บทที่ 4

การวิเคราะห์สภาพแวดล้อม
การรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดสุรินทร์

การวิเคราะห์สภาพแวดล้อมการรักษาความมั่นคงไซเบอร์ของ จังหวัดสุรินทร์
ประกอบด้วย 2 ส่วน ดังนี้

1. ความต้องการด้านเทคโนโลยีสารสนเทศ
2. การวิเคราะห์สถานภาพแวดล้อมด้วยการทำ SWOT Analysis

และภาพรวมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ

4.1 ความต้องการด้านเทคโนโลยีสารสนเทศ

จากการสำรวจและวิเคราะห์สถานภาพปัจจุบันทางด้านเทคโนโลยีสารสนเทศ พบว่าจังหวัดฯ ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไว้เป็นส่วนๆ อย่างชัดเจน ซึ่งส่วนมากจะเป็นแนวทางในการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของ จังหวัดฯ ประกอบกับจังหวัดฯ มีการดำเนินโครงการด้านไอซีทีต่าง ๆ ในรูปแบบของการจัดหาและติดตั้งอุปกรณ์ด้าน ICT โดยมีเจ้าหน้าที่ด้านเทคโนโลยีเป็นผู้ดูแลเท่าที่จำเป็นมาใช้ซึ่งยังไม่เต็มรูปแบบ และยังไม่ได้นำเทคโนโลยีสำหรับการบริหารจัดการด้าน ICT Security มาใช้งานมากนัก แต่ทั้งนี้ก็ถือได้สามารถดำเนินการป้องกันภัยทางไซเบอร์ได้เป็นอย่างดีในระดับหนึ่ง

ดังนั้น ในการพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ จังหวัดฯ จึงต้องคำนึงเทคโนโลยีสำหรับการบริหารจัดการและรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ทั้งด้านฮาร์ดแวร์และระบบซอฟต์แวร์ พร้อมทั้งแนวทางการปฏิบัติที่เป็นมาตรฐานในการสร้างระบบความมั่นคงปลอดภัย ซึ่งจำเป็นต้องคำนึงถึงองค์ประกอบต่าง ๆ ดังนี้

4.1.1 การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษาความปลอดภัยแบบบูรณาการของระบบสารสนเทศ (IT Security Detailed Design)

ระบบสารสนเทศของจังหวัดฯ นั้น จำเป็นต้องมีการออกแบบระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ที่ดีตั้งแต่ระดับของผู้ใช้งาน (End Point) ไปจนถึงระดับแอพลิเคชันของจังหวัดฯ โดยมีหลักการออกแบบ ดังนี้

4.1.1.1 สถาปัตยกรรมด้านความปลอดภัย (Security Architecture Principles)

ระบบสื่อสารเครือข่ายเป็นโครงสร้างพื้นฐานของระบบงานสารสนเทศทั้งหมดของ จังหวัดฯ รองรับการทำงานของหลายหน่วยงาน มีการรับส่งข้อมูลของระบบงานสารสนเทศด้านต่าง ๆ หลายระบบงานมีการใช้งานระบบสื่อสารทั้งรูปแบบภาพ เสียงและข้อมูล ดังนั้น ระบบเครือข่ายของ จังหวัดฯ จำเป็นต้องมีประสิทธิภาพและเสถียรภาพ มีความปลอดภัยสูง ดูแลรักษาได้ง่าย และมีความยืดหยุ่น

ในการปรับเปลี่ยนสามารถรองรับการขยายเพิ่มเติมได้ในอนาคต รวมถึงต้องมีระบบรักษาความปลอดภัยครอบคลุม ในทุกด้าน โดยมีเป้าหมายพื้นฐานในการออกแบบรักษาความมั่นคงปลอดภัย ด้วยการยึดหลักการของ CIA เพื่อให้ระบบสารสนเทศได้รับความมั่นคงปลอดภัย ดังต่อไปนี้

1) การรักษาความลับ (Confidentiality) การรักษาความลับเป็นการปกป้องการเข้าถึงและเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ข้อมูลที่เป็นความลับ จะยังคงไว้ซึ่งความพร้อมใช้ (Availability) และความแท้จริงของข้อมูล (Integrity)

2) ความแท้จริงของข้อมูล (Integrity) เป็นการป้องกันไม่ให้ข้อมูลถูกแก้ไขจากผู้ที่ไม่มีสิทธิ์ เพื่อให้ข้อมูลดังกล่าวมีความถูกต้อง และพร้อมใช้อยู่ตลอดเวลา

3) ความพร้อมใช้อยู่เสมอ (Availability) ระบบสารสนเทศ ที่ได้รับการป้องกันด้านความปลอดภัย จะมีคุณสมบัติพร้อมใช้ อยู่ตลอดเวลา โดยทั่วไป ความปลอดภัย (Security)

การบริหารจัดการระบบรักษาความปลอดภัยครบถ้วนสมบูรณ์ และเป็นระบบตรวจสอบและป้องกันการบุกรุกและป้องกันการโจรกรรมข้อมูลจากระบบงาน และระบบฐานข้อมูล ซึ่งระบบจะครอบคลุมการตรวจสอบและป้องกันการบุกรุกในรูปแบบต่าง ๆ ดังนี้

Security Matrix ของฮาร์ดแวร์และซอฟต์แวร์

ภาพรวมของระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของจังหวัดฯ จะครอบคลุมการตรวจสอบและการป้องกันการบุกรุกในรูปแบบต่างๆ แบ่งย่อยออกเป็น 5 กิจกรรมงานหลักด้านความมั่นคงปลอดภัยตามหลัก NIST Security Framework ได้แก่

