นโยบายและแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยไซเบอร์

สำนักงานเศรษฐกิจการเกษตร

คำนำ

สำนักงานเศรษฐกิจการเกษตร (สศก.) มีภารกิจเกี่ยวกับการเสนอแนะนโยบาย มาตรการและวางแผนพัฒนาการเกษตรและสหกรณ์ รวมทั้งจัดทำและให้บริการข้อมูลข่าวสารการเกษตรอย่างถูกต้อง รวดเร็ว และทั่วถึง โดยศึกษา วิเคราะห์ วิจัยเศรษฐกิจการเกษตร ติดตามและประเมินผล เพื่อให้การเกษตรของประเทศมีความพร้อมสำหรับการแข่งขันในตลาดโลกและเพื่อให้เกษตรกรมีคุณภาพชีวิตที่ดี ฉะนั้น สศก.จึงเป็นหน่วยงานที่มีการประมวลผลข้อมูลทางการเกษตรจำนวนมาก ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ จึงเป็นเรื่องสำคัญในการสนับสนุนให้การดำเนินภารกิจของ สศก. เป็นไปอย่างมีประสิทธิภาพและไม่กระทบต่อความมั่นคงปลอดภัยของรัฐและประเทศ

อนึ่งการตราขึ้นของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีบทบาทสำคัญในการสร้างรากฐานและความรับผิดชอบของ สศก. ทั้งรัฐและเอกชน ต่อการคุ้มครองข้อมูลของประชาชนให้พ้นจากภัยคุกคามทางไซเบอร์ ที่เพิ่มความรุนแรงขึ้นทุกวัน ภาครัฐและภาคเอกชนต้องดำเนินการสร้างความสอดคล้องต่อบทบัญญัติแห่งข้อกฎหมายที่เกี่ยวข้อง สศก. ถือเป็นหน่วยงานหนึ่งที่อยู่ภายใต้การบังคับใช้ของ พ.ร.บ. จึงจำเป็นอย่างยิ่งที่ต้องเร่งดำเนินการจัดทำนโยบายและเอกสารประกอบที่ต้องใช้ในการควบคุมกระบวนงานภายในของ สศก. ด้านความมั่นคงปลอดภัยไซเบอร์ความในข้างต้นนั้น นำมาสู่การดำเนินการจัดทำเอกสารฉบับนี้ เพื่อรวบรวมและสรุปการจัดทำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของ สศก.

คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
ของสำนักงานเศรษฐกิจการเกษตร

สารบัญ

คำนำ 1
สารบัญ 2
บทที่ 1 นโยบายความมั่นคงปลอดภัยไซเบอร์ 4
1.1 หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ 5
1.2 ภาวะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ 6
1.3 การปฏิบัติงานของเจ้าหน้าที่เพื่อความมั่นคงปลอดภัยไซเบอร์ 6
1.4 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 7
1.5 การบริหารจัดการความเสี่ยงด้านความมั่งคงปลอดภัยไซเบอร์ (Cyber Security Risk Management) 7
1.6 การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 7
1.7 แนวทางการรับมือภัยคุกคามทางไซเบอร์ 8
1.8 ช่องทางติดต่อ สศก. กรณีเกิดภัยคุกคามทางไซเบอร์ 8
บทที่ 2 นโยบายและแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ 9
2.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 9
2.2 แนวปฏิบัติของ NIST Cybersecurity Framework 14
2.3 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการเกษตร 17
บทที่ 3 ขั้นตอนการปฏิบัติงานต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ 20
3.1 ข้อมูลทั่วไป (General Information) 20
3.2 ขั้นตอนการเตรียมความพร้อมต่อการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation) 24
3.3 ขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ 27
3.4 ขั้นตอนการปฏิบัติงานตอบสนองเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ 39
3.5 ขั้นตอนอื่น ๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ 41
บทที่ 4 คู่มือการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (CYBER SECURITY PLAYBOOK) 44
4.1 ระยะการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Security Playbook Phase) 44
4.2 สถานการณ์จำลองเหตุภัยคุกคามสำหรับศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ 45
4.3 สถานการณ์จำลองเหตุภัยคุกคามสำหรับผู้ใช้งานทั่วไป 53
บทที่ 5 แผนงานการวัดประสิทธิภาพ (PERFORMANCE MATRIX) 57
5.1 แผนงานการวัดประสิทธิภาพ(Performance Matrix) ของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ 57
5.2 แผนการจัดทำรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์.. 61

สารบัญ

ภาคผนวก 64
ภาคผนวก ก: แม่แบบทะเบียนทรัพย์สิน 64
ภาคผนวก ข. แบบฟอร์มรับรายงานอุบัติการณ์ 65
ภาคผนวก ค. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำวัน 66
ภาคผนวก จ. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำสัปดาห์ 67
ภาคผนวก ช. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำเดือน 68

บทที่ 1
นโยบายความมั่นคงปลอดภัยไซเบอร์

ในปัจจุบันภัยคุกคามด้านไซเบอร์ถือเป็นหนึ่งประเด็นสำคัญในเวทีโลก สำหรับประเทศไทยนั้น การตราขึ้นของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017-2021) โดยสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี เป็นแนวนโยบายระดับชาติฉบับแรกของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้รับกับสภาพสังคมที่จะเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต อนึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ยังเป็นอีกหนึ่ง ความชัดเจนในการเตรียมความพร้อมของประเทศไทยให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์อันแสดงถึงศักยภาพของประเทศในเวทีโลก

สำนักงานเศรษฐกิจการเกษตรเป็นหน่วยงาน ที่ให้ความสำคัญอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจกระทบต่อความปลอดภัยของข้อมูลประชาชน จึงได้มีการประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

"สศก." หมายถึง สำนักงานเศรษฐกิจการเกษตร

"คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สศก." หมายถึง คณะทำงานที่มีอำนาจหน้าที่ในการกำหนดมาตรการ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สศก. รวมถึงการเฝ้าระวัง ติดตาม และประเมินผลความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์

"คณะทำงานคุ้มครองข้อมูลส่วนบุคคลของ สศก." หมายถึง คณะทำงานที่มีอำนาจหน้าที่ในการกำหนดมาตรการ แนวทางปฏิบัติและกรอบมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งการรักษาความลับของข้อมูลส่วนบุคคล และรับเรื่องร้องเรียนและดำเนินการแก้ไขการละเมิดข้อมูลส่วนบุคคลภายใต้การดูแลของ สศก.

"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" หมายถึง เจ้าหน้าที่ ซึ่งเป็นผู้แทนสำนัก/ศูนย์/กอง/สำนักงานเศรษฐกิจการเกษตรที่ 1-12 และกลุ่มพัฒนาระบบบริหาร ของ สศก. ในคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของ สศก.

"เจ้าหน้าที่" หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ตลอดจนบุคลากรของภายนอกที่จัดจ้างโดย สศก.

"ผู้บังคับบัญชา" หมายถึง เจ้าหน้าที่อาวุโสและสายบังคับบัญชาภายใต้โครงสร้างองค์กรของ สศก.

"ระบบคอมพิวเตอร์ (Computer System)" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุ อุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของ สศก. ของหน่วยงานภายนอกที่ถูกจัดจ้างหรือทรัพย์สินอยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของเจ้าหน้าที่ที่นำเข้ามาติดตั้ง หรือใช้งานภายใน สศก.

“ข้อมูลสารสนเทศ (Information Technology)” หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใด ๆ

“การรักษาความมั่นคงปลอดภัย” หรือ “ความมั่นคงปลอดภัย (Security)” หมายถึง กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใด ๆ ทั้งจากภายในและจากภายนอก ในการเข้าถึงเพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

“ไซเบอร์สเปซ (Cyberspace)” หมายถึง จินตภาพของระบบหรือพื้นที่อิเล็กทรอนิกส์หรือภูมิประเทศเสมือนที่อยู่บนการเชื่อมต่อของไซเบอร์

1.1 หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต
- ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของ สศก. ต้องไม่มีการแก้ไข ดัดแปลงโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูล และบริการได้
- ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ การเข้าถึงไซเบอร์สเปซ ต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

- การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการกระทำที่เกิดขึ้น การรักษาความมั่นคงปลอดภัยอย่างได้ผลจำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย
    - การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของเจ้าหน้าที่และบุคคลภายนอกทุกคน
    - การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
    - การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่าง ๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้เจ้าหน้าที่และบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

1.2 ภาวะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์

ผู้บังคับบัญชามีบทบาทหน้าที่สำคัญในการกำกับดูแล การปฏิบัติหน้าที่ของเจ้าหน้าที่ทุกระดับชั้นให้มีความมั่นคงปลอดภัยทางไซเบอร์ โดยสนับสนุนทรัพยากร เครื่องมือ และบุคลากรที่มีความรู้ความสามารถในการรับมือต่ออุบัติการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพ รวดเร็ว เพื่อลดผลกระทบต่อความมั่นคงปลอดภัยของประชาชน และความสงบสุขของบ้านเมือง อนึ่งผู้บังคับบัญชาต้องมีความเป็นธรรมและคงไว้ซึ่งความเสมอภาคในการสั่งการที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงการลงโทษทางวินัยแก่เจ้าหน้าที่ที่ละเมิดต่อกฎ ระเบียบ นโยบายด้านความมั่นคงปลอดภัยไซเบอร์

1.3 การปฏิบัติงานของเจ้าหน้าที่เพื่อความมั่นคงปลอดภัยไซเบอร์

เจ้าหน้าที่ต้องตระหนักทราบถึงภัยคุกคามทางไซเบอร์ และปฏิบัติตนให้สอดคล้องต่อกฎหมาย ระเบียบ และนโยบาย ด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของ สศก. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด
- ให้ความร่วมมืออย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ ข้อมูลสารสนเทศและไซเบอร์สเปซ ของ สศก.

- แจ้งให้หน่วยงานที่เกี่ยวข้องทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นอุบัติการณ์ทางไซเบอร์ หรือเหตุการณ์ที่มีแนวโน้มไปสู่อุบัติการณ์ทางไซเบอร์

1.4 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ถือเป็นพื้นฐานสำคัญที่ต้องนำมาประยุกต์ใช้เพื่อให้เกิดความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ และไซเบอร์สเปซของ สศก.

ทั้งนี้ สศก. ต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ตามที่ประกาศไว้บนเว็บไซต์ของ สศก.
(https://www.oae.go.th/assets/portals/1/files/rule/policyplan0204042565.pdf)

1.5 การบริหารจัดการความเสี่ยงด้านความมั่งคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

สศก. บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยเป็นระเบียบวิธีการเฉพาะที่พิจารณามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ตามแนวมาตรฐานสากล NIST Cybersecurity Framework และ ISO27032 และสร้างกรอบแนวทางการบริหารจัดการความเสี่ยงตามมาตรฐานสากล ISO 31000 โดยมีกระบวนการเบื้องต้นในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- การระบุและบ่งชี้ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคาม ผลกระทบและโอกาสการเกิดขึ้นของความเสี่ยงดังกล่าว
- การวิเคราะห์ระดับความเสี่ยง
- การขั้นเลือกมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง เพื่อการบริหารจัดการความเสี่ยง
- การกำหนดแนวทางการจัดการความเสี่ยงและแผนการจัดการความเสี่ยง พร้อมทั้งกำหนดเจ้าหน้าที่ผู้รับผิดชอบต่อการดำเนินการตามแผนการจัดการความเสี่ยง
- การประเมินความเสี่ยงคงเหลือ
- การติดตามและตรวจทานความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

อนึ่งผู้ดำเนินการตรวจประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต้องเป็น สศก. หรือบุคคลที่มีคุณสมบัติ คุณวุฒิ ความรู้ความเชี่ยวชาญ ด้านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หรือเป็นไปตามที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) กำหนด

1.6 การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

สศก. จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์และประสิทธิภาพของมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่ สศก. ใช้อย่างสม่ำเสมอ

อนึ่ง ผู้ดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ต้องเป็นหน่วยงานหรือบุคคลที่มีคุณสมบัติ คุณวุฒิ ความรู้ความเชี่ยวชาญ ด้านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หรือเป็นไปตามที่ กกม. กำหนด

1.7 แนวทางการรับมือภัยคุกคามทางไซเบอร์

ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ หรือไซเบอร์สเปซที่อยู่ในความรับผิดชอบของ สศก. จะดำเนินการตรวจสอบเหตุการณ์หรืออุบัติการณ์ดังกล่าวในทันที โดยมีแนวทางรับมือดังต่อไปนี้

- วางแผนการตรวจสอบและการเก็บรวบรวมหลักฐานทางดิจิทัล พยานเอกสาร พยานบุคคล หรือพยานวัตถุที่เกี่ยวข้อง
- ประเมินความเสี่ยงและสถานการณ์เพื่อกำหนดแนวทางรับมือต่อเหตุการณ์หรืออุบัติการณ์
- ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- แจ้งและรายงานผลไปยัง สศก. และหน่วยงานที่เกี่ยวข้อง อาทิ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ตามประกาศของ กกม.
- แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรง ผลกระทบจากภัยคุกคามทางไซเบอร์ และความสงบสุขของบ้านเมือง

ทั้งนี้ สศก. จะดำเนินการซ้อมแนวทางและแผนรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ หรือเมื่อ กกม. กำหนด

1.8 ช่องทางติดต่อ สศก. กรณีเกิดภัยคุกคามทางไซเบอร์

คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำนักงานเศรษฐกิจการเกษตร

ที่อยู่ : ถนนพหลโยธิน เขตจตุจักร กรุงเทพมหานคร 10900

เบอร์โทร : 02-9407038

อีเมล : csoc@oae.go.th

บทที่ 2
นโยบายและแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์

นโยบายและแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์เป็นมาตรฐานที่ สศก. พิจารณาใช้ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเป็นแนวปฏิบัติที่อ้างอิงกรอบแนวทางสากล NIST Cybersecurity Framework และปรับแต่งให้มีความสอดคล้องกับบทกฎหมาย พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งเป็นองค์ประกอบที่สำคัญในการสร้างความสอดคล้องต่อกฎหมาย (compliance) และเป็นมาตรฐานการทำงานที่ดีของหน่วยงาน (best practice)

2.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ถูกกำหนดไว้ใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตามอย่างเคร่งครัด

2.1.1 หลักการและเจตนารมณ์ของกฎหมาย

เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคมหรือการให้บริการโดยปกติของดาวเทียมในยุคปัจจุบันมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชนที่จะต้องมีการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชนไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพจึงจำเป็นต้องตราพระราชบัญญัตินี้

2.1.2 บทบัญญัติที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (ส่วนที่ 4)

มาตรา 58

ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

มาตรา 59

เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา 58 ให้หน่วยงานควบคุมหรือกำกับดูแลร่วมกับหน่วยงานตามมาตรา 50 รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยดำเนินการดังต่อไปนี้

(1) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงานในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(2) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

มาตรา 60

การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น 3 ระดับดังต่อไปนี้

(1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุขความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้

หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงครามซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด

มาตรา 61

เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้

(1) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(2) สนับสนุนให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(3) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(4) สนับสนุนให้สำนักงานและหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือและเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(5) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ตามความจำเป็นและเหมาะสมโดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(6) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

มาตรา 62

ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการดังต่อไปนี้

(1) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(2) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(3) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับภัยคุกคามทางไซเบอร์

(4) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้นผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

มาตรา 63

ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กกม. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตามวรรคหนึ่งในลักษณะที่อาจก่อให้เกิดความเสียหาย และให้ กกม. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความในวรรคหนึ่งและวรรคสองมาใช้บังคับในการร้องขอต่อเอกชนโดยความยินยอมของเอกชนนั้นด้วย

มาตรา 64

ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรงให้ กกม. ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตามวรรคหนึ่ง ให้ กกม. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใดๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

ให้เลขาธิการรายงานการดำเนินการตามมาตรานี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

มาตรา 65

ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(1) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(2) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(3) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(4) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(5) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (5) ให้ กกม. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา 66

ในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้

(1) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(2) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(3) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(4) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครอง โดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา 67

ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

มาตรา 68

ในกรณีที่เป็นเหตุจำเป็นเร่งด่วนและเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติคณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ ปราบปราม ระงับและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของคณะกรรมการหรือ กกม. มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่คณะกรรมการหรือ กกม. โดยเร็ว

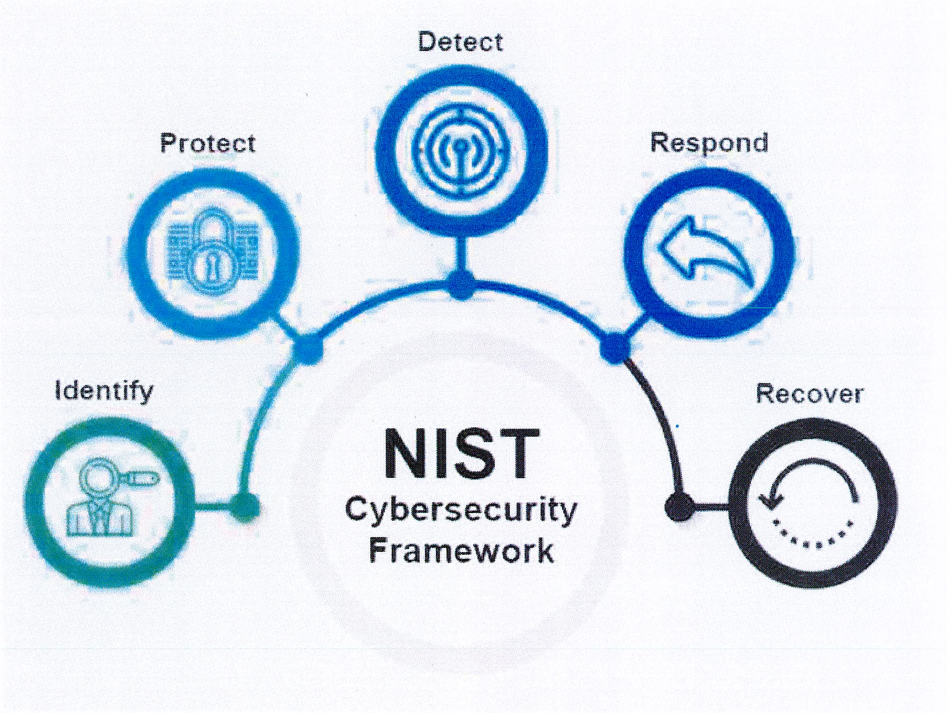
มาตรา 69

ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น

2.2 แนวปฏิบัติของ NIST Cybersecurity Framework

กรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework) เป็นหนึ่งในกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นที่นิยม กรอบแนวดังกล่าวยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลก กรอบแนวทางนี้นำเสนอหลักการและแนวทางปฏิบัติของการบริหารจัดการความเสี่ยงเพื่อยกระดับความมั่นคงปลอดภัยของ สศก. รวมไปถึงช่วยให้ สศก. สามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและเป็นระบบ กรอบแนวทางประกอบด้วย 5 ฟังก์ชั่นที่สำคัญ

- Identify การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง
- Protect การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร
- Detect การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ
- Respond การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น
- Recovery การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม



ภาพที่ 1 กรอบแนวทาง NIST Cybersecurity ในระดับฟังก์ชั่น

ทั้งนี้ในแต่ละฟังก์ชั่นจะประกอบด้วย กลุ่ม (categories) และกลุ่มย่อย (subcategories) และการกำหนดสารสนเทศอ้างอิง (information reference) โดยอธิบายได้ว่า

- กลุ่ม หมายถึง กลุ่มของกิจกรรมที่เป็นการแบ่งการทำงานออกมา ซึ่งมีเป้าประสงค์ที่ใกล้เคียงหรือสนับสนุนฟังก์ชั่น อาทิ การบริหารจัดการทรัพย์สิน (Asset Management)
- กลุ่มย่อย หมายถึง การแบ่งเนื้อหาของกลุ่มให้มีรายละเอียดที่ลึกยิ่งขึ้น ซึ่งเป็นการกำหนดเป้าหมายของกิจกรรมในระดับเทคนิคและการจัดการ และสนับสนุนเป้าหมายของกลุ่ม ได้แก่ การทำบัญชีระบบสารสนเทศภายนอก (external information system are catalogued)
- สารสนเทศอ้างอิง หมายถึง แหล่งข้อมูลอื่น ๆ ที่กรอบแนวทาง NIST Cybersecurity Framework ได้กำหนดไว้เพื่อใช้ในการอ้างอิง หรือเป็นแนวทางในการดำเนินงานเพื่อบรรลุวัตถุประสงค์ของกลุ่มและกลุ่มย่อย

2.2.1 การดำเนินการตามกรอบแนวทางในรูปแบบระดับขั้น (Framework Implementation Tiers)

