การรักษาความปลอดภัยทางไซเบอร์และความเป็นส่วนตัวของข้อมูล

การรักษาความปลอดภัยทางไซเบอร์

บมจ. ธนาคารกสิกรไทย (“ธนาคาร”) มีเป้าหมายในการพัฒนาอย่างยั่งยืนที่ครอบคลุมทั้งมิติด้านสิ่งแวดล้อม ด้านสังคม ด้านธรรมาภิบาลและเศรษฐกิจ ภายใต้ยุทธศาสตร์การเป็นผู้นำด้านดิจิทัลแบงกิ้งของประเทศไทย โดยตระหนักถึงความสำคัญด้านความปลอดภัยทางไซเบอร์และการปกป้องข้อมูลส่วนบุคคล เพื่อการส่งมอบบริการที่ปลอดภัย มีเสถียรภาพ และไว้วางใจได้ให้กับลูกค้า รวมถึงการร่วมยกระดับความปลอดภัยทางไซเบอร์ของลูกค้า พันธมิตรทางธุรกิจ คู่ค้า และกลุ่มธุรกิจทางการเงิน โดยมุ่งหวังให้เกิดความมั่นคงของระบบธนาคาร และสร้างเสถียรภาพของระบบเทคโนโลยีสารสนเทศทางการเงินในกลุ่มธุรกิจทางการเงินไทยทั้งในปัจจุบันและอนาคต

จากการดำเนินงานในปีที่ผ่านมา ธนาคารและกลุ่มธุรกิจทางการเงิน ไม่มีเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์และการรั่วไหลของข้อมูลที่มีนัยสำคัญ

กรอบการบริหารความเสี่ยงทางไซเบอร์

ธนาคารกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งครอบคลุมการกำกับดูแล การระบุความเสี่ยง การป้องกัน การเฝ้าระวังและตรวจจับ การตอบสนองและฟื้นฟูจากภัยคุกคามและการสร้างวัฒนธรรมองค์กรด้านความปลอดภัยไซเบอร์ โดยสอดคล้องตามกรอบการทำงานด้านความปลอดภัยทางไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST Cybersecurity Framework) และเป็นไปตามนโยบายและแนวทางการปฏิบัติที่ดีของหน่วยงานทางการ ในปี 2567 ธนาคารสามารถยกระดับศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Maturity) ได้ตามเป้าหมาย โดยมีระดับเทียบเท่าธนาคารชั้นนำของโลก จากการประเมินของบริษัทที่ปรึกษาชั้นนำภายนอก

แนวทางดำเนินงานด้านความปลอดภัยของข้อมูลสารสนเทศ

- จัดโครงสร้างองค์กรเพื่อกำกับดูแลการบริหารงานด้านเทคโนโลยีสารสนเทศและความปลอดภัยของข้อมูล โดยแบ่งแยกหน้าที่ออกเป็น หน่วยงานผู้ปฏิบัติงานในแต่ละส่วน (First Line of Defense) หน่วยงานที่ทำหน้าที่ในการบริหารความเสี่ยง (Second Line of Defense) และหน่วยงานที่ทำหน้าที่ตรวจสอบ (Third Line of Defense) ตามแนวทางการป้องกันความเสี่ยง 3 ระดับ (3 Lines of Defense) ทั้งนี้ โครงสร้างดังกล่าวมีการแบ่งแยกความรับผิดชอบอย่างชัดเจนและเป็นอิสระ ครอบคลุมตั้งแต่ระดับของคณะกรรมการ คณะอนุกรรมการ และหน่วยงานระดับปฏิบัติการ

- บริหารจัดการงานเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ (1) การรักษาความลับของระบบและข้อมูล (Confidentiality) (2) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และ (3) ความพร้อมใช้ของเทคโนโลยีสารสนเทศ (Availability)
- กำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมีการทบทวนและปรับปรุงเนื้อหาอย่างน้อยปีละหนึ่งครั้ง เพื่อให้สอดคล้องกับสถานการณ์และความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ พนักงาน พันธมิตรทางธุรกิจ และบุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานของธนาคาร จะต้องปฏิบัติตามแนวทางที่กำหนดไว้อย่างเคร่งครัด นโยบายดังกล่าว ครอบคลุมธนาคารและกลุ่มธุรกิจทางการเงิน โดยนโยบายฉบับนี้สอดคล้องกับมาตรฐานสากล ISO 27001 และครอบคลุมมาตรการบริหารจัดการด้านความมั่นคงปลอดภัยในหลายด้าน ดังนี้
    - การจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
    - การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
    - การรักษาความมั่นคงปลอดภัยของข้อมูล
    - การควบคุมเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ
    - การใช้งานอุปกรณ์คอมพิวเตอร์พกพา และการปฏิบัติงานจากนอกสถานที่
    - ความมั่นคงปลอดภัยในการจัดหาและพัฒนาระบบสารสนเทศ
    - การควบคุมการเข้ารหัสและการบริหารจัดการกุญแจ
    - การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
    - การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT
    - ความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร
    - การบริหารจัดการความมั่นคงปลอดภัยในการบริหารจัดการบุคคลภายนอก
    - การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัย
    - ความมั่นคงปลอดภัยของปัญญาประดิษฐ์ AI
    - การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับ

