Cybersecurity Enters the Boardroom

สรุปสัมภาษณ์งานเสวนา

Q: ประเด็นความเสี่ยงด้าน Cybersecurity ที่คณะกรรมการควรให้ความสำคัญ

A: "Cybersecurity" หรือ ความมั่นคงปลอดภัยทางไซเบอร์

คือ กระบวนการเพื่อปกป้องให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ซึ่งแต่เดิมก่อนที่จะมีสถานการณ์การแพร่ระบาดของ COVID-19 การลงทุนในระบบ Cybersecurity นับเป็นสิ่งที่จำเป็นต่อการดำเนินงานของทุกองค์กรอยู่แล้ว อย่างไรก็ตาม เมื่อมีสถานการณ์ COVID-19 เกิดขึ้น ถือเป็นการทวีความสำคัญของระบบ Cybersecurity เนื่องจากความจำเป็นของการที่ประชาชนจะต้องปฏิบัติตามมาตรการ Physical Distancing หรือการเว้นระยะห่างทางกายภาพ ทำให้องค์กรต่าง ๆ ต้องหันมาให้ความสำคัญกับการดำเนินงานผ่านระบบออนไลน์และใช้อุปกรณ์อิเล็กทรอนิกส์มากยิ่งขึ้น เช่น การทำงานที่บ้าน (Work From Home) ซึ่งเมื่อมีการใช้งานระบบออนไลน์ในรูปแบบและสถานที่ต่าง ๆ มากยิ่งขึ้น โอกาสที่จะเกิดความเสี่ยงด้านความปลอดภัยทาง Cyber ย่อมเพิ่มขึ้นไปด้วย

ดังนั้น สิ่งที่คณะกรรมการควรให้ความสำคัญคือ มาตรฐานความปลอดภัยด้านข้อมูลขององค์กรเพื่อป้องกันอันตรายทาง Cyber เช่น การขโมยข้อมูลไปใช้ประโยชน์ หรือการทำลายระบบ เป็นต้น Cyber Security จึงเข้ามาช่วยป้องกันและเป็นทางออกให้กับปัญหาเหล่านี้ ซึ่งแต่ละองค์กรอาจมีความพร้อมในการรับมือแตกต่างกัน

ตัวอย่างโอกาสในการเกิดอันตรายทาง Cyber

- ความปลอดภัยของการเชื่อมต่อระบบ VPN (Virtual Private Network) เพื่อให้พนักงานสามารถเข้าถึง Server ขององค์กรได้ ซึ่งหากระบบการเข้าถึงไม่ปลอดภัย เช่น ใช้รหัสผ่านชั้นเดียว อาจเป็นช่องทางให้บุคคลภายนอกเข้าไปขโมยข้อมูลได้
- การรับ-ส่ง E-mail อาจมีความเสี่ยงจากการพบ E-mail หลอกลวง หรือ Phishing Email
- ความปลอดภัยของอุปกรณ์ ซึ่งอาจมีการนำอุปกรณ์ส่วนตัวที่ไม่มีมาตรฐานมาใช้ร่วมกับอุปกรณ์ของสำนักงาน
- การใช้ Platform Online เช่น Microsoft Team, Zoom, Webex เพื่อใช้ประชุมออนไลน์ ซึ่งมักใช้วิธีการส่ง Link เชิญผู้เข้าร่วมประชุม จึงอาจเป็นช่องทางให้บุคคลภายนอกเข้ามาแทรกแซงได้

ดร.ฐิติพงศ์ นันทาภิวัฒน์
CIO บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.)
อดีตกรรมการ
การท่าเรือแห่งประเทศไทย ไปรษณีย์ไทย และ
บมจ.แกรนด์ แอสเสท โฮเทลส์ แอนส์ พรอพเพอร์ตี้
Facilitator หลักสูตร
IT Governance and Cyber Resilience Program (ITG)

คุณกุลเวช เจนวัฒนวิทย์
กรรมการผู้อำนวยการ
สถาบันกรรมการบริษัทไทย

Q: คณะกรรมการและฝ่ายจัดการควรทำงานร่วมกันอย่างไรเพื่อสร้างความมั่นใจในการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นและกำกับดูแลการปฏิบัติงานอย่างมีประสิทธิภาพ

A: คณะกรรมการมีบทบาทสำคัญในการกำกับดูแลฝ่ายจัดการเพื่อสร้างความมั่นใจว่า ความเสี่ยงด้าน Cyber ที่เกิดขึ้นใหม่จากการปรับเปลี่ยนพฤติกรรมในการทำงานมีการจัดการอย่างมีประสิทธิภาพ โดยประเด็นด้าน Cyber ที่คณะกรรมการควรให้ความสำคัญ มี 4 มิติ ได้แก่

Security

มาตรฐานความปลอดภัยของระบบภายในองค์กรเป็นไปตามมาตรฐานที่ได้รับการยอมรับเป็นการทั่วไปหรือไม่ เช่น ระบบ ISO เป็นต้น

Performance

ระบบที่องค์กรใช้งานอยู่สามารถทำให้บริษัทดำเนินงานได้อย่างมีประสิทธิภาพหรือไม่ เช่น พนักงานสามารถปฏิบัติงานได้ตามปกติหรือไม่ ลูกค้าสามารถใช้งานได้โดยสะดวกหรือไม่ เป็นต้น