ระดับขั้น (Tiers) เป็นการจัดมุมมองการบริหารจัดการกระบวนการและความเสี่ยงของหน่วยงานในการตอบสนองภัยคุกคามทางไซเบอร์ ซึ่งเป็นการแบ่งระดับขั้นเพื่อให้เกิดการวัดประเมินบริบทของหน่วยงานได้ ซึ่งสามารถจัดลำดับขั้นตั้งแต่ขั้นเริ่มต้น (Tier 1) ไปจนถึงระดับขั้นที่สูงขึ้นจนถึงระดับปรับตัว (Tier 4)

การกำหนดระดับขั้นยังเป็นกลไกสำคัญในการสร้างแรงผลักดันให้หน่วยงานมีการพัฒนาปรับปรุงกระบวนการบริหารความเสี่ยงและการจัดการภัยคุกคามทางไซเบอร์ตามความต้องการของธุรกิจ อาทิ การกำหนดตัวชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Performance Index)

การกำหนดลักษณะการจัดลำดับขั้นของหน่วยงานสามารถพิจารณาโดยยึดการวิเคราะห์กระบวนการบริหารความเสี่ยง

	Tier 1: Partial	Tier 2: Risk Informed	Tier 3: Repeatable	Tier 4: Adaptable
Risk Management Process The degree to which risk management processes are applied in alignment with organizational risk objectives, changes in business/mission requirements and a changing threat and technology landscape.	• Not formalized • Ad hoc • Prioritization is not informed	• Formalized, but no organizational-wide policy • Directly informed	• Formal • Regularly updated	• Incorporates: ○ Predictive indicators ○ Lessons Learned
Integrated Risk Management Program Definition and implementation of risk-informed policies, processes, and procedures to enable personnel to possess the knowledge and skill to perform their appointed cybersecurity roles and responsibilities.	• Irregular, case-by-case basis	• Regular, but no organizational-wide approach	• Consistent, organization-wide approach	• Cybersecurity risk management is part of the organization's culture
External Participation Understanding of an organization's role, dependencies, and dependents in the larger ecosystem by collaborating with and receiving information from other entities regularly that complements internally generated information, and sharing information with other entities	• Lack of: ○ Ecosystem understanding ○ Collaboration	• Dependencies or dependents known, but not both • Internal informal sharing	• Both dependencies and dependents are known • Internal and external information sharing	• Generates prioritized information • Communicates proactively

ภาพที่ 2 การจัดลำดับขั้นตามแนวปฏิบัติ NIST cybersecurity framework

2.2.2 ข้อมูลกรอบแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ (Framework Profile)

ข้อมูลกรอบแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์ (“ข้อมูลโปรไฟล์”) คือข้อมูลสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ข้อมูลเหล่านี้ช่วยให้หน่วยงานสามารถใช้ในการกำหนดทิศทางและการดำเนินงานของหน่วยงานให้บรรลุวัตถุประสงค์ของหน่วยงานได้อย่างเป็นแบบแผน และช่วยในการจัดลำดับความสำคัญของการดำเนินกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ได้อีกด้วย ข้อมูลโปรไฟล์ บ่งชี้ถึงสถานะปัจจุบันและอนาคต ใช้เพื่อการอธิบายและทำความเข้าใจกันในหน่วยงาน บุคลากร และบุคคลภายนอก ถึงแนวทางการดำเนินการและกิจกรรมต่าง ๆ การเปรียบเทียบระหว่างสถานะปัจจุบันและอนาคตบ่งชี้ช่องว่าง (gap) ด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานต้องดำเนินการ

2.3 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการเกษตร

แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการเกษตร ("แนวปฏิบัติ") เป็นการอ้างอิงจากแนวปฏิบัติของ NIST Cybersecurity Framework มาประยุกต์ใช้ในบริบทของ สศก. โดยมีขั้นตอนการดำเนินการดังนี้

2.3.1 ตรวจทานเบื้องต้นของหลักปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (Basic Review of Cybersecurity Practice)

ในขั้นตอนนี้ สศก. บ่งชี้กิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ที่ดำเนินการในปัจจุบันแล้วทำการเปรียบเทียบกับแนวทางของ NIST Cybersecurity Framework เพื่อบ่งชี้ช่องว่าง (gap) ของ สศก. โดยต้องจัดสรรทรัพยากรที่จำเป็นต่อการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุม กระบวนงาน บุคลากร และเทคโนโลยี

2.3.2 จัดตั้งหรือปรับปรุงไซเบอร์โปรแกรม (Establishing or Improving a Cybersecurity Program)

ขั้นตอนที่ 1 จัดลำดับความสำคัญและกำหนดขอบเขต (Prioritize and Scope)

สศก. บ่งชี้ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องต่อภารกิจและพันธกิจ โดยการพิจารณาถึงการสร้างยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องต่อยุทธศาสตร์ระดับชาติและกระทรวงเกษตรและสหกรณ์ การกำหนดความเสี่ยงที่ทนได้และระดับขั้นที่เป็นเป้าหมายของไซเบอร์โปรแกรม กำหนดเป็นขอบเขตของไซเบอร์โปรแกรมและดำเนินการจัดลำดับความสำคัญของกิจกรรมหรืองานบริการที่ต้องดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์

ขั้นตอนที่ 2: จัดการบริบท (Orient)

หลังจากที่มีการกำหนดขอบเขตและลำดับความสำคัญตามไซเบอร์โปรแกรมแล้ว สศก. บ่งชี้รายการทรัพย์สิน ระบบสารสนเทศ ข้อกำหนดของบทกฎหมายที่เกี่ยวข้อง และกระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เลือกใช้ และแหล่งข้อมูลเพื่อการบ่งชี้ภัยคุกคามและช่องโหว่ที่จะนำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในบริบทตามลำดับความสำคัญ

ขั้นตอนที่ 3 สร้างข้อมูลโปรไฟล์ปัจจุบัน (Create a Current Profile)

สศก. จัดทำข้อมูลโปรไฟล์ปัจจุบันที่รวมถึงการบ่งชี้กลุ่ม (categories) และกลุ่มย่อย (subcategories) ที่เป็นผลลัพธ์ของการประเมินศักยภาพของหน่วยงานตามฟังก์ชั่นในปัจจุบัน

ขั้นตอนที่ 4 ประเมินความเสี่ยง (Conduct a Risk Assessment)

สศก. ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยการพิจารณาถึงบริบทและผลการประเมินความเสี่ยงที่ผ่านมา โดยการบ่งชี้ถึงโอกาส (likelihood) การเกิดขึ้นของเหตุการณ์ (event) และผลกระทบ (consequence) กรณีเหตุการณ์ดังกล่าวเกิดขึ้น

ขั้นตอนที่ 5 สร้างข้อมูลโปรไฟล์เป้าหมาย (Create a Target Profile)

สศก. จัดทำเป้าหมายข้อมูลโปรไฟล์ที่รวมถึงการบ่งชี้กลุ่ม (categories) และกลุ่มย่อย (subcategories) ที่เป็นศักยภาพของหน่วยงานตามฟังก์ชั่นที่ตั้งเป็นเป้าหมายไว้ อนึ่ง สศก. สามารถบ่งชี้กลุ่มและกลุ่มย่อยเพิ่มเติมจากที่กรอบแนวทาง NIST Cybersecurity Framework ได้กำหนดไว้ขึ้นอยู่กับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นลักษณะเฉพาะของ สศก.

ขั้นตอนที่ 6 ตัดสินใจ วิเคราะห์ และจัดลำดับความสำคัญของช่องว่าง (Determine, Analyze, and Prioritize Gaps)

สศก. วิเคราะห์ช่องว่างจากการเปรียบเทียบข้อมูลโปรไฟล์ปัจจุบัน ข้อมูลโปรไฟล์เป้าหมาย และผลการประเมินความเสี่ยง เพื่อการตัดสินใจ วิเคราะห์ และจัดลำดับความสำคัญของช่องว่าง พร้อมจัดทำแผนปฏิบัติการ (Action Plan) โดยพิจารณาความคุ้มค่าและความเสี่ยงที่ได้รับการจัดการ

ขั้นตอนที่ 7 ดำเนินการตามแผนปฏิบัติการ (Implement Action Plan)

สศก. ดำเนินการตามแผนปฏิบัติการ ซึ่งสามารถอ้างอิงกรอบแนวทางมาตรฐานอื่น ๆ ที่เกี่ยวข้องหรือใช้ข้อมูลอ้างอิงตามแนวปฏิบัติของ NIST Cybersecurity Framework มาประกอบการดำเนินการตามแผนปฏิบัติ

อนึ่ง สศก. สามารถดำเนินการตามขั้นตอนข้างต้นซ้ำวนไป ตามรอบที่กำหนดในไซเบอร์โปรแกรมของ สศก. เพื่อให้มั่นใจว่า สศก. มีการติดตามการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างต่อเนื่องเป็นกิจวัตร

2.3.3 สื่อสารความต้องการด้านความมั่นคงปลอดภัยไซเบอร์กับผู้มีส่วนได้ส่วนเสีย (Communicating Cybersecurity Requirements with Stakeholders)

สศก. ใช้ข้อมูลโปรไฟล์ในการสื่อสารให้หน่วยงานผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในไซเบอร์โปรแกรม ซึ่งหมายรวมถึง

- สื่อสารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์กับผู้ให้บริการภายนอก และความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ที่หน่วยงานผู้ให้บริการเหล่านั้นต้องปฏิบัติตาม หมายรวมถึงการชี้แจงกิจกรรมที่อาจเกี่ยวข้องกับผู้ให้บริการที่ สศก. ต้องดำเนินการอาทิ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ การตรวจทานรายการมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ผู้ให้บริการมี
- สื่อสารผลการประเมินข้อมูลโปรไฟล์และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับ กกม. และคณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์ สศก.

สศก. ให้ความสำคัญในการสื่อสารภายใน สศก. เพื่อให้ทุกหน่วยงานและเจ้าหน้าที่ทุกระดับชั้นรับทราบถึงแนวทางและการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของ สศก. โดยสามารถติดตามข้อมูลข่าวสารและการแจ้งเตือนได้ตามช่องทางที่หน่วยงานจัดเตรียมไว้

2.3.4 ตัดสินใจและจัดหาทรัพยากรที่จำเป็น (Buying Decision)

แผนปฏิบัติการใดที่จำต้องมีการจัดซื้อจัดจ้างทั้งในมิติของ บุคลากร กระบวนงาน และเทคโนโลยี สศก. จะพิจารณาในแผนการจัดสรรงบประมาณซึ่งเป็นไปตามระเบียบของ สศก. และกรมบัญชีกลาง

2.3.5 บ่งชี้โอกาสในการเพิ่มหรือตรวจทานสารสนเทศอ้างอิง (Identifying Opportunities for New or Revised Informative Reference)

สศก. จัดให้มีรอบการตรวจทานสารสนเทศอ้างอิงตามกรอบแนวทาง NIST Cybersecurity Framework เพื่อให้มั่นใจว่า สศก. มีการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล (international standard) แนวปฏิบัติที่ดี (best practices) และสอดคล้องต่อบทกฎหมายที่เกี่ยวข้อง (regulatory requirements) อย่างสม่ำเสมอ

2.3.6 ระเบียบวิธีเพื่อการคุ้มครองความเป็นส่วนบุคคลและเสรีภาพพลเมือง

สศก. ตระหนักทราบและให้ความสำคัญในการคุ้มครองความเป็นส่วนบุคคลและเสรีภาพพลเมือง โดยเฉพาะของผู้ใช้บริการจาก สศก. เพื่อให้มั่นใจว่า สศก. จัดให้มีแนวทางในการคุ้มครองความเป็นส่วนบุคคล และนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลที่สอดรับกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ สศก.

บทที่ 3
ขั้นตอนการปฏิบัติงานต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

สศก. ให้ความสำคัญต่อการตอบสนองต่อเหตุการณ์และภัยคุกคามทางไซเบอร์ เพื่อให้สามารถป้องกัน ลดความรุนแรง และแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว มีประสิทธิภาพ จึงได้กำหนดขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ภายใต้ศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ อ้างอิงมาตรฐานสากล NIST.SP. 800-61r2 โดยสามารถจัดกลุ่มขั้นตอนการปฏิบัติที่ครอบคลุมดังนี้

- ข้อมูลทั่วไป (general information)
- ขั้นตอนการเตรียมความพร้อมต่อการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation)
- ขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Detection Workflow/Process)
- ขั้นตอนการปฏิบัติงานตอบสนองเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Incident Response Workflow/Process)
- ขั้นตอนอื่นๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ (Post Cyber Incident Workflow/Process)

3.1 ข้อมูลทั่วไป (General Information)

ศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ สำนักงานเศรษฐกิจการเกษตร (“ศูนย์ฯ”) เป็นหน่วยงานหลักที่มีหน้าที่ต่อการเฝ้าระวัง รับมือ และแก้ไขปัญหาที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ซึ่งมีโครงสร้างการทำงานและการกำหนดบทบาทหน้าที่ของเจ้าหน้าที่ประจำศูนย์ฯ

เวลาทำการของศูนย์ฯ	จันทร์-ศุกร์ เวลา: 08:30 – 16:30 เสาร์-อาทิตย์ เวลา: 08:30 – 16:30 วันหยุดราชการ เวลา: 08:30 – 16:30
จำนวนเจ้าหน้าที่ประจำศูนย์ฯ	20 คน
เบอร์ติดต่อ	Hotline 24x7: 02-9407038
E-mail	csoc@oae.go.th

3.1.1 เหตุการณ์ (Events) และอุบัติการณ์ (Incidents)

เหตุการณ์ หมายถึง สถานการณ์ผิดปกติที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือ ระบบเครือข่าย ซึ่งอาจ เกิดขึ้นกับผู้ใช้งานคนใดคนหนึ่ง หรือกลุ่มของผู้ใช้งานระบบสารสนเทศภายใต้การดูแลของ สศก. ขั้นตอนปฏิบัตินี้ครอบคลุมเหตุการณ์ที่เกิดขึ้นแล้วส่งผลกระทบด้านลบต่อระบบคอมพิวเตอร์และเครือข่าย ที่กระทำโดยภัยคุกคามไซเบอร์เท่านั้น เหตุการณ์ที่เกิดขึ้นอันเป็นผลมาจากภัยธรรมชาติไม่อยู่ในขอบเขต ของขั้นตอนปฏิบัตินี้

อุบัติการณ์ หมายถึง สถานการณ์ที่ละเมิดความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย ซึ่งอาจเป็นผลจากการวิเคราะห์เหตุการณ์ผิดปกติที่เกิดขึ้นมาก่อน หรือเป็นอุบัติการณ์ที่ตรวจจับได้โดยตรง (โดยไม่ต้องวิเคราะห์เหตุการณ์ เนื่องจากมีความชัดเจนของรูปแบบเหตุละเมิดที่เกิดขึ้น) ตัวอย่างอุบัติการณ์ ด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่

- ภัยคุกคามจากไวรัสคอมพิวเตอร์ทุกรูปแบบ
- การโจมตีที่ทำให้ระบบสารสนเทศ ระบบคอมพิวเตอร์ หรือระบบเครือข่ายไม่สามารถทำงานได้ หรือทำงานได้อย่างไม่เต็มประสิทธิภาพ เช่น network flood, DDOS (distributed denial of service)
- การเข้าถึงระบบสารสนเทศ ระบบคอมพิวเตอร์ หรือระบบเครือข่าย โดยไม่ได้รับอนุญาต หรือไม่ตรงตามการกำหนดสิทธิการเข้าถึง

ซึ่งในรายงานฉบับนี้จะใช้คำว่า “อุบัติการณ์” ซึ่งสามารถหมายถึงเหตุการณ์หรืออุบัติการณ์ก็ได้ แล้วแต่กรณี

3.1.2 การเปิดเผยข้อมูลแก่หน่วยงานภายนอก (sharing information with outside parties)

ในระหว่างการบริหารจัดการอุบัติการณ์ สศก. อาจมีการส่งต่อหรือเปิดเผยข้อมูลเกี่ยวกับอุบัติการณ์ ให้แก่หน่วยงานภายนอกที่เกี่ยวข้อง ซึ่งมีการกำหนดขอบเขตดังนี้

ภาพที่ 3 การเปิดเผยข้อมูลอุบัติการณ์แก่หน่วยงานภายนอก

1) กลุ่มลูกค้าและสื่อมวลชน (customers, constituents, and media)

สศก. อาจมีการเปิดเผยข้อมูลการเกิดอุบัติการณ์ให้แก่ผู้ใช้บริการภาครัฐที่ได้รับผลกระทบจากอุบัติการณ์ และการเปิดเผยต่อสื่อมวลชนทุกรูปแบบ (รวมถึงสื่อออนไลน์และโซเชียลมิเดีย) การเปิดเผยข้อมูลให้แก่หน่วยงานกลุ่มนี้ต้องได้รับอนุมัติจากผู้บริหารสูงสุดของ สศก. เท่านั้น และมีการตรวจทานข้อมูลก่อนมีการเปิดเผยแล้ว เพื่อให้มั่นใจว่าการเปิดเผยข้อมูลดังกล่าวถูกต้อง แม่นยำ และตรงตามวัตถุประสงค์ของการสื่อสารและสร้างภาพลักษณ์ต่อการรับมือ ต่ออุบัติการณ์ที่ดีของหน่วยงาน

2) กลุ่มผู้ให้บริการภายนอกของ สศก. (software and support vendors, internet service providers)

สศก. อาจมีความจำเป็นเปิดเผยข้อมูลอุบัติการณ์แก่ผู้ให้บริการภายนอกของ สศก. อาทิ ผู้ให้บริการเครือข่ายและอินเทอร์เน็ต ผู้รับเหมาจ้างพัฒนาและบำรุงรักษาระบบสารสนเทศ หรือเจ้าของผลิตภัณฑ์ทั้งระบบสารสนเทศและอุปกรณ์เครือข่ายที่มีการติดตั้ง ใช้งาน และเกี่ยวข้องกับอุบัติการณ์ที่เกิดขึ้น โดยการให้ข้อมูลแก่หน่วยงานในกลุ่มนี้ให้เป็นอำนาจการตัดสินใจของเจ้าหน้าที่ที่รับผิดชอบและได้รับมอบหมายหน้าที่ในการจัดการอุบัติการณ์ เพื่อให้ได้ข้อมูลที่เป็นจริง ถูกต้อง และสามารถนำไปใช้ประโยชน์ในการแก้ไขอุบัติการณ์ได้เว้นแต่ผู้บังคับบัญชามีคำสั่งเป็นอื่น

3) กลุ่มหน่วยงานกำกับดูแล (law enforcement agencies and incident reporting organization)

สศก. ต้องรายงานอุบัติการณ์ให้แก่หน่วยงานที่มีหน้าที่ในการกำกับดูแล สศก. หรือมีอำนาจตามกฎหมายในการควบคุมอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดย สศก. ต้องให้ข้อมูลดังกล่าวผ่านความเห็นชอบตามกระบวนการออกหนังสือราชการของ สศก. เท่านั้น เว้นแต่เป็นการติดต่อเพื่อขอความช่วยเหลืออย่างเร่งด่วนและไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ตามกฎหมายหรือตามมาตรฐานกระบวนการที่กำหนดไว้แล้ว ทั้งนี้ ศูนย์ฯ มีหน้าที่ประสานงานหน่วยงานที่เกี่ยวข้องเพื่อการเปิดเผยข้อมูลอุบัติการณ์ อาทิ หน่วยงานด้านกฎหมายของ สศก. เพื่อประกอบการเปิดเผยข้อมูล

4) กลุ่มหน่วยงานภายในที่เกี่ยวข้อง (incident response team)

ศูนย์ฯ มีหน้าที่ประสานงานหน่วยงานที่เกี่ยวข้องอื่น ๆ หรือคณะทำงานด้านการจัดการอุบัติการณ์อื่น ๆ ของ สศก. ที่สามารถให้การสนับสนุนและช่วยเหลือการจัดการอุบัติการณ์ได้อย่างมีประสิทธิภาพ ซึ่งสามารถจำแนกดังนี้

