การกำกับดูแลและการบริหารจัดการข้อมูลแบบบูรณาการ

เนื่องจากการดำเนินธุรกิจของสถาบันการเงินในปัจจุบันต้องใช้ข้อมูลในการดำเนินการ รวมถึงใช้ในการวิเคราะห์เพื่อขับเคลื่อนการดำเนินงานตามแนวโน้มของภาคธุรกิจในปัจจุบันเริ่มเข้าสู่การเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) ด้วยเหตุนี้กลุ่มทิสโก้จึงตระหนักและให้ความสำคัญกับการบริหารจัดการด้านข้อมูล ทั้งในเรื่องของปริมาณของข้อมูล (Volume) ความหลากหลายของรูปแบบข้อมูล (Variety) ความเร็วของการเปลี่ยนแปลงในวงจรชีวิตข้อมูล (Velocity) ความน่าเชื่อถือของข้อมูล (Veracity) เพื่อให้ความมั่นใจในคุณภาพของข้อมูล (Data Quality) ซึ่งรวมถึงความถูกต้องของข้อมูลวิเคราะห์ที่ใช้สำหรับการตัดสินใจ และทำความเข้าใจในความต้องการของลูกค้าผ่านปัญญาประดิษฐ์ และนอกจากวิวัฒนาการและเทคโนโลยีที่เปลี่ยนแปลงไปข้างต้น ในมุมมองของกฎเกณฑ์และกฎหมายก็ส่งผลให้การดำเนินการธุรกิจต้องปรับปรุงให้สอดคล้องกัน

จากปัจจัยเหล่านี้ กลุ่มทิสโก้เชื่อว่าการสร้างการกำกับดูแลข้อมูล (Data Governance) ที่ดีเป็นงานที่ต้องทำอย่างต่อเนื่องเพื่อเสริมความแข็งแกร่งให้กับการกำกับดูแลข้อมูลโดยรวม ดังนั้น กลุ่มทิสโก้จึงให้ความสำคัญกับการบริหารจัดการข้อมูลทั้งในส่วนของการดูแลรักษาความปลอดภัยและความพร้อมใช้งานของข้อมูล คุณภาพข้อมูล และการรักษาข้อมูลส่วนบุคคลในระดับสูงสุด ให้สอดคล้อง ไม่ขัดต่อนโยบายหรือกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยได้กำหนดให้มีโครงสร้างของคณะอนุกรรมการกำกับดูแลข้อมูล ผู้ควบคุมข้อมูล และผู้ปฏิบัติงานข้อมูลที่เกี่ยวข้องกับข้อมูล มีการระบุขอบเขตหน้าที่ กระบวนการดำเนินงาน ไปจนถึงกระบวนการวัดผลจากการกำกับดูแลข้อมูล เพื่อให้มั่นใจว่ากระบวนการกำกับดูแลข้อมูลจากมาตรการต่าง ๆ ที่กำหนดไว้ เพียงพอกับการปฏิบัติงาน ทำให้เกิดความมั่นคงปลอดภัยของข้อมูล มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน สร้างความมั่นใจกับเจ้าของข้อมูลหรือลูกค้าที่มีต่อบริษัทในการดำเนินธุรกิจ

โดยในปี 2566 การกำกับดูแลข้อมูลและการบริหารการจัดการข้อมูล (Data Governance and Data Management) ได้มีการดำเนินการดังนี้

การดำเนินการจัดการข้อมูลเพิ่มเติมในปี 2566

ทบทวนปรับปรุง นโยบาย แนวปฏิบัติ และมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล เพื่อใช้ในการบริหารจัดการข้อมูลองค์กรอย่างเหมาะสมกับแต่ละสายธุรกิจ ตั้งแต่การสร้าง การจัดเก็บ เผยแพร่ และการทำลายข้อมูล ให้เป็นมาตรฐาน และมั่นคงปลอดภัยเหมาะสมกับระดับชั้นข้อมูล ภายใต้หลักความจำเป็นในการรับรู้ข้อมูล (Need-to-Know Basis) และการอนุญาตการเข้าถึงข้อมูลตามภาระหน้าที่ความรับผิดชอบ (Least Privilege) ซึ่งมีการทบทวนทุก ๆ ปี หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

สร้างความตระหนักรู้และยกระดับความเข้าใจต่อแนวปฏิบัติในการกำกับดูแลและการบริหารการจัดการข้อมูลแก่ผู้เกี่ยวข้องที่มีความเสี่ยงสูงและผู้มีส่วนได้เสีย ผ่านการสัมมนา อบรม การประชุมเชิงปฏิบัติการ (Workshop) การสื่อสารผ่าน Social Network ขององค์กร และจัดให้มีการทดสอบความรู้ความเข้าใจต่อแนวปฏิบัติ (Compulsory Test) กับพนักงานทั้งองค์กร

