การประเมินความเสี่ยงที่เกิดขึ้นใหม่(Emerging Risk)และความเสี่ยงภัยคุกคามทางไซเบอร์หรือ (Cyber Security Risk)

สำหรับการประเมินความเสี่ยงเกี่ยวกับ ภัยคุกคามทางไซเบอร์ หรือ (Cyber Security Risk) บริษัทได้ให้ความสำคัญของเรื่องนี้ เนื่องจากมีความเสี่ยงที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์กับบริษัทต่างๆ มากขึ้น

บริษัทจึงได้มีการแนวทางการบริหารความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risk) ดำเนินการและการแก้ไขปัญหาที่เกิดภัยคุกคามทางไซเบอร์ (Cyber Security Risk) ดังนี้

1. บริษัทได้มีการจัดหาระบบสำหรับการพิสูจน์ตัวตนและสิทธิ์ในการเข้าถึงระบบงานต่างๆของบริษัทแก่พนักงานทุกท่าน
2. เฝ้าระวังภัยคุกคามด้านไซเบอร์โดยผู้เชี่ยวชาญเฉพาะ จัดหาเครื่องมือและผู้เชี่ยวชาญในการเฝ้าระวังภัยคุกคามทางไซเบอร์ในภาพรวมของบริษัท และจัดทำรายงานการเฝ้าระวัง
3. ปรับปรุงวิธีการเข้าถึงระบบงาน ให้มีความปลอดภัยและเชื่อถือได้โดยกำหนดสิทธิ์การเข้าถึงตามหน้าที่และบทบาทของแต่ละคนเพื่อจัดความเสี่ยง โดยได้มีการพัฒนาและใช้เครื่องมือระบบต่างๆ ในการกำหนดสิทธิ์ เช่นการใช้ O365
4. นโยบายการให้บริการด้าน IT ให้มีความรัดกุมเพิ่มขึ้น ปิดระบบที่ไม่มีความจำเป็นต้องใช้งานในเวลากลางคืนที่ไม่มีเจ้าหน้าที่คอยเฝ้าระวัง
5. ปรับปรุงเวอร์ชันของระบบฐานข้อมูล Active Directory รองรับการพิสูจน์ตัวตนรูปแบบใหม่อื่นๆ ที่มีความปลอดภัยมากขึ้นในปัจจุบัน
6. จัดหาอุปกรณ์ Firewall ใหม่สำหรับศูนย์ข้อมูลหลัก เพิ่มประสิทธิภาพการป้องกันภัยคุกคามและทำให้บริการสามารถปรับเปลี่ยนได้อย่างรวดเร็ว
7. จัดหาระบบและผู้เชี่ยวชาญในการเฝ้าระวังภัยคุกคามทางไซเบอร์ในภาพรวมของบริษัททั้งหมด (Managed Detect and Respond) โดยพิจารณาจ้างบริษัท Alphasec เพื่อป้องกันการโจมตีทางด้าน Cyber
8. จัดหาระบบพิสูจน์ตัวตนและสิทธิ์ (Authentication, Authority) ของผู้ใช้งาน รวมถึงเครื่องคอมพิวเตอร์หรืออุปกรณ์ก่อนที่จะเข้าถึงระบบงานต่างๆ (Zero Trust Network Access) อยู่ระหว่างพิจารณาเลือกผลิตภัณฑ์ที่สามารถทำงานได้ตามต้องการเหมาะสมกับการลงทุน
9. จัดจ้างผู้เชี่ยวชาญด้าน พรบ.คุ้มครองข้อมูลส่วนบุคคลในการให้คำแนะนำ และทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท ประสานงานกับหน่วยงานรัฐ จัดให้มีการอบรมให้ความรู้เกี่ยวกับ พรบ. คุ้มครองข้อมูลส่วนบุคคลกับพนักงานทุกระดับเพื่อปฏิบัติให้ถูกต้องป้องกันการเกิดเหตุละเมิดข้อกฎหมาย
10. ย้ายการวางเครื่องที่ให้บริการไปยังระบบคลาวด์ และศูนย์ข้อมูลที่เป็นมาตรฐานสากล เพื่อลดความเสี่ยงด้านสภาพแวดล้อมและเพิ่มการเฝ้าระวังตามบริการมาตรฐานของผู้ให้บริการ (Architecture & Environment Monitoring) ดำเนินการย้ายศูนย์ข้อมูลหลักแล้วเสร็จประมาณ 40%
11. ปรับเปลี่ยนเวลาการให้บริการของระบบต่างๆ และการใช้งานอินเตอร์เนตของสาขาจากเดิมตลอด 24 ชั่วโมงเป็นเฉพาะเวลา 05:00-23:59 น. และยกเว้นในบางกรณี โดยจัดทำกับสาขาแล้ว 100%

ทำ Workshop กับทุกแผนกของบริษัท เพื่อปรับปรุงแก้ไขเอกสารเกี่ยวกับกิจกรรมการใช้ข้อมูลส่วนบุคคลของบิรษัท (ROPA) ให้เป็นปัจจุบัน รวมถึงเอกสารอื่นๆ ที่จำเป็นตาม พรบ. ทั้งในส่วนของกรรมการ ผู้บริหาร และพนักงานทุกแผนก