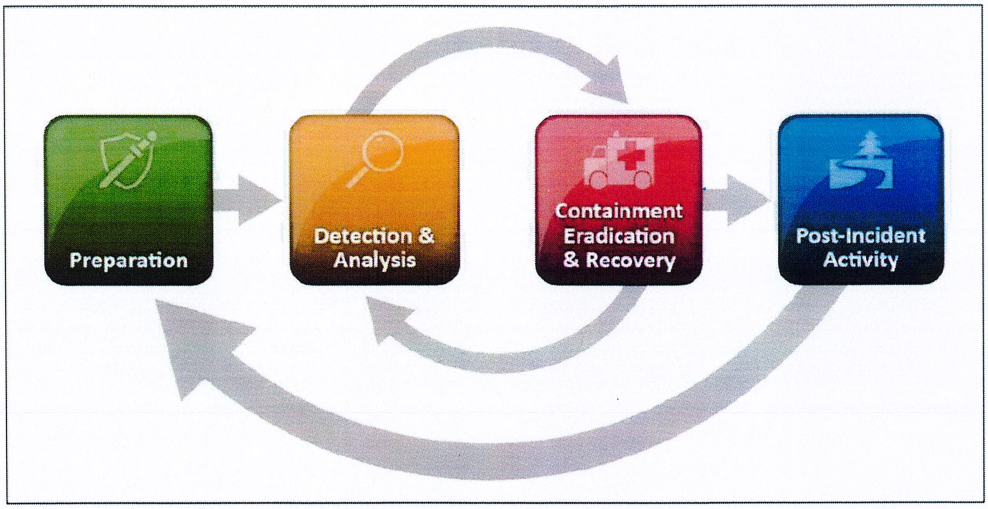
- กลุ่มผู้บริหาร (management) โดยมีหน้าที่สำคัญในการตัดสินใจ ให้คำปรึกษา นโยบาย และวางกรอบแนวทางการบริหารจัดการอุบัติการณ์ทั้งก่อน ขณะ และหลังจากการเกิดขึ้นของอุบัติการณ์
- เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ (IT staff) โดยมีหน้าที่สำคัญในการเตรียมข้อมูลสนับสนุนให้แก่ ศูนย์ฯ เพื่อให้การปฏิบัติงานเป็นไปอย่างราบรื่นและเต็มประสิทธิภาพ

- หน่วยงานด้านกฎหมาย (legal department) โดยมีหน้าที่สำคัญในการให้คำแนะนำ เพื่อสร้างความสอดคล้องต่อบทกฎหมาย หรือขั้นตอนปฏิบัติที่เกี่ยวข้องกับการดำเนินการตามกฎหมาย อาทิ การร่างสำนวนคดี
- ฝ่ายบุคคล (human resource department) โดยมีหน้าที่สำคัญในการให้คำแนะนำเกี่ยวกับนโยบาย บทลงโทษทางวินัย และข้อมูลส่วนบุคคลที่อาจเกี่ยวข้องกับการแก้ไขปัญหาอุบัติการณ์
- ฝ่ายอาคารสถานที่ (physical security and facilities department) โดยมีหน้าที่สำคัญในการให้คำแนะนำและช่วยเหลือสนับสนุนการปฏิบัติงานของศูนย์ฯ ในขอบเขตของอาคารสถานที่ และระบบสาธารณูปโภค

3.1.3 วัฏจักรการบริหารจัดการอุบัติการณ์ (incident response life cycle)

การบริหารจัดการอุบัติการณ์ของ สศก. สามารถพิจารณาเป็นวัฏจักรในการปฏิบัติตามขั้นตอนย่อย ๆ ที่จัดกลุ่มตามระยะการรับมือเป็น 4 ระยะที่อ้างอิงตามแนวทางมาตรฐานสากล NIST.SP.800-61 ดังนี้

- ระยะเตรียมความพร้อมต่อการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation) ประกอบด้วย
    - ขั้นตอนการเตรียมความพร้อมต่อการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation)
- ระยะการตรวจจับและวิเคราะห์ (Detection and Analysis) ประกอบด้วย
    - ขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Detection Workflow/Process)
- ระยะการจัดการและกู้คืน (Containment Eradication and Recovery)
    - ขั้นตอนการปฏิบัติงานตอบสนองเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Incident Response Workflow/Process)
- ระยะหลังจากอุบัติการณ์ (Post-Incident Activity) ประกอบด้วย
    - ขั้นตอนอื่น ๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ (Post Cyber Incident Workflow/Process)

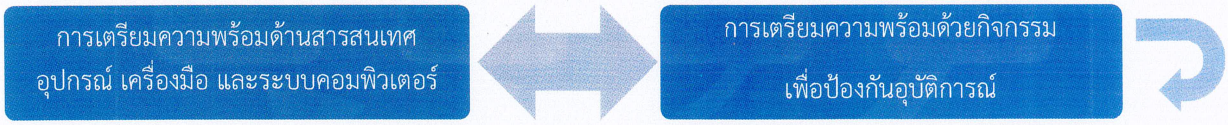


ภาพที่ 4 วัฏจักรการบริหารจัดการอุบัติการณ์อ้างอิงมาตรฐานสกาล NIST.SP.800-61

3.2 ขั้นตอนการเตรียมความพร้อมต่อการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation)

ในขั้นตอนนี้ประกอบด้วยขั้นตอนย่อย ๆ ที่เป็นวัฏจักรการปฏิบัติงานอย่างสม่ำเสมอหรือตามรอบความถี่ที่กำหนดไว้เป็นนโยบายของ สศก. ดังนี้

- การเตรียมความพร้อมด้านสารสนเทศ อุปกรณ์ เครื่องมือ และระบบคอมพิวเตอร์
- การเตรียมความพร้อมด้วยกิจกรรมเพื่อป้องกันอุบัติการณ์



3.2.1 การเตรียมความพร้อมด้านสารสนเทศ อุปกรณ์ เครื่องมือ และระบบคอมพิวเตอร์

ในการเตรียมความพร้อมเพื่อการรับมือต่ออุบัติการณ์ สศก. จัดให้มีสารสนเทศ เครื่องมือ อุปกรณ์ระบบสารสนเทศ ตลอดจนสถานที่ เพื่อใช้สนับสนุนก่อน ขณะ และหลังการเกิดอุบัติการณ์ดังนี้

เอกสาร	รายละเอียด	อ้างอิง/ข้อมูลปัจจุบัน
การสื่อสารและสนับสนุน		
ข้อมูลติดต่อ	ข้อมูลการติดต่อผู้รับผิดชอบหลัก (primary) และผู้รับผิดชอบรอง (secondary) ของแต่ละหน่วยงานทั้งภายในและภายนอกที่เกี่ยวข้อง	รายชื่อเจ้าหน้าที่ระดับบริหารและปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ช่องทางติดต่อหลัก	ช่องทางการติดต่อในการรายงานปัญหาสถานการณ์และการให้ข้อมูลใด ๆ ก่อน ขณะและหลังการเกิดอุบัติการณ์	csoc@oae.go.th 02-9407038

เอกสาร	รายละเอียด	อ้างอิง/ข้อมูลปัจจุบัน
ระบบการติดตามอุบัติการณ์	ระบบหรือเครื่องมือที่ใช้ในการบันทึก เพื่อการติดตามสถานะ ขั้นตอน และการดำเนินการ	ระบบการรักษาความปลอดภัยทางไซเบอร์ Trend Micro
อุปกรณ์สื่อสาร	อุปกรณ์สื่อสารของ สศก. ที่จำเป็นใช้ทั้งในและนอกเวลาราชการ รวมถึงรายชื่อผู้มีอำนาจถือครองตามรอบการจัดสรรเวลาที่กำหนดขึ้น	สศก. พิจารณาดำเนินภายหลัง
ห้องมั่นคง (war room)	บริเวณหรือสถานที่ที่มีความมั่นคงปลอดภัย ใช้เพื่อการติดตามประสานงานและปฏิบัติการ (อาจเป็นสถานที่ที่กำหนดขึ้นภายนอกศูนย์ฯ ก็ได้)	ห้อง NOC ชั้น 7 อาคารวิสัยทัศน์
อุปกรณ์จัดเก็บอย่างปลอดภัย (Secure storage facility)	อุปกรณ์หรือเครื่องมือที่ใช้ในการจัดเก็บเอกสารทางดิจิทัล (cloud storage) และสื่อทางกายภาพ (กระดาษ, CD) ที่มีความมั่นคงปลอดภัย	อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (SAN Storage) และ ระบบจัดเก็บและแชร์ไฟล์ cloud.oae.go.th
อุปกรณ์และเครื่องมือ		
อุปกรณ์หรือเครื่องมือเพื่อสนับสนุนการทำนิติวิทยาศาสตร์คอมพิวเตอร์ (digital forensic tools and work stations)	อุปกรณ์หรือเครื่องมือที่ช่วยในการเก็บรวบรวมหลักฐานจากภัยคุกคาม อาทิ การสร้าง disk image (การโคลนระบบ) การเก็บรักษาข้อมูลคอมพิวเตอร์ (computer log file)	สศก. พิจารณาดำเนินภายหลัง
คอมพิวเตอร์ (computer/laptop)	เครื่องคอมพิวเตอร์เพื่อการทำงาน เช่น การวิเคราะห์ข้อมูลภัยคุกคาม โดยมีการกำหนดสิทธิที่เป็นระดับสูงสุดหรือเหมาะสม	คอมพิวเตอร์ จำนวน 1 เครื่อง
อุปกรณ์สำรองอื่น ๆ	อุปกรณ์สำรองอื่น ๆ ทั้งทางระบบเครือข่ายและระบบคอมพิวเตอร์	อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (SAN Storage)
สื่อบันทึกข้อมูล	ใช้เพื่อการบันทึกข้อมูล (โดยจัดหาไว้ใช้งานเฉพาะเมื่อเกิดอุบัติการณ์ เพื่อให้เกิดความเข้าใจตรงกัน เมื่อเป็นไปได้ให้เป็นชนิดและประเภทที่สามารถเพิ่มความปลอดภัยของสารสนเทศที่ถูกบันทึกได้)	อุปกรณ์จัดเก็บข้อมูลภายนอกสำหรับสำรองข้อมูล (Backup Storage)

เอกสาร	รายละเอียด	อ้างอิง/ข้อมูลปัจจุบัน
เครื่องพิมพ์เอกสาร	เพื่อการจัดพิมพ์เอกสาร (โดยจัดหาไว้ใช้งานเฉพาะเมื่อเกิดอุบัติการณ์ ในศูนย์ฯ หรือในห้องมั่นคง เมื่อเป็นไปได้ให้เป็นชนิดที่สามารถควบคุมการทำงานในขณะสั่งพิมพ์ เพื่อให้เกิดความมั่นคงปลอดภัยสารสนเทศในสิ่งพิมพ์)	เครื่องพิมพ์สี 1 เครื่อง
อุปกรณ์ตรวจจับข้อมูลบนระบบเครือข่าย (packet sniffers and protocol analyzers)	เพื่อการตรวจจับและวิเคราะห์ข้อมูลบนระบบเครือข่าย รวบถึงการวิเคราะห์โปรโตคอลที่ใช้ (สำหรับภัยคุกคามทางเครือข่ายที่มีลักษณะการโจมตีผ่านการใช้โปรโตคอลบางประเภท)	ระบบป้องกันการโจมตีทาง DDoS (DDoS Protection)
โปรแกรมสำหรับนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (digital forensic software)	โปรแกรมเฉพาะเพื่อการวิเคราะห์และจัดการข้อมูลที่เกี่ยวข้องกับนิติวิทยาศาสตร์ทางคอมพิวเตอร์ อาทิ การวิเคราะห์ hard disk	สศก. พิจารณาดำเนินภายหลัง
อุปกรณ์การจัดเก็บหลักฐานอื่น ๆ	อุปกรณ์หรือเครื่องมือในการจัดเก็บหลักฐานอื่น ๆ อาทิ สมุดบันทึก เครื่องบันทึกเสียง เครื่องบันทึกภาพถ่าย และสายผ้าพันกั้นบริเวณ	อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (SAN Storage)
ข้อมูลสารสนเทศของเครือข่ายและระบบคอมพิวเตอร์		
รายการพอร์ท (port lists)	รายการหมายเลขพอร์ท (port numbers) ของอุปกรณ์บนระบบเครือข่ายที่มีการเปิดใช้งานทั้งหมด และรายการระบบสารสนเทศที่บ่งชี้การใช้งานพอร์ท	สศก. พิจารณาดำเนินภายหลัง
คู่มือระบบปฏิบัติการ (Operating Manual)	คู่มือระบบปฏิบัติการ ระบบสารสนเทศ อุปกรณ์เครือข่าย และอุปกรณ์อื่น ๆ	เผยแพร่คู่มือบนเว็บไซต์ สศก. intranet.oae.go.th
แผนผังเครือข่าย (network diagram)	แผนผังของระบบเครือข่ายที่บ่งชี้ลักษณะทั้งเชิงกายภาพ (physical) และเชิงตรรกะ (logical) ของการต่อเชื่อมของระบบเครือข่ายและอุปกรณ์บนระบบเครือข่าย	แผนผังเครือข่ายของ สศก.
แผนผังเครื่องแม่ข่าย	แผนผังของระบบสารสนเทศและเครื่องแม่ข่ายบ่งชี้ลักษณะทั้งเชิงกายภาพและเชิงตรรกะ ของระบบสารสนเทศที่มีการทำงานอยู่บนเครื่องแม่ข่าย, คอมพิวเตอร์ หรือเครื่องแม่ข่ายแบบ VM (virtual machine)	แผนผังเครื่องแม่ข่ายของ สศก.

เอกสาร	รายละเอียด	อ้างอิง/ข้อมูลปัจจุบัน
รหัสผ่านและไฟล์กุญแจรหัส	รหัสผ่านและไฟล์กุญแจรหัสที่อาจต้องใช้ ในการเข้าถึงระบบสารสนเทศ เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่าย	สศก. พิจารณาดำเนินภายหลัง
เครื่องมือในการลดผลกระทบจากภัยคุกคาม		
ระบบสารสนเทศ หรือโปรแกรมในการกู้คืนข้อมูล	ระบบสารสนเทศหรือโปรแกรมคอมพิวเตอร์ที่ช่วยในการกู้คืนข้อมูลคอมพิวเตอร์	ระบบการสำรองและการกู้คืนข้อมูล (Net Backup)

3.3 ขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Detection Workflow/Process)

ในขั้นตอนนี้ประกอบด้วยขั้นตอนย่อย ๆ ดังนี้

- การศึกษาลักษณะการโจมตีทางไซเบอร์ (Attack Vectors)
- การศึกษาตัวบ่งชี้อุบัติการณ์ (Signs of an Incident)
- การศึกษาแหล่งตัวบ่งชี้อุบัติการณ์ (Sources of Precursors and Indicators)
- การวิเคราะห์อุบัติการณ์ (Incident Analysis)
- การบันทึกอุบัติการณ์ (Incident Documentation)
- การจัดลำดับความสำคัญอุบัติการณ์ (Incident Prioritization)
- การแจ้งเตือนเหตุอุบัติการณ์ (Incident Notification)

3.3.1 การศึกษาลักษณะการโจมตีทางไซเบอร์ (Attack Vectors)

อุบัติการณ์สามารถเกิดขึ้นได้หลายรูปแบบ ซึ่งอาจจะเป็นไปได้ยากที่ สศก. จะกำหนดขั้นตอนการศึกษาวิเคราะห์อุบัติการณ์แบบจำเพาะ จึงจำต้องศึกษาลักษณะของการโจมตีไซเบอร์ที่เป็นไปได้เพื่อการวิเคราะห์และจัดกลุ่มรูปแบบของภัยคุกคามทางไซเบอร์ โดยการกำหนดไว้เป็นพื้นฐาน ดังนี้

- การโจมตีจากภายนอกหรือจากอุปกรณ์บันทึกข้อมูลเคลื่อนที่ (External/Removable Media): คือโจมตีมาจากการเชื่อมต่อหรือใช้งานอุปกรณ์สื่อบันทึกข้อมูล (removable media) เช่น การติดไวรัสคอมพิวเตอร์จากการใช้งาน USB flash drive
- การโจมตีแบบทำให้เสื่อมสภาพ (Attrition): คือการโจมตีด้วยวิธีการที่มีเจตนาให้ระบบสารสนเทศหรือระบบเครือข่าย เสื่อมประสิทธิภาพ หรือ หยุดชะงัก เช่น การโจมตีแบบ DDOS, การโจมตีแบบ Bruce Force เป็นต้น
- การโจมตีผ่านเทคโนโลยี Web (Web): คือการโจมตีผ่านเทคโนโลยีประเภท website หรือ web-application ตัวอย่างเช่น การโจมตีแบบ cross-site scripting
- การโจมตีผ่าน Email (Email): คือการโจมตีที่ฝังมากับการส่งจดหมายอิเล็กทรอนิกส์ (email) เช่น การฝังคอมพิวเตอร์ไวรัสในเอกสารแนบ email
- การปลอมตัวตน (Impersonation): คือการโจมตีผ่านการปลอมตัวตนผู้ใช้งานหรือการสวมรอยเป็นบุคคลอื่น ๆ เพื่อยกระดับสิทธิการเข้าถึงระบบสารสนเทศและเครือข่าย ตัวอย่างเช่น การโจมตีแบบ MITM (Man-In-The-Middle), การโจมตีแบบ Spoofing เป็นต้น

3.3.2 การศึกษาตัวบ่งชี้อุบัติการณ์ (Signs of an Incident)

ในการศึกษาตัวบ่งชี้อุบัติการณ์คือวิธีการที่เจ้าหน้าที่ประจำศูนย์ฯ ใช้ในการวิเคราะห์และบ่งชี้การเกิดขึ้นของอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นเหตุการณ์หรือความผิดปกติที่เกิดขึ้นในลักษณะที่แตกต่างกัน ตัวอย่างเช่น

- การตรวจพบอุบัติการณ์จากเครื่องมือ ระบบสารสนเทศ หรืออุปกรณ์ที่มีการติดตั้งบนระบบเครือข่าย ตัวอย่างคือ การตรวจพบภัยคุกคามจาก firewall, การตรวจพบจากระบบ Anti-Virus
- ปริมาณการสื่อสารหรือการใช้ทรัพยากรระบบสารสนเทศหรือระบบเครือข่ายที่ผิดปกติ อาทิ ปริมาณการใช้ bandwidth ที่สูงผิดวิสัย การใช้ทรัพยากรหน่วยประมวลผล (CPU) หรือหน่วยความจำชั่วคราว (RAM) ที่ผิดปกติ
- การวิเคราะห์ด้วยทักษะและประสบการณ์ของเจ้าหน้าที่ประจำศูนย์ฯ ซึ่งมาจากการตั้งข้อสังเกตส่วนบุคคล

3.3.3 การศึกษาแหล่งตัวบ่งชี้อุบัติการณ์ (Sources of Precursors and Indicators)

สศก. มีการศึกษาแหล่งตัวบ่งชี้อุบัติการณ์ ดังปรากฏในตารางต่อไปนี้

แหล่ง (Source)	คำอธิบาย (Description)
การแจ้งเตือนโดยอุปกรณ์หรือระบบ (Alert)	
IDS/IPS (Intrusion Detection System / Intrusion Prevention System)	อุปกรณ์ใช้เพื่อการตรวจจับและป้องกันภัยคุกคามส่วนมากนิยมติดตั้งเพื่อป้องกันการบุกรุกทางเครือข่าย ซึ่งเพิ่มเติมจากการป้องกันของ Firewall
SIEM (Security Information and Event Management)	อุปกรณ์ใช้เพื่อการเก็บรวบรวม บันทึก วิเคราะห์ และรายงานข้อมูล Log จากเครื่องแม่ข่าย อุปกรณ์ต่อพ่วง และอุปกรณ์บนระบบเครือข่าย
Anti-Virus System	ระบบสารสนเทศหรืออุปกรณ์ (กรณี APT) เพื่อการตรวจจับการโจมตีหรือตกเป็นเป้าหมายของโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ (Malicious Program)
File Integrity Checking	การตรวจสอบความถูกต้องของไฟล์ด้วยวิธีการที่หลากหลาย อาทิ การตรวจสอบ hash value, การตรวจสอบค่า checksum
การเฝ้าระวังโดยหน่วยงานอื่น	การเฝ้าระวังภัยคุกคามโดยผู้ให้บริการหรือหน่วยงานอื่น ๆ ที่มีส่วนเกี่ยวข้อง
ข้อมูลบันทึกทางคอมพิวเตอร์ (log)	
บันทึกของระบบปฏิบัติการ (Operating System Log)	การตรวจสอบความผิดปกติหรือการแจ้งเตือนจากบันทึกของระบบปฏิบัติการ
บันทึกบนระบบเครือข่าย (Network Log)	การตรวจสอบความผิดปกติหรือการแจ้งเตือนจากบันทึกของอุปกรณ์เครือข่ายแสดงการใช้งานเครือข่าย
ข้อมูลภัยคุกคามที่เปิดเผย (Publicly Available Information)	
ข้อมูลภัยคุกคามที่เปิดเผยโดยหน่วยงานอื่น (เช่น เจ้าของผลิตภัณฑ์)	ข้อมูลที่เกี่ยวข้องกับภัยคุกคามอาจมีการเปิดเผยและยืนยันโดยหน่วยงานอื่น ๆ สศก. มีมาตรการที่ติดตามและเฝ้าระวังการเปิดเผยข้อมูลภัยคุกคามที่มีส่วนเกี่ยวข้องกับ สศก.
บุคคล (People)	
ผู้เชี่ยวชาญ	ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์อาจมาจากการให้ข้อมูลจากผู้เชี่ยวชาญทั้งภายในและภายนอก