- เสริมสร้างมาตรการควบคุมความเสี่ยงด้านไซเบอร์ ทั้งการป้องกันภัยคุกคามที่มีความซับซ้อน การเสริมประสิทธิภาพของระบบป้องกันภัยไซเบอร์เพื่อป้องกันการโจมตีที่ไม่รู้จัก การเพิ่มขีดความสามารถในการเฝ้าระวังและตรวจจับภัยคุกคามเชิงรุก และการตอบสนองต่อเหตุการณ์ภัยคุกคามอย่างทันท่วงที มีประสิทธิภาพ และสอดคล้องตามมาตรฐานสากล

- ยกระดับความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ด้านการตอบสนองต่อสถานการณ์ (Incident Response) โดยจัดตั้งคณะทำงานแก้ไขเหตุการณ์ฉุกเฉิน (Incident Response Team) ทำหน้าที่บริหารจัดการเหตุการณ์แบบรวมศูนย์ นอกจากนี้ ธนาคารจัดทำแผนฉุกเฉินครอบคลุม

การจัดการต่างๆ อาทิ แผนบริหารวิกฤติการณ์ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนกู้คืนระบบด้านเทคโนโลยีสารสนเทศ ซึ่งมีการทบทวนแผน และฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Drill) เป็นประจำทุกปี เพื่อให้มั่นใจว่ากระบวนการและแนวทางปฏิบัติยังเหมาะสม ตลอดจนผู้เกี่ยวข้องในระดับของผู้บริหารและผู้ปฏิบัติงานมีความเข้าใจ มีความพร้อมรับมือเหตุภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และธนาคารยังคงดำเนินธุรกิจได้อย่างต่อเนื่องในทุกสถานการณ์

- สร้างวัฒนธรรมองค์กรด้านความปลอดภัยไซเบอร์ (Cyber Hygiene Culture) อย่างต่อเนื่องในทุกระดับ ตั้งแต่คณะกรรมการธนาคาร ผู้บริหาร และพนักงาน ผ่านการจัดทำองค์ความรู้ในรูปแบบต่าง ๆ ได้แก่ การจัดหลักสูตรความมั่นคงปลอดภัยไซเบอร์พื้นฐานในรูปแบบ e-Learning การให้ความรู้เรื่องภัยไซเบอร์ในรูปแบบ Security Newsletter เป็นประจำ เป็นต้น นอกจากนี้ ยังจัดทดสอบการตอบสนองเมื่อพบอีเมลปลอมและเว็บไซต์ปลอมแบบเสมือนจริง (Phishing Drill) ทุกไตรมาส เพื่อให้มั่นใจว่าพนักงานสามารถแยกแยะ ตอบสนอง และป้องกันภัยไซเบอร์ได้อย่างถูกต้อง ทั้งนี้ ธนาคารได้กำหนดกระบวนการแจ้งเหตุการณ์ต้องสงสัยอย่างชัดเจน พนักงานสามารถรายงานเหตุการณ์ที่อาจเป็นภัยคุกคามทางไซเบอร์ได้ผ่านช่องทางอีเมลและสายด่วนแจ้งเหตุการณ์ต้องสงสัย

- สร้างความตระหนักรู้และความพร้อมรับมือภัยทุจริตดิจิทัลให้กับลูกค้า โดยดำเนินการผ่านโครงการ “สติ” เพื่อให้ลูกค้าเท่าทันต่อภัยทางออนไลน์ และสามารถรับมือกับเหตุการณ์หลอกลวงในปัจจุบันได้ ผ่านการสื่อสารหลากหลายช่องทางของธนาคาร อาทิ เว็บไซต์ สาขา สื่อโซเชียลมีเดีย เป็นต้น ที่สามารถเข้าถึงลูกค้าอย่างทั่วถึงและเป็นวงกว้าง นอกจากนี้ ธนาคารมีการให้ความรู้เกี่ยวกับภัยคุกคามและมาตรฐานความปลอดภัยทางไซเบอร์กับพันธมิตรทางธุรกิจและคู่ค้า และร่วมดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Drill) อย่างสม่ำเสมอ

- ยกระดับการบริหารความเสี่ยงของพันธมิตรทางธุรกิจและบุคคลภายนอก เพื่อควบคุมความเสี่ยงจากการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลของพันธมิตรทางธุรกิจและบุคคลภายนอก โดยธนาคารกำหนดนโยบาย มาตรฐานความปลอดภัยข้อมูลสารสนเทศ และจัดหาเครื่องมือมาใช้ประเมินความเสี่ยงของพันธมิตรทางธุรกิจและบุคคลภายนอกตั้งแต่ขั้นตอนการเตรียมความพร้อมในการทำงานร่วมกัน (Onboard) และมีการติดตามเฝ้าระวังความเสี่ยงอย่างต่อเนื่องตลอดเวลาที่มีความสัมพันธ์ทางธุรกิจ รวมถึงมีระบบการแจ้งเตือนหากพบความผิดปกติทางไซเบอร์ที่มีนัยสำคัญ

การได้รับรองมาตรฐานสากล

ธนาคารได้รับการรับรองมาตรฐานสากลในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO 27001 มาอย่างต่อเนื่อง ตั้งแต่ปี 2557 และได้รับการรับรองมาตรฐาน PCI DSS สำหรับระบบการรักษาความปลอดภัยของข้อมูลบัตรเครดิต ตั้งแต่ปี 2562 เป็นต้นมา