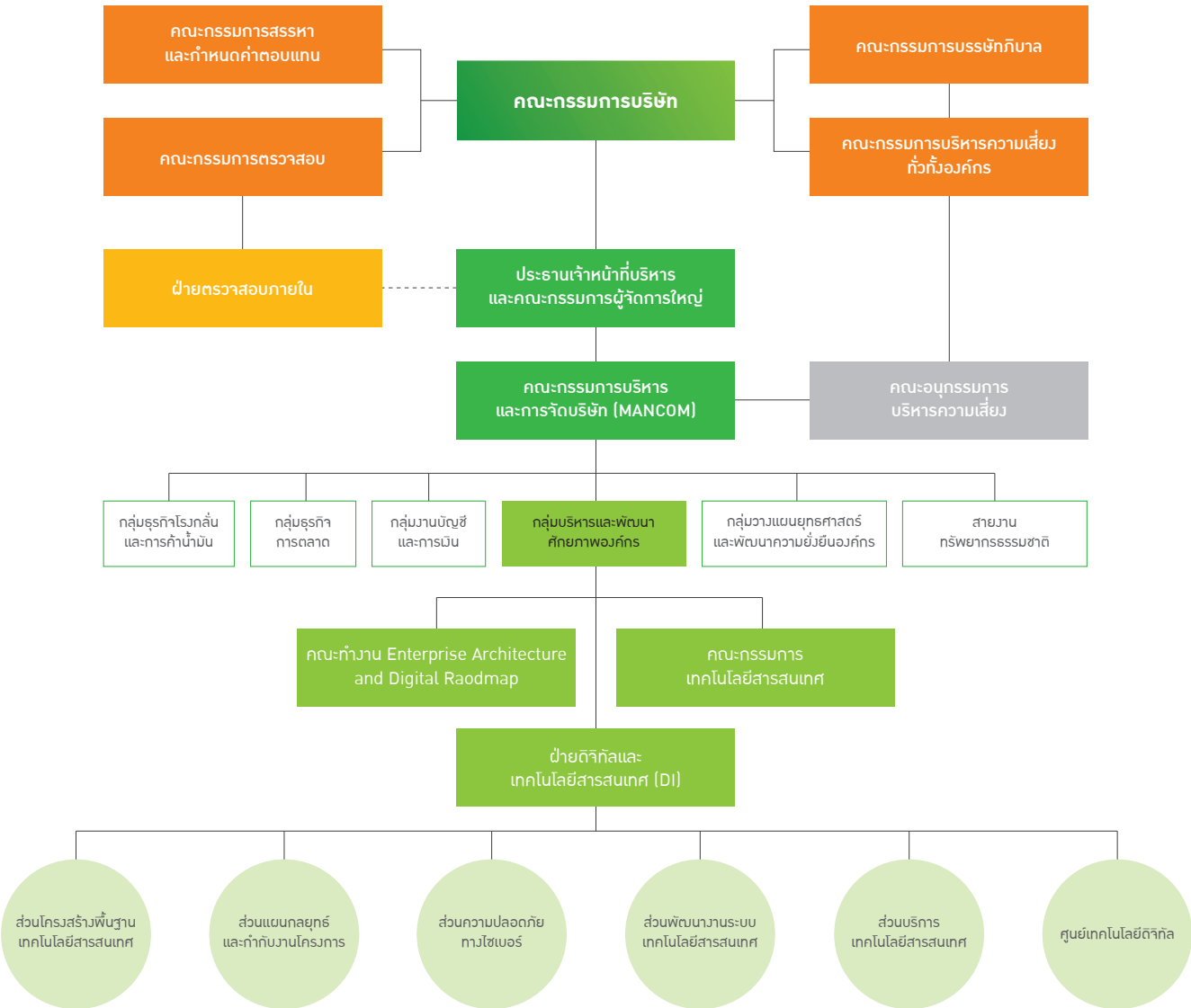


การนำเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในการพัฒนาธุรกิจ

บริษัทฯ” ส่งเสริมการนำระบบเทคโนโลยีสารสนเทศซึ่งเป็นเครื่องมือสำคัญที่จะตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติ มีเครื่องมือ มีมาตรฐานที่ใช้ดำเนินการที่ทันสมัย มีประสิทธิภาพ และให้ความสำคัญกับระบบความปลอดภัยสอดคล้องตามมาตรฐานสากล เพื่อให้สามารถรองรับการขยายธุรกิจ ตามแผนยุทธศาสตร์องค์กร

