Strategic Oversight: The Board's Role in Setting the Cybersecurity & Privacy Agenda

นายกำพล ศรธนะรัตน์

นายกสมาคมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไทย

ขอบคุณหน่วยงานที่เรียกใช้งาน

- กรรมการและกรรมการสรรหาและกำหนดค่าตอบแทน สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย
- กรรมการอิสระ บริษัทเมืองไทยประกันภัย จำกัด (มหาชน)
- กรรมการผู้เชี่ยวชาญเรื่องร้องเรียน เกี่ยวกับการเงินและเศรษฐกิจ ตาม พรบ.คุ้มครองข้อมูลส่วน บุคคล และผู้เชี่ยวชาญเพื่อพิจารณาหลักสูตรและการฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วน บุคคลตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล
- ประธานอนุกรรมการบริหารเทคโนโลยีสารสนเทศและนวัตกรรม (IT Steering) บริษัท ไอร่า แคปปิตอล จำกัด (มหาชน)
- ประธานอนุกรรมการ IT Steering กองทุนเพื่อความเสมอภาคทางการศึกษา และที่ปรึกษา คณะกรรมการกองทุนเพื่อความเสมอภาคทางการศึกษา
- อนุกรรมการพัฒนาคุณภาพโรงเรียนทั้งระบบ /อนุกรรมการด้านการลงทุน / อนุกรรมการด้าน Data Governance กองทุนเพื่อความเสมอภาคทางการศึกษา
- อนุกรรมการบริหารความเสี่ยง สถาบันคุ้มครองเงินฝาก
- อนุกรรมการกลั่นกรองพิจารณาโครงการ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและ สังคมแห่งชาติ
- อนุกรรมการด้านยุทธศาสตร์ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)
- อนุกรรมการ IT Steering สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- ที่ปรึกษาคณะกรรมการดำเนินงานด้านการรับรองระบบควบคุมการประชุม (คณะกรรมการ รับรอง) สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
- กรรมการตัดสินรางวัล DG Awards (Digital Government Awards) ของสำนักงานพัฒนา รัฐบาลอิเล็กทรอนิกส์ (DGA)

นโยบาย Privacy & Cybersecurity: ความจำเป็นและความสำคัญ

- นโยบายเกี่ยวกับความปลอดภัยไซเบอร์และความเป็นส่วนตัว (Privacy & Cybersecurity) มีความสำคัญอย่างยิ่งในการปกป้องข้อมูลและระบบขององค์กรจากการโจมตีทางไซเบอร์และการละเมิดข้อมูล เพื่อให้มั่นใจว่าองค์กรมีการป้องกันที่เพียงพอและสามารถรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้

สรุป 9 เหตุการณ์การโจมตีทางไซเบอร์ที่เกี่ยวข้องกับ privacy (ตามข่าว)

ครั้งที่ 1 เดือนเมษายน 2561 : ข้อมูลลูกค้า TrueMove H หลุดรั่ว

ครั้งที่ 2 เดือนกันยายน 2563 : โรงพยาบาลสระบุรี ถูก Ransomware โจมตี

ครั้งที่ 3 เดือนมกราคม 2564 : ข้อมูลส่วนบุคคลของลูกค้า 3BB และช่อง MONO รั่วไหล

ครั้งที่ 4 เดือนสิงหาคม 2564 : Bangkok Airways ถูก Ransomware โจมตี

ครั้งที่ 5 เดือนกันยายน 2564 : สถาบันโรคไตภูมิราชนครินทร์ ถูกโจรกรรม ข้อมูลคนไข้

ครั้งที่ 6 เดือนกันยายน 2564 : CP Freshmart ถูกขโมยข้อมูลลูกค้า

ครั้งที่ 7 เดือนตุลาคม 2564 : Central Restaurant Group ถูกโจมตีทาง

ครั้งที่ 8 เดือนกุมภาพันธ์ 2565 : ข้อมูลนักเรียนไทยในระบบ TCAS รั่วไหล

ครั้งที่ 9 เดือนมีนาคม 2566 : แฮกเกอร์ 9near ประกาศขายข้อมูลคนไทย 55 ล้านคน

สรุป 9 เหตุการณ์การโจมตีทางไซเบอร์ครั้งใหญ่ในไทย | SOSECURE

การทำให้คณะกรรมการบริหารให้ความสำคัญกับภารกิจนี้

1. การนำเสนอข้อมูลที่ชัดเจนและเป็นระบบ:
   - ใช้ข้อมูลสถิติและตัวอย่างจากเหตุการณ์จริง
   - แสดงให้เห็นถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
2. การเสนอผลประโยชน์/โอกาสทางธุรกิจ:
   - เน้นย้ำถึงผลกระทบทางการเงิน บทลงโทษทาง กม ชื่อเสียงและภาพลักษณ์ที่อาจเกิดขึ้น
   - ชี้ให้เห็นถึงโอกาสในการปรับปรุงประสิทธิภาพการดำเนินงาน โอกาสทางธุรกิจ
3. การสร้างความเข้าใจในระดับผู้บริหาร/กรรมการ:
   - Board engagement
   - **เชิญผู้เชี่ยวชาญมาให้ข้อมูลและแนะนำแนวทางการปฏิบัติที่เหมาะสม**
   - จำลองสถานการณ์ fire drill / table top exercise