มีการนำแนวปฏิบัติการกำกับดูแลข้อมูล และกำหนดมาตรฐานไปบังคับใช้ (Adoption) กับระบบงานต่าง ๆ ที่พัฒนาขึ้นใหม่ทั้งหมด รวมถึงตรวจทานการดำเนินการกับระบบนัยสำคัญที่มีอยู่เดิมอย่างต่อเนื่องตามแผนงานที่เสนออนุมัติไว้ โดยมีการสรุปรายงานผลการกำกับดูแลข้อมูล ความเสี่ยงที่เกิดจากการปฏิบัติงานและผลจากการจัดการความเสี่ยงที่เชื่อมโยงกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทั้งระบบที่พัฒนาขึ้นใหม่และระบบที่มีอยู่ให้เป็นไปตามมาตรการควบคุมต่าง ๆ ต่อคณะกรรมการกำกับดูแลข้อมูลในทุกไตรมาส

สร้างและขยายประสิทธิภาพของการจัดการข้อมูลแบบรวมศูนย์ เพื่อง่ายต่อการจัดการเบ็ดเสร็จ ง่าย สะดวกต่อการดำเนินการให้เป็นไปตามมาตรการควบคุม โดยครอบคลุมการจัดเก็บคำอธิบายข้อมูล (Metadata) ให้เข้าถึงได้สะดวกภายใต้การควบคุมของผู้ดูแลข้อมูล การลบทำลายข้อมูล (Data Retention) และการตรวจสอบคุณภาพข้อมูล (Data Quality) รวมถึงการควบคุมการใช้งานและแชร์ข้อมูล เป็นต้น

การดำเนินการรักษาความปลอดภัยและคุ้มครองข้อมูลลูกค้า

กลุ่มทิสโก้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล โดยดำเนินการเป็นส่วนหนึ่งของระบบการกำกับดูแลข้อมูล รวมถึงกำหนดกระบวนการและระบบงานควบคุมข้อมูลส่วนบุคคลให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการ โดยมีการทบทวนแนวปฏิบัติ ขั้นตอนหรือวิธีการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการจัดการรักษาความปลอดภัยและคุ้มครองข้อมูลลูกค้าอย่างสม่ำเสมอ เพื่อให้เป็นปัจจุบัน และสอดคล้องกับวิธีปฏิบัติงานของกลุ่มทิสโก้ ป้องกันความเสี่ยงที่เกิดขึ้นจากการละเมิดการใช้และเปิดเผยข้อมูลส่วนบุคคลที่ไม่เป็นไปตามวัตถุประสงค์ของการให้ข้อมูลของเจ้าของข้อมูลส่วนบุคคลหรือไม่เป็นไปตามข้อกำหนดของกฎหมาย นอกจากนี้ยังกำหนดให้มีแผนรองรับกรณีเกิดเหตุละเมิดข้อมูล (Data Breach Response Plan) เพื่อเป็นกลไกป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นเมื่อเกิดเหตุละเมิดข้อมูล

นอกจากนี้ กลุ่มทิสโก้ยังได้มีการจัดทำวิธีปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เพื่อใช้เป็นแนวทางการปฏิบัติงานให้ผู้ที่เกี่ยวข้องสามารถทำการประเมินผลกระทบและความเสี่ยงที่อาจจะเกิดขึ้น จากการนำข้อมูลส่วนบุคคลมาประมวลผลอย่างไม่เหมาะสม หรืออาจทำให้เกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เพื่อให้สามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและลดโอกาสหรือความรุนแรงที่จะเกิดผลกระทบได้

ตัวอย่างแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

- การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคล
- การขอความยินยอม
- การจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล
- การกำหนดมาตราการรักษาความปลอดภัยของข้อมูลส่วนบุคคล
- การเก็บ ระยะเวลาในการเก็บและการทำลายข้อมูล
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- การจัดการกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล

การดำเนินการเพิ่มเติมในปี 2566

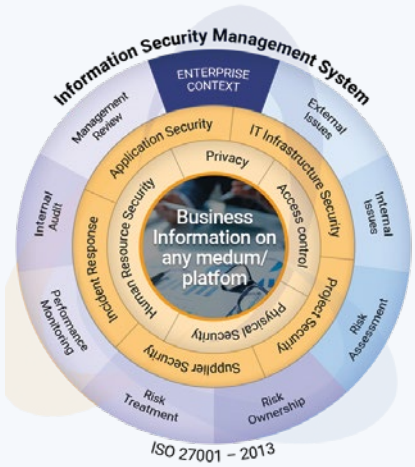
- ทบทวนปรับปรุง แนวปฏิบัติ ขั้นตอนหรือวิธีการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการจัดการรักษาความปลอดภัยและคุ้มครองข้อมูลลูกค้าให้เป็นปัจจุบัน และสอดคล้องกับวิธีปฏิบัติงานของกลุ่มทิสโก้
- การดูแลและคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้า ในปี 2566 กลุ่มทิสโก้ไม่มีข้อร้องเรียนที่เกี่ยวข้องกับการละเมิดความเป็นส่วนตัวของลูกค้าอย่างมีนัยยะสำคัญ

ความมั่นคงปลอดภัยทางไซเบอร์

ในปัจจุบัน ข้อมูลส่วนบุคคลและข้อมูลสำคัญต่าง ๆ ที่มีการใช้งานภายในองค์กรได้กลายเป็นสินทรัพย์ที่มีความสำคัญมากต่อการดำเนินธุรกิจโดยเฉพาะธุรกิจด้านการเงินการธนาคาร รวมถึงภัยคุกคามทางไซเบอร์ที่ถือเป็นความเสี่ยงที่ภาคการเงินการธนาคารต้องให้ความสำคัญ จากรูปแบบการดำเนินธุรกิจในปัจจุบันที่มีการนำเทคโนโลยีสารสนเทศที่ทันสมัยหลากหลายรูปแบบมาใช้ในการพัฒนาผลิตภัณฑ์และบริการทางการเงินรูปแบบใหม่ ๆ เพื่อให้ได้ผลิตภัณฑ์และบริการที่ตรงตามความต้องการของลูกค้าและพันธมิตรทางธุรกิจของกลุ่มทิสโก้ และเป็นการสร้างโอกาสทางธุรกิจและความได้เปรียบในการแข่งขันซึ่งจะส่งผลให้เกิดการเติบโตทางธุรกิจอย่างยั่งยืน

ด้วยเหตุนี้ กลุ่มทิสโก้จึงให้ความสำคัญเป็นอย่างยิ่งในกำหนดนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยทางไซเบอร์และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ชัดเจนและสอดคล้องกับมาตรฐานสากล มุ่งเน้นไปที่การนำเทคโนโลยีที่ทันสมัยมาใช้ในการบริหารและควบคุมความเสี่ยงทั้งในเชิงการป้องกัน (Preventive) การตรวจจับ (Detective) และการตอบสนอง (Response) ต่อภัยคุกคามด้านไซเบอร์และเทคโนโลยีสารสนเทศ โดยมีการนำมาตรการควบคุมที่เป็นมาตรฐานสากล ได้แก่ ISO/IEC 27001 และ NIST Cybersecurity Framework มาประยุกต์ใช้ในการกำหนดแนวนโยบายและแนวปฏิบัติด้านความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจของกลุ่มทิสโก้ให้สามารถใช้บริการได้ปลอดภัย

NIST Cybersecurity Framework



ISO/IEC 27001 Framework

กลุ่มทิสโก้ยังได้มีการจัดโครงสร้างองค์กรภายในให้มีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) ที่ดี โดยมีการกำหนดโครงสร้างและกำหนดบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างชัดเจนและเหมาะสม ตั้งแต่ระดับคณะกรรมการและผู้บริหารระดับสูงที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยง รวมถึงมีการนำหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defense) มาใช้ เพื่อให้การปฏิบัติงานและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีระบบและมีความต่อเนื่อง โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน ดังนี้

การป้องกันความเสี่ยงระดับที่ 1 (1st Line of Defense)

ได้แก่ หน่วยงานผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ทำหน้าที่ดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมทั้งการบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศภายในองค์กร

การป้องกันความเสี่ยงระดับที่ 2 (2nd Line of Defense)

ได้แก่ หน่วยงานที่ทำหน้าที่ในการบริหารความเสี่ยง กำกับดูแล และติดตามการบริหารจัดการความเสี่ยงในภาพรวมขององค์กรโดยครอบคลุมทั้งการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และการบริหารความเสี่ยงด้านการดำเนินงาน (Operation Risk)

การป้องกันความเสี่ยงระดับที่ 3 (3rd Line of Defense)

ได้แก่ หน่วยงานที่ทำหน้าที่ในการตรวจสอบเพื่อสอบทานการปฏิบัติงานอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

