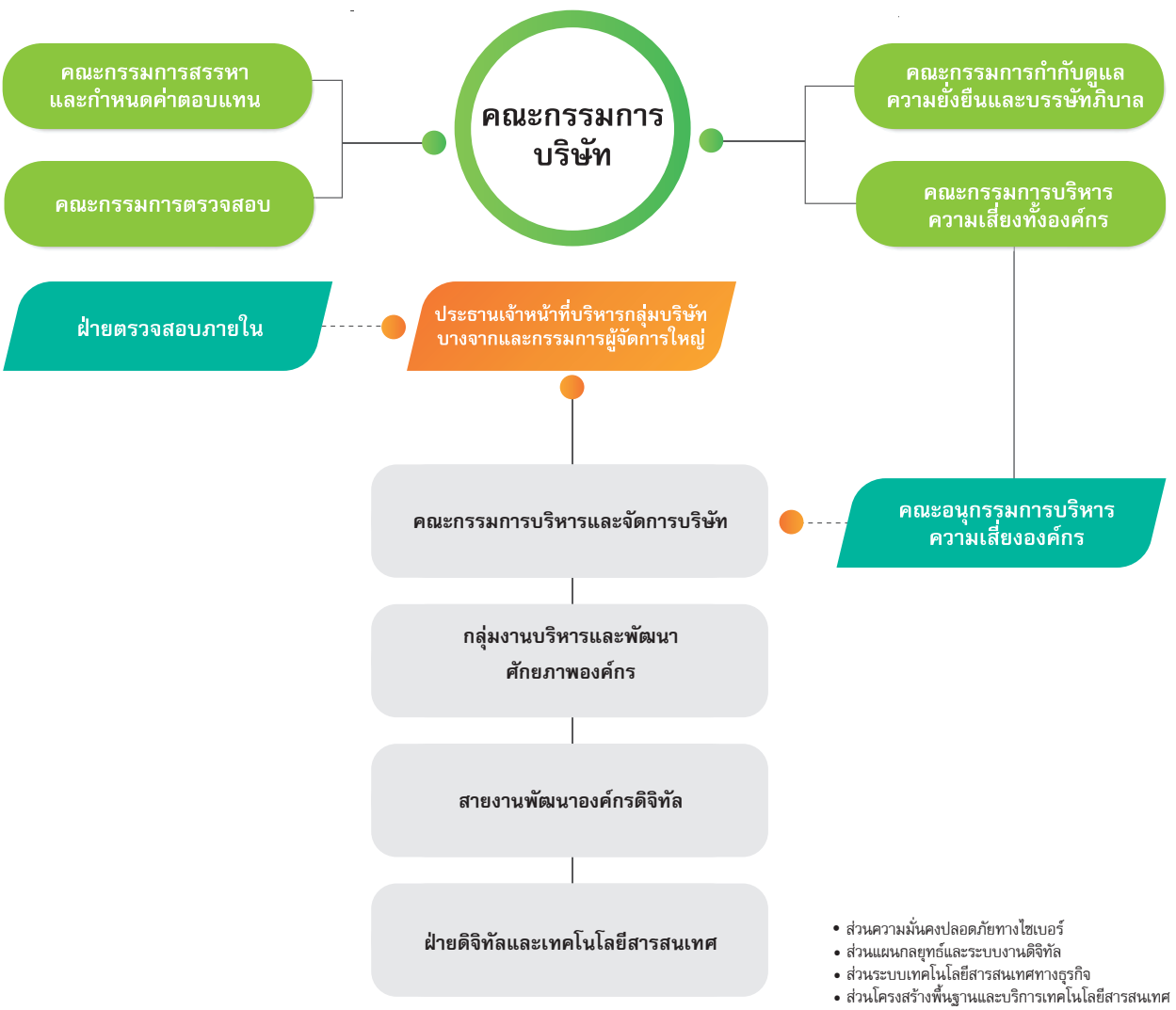
การนำเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในการพัฒนาธุรกิจ

ความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นประเด็นสำคัญที่อาจก่อให้เกิดผลกระทบต่อผู้มีส่วนได้เสียทั้งภายในและภายนอก เช่น โอกาสในเกิดผลกระทบต่อความปลอดภัยในการดำเนินงาน กรณีระบบการทำงานล่ม รวมถึงโอกาสในการละเมิดข้อมูลส่วนบุคคลทั้งของพนักงาน คู่ค้า และลูกค้า

ดังนั้น บริษัทฯ จึงนำระบบเทคโนโลยีสารสนเทศซึ่งเป็นเครื่องมือสำคัญที่จะตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติ มีเครื่องมือ มีกรอบในการดำเนินการและมาตรฐานที่ใช้ดำเนินการที่ทันสมัย มีประสิทธิภาพ มีการบริหารจัดการความเสี่ยงและให้ความสำคัญกับระบบความปลอดภัยสอดคล้องตามมาตรฐานสากล และเป็นไปตามข้อกำหนดของรัฐ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้สามารถรองรับการขยายธุรกิจตามแผนยุทธศาสตร์องค์กร และป้องกันกรณีการละเมิดสิทธิของผู้มีส่วนได้เสียจากการใช้ข้อมูลส่วนบุคคลในทางที่ไม่ถูกต้อง

โครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์

โครงสร้างการบริหาร เพื่อการพัฒนาองค์กรด้วยเทคโนโลยีสารสนเทศ บริษัทฯ มีการจัดตั้งคณะทำงานและคณะกรรมการ รายงานต่อคณะอนุกรรมการและคณะกรรมการบริหารความเสี่ยงองค์กร (ERMC) โดยมีสายงานพัฒนาองค์กรดิจิทัล และฝ่ายดิจิทัลและเทคโนโลยีสารสนเทศดูแลบริหารงาน



ตั้งแต่ปี 2561 บริษัทฯ ได้ตั้งส่วนความมั่นคงปลอดภัยทางไซเบอร์ขึ้นเพื่อรับผิดชอบงานบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ และมีการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ได้สอดคล้องตามมาตรฐานสากล คือ ISO/IEC 27001:2013 ISO/IEC 27032:2012 ISO/IEC 27018:2019 และ NIST Cyber Security Framework

การบริหารระบบการจัดการความปลอดภัยของข้อมูลตามมาตรฐานสากล

- ISO/IEC 27001:2013 เป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS) บริษัทฯ ได้รับการรับรองต่อเนื่องมาตั้งแต่ปี 2555 มีการดำเนินการตามระบบนับตั้งแต่การประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัย ทำให้เกิดความยืดหยุ่นในการควบคุมหรือพัฒนาธุรกิจของบริษัทฯ
- ISO/IEC 27032:2012 ตั้งแต่ปี 2561 บริษัทฯ ได้รับการรับรองเพิ่มเติมจาก ISO 27001 เป็นต้นมา ซึ่งเน้นที่ Confidentiality, Integrity และ Availability ใน Cyberspace คือความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บริการ รวมไปถึงสิ่งที่จับต้องไม่ได้ (Virtual Assets) เช่น ชื่อเสียง แบรนด์ เป็นต้น
- ISO/IEC 27018:2012 ตั้งแต่ปี 2564 ซึ่งมุ่งเน้นการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสำหรับปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (Personal Identifiable Information) ในคลาวด์ของบริษัทฯ

การป้องกันภัยคุกคามต่อทรัพย์สิน ข้อมูลและระบบสารสนเทศ

บริษัทฯ ได้ดำเนินการตาม “นโยบายรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ” ซึ่งจะมีการดูแลอย่างครอบคลุมนับตั้งแต่