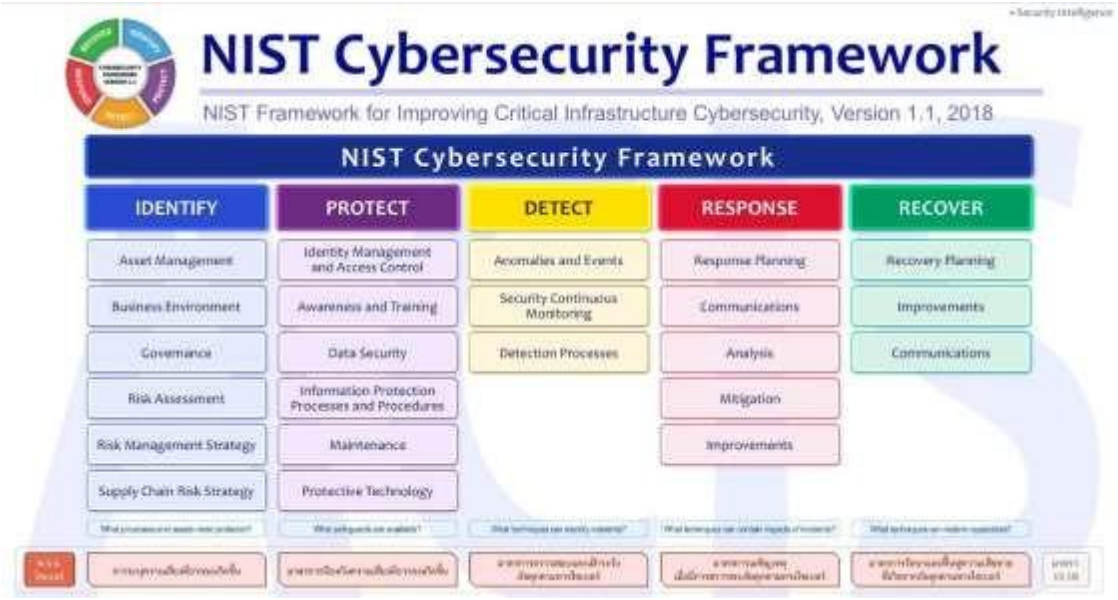
1) การระบุ (Identify) เป็นขั้นตอนการบริหารจัดการทรัพย์สิน และกิจกรรมงานสำคัญ ด้วยการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยที่มีต่อระบบ ทรัพย์สิน และข้อมูล เพื่อกำหนดกลยุทธ์ในการบริหารความเสี่ยง

2) การป้องกัน (Protect) จะเน้นการป้องกัน เพื่อจากัดระดับผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัย มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการ รวมไปถึงการตรวจสอบหาช่องโหว่ที่อาจพบในระบบและดำเนินการแก้ไข

3) การตรวจจับ (Detect) เป็นการเฝ้าระวังแบบเรียลไทม์จะมีการตรวจสอบวิเคราะห์ภัยคุกคามด้วยเทคนิคขั้นสูง ด้วยการรวบรวมข้อมูลและศึกษาพฤติกรรมที่เกิดขึ้น เพื่อตรวจหาภัยคุกคามที่อาจเกิดขึ้น

4) การตอบสนอง (Respond) เป็นการตอบสนองต่อภัยคุกคาม ตามขั้นตอนที่กำหนดไว้ โดยจะมีการสืบสวนทางข้อมูลดิจิทัล Packet Capture (PCAP) เพื่อการวิเคราะห์หาต้นเหตุของภัยคุกคามที่เกิดขึ้น

5) การคืนสภาพหรือการกู้คืน (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนระบบที่สามารถให้บริการตามที่กำหนด ทั้ง Transaction Log และ Backup



ภาพที่ 4–1 แสดงการวางแนวทางระบบรักษาความปลอดภัย
อ้างอิงข้อกำหนดตามมาตรฐาน NIST Cybersecurity Framework

ในการออกแบบ Security Matrix ให้ครอบคลุม 5 กิจกรรมหลักตามแนวทางของ NIST Cybersecurity Framework เพื่อป้องกันการบุกรุกและภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ แบ่งได้ ดังนี้

1) การระบุ (Identify)

ในระดับอุปกรณ์ (Device Layer) มีการจัดทำบัญชีรายชื่อครุภัณฑ์คอมพิวเตอร์ และอุปกรณ์ พร้อมมีระบบตรวจสอบพัสดุครุภัณฑ์ จังหวัดฯ เพื่อบริหารจัดการบัญชีครุภัณฑ์ของจังหวัดฯ

ในระดับระบบสารสนเทศ (Application Layer) มีการจัดหาอุปกรณ์เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น Firewall Web-App Firewall และ Anti-Virus เป็นต้น

ในระดับเครือข่าย (Network Layer) มีการกำหนดมาตรการป้องกันต่าง ๆ ในการเข้าถึงและใช้งานระบบต่าง ๆ ภายใน จังหวัดฯ

ในระดับข้อมูล (Data Layer) การมาตรการป้องกันการเข้าถึงและใช้งานข้อมูล และระบบงานสารสนเทศของ จังหวัดฯ

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้เพื่อให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการวิธีการป้องกันภัยทางไซเบอร์ในรูปแบบต่างๆ

2) การป้องกัน (Protect)

มีการทำ Identity and Access Management เพื่อแยกแยะกลุ่มผู้ใช้งานและสิทธิ์การใช้งานระบบสารสนเทศของ จังหวัดฯ