ชุดข้อมูลที่ใช้ในการนำเสนอ

- รายงานความเสี่ยงและการประเมินผลกระทบ
- ตัวอย่างเหตุการณ์จริง ที่ใกล้เคียงธุรกิจ ผลกระทบเชิงบวกและลบ
- ข้อมูลสถิติจากการวิจัยและรายงานจากองค์กรที่เชื่อถือได้ รวมถึงการทำ research / study เพื่อสร้างความน่าเชื่อถือ
- ชุดข้อมูลที่ทำให้ตระหนักใน Pain หรือสร้างโอกาสเชิงธุรกิจ

การสร้าง Mindset จาก 'Are We Secure?' เป็น 'Are We Ready?'

- 1. การเน้นย้ำความสำคัญของการเตรียมการให้มีความพร้อมรับมืออยู่เสมอ เพราะวันหนึ่งต้องเกิดกับเราไม่ว่าจะเตรียมความพร้อมขนาดไหนก็ตาม :
  - อธิบายให้คณะกรรมการเห็นว่าการรักษาความมั่นคงปลอดภัยไม่ใช่มีเพียงแค่มาตรการเชิงป้องกัน
  - ต้องมีการเตรียมพร้อมรับมือกับเหตุการณ์ที่อาจเกิดขึ้น
  - สร้างวัฒนธรรมการรายงาน การเปิดเผย หากเกิดเหตุการณ์หรือเป็นต้นเหตุให้เกิดเหตุ

- 2. การวางแผนการตอบสนอง:
  - มีแผน/คู่มือการตอบสนองต่อเหตุการณ์ที่ชัดเจนและเป็นรูปธรรม
  - ความจำเป็นของการมีทีมงานที่สามารถและพร้อมรับมือ

- 3. การฝึกซ้อมและทดสอบ:
  - จัดการฝึกซ้อมสถานการณ์จำลองทั้งแบบ table top execrcise และจำลองสถานการณ์จริง
  - ให้คณะกรรมการและทีมงานทราบบทบาท ตอบสนองได้ทัน ตัดสินใจได้ดี มีความพร้อมในการรับมือกับเหตุการณ์จริง

การรับมือกับความเสี่ยงภัยไซเบอร์ VS ข้อมูลรั่วไหล VS การลงทุน

1. การบริหารจัดการความเสี่ยง / การปฏิบัติตาม กม :
   - ความจำเป็นของการมีโครงสร้างรองรับ risk governance, data governance, cyber governance
   - มีแนวทางและเครื่องมือช่วย เช่น มีการประยุกต์กรอบการประเมินความเสี่ยงที่เป็นที่ยอมรับ เช่น NIST Cybersecurity Framework
   - ระบุความเสี่ยงที่สำคัญ จัดลำดับความสำคัญในการจัดการ และทำอย่างต่อเนื่องแบบมีพัฒนาการ
   - การตอบสนอง ที่ต้องมีการเตรียมความพร้อม ทดสอบและปรับปรุงอย่างสม่ำเสมอ
2. การจัดสรรงบประมาณ:
   - การสร้างความตระหนักอย่างต่อเนื่องและเท่าทัน
   - มีการลงทุนในเทคโนโลยี มาตรการที่มีประสิทธิภาพ และบุคลากรและการพัฒนา
   - มีการวิเคราะห์ความคุ้มค่า เพื่อประกอบการตัดสินใจลงทุน เช่น เปรียบเทียบค่าใช้จ่ายในการป้องกันกับค่าใช้จ่ายที่จะเกิดขึ้นหากเกิดเหตุการณ์ไซเบอร์
3. การสร้างวัฒนธรรมความร่วมมือ:
   - สร้างเครือข่ายการเรียนรู้ แลกเปลี่ยน
   - ส่งเสริมการทำงานร่วมกันระหว่างแผนกต่าง ๆ ในองค์กร เช่น IT, การเงิน, และกฎหมาย
   - สนับสนุนการแลกเปลี่ยนข้อมูลและประสบการณ์ระหว่างองค์กรในอุตสาหกรรมเดียวกัน

Q & A