1. การประเมินความเสี่ยง คัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ จัดให้มีการทดสอบสภาพความพร้อมใช้ ระบบสำรองและซ้อมแผนรองรับแผนรองรับกรณีเกิดเหตุฉุกเฉินและแผนการบริหารความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ
2. การบริหารจัดการทรัพยากรด้านทรัพย์สินสารสนเทศ ต้องมีมาตรการควบคุมการใช้และรักษาทรัพย์สิน อุปกรณ์ให้สมบูรณ์พร้อมใช้และป้องกันการเข้าถึงทรัพย์สินหรือข้อมูลโดยไม่ได้รับอนุญาต
3. การจัดการข้อมูลและการรักษาความลับ บริษัทฯ มีมาตรการรักษาความปลอดภัย โดยมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ ตามลำดับความสำคัญ หรือลำดับชั้นความลับในการเข้าถึง การควบคุมการรับส่งข้อมูล รวมทั้งจัดให้มีการทำสัญญาเป็นลายลักษณ์อักษรในการรักษาความลับและไม่เปิดเผยข้อมูลของบริษัทฯ กับหน่วยงานภายนอก
4. การจัดให้มีการยืนยันตัวตนผู้ใช้งานหลายเงื่อนไข (Multi-Factor Authentication หรือ MFA) มีระบบป้องกันคอมพิวเตอร์ (Advance Endpoint Protection) การป้องกันการเข้าถึงเครือข่ายและออกแบบการตรวจสอบความปลอดภัยที่เข้มงวด ที่เรียกว่า Zero Trust มีระบบตรวจจับภัยคุกคาม (Advance Security Information And Event Management หรือ Advance SIEM) ที่มีความทันสมัย รวมทั้งระบบหลอกล่อผู้ไม่หวังดี (Deception Technology) ทำให้สามารถวิเคราะห์ตรวจจับภัยการโจมตีใหม่ๆ ในลักษณะต่างๆ รวมถึงซอฟต์แวร์เรียกค่าไถ่ และป้องกันพร้อมแจ้งเตือนที่รวดเร็วและแม่นยำ ช่วยให้ผู้ดูแลระบบตอบสนองได้อย่างมั่นใจต่อระบบสารสนเทศ ทั้งจากการบุกรุกผ่านระบบเครือข่ายและโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้กับข้อมูลของบริษัทฯ โดยบริษัทฯ จะมีการตรวจจับ ป้องกัน และการกู้คืน รวมทั้งการสร้างความตระหนักรู้แก่ผู้เกี่ยวข้อง รวมไปถึงการบริหารจัดการช่องโหว่ทางเทคนิค ซึ่งมีการดำเนินการดังนี้

- การทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศในระดับรุนแรงที่ส่งผลให้โครงสร้างพื้นฐานไม่สามารถให้บริการได้อย่างน้อยปีละครั้ง (Cyber Security Drill)
- จัดให้มีการทดสอบโดยจ้างผู้เชี่ยวชาญมาทดสอบเจาะระบบ (Penetration Test) กับระบบงานที่สำคัญเพื่อวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Impact for Business) โดยจะทดสอบอย่างน้อยทุกปีหรือเมื่อมีการเปลี่ยนแปลงระบบงานที่มีนัยสำคัญ
- การทำประเมิน Vulnerability Assessment ซึ่งเป็นการตรวจระบบปฏิบัติการ (OS) ซอฟต์แวร์ หรืออุปกรณ์ Network/Security ว่ามีช่องโหว่ใดบ้างและมีระดับความรุนแรงเท่าใด เพื่อประเมินความเสี่ยงว่ามีโอกาสถูกเจาะระบบจากผู้ไม่ประสงค์ดีมากน้อยเพียงใด และทำการแก้ไขเพื่อปิดช่องโหว่นั้น ทั้งก่อนใช้งานจริงและหลังการใช้งาน

การสื่อสารภายในองค์กรเพื่อสร้างความตระหนักรู้และเพิ่มประสิทธิภาพการใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลเทคโนโลยี (Internal Communication)