ในระดับอุปกรณ์ (Device Layer) จะมีการติดตั้ง Endpoint Anti-Virus และ Intrusion Prevention System (IPS) เพื่อป้องกันภัยคุกคาม

ในระดับระบบสารสนเทศ (Application Layer) จะมีติดตั้ง Web Application Firewall (WAF) เพื่อตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application)

ในระดับเครือข่าย (Network Layer) จะใช้เทคโนโลยี Next-Generation Firewall (NG-FW) ในการป้องกันระบบเครือข่าย

ในระดับข้อมูล (Data Layer) จะมีการดำเนินการด้าน Personal Data Protection Act (PDPA) เพื่อรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และการสำรองข้อมูลของระบบสารสนเทศ

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้ให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการวิธีการป้องกันภัยทางไซเบอร์ในรูปแบบต่าง ๆ

3) การตรวจจับ (Detect) และการตอบสนอง (Response)

ในระดับอุปกรณ์ (Device Layer) จะมีการติดตั้งป้องกันไวรัส (Anti-Virus) เพื่อป้องกันการโจมตีจากไวรัส และพวก Malware

ในระดับเครือข่าย (Network Layer) มีการติดตั้งอุปกรณ์ป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์ เพื่อป้องกันระบบเครื่องคอมพิวเตอร์แม่ข่าย-ลูกข่าย และระบบเครือข่ายภายใน จังหวัดฯ

ในระดับข้อมูล (Data Layer) ใช้การบริหารจัดการสิทธิ์ในการเข้าถึงระบบงานสารสนเทศ และข้อมูล

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้เพื่อให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ให้สามารถเฝ้าระวังเพื่อลดความเสี่ยงของการเกิดภัยทางไซเบอร์ และให้สามารถแก้ไขปัญหาเบื้องต้นได้

4) การคืนสภาพหรือการกู้คืน (Recover)

ในระดับระบบสารสนเทศ (Application Layer) ที่มีการเก็บ Transaction Log และในระดับข้อมูล (Data Layer) รวมถึงในระดับข้อมูล (Data Layer) จะทำการ Backup ข้อมูลอย่างสม่ำเสมอ เพื่อกู้คืนข้อมูลที่ในกรณีที่ข้อมูลหรือระบบได้รับความเสียหาย

การให้บริการระบบสารสนเทศผ่านการรักษาความมั่นคงปลอดภัย แบ่งออกเป็น 2 ส่วน คือ

1) การให้บริการระบบเทคโนโลยีสารสนเทศภายใน (Intranet) ให้เจ้าหน้าที่ของ จังหวัดฯ เข้าใช้งานระบบจากเครือข่ายภายในเครือข่ายของ จังหวัดฯ

2) การให้บริการระบบเทคโนโลยีสารสนเทศภายนอก (Internet) ให้เจ้าหน้าที่และผู้ใช้งานทั่วไปเข้าใช้งานระบบสารสนเทศของ จังหวัดฯ จากเครือข่ายอินเทอร์เน็ต

การออกแบบระบบรักษาความมั่นคงปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และข้อมูลหลัก (Server and Data Center Zone) จะกำหนดให้อยู่ในโซนแม่ข่าย (DMZ Zone) และมีการป้องกันการถูกโจมตีด้วย Web Application Firewall และอุปกรณ์ DNS ที่ช่วยในการป้องกันการโจมตีข้อมูล ในขณะที่โซนเครื่องคอมพิวเตอร์ลูกข่ายจะได้รับการป้องกันการถูกโจมตี ทั้งจาก Firewall และ Anti-Virus และมีการอัพเดท Patch ความปลอดภัยอย่างสม่ำเสมอ ในส่วนของระบบงานสารสนเทศ และชุดข้อมูลใน Database จะมีการสำรองข้อมูลอย่างสม่ำเสมอ

ดังนั้น ในภาพรวมของระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ จังหวัดฯ จะสามารถแบ่งออกตามลักษณะของการให้บริการต่าง ๆ ดังนี้

1) ระบบรักษาความมั่นคงปลอดภัยสำหรับระบบเครือข่ายภายใน เป็นส่วนของการรักษาความมั่นคงปลอดภัยสำหรับช่องทางการเข้าถึงระบบงานสารสนเทศภายในเครือข่ายของจังหวัดฯ

2) ระบบรักษาความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบอินเทอร์เน็ตของจังหวัดฯ เป็นส่วนที่รักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบอินเทอร์เน็ต จากเครือข่าย คอมพิวเตอร์ ทั้งหมดของ จังหวัดฯ ทั้งแบบมีสาย (Wired) และแบบไร้สาย (Wireless)

การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษาความปลอดภัยระบบเครือข่ายในส่วนของอินเตอร์เน็ตโซน (Internet Zone) ระบบเครือข่ายของ จังหวัดฯ จำเป็นต้องมีการรักษา ความมั่นคงปลอดภัย ที่มีประสิทธิภาพ และมีความน่าเชื่อถือ ดังนั้น จึงมีการติดตั้งอุปกรณ์การรักษาความมั่นคงปลอดภัย ดังนี้

1)อุปกรณ์ Next Generation Firewall (NG–Firewall) ทำหน้าที่ป้องกันและควบคุมการใช้งานอินเตอร์เน็ตในระดับแอปพลิเคชัน สามารถกำหนดการเข้า-ออกของจราจรทางคอมพิวเตอร์ตามนโยบาย ของ จังหวัดฯ และการป้องกันการโจมตี เช่น HTTP Flood Attacks, DNS Flood Attacks และ SSL Flood Attacks รวมถึงการบริหารจัดการ ช่องทางเชื่อมต่อ อินเตอร์เน็ตตามนโยบายของ จังหวัดฯ และการรักษาความปลอดภัย ด้วยวิธีการแปลงหมายเลข IP Address ด้วยวิธีการทำ Network Address Translation (NAT)

