5.4 นโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศ

บริษัทฯ ให้ความสำคัญและตระหนักถึงความจำเป็นในการบริหารจัดการความเสี่ยง การรักษาความมั่นคงปลอดภัยทางไซเบอร์ และระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด เพื่อป้องกันและเตรียมความพร้อมในการรับมือกับภัยคุกคามที่อาจเกิดขึ้น

บริษัทฯ ได้แต่งตั้ง คณะกรรมการกำกับดูแลและติดตามการบริหารจัดการความเสี่ยง รวมถึงจัดตั้งคณะทำงานด้านเทคนิค เพื่อวิเคราะห์และพิจารณาประเด็นเชิงเทคนิคอย่างเป็นระบบ พร้อมดำเนินการประเมิน ระดับวุฒิภาวะ ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Maturity) ตามกรอบมาตรฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST)

ทั้งนี้ เพื่อเสริมสร้างความเชื่อมั่นและความมั่นคงให้แก่ลูกค้า ตลอดจนผู้มีส่วนได้เสียทุกภาคส่วน รวมถึงขับเคลื่อนการดำเนินงานให้เป็นไปตามนโยบายด้านความมั่นคงทางไซเบอร์และระบบเทคโนโลยีสารสนเทศ ขององค์กรอย่างต่อเนื่องและมีประสิทธิภาพ

แนวทางการจัดการความเสี่ยงความปลอดภัยของข้อมูล และระบบสารสนเทศ

บริษัทฯ ได้กำหนดแนวทางในการบริหารจัดการและควบคุมความเสี่ยง ด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ อย่างเป็นระบบและมีประสิทธิภาพ โดยยึดหลักการและแนวทางปฏิบัติที่สอดคล้องกับมาตรฐานสากล อาทิ ISO/IEC 27001 และ NIST Cybersecurity Framework เพื่อเสริมสร้างความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศอย่างเข้มแข็ง ทำให้บริษัทฯ มีความพร้อมในการวางแผน ป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามต่างๆ ได้อย่างทันท่วงที เป็นระบบ และมีประสิทธิผลสูงสุด

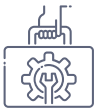
แนวทางดังกล่าวมีเป้าหมาย เพื่อเสริมสร้างความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ ให้แข็งแกร่ง พร้อมรองรับการวางแผน ป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นได้อย่าง ทันท่วงที เป็นระบบ และมีประสิทธิผล โดยบริษัทฯ ดำเนินงานตามแนวทางดังต่อไปนี้:

การกำกับดูแล

การกำกับดูแลด้านความมั่นคงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

การเข้าใจตนเอง

การประเมินขีดความสามารถในการบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ



การวางแผนและปรับปรุง

ทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

การส่งเสริมความและระบบสารสนเทศ

สร้างความตระหนักรู้ และเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ให้พนักงานทุกระดับ ตลอดจนคู่ค้าอย่างต่อเนื่อง

การติดตามและประเมินความเสี่ยง

ติดตามผลการดำเนินงาน นำกลยุทธ์ มาตรการมาใช้เพื่อลดโอกาสความเสี่ยง หรือลดความเสียหาย

การกำกับดูแลด้านความมั่นคงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทฯ ได้ประกาศและทบทวนนโยบาย ด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาจากข้อกำหนด ทางกฎหมายที่เกี่ยวข้อง รวมถึงความคาดหวังของผู้มีส่วนได้เสียเพื่อกำหนดทิศทาง หลักการ และกรอบการดำเนินงานด้านความมั่นคงปลอดภัยอย่างเหมาะสม

นอกจากนี้ บริษัทฯ ได้แต่งตั้งคณะกรรมการกำกับดูแลด้านการบริหารความเสี่ยง และจัดตั้งคณะทำงานด้านเทคนิคโดยมีหน่วยงานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบหลักในการดำเนินงานติดตาม และรายงานผลต่อคณะกรรมการที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่สนใจสามารถดาวน์โหลดเอกสารนโยบายฉบับเต็มได้ที่

https://www.satpcl.co.th/storage/content/sd/disclosure-documents/20230328-sat-policy-cyber-security-and-it-systems-th.pdf

การสร้างความเข้าใจและตระหนักรู้เกี่ยวกับศักยภาพขององค์กรผ่านกระบวนการประเมินขีดความสามารถในการบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

