CVC ลงทุนในสตาร์ทอัพโดยตรง โดยลงทุนไปแล้วกว่าร้อยละ 58 ของเงินงบลงทุนทั้งหมด ซึ่งมีทั้งการลงทุนแบบ Follow-on Investment และ Initial Investment และนอกจากการลงทุนแล้ว CVC ยังได้มีการวางแผนและศึกษาความเป็นไปได้ในการนำเอาเทคโนโลยีจากสตาร์ทอัพที่ CVC ลงทุนไปแล้วมาพัฒนาธุรกิจในกลุ่มธุรกิจของบางจาก รวมทั้งร่วมพัฒนาเทคโนโลยีกับสตาร์ทอัพที่ CVC ลงทุนไปด้วย เช่น การร่วมพัฒนามาตรฐานแบตเตอรี่กับ Winnonie ซึ่งเป็นสตาร์ทอัพที่นำนวัตกรรมพลังงานสีเขียวจากมอเตอร์ไซค์ไฟฟ้าช่วยยกระดับคุณภาพชีวิตผู้ประกอบอาชีพขับขี่รถจักรยานยนต์สาธารณะ

3. ด้านการบ่มเพาะธุรกิจ (Ecosystem and Incubation: E&I)

Ecosystem and Incubation (E&I) ภายใต้สถาบันนวัตกรรมและบ่มเพาะธุรกิจ (BiiC) จัดทำโครงการ “Wrong DI (Wrong-Deliver-Innovation) ผิดถูกไม่ว่า ขอให้กล้าส่งมอบนวัตกรรมของคุณ” ซึ่งเป็นเครื่องมือในการกระตุ้นให้เกิดระบบนิเวศในการสร้างสรรค์นวัตกรรมและก่อให้เกิดการแลกเปลี่ยนองค์ความรู้ของพนักงานภายในองค์กรและบริษัทในกลุ่ม โดยเริ่มจากการส่งเสริมให้พนักงานแชร์ความคิดที่เกี่ยวกับนวัตกรรมผ่านทางแพลตฟอร์มออนไลน์ และเสริมองค์ความรู้ผ่านการทำ Workshop ในด้านการสร้างไอเดียให้กลายเป็นธุรกิจนวัตกรรม รวมถึงให้การสนับสนุนในด้านการบ่มเพาะธุรกิจเพื่อเพิ่มศักยภาพในการขยายเชิงพาณิชย์ต่อไป โดยมีผลการดำเนินงานในโครงการต่อเนื่อง ได้แก่

- **โครงการปั๊มน้ำมันหยอดเหรียญอัจฉริยะ (กระทิง)** เริ่มก่อตั้งในปี 2564 โดยนำนวัตกรรมและการให้บริการด้านการเงินและ Lifestyle เช่น การเติมเงิน Wallet เข้าสู่ชุมชนห่างไกลสถานีบริการน้ำมัน เมื่อโครงการได้รับการบ่มเพาะธุรกิจเพื่อขยายผลในเชิงพาณิชย์ โดยในปัจจุบันกระทิงมีจำนวนตู้หยอดเหรียญอัจฉริยะ 110 ตู้ จำนวนสมาชิกมากกว่า 4,000 ราย ครอบคลุม 50 หมู่บ้าน 5 จังหวัด สร้างรายได้ทั้งสิ้น 1.2 ล้านบาทในปี 2565 และ 1.3 ล้านบาทในปี 2566
- **โครงการวิจัยเพาะเลี้ยงสาหร่ายเพื่อการผลิตสารสกัดมูลค่าสูง** ร่วมกับหน่วยงานวิจัยและพัฒนาในการระดมทุนเพื่อขยายกำลังการผลิตรองรับตลาดในประเทศ โดยมีเป้าหมายเป็นศูนย์กลางการเพาะเลี้ยงและสกัดสารสำคัญที่มีมูลค่าสูงจากสาหร่ายในตลาดเอเชียตะวันออกเฉียงใต้ ปัจจุบันมีผลิตภัณฑ์เสริมอาหารและเครื่องสำอาง ภายใต้แบรนด์ Asta.A ผลิตจากสารสำคัญจากสาหร่ายสีแดง (แอสตาแซนติน) เป็นสารต้านอนุมูลอิสระประสิทธิภาพสูงกว่าวิตามินซี 500 เท่า โดยมีแผนต่อยอดผลิตภัณฑ์ไปยังกลุ่มอาหารคนและอาหารสัตว์ต่อไป