2) อุปกรณ์ Wireless Controller ทำหน้าที่บริหารจัดการ การเชื่อมต่อ อุปกรณ์กับระบบเครือข่ายอินเทอร์เน็ตผ่านอุปกรณ์กระจายสัญญาณเครือข่ายแบบไร้สาย (Wireless)

3) อุปกรณ์ Web Application Firewall (WAF) เป็นอุปกรณ์ป้องกัน การโจมตีระดับเน็ตเวิร์ค และแอปพลิเคชันที่ทำหน้าที่ตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application) ซึ่งตรวจจับและป้องกันการบุกรุกเครือข่ายแบบ Real–Time รวมทั้งสามารถ กำหนดการใช้งานของแอปพลิเคชันต่าง ๆ ของ จังหวัดฯ ได้

การออกแบบสถาปัตยกรรมฮาร์ดแวร์ และซอฟต์แวร์ของระบบรักษาความปลอดภัย ในส่วน DMZ Zone (โซนเครือข่ายความปลอดภัยที่แยกเซิร์ฟเวอร์สาธารณะออกจากเครือข่ายภายใน ช่วยป้องกันการโจมตีจากอินเทอร์เน็ต) แอปพลิเคชันและเซอร์วิส (Application and Service) ที่ให้บริการทั้งผู้ใช้งานภายในและผู้ใช้งานภายนอกของจังหวัดฯ ได้ทำการแยกออกจากส่วนของระบบเครือข่าย เพื่อป้องกันภัยจากการบุกรุก และการโจมตีจากอินเตอร์เน็ต แต่ยังให้บริการแอปพลิเคชันและเซอร์วิสได้ โดยมีดังนี้

1) อุปกรณ์ Web Application Firewall (WAF) เป็นอุปกรณ์ป้องกันการโจมตี ทำหน้าที่ตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application) ของ จังหวัดฯ จากผู้ใช้งานภายใน และผู้ใช้งานภายนอก โดยการกำหนดนโยบาย (Policy) การเข้าถึงระบบงานต่าง ๆ

2) ระบบป้องกันไวรัส (Anti-Virus) ทำหน้าที่ป้องกันการบุกรุกจากภัยประเภทไวรัสและซอร์สโค้ด (Source Code) ที่ไม่ประสงค์ดี เช่น สามารถป้องกันสแปม (Spam) จัดการปัญหาสแปมจากแหล่งที่มาต่าง ๆ (Reputation) ป้องกัน Virus ประเภทมัลแวร์ (Malware) และสปายแวร์ (Spyware) เป็นต้น

3) อุปกรณ์บริหารจัดการ DNS/DHCP สำหรับติดตั้งในโซน DMZ เป็นอุปกรณ์ที่ทำหน้าที่กำหนดการให้บริการ IP Address (DHCP) และ DNS ภายในกับเครื่องลูกข่ายในระบบ โดยการทำ DNS Query และทำ Real-Time update (ในส่วนของ DNS)

4.1.3 การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษา ความปลอดภัยระบบเครือข่ายในส่วนของโซนภายใน (Internal Zone)

4.1.4 การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ระบบพิสูจน์ตัวตนและกำหนดสิทธิ์ในการเข้าถึงระบบเครือข่ายของ จังหวัดฯ

จังหวัดฯ มีระบบพิสูจน์ตัวตนของผู้เข้าใช้งานระบบเครือข่ายภายใน และระบบสารสนเทศสำหรับบุคคลของจังหวัดฯ ซึ่งเป็นการตรวจสอบ ระบุตัวตน และกำหนดสิทธิ์ ในการเข้าใช้งานระบบต่างๆ ภายในจังหวัดฯ ซึ่งกำหนดให้ผู้ใช้งาน จะต้องมีการดำเนินการพิสูจน์ตัวตน ทั้งระบบเครือข่ายแบบมีสาย (Wire LAN) และแบบไร้ สาย (Wireless LAN)

4.1.5 การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ระบบรักษาความปลอดภัยของระบบ เครื่องแม่ข่ายในส่วนของ Data Center

1) อุปกรณ์ป้องกันการบุกรุกและโจมตีระบบเครือข่าย (Firewall) เป็นอุปกรณ์ป้องกันการบุกรุกและการโจมตีระบบ ทำหน้าที่ตรวจจับ และคัดกรองข้อมูล จราจรทางคอมพิวเตอร์ ที่จะเข้ามาสู่ระบบเครื่องแม่ข่าย เพื่อป้องกันการถูกโจมตีจากภัยทางไซเบอร์ต่าง ๆ ที่จะเข้าถึงระบบงาน และข้อมูลสำคัญของ จังหวัดฯ และยังกำหนดนโยบาย (Policy) การเชื่อมต่อข้อมูลกับภายนอกอีกด้วย

2) ระบบป้องกันไวรัส (Anti-Virus) สำหรับเครื่องแม่ข่าย ทำหน้าที่ป้องกันภัยคุกคามในระดับเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual machines) โดยรองรับการ integrates กับ Endpoint เพื่อป้องกันการโจมตีที่ซับซ้อน อาทิ ไวรัสมัลแวร์ (Malware) สปายแวร์ (Spyware) และโทรจัน (Trojans) เป็นต้น