Availability

ความพร้อมในการใช้งานเป็นอย่างไร เช่น ลูกค้าสามารถใช้งานได้ 24 ชั่วโมงหรือไม่ มีระบบสำรองหรือไม่ เป็นต้น

Compliance

การปฏิบัติตามกฎเกณฑ์และระเบียบต่าง ๆ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น โดยล่าสุด กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 27 พฤษภาคม 2563 เป็นต้นไป เพื่อแก้ไขปัญหาของการใช้ระบบ Video Conference

ดังนั้น เพื่อให้องค์กรมีมาตรฐานความปลอดภัยด้าน Cyber อย่างมีประสิทธิภาพ คณะกรรมการจึงควรกำกับดูแลฝ่ายจัดการในประเด็นดังนี้

01 การจัดประเภทและลำดับความสำคัญของข้อมูล

คณะกรรมการควรสอบถามฝ่ายจัดการให้มั่นใจว่า การดำเนินธุรกิจขององค์กรมีข้อมูลใดบ้างและมีลำดับความสำคัญอย่างไร อะไรคือข้อมูลที่มีความอ่อนไหว (Sensitive Data) มากที่สุด และมีมาตรฐานความปลอดภัยอย่างไร เช่น ในธุรกิจทางการแพทย์อาจเป็นข้อมูลส่วนบุคคลของคนไข้ หรือธุรกิจการเงินอาจเป็นธุรกรรมทางการเงินของลูกค้า เป็นต้น

02 สร้างความตระหนักด้านความปลอดภัยในองค์กรให้เกิดเป็นวัฒนธรรมการทำงาน

คณะกรรมการควรให้ความสำคัญในการสื่อสารเพื่อสร้างความตระหนักถึงความสำคัญของความปลอดภัย (Security Awareness) ผ่านรูปแบบและช่องทางต่าง ๆ เช่น การจัดทำนโยบาย Townhall เสียงตามสาย เป็นต้น เพื่อให้พนักงานเข้าใจและเห็นถึงความสำคัญของมาตรฐานความปลอดภัย อันจะทำให้เกิดความระวังระวังในการดำเนินงานทุกขั้นตอน และกลายเป็นวัฒนธรรมการทำงานปกติ

Q: สิ่งสำคัญที่คณะกรรมการควรคำนึงถึงในการดำเนินธุรกิจในโลกที่เปลี่ยนแปลงไปหลังจากสถานการณ์ COVID-19 (Next Normal)

A: 1. มาตรฐานความปลอดภัย

เมื่อสำนักงานมีการเปิดทำการตามปกติ การกลับเข้ามาใช้ระบบต่าง ๆ ของบริษัทต้องคำนึงถึงความปลอดภัยเป็นลำดับแรก โดยควรมีการตรวจสอบระบบความปลอดภัยต่าง ๆ อย่างเคร่งครัด เช่น การสแกนไวรัส การตรวจสอบ Server การตรวจสอบอุปกรณ์ เป็นต้น

2. การลงทุนด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ (IT Security Investment)

โดยคาดการณ์พฤติกรรมการดำเนินงานและการดำเนินธุรกิจที่เปลี่ยนแปลงไป เช่น การให้พนักงาน Work From Home มากขึ้น การทำธุรกรรมออนไลน์ เป็นต้น เพื่อที่จะได้จัดสรรงบประมาณและทรัพยากรในการบริหารจัดการที่เกี่ยวข้อง ทั้งในแง่ของ Hardware Software หรือบุคลากร อย่างไรก็ตาม ด้วยสถานการณ์ทางเศรษฐกิจอาจทำให้แต่ละบริษัทมีความพร้อมทางด้านการเงินที่แตกต่างกัน ดังนั้น คณะกรรมการจึงควรร่วมกับฝ่ายจัดการจัดลำดับความจำเป็นเพื่อให้การดำเนินธุรกิจไปต่อได้อย่างมีประสิทธิภาพ เช่น อาจเริ่มต้นจากการทำแบบประเมินรูปแบบพฤติกรรมและความพร้อมของพนักงานปัจจุบัน เนื่องจากความต้องการและความจำเป็นของพนักงานในส่วนงานต่าง ๆ อาจมีความแตกต่างกัน เพื่อวางแผนในการทำงานให้เหมาะสมกับสถานการณ์

3. การมอบหมายหน้าที่ความรับผิดชอบ

คณะกรรมการควรหารือกับฝ่ายจัดการถึงปัญหาหรือเหตุการณ์ความผิดปกติที่เกิดขึ้นในการใช้ระบบ Cyber ของบริษัท เพื่อประเมินความเป็นไปได้และวางแผนในการบริหารจัดการ โดยอาจพิจารณาจัดตั้งทีม Incident Respond ประกอบด้วยผู้แทนจากหน่วยงานที่เกี่ยวข้อง เช่น ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายกฎหมาย ฝ่ายการเงิน เป็นต้น เพื่อให้มีผู้รับผิดชอบและช่องทางที่ชัดเจนในรับมือกรณีเกิดเหตุการณ์ต่าง ๆ