5.5 ความปลอดภัยของข้อมูลและระบบสารสนเทศ และการรักษาความปลอดภัยจากการโจมตีทางไซเบอร์

เทคโนโลยีสารสนเทศได้ช่วยให้ธุรกิจในปัจจุบันมีประสิทธิภาพในการบันทึกและประสานการทำงานในขั้นตอนต่าง ๆ ซึ่งทำให้กระบวนการทางธุรกิจเป็นไปได้อย่างรวดเร็วและราบรื่น แต่ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศได้กลายเป็นจุดสำคัญที่จะทำให้ธุรกิจหยุดชะงักและเกิดความเสียหายได้เมื่อมีการขัดข้องของระบบ อีกทั้งยังเป็นจุดที่สามารถถูกโจมตีเพื่อสร้างความเสียหาย หรือเพื่อขโมยและยึดครองข้อมูลหรือระบบได้ ซึ่งเรียกโดยรวมว่าภัยคุกคามทางไซเบอร์ บริษัทคำนึงถึงความปลอดภัยของข้อมูลผู้มีส่วนได้เสียทุกฝ่าย รวมถึงข้อมูลผู้บริโภค ลูกค้า พนักงาน ผู้ผลิตวัตถุดิบและภาคส่วนอื่น ๆ ที่เกี่ยวข้อง จึงได้จัดทำนโยบายความปลอดภัยข้อมูลด้านสารสนเทศ โดยจัดให้มีกลไกเพื่อป้องกันการเข้าถึงระบบและข้อมูลที่อาจทำให้เกิดความเสียหายทางธุรกิจ การเพิ่มความปลอดภัยของข้อมูลเทคโนโลยีสารสนเทศขององค์กร รวมถึงการวางแผนสำหรับเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้น

แนวทางการบริหารจัดการความเสี่ยงความปลอดภัยของข้อมูลและระบบสารสนเทศ

บริษัทมีแนวทางการจัดการและการบริหารความเสี่ยงในเรื่องความปลอดภัยทางด้านข้อมูลและระบบสารสนเทศตามแนวทาง NIST Cybersecurity Framework ของหน่วยงาน National Institute of Standards and Technology (NIST) ประเทศสหรัฐอเมริกา ซึ่ง NIST Cybersecurity Framework เป็นแนวคิดกรอบการทำงานเพื่อช่วยให้องค์กรสามารถวางแผนประเมิน ป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูต่อภัยคุกคามได้อย่างมีประสิทธิผล

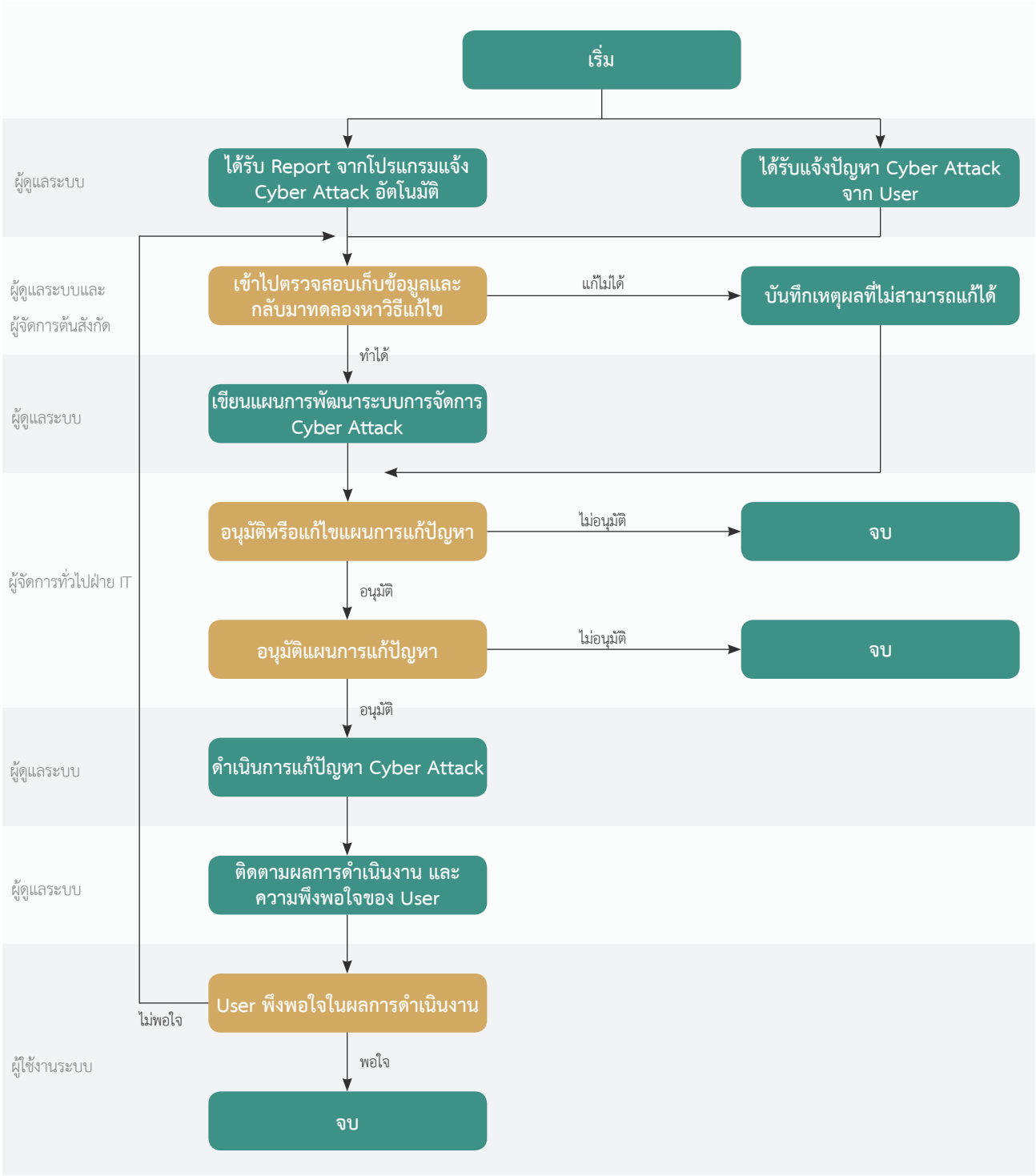
ผู้บริหารของบริษัทได้กำหนดกลยุทธ์ความปลอดภัยของระบบและข้อมูลสารสนเทศ การป้องกันการโจมตีทางไซเบอร์ และกระบวนการทั้งหมดให้สอดคล้องกับกฎหมายและแนวปฏิบัติด้านการกำกับดูแลกิจการที่ดีที่บริษัทจดทะเบียนพึงปฏิบัติ ซึ่งฝ่ายเทคโนโลยีสารสนเทศได้จัดทำกระบวนการ นโยบายและกฎระเบียบ สื่อสารให้พนักงานรับทราบผ่านคู่มือจริยธรรมธุรกิจ ข้อพึงปฏิบัติในการทำงาน (Code of conduct) พร้อมทั้งจัดหาเทคโนโลยีและเครื่องมือที่ใช้ในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟู อย่างครบถ้วนตามกลยุทธ์ความปลอดภัย