- ❏ **โครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์**
บริษัทฯ มีการจัดตั้งคณะทำงานEnterprise Architecture and Digital Roadmapเป็นที่ปรึกษาให้คำแนะนำด้านนโยบาย กลยุทธ์ รวมถึงสถาปัตยกรรมด้านเทคโนโลยีที่เหมาะสมกับความต้องการของกลุ่มธุรกิจ ทำงานร่วมกับคณะกรรมการเทคโนโลยี



สารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ในการพัฒนาระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับการขยายตัวของธุรกิจ โดยมีรองกรรมการผู้จัดการใหญ่กลุ่มงานบริหารและพัฒนาศักยภาพองค์กร เป็นประธาน และมีฝ่ายดิจิทัลและเทคโนโลยีสารสนเทศดูแลบริหารงาน ซึ่งจะมีการรายงานต่อคณะกรรมการบริหารและจัดการบริษัท ร่วมถึงการรายงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์กับคณะอนุกรรมการและคณะกรรมการบริหารความเสี่ยงทั่วองค์กร

ในปี 2561 บริษัทฯ ได้ตั้งส่วนความปลอดภัยทางไซเบอร์ขึ้นเพื่อรับผิดชอบงานบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ ตามมาตรฐานสากลการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ ISO/IES 27001: 2013 ISO/IES 27032: 2012 และ NIST Cyber Security Framework

การบริหารระบบการจัดการความปลอดภัยของข้อมูลตามมาตรฐานสากล

- **ISO/IES27001:2013** เป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems : ISMS) บริษัท ได้รับการรับรองต่อเนื่องมาตั้งแต่ปี 2012 มีการดำเนินการตามระบบนับตั้งแต่การประเมินความเสี่ยงการออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัยทำให้เกิดความยืดหยุ่นในการควบคุมหรือพัฒนาธุรกิจของบริษัท
- **ISO/IES 27032: 2012** ในปี 2561 บริษัท ได้รับการรับรอง ISO/IES 27032: 2012 เพิ่มนอกจาก ISO 27001 ซึ่งเน้นที่ Confidentiality, Integrity และ Availability ใน Cyberspace คือความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ เช่น อุปกรณ์ซอฟต์แวร์ ข้อมูล บริการรวมไปถึงสิ่งที่จับต้องไม่ได้ (Virtual Assets) เช่น ชื่อเสียง แบนด์ เป็นต้น



- การป้องกันภัยคุกคามต่อทรัพย์สิน ข้อมูลและระบบสารสนเทศ บริษัท ได้ดำเนินการตาม “นโยบายรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ” ซึ่งจะมีการดูแลอย่างครอบคลุมนับตั้งแต่

1. การประเมินความเสี่ยง คัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์จัดให้มีการทดสอบสภาพความพร้อมใช้ ระบบสำรองและซ่อมแผนรองรับแผนรองรับกรณีเกิดเหตุฉุกเฉินและแผนการบริหารความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ
2. การบริหารจัดการทรัพยากรด้านทรัพย์สินสารสนเทศ ต้องมีมาตรการ ควบคุมการใช้และรักษาทรัพย์สินอุปกรณ์ให้สมบูรณ์พร้อมใช้และป้องกันการเข้าถึงทรัพย์สินหรือข้อมูลโดยไม่ได้รับอนุญาตทั้งในการใช้งานปกติและการใช้งานนอกสถานที่
3. การจัดการข้อมูลและการรักษาความลับบริษัท มีมาตรการรักษาความปลอดภัยโดยมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทตามลำดับความสำคัญ หรือลำดับชั้น