บริษัทฯ ได้เข้าร่วมโครงการประเมินระดับความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทจดทะเบียน (Cyber Resilience Survey 2024) ซึ่งดำเนินการโดยตลาดหลักทรัพย์แห่งประเทศไทยในปี พ.ศ. 2567 รวมทั้งได้ดำเนินการประเมินในโครงการที่เกี่ยวข้องกับลูกค้ารายสำคัญ โดยอ้างอิงตามกรอบการประเมินมาตรฐานสากล NIST Cybersecurity Framework ทั้ง Version 1 และ Version 2 เพื่อให้ทราบถึงระดับขีดความสามารถในการบริหารจัดการความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและสามารถนำผลการประเมินดังกล่าว มาใช้ในการปรับปรุง นโยบายวางแผนดำเนินงาน และพัฒนาอย่างต่อเนื่อง เพื่อรักษาสถานะการเป็นบริษัทชั้นนำในอุตสาหกรรมเดียวกันอย่างยั่งยืน ภายใต้การบริหารจัดการทรัพยากร ที่มีประสิทธิภาพและเหมาะสม

การจัดทำแผนกลยุทธ์ และการปรับปรุงนโยบายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

บริษัทฯ ได้จัดทำแผนปฏิบัติการด้านการควบคุมดูแล ระบบเทคโนโลยีสารสนเทศ ควบคู่ไปกับการพัฒนาปรับปรุงกระบวนการ รักษาความมั่นคง ปลอดภัย ทางเทคโนโลยีสารสนเทศและการปกป้องข้อมูลโดยเพิ่มเติมแนวทาง ในการวิเคราะห์ข้อมูล และขยายขอบเขตการดำเนินการ ให้ครอบคลุมทุกกลุ่มบริษัทฯ รวมถึงบริษัทในเครือ เพื่อให้มั่นใจได้ว่าระบบยังคงมีมาตรฐานที่ เหมาะสม พร้อมทั้งจัดทำแผนป้องกัน และรับมือกับภัยคุกคามอย่างมีประสิทธิภาพ ดังนี้

Improvement

ทบทวนแผนงานความต่อเนื่องทางธุรกิจ (BCP)

Supply Chain Risk Management

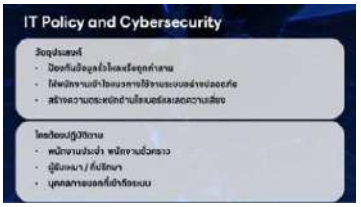
ดำเนินการร่วมทดสอบการซ้อมแผน (BCP) ร่วมกับคู่ค้าที่เกี่ยวข้อง

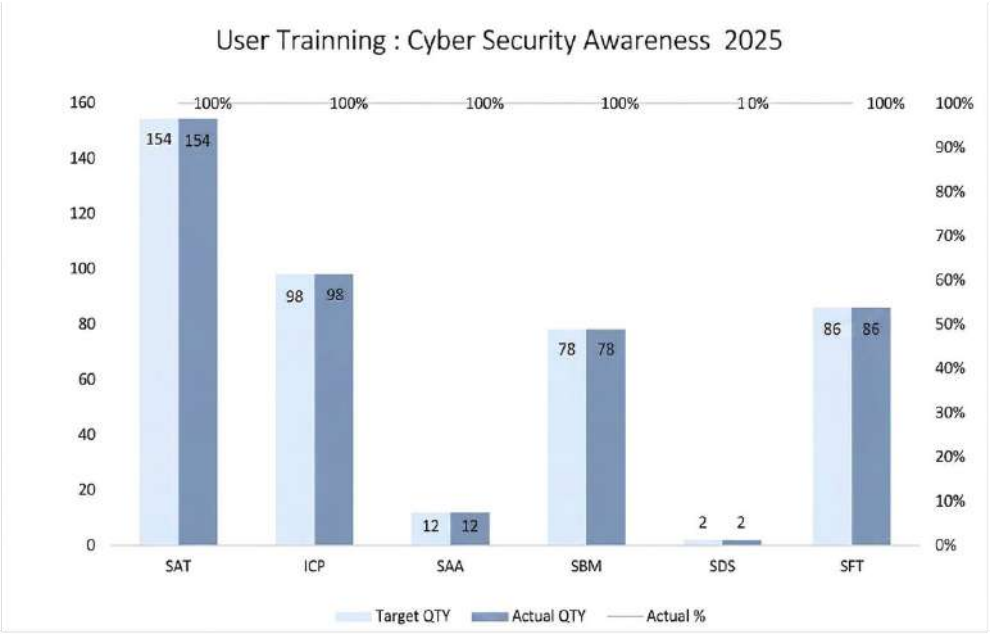
Analysis

ปรับปรุงขั้นตอนในการวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย ไซเบอร์ (Security Incident) เมื่อได้รับการแจ้งเตือน