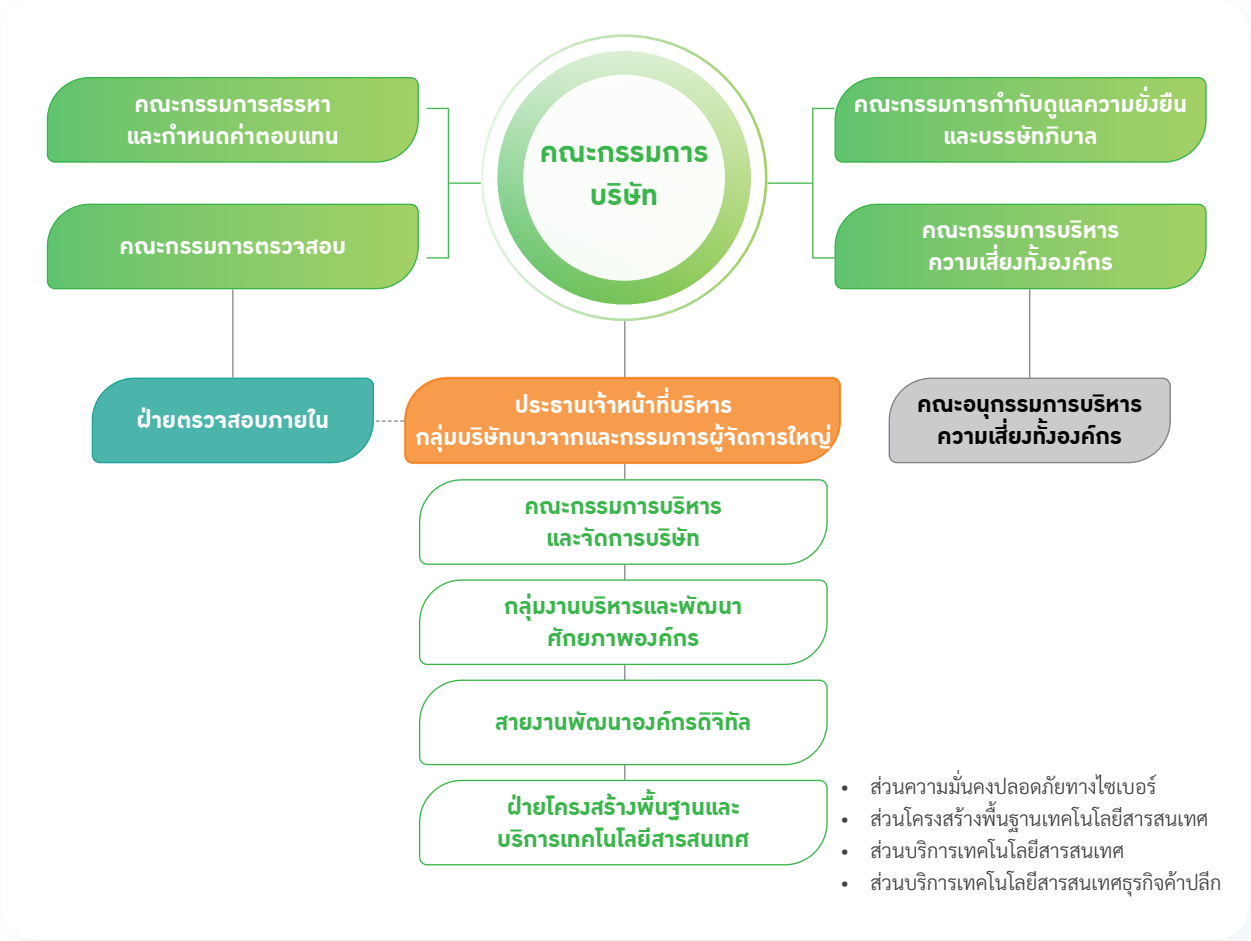
บริษัทฯ สื่อสารและรับฟังความคิดเห็นของผู้มีส่วนได้เสียที่เกี่ยวข้องในด้านนวัตกรรมอย่างต่อเนื่องผ่านช่องทางต่างๆ ได้แก่ การสำรวจความคิดเห็นของผู้มีส่วนได้เสีย (Stakeholder Engagement Survey) ต่อประเด็นต่างๆ เพื่อนำมาพัฒนาและปรับปรุงรูปแบบธุรกิจและการบ่มเพาะนวัตกรรมอื่นๆ

การนำเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในการพัฒนาธุรกิจ

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

โครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์

โครงสร้างการบริหารเพื่อการพัฒนาองค์กรด้วยเทคโนโลยีสารสนเทศ รวมถึงบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นไปตามมาตรฐานสากล บริษัทฯ คณะกรรมการด้านบริหารจัดการ คณะทำงาน และคณะผู้ตรวจสอบภายใน ด้านความมั่นคงปลอดภัยสารสนเทศ ISO 27001 รายงานต่อคณะอนุกรรมการและคณะกรรมการบริหารความเสี่ยงองค์กร (ERMC) โดยมีสายงานพัฒนาองค์กรดิจิทัล และฝ่ายดิจิทัลและเทคโนโลยีสารสนเทศ ดูแลบริหารงาน ซึ่งผู้บริหารระดับรองกรรมการผู้จัดการใหญ่กลุ่มงานบริหารและพัฒนาศักยภาพองค์กร ดำรงตำแหน่งประธานกรรมการคณะกรรมการทำหน้าที่เป็นตำแหน่งผู้บริหารระดับสูงทางด้านการรักษาความปลอดภัยให้กับโครงสร้างเครือข่ายและความปลอดภัยข้อมูลสารสนเทศ (Chief Information Security Officer: CISO) ซึ่งเป็นผู้มีความรู้ความสามารถด้าน Information Technology และ Information Security ในระดับบริหารจัดการ



ตั้งแต่ปี 2561 บริษัทฯ ได้ตั้งส่วนความมั่นคงปลอดภัยทางไซเบอร์ขึ้นเพื่อรับผิดชอบงานบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ และมีการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ได้สอดคล้องตามมาตรฐานสากล คือ ISO/IEC 27001 : 2022, ISO/IEC 27032 : 2012, ISO/IEC 27018 : 2019 และ NIST Cyber Security Framework

การบริหารระบบการจัดการความปลอดภัยของข้อมูลตามมาตรฐานสากล

- ISO/IEC 27001 : 2022 เป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS) บริษัทฯ ได้รับการรับรองต่อเนื่องมาตั้งแต่ปี 2555 Version 2013 และยังสอดคล้องกับ Version ล่าสุด 2022 ในปี 2566 คือมีการดำเนินการตามระบบนับตั้งแต่การประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัย ทำให้เกิดความยืดหยุ่นในการควบคุมหรือพัฒนาธุรกิจของบริษัทฯ
- ISO/IEC 27032 : 2012 ตั้งแต่ปี 2561 บริษัทฯ ได้รับการรับรองเพิ่มเติมจาก ISO 27001 เป็นต้นมา ซึ่งเน้นที่ Confidentiality, Integrity และ Availability ใน Cyberspace คือ ความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ 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 จัดให้มีการทดสอบสภาพความพร้อมใช้ระบบสำรองและซ้อมแผนรองรับแผนรองรับกรณีเกิดเหตุฉุกเฉินและแผนการบริหารความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ มีการติดตามและรายงานไปยังส่วนบริหารจัดการความเสี่ยงขององค์กรเป็นประจำทุกไตรมาส ซึ่งจะนำพิจารณาสู่การรายงานคณะกรรมการบริษัท ด้านบริหารจัดการความเสี่ยงต่อไป
2. การบริหารจัดการทรัพยากรด้านทรัพย์สินสารสนเทศ ต้องมีมาตรการควบคุมการใช้และรักษาทรัพย์สินอุปกรณ์ให้สมบูรณ์พร้อมใช้ และป้องกันการเข้าถึงทรัพย์สินหรือข้อมูลโดยไม่ได้รับอนุญาต
3. การจัดการข้อมูลและการรักษาความลับ บริษัทฯ มีมาตรการรักษาความปลอดภัย โดยมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทตามลำดับความสำคัญ หรือลำดับชั้นความลับในการเข้าถึง การควบคุมการรับส่งข้อมูล รวมทั้งจัดให้มีการทำสัญญาเป็นลายลักษณ์อักษรในการรักษาความลับและไม่เปิดเผยข้อมูลของบริษัทฯ กับหน่วยงานภายนอก
4. การจัดให้มีการยืนยันตัวตนผู้ใช้งานหลายเงื่อนไข (Multi-factor Authentication: MFA) มีระบบป้องกันคอมพิวเตอร์ (Advance Endpoint Protection) ซึ่งมีความสามารถตรวจสอบ ตรวจจับ และการตอบสนองต่อภัยคุกคามไซเบอร์ให้แก่ระบบคอมพิวเตอร์ที่เรียกว่า Endpoint Detection and Response หรือ EDR มีระบบป้องกันการเข้าถึงเครือข่ายและออกแบบการตรวจสอบความปลอดภัยที่เข้มงวด ที่เรียกว่า Zero Trust มีระบบตรวจจับภัยคุกคาม (Advance Security Information and Event Management หรือ Advance SIEM) ที่มีความทันสมัย พร้อมระบบหลอกล่อผู้ไม่หวังดี (Deception Technology) เพื่อการตรวจจับที่รวดเร็วและแม่นยำยิ่งขึ้น มีระบบที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threat) จากแหล่งข่าวทั่วโลกหรือที่เรียกว่า Threat Intelligence ที่จะแจ้งเตือนผ่านระบบตรวจจับภัยคุกคามทำให้สามารถในการวิเคราะห์ตรวจจับภัยการโจมตีใหม่ๆ ในลักษณะต่างๆ รวมถึงซอฟต์แวร์เรียกค่าไถ่ และป้องกันพร้อมแจ้งเตือนที่รวดเร็วและแม่นยำ รวมทั้งการจัดจ้างผู้ให้บริการบริหารจัดการความปลอดภัย (Managed Security Service Provider) เพื่อเสริมความเข้มข้นในการเฝ้าระวังในส่วนของระบบที่สำคัญตลอด 24 ชั่วโมง พร้อมการติดตามข่าวสารภัยและรายงานเป็น