นอกจากนี้ หน่วยงานเทคโนโลยีสารสนเทศยังได้จัดทำการประเมินความเสี่ยง โดยมี Key Risk Indicator ที่สำคัญในการประเมิน เพื่อรายงานไปยังคณะกรรมการความเสี่ยงระดับองค์กรทุกเดือน รายงานการกำกับดูแลด้านความปลอดภัยของสารสนเทศและไซเบอร์ เพื่อให้มั่นใจว่าจะสามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ และลดผลกระทบที่อาจเกิดขึ้นกับองค์กรและโอกาสทางธุรกิจ

หลักปฏิบัติในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

บริษัทได้ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัว (Privacy Right) ที่ต้องได้รับการคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย และหลักปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Right) ซึ่งบุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น รวมถึงเพื่อสนับสนุนและเคารพการปกป้องมนุษยชนตามที่ประกาศใช้ในระดับสากลตามหลักการของข้อตกลงโลกแห่งสหประชาชาติ (UN Global Compact) รวมถึงกฎหมายที่ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล บริษัทได้จัดทำและประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคลตั้งแต่วันที่ 18 พฤษภาคม 2564

ระบบรับข้อร้องเรียนและตอบสนองเหตุการณ์ด้านความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ



บริษัทจัดให้มีระบบจัดการรับข้อร้องเรียนด้านความปลอดภัยของเทคโนโลยีสารสนเทศผ่านทางระบบเว็บแอปพลิเคชัน อีเมล และโทรศัพท์ โดยพนักงานสามารถใช้ช่องทางโทรศัพท์หรืออีเมลไปยังผู้รับเรื่องได้ตลอด 24 ชม. โดยใช้ทาง helpdesk เว็บแอปพลิเคชันภายในของบริษัท หรือ อีเมล cybersecurity@somboon.co.th

ระบบรับข้อร้องเรียนและตอบสนองเหตุการณ์ด้านความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ

ผลการดำเนินงานด้านความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ ปี 2564

ความสามารถในการป้องกันไวรัสคอมพิวเตอร์ขององค์กรปี พ.ศ. 2564			
เดือน	จำนวนครั้งที่ถูกโจมตี	จำนวนครั้งที่ป้องกันได้	จำนวนครั้งการโจมตีที่สำเร็จ
มกราคม	274	274	0
กุมภาพันธ์	309	309	0
มีนาคม	283	283	0
เมษายน	154	154	0
พฤษภาคม	515	515	0
มิถุนายน	284	284	0
กรกฎาคม	379	379	0
สิงหาคม	376	376	0
กันยายน	470	470	0
ตุลาคม	774	774	0
พฤศจิกายน	504	504	0
ธันวาคม	829	829	0
รวม	**5,151**	**5,151**	**0**

ป้องกันการโจมตีจากไวรัสคอมพิวเตอร์ได้ **100%**

ไม่มี **(0)** เหตุการณ์หยุดชะงักทางธุรกิจอันเนื่องมาจากความเสี่ยงด้านเทคโนโลยีสารสนเทศ