นโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทฯ จัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนหนึ่งของจริยธรรมทางธุรกิจและแนวปฏิบัติของบริษัทฯ นโยบายนี้จัดทำขึ้นเพื่อให้แน่ใจว่าบริษัทฯ มีการใช้เทคโนโลยีอย่างมีจริยธรรมและเป็นไปตามแนวทางการกำกับดูแล บริษัทฯ ได้จัดทำและดำเนินการตาม ‘นโยบายระบบการจัดการความปลอดภัยของข้อมูล’ เพื่อให้มั่นใจว่าข้อมูลที่มีความละเอียดอ่อนได้รับการป้องกันและรักษาเป็นความลับ ผ่านมาตรการรักษาปลอดภัยที่เหมาะสม พนักงานประจำสำนักงานและบนเรือได้รับการฝึกอบรมเรื่องความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

การคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ มีความมุ่งมั่นที่จะปกป้องและคุ้มครองของข้อมูลส่วนบุคคลผ่าน **“นโยบายคุ้มครองข้อมูลส่วนบุคคล”** นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดกรอบงานที่เหมาะสมสำหรับการจัดการข้อมูลส่วนบุคคล และเพื่อให้แน่ใจว่ามีมาตรการรักษาความปลอดภัยที่เพียงพอในการคุ้มครองและรักษาความปลอดภัยข้อมูลส่วนบุคคลที่บริษัทฯ รวบรวม ใช้ และเปิดเผย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และข้อบังคับที่เกี่ยวข้อง บริษัทฯ ได้เริ่มดำเนินการเพื่อปฏิบัติตามกฎเกณฑ์และเพื่อป้องกันการละเมิดและใช้ข้อมูลส่วนบุคคลในทางที่ผิด บริษัทฯ ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อให้แน่ใจว่าบริษัทฯ มีการเก็บรวบรวม ใช้และเปิดเผยข้อมูลของผู้มีส่วนได้เสียแต่ละราย ตามพระราชบัญญัติฯและกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง

ความปลอดภัยทางด้านไซเบอร์

เพื่อตอบสนองต่อการเปลี่ยนแปลงการปฏิบัติการทางทะเลสมัยใหม่ บริษัทฯ ตระหนักถึงความจำเป็นในดำเนินการด้านความปลอดภัยทางไซเบอร์ ไม่เพียงแต่ในทะเลเท่านั้น แต่ยังรวมถึงสภาพแวดล้อมภายในสำนักงานด้วย เมื่อเรือต่างๆ มีการเชื่อมโยงกันมากขึ้นและรวมถึงการใช้ซอฟต์แวร์ขั้นสูง การสร้างความตระหนักถึงความปลอดภัยทางไซเบอร์จึงกลายเป็นเรื่องที่สำคัญในการลดความเสี่ยงในการปฏิบัติงานและความเสี่ยงด้านความปลอดภัย อุตสาหกรรมการขนส่งทางทะเลทั่วโลกจึงหันมาให้ความสำคัญกับเรื่องนี้ ซึ่งการจัดการกับความกังวลด้านความปลอดภัยทางไซเบอร์ยังคงเป็นเรื่องท้าทายที่สำคัญของบริษัทต่างๆ ทั่วโลก

ความมุ่งมั่นของบริษัทฯ ในการรักษาความปลอดภัยทางไซเบอร์นั้นครอบคลุมหลากหลายแนวทาง บริษัทฯ ได้ประเมินและจัดการกับภัยคุกคามที่เกิดขึ้นใหม่อย่างต่อเนื่อง เพื่อยกระดับมาตรการรักษาความปลอดภัยโดยรวมของบริษัทฯ และรวมถึงการสร้างสภาพแวดล้อมที่ส่งเสริมการทำงานขององค์กร ในขณะเดียวกันก็ลดโอกาสที่จะเกิดการละเมิดความปลอดภัยให้เหลือน้อยที่สุด การเชื่อมโยงของความเสี่ยงระดับโลกหลายรูปแบบรวมมาบรรจบกันกับปัญหาด้านความปลอดภัยทางไซเบอร์ ซึ่งทำให้เกิดความเสี่ยงที่สูงและมีความซับซ้อนยิ่งขึ้น ภูมิรัฐศาสตร์มีส่วนสำคัญให้เกิดความเสี่ยงนี้ เนื่องจากการโจมตีทางไซเบอร์อาจได้รับการสนับสนุนจากรัฐ ซึ่งทำให้เกิดภัยคุกคามทางไซเบอร์ที่มีแรงจูงใจทางการเงินซึ่งแพร่หลายในอุตสาหกรรมของบริษัทฯ ให้มีความรุนแรงยิ่งขึ้น