3.3.4 การวิเคราะห์อุบัติการณ์ (Incident Analysis)

ถ้าแหล่งตัวบ่งชี้ ตัวบ่งชี้ และลักษณะการโจมตี มีความชัดเจน แม่นยำ จะส่งผลให้การวิเคราะห์อุบัติการณ์ง่ายขึ้นและมีประสิทธิภาพ แต่ในความเป็นจริงแล้วการวิเคราะห์อุบัติการณ์อาจอยู่บนสมมุติฐานของแหล่งตัวบ่งชี้ ตัวบ่งชี้ และลักษณะการโจมตีเท่านั้น ในการวิเคราะห์อุบัติการณ์จึงต้องใช้เครื่องมือหรือมีกิจกรรมและมาตรการประกอบ ได้แก่

- การทำโปรไฟล์เครือข่ายและระบบ (Profile Networks and Systems): คือการประเมินสภาพปกติของเครือข่ายและระบบ ดังนั้นเมื่อมีการเปลี่ยนแปลงไปจากเดิมจึงเป็นที่สังเกตถึงความผิดปกติที่เกิดขึ้นได้ ตัวอย่างกิจกรรม ได้แก่ การตรวจสอบตวามถูกต้องของไฟล์เทียบกับโปรไฟล์ปัจจุบัน การตรวจความผิดปกติของการใช้ bandwidth ของเครือข่าย หรือการใช้งานที่ผิดปกติในช่วงเวลาที่ผิดแปลกไป
- ความเข้าใจในพฤติกรรมและสถานการณ์ปกติ (Understand Normal Behaviors): เจ้าหน้าที่ประจำศูนย์ฯ ควรมีความเข้าใจและคุ้นชินต่อสถานการณ์หรือพฤติกรรมการใช้งานปกติ และมีความรู้ความเข้าใจถึงบริบท การอาศัยประสบการณ์และการสังเกตของเจ้าหน้าที่จะทำให้ทราบถึงความผิดปกติเบื้องต้นที่นำไปสู่การวิเคราะห์ที่ลุกยิ่งขึ้น เช่น การตรวจบันทึก log
- การจัดเก็บบันทึก log ตามระยะเวลาที่เหมาะสม (Log Retention): เพื่อให้มีข้อมูลบันทึกที่เพียงพอต่อการวิเคราะห์ ศูนย์ฯ ต้องพิจารณาระยะเวลาการจัดเก็บข้อมูลบันทึกที่เหมาะสมในสื่อที่ง่ายต่อการเรียกดู
- การเทียบเวลามาตรฐานสากล (Clocks Synchronization): เพื่อให้ข้อมูลบันทึกจากแหล่งที่มาที่ต่างกันมีการบันทึกเวลา (time stamp) ที่สอดคล้องกันและเป็นประโยชน์ต่อการวิเคราะห์เชิงเวลา (time series) ของเหตุการณ์หรืออุบัติการณ์ที่เกิดขึ้น
- จัดการฐานองค์ความรู้ (Knowledge Database): เพื่อให้มีองค์ความรู้และสารสนเทศประกอบการศึกษาวิเคราะห์อุบัติการณ์ อาทิ ข้อมูลจากการเรียนรู้การเกิดขึ้นของอุบัติการณ์ที่ผ่านมา (previous incident lesson leant) ข้อมูลเทคนิคพิเศษที่ช่วยให้การวิเคราะห์อุบัติการณ์รวดเร็ว แม่นยำ และมีประสิทธิภาพ
- การใช้ข้อมูลเพื่อการวิจัยค้นคว้า (Search Engines for Research): แหล่งข้อมูลที่ดีอีกแหล่งคือการใช้ระบบค้นหาบน Internet ในการเข้าถึงข้อมูลมหาศาลที่เป็นประโยชน์ อาทิ หมายเลข port ของระบบต่างๆ ที่เป็นสากล
- ใช้เครื่องมือตรวจจับแพคเกตบนระบบเครือข่าย (Run Packet Sniffers to Collect Additional Data): เป็นการใช้เครื่องมือเพื่อตรวจจับข้อมูลจราจรบนระบบเครือข่ายเพิ่มเติม
- กรองข้อมูล (Filter the Data): ข้อมูลมหาศาลอาจใช้ระยะเวลานานในการวิเคราะห์อุบัติการณ์ เจ้าหน้าที่อาจใช้เทคนิคการจำกัดขอบเขตของข้อมูล (filtering) จำแนกตามประเภทเพื่อให้ การวิเคราะห์อุบัติการณ์มีเป้าหมายและขอบเขตที่แคบลงมา

- การขอคำปรึกษา (Seek Assistance from Others): ในบางสถานการณ์การขอคำปรึกษาจากหน่วยงานอื่น หรือจากผู้เชี่ยวชาญภายนอกเป็นมาตรการที่ต้องพิจารณาใช้เพื่อให้ได้ข้อมูลที่เป็นประโยชน์ต่อการขยายผลหรือวิเคราะห์อุบัติการณ์ต่อไป

3.3.5 การบันทึกอุบัติการณ์ (Incident Documentation)

ในการบันทึกอุบัติการณ์ เจ้าหน้าที่ประจำศูนย์ฯ ต้องพิจารณาความครบถ้วนของข้อมูลเกี่ยวกับอุบัติการณ์ ดังนี้

- สถานะของอุบัติการณ์ (new, in progress, forwarded for investigation, resolved, re-open, closed)
- คำอธิบายสรุปอุบัติการณ์
- ตัวบ่งชี้ แหล่งตัวบ่งชี้ และลักษณะการโจมตี
- ความเชื่อมโยงต่ออุบัติการณ์อื่น
- ขั้นตอนการจัดการที่ได้ดำเนินการไป
- ผลกระทบลูกโซ่ (ถ้ามี)
- การประเมินผลกระทบของอุบัติการณ์
- บุคคลและผู้ที่เกี่ยวข้องพร้อมช่องทางติดต่อ (ถ้ามี)
- รายการหลักฐานที่มีการเก็บรวบรวมระหว่างการสืบสวน
- คำแนะนำอื่น ๆ
- ขั้นตอนถัดไปที่ต้องดำเนินการ

3.3.6 การจัดลำดับความสำคัญ (Incident Prioritization)

การจัดลำดับความสำคัญของอุบัติการณ์ต้องพิจารณาปัจจัยที่เกี่ยวข้อง ดังนี้

- การวิเคราะห์ผลกระทบด้านการปฏิบัติงาน (Functional Impact of the Incident) เป็นการวิเคราะห์ผลกระทบต่อการปฏิบัติงานอันเนื่องจากอุบัติการณ์ที่เกิดขึ้นจากระบบสารสนเทศ
- การวิเคราะห์ผลกระทบด้านสารสนเทศ (Information Impact of the Incident) เป็นการวิเคราะห์ผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศรวมถึงการละเมิดความเป็นส่วนบุคคล
- การวิเคราะห์ผลกระทบด้านกฎหมายและสัญญา (Contractual and Legal Impact of the Incident) เป็นการวิเคราะห์ผลกระทบต่อความสอดคล้องต่อกฎหมาย หรือเป็นผลกระทบต่อเนื่องที่ทำให้หน่วยงานผิดกฎหมาย สัญญาบริการ หรือเงื่อนไขการให้บริการ

- การวิเคราะห์ความสามารถด้านการกู้คืน (Recoverability from the Incident) เป็นการวิเคราะห์ถึงขนาดและขอบเขตของอุบัติการณ์ที่กระทบต่อ ระยะเวลา ต้นทุน บุคลากร และขอบเขตที่ต้องดำเนินการแก้ไขหรือระงับเหตุ

อนึ่ง สศก. กำหนดการพิจารณาระดับผลกระทบของอุบัติการณ์ร่วมกับการกำหนดลักษณะของภัยคุกคามไซเบอร์ตาม มาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ดังนี้

ด้านผลกระทบ	ระดับไม่ร้ายแรง	ระบบที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	
		ระดับร้ายแรง	ระดับวิกฤต
การปฏิบัติงาน	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยง อย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของ สศก.หรือการให้บริการของ สศก. ด้อยประสิทธิภาพลง	ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีระบบงานของ สศก. ที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศของ สศก. ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้	เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ สศก. และมีแนวโน้มการแพร่กระจายไปในระดับประเทศ ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากของ สศก. และมีแนวโน้มที่แพร่กระจายทำให้เกิดการถูกทำลายเป็นวงกว้างในระดับประเทศหรือเป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจ

ด้านผลกระทบ	ระดับไม่ร้ายแรง	ระบบที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	
		ระดับร้ายแรง	ระดับวิกฤต
			กระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงครามซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ด้านผลกระทบ	ระดับไม่ร้ายแรง	ระบบที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	
		ระดับร้ายแรง	ระดับวิกฤต
สารสนเทศ	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความมั่นคงปลอดภัยของสารสนเทศระดับชั้นความลับสาธารณะของ สศก.	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความมั่นคงปลอดภัยของสารสนเทศระดับชั้นความลับราชการหรือข้อมูลส่วนบุคคลตามมาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
กฎหมาย	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความสอดคล้องต่อระเบียบภายใน สศก.	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความสอดคล้องต่อสัญญาบริการและความสอดคล้องด้านสัญญา	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่กระทบต่อความสอดคล้องต่อกฎหมาย
ความสามารถในการกู้คืน	การกู้คืนสามารถกำหนดระยะเวลาที่คาดหมายได้ด้วยการใช้ทรัพยากรที่มีอยู่ของหน่วยงาน	การกู้คืนสามารถกำหนดระยะเวลาที่คาดหมายได้ด้วยการใช้ทรัพยากรที่ต้องมีการจัดหาเพิ่มเติมเร่งด่วน	การกู้คืนไม่สามารถคาดการณ์หรือกำหนดระยะเวลาที่คาดหมายได้

3.3.7 การแจ้งเตือนอุบัติการณ์ (Incident Notification)

เมื่อเสร็จสิ้นการวิเคราะห์อุบัติการณ์ให้หน่วยงานดำเนินการแจ้งเตือนอุบัติการณ์แก่ผู้มีส่วนได้ส่วนเสีย และผู้ที่เกี่ยวข้องจำแนกตามระดับความรุนแรงและผลกระทบ กรณีที่การดำเนินการแก้ไขไม่สามารถดำเนินการได้ภายใต้กรอบระยะเวลาที่กำหนดไว้ให้มีมาตรการการยกระดับความรุนแรงและการแจ้งเตือน และกำหนดช่องทางการสื่อสารไว้เป็นมาตรฐานจำแนกตามความเป็นทางการของเนื้อหาการสื่อสาร ดังนี้

ลักษณะการสื่อสาร	ผู้รับสาร	ช่องทาง
การสื่อสารภายใน สศก.	เจ้าหน้าที่ภายใต้ศูนย์ฯ	Email / LINE / โทรศัพท์ หรือช่องทางอื่นใดที่พิจารณาถึงความรวดเร็วและประสิทธิภาพในการสื่อสาร
	เจ้าหน้าที่ทั่วไป	Email / ประกาศบนระบบอินทราเน็ตของ สศก.
การสื่อสารภายนอก สศก.	ประชาชน	ประกาศบนเว็บไซต์ของ สศก.
	หน่วยงานรัฐและเอกชน	• หนังสือ (ทางการ) • Email (กรณีไม่เป็นทางการ แบบไม่เร่งด่วน) • โทรศัพท์ (กรณี เร่งด่วน) หน่วยงานสามารถพิจารณาการจัดทำเอกสารหนังสือในภายหลังได้ตามความเหมาะสม การปฏิเสธการดำเนินการของหน่วยงานรัฐอื่น ๆ ด้วยเหตุผลหรือข้อจำกัดใดๆ ให้มีการบันทึกไว้เป็นหลักฐานเสมอ

เจ้าหน้าที่ประจำศูนย์ฯ สามารถพิจารณาการใช้แบบรับรายงานอุบัติการณ์ (ภาคผนวก ค.) ในกรณีไม่มีระบบสารสนเทศเพื่อการบันทึก

3.3.8 การกำหนดเงื่อนไขและกระบวนการในการเพิ่มระดับและสื่อสารเมื่อเกิดเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Incident Escalation and Communication Workflow/Process)

ในการกำหนดเงื่อนไขการเพิ่มระดับความรุนแรงและการสื่อสารใช้เกณฑ์ในการกำหนด อนึ่งการยกระดับการสื่อสารและความรุนแรงประกอบด้วย 2 ขั้นโดยมีเงื่อนไขและกระบวนการดังต่อไปนี้

- ขั้นที่ 1: การยกระดับความรุนแรงและการสื่อสารภายในหน่วยงาน สศก. อันเนื่องมาจากการดำเนินการรับมือต่ออุบัติการณ์ไม่เป็นไปตามแนวทางปฏิบัติหรือแผนงานที่กำหนดไว้เป็นมาตรฐาน อาทิ ความล่าช้าในการปฏิบัติงานของเจ้าหน้าที่ ในกรณีที่ปัญหามีแนวโน้มที่จะรุกรามและก่อให้เป็นอุบัติการณ์ในระดับที่สูงขึ้น (จะไม่ใช่การยกระดับความรุนแรงแต่เป็นการเปลี่ยนระดับความสำคัญ)
- ขั้นที่ 2: การยกระดับความรุนแรงและการสื่อสารถึงหน่วยงานภายนอกที่กำกับดูแล สศก. อาทิ กระทรวงเกษตรและสหกรณ์, หน่วยงานกำกับดูแลตามประกาศของกฎหมาย เป็นต้น เมื่อยกระดับคาวมรุนแรงถึงขั้นที่ 2 อำนาจการตัดสินใจและการดำเนินการอาจตกอยู่ภายใต้ ผู้มีอำนาจจากหน่วยงานอื่นในทันที

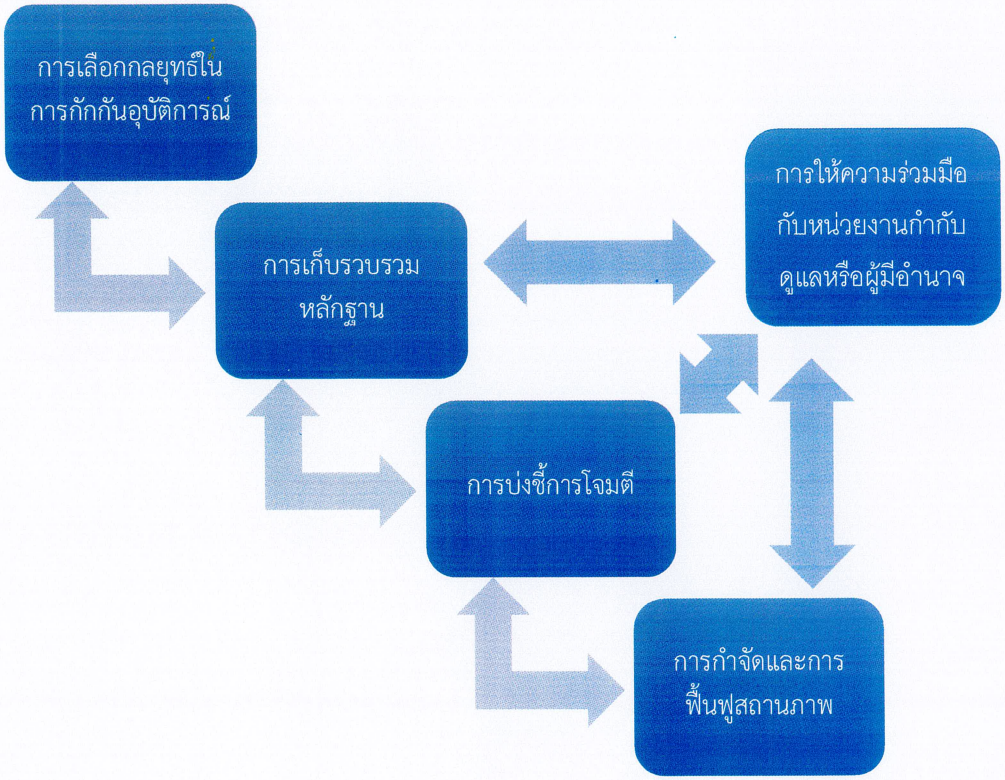
กระบวนการ/ขั้นตอน	การยกระดับ	เงื่อนไขและกรอบระยะเวลาการตอบสนอง	ระดับความรุนแรง		
			ไม่ร้ายแรง	โครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	
				ร้ายแรง	วิกฤต
ขั้นตอนการปฏิบัติงานเฝ้าระวังเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ในศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์	ปกติ	วิเคราะห์ ประเมินผลกระทบบันทึกและแจ้งเตือนเหตุอุบัติการณ์	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สศก.	กกม.	สภาความมั่นคงแห่งชาติ
	ยกระดับขั้นที่ 1	ไม่สามารถวิเคราะห์และประเมินผลกระทบได้อย่างชัดเจน	คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สศก.	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	
	ยกระดับขั้นที่ 2	ไม่สามารถวิเคราะห์และประเมินผลกระทบได้ แต่มีการรุกรานของปัญหาและอุบัติการณ์ภายใน สศก.	กระทรวงเกษตรและสหกรณ์ / หน่วยงานกำกับดูแล		
ขั้นตอนการปฏิบัติงานตอบสนองเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์	ปกติ	บ่งชี้การโจมตี เก็บรวบรวมหลักฐาน แก้ไขและกู้คืนสถานการณ์ภายในกรอบระยะเวลาตามระดับบริการ	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สศก.	กกม.	สภาความมั่นคงแห่งชาติ
	ยกระดับขั้นที่ 1	กักกันอุบัติการณ์และจำกัดผลกระทบได้ แต่ไม่สามารถบ่งชี้การโจมตี เก็บรวบรวมหลักฐาน แก้ไขและกู้คืนสถานการณ์ภายในกรอบระยะเวลาตามระดับบริการ	คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สศก.	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	
	ยกระดับขั้นที่ 2	ไม่สามารถกักกันและป้องกันการรุกรานของอุบัติการณ์ได้ภายในกรอบระยะเวลาตามระดับบริการ	กระทรวงเกษตรและสหกรณ์ / หน่วยงานกำกับดูแล	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	

กระบวนการ/ขั้นตอน	การยกระดับ	เงื่อนไขและกรอบระยะเวลาการตอบสนอง	ระดับความรุนแรง		
			ไม่ร้ายแรง	โครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	
				ร้ายแรง	วิกฤต
ขั้นตอนอื่นๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ (Post Cyber Incident Workflow/Process)	ปกติ	สรุปอุบัติการณ์ บทเรียน และจัดเก็บหลักฐานที่เกี่ยวข้อง	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สศก.	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	
	ยกระดับขั้นที่ 1	ไม่สามารถสรุปอุบัติการณ์ บทเรียน หรือจัดเก็บหลักฐาน เนื่องจากปัญหาเชิงเทคนิค	คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สศก.	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	
	ยกระดับขั้นที่ 2	หลักฐานในการดำเนินคดีสูญหายเสียหาย (กรณีมีการดำเนินคดี)	กระทรวงเกษตรและสหกรณ์ / หน่วยงานกำกับดูแล	(ดุลยพินิจของ กกม. และ สภาความมั่นคงแห่งชาติ)	

3.4 ขั้นตอนการปฏิบัติงานตอบสนองเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Incident Response Workflow/Process)

ในขั้นตอนนี้ประกอบด้วยขั้นตอนย่อย ๆ ดังนี้

- การเลือกกลยุทธ์ในการกักกันอุบัติการณ์ (Choosing a Containment Strategy)
- การเก็บรวบรวมหลักฐาน (Evidence Gathering and Handling)
- การบ่งชี้การโจมตี (Identifying the Attacking Hosts)
- การกำจัดและการกู้คืนสถานภาพ (Eradication and Recovery)
- การให้ความร่วมมือกับหน่วยงานกำกับดูแลหรือผู้มีอำนาจ (Collaboration)



3.4.1 การเลือกกลยุทธ์ในการกักกันอุบัติการณ์

การกักกันอุบัติการณ์คือการจำกัดการขยายและรุกรามของผลกระทบของอุบัติการณ์ให้อยู่ภายในขอบเขตที่สามารถควบคุมได้โดยง่ายต่อการกำจัดและการฟื้นฟูในภายหลัง ความสำคัญของการกักกันคือการตัดสินใจในการตอบโต้ต่อสถานการณ์ บริบท และเงื่อนไขต่าง ๆ ซึ่งต้องพิจารณาให้ถี่ถ้วนรัดกุม โดยสามารถพิจารณาตามเกณฑ์ประกอบการตัดสินใจได้ดังนี้