3) การสำรองข้อมูลเครื่องแม่ข่าย (Data Center Backup) โดยมีการทำการสำรองข้อมูลให้ระบบสารสนเทศต่าง ๆ ของ จังหวัดฯ เป็นประจำทั้งระบบเครื่องแม่ข่าย และระบบเครื่องแม่ข่ายเสมือน โดยมีการทำการสำรองข้อมูล 3 รูปแบบ ได้แก่ แบบ Incremental แบบ Full Backup และ การสำรองข้อมูล Backup ที่อุปกรณ์จัดเก็บข้อมูลภายนอก (Storage)

4.1.2 การออกแบบการบริหารข้อมูลส่วนบุคคล (Identity Management)

การบริหารข้อมูลส่วนบุคคล หรือ Identity Management หมายถึง ระบบที่สามารถใช้บริหารรายชื่อผู้ใช้งานรวมถึงรายละเอียดในการใช้งานระบบงานสารสนเทศ (User Information and User Profiles) แต่ระบบได้ ในขณะที่ Single Sign-on หมายถึง กระบวนการ ที่จะบริหารจัดการเรื่องของรหัสผ่าน ซึ่งปกติผู้ใช้งานจะมีรหัสผ่าน มากกว่าหนึ่งรหัส เพื่อเข้าใช้งานระบบสารสนเทศ อาทิ รหัสสำหรับระบบ เครือข่ายภายในหรือเข้าสู่ระบบอินเทอร์เน็ต รหัสสำหรับการใช้งานวินโดวส์ รหัสสำหรับเข้ารับระบบสารสนเทศ หรือระบบฐานข้อมูล รวมถึงปัญหาเรื่องของการลืมรหัสผ่าน การเปลี่ยนรหัสตามเวลาที่กำหนด

การบริหารจัดการการเข้าถึงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ แอปพลิเคชันต่าง ๆ และระบบฐานข้อมูลของผู้ใช้งาน จึงเป็นสิ่งจำเป็น ด้วยระบบบริหารแบบศูนย์กลาง Identity Management ผู้ดูแลระบบจะสามารถสร้าง แก้ไข และลบข้อมูลรายชื่อผู้ใช้งานทั้งบน Active Directory และ LDAP ที่ออกแบบไว้ โดยระบบ Identity Management จะมีฟังก์ชันการทำงานหลัก อาทิ User Provisioning, Password Management และ User Profile Management

4.2 การวิเคราะห์สถานภาพแวดล้อมด้วยการทำ SWOT Analysis และภาพรวมของระบบรักษาความมั่นคง ปลอดภัยไซเบอร์

การวิเคราะห์สถานภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ จังหวัดฯ เพื่อค้นหาโอกาสภัยคุกคาม จุดแข็ง จุดอ่อนหรือข้อด้อย และสิ่งที่เป็นปัญหาสำคัญในการดำเนินงานทางด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ จังหวัดฯ โดยวางกรอบแนวคิดในการวิเคราะห์สภาพแวดล้อม (SWOT Analysis) เพื่อวิเคราะห์สภาพแวดล้อมด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ จังหวัดฯ ซึ่งได้มีการแยก การวิเคราะห์ สภาพแวดล้อมที่เป็นผลจากปัจจัยจากภายนอกและปัจจัยจากภายใน ซึ่งสามารถแสดงได้ดังภาพที่ 4-2

ภาพที่ 4–2 การวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ ด้วย SWOT

การดำเนินการวิเคราะห์สถานภาพแวดล้อมด้วยการทำ SWOT Analysis ได้นำผลการวิเคราะห์จากแผนปฏิบัติการดิจิทัลจังหวัดสุรินทร์ พ.ศ. 2568 - 2570 และจากประสบการณ์ของเจ้าหน้าที่ผู้ดูแลระบบงานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และะระบบสารสนเทศของจังหวัดฯ

4.2.1 ผลการวิเคราะห์ SWOT Analysis ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ การวิเคราะห์สภาพแวดล้อมซึ่งมีผลจากปัจจัยภายใน ประกอบด้วยการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดแข็ง (Strengths) และการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดอ่อน (Weaknesses) ดังนี้

ตารางที่ 4–1 ผลการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดแข็ง (Strengths)

รหัส	จุดแข็ง (Strengths)
S1	ผู้นำและผู้บริหารระดับสูงของ จังหวัดฯ มีวิสัยทัศน์ และให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์
S2	จังหวัดฯ มีนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนตามแผนปฏิบัติการดิจิทัลจังหวัดฯ พ.ศ. 2568 - 2570 ในยุทธศาสตร์ที่ 2
S3	จังหวัดฯ มีผู้บริหารด้านเทคโนโลยีสารสนเทศ และคณะกรรมการ PCIO ในการขับเคลื่อนงานด้านเทคโนโลยีของจังหวัดฯ และสามารถเข้ามากำกับดูแล ให้ข้อเสนอแนะงานด้านความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ ได้
S4	จังหวัดฯ มีแนวคิดมุ่งให้ความสำคัญในการดำเนินงานและพัฒนางานด้านความมั่นคงปลอดภัยด้านไซเบอร์ ทั้งในส่วนของฮาร์ดแวร์ และซอฟต์แวร์
S5	มีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและดิจิทัลที่ค่อนข้างเพียงพอต่อการใช้งานและมีความยืดหยุ่นพอสมควร
S6	บุคลากรด้าน ICT ค่อนข้างมีความพร้อมเรียนรู้ในการพัฒนางาน ด้านความมั่นคงปลอดภัยไซเบอร์ และเฝ้าระวังภัยทางไซเบอร์อย่างต่อเนื่อง
S7	บุคลากรของจังหวัดฯ มีทักษะการใช้ระบบคอมพิวเตอร์ และเทคโนโลยีในปฏิบัติงาน
S8	บุคลากรของ จังหวัดฯ สามารถปรับตัวกับเทคโนโลยีใหม่ และพร้อมเรียนรู้และพัฒนาตนเอง