ความเสี่ยงทางไซเบอร์ที่เพิ่มมากขึ้นภายในบริษัทเป็นผลมาจากการแพร่กระจายอย่างรวดเร็วของการใช้อุปกรณ์ที่เชื่อมต่อถึงกัน การบูรณาการในการใช้เทคโนโลยีที่เกิดขึ้นใหม่บนเรือ และการใช้ปัญญาประดิษฐ์ (AI) เพื่อเป็นแนวทางในการรักษาความปลอดภัยต่อภัยคุกคามทางไซเบอร์ที่ซับซ้อนนี้ อุตสาหกรรมการเดินเรือได้ให้ความสำคัญกับความสามารถในการตอบสนองอย่างมีประสิทธิภาพต่อความถี่และความซับซ้อนของการโจมตีทางไซเบอร์

นอกจากนี้ บริษัทฯ แสดงถึงความมุ่งมั่นของบริษัทฯ ต่อความปลอดภัยทางไซเบอร์ด้วยการได้รับใบรับรอง ISO/IEC 27001 ซึ่งเป็นมาตรฐานที่ได้รับการยอมรับทั่วโลกสำหรับระบบการจัดการความปลอดภัยของข้อมูล การรับรองนี้ไม่เพียงแต่ยืนยันความมุ่งมั่นของบริษัทฯ ต่อความปลอดภัยทางไซเบอร์เท่านั้น แต่ยังรวมถึงการมีกรอบแนวทางแบบองค์รวมที่ครอบคลุมการตรวจสอบบุคคล การมีนโยบายที่ชัดเจน และการใช้เทคโนโลยีที่ทันสมัย

ในขณะที่บริษัทฯ มีระบบป้องกันภัยคุกคามทางไซเบอร์ ทั้งในการปฏิบัติการทางทะเลและภายในสภาพแวดล้อมสำนักงาน บริษัทฯ มุ่งมั่นที่จะให้เกิดความยั่งยืนในการดำเนินงานและมีความยืดหยุ่นหากบริษัทฯเผชิญกับภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นด้วยมาตรการเชิงรุก การลงทุนเชิงกลยุทธ์ และแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่ครอบคลุม ทำให้บริษัทฯ สามารถปรับตัวและเติบโตในยุคดิจิทัลได้ ในขณะเดียวกันก็ทำให้เกิดเอกภาพในการดำเนินงานและได้รับความไว้วางใจจากผู้มีส่วนได้ส่วนเสีย

การจัดการระบบข้อมูล

เช่นเดียวกับการรายงานเมื่อปีก่อน บริษัทฯ ปรับปรุงโปรแกรมคอมพิวเตอร์ใหม่ซึ่งครอบคลุมทุกการปฏิบัติงานในสำนักงานใหญ่และเชื่อมต่อกับกองเรือของบริษัทฯ โปรแกรมนี้แสดงข้อมูลเกี่ยวกับการปฏิบัติงานบนเรือ ต้นทุนที่เกิดขึ้นและข้อมูลอื่นๆ แบบทันที และช่วยให้สำนักงานใหญ่สามารถติดต่อกับกัปตันเรือทุกคนบนเรือทุกลำได้อย่างใกล้ชิด ซึ่งช่วยในการตัดสินใจเมื่อมีเหตุการณ์เกิดขึ้น นอกจากนี้ โปรแกรมดังกล่าว ยังช่วยให้บริษัทฯ สามารถให้บริการลูกค้าได้ดียิ่งขึ้น และสนับสนุนให้การทำงานระหว่างพนักงานในสำนักงานใหญ่กับกองเรือมีประสิทธิภาพยิ่งขึ้นด้วย ระบบนี้ได้มีการยกระดับให้สามารถรองรับการเก็บข้อมูลเพิ่มเติม สำหรับข้อกำหนดการรายงานข้อมูลใหม่และติดตามผลการดำเนินงานของเรือผ่านระบบดิจิทัลมากขึ้น

