ระดับ 1 : Assessment

ตัวชี้วัด 4.20 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ระดับ 1 : Assessment ศึกษาและการวิเคราะห์สถานการณ์ของการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด

ด้วยกรมอนามัยมีภารกิจหลักในการส่งเสริมให้ประชาชนมีสุขภาพดี มีการศึกษาวิเคราะห์ วิจัย พัฒนาและถ่ายทอดองค์ความรู้และเทคโนโลยีด้านการสร้างเสริมสุขภาพและและอนามัยสิ่งแวดล้อม เพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ภารกิจหรือบริการด้านสาธารณสุขซึ่งเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ จะต้องมีการป้องกัน มีมาตรการรับมือและบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงปลอดภัยทางด้านสาธารณสุขของประเทศ ซึ่งกรมอนามัย ได้ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้มีการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ โดยมีการสรุปผลการวิเคราะห์สถานการณ์ของตัวชี้วัด และความรู้ที่นำมาใช้ประกอบการวิเคราะห์ ดังนี้

1.1.1 ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน

การทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่ละขั้นตอนจะช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ ดังนี้

- การบริหารจัดการความเสี่ยง (Identity)
- การวางมาตรฐานควบคุมเพื่อปกป้องระบบองค์กร (Protect)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Response)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้องค์กรสามารถดำเนินได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery)

ดังนั้น เพื่อแก้ไขปัญหาความเสี่ยงและยกระดับขีดความสามารถขององค์กร โครงการนี้จึงถูกนำมาใช้เป็นกลไกหลักในการแก้ปัญหา โดยมุ่งเน้นการดำเนินงาน 2 มิติสำคัญ ได้แก่:

1) มิติความมั่นคงปลอดภัย (Cyber Security & Governance) กำหนดมาตรฐานกลางยกระดับโครงสร้างพื้นฐานด้าน IT และสร้างระบบเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อลดความเสี่ยงเชิงประจักษ์

2) มิติการพัฒนาบุคลากร (Digital and Data Capability) พัฒนาทักษะบุคลากรให้เป็นนักวิทยาการข้อมูลภาครัฐและมีความตระหนักด้านความปลอดภัย เพื่อให้สามารถใช้ประโยชน์จากข้อมูลขนาดใหญ่ในการตัดสินใจและวางแผนยุทธศาสตร์ได้อย่างมีประสิทธิภาพ

ผลการดำเนินการในปัจจุบันมีการดำเนินงานในปีงบประมาณ พ.ศ. 2568 ดังนี้

การดำเนินงานด้านปีรักษาความมั่นคงปลอดภัยไซเบอร์งบประมาณ พ.ศ. 2568 ได้ก่อให้เกิดผลสัมฤทธิ์ที่สำคัญ ในการยกระดับองค์กรอย่างชัดเจน ทั้งในมิติของการสร้างความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) และการสร้างความพร้อมด้านข้อมูล (Data Readiness) เพื่อรองรับการเป็นองค์กรที่มีความสามารถในการตัดสินใจบนพื้นฐานของข้อมูลจริง ดังนี้:

1) ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กรมอนามัยได้กำหนดให้ใช้มาตรฐานกลางด้านความมั่นคงปลอดภัย (Cyber Security Standard) โดยอ้างอิงตามเกณฑ์การประเมิน CTAM (Cybersecurity Technical Assessment Matrix) และ มาตรฐานโรงพยาบาลอัจฉริยะ (Smart Hospital) ของกระทรวงสาธารณสุข ซึ่งประกอบด้วย 9 ด้านหลัก ได้แก่ 1) ห้อง Data Center ที่ได้มาตรฐาน 2) การควบคุมการเข้าถึงและสิทธิ์ 3) ระบบ Compute and Storage 4) ระบบสำรองข้อมูล 5) ระบบเครือข่ายภายในองค์กร 6) การวางแผนและรับมือเหตุการณ์ 7) ระบบเครือข่ายอินเทอร์เน็ต 8) Computer and Computer-like device 9) Software/Application

1.1) ยกระดับมาตรฐานห้อง Server ดำเนินการประเมินตนเองตามมาตรฐาน 9 ด้าน ใน 17 หน่วยงานที่มีห้อง Server ผลการประเมินพบว่า มี 1 หน่วยงาน (กองแผนงาน) ที่ผ่านเกณฑ์ โดยได้คะแนนสูงถึง 193 จาก 200 คะแนน (96.50%) แสดงให้เห็นถึงมาตรฐานห้อง Server ที่ยกระดับขึ้นเพื่อเป็นต้นแบบ

1.2) ระบบเฝ้าระวังและลดภัยคุกคาม ใช้เครื่องมือ VA Scan (Vulnerability Assessment Scan) ด้วยโปรแกรม Nessus ในการเฝ้าระวังเชิงรุก ส่งผลให้สามารถตรวจพบและดำเนินการแก้ไขช่องโหว่ในระบบสารสนเทศได้อย่างทันท่วงที โดยเฉพาะ ช่องโหว่ในระดับวิกฤต (Critical) จำนวน 5 รายการ และช่องโหว่ระดับสูง (High) จำนวน 106 รายการ ซึ่งได้ดำเนินการแก้ไขทั้งหมดแล้ว ทำให้ความเสี่ยงถูกควบคุมและลดลงอย่างชัดเจน และเป็นการเตรียมความพร้อมเพื่อบรรลุเป้าหมายการลดจำนวนการละเมิดความปลอดภัยทางไซเบอร์ลง 50% (จาก 32 ครั้ง/ปี เหลือไม่เกิน 16 ครั้ง/ปี)