ตารางที่ 4–2 ผลการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดอ่อน (Weaknesses)

รหัส	จุดอ่อน (Weaknesses)
W1	กลยุทธ์การพัฒนาดิจิทัลของจังหวัดฯ ที่ผ่านมายังไม่ครอบคลุมทุกยุทธศาสตร์ของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย
W2	การประชาสัมพันธ์และการสร้างการตระหนักรู้ในเรื่องความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรของจังหวัดฯ ยังไม่มากเท่าที่ควร
W3	สถานที่และพื้นที่ในส่วนของงานบริหารและปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์มีโครงสร้างและพื้นที่จำกัด ในการจัดวางอุปกรณ์ของระบบรักษาความมั่นคงปลอดภัยด้าน ICT
W4	ระบบรักษาความปลอดภัยด้าน ICT ของจังหวัดฯ ยังมีไม่เต็มประสิทธิภาพเพียงพอ
W5	ยังไม่มีการจัดทำแนวทางและมาตรการการรับมือภัยคุกคามทางไซเบอร์อย่างเป็นลายลักษณ์อักษร
W6	ยังไม่มีมาตรการหรือแนวทางที่ชัดเจนในการดำเนินการเกี่ยวกับระบบติดตาม เฝ้าระวัง และเตือนภัย (Warning System)
W7	บุคลากรด้าน ICT ของ จังหวัดฯ ที่มีความรู้ ทักษะ และความเชี่ยวชาญ เฉพาะทางด้านความมั่นคงปลอดภัย (Digital Skill) ยังมีจำนวนไม่เพียงพอ
W8	บุคลากรของ จังหวัดฯ บางส่วนยังขาดความรู้ ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยไซเบอร์

การวิเคราะห์สภาพแวดล้อมซึ่งมีผลจากปัจจัยภายนอก ประกอบด้วย การวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นโอกาส (Opportunities) และการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นภัยคุกคามและอุปสรรค (Threats) ดังนี้

ตารางที่ 4–3 ผลการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นโอกาส (Opportunities)

รหัส	ปัจจัยสภาพแวดล้อมภายนอกที่เป็นโอกาส (Opportunities)
O1	การปรับเปลี่ยนจังหวัดฯ สู่การเป็นองค์กรดิจิทัล และได้รับการประกาศให้เป็นเขต Smart City ทำให้เกิดการออกแบบและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
O2	การเข้าสู่ยุคสังคมออนไลน์ ทำให้ประชาชนให้ความสนใจข้อมูลข่าวสารต่างๆ จากสื่อสังคมออนไลน์ ทำให้จังหวัดฯ มีช่องทางในการสื่อสารกับประชาชนมากขึ้นไปด้วย
O3	มีหน่วยงานภายนอกที่สามารถให้การสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัย เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นต้น
O4	รัฐบาลให้ความสำคัญในการกำหนดทิศทางพัฒนารัฐบาลดิจิทัล เพื่อบูรณาการข้อมูลประชาชนให้เป็นภาพเดียวกัน และหน่วยงานในภาครัฐให้ความสำคัญกับการบูรณาการฐานข้อมูล ตลอดจนประสานเชื่อมโยงกระบวนงานสารสนเทศร่วมกัน
O5	การพัฒนาของเทคโนโลยีที่หลากหลายและมีความทันสมัย ทำให้จังหวัดฯ มีทางเลือกในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ให้มีความเหมาะสมและมีประสิทธิภาพ

ตารางที่ 4–4 ผลการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นอุปสรรค (Threats)
งหวัดฯ

รหัส	ปัจจัยสภาพแวดล้อมที่กำหนดภายนอกที่เป็นอุปสรรค
T1	การได้รับจัดสรรงบประมาณดำเนินการเกี่ยวกับแผนงาน/โครงการด้านความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ ยังมีข้อจำกัด
T2	การเปลี่ยนแปลงของเทคโนโลยีด้าน ICT ที่รวดเร็ว ทำให้มีความเสี่ยงจากภัยทางไซเบอร์มากขึ้น
T3	อุปกรณ์และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการพัฒนาตลอดเวลาและมีราคาสูง ส่งผลต่อการขอรับการจัดสรรงบประมาณในการลงทุนของจังหวัดฯ
T4	ภัยทางไซเบอร์มีการพัฒนารูปแบบ กระบวนการ และความรุนแรงในการโจมตีอย่างต่อเนื่อง
T5	ระบบความมั่นคงปลอดภัยทางด้าน ICT ของหน่วยงานภาครัฐส่วนใหญ่ยังขาดการบูรณาการร่วมกัน