- ความเสียหายที่เกิดขึ้นและการสูญเสียทรัพยากร
- ความต้องการในคุ้มครองหลักฐาน
- ความพร้อมในบริการ
- เวลาและทรัพยากรที่ต้องใช้
- ประสิทธิภาพของกลยุทธ์ในการกักกันอุบัติการณ์

- ระยะเวลาการแก้ไขปัญหา
- ความเสี่ยงจากการใช้กลยุทธ์แต่ละวิธีในการกักกันอุบัติการณ์

ในการเลือกกลยุทธ์ที่เหมาะสม สศก. ควรพิจารณาตามเกณฑ์ดังกล่าวให้ครบทุกมิติและให้ผู้มีอำนาจตัดสินใจในการตอบสนอง อนึ่งกลไกในการกักกันภัยคุกคามบางประเภทอาจทำให้เกิดการแพร่กระจายของผลกระทบได้เช่นเดียวกัน

3.4.2 การเก็บรวบรวมหลักฐาน

เป้าหมายของการเก็บรวบรวมหลักฐานคือการได้มาซึ่งข้อเท็จจริงและสารสนเทศที่ใช้ในกระบวนการทางกฎหมายเพื่อการบ่งชี้และเอาผิดต่อผู้กระทำการให้เกิดอุบัติการณ์หรือข้อเท็จจริงเพื่อแสดงความบริสุทธิของเจตนาของเจ้าหน้าที่ประจำศูนย์ฯ ในการใช้ความสามารถเพื่อลดผลกระทบจากอุบัติการณ์ อนึ่งรายละเอียดของบันทึกที่ต้องได้รับการจัดเก็บได้แก่

- ข้อมูลบ่งชี้ผู้กระทำ อาทิ สถานที่, เลขประจำเครื่อง (serial number), เลขรุ่น (model number), ชื่อเครื่อง (hostname), หมายเลข MAC (MAC address), หมายเลข IP (IP address)
- ชื่อและข้อมูลติดต่อของผู้ส่งมอบหลักฐานหรือเก็บรวบรวมหลักฐาน
- วันและเวลาของหลักฐาน
- สถานที่ที่ได้มาซึ่งหลักฐาน

3.4.3 การบ่งชี้การโจมตี

ในการบ่งชี้การโจมตีการมีการพุ่งเป้าไปที่หลักฐานขั้นต้นที่ได้มีการเก็บรวบรวม อาทิ หมายเลข IP ที่มีการโจมตี ในบางกรณีอาจต้องมีการสังเกตการเชื่อมโยง (connectivity) ประกอบเพื่อการบ่งชี้ความเป็นไปได้อื่น นอกจากหมายเลขเครื่องที่ตรวจพบ อาทิ กรณีการใช้เครื่อง zombie ในการโจมตีเป้าหมายผ่านการสั่งการและการทำ DDOS (Distributed Denial of Service) อนึ่ง การตรวจสอบข้อมูลที่สามารถสนับสนุนการบ่งชี้การโจมตี ได้แก่

- การตรวจสอบและยืนยันหมายเลข IP Address ที่ทำการโจมตี (Validating the Attaching Host's IP address)
- การตรวจสอบการโจมตีด้วยระบบค้นหา (Researching the Attacking Host though Search Engine)
- การใช้ฐานข้อมูลอุบัติการณ์ (Using Incident Database)
- การเฝ้าระวังและตรวจสอบจากช่องทางการโจมตีที่เป็นไปได้ (Monitoring Possible Attacker Communication Channels)

3.4.4 การกำจัดและการฟื้นฟูสถานภาพ

หลังจากที่อุบัติการณ์ได้รับการควบคุมและกำจัดแล้วนั้น เช่น การลบและทำลายโปรแกรมไม่พึงประสงค์ (malware) หรือการปลดบัญชีผู้ใช้งานที่เป็นสาเหตุ (disable user account) เจ้าหน้าที่ต้องดำเนินการตรวจสอบช่องโหว่ของระบบอีกครั้ง เพื่อให้มั่นใจว่าช่องโหว่ที่ก่อให้เกิดอุบัติการณ์หรือช่องโหว่ใหม่ที่เป็นผลจากการแก้ไขอุบัติการณ์ถูกบ่งชี้และจัดการแก้ไข

ในขั้นตอนของการฟื้นฟูสถานภาพ เจ้าหน้าที่อาจตรวจสอบการกู้คืนระบบ ข้อมูลสารสนเทศ และยืนยันผลการฟื้นฟูสถานภาพกับผู้ใช้งาน ในการฟื้นฟูหมายรวมถึงการติดตั้ง patch การเปลี่ยนแปลงรหัสผ่าน การแก้ไขรายการ port ของระบบสารสนเทศ การแก้ไขรายการควบคุมการเข้าถึง (ACL: Access Control List) และการเพิ่มกระบวนการในการเฝ้าระวัง การแก้ไขและฟื้นฟูอาจเป็นลักษณะของการวางแผนระยะยาว และมีการจัดลำดับความสำคัญในการแก้ไขอย่างเป็นระบบ

3.4.5 การให้ความร่วมมือกับหน่วยงานกำกับดูแลหรือผู้มีอำนาจ

ในกรณีที่อุบัติการณ์เป็นระดับร้ายแรงหรือวิกฤต สศก. ในฐานะโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องให้ความร่วมมือต่อหน่วยงานกำกับดูแล กกม. หรือสภาความมั่นคงแห่งชาติ เพื่อการเข้าปฏิบัติหน้าที่ตามบทบัญญัติของกฎหมายที่เกี่ยวข้อง หากพิจารณาในบริบทพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สศก. ต้องให้ความร่วมมือประกอบมาตรา 61 – 68

3.5 ขั้นตอนอื่น ๆ ที่เกี่ยวข้องหลังจากเกิดเหตุการณ์ภัยคุกคามด้านไซเบอร์ (Post Cyber Incident Workflow/Process)

เมื่อสิ้นสุดอุบัติการณ์และ สศก. ได้ฟื้นฟูสถานภาพของหน่วยงานกลับสู่สถานะปกติ รวมถึงการแก้ไขปัญหาทุกประการได้แล้วเสร็จ เจ้าหน้าที่ประจำศูนย์ฯ ต้องพิจารณาการดำเนินกิจกรรมย่อย ๆ ได้แก่

- การสรุปและจัดทำบทเรียน (ถ้ามี) (Summary and Lessons Learned) (if any)
- การวัดประเมินประสิทธิภาพของศูนย์ฯ (Performance Evaluation)
- การเก็บรักษาหลักฐาน (Evidence Retention)

3.5.1 การสรุปและจัดทำบทเรียน (ถ้ามี)

เจ้าหน้าที่ประจำศูนย์ฯ ดำเนินการเขียนสรุปรายงานอุบัติการณ์ทั้งในระบบสารสนเทศที่ใช้บันทึกผลหรือตามที่ได้รับมอบหมาย พร้อมจัดส่งเผยแพร่ให้แก่เจ้าหน้าที่ประจำศูนย์ฯ ท่านอื่นเพื่อร่วมกันวิเคราะห์และเสนอข้อเสนอแนะในบันทึกรายงาน อนึ่ง การสรุปรายงานต้องคำนึงถึงสารสนเทศดังต่อไปนี้

- สาเหตุและอุบัติการณ์ที่เกิดขึ้นพร้อมวันและเวลาที่เกิดขึ้นหรือตรวจพบ (กรณีไม่ทราบแน่ชัดถึงวันและเวลาของการเกิดขึ้นของอุบัติการณ์)
- ขั้นตอนที่ได้มีการดำเนินการเพื่อการแก้ไขอุบัติการณ์รวมถึงขั้นตอนอื่น ๆ ที่มีการอ้างอิงใช้เป็นแนวทางในการจัดการอุบัติการณ์
- ข้อมูลสารสนเทศใดที่มีความสำคัญในการแก้ไขปัญหาหรือควรได้รับทราบอย่างรวดเร็วเพื่อเป็นประโยชน์ต่อการแก้ไขอุบัติการณ์
- ขั้นตอนหรือกิจกรรมใดที่เป็นประโยชน์อย่างมากต่อแก้ไขและฟื้นฟูสถานภาพ
- ขั้นตอนหรือกิจกรรมใดที่เป็นอุปสรรคอย่างมากต่อแก้ไขและฟื้นฟูสถานภาพ
- กรณีมีการเกิดขึ้นของอุบัติการณ์ลักษณะเดียวกัน อะไรคือข้อแนะนำที่จะทำให้การแก้ไขอุบัติการณ์แตกต่างออกไป
- แนวทางที่ช่วยป้องกันการเกิดอุบัติการณ์เดียวกันในอนาคต (ถ้ามี)
- สรุปแหล่งตัวบ่งชี้ ตัวบ่งชี้ และลักษณะการโจมตีที่จะทำให้การตรวจจับการเกิดขึ้นของอุบัติการณ์ ในลักษณะเดียวกันในอนาคต (ถ้ามี) เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ
- เครื่องมือหรือทรัพยากรอื่นใดที่จะเป็นประโยชน์ต่อการแก้ไขอุบัติการณ์ในลักษณะเดียวในอนาคต

เมื่อเป็นไปได้ผู้บริหารและผู้มีส่วนได้ส่วนเสียควรจัดให้มีการประชุมหารือเพื่อการสรุปผลการดำเนินการแก้ไขอุบัติการณ์ เพื่อการขยายผลหรือการแลกเปลี่ยนมุมมองและองค์ความรู้ที่ได้จากอุบัติการณ์หรือการดำเนินการแก้ไขคงค้างที่ต้องพิจารณาจัดลำดับความสำคัญในระยะยาวต่อไป อาทิ การแก้ไขสัญญาบริการกับหน่วยงานภายนอกเพื่อการตอบสนองต่ออุบัติการณ์ที่รวดเร็วยิ่งขึ้น

3.5.2 การวัดประเมินประสิทธิภาพของศูนย์

เจ้าหน้าที่ประจำศูนย์ฯ ต้องใช้ข้อมูลการเกิดอุบัติการณ์เพื่อการวัดประเมินประสิทธิภาพของศูนย์ฯ ตามตัวชี้วัดประสิทธิภาพ (Performance Matrix) ที่ได้มีการกำหนดไว้

3.5.3 การเก็บรักษาหลักฐาน

เจ้าหน้าที่ประจำศูนย์ฯ ต้องเก็บรักษาพยานหลักฐานที่เกี่ยวกับอุบัติการณ์ทั้งหมดไว้ในที่ปลอดภัยและควบคุมการเข้าถึงทั้งเชิงกายภาพและระบบ รวมถึงการเพิกถอนหรือจำกัดการเข้าถึงแม้จะเป็นบุคลากรของ สศก. ก็ตาม ในกรณีที่อุบัติการณ์ถูกสงสัยว่ามีส่วนเกี่ยวข้องกับบุคลากรภายใน สศก. ในการสมรู้ร่วมคิดหรือเพิกเฉยต่อหน้าที่จนเป็นเหตุให้เกิดอุบัติการณ์ได้ ในการพิจารณาระยะเวลาการจัดเก็บหลักฐานสามารถพิจารณาได้ดังนี้

- อายุความ: ให้ดำเนินการจัดเก็บหลักฐานตามอายุความสูงสุด (ทั้งอาญาและแพ่ง) โดยให้มั่นใจว่ามีการยื่นเรื่องทางกฎหมายและมอบหมายให้หน่วยงานด้านกฎหมายของ สศก. ดำเนินการออกเอกสารสำคัญเพื่อบ่งชี้การต่ออายุความหรือดำเนินการใดๆ ที่จำเป็นทางกฎหมายต่อไป
- นโยบาย: สศก. มีนโยบายในการจัดเก็บเอกสารและสารสนเทศภายใน ดังนั้นหลักฐานสามารถถูกจัดเก็บตามระยะเวลาที่กำหนดไว้เป็นนโยบายได้ แต่ต้องไม่ขัดต่อความจำเป็นทางกฎหมายและอายุความ กรณีที่มีการดำเนินคดี
- ต้นทุน: การจัดเก็บหลักฐานบางประเภทมีต้นทุนการจัดเก็บที่ต้องนำมาพิจารณาประกอบด้วย

บทที่ 4
คู่มือการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Security Playbook)

คู่มือการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (“คู่มือ”) เป็นเอกสารสำคัญที่เจ้าหน้าที่ประจำศูนย์ฯ ใช้ในการอ้างอิงเพื่อการกำหนดแนวทางการรับมือและตอบสนองต่อภัยคุกคามและการโจมตีทางไซเบอร์ในรูปแบบต่างๆ โดยพิจารณาจากความเสี่ยงที่ สศก. อาจต้องเป็นเป้าหมายของการโจมตี หรือพิจารณาตามระดับผลกระทบที่เกิดขึ้นกับระบบสารสนเทศและบริการของ สศก.

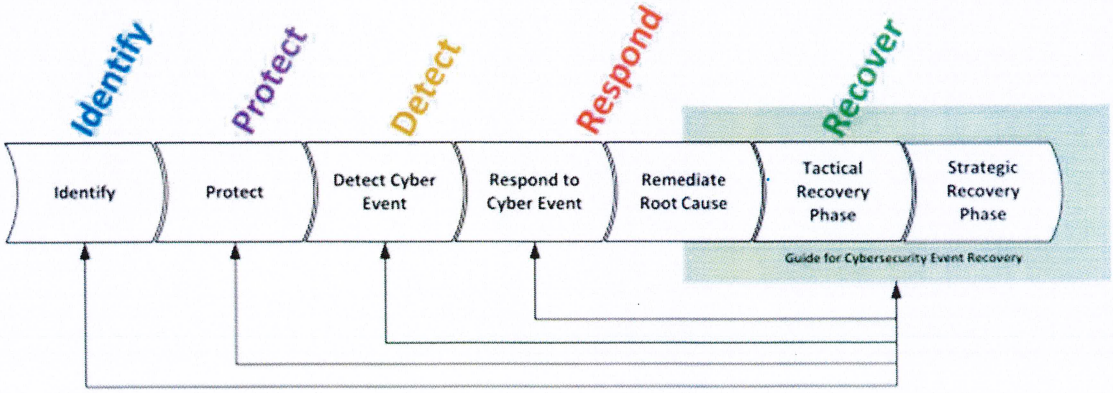
อนึ่ง การใช้คู่มือในการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์อาจมีความแตกต่างหรือดัดแปลงตามบริบทและสถานการณ์จริง ภัยคุกคามที่อยู่ในระดับร้ายแรงและวิกฤตต้องได้รับการตอบสนองหรือสั่งการจาก กกม. และสภาความมั่นคงแห่งชาติ หรือเจ้าหน้าที่ที่ได้รับการแต่งตั้ง การปฏิบัติตามคู่มือที่นอกเหนือคำสั่งอาจนำมาซึ่งผลกระทบต่อการปฏิบัติงานหรือการเก็บรวบรวมพยานหลักฐานของเจ้าหน้าที่ได้

คู่มือฉบับนี้ต้องได้รับการตรวจทานอย่างสม่ำเสมอเพื่อให้มั่นใจว่าเนื้อหาและแนวทางการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์เป็นปัจจุบัน เหมาะสมต่อบริบท และสอดรับต่อผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไวเบอร์ของ สศก. ทั้งนี้ข้อมูลและแนวทางที่นำมาประยุกต์ใช้เพื่อการออกแบบคู่มือมีแหล่งที่มาจาก แนวทางการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ของ NIST (Guide for Cybersecurity Event Recovery) (“NIST SP.800-184”)

4.1 ระยะการตอบสนองภัยคุกคามและการโจมตีทางไซเบอร์ (Cyber Security Playbook Phase)

อ้างอิงตาม NIST SP.800-184 สศก. ได้กำหนดระยะของการตอบสนองและฟื้นฟูภัยคุกคามและการโจมตีทางไซเบอร์ออกเป็น 2 ระยะได้แก่

- การฟื้นฟูเชิงกลยุทธ์ (Tactical Recovery)
- การฟื้นฟูเชิงยุทธศาสตร์ (Strategic Recovery)



ภาพที่ 5 การตอบสนองและฟื้นฟูภัยคุกคามและการโจมตีทางไซเบอร์

4.1.1 การฟื้นฟูเชิงกลยุทธ์

การพื้นฟูเชิงกลยุทธ์คือการดำเนินการรับมือและตอบสนองต่ออุบัติการณ์ตามขั้นตอนที่ระบุและวางแผนไว้ในคู่มือ การฟื้นฟูเชิงกลยุทธ์มีส่วนเกี่ยวข้องกับกิจกรรมที่ดำเนินการก่อนและระหว่างอุบัติการณ์ อาทิ

- การจัดทำสารสนเทศที่ใช้เพื่อการบ่งชี้กระบวนการ บุคลากร ตลอดจนทรัพย์สินที่มีส่วนเกี่ยวข้องกับอุบัติการณ์ การใช้แผนผังต่างๆ เช่น แผนผังเครือข่าย แผนผังเครื่องแม่ข่าย เป็นต้น
- การจัดทำบัญชีทรัพย์สินและความสัมพันธ์เพื่อการจัดลำดับความสำคัญในการฟื้นฟูอย่างเป็นระบบ
- การบ่งชี้บุคคลสำคัญผู้มีหน้าที่และความรับผิดชอบต่ออุบัติการณ์ตามสถานการณ์
- การตั้งสมมุติฐานเกี่ยวกับอุบัติการณ์ได้อย่างถูกต้องเพื่อลดระยะเวลาการฟื้นฟู
- การออกแบบและจัดทำขั้นตอนการรับมือเหตุอุบัติการณ์อย่างถูกต้อง กำหนดเป้าหมายและผลลัพธ์ของแต่ละขั้นตอน
- การตรวจทานผลการตอบสนองและฟื้นฟูเพื่อบ่งชี้กิจกรรมหรือขั้นตอนที่ต้องดำเนินการเป็นการเพิ่มเติม
- การปรับแต่งคู่มือบางประเด็นระหว่างการรับมือสถานการณ์เพื่อให้เกิดทางเลือกและแนวปฏิบัติที่ตอบสนองต่อสถานการณ์ได้อย่างมีประสิทธิภาพ

4.1.2 การฟื้นฟูเชิงยุทธศาสตร์

การพื้นฟูเชิงยุทธศาสตร์มุ่งเน้นการพัฒนาปรับปรุงองค์กรและกระบวนการในการรับมือต่ออุบัติการณ์ อาทิ

- การจัดทำแผนการพัฒนาปรับปรุงองค์กรด้านความมั่นคงปลอดภัยไซเบอร์
- การฝึกซ้อมแผนรับมือและการสื่อสารระหว่างเมื่อเกิดเหตุอุบัติการณ์อย่างสม่ำเสมอ และพัฒนาปรับปรุง กระบวนการ บุคลากร และเทคโนโลยีที่มีความสำคัญ
- การตรวจทานประสิทธิภาพของศูนย์ฯ

4.2 สถานการณ์จำลองเหตุภัยคุกคามสำหรับศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

สศก. พิจารณาเหตุภัยคุกคามที่ส่งผลกระทบสูงต่อความมั่นคงปลอดภัยไซเบอร์ โดยสามารถแบ่งเป็นกรณีศึกษาได้ดังนี้

- เหตุละเมิดความมั่นคงปลอดภัยข้อมูลเกษตรกร (Personal Data Breach by Hacker)
- การโจมตีทางไซเบอร์ด้วยโปรแกรมไม่พึงประสงค์ (Ransomware)
- การโจมตีแบบ DDOS

4.2.1 กรณีศึกษาที่ 1: เหตุละเมิดความมั่นคงปลอดภัยข้อมูลเกษตรกร

บนสมมุติฐานของการตรวจพบภัยคุกคามทางระบบเครือข่ายที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศของ สศก. และเป็นข้อมูลส่วนบุคคลของเกษตรกรในระบบ Farmer One

เงื่อนไขสำหรับการตอบสนองอย่างมีประสิทธิภาพ

- สศก. มีการจัดเตรียมสารสนเทศที่จำเป็นไว้อย่างครบถ้วนสมบูรณ์ รวมถึง รายการติดต่อเจ้าหน้าที่ภายใน รายการระบบเครื่องแม่ข่าย แผงผังระบบเครือข่าย
- สศก. มีทรัพยากรและเครื่องมือที่จำเป็นอย่างครบถ้วน

