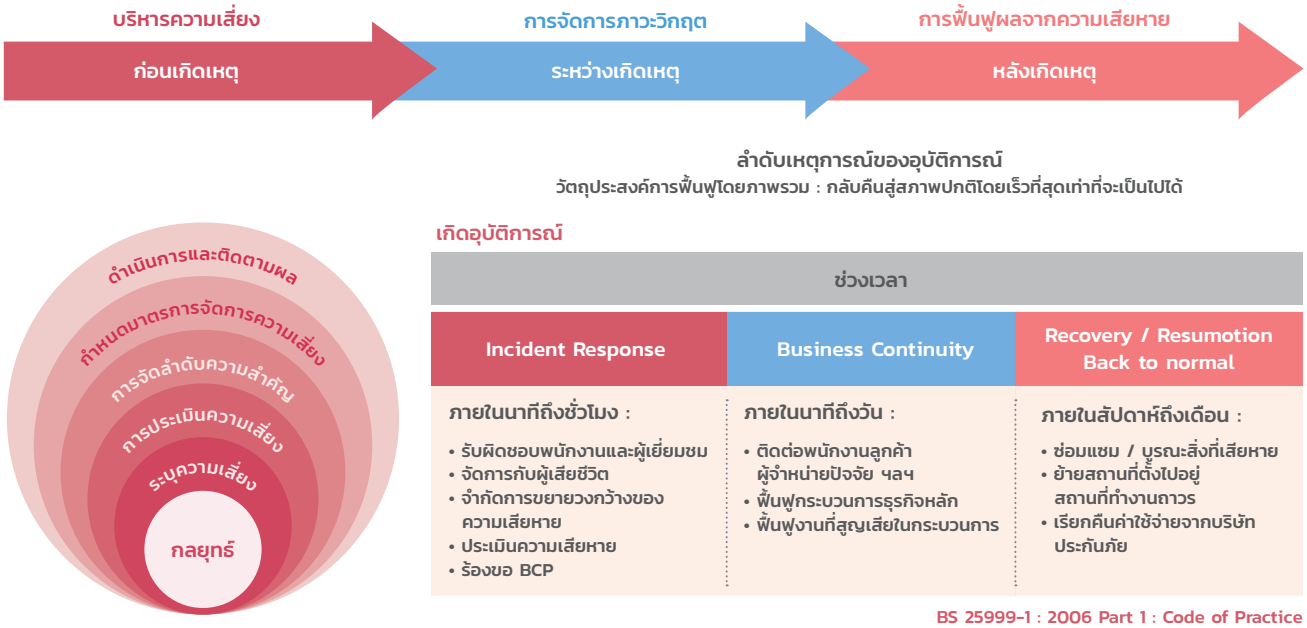
การบริหารจัดการความเสี่ยง

บริษัทมีความมุ่งมั่นในการจัดการบริหารความเสี่ยง ซึ่งถือเป็นกลไกสำคัญในการระบุแนวโน้มความเสี่ยงและปัญหาที่อาจเกิดขึ้นและอาจส่งผลกระทบต่อองค์กร พร้อมกันนี้ การบริหารความเสี่ยงที่มีประสิทธิภาพและมีมาตรการในการลดความเสี่ยง ยังเป็นปัจจัยสำคัญในการขับเคลื่อนองค์กรให้สามารถบรรลุตามเป้าหมายได้ พร้อมทั้งสร้างคุณค่าให้กับผู้มีส่วนได้ส่วนเสียทุกกลุ่ม ดังนั้น บริษัทจึงกำหนดกรอบนโยบายการบริหารความเสี่ยง เพื่อให้องค์กรสามารถดำเนินงานตามแนวทางการบริหารความเสี่ยงได้ รวมถึงสามารถค้นหาและคาดการณ์ความเสี่ยงล่วงหน้าที่อาจส่งผลกระทบเชิงลบต่อการดำเนินการและเป้าหมายองค์กรที่กำหนดไว้ในทุกด้าน พร้อมทั้งจัดทำแผนควบคุมติดตามปรับปรุงความเสี่ยงอย่างต่อเนื่อง ด้วยกลไก การบริหาร การควบคุมและสอบทานเพื่อกำกับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ รวมไปถึงสามารถปลูกฝังวัฒนธรรมความเสี่ยงภายในองค์กร เพื่อเสริมสร้างความเข้าใจ สร้างความตระหนัก และสร้างการมีส่วนร่วมให้กับพนักงานทุกระดับในการบริหารความเสี่ยงทุกด้านขององค์กร