การส่งเสริมความตระหนักรู้ถึงนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทฯ ให้ความสำคัญกับการพัฒนาความรู้ และความตระหนักรู้ของพนักงานเกี่ยวกับ การรักษาความมั่นคง ปลอดภัยไซเบอร์และการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย โดยจัดให้มีการอบรม การสื่อสาร และการเรียนรู้ผ่านระบบ Self Learning อย่างต่อเนื่อง ครอบคลุมพนักงานทุกระดับ รวมถึงพนักงานใหม่



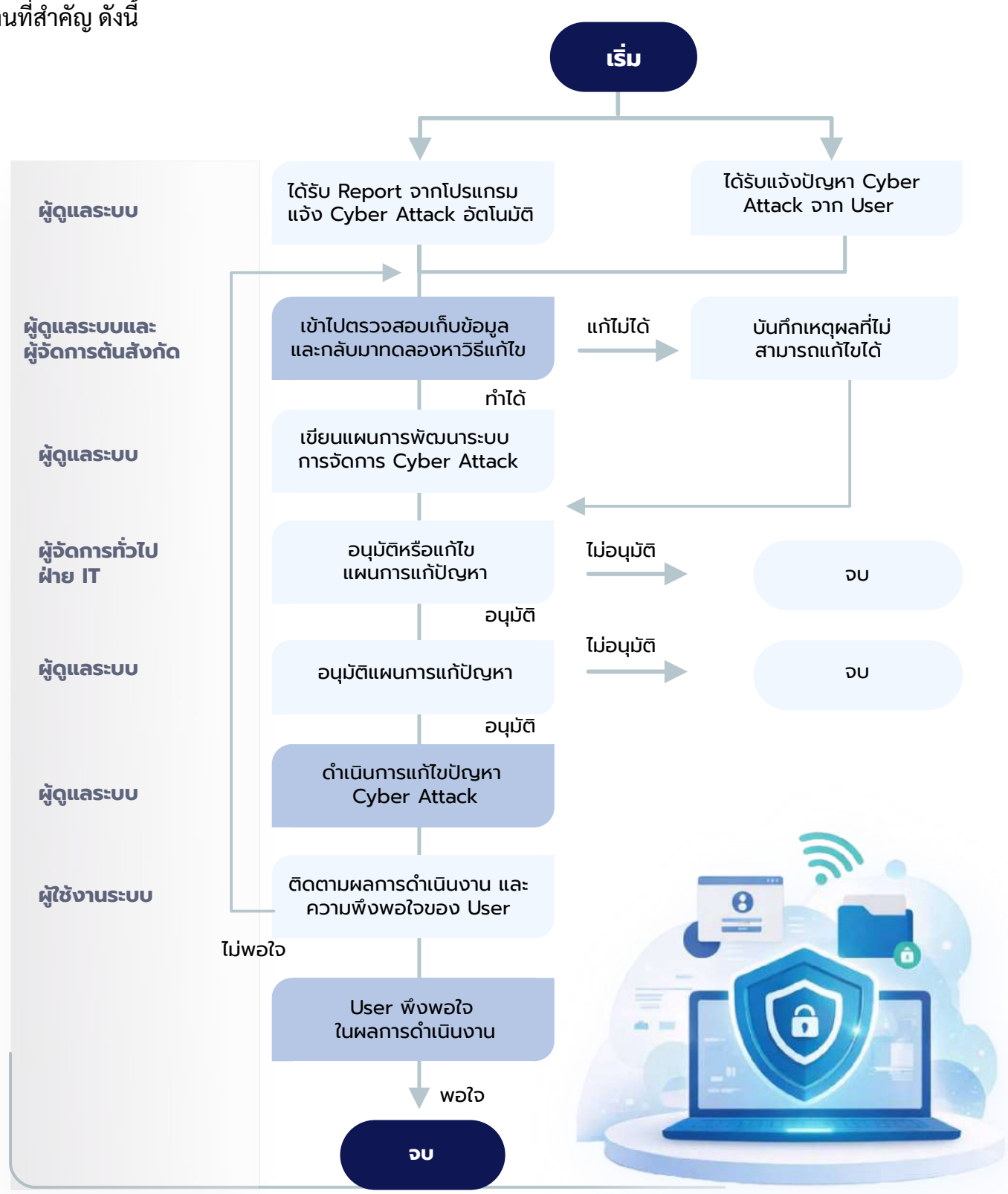


การติดตามและประเมินความเสี่ยงอย่างต่อเนื่อง

ปัจจุบันหน่วยงานเทคโนโลยีสารสนเทศได้ดำเนินการจัดทำ การประเมินความเสี่ยงอย่างสม่ำเสมอ โดยใช้ตัวชี้วัดความเสี่ยงหลัก (Key Risk Indicators: KRIs) เป็นเกณฑ์สำคัญในการประเมินและติดตามผล พร้อมรายงานผลการประเมินดังกล่าวไป ยังคณะกรรมการบริหารความเสี่ยงระดับองค์กร เป็นประจำทุกเดือน เพื่อให้มั่นใจได้ว่าการบริหารจัดการความเสี่ยงดำเนินไป อย่างมีประสิทธิภาพ สามารถลดผล กระทบที่อาจเกิดขึ้นกับองค์กร รวมถึงปกป้องโอกาสทางธุรกิจอย่างเหมาะสม

การรับข้อร้องเรียนและการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์และระบบเทคโนโลยีสารสนเทศ

บริษัทฯ ได้กำหนดช่องทางและระบบบริหารจัดการเพื่อรับข้อร้องเรียน และตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ทางเทคโนโลยีสารสนเทศอย่างเป็นระบบ โดยพนักงานสามารถแจ้งเหตุการณ์หรือข้อร้องเรียนผ่านช่องทางต่าง