตัวชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยง เพิ่มขึ้น พร้อมทั้งสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์และความเสี่ยงในอนาคต และเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
5) ผู้ให้บริการภายนอก หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้าน เทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน หรือเป็นผู้ที่ สามารถเข้าถึงข้อมูลสำคัญของหน่วยงาน หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานได้
6) Interface หมายถึง การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์สามารถ ถ่ายโอนข้อมูลซึ่งกัน และกันได้
7) คอมไพเลอร์ (Compiler) หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรม คอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
8) แพตช์ (Patch) หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์โดยส่วนใหญ่จะอยู่ใน ลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท ไมโครซอฟท์ (Microsoft) จะ เผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบวินโดว์อัพเดท (Windows Update)

9) Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

10) Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

11) Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอม ให้การนำเนินงานตามภารกิจหยุดชะงัก เพื่อรองรับการดำเนินภารกิจหรือบริการสำคัญอย่างต่อเนื่องของ หน่วยงาน และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหาย ต่อระบบ เช่น ระยะเวลาแก้ไขภัยคุกคามให้ทำงานได้ตามปกติให้เร็วที่สุด

12) เหตุการณ์ (Event) หมายถึง การเกิดขึ้นที่สังเกตได้ (Observable Occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการลำดับ การดำเนินการ หรือบุคลากร เหตุการณ์อาจมี หรือไม่มีลักษณะ ที่ส่งผลเชิงลบก็ได้

13) เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident) หมายถึง เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการ กระทำหรือการตำาเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึง ๆ ประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่ เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของ คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

14) ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำาเนินการใด ๆ โดย มิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือ โปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

15) เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่ ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทาง สารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตาม มาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3. ขอบเขต

เอกสารนี้ครอบคลุมกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับสารสนเทศที่สำคัญของหน่วยงาน

4. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกอบไปด้วย 5 หัวข้อหลัก

4.1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

1) การจัดการทรัพย์สิน (Asset Management)

2) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

3) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

4) การจัดการผู้ให้บริการภายนอก (Third Party Management)

4.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

1) การควบคุมการเข้าถึง (Access Control)

2) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

3) การเชื่อมต่อระยะไกล (Remote Connection)

4) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

5) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

6) การแบ่งปันข้อมูล (Information Sharing)

4.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

4.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

1) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

2) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

4.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

หัวข้อหลักที่ 1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

<u>กรอบมาตรฐาน</u>

1.1. การจัดการทรัพย์สิน (Asset Management)

1.1.1 ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงาน และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

ก) ชื่อ/คำอธิบายของทรัพย์สินของบริการที่สำคัญ

ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญ

ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สินบริการที่สำคัญ

ง) เจ้าของและ/หรือผู้ค้าเนินการของทรัพย์สินของบริการที่สำคัญ

จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญแต่ละรายการ และ

ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญบนระบบเครือข่ายภายใน และ/หรือภายนอก

1.1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงาน และระบบคอมพิวเตอร์ที่ เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

1.1.3 ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละหนึ่งง (1) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

1.1.4 ต้องด่าเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการ ที่สำคัญหน่วยงาน ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละหนึ่ง (1) ครั้ง

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1.2.1 ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงาน ตามเกณฑ์ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ก้าหนดไว้ในการบริหารความเสี่ยง
(Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

1.2.2 ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

2.1 วันที่ระบุความเสี่ยง (Date the Risk is Identified)

2.2 คำอธิบายของความเสี่ยง (Description of the Risk)

2.3 โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

2.4 ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

2.5 การจัดการความเสี่ยง (Risk Treatment)

2.6 เจ้าของความเสี่ยง (Risk Owner)

2.7 สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ

2.8 ความเสี่ยงที่เหลือ (Residual Risk)

1.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

1.3.1 ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน อ้างอิงตามหลักการบริ หารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงาน ซึ่งเป็น

ก) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

ข) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

1.3.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

1.3.3 ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความ มั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลง ระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงานการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่การเพิ่มโมดูล แอปพลิเคชั่น (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

1.3.4 ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของ หน่วยงาน โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับ อินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยง จากการทดสอบเจาะระบบด้วย

1.3.5 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ ของหน่วยงานโดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

1.3.6 ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง) ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานก่อนที่ จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการ ปรับเปลี่ยนเทคโนโลยี เป็นต้น

1.3.7 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับ ประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจาก ระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการ ที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

1.3.8 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะ ระบบคำเนินการภายใต้การดูแลของหน่วยงาน