กรอบการบริหารความเสี่ยงและภาวะวิกฤตเพื่อการดำเนินธุรกิจอย่างยั่งยืน



BS 25999-1 : 2006 Part 1 : Code of Practice

บริษัทมีการจัดตั้งหน่วยงานบริหารความเสี่ยง (Risk Management Unit) และหน่วยงานกำกับดูแลการปฏิบัติงานให้เป็นไปตามกฎหมาย กฎระเบียบและข้อบังคับ (Compliance Unit) ภายใต้การดำเนินงานของคณะกรรมการบริหารความเสี่ยง (Risk Management Committee) บริษัทมอบหมายให้ตัวแทนในแต่ละหน่วยงานทำหน้าที่ร่วมเป็นคณะทำงาน พร้อมทั้งสรุปและรายงานผลการปฏิบัติงานนำเสนอต่อที่ประชุมคณะกรรมการบริหาร คณะกรรมการตรวจสอบและคณะกรรมการบริษัท ปีละ 2 ครั้ง เพื่อสอบทานประสิทธิภาพและประสิทธิผลของกระบวนการบริหารความเสี่ยง อาทิ ความเสี่ยงด้านการเงิน ความเสี่ยงด้านภาษี ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านสังคม ความเสี่ยงด้านสิ่งแวดล้อม การเปลี่ยนแปลงของสภาพภูมิอากาศ ความเสี่ยงด้านเศรษฐกิจ ความเสี่ยงด้านทุจริตคอร์รัปชัน และความเสี่ยงด้านชื่อเสียง รวมถึงมีการทบทวนและประเมินระบบบริหารความเสี่ยงตามกรอบ COSO ปีละครั้ง

โดยในปี 2562 หน่วยงานบริหารความเสี่ยงได้จัดโครงสร้างการบริหารความเสี่ยงออกเป็น 3 หมวด ได้แก่

1. ความเสี่ยงทั่วไปที่สามารถเกิดขึ้นได้ในการดำเนินงานประจำวัน (Operational risk)
2. ความเสี่ยงที่ไม่เกี่ยวข้องกับการเงิน (Sustainability risk) และ
3. ความเสี่ยงที่เกิดใหม่ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ (Emerging risk)

โดยมีการประสานงานกับหน่วยงานต่าง ๆ ผ่านการประเมินความเสี่ยงประจำปี และอบรมสัมมนาตัวแทนจากหน่วยงานต่าง ๆ ที่ทำหน้าที่ผลักดันในการออกมาตรการและการดำเนินงานตามมาตรการเพื่อลดความเสี่ยง (Risk Champion) ในแต่ละไตรมาส และมีการจัดตั้ง Data Protection Officer เพื่อให้ความรู้ รวมถึงมีกระบวนการควบคุมภายใน และติดตามความเสี่ยงโดยทำงานอย่างใกล้ชิดกับ Risk Champion ซึ่งสามารถสรุปขั้นตอนและผลการดำเนินงานได้ดังแผนภูมิ

ความเสี่ยงที่เกิดใหม่ (Emerging Risks)

บริษัทมีการทบทวนประเด็นความเสี่ยงและวิเคราะห์ความเสี่ยงที่เกิดใหม่ที่อาจส่งผลต่อการดำเนินธุรกิจขององค์กรประจำปีอย่างสม่ำเสมอ เพื่อการพัฒนามาตรการรองรับและสามารถตอบสนองต่อความเสี่ยงได้ทันท่วงที โดยในปี 2562 มีความเสี่ยงเกิดใหม่ที่ส่งผลต่อการดำเนินธุรกิจ (Emerging Risks) 2 ประเภท ดังนี้ ความเสี่ยงด้านการเปลี่ยนแปลงเทคโนโลยีดิจิทัล (Digital Transformation) และความเสี่ยงด้านความมั่นคงและความปลอดภัยทางไซเบอร์ (Cyber Security)