ๆ ได้ตลอด 24 ชั่วโมง อาทิ ระบบ Helpdesk ผ่านเว็บแอปพลิเคชันภายในองค์กร หรือทางอีเมล cybersecurity@somboon.co.th ทั้งนี้ มีขั้นตอนการดำเนินงานที่สำคัญ ดังนี้



ความสามารถในการป้องกันไวรัสคอมพิวเตอร์ขององค์กร ปี 2568

เดือน	จำนวนครั้งที่ถูกโจมตี	จำนวนครั้งที่ป้องกันได้	จำนวนครั้งการโจมตีที่สำเร็จ
มกราคม	573	573	0
กุมภาพันธ์	575	575	0
มีนาคม	620	620	0
เมษายน	569	569	0
พฤษภาคม	615	615	0
มิถุนายน	663	663	0
กรกฎาคม	744	744	0
สิงหาคม	608	608	0
กันยายน	654	654	0
ตุลาคม	659	659	0
พฤศจิกายน	649	649	0
ธันวาคม	916	916	0
รวม	7,845	7,845	0

รูปแบบการป้องกัน

จัดทำระบบสำรองเซิร์ฟเวอร์ที่ให้บริการตรวจสอบสิทธิ์และอนุญาตอุปกรณ์ที่เข้าถึงเครือข่ายภายใน Cloud

3. ป้องกันการโจมตีจากไวรัสคอมพิวเตอร์ได้ 100%

ผลการดำเนินงาน

1. โครงการอัพเกรโปรแกรม ERP-SAP ECC เป็น ERP-SAP S/4 HANA (เริ่มใช้งาน 2 พฤษภาคม 2568)

2. ป้องกันการโจมตีจากไวรัสคอมพิวเตอร์ได้ 100%

3. เปิดการใช้ งานระบบความปลอดภัย การยืนยันตัวตน 2 ขั้นตอน

4. ไม่มี (0) เหตุการณ์หยุดชะงักทางธุรกิจอันเนื่องมาจากความเสี่ยงด้านมั่นคงความปลอดภัยทางไซเบอร์

5. ได้รับการรับรองการทดสอบช่องโหว่ของระบบ SAP-ERP จากหน่วยงานทดสอบอิสระ

6. อบรมความมั่นคงความปลอดภัยทางไซเบอร์ และข้อมูลสารสนเทศ ให้กับพนักงานที่ใช้คอมพิวเตอร์ 100%