2) ด้านการพัฒนาศักยภาพบุคลากร (Data & Digital Skill Outcome) โครงการได้พัฒนาทักษะด้านเทคโนโลยีดิจิทัลแก่บุคลากรในทุกระดับ

2.1) ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) ดำเนินการฝึกอบรมตามแผนตั้งแต่ปี 2566 รวมแล้วมีบุคลากรได้รับการพัฒนาทักษะด้านนี้ 150 คน (50 คน/ปี ในปี 2566, 2567, 2568)

2.2) การบริหารจัดการความมั่นคงปลอดภัย (Cyber Governance) และ PDPA จัดอบรมเชิงปฏิบัติการให้แก่บุคลากรส่วนกลางและส่วนภูมิภาค จำนวน 50 คน ในปี 2568 โดยครอบคลุมหัวข้อการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ การตอบสนองต่อภัยคุกคาม (Incident Response) และการดำเนินงานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) บุคลากรมีความรู้เพิ่มขึ้น และสามารถนำความรู้ไปใช้ในการปฏิบัติงานได้

1.2 ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อนตัวชี้วัด

ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อน ได้แก่ กลุ่มผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย โดยมีการสรุปผล ดังนี้

1.2.1 กลุ่มผู้รับบริการ

รายการข้อมูล	รายละเอียด
กลุ่มผู้รับริการ	1. เจ้าหน้าที่สังกัดกรมอนามัย 2. ประชาชน
ความต้องการ	ระบบงานที่มีความมั่นคงปลอดภัย สามารถป้องกันการเข้าถึงข้อมูลได้
ความคาดหวัง	การรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีระดับที่สูงขึ้นและการตอบสนองที่รวดเร็วต่อการละเมิดภัยคุกคามทางไซเบอร์
ความผูกพัน	การปฏิบัติตามกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้รับบริการมีความตระหนักถึงความเสี่ยงทางด้านความมั่นคงปลอดภัยทางไซเบอร์
ความไม่พึงพอใจ	1. การไม่เข้าใจในกระบวนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. การใช้ภาษาด้านเทคนิคเข้าใจยาก
ข้อเสนอแนะจากผู้รับบริการ	1. ความปลอดภัยของข้อมูลส่วนตัวที่ภาครัฐเก็บไว้ต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

1.2.2 กลุ่มผู้มีส่วนได้ส่วนเสีย

รายการข้อมูล	รายละเอียด
กลุ่มผู้มีส่วนได้ส่วนเสียปัจจุบัน	1. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย (CIO) 2. เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย (Anamai-CIRT) 3. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้านสาธารณสุข (Health-CIRT) 4. สำนักคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
ความต้องการ	การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องตามกฎหมาย มาตรฐาน และนโยบายที่เกี่ยวข้อง

ความคาดหวัง	การป้องกันการเข้าถึงข้อมูลที่เป็นความลับ สามารถเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
ความผูกพัน	การกำหนดนโยบายและมาตรการที่เข้มงวด เพื่อสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้มีส่วนได้ส่วนเสียรับทราบและตระหนักถึงความเสี่ยงอย่างรวดเร็ว
ความไม่พึงพอใจ	การปรับปรุงระบบงานอาจต้องใช้งบประมาณจำนวนมากในการแก้ไขและปิดช่องโหว่ต่าง ๆ
ข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย	1. การพัฒนาระบบงานให้เน้นที่ความมั่นคงปลอดภัยและประสิทธิภาพ 2. การพัฒนาทักษะบุคลากรและผู้ที่มีส่วนเกี่ยวข้องให้มีความตระหนักและการระมัดระวังต่อการละเมิดความปลอดภัยทางไซเบอร์ 3. ส่งเสริมและสนับสนุนให้ผู้ปฏิบัติงานมีเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์

จากการวิเคราะห์สถานการณ์และผลการดำเนินงานเพื่อปิด GAP Analysis ให้บรรลุเป้าหมายของหน่วยงาน ดังนี้

1. ยกระดับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ตามเกณฑ์ CTAM และ Smart Hospital
    - ยกระดับมาตรฐานความปลอดภัยให้ครบทุกหน่วย
    - ขยายการควบคุมการเข้าถึง ระบบสำรองข้อมูล เครือข่าย และอุปกรณ์คอมพิวเตอร์
    - ทำให้การประเมินเป็นวงรอบสม่ำเสมอทั้งองค์กร
2. เสริมมาตรการเฝ้าระวังและลดความเสี่ยงจากภัยคุกคามเชิงรุก
    - เพิ่มความสามารถในการตรวจจับเหตุการณ์ผิดปกติ (Detection)
    - ใช้ระบบเฝ้าระวังภัยไซเบอร์ที่ครอบคลุมมากขึ้น
    - ลดจำนวนเหตุการณ์ละเมิดให้เป็นไปตามเป้าหมาย 50% อย่างต่อเนื่อง
    - เชื่อมโยงข้อมูลความเสี่ยงกับการวางแผนเชิงรุก
3. พัฒนาศักยภาพบุคลากรและความตระหนักด้านความปลอดภัยข้อมูล
    - เพิ่มการอบรมเชิงลึกด้าน Incident Response, PDPA, และภัยคุกคามใหม่
    - สร้างช่องทางสื่อสารความรู้ด้านไซเบอร์ให้เข้าถึงง่าย
    - ลดช่องว่างความรู้ระหว่าง IT ส่วนกลางและศูนย์อนามัย
    - เพิ่มกิจกรรมสร้างความตระหนัก เช่น คู่มือ, Infographic, การแจ้งเตือน