ความเสี่ยงด้านการเปลี่ยนแปลงเทคโนโลยีดิจิทัล (Digital Transformation)

การปรับเปลี่ยนรูปแบบการดำเนินธุรกิจหรือกระบวนการดำเนินงานภายในให้เป็นระบบดิจิทัลอย่างรวดเร็ว ทำให้การแข่งขันทางธุรกิจที่สูงขึ้น และส่งผลให้ความต้องการและพฤติกรรมของผู้บริโภคเปลี่ยนแปลงไป ก่อให้เกิดความเสี่ยงในการดำเนินธุรกิจ บริษัทจึงกำหนดกลยุทธ์และแผนการดำเนินธุรกิจด้านเทคโนโลยีดิจิทัลที่เหมาะสมผ่านแนวทาง ดังนี้

1 การพัฒนาช่องทางในการบริโภคสินค้าสำหรับผู้บริโภคที่หลากหลายมากยิ่งขึ้น อาทิ Omni Channel เป็นช่องทางการจัดจำหน่ายสินค้าที่ช่วยให้ผู้บริโภคเข้าถึงได้ง่าย สะดวกสบาย โดยผ่านการผสมผสานช่องทางการจัดจำหน่าย ทั้งระบบออฟไลน์และออนไลน์ สร้างประสบการณ์แบบไร้รอยต่อ

2 การพัฒนาระบบการชำระสินค้าที่หลากหลายรูปแบบมากยิ่งขึ้น เช่น ระบบ Alipay Wallet ระบบ TrueMoney Wallet

3 สร้างโปรแกรมสมาชิก ALL Member รับคะแนนสะสมจากการซื้อสินค้าที่ร้านเซเว่นอีเลฟเว่น เซ็อมโยงสิทธิพิเศษ กับบริษัทย่อยรวมถึงพัฒนารูปแบบการจัดกิจกรรมส่งเสริมการขายผ่านแอปพลิเคชันและกิจกรรมการตลาดออนไลน์ (Digital Marketing) เพื่อสร้างโอกาสทางธุรกิจให้กับผู้ประกอบการต่าง ๆ และสร้างความผูกพันกับผู้บริโภค (Customer Engagement)

4 ศึกษารูปแบบการให้บริการใหม่ ๆ (Service Solution) เพื่อตอบโจทย์ลูกค้าในยุคดิจิทัล

5 พัฒนาระบบการกระจายสินค้า

6 ปรับโครงสร้างและรูปแบบการทำงานให้สนับสนุนการทำงานในยุคดิจิทัล พร้อมทั้งวางระบบ การป้องกันความเสี่ยงด้านดิจิทัล อาทิ การปกป้องข้อมูลบุคคลส่วนบุคคลและความปลอดภัยของสารสนเทศและการโจมตีทางไซเบอร์

7 พัฒนาบุคลากรปรับรูปแบบการทำงานให้มีความคล่องตัวมากขึ้นเตรียมความพร้อมสู่ยุคดิจิทัล

ความเสี่ยงด้านความมั่นคงและความปลอดภัยทางไซเบอร์ (Cyber Security)

การเปลี่ยนแปลงรูปแบบการดำเนินธุรกิจภายในองค์กรให้เป็นระบบดิจิทัลมากยิ่งขึ้น ส่งผลให้การดำเนินธุรกิจมีความเสี่ยงด้านความมั่นคงและความปลอดภัยทางไซเบอร์มากขึ้น ซึ่งอาจส่งผลกระทบต่อชื่อเสียง ภาพลักษณ์ และความน่าเชื่อถือขององค์กรได้ บริษัทจึงได้กำหนดมาตรฐานการจัดการเทคโนโลยีสารสนเทศ (Information Technology Security Management) และระบบจัดการกลยุทธ์ความปลอดภัยทางอินเตอร์เน็ต ซึ่งประกอบด้วย 3 องค์ประกอบได้แก่