ความลับในการเข้าถึงการควบคุมการรับส่ง Electronic Messaging เช่น email หรือ EDI รวมทั้งจัดให้มีการทำสัญญาเป็นลายลักษณ์อักษรในการรักษาความลับและไม่เปิดเผยข้อมูลของบริษัท กับหน่วยงานภายนอก

4. การจัดให้มีการป้องกันภัยคุกคามต่อระบบสารสนเทศทั้งจากการบุกรุกผ่านระบบเครือข่ายและโปรแกรม ที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้กับข้อมูลของบริษัท โดยบริษัท จะมีการตรวจจับ ป้องกัน และการกู้คืน รวมทั้งการสร้างความตระหนักรู้แก่ผู้เกี่ยวข้อง รวมไปถึงการบริหารจัดการช่องโหว่ทางเทคนิค ซึ่งมีการดำเนินการดังนี้

- การทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง ซึ่งครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)
- จัดให้มีการทดสอบโดยจ้างผู้เชี่ยวชาญมาทดสอบเจาะระบบ (Penetration Test) กับระบบงานที่สำคัญเพื่อวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Impact for Business) โดยจะทดสอบอย่างน้อยทุก 3 ปีหรือเมื่อมีการเปลี่ยนแปลงระบบงานที่มีนัยสำคัญ สำหรับระบบงานอื่น ๆ จะทดสอบทุก 5 ปี
- การทำประเมิน Vulnerability Assessment ซึ่งเป็นการตรวจระบบปฏิบัติการ (OS) ซอฟต์แวร์ หรืออุปกรณ์ Network/Security ว่ามีช่องโหว่ใดบ้างและมีระดับความรุนแรงเท่าใด เพื่อให้ผู้ดูแลระบบประเมินความเสี่ยงว่ามีโอกาสถูกเจาะระบบจากผู้ไม่ประสงค์ดีมากน้อยเพียงใด และทำการแก้ไขเพื่อปิดช่องโหว่นั้น



การสื่อสารภายในองค์กรเพื่อสร้างความตระหนักรู้และเพิ่มประสิทธิภาพการใช้งานระบบเทคโนโลยีสารสนเทศ

รวมทั้งดิจิทัลเทคโนโลยี (Internal Communication) ที่บริษัทฯ นำมาใช้เพิ่มขึ้นอย่างต่อเนื่องทั้งในด้านการบริหารงานภายในองค์กร และธุรกิจต่างๆ บริษัทฯ จึงให้ความสำคัญกับพนักงาน และผู้ปฏิบัติงานโดยจัดให้มีการสื่อสารและอบรมดังนี้

- จัดให้มีการอบรมพนักงานที่เข้าใหม่ รวมถึงผู้บริหารและพนักงานเกี่ยวกับนโยบาย ข้อกฎหมายด้าน IT การใช้งานโปรแกรม หรือ Application ต่าง ๆ แนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่างๆ ของบริษัทฯ
- การสื่อสารประเด็นความเสี่ยงทาง Cyber ที่เกิดขึ้นเพื่อให้ความรู้และสร้างความตระหนักต่อภัยทางไซเบอร์ (Security Awareness) โดยจะมีข่าวสารต่าง ๆ ออกแจ้งพนักงานทาง Outlook ต่อเนื่องเป็นประจำ
- Cybersecurity Awareness Improvement Program จะมีการจัดเป็นประจำทุกปี โดยการให้การทำแบบประเมินทดสอบความเข้าใจเรื่อง Phishing Mail จากนั้นจะความรู้เรื่อง email ที่หลอกเอารหัสผ่าน (Phishing Mail) และทำ Phishing Simulation คือ การจำลองอีเมลฟิชชิงส่งให้กลุ่มผู้ใช้งานภายในองค์กรเพื่อวัดระดับความเสี่ยงขององค์กรต่อภัยคุกคามประเภทฟิชชิง และวัดความตระหนักของผู้ใช้งานในการแยกแยะฟิชชิงอีเมล (Security Awareness Assessment) โดยมีการเก็บบันทึกผลการทดสอบและวิเคราะห์ข้อมูล เพื่อนำไปวางแผนและจัดอบรมพัฒนาความรู้ รวมถึงปรับปรุงมาตรการป้องกันภัยฟิชชิงขององค์กร ในปี 2019 มีการดำเนินการ 2 ครั้ง พบว่าพนักงานมีความเข้าใจ ระวังระวังและรู้จักวิธีจัดการกับ Phishing Mail ดีขึ้นอย่างมาก