การฟื้นฟูเชิงกลยุทธ์

- เจ้าหน้าที่ประจำศูนย์ฯ ยืนยันการตรวจพบภัยคุกคามไซเบอร์ที่กระทบต่อฐานข้อมูลเกษตรกร Farmer One และยืนยันว่ามีการเผยแพร่ข้อมูลเกษตรกรจากกลุ่มผู้โจมตีบนเว็บไซต์สาธารณะทำให้เกิดการเสื่อมเสียภาพลักษณ์ของ สศก.
- คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (“คณะทำงาน”) สศก. เรียกประชุมเจ้าหน้าที่และผู้ที่เกี่ยวข้องทุกฝ่ายเพื่อมอบหมายหน้าที่และแนวทางการดำเนินการจัดการต่อเหตุอุบัติการณ์
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สศก. ดำเนินการตามกระบวนการรับมือต่อเหตุละเมิดข้อมูลส่วนบุคคลและติดต่อไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามระเบียบของกฎหมาย โดยได้รับความช่วยเหลือจากคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของ สศก. และหน่วยงานด้านกฎหมายของ สศก.
- คณะทำงาน ใช้อุปกรณ์ในการตรวจจับการเข้าระบบเครือข่าย หมายเลข IP และข้อมูลยืนยันของตัวผู้กระทำการโจมตี และทำการตรวจสอบสถานที่ในการก่อเหตุโดยประสานงานไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย เพื่อร่วมตรวจสอบ
- คณะทำงาน นำเรื่องเรียนถึงผู้อำนวยการศูนย์สารสนเทศ สศก. (“ผู้อำนวยการ”) เพื่อตัดสินใจปิดระบบ Farmer One เป็นการชั่วคราว เพื่อลดผลกระทบและความเสี่ยงแอบแฝง (hidden risk) หลังจากที่ได้มีการเก็บรวบรวมพยานหลักฐานและบันทึกทางคอมพิวเตอร์ของเครื่องแม่ข่ายของระบบ Farmer One เป็นที่เรียบร้อยแล้ว
- คณะทำงาน ดำเนินการตรวจสอบช่องโหว่ของระบบ Farmer One โดยความช่วยเหลือของหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการพัฒนาระบบ Farmer One ผลการดำเนินการยืนยันถึงช่องโหว่เชิงเทคนิคแบบ SQL Injection บนระบบ Farmer One เป็นเหตุให้ผู้โจมตีใช้ script ที่ทำให้การเข้าถึงฐานข้อมูลในระบบในส่วนของผู้ดูแลระบบ (admin right) และเรียกดูข้อมูลเกษตรกรได้

- คณะทำงาน นัดหมายประชุมหน่วยงานผู้พัฒนาและหารือถึงแนวทางการแก้ไข อนึ่ง คณะทำงานพบว่า ระบบสารสนเทศอื่นๆ ใน สศก. ก็ปรากฏช่องโหว่ในลักษณะเดียวกัน จึงได้ ขออนุมัติ จากผู้อำนวยการในการปิดระบบสารสนเทศทั้งหมดของ สศก. เป็นการชั่วคราวจนกว่า จะได้แนวทางการป้องกัน
- หน่วยงานผู้พัฒนาได้วิเคราะห์ผลและสรุปว่าต้องใช้เวลาในการพัฒนาปรับปรุงระบบมากกว่า 3 วันทำการจึงจะสามารถแก้ไขปัญหาได้
- คณะทำงาน ยื่นเรื่องต่อหน่วยงานที่เกี่ยวข้องใน สศก. เพื่อประกาศว่าระบบ Farmer One จะไม่สามารถให้บริการได้เป็นระยะเวลามากกว่า 3 วัน (รวมระยะเวลาทดสอบ) เพื่อให้หน่วยงานที่เกี่ยวข้องประกาศและสื่อสารไปยังเกษตรกรที่มีความจำเป็นใช้งาน
- หน่วยงานรับขึ้นทะเบียนเกษตรกรสามารถส่งรายการขึ้นทะเบียนเกษตรกรในรูปแบบ .csv ไว้เพื่อใช้ในการขึ้นทะเบียนเกษตรกรรายใหม่หลังจากที่มีการแก้ไขระบบ Farmer One แล้วเสร็จ
- คณะทำงานร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ประกาศแจ้งเหตุละเมิดและพร้อมดำเนินคดีหรือชดใช้ค่าเสียหายแก่เกษตรกรผู้ยื่นเรื่องร้องเรียนแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- คณะทำงานร่วมกับนิติกรนำเสนอร่างเอกสารประกอบการดำเนินคดีกับผู้กระทำผิด โดยใช้พยานหลักฐานของบันทึกการเข้าใช้ระบบ Farmer One และการเชื่อมต่อเครือข่าย

การฟื้นฟูด้านยุทธศาสตร์

- คณะทำงาน นำเสนอต่อผู้อำนวยการในการพิจารณาแก้ไขระบบสารสนเทศอื่นๆ ที่มีช่องโหว่ในลักษณะเดียวกัน โดยการจัดลำดับความสำคัญของระบบดังกล่าว และจัดประชุมนัดหมายเพื่อให้หน่วยงานผู้พัฒนาเข้าร่วมปรึกษาหารือแนวทางการแก้ไข
- คณะทำงาน รับทราบว่าหน่วยงานผู้พัฒนาบางรายปฏิเสธการแก้ไขโดยอาศัยช่องโหว่เชิงสัญญา และไม่รับผิดชอบต่อการแก้ไข เว้นแต่ สศก. จะจัดสรรงบประมาณเพื่อการแก้ไขดังกล่าว
- คณะทำงาน จัดประชุมกับหน่วยงานผู้เป็นเจ้าของระบบสารสนเทศร่วมกับนิติกรเพื่อตรวจทานร่างสัญญาพัฒนาและจัดซื้อจัดจ้าง ในการยื่นเสนอดำเนินคดี หรือไกล่เกลี่ยระหว่าง สศก. กับหน่วยงานผู้พัฒนาบางราย
- คณะทำงาน นำเสนอแนวทางการพัฒนาปรับปรุงสัญญาจ้างพัฒนาระบบ ในอนาคตให้บ่งชี้ความรับผิดชอบของหน่วยงานผู้รับจ้างต่อการแก้ไขในกรณีเกิดเหตุละเมิดความมั่นคงปลอดภัยอันพิสูจน์ได้ว่ามาจากความบกพร่องของระบบที่ถูกพัฒนา แม้ว่าจะได้รับการทดสอบจากผู้ใช้งานแล้วก็ตาม

- คณะทำงาน นำเสนอแนวทางการตรวจสอบช่องโหว่ของผลิตภัณฑ์และระบบสารสนเทศก่อนการขึ้นใช้งานภายใน สศก. โดยกำหนดเป็นข้อบังคับแก่ระบบสารสนเทศที่เชื่อมต่อจาก internet เป็นสำคัญ ต้องได้รับการตรวจสอบช่องโหว่อย่างน้อยทุกไตรมาส
- คณะทำงาน ประชุมเพื่อสรุปผลการดำเนินการต่อเหตุอุบัติการณ์

การพิจารณาการตอบสนองต่ออุบัติการณ์

- ความสอดคล้องต่อกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- การดำเนินคดีต่อผู้กระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560
- ต้นทุนและราคาของการแก้ไขปัญหาในระบบสารสนเทศของ สศก.

4.2.2 กรณีศึกษาที่ 2: การโจมตีทางไซเบอร์ด้วยโปรแกรมไม่พึงประสงค์

บนสมมุติฐานของการตรวจพบภัยคุกคามบนเครื่องคอมพิวเตอร์เจ้าหน้าที่คนหนึ่ง ในการติดไวรัสเรียกค่าไถ่ (Ransomware) (“ไวรัส”) ซึ่งเชื่อได้ว่าเกิดจากการเปิดอ่าน email ฉบับหนึ่งที่มีข้อความให้เปิดดูเอกสารไฟล์แนบ

เงื่อนไขสำหรับการตอบสนองอย่างมีประสิทธิภาพ

- สศก. มีการจัดเตรียมสารสนเทศที่จำเป็นไว้อย่างครบถ้วนสมบูรณ์ รวมถึง รายการติดต่อเจ้าหน้าที่ภายใน รายการระบบเครื่องแม่ข่าย และแผงผังระบบเครือข่าย
- สศก. มีทรัพยากรและเครื่องมือที่จำเป็นอย่างครบถ้วน

การฟื้นฟูเชิงกลยุทธ์

- เจ้าหน้าที่ประจำศูนย์ฯ ยืนยันการตรวจพบภัยคุกคามไซเบอร์ที่กระทบและกระจายไปยังเครื่องคอมพิวเตอร์แม่ข่าย ระบบแชร์ไฟล์ (File Server) และเครื่องคอมพิวเตอร์ของผู้บริหารระดับสูงอีก 2 ท่านของ สศก.
- เจ้าหน้าที่ประจำศูนย์ฯ แจ้งต่อคณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (“คณะทำงาน”) ในทันที
- คณะทำงาน สั่งการเร่งด่วนในการตัดระบบเครือข่ายของ สศก. และแยกระหว่างโซนเครือข่ายของผู้ใช้งานและโซนของเครื่องคอมพิวเตอร์แม่ข่าย ในกรณีที่ปัญหารุกราน คณะทำงานเฝ้าระวังและดำเนินการแจ้งไปยังหน่วยงานรัฐอื่นๆ ที่เกี่ยวข้องรวมถึง กกม. เพื่อเฝ้าระวังระดับความรุนแรงของอุบัติการณ์
- คณะทำงาน ใช้ช่องทางสื่อสารที่รวดเร็วที่สุดติดต่อผู้อำนวยการศูนย์สารสนเทศ สศก. เพื่อให้มีคำสั่งเร่งด่วนถึงหน่วยงานอื่น ๆ ใน สศก. ในการหยุดใช้สื่อบันทึกข้อมูลส่วนกลางและการตรวจทาน email ทุกฉบับ และไม่ให้มีการดำเนินการตามคำเรียกค่าไถ่

(ไม่จ่ายเงิน) โดยให้เจ้าหน้าที่ที่ประสบปัญหาหรือตกเป็นเหยื่อส่งรายชื่อเครื่องคอมพิวเตอร์และความจำเป็นใช้ข้อมูลต่าง ๆ ให้แก่คณะทำงาน

- กรณีระบบสารสนเทศและบริการของ สศก. ได้รับผลกระทบ ให้คณะทำงานประชุมร่วมกับเจ้าหน้าที่ของหน่วยงานอื่นๆ เพื่อประกาศปิดระบบสารสนเทศเป็นการชั่วคราว โดยการเพิ่มข้อมูลใด ๆ ในระบบให้ดำเนินการในรูปแบบ manual หรือเป็นลักษณะไฟล์บันทึก เพื่อนำข้อมูลเข้าระบบในภายหลัง
- คณะทำงานติดต่อไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย เพื่อขอการสนับสนุนแนวทางการป้องกันไวรัส โดยให้ข้อมูลชื่อไวรัส หรือลักษณะการเกิดขึ้น และข้อมูลบันทึกทางคอมพิวเตอร์ต่าง ๆ เท่าที่สามารถส่งให้ได้
- คณะทำงานติดต่อไปยังเจ้าของผลิตภัณฑ์โปรแกรมป้องกันคอมพิวเตอร์ไวรัสเพื่อปรึกษาและหารือถึงแนวทางการแก้ไขและการรับมือ รวมถึงการขอ patch ของโปรแกรมป้องกันไวรัส (ถ้ามี) เพื่อติดตั้งและทดสอบ
- คณะทำงานพิจารณาถึงความเสี่ยงในการเชื่อมต่อคอมพิวเตอร์ลูกข่ายของผู้ใช้งานกับระบบเครือข่าย กรณีมีความเสี่ยงคงเหลือให้ดำเนินการแจ้งเจ้าหน้าที่ สศก. นำเครื่องคอมพิวเตอร์ (laptop) มาให้เจ้าหน้าที่ประจำศูนย์ดำเนินการติดตั้ง patch แบบ manual หรือตามคู่มือการติดตั้งที่ทางคณะทำงานประกาศกำหนดและเผยแพร่ให้เจ้าหน้าที่ สศก. รับทราบ
- คณะทำงาน รับเรื่องความจำเป็นใช้ข้อมูล และจัดทำเครื่องคอมพิวเตอร์แม่ข่าย (VM) ชุดใหม่โดยไม่เชื่อมต่อเครือข่ายเดิมของ สศก. แล้วดำเนินการกู้คืนข้อมูลสารสนเทศส่วนกลางเพื่อส่งให้เจ้าหน้าที่หน่วยงานอื่น ๆ ที่ได้รับผลกระทบให้สามารถปฏิบัติหน้าที่ได้
- คณะทำงาน วิเคราะห์หมายเลข IP ของผู้จัดส่ง email ที่ทำให้เกิดการแพร่กระจายของไวรัส และให้เจ้าหน้าที่ที่ได้รับมอบหมายดำเนินการตรวจสอบระบบ email server เพื่อการตรวจสอบ ระงับ และป้องกัน email ในลักษณะเดียวกัน
- คณะทำงาน กู้คืนข้อมูลที่ได้มีการสำรองไว้และนำเสนอแก่ผู้อำนวยการ เพื่อจัดประชุมร่วมกับหน่วยงานอื่นๆ ที่เกี่ยวข้องในการวิเคราะห์ผลกระทบต่อสารสนเทศที่ไม่สามารถกู้คืนได้ หน่วยงานที่เกี่ยวข้องวางแผนการแก้ไขปัญหาหรือติดต่อไปยังประชาชนที่ได้รับผลกระทบ (ข้อมูลสูญหาย) โดยกำหนดมาตรฐานการติดต่อสื่อสารไปยังหน่วยงานภายนอก
- คณะทำงานดำเนินการกู้คืนระบบสารสนเทศและเปิดการเชื่อมต่อเครือข่ายเมื่อแน่ใจว่าได้ดำเนินการกำจัดไวรัสบนเครื่องที่ตกเป็นเป้าหมายได้เรียบร้อยแล้ว

การฟื้นฟูด้านยุทธศาสตร์

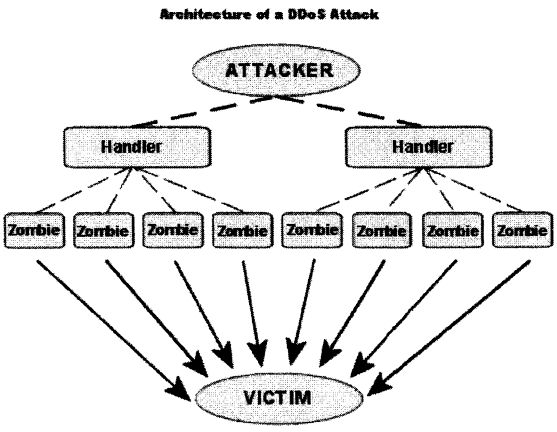
- จัดอบรมและสร้างความตระหนักทราบให้แก่เจ้าหน้าที่ของ สศก. ในการใช้ความระมัดระวังในการปฏิบัติหน้าที่และการใช้สื่อบันทึกข้อมูลที่อาจเป็นเป้าหมายการโจมตีของโปรแกรมไม่พึงประสงค์ทุกรูปแบบ
- คณะทำงานตรวจสอบประสิทธิภาพของมาตรการในการสำรองข้อมูลสารสนเทศและพิจารณาถึงความจำเป็นในการเพิ่มรอบความถี่ของการสำรองข้อมูลตามการรายงานผลกระทบจากผู้ใช้งานใน สศก.
- คณะทำงานตรวจสอบประสิทธิภาพของมาตรการในการป้องกันคอมพิวเตอร์ไวรัส (malware protection) และพิจารณาถึงความจำเป็นในการปรับเปลี่ยนแนวทางการติดตั้ง patch หรือการเลือกใช้ผลิตภัณฑ์ที่มีประสิทธิภาพรายใหม่ ๆ

การพิจารณาการตอบสนองต่ออุบัติการณ์

- ระดับสัญญาบริการของระบบสารสนเทศที่กระทบจากอุบัติการณ์ และความจำเป็นใช้ของข้อมูลสารสนเทศจากผู้ใช้งานของ สศก.
- การดำเนินคดีต่อผู้กระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560
- ต้นทุนและราคาของการกู้คืนระบบสารสนเทศหรือการใช้กระบวนการบันทึกรวบรวมสารสนเทศระหว่างการดำเนินการแก้ไขแบบ manual
- ประสิทธิภาพของมาตรการด้านการป้องกันคอมพิวเตอร์ไวรัสของ สศก. และความรับผิดชอบของเจ้าของผลิตภัณฑ์ต่อเหตุการณ์ที่เกิดขึ้น (กรณีที่ สศก. ได้ดำเนินการติดตั้ง patch อย่างถูกต้องตามรอบคำแนะนำของเจ้าของผลิตภัณฑ์แล้ว)

4.2.3 กรณีศึกษาที่ 3: การโจมตีแบบ DDOS

บนสมมุติฐานของการตรวจพบภัยคุกคามบนระบบเครือข่ายถึงการส่งคำร้อง (request) เพื่อเข้าถึงระบบสารสนเทศของ สศก. จาก internet เป็นจำนวนมาก ทำให้การตอบสนองของเครื่องแม่ข่ายและขีดจำกัดของ bandwidth ไม่เพียงพอ ส่งผลถึงระบบสารสนเทศที่เข้าถึงไม่ได้ (unavailability)



ภาพที่ 1 ลักษณะการโจมตีของ DDOS

เงื่อนไขสำหรับการตอบสนองอย่างมีประสิทธิภาพ

- สศก. มีการจัดเตรียมสารสนเทศที่จำเป็นไว้อย่างครบถ้วนสมบูรณ์ รวมถึงรายการติดต่อเจ้าหน้าที่ภายใน รายการระบบเครื่องแม่ข่าย และแผงผังระบบเครือข่าย
- สศก. มีทรัพยากรและเครื่องมือที่จำเป็นอย่างครบถ้วน

การฟื้นฟูเชิงกลยุทธ์

- เจ้าหน้าที่ประจำศูนย์ฯ ยืนยันการตรวจพบภัยคุกคามไซเบอร์
- เจ้าหน้าที่ติดต่อไปยังคณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สศก. พร้อมข้อมูลเบื้องต้น ได้แก่
    - ลักษณะการโจมตี
    - ตัวบ่งชี้และแหล่งของตัวบ่งชี้ภัยคุกคาม
    - การประเมินระดับผลกระทบของอุบัติการณ์
- คณะทำงานจัดประชุมร่วมกับผู้อำนวยการเพื่อตัดสินใจปิดระบบสารสนเทศที่ได้รับผลกระทบ และแจ้งต่อหน่วยงานที่เกี่ยวข้อง เพื่อพิจารณาการแจ้งไปยังหน่วยงานภายนอกหรือประชาชนผู้มีส่วนได้ส่วนเสียกับการปิดระบบ
- คณะทำงาน วิเคราะห์เชิงลึกถึงข้อมูลบนระบบเครือข่ายเพื่อกำหนดหมายเลข IP, ประเภทบริการ (service), ที่ทำให้เกิดอุบัติการณ์ ซึ่งตรวจพบว่าเป็นในลักษณะ Distributed หมายถึงการโจมตีมาจากหลายเครื่องต้นทาง
- คณะทำงาน วิเคราะห์ความจำเป็นใช้งานของบริการ (service) และรูปแบบการโจมตีที่เป็นสาเหตุโดยจำแนกดังนี้
    - การโจมตีแบบ SYN Flood การโจมตีโดยการส่งแพ็คเกจ TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source IP address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source IP address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมากยังอาจจะทำให้เกิดการใช้ bandwidth เต็ม ทำให้เครือข่ายไม่สามารถให้บริการได้แล้วกระทบต่อระบบสารสนเทศอื่น ๆ และการใช้งานผ่านเครือข่ายทั้งหมด
    - การโจมตีแบบ ICMP Flood การส่งแพ็คเกจ ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งาน bandwidth เต็ม ซึ่งมีผลกระทบไม่ต่างจาก SYN Flood

- การโจมตีแบบ UDP Flood การส่งแพ็คเกจ UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้ bandwidth อย่างเต็มที่ และหรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)
- การโจมตีแบบ Teardrop โดยปกติอุปกรณ์ router จะไม่ยอม ให้แพ็คเกจขนาดใหญ่ผ่านได้ จะต้องทำ Fragment และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทางจะนำแพ็คเกจที่ถูกแบ่งออกเป็น ชิ้นส่วนต่าง ๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็นแพ็คเกจที่สมบูรณ์ การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็คเกจแรกและแพ็คเกจต่อ ๆ ไป
- สำหรับการโจมตีแบบ Teardrop นี้ ผู้โจมตีจะส่งค่า Offset ในแพ็คเกจที่สองและต่อ ๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสน หากระบบปฏิบัติการไม่สามารถรับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานในทันที
- การโจมตีแบบ Land Attack ลักษณะการโจมตีประเภทนี้ เป็นการส่ง SYN ไปที่เครื่องเป้าหมายเพื่อขอการเชื่อมต่อ ซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอ แต่เนื่องจากว่าหมายเลข IP Address ของเครื่องต้นทางกับเครื่องที่เป็นเป้าหมายนี้มีหมายเลข IP Address เดียวกัน โดยการใช้วิธีการสร้างหมายเลข IP Address ลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมีหมายเลข IP Address ที่ต่างกับเครื่องเป้าหมายอยู่แล้ว แต่จะใช้วิธีการทางซอฟต์แวร์ในการส่งแพ็คเกจที่ประกอบด้วยคำขอการเชื่อมต่อ พร้อมด้วยหมายเลข IP Address ปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่าหมายเลข IP Address ที่เข้ามาเป็นเครื่องปัจจุบันหรือไม่ ก็จะทำการตอบสนองด้วย SYN ACK ออกไป หากหมายเลข IP Address ที่ขอเชื่อมต่อเข้ามาเป็นอันเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของหน่วยความจำเพื่อการนี้จำนวนหนึ่ง ซึ่งหากผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรรหน่วยความจำของเครื่องแม่ข่ายได้
- Smurf ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast ในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอมหมายเลข source IP address เป็นหมายเลข IP address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยังหมายเลข IP address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งาน bandwidth อย่างเต็มที่