1

หน่วยงานและบุคลากร
โดยกำหนดบทบาทหน้าที่ของหน่วยงาน Cyber Security Officer ให้สอดคล้องและครอบคลุมความเสี่ยงทำหน้าที่เฝ้าระวังและควบคุมความเสี่ยงที่เกิดขึ้นให้อยู่ในระดับที่สามารถยอมรับได้ จัดตั้งหน่วยงานด้านความปลอดภัยข้อมูลและเครือข่าย การจัดการอบรมและทดสอบความสามารถอย่างสม่ำเสมอเพื่อให้ทันต่อเหตุการณ์และเทคโนโลยี รวมถึงส่งเสริมให้มีการสร้างความตระหนักรู้ในการใช้เทคโนโลยี (Cyber Security Awareness) ให้กับพนักงานอย่างต่อเนื่องผ่านช่องทางการสื่อสารภายใน และทดสอบผ่านโปรแกรมการจำลองเหตุการณ์ทางไซเบอร์ (Cyber Simulation Program)

2

มาตรการและขั้นตอนการดำเนินงาน
โดยนอกจากนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่ายของบริษัทแล้ว บริษัทยังกำหนดให้มีการทบทวนมาตรการอย่างน้อยปีละ 1 ครั้ง มาตรการและขั้นตอนที่กำหนดขึ้นนี้ มีการดำเนินงานโดยบริษัท โกซอฟท์ (ประเทศไทย) จำกัด ภายใต้มาตรฐานสากล ISO 20000 และ ISO27001 และบริษัทยังกำหนดแผนการตอบสนองกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Plan)

3

เทคโนโลยี
โดยบริษัทให้ความสำคัญกับการใช้ระบบเทคโนโลยีที่ทำงานเชิงป้องกันตามแนวปฏิบัติด้านความปลอดภัยระดับสากล หรือ NIST Framework พัฒนาศูนย์คอมพิวเตอร์ให้ได้ระดับมาตรฐานในการเฝ้าระวัง และการเข้าถึงระบบข้อมูลตามที่กำหนดและมุ่งแลกเปลี่ยนความรู้กับผู้ให้บริการและลงทุนในระบบป้องกันใหม่ ๆ เพื่อให้ทันต่อเทคโนโลยี และความเสี่ยงใหม่ ๆ เสมอ

บุคลากร

- Cyber Security Officer (CSO) รายงานตรงต่อคณะกรรมการเจ้าหน้าที่ผู้บริหารระดับสูง
- หน่วยงานด้านระบบความปลอดภัยและบุคคลากรที่ผ่านการรับรองด้วย Security Certificate
- อบรมและทดสอบบุคคลากรทุกระดับ เช่น Phishing Simulation Test, Cyber Awareness และ War Game

ขั้นตอน

- นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่ายภายในบริษัท
- กระบวนการมาตรฐานที่ได้รับการรับรอง ISO20000 และ ISO27001
- แผนการตอบสนอง และจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security Incident Response Plan)

เทคโนโลยี

- ระบบเทคโนโลยีที่ทำงานเชิงป้องกันตามแนวปฏิบัติ NIST
- ศูนย์คอมพิวเตอร์ระดับมาตรฐานที่รวมถึงการเฝ้าระวังและการเข้าถึงระบบข้อมูลตามที่กำหนด
- แลกเปลี่ยนความรู้กับผู้ให้บริการและลงทุนในระบบป้องกันใหม่ ๆ

พร้อมกันนี้ บริษัทยังมุ่งดำเนินงานสร้างความตระหนักในการค้นหาความเสี่ยงภายในองค์กรผ่าน “โครงการค้นหาความเสี่ยงขององค์กรอย่างมีส่วนร่วม” เพื่อให้ผู้บริหารจนถึงพนักงานทำการค้นหาความเสี่ยงจากภัยมืด (Black Swan) ที่อาจทำให้องค์กรไม่บรรลุเป้าหมายหรือเกิดความไม่มั่นคง ปลอดภัยต่อองค์กรอย่างยั่งยืน ภายใต้ประเด็นความเสี่ยงที่เกี่ยวข้อง 6 ประเด็น ได้แก่

1. การดำเนินกิจกรรมทางธุรกิจอย่างต่อเนื่อง
2. กระบวนการทำงาน
3. สินค้าและบริการ
4. การว่าจ้างหน่วยงานภายนอก
5. ความยั่งยืนองค์กร
6. กิจกรรมอื่นที่เกี่ยวข้องกับบริษัทในกลุ่ม