ประจำอย่างน้อยทุกเดือน มีระบบสำรองข้อมูลที่จัดเก็บไว้อย่างปลอดภัยพร้อมระบบป้องกันซอฟต์แวร์เรียกค่าไถ่ และมีความสามารถกู้คืนระบบได้รวดเร็ว การดำเนินการดังกล่าวช่วยให้ผู้ดูแลระบบตอบสนองได้อย่างมั่นใจต่อระบบสารสนเทศ ทั้งจากการบุกรุกผ่านระบบเครือข่ายและโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้กับข้อมูลของบริษัท โดยบริษัทฯ จะมีการตรวจจับ ป้องกันและการกู้คืน รวมทั้งการสร้างความตระหนักรู้แก่ผู้เกี่ยวข้อง รวมไปถึงการบริหารจัดการช่องโหว่ทางเทคนิค ซึ่งมีการดำเนินการ ดังนี้

- 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
- มีการประเมินผู้ให้บริการภายนอกที่ให้บริการประมวลผลข้อมูลเกี่ยวกับบุคคล เพื่อให้เกิดความมั่นใจในการดูแลข้อมูลสอดคล้องเป็นอย่างน้อยตามข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การสื่อสารภายในองค์กรเพื่อสร้างความตระหนักรู้และเพิ่มประสิทธิภาพการใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลเทคโนโลยี (Internal Communication)

บริษัทฯ ให้ความสำคัญกับพนักงานและผู้ปฏิบัติงานในการเพิ่มความรู้และทักษะในการใช้งานระบบเทคโนโลยีสารสนเทศและดิจิทัลเทคโนโลยี โดยมีกิจกรรมดังนี้