1.3.9 ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

1.3.10 หากได้รับการร้องขอจาก กกม. หรือสำนักงานหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าวไปยังสำนักงานภายในกำหนด 30 (สามสิบ) วัน นับแต่ วันที่ ได้รับหนังสือด้วย ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และ วิธีการที่หน่วยงาน ประกาศกำหนด

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

1.4.1 ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแล รักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอก คำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของหน่วยงาน

1.4.2 ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับ การเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับ ผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงานตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย
ไซเบอร์

ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์

ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ และ

ง) สิทธิ์ของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

1.4.3 ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

1.4.4. ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มี ข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

หัวข้อหลักที่ 2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

<u>กรอบมาตรฐาน</u>

2.1 การควบคุมการเข้าถึง (Access Control)

2.1.1 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานถูกจำกัดไว้ที่

ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ

ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

2.1.2 ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ 2.1.1 หน่วยงานต้องก้าหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึง บริการที่สำคัญของหน่วยงาน

2.1.3 ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายาม ทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงานและตรวจสอบ บันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็น ประจำ ความสม่าเสมอในการตรวจสอบบันทึกเหล่านี้ ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

2.1.4 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของ หน่วยงาน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทาง ลอจิคอล (Logical) มีการกำกับดูแลโดย

ก) ทำภายใต้การดูแลของหน่วยงานเท่านั้น และ

ข) นำเนินการในสถานที่ หากเป็นไปได้

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.2.1 ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการแอปพลิเคชั่น และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงาน

2.2.2 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

ข) การแบ่งแยกหน้าที่ (Separation of Duties)

ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

ง) การลบบัญชีที่ไม่ได้ใช้

จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

ช) การป้องกันมัลแวร์ (Malware) และ

ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทัน การณ์และเหมาะสม

2.2.3 ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคง ปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการ เปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

2.2.4 ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงาน อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้ แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

2.2.5 ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่อ อนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

2.3 การเชื่อมต่อระยะไกล (Remote Connection)

2.3.1 ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.2 สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็น เท่านั้น

ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของ ข้อความ (Message Integrity) ที่แข็งแกร่ง

ค) ใช้การเข้ารหัส าหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการนำเนินการบริการที่สำคัญหน่วยงาน เว้นแต่จะได้รับอนุญาต อย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ

จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

2.4.1 ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึก ข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น คอมพิวเตอร์พกพา (Laptop) กับบริการที่ สำคัญของหน่วยงาน โดยใช้มาตรการอย่างน้อย ดังนี้

ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้ งานเมื่อจำเป็น เท่านั้น

ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ 2.1.1 (ข) เท่านั้น และ

ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

2.4.2 ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึก ข้อมูลแบบถอดได้

2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.5.1 ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์(Cybersecurity Awareness) สำหรับเจ้าหน้าที่ ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- เจ้าหน้าที่ใหม่ (New Employees)
- ผู้ใช้และระดับบริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ ITและ ICS และ
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงาน

ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐานและขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ และ

ง) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความ ตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

2.5.2 ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่าง น้อยปีละ หนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

2.6 การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศและมาตรการบรรเทา ผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบ หรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้าน ความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมา

ที่ให้บริการแก่บริการที่สำคัญของหน่วยงาน และเจ้าของ คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

หัวข้อหลักที่ 3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

<u>กรอบมาตรฐาน</u>

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

3.1.1 ต้องสร้างกลไกและกระบวนการเพื่อ

ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และ

ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานหรือไม่

3.1.2 ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ 3.1.1 อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อหลักที่ 4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

<u>กรอบมาตรฐาน</u>

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้งเพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.2.1 ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่ เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.2.2 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้

ค)และแผนการดำเนินการที่เกี่ยวข้องระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย)สำหรับการเผยแพร่ข้อมูล

4.2.3 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

4.2.4 ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้ แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

4.3.1 ตามมาตรา 22 วรรคหนึ่ง (13) หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัย คุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความ มั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจ าเนินการได้ทั้งในระดับชาติ หรือระดับภาคส่วนหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ใน แผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

4.3.2 ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ ของหน่วยงานเพื่อวัตถุประสงค์ในการวางแผนและ ดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่ วิกฤตที่กำหนดขึ้นตามข้อ 4.1 และข้อ 4.2 ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของ บริการที่สำคัญของหน่วยงานคณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะ

หัวข้อหลักที่ 5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

<u>กรอบมาตรฐาน</u>

5.1. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

5.1.1. ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงรวมถึงสอบทานแผนของผู้ ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตคำ นิยามและการกำหนดระยะเวลาที่สำคัญ: Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไป ตาม หลักเกณฑ์ และวิธีการที่ สกมช. ประกาศกำหนด

5.1.2. ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อประเมิน ประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์