นอกจากนี้ กลุ่มทิสโก้ยังได้ให้ความสำคัญอย่างยิ่งในการสร้างวัฒนธรรมด้านความเสี่ยงจากภัยทางไซเบอร์ภายในองค์กรด้วยการสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ (Cyber Security Swareness) โดยเน้นที่กลุ่มเป้าหมาย 4 กลุ่ม ได้แก่

คณะกรรมการและผู้บริหารระดับสูง :

ให้ความสำคัญในเรื่องภัยคุกคามทางไซเบอร์เป็นหนึ่งในเป้าหมายหลักของคณะกรรมการและผู้บริหารระดับสูง โดยมีการเข้าร่วมการฝึกอบรมในหลักสูตร IT Security Awareness Training ประจำปีสำหรับผู้บริหารระดับสูง เพื่อให้ผู้บริหารรับทราบและเข้าใจรูปแบบและเทรนด์การโจมตีทางไซเบอร์ใหม่ ๆ ที่ซับซ้อนและหลากหลาย เพื่อนำมาใช้เป็นข้อมูลประกอบการวางแนวนโยบายและมาตรการในการจัดการกับความเสี่ยงและการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ

พนักงานด้านเทคโนโลยีสารสนเทศ :

พนักงานที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศได้รับการฝึกอบรมเกี่ยวกับความรู้ด้านเทคโนโลยีที่จำเป็นต่อการปฏิบัติงาน รวมถึงได้มีการเข้าร่วมการจัดซ้อมแผนรับมือการโจมตีทางไซเบอร์ (Cyber Drill Exercise) ที่จัดขึ้นเป็นประจำทุกปี โดยมีการจำลองเหตุการณ์โจมตีทางไซเบอร์แบบเสมือนจริง ทั้งที่จัดขึ้นภายในองค์กร และสถาบันภายนอก เช่น ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร สมาคมธนาคารไทย (TB-CERT: Thailand Banking Sector Computer Emergency Response Team) เพื่อยกระดับความร่วมมือและความเข้าใจในระดับอุตสาหกรรมการเงิน เพื่อทดสอบและซักซ้อมแนวปฏิบัติที่ใช้ในการตอบสนองต่อเหตุโจมตี (Incident Response Plan) และเพื่อเป็นการยกระดับความพร้อมในการรับมือกับเหตุโจมตีทางไซเบอร์ที่อาจเกิดขึ้นกับกลุ่มทิสโก้

พนักงานของกลุ่มทิสโก้ :

พนักงานทุกคนได้รับการฝึกอบรมและการให้ความรู้ในเรื่องการรักษาความปลอดภัยข้อมูลสารสนเทศและความรู้ด้านภัยคุกคามทางไซเบอร์ใหม่ ๆ ผ่านสื่อการเรียนรู้ทั้งรูปแบบของ E-Learning โปสเตอร์ Infographic และการอบรมที่เกี่ยวกับมาตรฐานสากลด้านความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อให้พนักงานทุกคนสามารถนำความรู้ดังกล่าวไปใช้ในการปฏิบัติงาน อันจะส่งผลให้เกิดความปลอดภัยในผลิตภัณฑ์และบริการต่าง ๆ ของกลุ่มทิสโก้ นอกจากนี้ พนักงานทุกคนได้เข้าร่วมทดสอบ Phishing Drill โดยการส่ง Phishing Email ปลอมให้กับพนักงานทุกคนเพื่อเป็นการทดสอบวิธีการรับมือในสถานการณ์จริง ซึ่งผลการทดสอบพบว่าพนักงานมีความตระหนักรู้และสามารถตอบสนองต่อ Phishing Email ในองค์กรได้อย่างถูกต้อง

ลูกค้า :

กลุ่มทิสโก้ได้มีการให้ความรู้และสร้างการตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ รวมถึงวิธีการทำธุรกรรมทางออนไลน์อย่างปลอดภัยให้แก่ลูกค้าอย่างสม่ำเสมอ ผ่านช่องทางการสื่อสารหลักที่หลากหลายของกลุ่มทิสโก้ เช่น หน้าเว็บไซต์ หรือสื่อเครือข่ายสังคมออนไลน์ เป็นต้น เพื่อให้ลูกค้ามีความตระหนักรู้และสามารถรับมือกับการหลอกลวงและภัยคุกคามทางไซเบอร์ที่แพร่หลายอยู่ในปัจจุบันได้

จากการประเมินและตรวจสอบในปี 2566 **ไม่พบเรื่องร้องเรียนในประเด็นที่เกี่ยวข้องกับความปลอดภัยข้อมูลของลูกค้า การสูญหาย การแก้ไขปลอมแปลงข้อมูล รวมถึงการเข้าถึงข้อมูลโดยผู้ที่ไม่มีส่วนเกี่ยวข้อง**