- คณะทำงาน ดำเนินการแก้ไขปัญหาตามรูปแบบการโจมตีที่ได้วิเคราะห์ อาทิ
    - การแก้ไขการตั้งค่าบนอุปกรณ์เครือข่าย router/firewall ให้ป้องกัน (ACL) ตัดการเชื่อมต่อ หรือจำกัดจำนวนคำร้อง (request)
    - การแก้ไขการตั้งค่าบนเครื่องคอมพิวเตอร์แม่ข่าย
    - การเปลี่ยนหมายเลข IP ของเป้าหมายการโจมตี

การฟื้นฟูด้านยุทธศาสตร์

- การยกระดับความมั่นคงปลอดภัยทางเครือข่ายและตรวจสอบช่องโหว่ที่จะเป็นจุดทำให้เกิดการโจมตีได้
- การใช้งบประมาณในการจัดซื้ออุปกรณ์ป้องกันทางเครือข่ายที่ช่วยในการลดผลกระทบและความเสี่ยงในการเกิดอุบัติการณ์
- การพิจารณาการตอบสนองต่ออุบัติการณ์
- ระดับสัญญาบริการของระบบสารสนเทศที่กระทบจากอุบัติการณ์ และความจำเป็นใช้ของข้อมูลสารสนเทศจากผู้ใช้งานของ สศก.
- การดำเนินคดีต่อผู้กระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560

4.3 สถานการณ์จำลองเหตุภัยคุกคามสำหรับผู้ใช้งานทั่วไป

สศก. พิจารณาเหตุภัยคุกคามทางไซเบอร์ที่มีโอกาสสูงที่เจ้าหน้าที่ของ สศก. จะตกเป็นเหยื่อการโจมตีและกระทบต่อการปฏิบัติหน้าที่ภายใน สศก. หรือกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของ สศก.จำแนกตามกรณีศึกษาได้ดังนี้

- การตกเป็นเหยื่อไวรัสเรียกค่าไถ่ (Ransomware)
- การถูกจารกรรมอุปกรณ์สื่อสารหรือสื่อบันทึกข้อมูลสำคัญของหน่วยงาน (Theft and Loss of Media)

4.3.1 กรณีศึกษาที่ 1: การตกเป็นเหยื่อไวรัสเรียกค่าไถ่

ผู้ใช้งานได้รับ email ฉบับหนึ่งจากกระทรวงเกษตรและสหกรณ์ โดยแสดงหัวเรื่องถึงปัญหาเร่งด่วนที่ต้องได้รับการแก้ไขจาก สศก. จึงได้เร่งรีบเปิดอ่าน email ฉบับนั้นและมีเนื้อความถึงการเปิดดูเอกสารที่แนบมา เมื่อผู้ใช้งานดาวน์โหลดเอกสารที่แนบมาเสร็จจึงเร่งดับเบิลคลิกเปิดไฟล์โดยไม่ทันระวังและสำรวจถึงชนิดและประเภทของไฟล์ ทันทีที่ไฟล์ถูกเปิดระบบปฏิบัติการก็ได้ start เมื่อกลับเข้าสู่หน้าปฏิบัติการผู้ใช้งานพบว่าไฟล์ใน drive D: และไฟล์เอกสารประเภท .doc และ .docx ทั้งหมดไม่สามารถเปิดอ่านได้แต่มีโปรแกรมคอมพิวเตอร์หนึ่งถูกเปิดขึ้นตามภาพด้านล่าง

ภาพที่ 2 ภาพตัวอย่างการติดไวรัสคอมพิวเตอร์เรียกค่าไถ่

ผู้ใช้งานตกอยู่ภาวะสับสนแต่ก็เข้าใจได้ในทันทีว่าได้ตกเป็นเหยื่อของการโจมตีด้วยไวรัสคอมพิวเตอร์ที่กำลังเป็นที่กล่าวถึงในสังคมไทย “ไวรัสเรียกค่าไถ่”

แนวทางการแก้ไขและรับมือต่ออุบัติการณ์

- ตัดการเชื่อมต่อระบบเครือข่ายและงดใช้สื่อบันทึกข้อมูลทุกชนิดที่ต้องเชื่อมต่อกับเครื่องคอมพิวเตอร์
- รีบแจ้งไปยังเจ้าหน้าที่ สศก. ท่านอื่นที่ท่านเชื่อว่าอยู่ในรายการผู้รับของ email ฉบับนั้น
- บันทึกเหตุการณ์ ชื่อ email วันเวลา และรายละเอียดเท่าที่ท่านจดจำได้ในทันที
- แจ้งเจ้าหน้าที่ประจำศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ของ สศก. ในทันที
- กรณีที่ท่านมีภารกิจเร่งด่วนต้องดำเนินการให้รีบปรึกษาเจ้าหน้าที่ เพื่อหาแนวทางแก้ไขและขอรับข้อมูลกู้คืนที่จำเป็นต่อการปฏิบัติหน้าที่
- ไม่พยายามเข้าลบหรือเคลื่อนย้ายเอกสารใด ๆ ในเครื่องคอมพิวเตอร์นั้น (รวมถึง email ฉบับนั้น)

แนวปฏิบัติการป้องกันอุบัติการณ์

- ใช้ความระมัดระวังในการเปิดไฟล์แนบ email หรือเอกสารใดๆ ที่มาจากหน่วยงานภายนอก และวิเคราะห์ถึงชื่อผู้ส่ง ลักษณะการสะกดคำ และไม่คลิกลิงค์ที่อยู่ในเนื้อหา email
- ติดตั้งโปรแกรมตรวจจับไวรัสและอัพเดตปรับปรุงให้เป็นปัจจุบัน กรณีเป็นการปรับปรุงจากส่วนกลาง ให้นำเครื่องเชื่อมต่อเครือข่ายหน่วยงานเพื่อให้เกิดการเรียกปรับปรุงโปรแกรมตรวจจับไวรัส (Anti-Virus) อัตโนมัติ
- สำรองข้อมูลในการปฏิบัติภารกิจที่สำคัญๆ กรณีพบว่าข้อมูลไม่ได้รับการสำรองจากส่วนกลาง ให้ทำเรื่องนำเสนอผู้บังคับบัญชาและพิจารณาส่งเรื่องถึงหน่วยงานที่รับผิดชอบเพื่อการสนับสนุนมาตรการที่จำเป็น หากไม่มีการสนับสนุนจากส่วนกลาง ให้ใช้สื่อบันทึกข้อมูลของ สศก. บันทึกข้อมูลที่สำคัญ และเก็บรักษาตามนโยบายของ สศก. หรือการใช้ cloud storage ที่ สศก. จัดหาไว้ให้
- ศึกษาแนวปฏิบัติเพิ่มเติมจากแหล่งข้อมูล อาทิ https://www.etda.or.th/th/Useful-Resource/documents-for-download.aspx

4.3.2 กรณีศึกษาที่ 2: การถูกจารกรรมอุปกรณ์สื่อสารหรือสื่อบันทึกข้อมูลสำคัญของหน่วยงาน

กรณีที่หน่วยงานอนุญาตให้เจ้าหน้าที่ใช้อุปกรณ์สื่อสารส่วนบุคคลในการเข้าถึงข้อมูลของ สศก. อาทิ email, cloud ทำให้อุปกรณ์สื่อสารดังกล่าวมีข้อมูลสำคัญของ สศก. จัดเก็บหรือสามารถเชื่อมต่อระบบสารสนเทศของหน่วยงานได้ (ผู้ใช้งานส่วนใหญ่อนุญาตให้ browser จดจำรหัสผ่านและบัญชีผู้ใช้งานไว้) เมื่อเกิดการสูญหาย จึงอาจกระทบต่อความมั่นคงปลอดภัยสารสนเทศของ สศก. ได้

แนวทางการแก้ไขและรับมือต่ออุบัติการณ์

- ใช้โปรแกรมช่วยค้นหา อาทิ FIND MY DEVICE/FIND MY I-PHONE (เผื่อไม่ได้สูญหายเพียงแต่ลืม)
- รีบจดบันทึกเวลาและสถานที่ที่คาดว่าอุปกรณ์สื่อสารหรือสื่อบันทึกสูญหาย เมื่อเป็นไปได้ให้ดำเนินการแจ้งความเพื่อลงบันทึกในสถานีตำรวจใกล้เคียง
- จดบันทึกระบบสารสนเทศที่สามารถเชื่อมต่อผ่านอุปกรณ์สื่อสารดังกล่าว และรายการสารสนเทศสำคัญที่ถูกบันทึกไว้
- ดำเนินการเปลี่ยนรหัสผ่านและอุปกรณ์สื่อสารที่ใช้เชื่อมต่อระบบรหัสผ่านใช้ครั้งเดียว ของระบบสารสนเทศที่สำคัญ
- แจ้งเจ้าหน้าที่ประจำศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ของ สศก. เพื่อระงับบัญชีผู้ใช้งานชั่วคราว เมื่อเป็นไปได้ให้ดำเนินการตัด session การใช้งานระบบสารสนเทศทั้งหมดที่ค้างไว้
- กรณีคาดว่ามีข้อมูลส่วนบุคคลภายนอกอาจได้รับผลกระทบ ให้ดำเนินการแจ้งเจ้าหน้าคุ้มครองข้อมูลส่วนบุคคล สศก. เพื่อพิจารณาและดำเนินการต่อไป

แนวทางการป้องกันอุบัติการณ์

- ใช้ความระมัดระวังในการใช้อุปกรณ์ส่วนบุคคลและสื่อบันทึกข้อมูล ไม่ทำหล่นหาย
- จดจำลักษณะการใช้งานของตนเอง รายการระบบสารสนเทศ และข้อมูลสำคัญของ สศก. ที่ท่านได้ทำการบันทึกไว้
- หมั่นเปลี่ยนรหัสผ่านการเข้าใช้ระบบสารสนเทศสำคัญและ email ของ สศก.
- ศึกษาแนวปฏิบัติเพิ่มเติมจากแหล่งข้อมูล อาทิ https://www.etda.or.th/th/Useful-Resource/documents-for-download.aspx

บทที่ 5
แผนงานการวัดประสิทธิภาพ (Performance Matrix)

ศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ สศก. จะให้มีแผนงานการวัดประสิทธิภาพ โดยมีองค์ประกอบดังต่อไปนี้

- แผนงานการวัดประสิทธิภาพ (Performance Matrix) ของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย
    - ตัวชี้วัดประสิทธิภาพ (Key Performance Indicator) ด้านความมั่นคงปลอดภัยไซเบอร์
    - วัตถุประสงค์ (Objectives)
    - การคำนวณประสิทธิภาพ (Formula)
    - ค่าเป้าหมาย (Target)
    - รอบความถี่ของการวัดประเมิน (Frequency)
    - ผู้รับผิดชอบต่อการวัดประเมินและรายงานผล (Responsible Person)
- แผนการจัดทำรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์

5.1 แผนงานการวัดประสิทธิภาพ (Performance Matrix) ของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

สศก. จัดให้มีการวัดประสิทธิภาพของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีตัวชี้วัดดังนี้

ตัวชี้วัดที่เป็นรายปี จำนวน 2 รายการ

- ตัวชี้วัดที่ 1: การวัดประสิทธิภาพของการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ของ สศก.
- ตัวชี้วัดที่ 2: ความสอดคล้องต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ตัวชี้วัดที่เป็นรายไตรมาส จำนวน 2 รายการ

- ตัวชี้วัดที่ 3: ประสิทธิภาพการจัดการช่องโหว่ในระดับความเสี่ยงสูง
- ตัวชี้วัดที่ 4: ความพึงพอใจของผู้ใช้บริการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ สศก.

ตัวชี้วัดที่เป็นรายเดือน จำนวน 3 รายการ

- ตัวชี้วัดที่ 5: รายการอุบัติการณ์ด้านความมั่นปลอดภัยไซเบอร์
- ตัวชี้วัดที่ 6: ประสิทธิภาพมาตรการป้องกันไวรัสคอมพิวเตอร์
- ตัวชี้วัดที่ 7: ประสิทธิภาพมาตรการการรายงานผลการปฏิบัติงานของศูนย์ฯ

5.1.1 รายการตัวชี้วัดประสิทธิภาพของศูนย์ฯ (รายปี)

การวัดประสิทธิภาพ	รายละเอียด
ตัวชี้วัดที่ 1: การวัดประสิทธิภาพของการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ของ สศก.	
วัตถุประสงค์	• เพื่อบ่งชี้สัดส่วนการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ของ สศก. ที่สะท้อนถึงการให้ความสำคัญของหน่วยงานในการพัฒนาปรับปรุงอย่างต่อเนื่อง
ตัวชี้วัด	ร้อยละ ของงบประมาณด้านความมั่นคงปลอดภัยไซเบอร์เมื่อเทียบกับงบประมาณด้านเทคโนโลยีสารสนเทศทั้งหมด
การคำนวณ	$\left(\frac{\text{งบประมาณด้านความมั่นคงปลอดภัยไซเบอร์}}{\text{งบประมาณด้านเทคโนโลยีสารสนเทศและดิจิทัล}}\right) \times 100$
ค่าเป้าหมาย	ร้อยละ 10-20
รอบความถี่	รายปี
ผู้รับผิดชอบ	
ตัวชี้วัดที่ 2: ความสอดคล้องต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	
วัตถุประสงค์	• เพื่อให้มั่นใจว่า สศก. ได้ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ครบถ้วนทุกมาตรา
ตัวชี้วัด	ร้อยละ ของความสอดคล้องโดยดำเนินกิจกรรมได้แก่ • ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยมีรายงานและได้รับการอนุมัติ อย่างน้อย 1 ครั้งต่อปี • ดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยมีรายงานและได้รับการอนุมัติ อย่างน้อย 1 ครั้งต่อปี • ดำเนินการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรของ สศก. โดยมีรายงานเข้าร่วม อย่างร้อย 1 ครั้งต่อปี
การคำนวณ	$\left(\frac{\text{จำนวนกิจกรรมที่ได้ดำเนินการเรียบร้อย}}{\text{จำนวนกิจกรรมที่ต้องดำเนินการทั้งหมด}}\right) \times 100$
ค่าเป้าหมาย	ร้อยละ 100
รอบความถี่	รายปี
ผู้รับผิดชอบ	

5.1.2 รายการตัวชี้วัดประสิทธิภาพของศูนย์ฯ (รายไตรมาส)

การวัดประสิทธิภาพ	รายละเอียด
ตัวชี้วัดที่ 3: ประสิทธิภาพการจัดการช่องโหว่ในระดับความเสี่ยงสูง	
วัตถุประสงค์	• เพื่อบ่งชี้ประสิทธิภาพของกระบวนการการจัดการช่องโหว่ที่ตรวจพบของ สศก. • เพื่อบ่งชี้ความเสี่ยงคงเหลือที่เกิดจากการจัดการช่องโหว่ที่ยังไม่ได้ดำเนินการแล้วเสร็จของ สศก.
ตัวชี้วัด	ร้อยละ ของจำนวนช่องโหว่ความเสี่ยงสูงที่ได้รับการแก้ไขในระยะเวลาที่กำหนด เมื่อเทียบกับจำนวนช่องโหว่ความเสี่ยงสูงทั้งหมดของ สศก. ที่ตรวจพบ
การคำนวณ	$\left(\frac{\text{จำนวนช่องโหว่ความเสี่ยงสูงที่ได้รับการแก้ไขในระยะเวลาที่กำหนด}}{\text{จำนวนช่องโหว่ความเสี่ยงสูงทั้งหมด}}\right) \times 100$
ค่าเป้าหมาย	ร้อยละ 90 ขึ้นไป
รอบความถี่	รายไตรมาส
ผู้รับผิดชอบ	
ตัวชี้วัดที่ 4: ความพึงพอใจของผู้ใช้บริการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ สศก.	
วัตถุประสงค์	• เพื่อแสดงศักยภาพของเจ้าหน้าที่ประจำศูนย์ฯ ในการปฏิบัติหน้าที่และให้บริการแก่เจ้าหน้าที่ของ สศก. ในการรับเรื่องและแก้ไขปัญหาอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
ตัวชี้วัด	ค่าเฉลี่ยความพึงพอใจในภาพรวม
การคำนวณ	$\frac{\sum_{i=1}^{n} \text{คะแนนความพึงพอใจในภาพรวมของบริการ}}{n}$ เมื่อ n คือจำนวนผู้ทำแบบสอบถามความพึงพอใจ
ค่าเป้าหมาย	มากกว่า ค่าที่ 80% ของเกณฑ์วัด (ตัวอย่างถ้าวัดประเมินที่ 1-5 ต้องได้มากกว่า 4 ถ้าวัดประเมินที่ 1-10 ต้องได้มากกว่า 8)
รอบความถี่	รายไตรมาส
ผู้รับผิดชอบ	

5.1.3 รายการตัวชี้วัดประสิทธิภาพของศูนย์ฯ (รายเดือน)

การวัดประสิทธิภาพ	รายละเอียด
ตัวชี้วัดที่ 5: รายการอุบัติการณ์ด้านความมั่นปลอดภัยไซเบอร์	
วัตถุประสงค์	• เพื่อตรวจสอบความสามารถในการจัดการอุบัติการณ์ที่เกิดขึ้น
ตัวชี้วัด	ร้อยละ ของอุบัติการณ์ที่ได้รับการแก้ไขแล้วเสร็จเทียบกับจำนวนอุบัติการณ์ทั้งหมด
การคำนวณ	$\left(\frac{\text{จำนวนอุบัติการณ์ที่ได้รับการแก้ไขแล้วเสร็จ}}{\text{จำนวนอุบัติการณ์ทั้งหมด}}\right) \times 100$
ค่าเป้าหมาย	ร้อยละ 100
รอบความถี่	รายเดือน
ผู้รับผิดชอบ	
ตัวชี้วัดที่ 6: ประสิทธิภาพมาตรการป้องกันไวรัสคอมพิวเตอร์	
วัตถุประสงค์	• เพื่อบ่งชี้ประสิทธิภาพของมาตรการด้านการป้องกันคอมพิวเตอร์ไวรัส • เพื่อบ่งชี้การปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์จากส่วนกลางให้เป็นปัจจุบัน
ตัวชี้วัด	จำนวน เครื่องคอมพิวเตอร์ที่ได้รับรายงานการติดไวรัสคอมพิวเตอร์ทุกชนิดหรือเครื่องคอมพิวเตอร์ที่ได้รับรายงานถึงการติดตั้ง patch หรือโปรแกรมป้องกันคอมพิวเตอร์ไวรัสไม่ครบถ้วนเป็นปัจจุบัน
การคำนวณ	จำนวน เครื่องที่ได้รับรายงาน
ค่าเป้าหมาย	กรณีเป็นข้อยกเว้นทางเทคนิคที่ไม่สามารถดำเนินการได้ ให้นำรายการเครื่องคอมพิวเตอร์ประเมินความเสี่ยงและให้คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พิจารณาอนุมัติถ้าพ้นวิสัยของอำนาจการตัดสินใจให้ส่งเรื่องเข้าคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สศก.
รอบความถี่	รายเดือน
ผู้รับผิดชอบ	
ตัวชี้วัดที่ 7: ประสิทธิภาพมาตรการการรายงานผลการปฏิบัติงานของศูนย์ฯ	
วัตถุประสงค์	เพื่อให้มั่นใจว่ากลไกในการรายงานผลการปฏิบัติการของศูนย์ฯ ได้รับการปฏิบัติตามและสอดคล้องต่อนโยบายและกรอบแนวทางที่กำหนด
ตัวชี้วัด	ร้อยละ ของรายงานที่ศูนย์ฯ จัดทำและจัดส่งแก่คณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์ เทียบกับรายงานที่ต้องดำเนินการทั้งหมดตามนโยบายและกรอบแนวทางที่กำหนด ได้แก่ • รายงานภัยคุกคามและการโจมตีทางไซเบอร์ (รายวัน) ตามจำนวนวันในเดือนนั้น ๆ

	• รายงานภัยคุกคามและการโจมตีทางไซเบอร์ (รายสัปดาห์) ตามจำนวนสัปดาห์ในเดือนนั้น ๆ • รายงานภัยคุกคามและการโจมตีทางไซเบอร์ (รายเดือน) รายงานการวัดประเมินประสิทธิภาพศูนย์ฯ ประกอบด้วยรายการตัวชี้วัดที่ครบกำหนดรอบการรายงาน
การคำนวณ	$\left(\frac{\text{รายงานที่ศูนย์ฯ จัดทำและจัดส่งแก่คณะทำงาน}}{\text{รายงานที่ต้องดำเนินการทั้งหมดตามนโยบายและกรอบแนวทาง}}\right) \times 100$
ค่าเป้าหมาย	ร้อยละ 100
รอบความถี่	รายเดือน
ผู้รับผิดชอบ	

5.2 แผนการจัดทำรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์

ศูนย์ฯ ได้จัดให้มีแผนการจัดทำรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์โดยมีรายละเอียดดังนี้

- ระเบียบการสื่อสารและอนุมัติรายงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของ สศก.
- แผนการรายงานผลประจำปี

5.2.1 ระเบียบการสื่อสารและอนุมัติรายงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของ สศก.