PHISHING SIMULATION RESULT #1

OVERALL OPERATION

ส่ง email ทดสอบ	541 คน (24.9%) มีการเปิด email	373 คน (17.2%) เปิด email อ่าน และเปิด Link	133 คน (6.2%) กรณข้อมูลและเปิด Link
2,170 คน			



PHISHING SIMULATION RESULT #2

OVERALL OPERATION

ส่ง email ทดสอบ	261 คน (12.07%) มีการเปิด email	127 คน (5.87%) เปิด email อ่าน และเปิด Link	45 คน (2.08%) กรณข้อมูลและเปิด Link
2,163 คน			



สรุปผล การทดสอบ 2 ครั้ง :	Open 📈 50%	Click 📈 70%	Fill 📈 70%
------------------------------	---------------	----------------	---------------

- Cyber Security Response ของกลุ่มบริษัท บางจากฯ เป็นอีกแนวทางที่บริษัทฯ มีการดำเนินการ โดยจะมีการติดตามกรณีศึกษาทางด้านไซเบอร์ เพื่อนำมาอบรมให้ความรู้แนวทางแก่พนักงาน ผู้บริหาร รวมทั้งบริษัทในกลุ่มบางจากฯ ให้ระมัดระวังและมีความตระหนักในเรื่องการหลอกลวงผ่านทางอีเมลธุรกิจ (Business Email Compromise) เช่น การส่งใบแจ้งหนี้ปลอม โดย

จัดอบรมให้กับส่วนงาน/สายงานที่เกี่ยวข้อง เพื่อให้เกิดความตระหนักและระมัดระวัง โดยได้กำหนดแนวทางการควบคุมที่มีประสิทธิภาพ (Strictly Process Confirming) ดังนี้

1. การร้องขอ: ลงทะเบียนหรือเปลี่ยนแปลงข้อมูลสำคัญโดยเฉพาะข้อมูลบัญชีธนาคาร
2. ให้ใช้แบบฟอร์มจาก ส่วนบริหารสภาพคล่อง เพื่อยืนยัน
3. ต้องลงนามโดยผู้มีอำนาจของคู่ค้านั้น ๆ
4. ต้องมีหลักฐานเอกสารที่เกี่ยวข้อง และนำเชื่อถือตามกฎหมาย
5. Re-Check กับผู้ร้องขอทางโทรศัพท์ที่เคยติดต่อ
6. ให้มีการเพิ่มขึ้นตอนเหล่านี้ใน Work Flow การทำงาน

การซ้อมแผนฉุกเฉินและแผนความต่อเนื่องทางธุรกิจ เป็นการจำลองกรณี “เกิดวิกฤตการณ์กับ Data Center ของ บริษัทฯ” ทำให้ไม่สามารถใช้งานได้ ฝึกซ้อมทดลองร่วมกับบริษัทในเครือและคู่ค้า ที่ดูแลระบบงาน IT รวมทั้งการทดสอบความเป็นไปได้ของแนวทางในการกอบกู้และฟื้นฟูอุปกรณ์เทคโนโลยี/ เทคโนโลยีสารสนเทศ/ระบบสารสนเทศ ตามแนวทางที่กำหนดไว้ใน Disaster Recovery Plan ในกรณีต่างๆ ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ กับแผนความเสี่ยงและความต่อเนื่องทางธุรกิจต่างๆ ที่กำหนดไว้ร่วมกับส่วนบริหารความเสี่ยง