การตอบสนองต่อเหตุการณ์ทางไซเบอร์

บริษัทฯ ตอบสนองต่ออันตรายและภัยคุกคามด้านความปลอดภัยทางไซเบอร์ ผ่านการวิเคราะห์ช่องโหว่ด้านความปลอดภัยทางไซเบอร์และปิดช่องโหว่เหล่านี้ บริษัทฯ ทำการติดตั้งไฟร์วอลล์เพื่อป้องกันการโจมตีจากภายนอกผ่านแอปพลิเคชั่นการใช้เครือข่ายส่วนตัวเสมือน (VPN) และการตรวจสอบอีเมล์ที่ส่งมาจากภายนอกบริษัทฯ นอกจากนี้ บริษัทฯ ได้จำกัดการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย กำหนดให้มีมาตรการเพื่อป้องกันไวรัส และทำการสำรองข้อมูลของบริษัทฯ เพื่อเตรียมพร้อมกับกรณีฉุกเฉิน เพื่อป้องกันความเสียหายจากการโจรกรรมข้อมูลหรือเหตุการณ์อื่นๆ ที่อาจสร้างผลกระทบต่อระบบข้อมูลของบริษัทฯ

มติ MSC.428(98) ของ IMO ในเรื่องการจัดการความเสี่ยงทางไซเบอร์ทางพาณิชย์นาวีของระบบการจัดการทางด้านความปลอดภัยมีผลใช้บังคับเมื่อวันที่ 1 มกราคม 2564 โดยมติดังกล่าวได้ระบุว่าระบบการจัดการทางด้านความปลอดภัยที่ได้รับการอนุมัติจะต้องรวมการจัดการความเสี่ยงทางไซเบอร์ทางพาณิชย์นาวีที่เป็นไปตามวัตถุประสงค์และข้อกำหนดของกฎระเบียบของ ISM Code ซึ่งเป็นการจัดการเพื่อให้แน่ใจได้ว่าระบบการจัดการทางด้านความปลอดภัยมีการประเมินความเสี่ยงอย่างเหมาะสมและมีมาตรการในการป้องกันเรือจากเหตุการณ์โจมตีทางไซเบอร์ มติดังกล่าวยังกำหนดให้บังคับใช้มาตรการดังกล่าวก่อนการออกใบรับรองการปฏิบัติตาม (Document of Compliance) ตั้งแต่วันที่ 1 มกราคม 2564 เป็นต้นไป บริษัทฯ ได้ดำเนินการให้มีมาตรการดังกล่าวบนเรือทุกลำในกองเรือของบริษัทฯ แล้ว

แม้ว่าไม่มีเหตุการณ์การโจมตีทางไซเบอร์เกิดขึ้นกับบริษัทฯ จนถึงบัดนี้ บริษัทฯ ได้ตรวจสอบภายในองค์กรอย่างสม่ำเสมอและพบว่า

- ปัจจุบันระบบคอมพิวเตอร์ของบริษัทฯ ซึ่งใช้ในสำนักงานและบนเรือมีประสิทธิภาพเพียงพอ เนื่องจากบริษัทฯ เชื่อว่าทั้งระบบเทคโนโลยีสารสนเทศ (Information Technology) และเทคโนโลยีภาคปฏิบัติการ (Operational Technology) ต่างต้องอยู่ภายใต้ความปลอดภัยทางไซเบอร์
- ภัยคุกคามไซเบอร์มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว และสิ่งสำคัญคือระบบรักษาความปลอดภัยทางไซเบอร์ของบริษัทฯ ที่จะต้องสามารถตอบสนองการเปลี่ยนแปลงเหล่านี้ได้ บริษัทฯ ได้ทำงานร่วมกับผู้ให้บริการตรวจจับ และตอบสนองต่อภัยคุกคามขั้นสูงจากภายนอก ซึ่งจะช่วยระบุช่องโหว่ รวมถึงตรวจสอบและตรวจจับภัยคุกคามของระบบโครงสร้างพื้นฐานด้าน IT ที่สำคัญของบริษัทฯ ตลอด 24 ชั่วโมงทุกวัน นอกจากนี้ ยังมีการประเมินและตรวจสอบระบบปฏิบัติการบนเรืออีกด้วย จากรายงานการวิเคราะห์ประสิทธิภาพการดำเนินงาน (Gap Analysis) พบว่า บริษัทฯ ได้ดำเนินการและปฏิบัติตามมาตรการแนะนำในการปฏิบัติงานบนเรือของบริษัทฯ อย่างครบถ้วนเพื่อเพิ่มความปลอดภัยทางไซเบอร์
- นอกจากนี้ ความสมบูรณ์และความเปราะบางของฐานข้อมูลที่เกี่ยวข้องทางการเงินและบัญชีของบริษัทฯ ได้รับการตรวจสอบโดยบริษัทสำนักงาน EY ปีละหนึ่งครั้ง
- ถึงแม้ว่าขณะนี้เรือส่วนใหญ่จะเชื่อมต่อกับระบบอินเตอร์เน็ต แต่ได้มีการอนุญาตให้เข้าถึงเฉพาะบางเว็บไซต์เท่านั้น เพื่อป้องกันโปรแกรมที่ถูกสร้างขึ้นมาเพื่อโจมตีระบบแชร์ไฟล์ (มัลแวร์: Malware) และการหลอกลวงผ่านทางระบบอีเมลล์ (ฟิชชิ่ง : Phishing) ระบบ OT ในเครื่องจักรและอุปกรณ์ระบบนำทางได้แยกออกจากกันและไม่สามารถเข้าถึงอินเตอร์เน็ต ซึ่งจะช่วยลดความเสี่ยงอันเนื่องมาจากการโจมตีทางไซเบอร์บนเรือ
- ระบบ AIS ระบบ ECDIS และระบบบันทึกข้อมูลบนเรือ (VDR) ถือเป็นส่วนหนึ่งของการบูรณาการ ระบบสะพานเรือ (Integrated Bridge System: IBS) ระบบคอมพิวเตอร์ที่ใช้บนเรือของบริษัทฯ มีการตั้งค่าเพื่อให้แน่ใจว่า ระบบดังกล่าวนั้นไม่มีการเชื่อมต่อโดยตรงกับอินเตอร์เน็ตตลอดเวลา และไม่มีการส่งข้อมูลจากอุปกรณ์เหล่านี้ออกไปออนไลน์โดยตรง