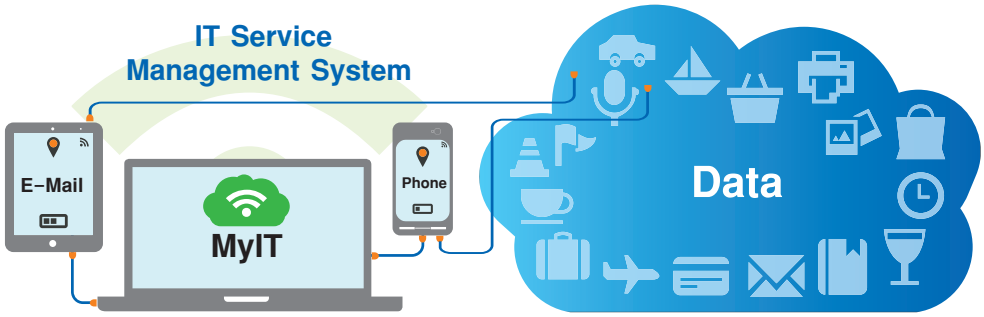
บริษัทฯ ให้ความสำคัญกับพนักงาน และผู้ปฏิบัติงานในการเพิ่มความรู้และทักษะในการใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลเทคโนโลยี โดยมีกิจกรรมดังนี้

- จัดให้มีการอบรมพนักงานที่เข้าใหม่ในรูปแบบเชิงปฏิบัติการพร้อมกับการวัดผลเกี่ยวกับความตระหนักถึงภัยทางไซเบอร์ และรวมถึงข้อกำหนดการใช้ระบบสารสนเทศขององค์กร และการปฏิบัติตามกฎหมาย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น
- การสื่อสารประเด็นความเสี่ยงทาง Cyber ที่เกิดขึ้นเพื่อให้ความรู้และสร้างความตระหนักต่อภัยทางไซเบอร์ (Security Awareness) โดยจะมีข่าวสารต่างๆ แจ้งพนักงานทางระบบสารสนเทศภายใน เช่น E-mail หรือ Pop Up เป็นประจำ
- Cybersecurity Awareness Improvement Program จะมีการดำเนินการอย่างสม่ำเสมอทุกปี โดยการให้ความรู้ความเข้าใจเกี่ยวกับภัยทาง E-mail และมีการวัดผลความเข้าใจด้วยการทำ Phishing Simulation คือ การจำลองอีเมลประเภทฟิชชิงส่งให้กลุ่มผู้ใช้งานภายในองค์กร เพื่อวัดระดับความเสี่ยงขององค์กรต่อภัยคุกคามประเภทฟิชชิง และวัดความตระหนักของผู้ใช้งานในการแยกแยะฟิชชิงอีเมล (Security Awareness Assessment) โดยมีการเก็บบันทึกผลการทดสอบและวิเคราะห์ข้อมูล เพื่อนำไปวางแผนและจัดอบรมพัฒนาความรู้ รวมถึงปรับปรุงมาตรการป้องกันภัยฟิชชิงขององค์กร ซึ่งปัจจุบันมีการวัดผลปีละ 4 ครั้ง ในสถานการณ์จำลองลักษณะต่างๆ พร้อมมีแบบประเมินความผิดพลาดจากการทดสอบให้กับพนักงานนั้นอย่างทันทีเพื่อให้เกิดการรับรู้และเกิดความตระหนักต่อไป (Rapid Improvement Program) และในการจำลองสถานการณ์ต่างๆ ทำให้ได้พบจุดอ่อนบางจุดและนำข้อมูลไปวิเคราะห์เพื่อปิดช่องโหว่ โดยการสื่อสารทำความเข้าใจกับพนักงาน เพื่อให้ได้เรียนรู้ ระมัดระวัง รู้จักวิธีจัดการกับภัยด้าน Phishing Mail ให้ดียิ่งขึ้น
- Cyber Security Response เป็นอีกแนวจัดการความปลอดภัยทางไซเบอร์หนึ่งที่บริษัทฯ ได้มีการดำเนินการ โดยจะมีการติดตามกรณีศึกษาทางด้านไซเบอร์ เพื่อนำมาอบรมให้ความรู้แนวทางแก่พนักงาน ผู้บริหาร รวมทั้งบริษัทในกลุ่มบางจาก ให้ระมัดระวังและมีความตระหนักในเรื่องการหลอกลวงผ่านทางอีเมลธุรกิจ (Business Email Compromise หรือ BEC) เช่น การส่งใบแจ้งหนี้ปลอม โดยจัดอบรมให้กับส่วนงาน/สายงานที่เกี่ยวข้อง เพื่อให้เกิดความตระหนักและระมัดระวัง โดยได้กำหนดแนวทางการควบคุมที่มีประสิทธิภาพ (Strictly Process Confirming) ดังนี้