มาตรการการดูแลรับมือกรณีเกิดการคุกคามทางไซเบอร์

บริษัทฯ ได้การรับรองมาตรฐาน ISO/IEC 20000-1:2011 ด้าน IT Service Management System ซึ่งจะขึ้นตอนปฏิบัติการจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ หากพนักงานสามารถ แจ้งได้ 3 ช่องทาง

- แจ้งผ่านระบบ myit : <https://myit.bangchak.co.th/ux/myitapp> เป็นระบบ BMC Remedy
- email ที่ IT-Service
- โทร 4336

ซึ่งบริษัทฯ มีการทำ Cybersecurity Awareness Improvement Program ปีละ 2 ครั้ง ทำให้พนักงานสามารถใช้ช่องทางเหล่านี้แจ้งเหตุที่สงสัยว่าจะเกิดการคุกคามทางไซเบอร์ เมื่อเจ้าหน้าที่ผู้ดูแลระบบรับเรื่องก็จะพิจารณาผลกระทบความเร่งด่วนและความสำคัญของเหตุขัดข้อง หากเป็นเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ จะดำเนินการใช้แผน BCP โดยร่วมกับส่วนบริหารความเสี่ยงองค์กร และสื่อสารกับผู้มีส่วนได้เสีย ตามแผนการสื่อสารในภาวะวิกฤต

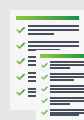
สำหรับพนักงานจะแจ้งระดับความเสี่ยงและผลกระทบต่อธุรกิจที่เกิดขึ้นเป็นระยะ โดยผ่านทางผู้จัดการส่วน/สายงานโดยตรงเพื่อให้ทราบสถานการณ์และปณิปฏิบัติ การประกาศพร้อมแจ้งแนวปฏิบัติอย่างเป็นทางการจากบริษัท ทางช่องทางการสื่อสารภายในองค์กร รวมทั้งการสื่อสารตรงถึงพนักงานจากประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่และทีมด้านดิจิทัลและเทคโนโลยีสารสนเทศเป็นระยะ ๆ จนกว่าจะยุติเหตุฉุกเฉินและสามารถกลับมาดำเนินการได้ตามปกติ

สำหรับการดูแลข้อมูลลูกค้า บริษัทฯ เก็บข้อมูลทั้งหมดไว้ที่ data center ของบริษัทฯ การป้องกันจากภายนอกมีระบบ firewall ในการคัดกรองข้อมูลเข้าและออกและป้องกันการเข้าถึงข้อมูลต่าง ๆ ขององค์กร นอกจากนี้ยังได้กำหนดสิทธิ์ในการเข้าถึงข้อมูลของลูกค้าให้กับผู้ที่เกี่ยวข้องเท่านั้น

ในปี 2562 บริษัทฯ ได้ดำเนินการพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act- PDPA) โดยทำการศึกษา จัดระบบและวางมาตรการในการดูแลคุ้มครองข้อมูลส่วนบุคคลในระบบงานต่าง ๆ ของบริษัทฯ รวมถึงข้อมูลของลูกค้าด้วย



จำนวนครั้งที่เกิดการละเมิดข้อมูล การเปิดเผยข้อมูล
ที่ไม่ได้ตั้งใจ การรั่วไหลของข้อมูลและ เป็นต้น
(Information security breaches or Cybersecurity incidents)



0

2559

0

2560

0

2561

0

2562

จำนวนครั้งที่ข้อมูลลูกค้ารั่วไหลหรือถูกนำไปผิด
เผย/ใช้โดยไม่ได้รับอนุญาต



0

2559

0

2560

0

2561

0

2562