- จัดให้มีการอบรมพนักงานที่เข้าใหม่ในรูปแบบเชิงปฏิบัติการ พร้อมกับการวัดผลเกี่ยวกับความตระหนักถึงภัยทางไซเบอร์ และรวมถึงข้อกำหนดการใช้ระบบสารสนเทศขององค์กร และการปฏิบัติตามกฎหมาย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น
- การสื่อสารประเด็นความเสี่ยงทางไซเบอร์ ที่เกิดขึ้นเพื่อให้ความรู้และสร้างความตระหนักต่อภัยทางไซเบอร์ (Security Awareness) โดยจะมีข่าวสารต่างๆ แจ้งพนักงานทางระบบสารสนเทศภายใน เช่น Email หรือ Popup เป็นประจำ
- Cybersecurity Awareness Improvement Program จะมีการดำเนินการอย่างสม่ำเสมอทุกปี โดยการให้ความรู้ความเข้าใจถึงเกี่ยวกับภัยทาง Email และมีการวัดผลความเข้าใจด้วยการทำ Phishing Simulation คือ การจำลองอีเมลประเภทฟิชชิงส่งให้กลุ่มผู้ใช้งานภายในองค์กร เพื่อวัดระดับความเสี่ยงขององค์กรต่อภัยคุกคามประเภทฟิชชิง และวัดความตระหนักของผู้ใช้งานในการแยกแยะฟิชชิงอีเมล (Security Awareness Assessment) โดยมีการเก็บบันทึกผลการทดสอบและวิเคราะห์ข้อมูล เพื่อนำไปวางแผนและจัดอบรมพัฒนาความรู้ รวมถึงปรับปรุงมาตรการป้องกันภัยฟิชชิงขององค์กร ซึ่งปัจจุบันมีการวัดผลปีละ 4 ครั้ง ในสถานการณ์จำลองลักษณะต่างๆ พร้อมมีแบบประเมินความผิดพลาดจากการทดสอบให้กับพนักงานนั้นอย่างทันที เพื่อให้เกิดการรับรู้และเกิดความตระหนักต่อไป (Rapid Improvement Program) และในการจำลองสถานการณ์ต่างๆ ทำให้ได้พบจุดอ่อนบางจุดและนำข้อมูลไปวิเคราะห์เพื่อปิดช่องโหว่ โดยการสื่อสารทำความเข้าใจกับพนักงานเพื่อให้ได้เรียนรู้ ระมัดระวัง รู้จักวิธีจัดการกับภัยด้าน Phishing Mail ให้ดียิ่งขึ้น

- Cyber Security Response เป็นอีกแนวจัดการความปลอดภัยทางไซเบอร์หนึ่งที่บริษัทฯ ได้มีการดำเนินการโดยจะมีการติดตามกรณีศึกษาทางด้านไซเบอร์ เพื่อนำมาอบรมให้ความรู้แนวทางแก่พนักงาน ผู้บริหาร รวมทั้งกลุ่มบริษัทบางจาก ให้ระมัดระวังและมีความตระหนักในเรื่องการหลอกลวงผ่านทางอีเมล์ธุรกิจ (Business Email Compromise: BEC) เช่น การส่งใบแจ้งหนี้ปลอม โดยจัดอบรมให้กับส่วนงาน/สายงานที่เกี่ยวข้อง เพื่อให้เกิดความตระหนักและระมัดระวัง โดยได้กำหนดแนวทางการควบคุมที่มีประสิทธิภาพ (Strictly Process Confirming) ดังนี้

1. การร้องขอลงทะเบียนหรือเปลี่ยนแปลงข้อมูลสำคัญ โดยเฉพาะข้อมูลบัญชีธนาคาร
2. ให้ใช้แบบฟอร์มที่กำหนดเพื่อยืนยันการเปลี่ยนแปลงข้อมูลโดยการเปลี่ยนแปลงข้อมูลต้องลงนามในแบบฟอร์มที่กำหนดโดยผู้มีอำนาจของคู่ค้านั้นๆ
3. ต้องมีหลักฐานเอกสารที่เกี่ยวข้องกับการขอเปลี่ยนแปลงโดยดูความน่าเชื่อถือของเอกสารนั้นประกอบด้วย เช่น เอกสารที่ออกให้โดยหน่วยงานรัฐ
4. มีการยืนยันให้มั่นใจว่าผู้ร้องขอเปลี่ยนแปลงข้อมูลนั้นมาจากผู้ร้องขอจริงโดยให้ติดต่อเพื่อทางโทรศัพท์ที่เคยติดต่อ
5. ให้มีการเพิ่มขั้นตอนเหล่านี้ในกระบวนการทำงาน

มาตรการการดูแลรับมือกรณีเกิดการคุกคามทางไซเบอร์

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

จำนวนเหตุการณ์ที่เกิดการละเมิดข้อมูล การเปิดเผยข้อมูลที่ไม่ตั้งใจและการรั่วไหลของข้อมูล

ปี 2562 **0** ครั้ง
ปี 2563 **0** ครั้ง
ปี 2564 **0** ครั้ง
ปี 2565 **0** ครั้ง
ปี 2566 **0** ครั้ง

จำนวนครั้งที่ข้อมูลลูกค้ารั่วไหลหรือถูกนำไปเปิดเผย/ใช้โดยไม่ได้รับอนุญาต

ปี 2562 **0** ครั้ง
ปี 2563 **0** ครั้ง
ปี 2564 **0** ครั้ง
ปี 2565 **0** ครั้ง
ปี 2566 **0** ครั้ง