โดยให้ผู้บริหารและพนักงานในองค์กรเข้าร่วมประกวดประเด็นความเสี่ยงผ่านช่องทางที่หลากหลาย เช่น แพลตฟอร์มอิเล็กทรอนิกส์ คิวอาร์โค้ด ซึ่งสร้างความสะดวกและสามารถสร้างการมีส่วนร่วมของพนักงานได้มากยิ่งขึ้น ภายใต้แนวคิด “การค้นหาและการแก้ไขเพื่อช่วยควบคุมป้องกันและรับมือภัยมืดที่อาจจะเกิดขึ้น”

โครงการนักค้นหาภัยมืด (Black Swan Award)

ในปี 2562 มีประเด็นความเสี่ยงที่พนักงานส่งเข้าประกวดทั้งหมด **1,169 ประเด็น**

และมีประเด็นความเสี่ยงที่ได้รับรางวัล **5 ประเด็น**

1) ความสามารถในการปฏิบัติตามกฎและข้อบังคับ
2) ข้อมูลสำคัญรั่วไหล
3) สิทธิมนุษยชนและความปลอดภัย
4) ประเด็นด้านสิ่งแวดล้อม
5) สินค้าและบริการ

โดยประเด็นความเสี่ยงที่ได้รับรางวัลจะถูกนำมาใช้ประกอบการพิจารณาสำหรับผู้บริหารในการออกมาตรการรองรับ ซึ่งสามารถนำไปสู่การพัฒนาให้สามารถนำไปปฏิบัติจริงได้อย่างมีประสิทธิภาพ

โครงการเตรียมความพร้อมด้าน Cyber Resilience

สถานการณ์ความเสี่ยงจากภัยคุกคามทางไซเบอร์

บริษัทตระหนักถึงความสำคัญของข้อมูลลูกค้าการทำธุรกรรมบนโลกออนไลน์ที่อาจมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น ในปีที่ผ่านมาบริษัทได้ทบทวนและมีมาตราการให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งการวางกรอบการกำกับดูแล การบริหารจัดการความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือหรือเทคโนโลยี เพื่อลดผลกระทบต่อลูกค้า และต่อระบบโดยรวม บริษัทจึงได้กำหนดกรอบการประเมินความพร้อมด้าน Cyber Resilience ในปี 2562 ได้มีการจัดอบรมสัมนาสร้างความตระหนักและความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับผู้บริหารและพนักงานในเชิงรุกและมีการทดสอบบนสถานการณ์เสมือนจริง (phishing simulation test) เพื่อเตรียมความพร้อมในการรับมือและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์

ผลลัพธ์

ทบทวนกระบวนการทำงานเพื่อจัดการกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานต่างๆ กำหนดแนวทางในการดำเนินการเพื่อลดความเสี่ยงในระดับความรุนแรงต่าง ๆ

ร้อยละ **100** ของผู้บริหารที่เกี่ยวข้องได้รับการให้ความรู้และเข้าร่วมสัมมนาเชิงปฏิบัติการ

สถานการณ์การจัดการภาวะวิกฤตจากภัยคุกคามทางไซเบอร์

ในปี 2562 บริษัทได้จัดทำโครงการจำลองสถานการณ์การโจมตีทางไซเบอร์ (Cyber War-game) ซึ่งเป็นการสร้างสถานการณ์สมมุติเพื่อให้ผู้บริหารระดับสูงได้ทดลองแก้ไขสถานการณ์ต่อกรณีภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในระบบบริษัท โดยการจัดการภาวะวิกฤตจากภัยคุกคามนี้ มีผู้บริหารระดับสูง ที่เกี่ยวข้อง เช่น CEO, CIO, CSO, CFO, COO รวมทั้งผู้บริหารด้านสื่อสารองค์กร ด้านกฎหมาย เป็นต้น โดยกำหนดมีการจัดกิจกรรมดังกล่าวขึ้นปีละ 1 ครั้ง

ผลลัพธ์

- ร้อยละ **100** ของผู้บริหารระดับสูงที่ได้เข้าร่วมโครงการ
- มีความพร้อมในการจัดการต่อภาวะวิกฤตได้อย่างรวดเร็ว
- ลดความเสี่ยงด้านความเสียหายและเกิดภาพลักษณ์องค์กรเชิงลบ