4.1.1 การวิเคราะห์ด้วย TOWS Matrix

จากการวิเคราะห์สภาพแวดล้อมด้วยการทำ SWOT Analysis ทำให้ทราบถึงปัจจัยสภาพแวดล้อมภายนอก ซึ่งได้แก่ โอกาสและอุปสรรค และปัจจัยสภาพแวดล้อมภายใน ซึ่งได้แก่ จุดแข็งและจุดอ่อน ที่ส่งผลต่อกระทบต่อนโยบายการพัฒนาและการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ ซึ่งสามารถนำสิ่งที่ได้จากการวิเคราะห์มากำหนดเป็นแผนงาน เพื่อนำไปสู่การกำหนดโครงการต่าง ๆ โดยการวิเคราะห์ด้วยเครื่องมือ TOWS Matrix สามารถแสดงได้ดังในภาพที่ 4–3

ภาพที่ 4–3 การวิเคราะห์สภาพแวดล้อมโดยใช้เครื่องมือ TOWS Matrix

TOWS Matrix เป็นเครื่องมือในการกำหนดกลยุทธ์ โดยวิธีการจับคู่กันระหว่างปัจจัยสภาพแวดล้อมภายนอกกับปัจจัยสภาพแวดล้อมภายใน คำว่า “TOWS” เป็นตัวย่อที่มาจากแต่ละปัจจัย ได้แก่ อุปสรรค (Threats) โอกาส (Opportunities) จุดอ่อนหรือข้อด้อย (Weaknesses) และ จุดแข็ง (Strengths) ซึ่งการจับคู่กันนี้ จะได้ผลเป็นกลยุทธ์ทั้งหมด 4 รูปแบบ ได้แก่

1) กลยุทธ์ SO การจับคู่กันระหว่างจุดแข็งกับโอกาส (SO) เพื่อนำจุดแข็งที่มีอยู่ร่วมกับโอกาสที่ปรากฏมากำหนดแผนงานโครงการที่จะพัฒนา

2) กลยุทธ์ ST การจับคู่กันระหว่างจุดแข็งกับความเสี่ยง (ST) เพื่อนำจุดแข็งที่มีอยู่มากำหนดเป็นกลยุทธ์ในการขับเคลื่อนแผน เพื่อป้องกันหรือหลีกเลี่ยงอุปสรรคที่จะเกิดขึ้นจากภายนอก

3) กลยุทธ์ WO การจับคู่กันระหว่างจุดอ่อนกับโอกาส (WO) เพื่อนำโอกาสที่ปรากฏอยู่มากำหนดเป็นกลยุทธ์ในการขับเคลื่อนแผนเพื่อกำจัดหรือลดจุดอ่อนที่มี

4) กลยุทธ์ WT การจับคู่กันระหว่างจุดอ่อนกับอุปสรรค (WT) เป็นการกำหนดกลยุทธ์ในการขับเคลื่อนแผน เพื่อกำจัดหรือลดจุดอ่อนที่มี และป้องกันหรือหลีกเลี่ยงภัยคุกคามที่เกิดจาก ภายนอกด้วยในเวลาเดียวกัน

ตารางที่ 4-5 กลยุทธ์ที่ได้จากการวิเคราะห์ TOWS Matrix

	จุดแข็ง (Strengths–S)	จุดอ่อน (Weaknesses–W)
โอกาส (Opportunities–O)	กลยุทธ์เชิงรุก SO - การทบทวนนโยบายและแผนงานของหน่วยงาน เพื่อสร้างนิเวศที่เอื้อต่องานด้านความมั่นคงปลอดภัยไซเบอร์ (S1, S2, S3, S4 กับ O1, O2) - การเฝ้าระวังภัยไซเบอร์และการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (S5, S6, S7 กับ O3, O4) - การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้ได้มาตรฐานสากล (S4, S5, S6, S7 กับ O3, O4, O5, O6) - การพัฒนาบุคลากร ICT ให้มีความรู้ทักษะ และความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ และมีความเป็นมืออาชีพ (S1, S3, S4, S8, S9 กับ O1, O2, O6)	กลยุทธ์เชิงแก้ไข WO - การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ให้ทันสมัยและปลอดภัย (W4 กับ O1, O6) - การปรับปรุงแนวทาง มาตการและแนวปฏิบัติ เพื่อเพิ่มศักยภาพงานความมั่นคงปลอดภัยไซเบอร์ (W1, W5, W6 กับ O1, O3, O4, O6) - การสร้างความตระหนักรู้ด้านภัยทางไซเบอร์แก่บุคลากรของ จังหวัดฯ (W2, W8 กับ O1, O3, O5)
อุปสรรค (Threats–T)	กลยุทธ์เชิงป้องกัน ST - การพัฒนาศักยภาพงานป้องกันและรับมือภัยคุกคามทางไซเบอร์ (S4, S5, S6, S7 กับ T1, T2 ,T3, T4, T4) - การบริหารความต่อเนื่องของงาน ด้าน ICT (S4, S5 กับ T1, T2, T3, T4) - การสร้างความร่วมมือในงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น (S6 กับ T5)	กลยุทธ์เชิงรับ WT - การพัฒนาบุคลากรด้าน ICT ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี (W3, W4, W7 กับ T2, T4) - การบริหารความเสี่ยงและการกำหนดมาตการและแนวทางการรับมือภัยคุกคามทางไซเบอร์ (W1, W5, W6 กับ T1, T2, T3, T4, T5) - การแก้ปัญหาด้านภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (W3, W4, W5, W6 W4, กับ T1, T2, T4, T5)

จากการวิเคราะห์ TOWS Matrix สามารถนำมาเชื่อมโยงเพื่อหาความสัมพันธ์และจัดกลุ่มเข้าด้วยกัน เพื่อกำหนดเป็นแผนงาน ได้ดังนี้

ตารางที่ 4–6 การเชื่อมโยงกลยุทธ์ที่ได้จาก TOWS Matrix ไปสู่การกำหนดแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จังหวัดฯ พ.ศ. 2568 - 2570)

