ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Assessment

1. บทวิเคราะห์สถานการณ์ของตัวชี้วัด

1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด (0.5)

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

- ผลผลิต/ ผลลัพธ์ระดับ C (Comparisons) การเปรียบเทียบ
- ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม
- ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน

ตาราง แสดงข้อมูลรายละเอียดผลผลิต/ผลลัพธ์ ได้แก่ ระดับ C (Comparisons) การเปรียบเทียบ, T (Trends) แนวโน้ม และ Le (Level) ของผลการดำเนินการในปัจจุบัน

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
ผลผลิต/ ผลลัพธ์ระดับ C (Comparisons) การเปรียบเทียบ	การวิเคราะห์เปรียบเทียบรูปแบบมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับป้องกันหรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที แสดงให้เห็นว่าการเตรียมความพร้อมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ คือ ปัจจัยสู่ความสำเร็จในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม สามารถสรุปการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ดังนี้ • **หน่วยงานที่ 1 : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
	• **หน่วยงานที่ 2 : กระทรวงสาธารณสุข** เป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) รับแจ้งเหตุภัยคุกคามทางไซเบอร์ และร่วมกับ Sectoral CERT รวบรวมข้อมูลตรวจสอบ ช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ดังนั้นเพื่อเป็นการขับเคลื่อนการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อทำหน้าหน้าที่ประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข
ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม	การมีมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ช่วยให้องค์กรสามารถวางแนวทางการยืนยันตัวตน ปกป้อง ตรวจสอบ และตอบสนองต่อภัยคุกคาม และฟื้นฟูระบบหลังจากได้รับผลกระทบไว้ได้อย่างดี พร้อมทั้งกำหนดบทบาทหน้าที่ให้สามารถนำมาใช้ได้ทันที
ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน	การทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่ละขั้นตอนจะช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ ดังนี้ - การบริหารจัดการความเสี่ยง (Identity) - การวางมาตรฐานควบคุมเพื่อปกป้องระบบองค์กร (Protect) - การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect) - การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Respone) - การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้องค์กรสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery) ผลการดำเนินการในปัจจุบันมีการดำเนินงาน ดังนี้ - การให้ความรู้และทำความเข้าใจกับบุคลากร โดยมีการประชุมแนวทางดำเนินงานด้านความปลอดภัยไซเบอร์ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ และการสแกนช่องโหว่บนเครือข่าย และตรวจสอบเฝ้าระวังสถานะเครื่องแม่ข่าย