1. การร้องขอ: ลงทะเบียนหรือเปลี่ยนแปลงข้อมูลสำคัญโดยเฉพาะข้อมูลบัญชีธนาคาร
2. ให้ใช้แบบฟอร์มที่กำหนดเพื่อยืนยันการเปลี่ยนแปลงข้อมูล โดยการเปลี่ยนแปลงข้อมูล ต้องลงนามในแบบฟอร์มที่กำหนดโดยผู้มีอำนาจของคู่ค้านั้นๆ
3. ต้องมีหลักฐานเอกสารที่เกี่ยวข้องกับการขอเปลี่ยนแปลง โดยดูความน่าเชื่อถือของเอกสารนั้นประกอบด้วย เช่น เอกสารที่ออกให้โดยหน่วยงานรัฐ
4. มีการยืนยันให้มั่นใจว่าผู้ร้องขอเปลี่ยนแปลงข้อมูลนั้นมาจากผู้ร้องขอจริง โดยให้ติดต่อเพื่อทางโทรศัพท์ที่เคยติดต่อ
5. ให้มีการเพิ่มขั้นตอนเหล่านี้ในกระบวนการทำงาน

มาตรการการดูแลรับมือกรณีเกิดการคุกคามทางไซเบอร์

บริษัทฯ มีการประเมินรูปแบบของภัยคุกคามปัจจุบันที่มีความเสี่ยงสูง จัดทำแผนและวิธีปฏิบัติสำหรับเหตุความไม่ปลอดภัย (Incident Response Plan) และมีการซ้อมอย่างน้อยปีละครั้งต่อแผนนั้น (Cyber Security Drill) ในการป้องกัน กู้คืน ได้อย่างมีประสิทธิภาพ รวดเร็ว เพื่อให้บริษัทฯ คงดำเนินธุรกิจได้ต่อเนื่อง และผลกระทบน้อยที่สุด โดยในการดำเนินงาน บริษัทฯ มีระบบสนับสนุนด้าน IT Service Management System เป็นระบบ BMC Remedy โดยมีชื่อภายในบริษัทฯ ว่า MyIT ซึ่งจะมีขั้นตอนปฏิบัติการจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ โดยพนักงานสามารถแจ้งมายังหน่วยงานได้ 3 ช่องทาง คือ



จำนวนเหตุการณ์ที่เกิดการละเมิดข้อมูล การเปิดเผยข้อมูลที่ไม่ตั้งใจและการรั่วไหลของข้อมูล

ปี	ปี 2560	ปี 2561	ปี 2562	ปี 2563	ปี 2564	ปี 2565
จำนวนครั้ง	0	0	0	0	0	0

จำนวนครั้งที่ข้อมูลลูกค้ารั่วไหลหรือถูกนำไปเปิดเผย/ใช้โดยไม่ได้รับอนุญาต

ปี	ปี 2560	ปี 2561	ปี 2562	ปี 2563	ปี 2564	ปี 2565
จำนวนครั้ง	0	0	0	0	0	0