การสื่อสารและอนุมัติรายงานแต่ละรายการมีความแตกต่างขึ้นอยู่กับวัตถุประสงค์ของรายงาน โดยสรุปเป็นกลุ่มรายงานได้ดังนี้

กลุ่มที่ 1: กลุ่มรายงานจากระบบสารสนเทศหรือเครื่องมือที่ใช้เพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์	
ตัวอย่างรายงาน	• รายงานจากโปรแกรมป้องกันไวรัสคอมพิวเตอร์ส่วนกลาง (Centralized Anti-Virus System) • รายงานจากตรวจพบเหตุผิดปกติบนระบบเครือข่ายจากอุปกรณ์ Firewall • เอกสารประกอบมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ เช่น รายการ port, แผนผังเครือข่าย แผนผังเครื่องแม่ข่าย เป็นต้น
ผู้จัดทำ	เจ้าหน้าที่ประจำศูนย์ฯ
ผู้ตรวจทาน	
ผู้อนุมัติ	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กลุ่มที่ 2: กลุ่มรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์	
ตัวอย่างรายงาน	• รายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (รายวัน) • รายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (รายสัปดาห์) • รายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์ (รายเดือน)
ผู้จัดทำ	เจ้าหน้าที่ประจำศูนย์ฯ
ผู้ตรวจทาน	
ผู้อนุมัติ	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
กลุ่มที่ 3: กลุ่มรายงานความสอดคล้องต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์	
ตัวอย่างรายงาน	• รายงานการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ • รายงานการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ • รายงานการอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรของ สศก.
ผู้จัดทำ	เจ้าหน้าที่ประจำศูนย์ฯ
ผู้ตรวจทาน	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
ผู้อนุมัติ	คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มที่ 4: กลุ่มรายงานประสิทธิภาพของศูนย์	
ตัวอย่างรายงาน	• รายงานผลการวัดประสิทธิภาพของศูนย์ (รายเดือน) • รายงานผลการวัดประสิทธิภาพของศูนย์ (รายไตรมาส) • รายงานผลการวัดประสิทธิภาพของศูนย์ (รายปี)
ผู้จัดทำ	เจ้าหน้าที่ประจำศูนย์ฯ
ผู้ตรวจทาน	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
ผู้อนุมัติ	• คณะทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (เฉพาะรายเดือน) • คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร (เฉพาะรายไตรมาสและรายปี)

5.2.2 แผนการรายงานผลประจำปี

แผนการรายงานผลประจำปี 2565 ปรากฏตามตารางดังนี้

รายงาน	เดือน											
	1	2	3	4	5	6	7	8	9	10	11	12
กลุ่มรายงานจากระบบสารสนเทศหรือเครื่องมือที่ใช้เพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์	■	■	■	■	■	■	■	■	■	■	■	■
กลุ่มรายงานผลการปฏิบัติงานเฝ้าระวังและรับมือเหตุการณ์ภัยคุกคามและการโจมตีทางไซเบอร์	■	■	■	■	■	■	■	■	■	■	■	■
กลุ่มรายงานความสอดคล้องต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562												
● รายงานการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	■	■	■									
● รายงานการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	■	■	■									
● รายงานการอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรของ สศก.	■	■	■									
กลุ่มรายงานประสิทธิภาพของศูนย์												
● รายงานผลการวัดประสิทธิภาพของศูนย์ (รายเดือน)	■	■	■	■	■	■	■	■	■	■	■	■
● รายงานผลการวัดประสิทธิภาพของศูนย์ (รายไตรมาส)			■			■			■			■
● รายงานผลการวัดประสิทธิภาพของศูนย์ (รายปี)												■

ภาคผนวก

ภาคผนวก ก: แม่แบบทะเบียนทรัพย์สิน

ไฟล์เอกสาร:

แม่แบบในการเก็บ
ข้อมูลและจัดทำทะเบีย

แม่แบบในการเก็บข้อมูลและจัดทำทะเบียนทรัพย์สินด้านสารสนเทศเพื่อใช้เป็นข้อมูลในการรับมือกับภัยคุกคามในด้านต่างๆ ซึ่งเป็นความเสี่ยงด้านไซเบอร์ที่มีผลกระทบสูงต่อ สศก.																ผลกระทบด้านการปฏิบัติงาน			ผลกระทบด้านสารสนเทศ			ผลกระทบด้านกฎหมาย			ผลกระทบด้านความสามารถในการกู้คืน			ความสำคัญของทรัพย์สิน	
ลำดับที่	บริการ	หน่วยงานผู้ดูแล	ชื่อระบบ/กระบวนการ	ปี	การรับประกัน	ชนิด	ยี่ห้อ	รุ่น	โมเดล	ผู้ขาย	หน่วยทรัพย์สิน	การทำงานของอุปกรณ์/ทรัพย์สิน	จำนวน	สถานะ	ที่ตั้ง	เจ้าของ (ผู้ถือครอง)	C.Value	I.Value	A.Value	C.Value	I.Value	A.Value	C.Value	I.Value	A.Value	C.Value	I.Value	A.Value	Total Value	Asset Value Level
																													0	
																													0	
																													0	
																													0	
																													0	
																													0	

ภาคผนวก ข. แบบฟอร์มรับรายงานอุบัติการณ์

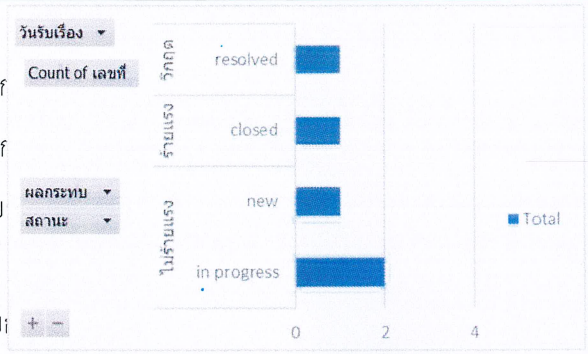
แบบรายงานอุบัติการณ์ เลขที่:_____			
ผู้รายงาน:			
ตำแหน่ง:		แผนก / ที่ตั้ง:	
Email:		หมายเลขโทรศัพท์:	
รายละเอียดอุบัติการณ์: ลงนามผู้รายงาน _____ วันและเวลาแล้วเสร็จ_____			
สถานะ: รับเรื่อง /กำลังดำเนินการ /แก้ไข /ปิดคำร้อง /ไม่ใช่อุบัติการณ์			
เจ้าหน้าที่ประจำศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์	บันทึกโดย ลงนาม:_____ เวลา:_____	หมายเหตุ (รับเรื่อง)	
รายละเอียดปัญหา (วิเคราะห์) ลักษณะการโจมตี: ตัวบ่งชี้อุบัติการณ์: แหล่งตัวบ่งชี้อุบัติการณ์: การรุกรามของอุบัติการณ์: รุกราม / ไม่รุกราม ผลกระทบ: ไม่ร้ายแรง / ร้ายแรง / วิกฤต (กรณี ร้ายแรงหรือวิกฤต ให้เร่งติดต่อ กกม.) วิธีการรับมือและตอบสนองต่ออุบัติการณ์ ลงนามผู้ดำเนินการ (ตัวแทน) _____ วันและเวลาแล้วเสร็จ_____			
บทเรียน (ถ้ามี) ขั้นตอนการป้องกันในอนาคต (ถ้ามี) ลงนามผู้บันทึก (ตัวแทน) _____ วันและเวลาแล้วเสร็จ_____			

ภาคผนวก ค. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำวัน

แบบสรุปรายงานอุบัติการณ์ประจำวัน **เลขที่:**_____			
ผู้รายงาน:			
ตำแหน่ง:		**รายงานประจำวันที่**	(วัน-เดือน-ปี)

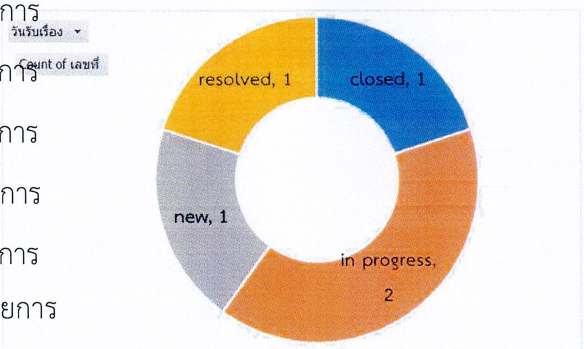
จำนวนอุบัติการณ์ทั้งหมด: ..... รายการ

- ผลกระทบระดับไม่ร้ายแรง จำนวน ..... รายก
- ผลกระทบระดับร้ายแรง จำนวน ..... รายก
- ผลกระทบระดับวิกฤต จำนวน ..... ราย



จำแนกตามสถานะล่าสุด

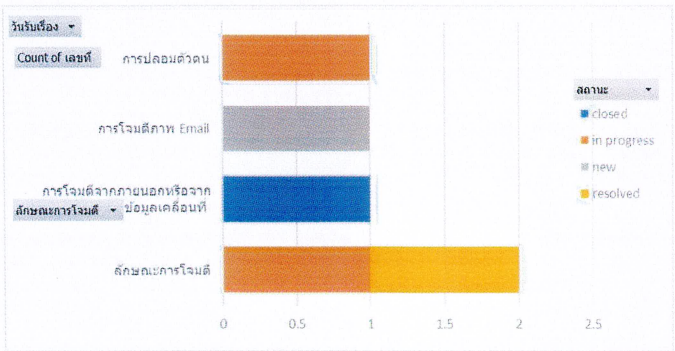
- new จำนวน ..... รายก
- forwarded จำนวน ..... รายการ
- resolved จำนวน ..... รายการ
- in progress จำนวน ..... รายการ
- closed จำนวน ..... รายการ
- reopen จำนวน ..... รายการ



อุบัติการณ์คงค้างรวมทั้งสิ้น จำนวน ..... รายการ

*กรุณาแนบแบบบันทึกรายงานอุบัติการณ์มาพร้อมรายงานฉบับนี้ด้วย

ลักษณะการโจมตีที่พบ



บทเรียน (ถ้ามี)

ภาคผนวก ง. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำสัปดาห์

แบบสรุปรายงานอุบัติการณ์ประจำสัปดาห์ **เลขที่:**_____			
ผู้รายงาน:			
ตำแหน่ง:		**รายงานประจำวันที่**	(วัน-เดือน-ปี) - (วัน-เดือน-ปี)

จำนวนอุบัติการณ์ทั้งหมด: ..... รายการ

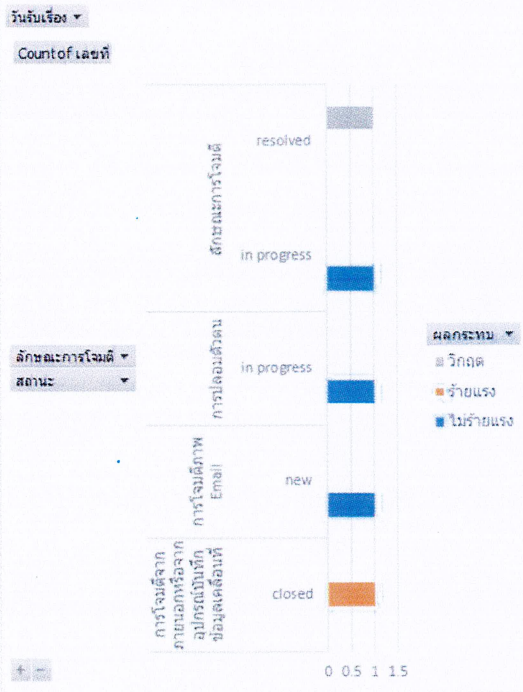
- ผลกระทบระดับไม่ร้ายแรง จำนวน ..... รายการ
- ผลกระทบระดับร้ายแรง จำนวน ..... รายการ
- ผลกระทบระดับวิกฤต จำนวน ..... รายการ

จำแนกตามสถานะล่าสุด

- new จำนวน ..... รายการ
- forwarded จำนวน ..... รายการ
- resolved จำนวน ..... รายการ
- in progress จำนวน ..... รายการ
- closed จำนวน ..... รายการ
- reopen จำนวน ..... รายการ

อุบัติการณ์คงค้างรวมทั้งสิ้น จำนวน ..... รายการ

*กรุณาแนบสรุปรายงานอุบัติการณ์ประจำวันมาพร้อมรายงานฉบับนี้ด้วย



สรุปกิจกรรมที่เกี่ยวข้องที่ต้องดำเนินการ	
1. ติดตั้ง Firewall และปรับค่า Configuration ของอุปกรณ์ตัวเดิม โดยบริษัท AAA Co. Ltd. ในวันที่ 13 สิงหาคม 2564 2. จัดอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ ในวันที่ 14 สิงหาคม 2564 โดยวิทยากรภายนอก 3. นำส่งเอกสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้ ETDA	**ข้อเสนอแนะ** **ลงนามผู้ตรวจทานรายงาน** _____

ภาคผนวก จ. แม่แบบรายงานภัยคุกคามและการโจมตีทางไซเบอร์ ประจำเดือน

แบบสรุปรายงานอุบัติการณ์ประจำเดือน

เลขที่:_____

ผู้รายงาน:			
ตำแหน่ง:		**รายงานประจำเดือน**	(เดือน-ปี)

จำนวนอุบัติการณ์ทั้งหมด: ..... รายการ

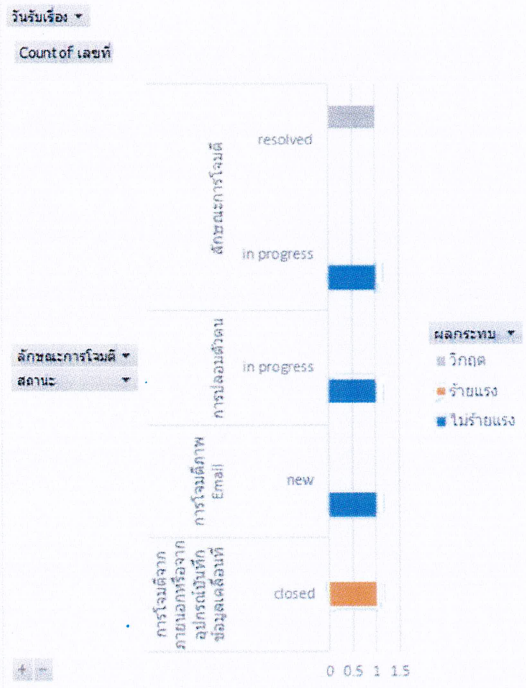
- ผลกระทบระดับไม่ร้ายแรง จำนวน ..... รายการ
- ผลกระทบระดับร้ายแรง จำนวน ..... รายการ
- ผลกระทบระดับวิกฤต จำนวน ..... รายการ

จำแนกตามสถานะล่าสุด

- new จำนวน ..... รายการ
- forwarded จำนวน ..... รายการ
- resolved จำนวน ..... รายการ
- in progress จำนวน ..... รายการ
- closed จำนวน ..... รายการ
- reopen จำนวน ..... รายการ

อุบัติการณ์คงค้างรวมทั้งสิ้น จำนวน ..... รายการ

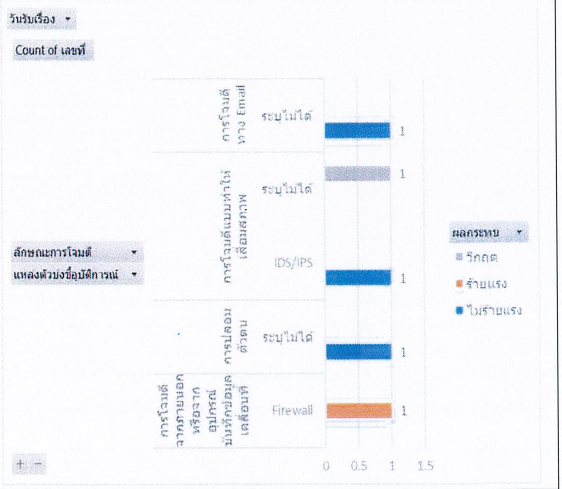
*กรุณาแนบแบบสรุปรายงานอุบัติการณ์ประจำสัปดาห์มาพร้อมรายงานฉบับนี้ด้วย

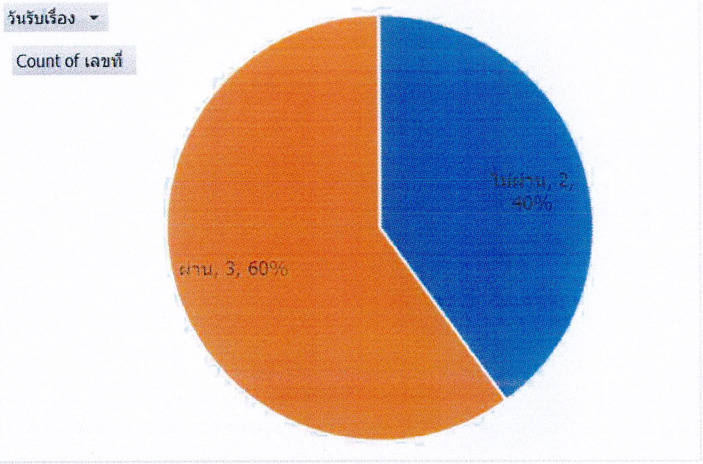


การวิเคราะห์อุบัติการณ์ตามแหล่งตัวบ่งชี้อุบัติการณ์และลักษณะการโจมตี

พบว่าคณะทำงานสามารถบ่งชี้แหล่งตัวบ่งชี้อุบัติการณ์ได้จำนวน 2/5 รายการ (40%) โดยที่อุบัติการณ์เกิดจาก

- การตรวจพบของอุปกรณ์ IDS/IPS จำนวน 1 รายการ (ระดับไม่ร้ายแรง)
- การตรวจพบของอุปกรณ์ Firewall จำนวน 1 รายการ (ระดับร้ายแรง)





การวิเคราะห์ตามสัญญาระดับบริการ

พบว่าระดับสัญญาบริการผ่านที่ร้อยละ 60 ของจำนวนอุบัติการณ์ (รวม 5 รายการ) หมายเลขอุบัติการณ์ที่ตกได้แก่

- อุบัติการณ์หมายเลข 1
- อุบัติการณ์หมายเลข 2

สาเหตุของการไม่ผ่านสัญญาระดับบริการ

เนื่องจากความคลาดแคลนเจ้าหน้าที่ในการแก้ไขปัญหา ทำให้ศูนย์ฯ ไม่สามารถตอบสนองต่ออุบัติการณ์ได้ภายในกรอบระยะเวลา และการคาดเครื่องมืออำนวยความสะดวกทำให้เจ้าหน้าที่ใช้เวลานานในการวิเคราะห์รูปแบบการโจมตีเพื่อการดำเนินการแก้ไข

ความต้องการทรัพยากรเพิ่มเติม

1 บุคลากร เจ้าหน้าที่ประจำศูนย์ฯ นักการคอมพิวเตอร์ ที่มีทักษะในการรับมือภัยคุกคามทางไซเบอร์ 3 อัตรา (ด่วน)

2 เครื่องมือในการวิเคราะห์การโจมตีทางเครือข่ายและการวิเคราะห์แพ็คเกจ

3 การอบรมหลักสูตร CISSP ให้แก่เจ้าหน้าที่ประจำศูนย์ฯ

รายการกิจกรรมที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของ สศก.

1. ปรับปรุงฐานข้อมูลเกษตรกร Farmer One (CHG00001)
2. ติดตั้ง NAS Storage (CHG00002)

ข้อเสนอแนะ

ลงนามผู้ตรวจทานรายงาน

_____