อย่างไรก็ตาม เพื่อลดช่องโหว่ที่อาจเกิดขึ้นจากความผิดพลาดทางไซเบอร์และการโจมตีทางไซเบอร์และเพื่อให้แน่ใจว่ากองเรือของบริษัทฯ เดินเรืออย่างปลอดภัยและมีประสิทธิภาพ บริษัทฯ ได้นำระเบียบและแนวปฏิบัติเพิ่มเติมดังต่อไปนี้มาใช้ในการดำเนินงาน

- พนักงานทุกคน ตั้งแต่ระดับผู้บริหารระดับสูงที่อยู่สำนักงานจนถึงลูกเรือบนเรือ มีส่วนร่วมในวัฒนธรรมองค์กรในเรื่องความปลอดภัย และการรักษาความปลอดภัยทางไซเบอร์ของเรือแต่ละลำ
- รวมความเสี่ยงทางไซเบอร์ไว้ในนโยบายของบริษัทฯ เพื่อให้แน่ใจว่าสอดคล้องกับมาตรการความปลอดภัยและการจัดการความเสี่ยงที่ระบุใน ISPS และ ISM Code
- รวมข้อกำหนดใหม่ๆ ที่เกี่ยวข้องกับไซเบอร์ไว้ในแผนการฝึกอบรมลูกเรือ และสำหรับการเดินเรือ รวมถึงการบำรุงรักษาระบบไซเบอร์ที่สำคัญที่อาจมีอยู่บนเรือ
- บริษัทฯ รณรงค์ในการสร้างความตระหนักรู้ให้กับพนักงานเกี่ยวกับการรักษาความมั่นคงปลอดภัย โดยการให้ความรู้แก่พนักงานอย่างสม่ำเสมอ เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการหลีกเลี่ยง ซึ่งจะช่วยสร้างวัฒนธรรมด้านความปลอดภัยภายในองค์กร
- บริษัทฯ ดูแลให้แน่ใจว่าระบบทั้งหมดได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อป้องกันช่องโหว่ที่ทราบจากการถูกโจมตี
- บริษัทฯ ลงทุนในเทคโนโลยีขั้นสูงเพื่อปรับปรุงมาตรการรักษาความปลอดภัยทางไซเบอร์ ซึ่งรวมถึงการใช้ปัญญาประดิษฐ์ (AI: Artificial Intelligence) และการเรียนรู้ของเครื่องมือต่างๆ เพื่อตรวจจับและป้องกันภัยคุกคามทางไซเบอร์
- บริษัทฯ ดำเนินการตรวจสอบและทดสอบรายการอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ามีการปฏิบัติตามระเบียบด้านความปลอดภัยและการรักษาความปลอดภัยทั้งหมดรวมถึงการตรวจสอบประสิทธิภาพของระบบบริหารความเสี่ยงทางไซเบอร์และทำการปรับเปลี่ยนเมื่อมีความจำเป็น