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
1	การทบทวนนโยบายและแผนงานของหน่วยงาน เพื่อสร้างนิเวศที่เอื้อต่องานด้านความมั่นคงปลอดภัยไซเบอร์ (S1, S2, S3, S4 กับ O1, O2)	กลยุทธ์เชิงรุก (SO)	1.จัดทำแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จังหวัดฯ 2.จัดทำและทบทวน ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 3.จัดทำและทบทวน แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของจังหวัดฯ 4.จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) 5.จัดทำและทบทวน แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) 6.จัดทำและทบทวน แผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) 7.จัดทำและทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดฯ 8.การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของจังหวัดฯ

2	การเฝ้าระวังภัยไซเบอร์ (S5, S6, S7 กับ O3, O4)	กลยุทธ์เชิงรุก (SO)	1.การดำเนินการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์ 2.การกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ
3	การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้ได้มาตรฐานสากล (S4, S5, S6, S7 กับ O3, O4, O5, O6)	กลยุทธ์เชิงรุก (SO)	1.จัดหาโครงสรางพื้นฐานและอุปกรณ์ดิจิทัลทั้ง Hardware Software และ Network ให้เหมาะสมและเพียงพอต่อการปฏิบัติงาน 1.จัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture) ของ จังหวัดฯ 2.โครงการพัฒนาระบบเว็บท่า จังหวัดฯ 3.โครงการจัดจ้างผู้เชี่ยวชาญเพื่อพัฒนาและปรับปรุงระบบสารสนเทศ ให้ผ่านการรับรองมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ISO/IEC 27001:2013
4	การพัฒนาบุคลากร ICT ให้มีความรู้ทักษะ และความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ และมีความเป็นมืออาชีพ (S1, S3, S4, S8, S9 กับ O1, O2, O6)	กลยุทธ์เชิงรุก (SO)	การพัฒนาทักษะ และยกระดับความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากร ICT จังหวัดฯ
5	การพัฒนาศักยภาพงานป้องกันและรับมือภัยคุกคามทางไซเบอร์ (S4, S5, S6, S7 กับ T1, T2 ,T3 T4, T4)	กลยุทธ์เชิงป้องกัน (ST)	1. โครงการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย 2. โครงการบำรุงรักษาระบบเว็บท่า จังหวัดฯ

6	การบริหารความต่อเนื่องของงานด้าน ICT (S4, S5 กับ T1, T2, T3, T4)	กลยุทธ์เชิงป้องกัน (ST)	1.จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) 2.จัดทำและทบทวน แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) 3.จัดทำและทบทวน แผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) 4.จัดทำและทบทวน แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของจังหวัดฯ 5.จัดทำและทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดฯ
7	การสร้างความร่วมมือในงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น (S6 กับ T5)	กลยุทธ์เชิงป้องกัน (ST)	การดำเนินงานให้สอดคล้องและเป็นไปตามหน่วยงานกลางที่รับผิดชอบขับเคลื่อนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ
8	การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ให้ทันสมัยและปลอดภัย (W4 กับ O1, O6)	กลยุทธ์เชิงแก้ไข (WO)	1. โครงการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย 2. โครงการบำรุงรักษาระบบเว็บท่าจังหวัดฯ 3. การดำเนินการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์
9	การปรับปรุงแนวทาง มาตรการและแนวปฏิบัติ เพื่อเพิ่มศักยภาพงานด้านความมั่นคงปลอดภัยไซเบอร์ (W1, W5, W6 กับ O1, O3, O4, O6)	กลยุทธ์เชิงแก้ไข (WO)	จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ จังหวัดฯ

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
10	การสร้างความตระหนักรู้ด้านภัยทางไซเบอร์แก่บุคลากรของจังหวัดฯ (W2, W8 กับ O1, O3, O5)	กลยุทธ์เชิงแก้ไข (WO)	1.ฝึกอบรมและการสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของบุคลากร จังหวัดฯ 2.การจัดทำ และเผยแพร่สื่อประชาสัมพันธ์ หรือสื่ออินโฟกราฟิกเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
11	การพัฒนาบุคลากรด้าน ICT ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี (W3, W4, W7 กับ T2, T4)	กลยุทธ์เชิงรับ (WT)	พัฒนาทักษะ และยกระดับความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากร ICT จังหวัดฯ
12	การบริหารความเสี่ยงและการกำหนดมาตรการและแนวทางการรับมือภัยคุกคามทางไซเบอร์ (W1, W5, W6 กับ T1, T2, T3, T4, T5)	กลยุทธ์เชิงรับ (WT)	1.จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) 2.จัดทำและทบทวน แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) 3.จัดทำและทบทวน แผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) 4.จัดทำและทบทวน แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของจังหวัดฯ 5.จัดทำและทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดฯ
13	การแก้ปัญหาด้านภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (W3, W4, W5, W6 W4, กับ T1, T2, T4, T5)	กลยุทธ์เชิงรับ (WT)	1. โครงการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย 2. การดำเนินการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์

จากการวิเคราะห์ TOWS Matrix ทำให้สามารถสรุปประเด็น และกลยุทธ์ในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งสามารถนำไปกำหนดเป็นแผนงาน/โครงการเพื่อนำไปสู่การขับเคลื่อน และเพิ่มศักยภาพให้ได้ครอบคลุมตามประเด็นดังกล่าวข้างต้นด้วย