SET | Make it **Work** for **Everyone**

ภัยคุกคามทางไซเบอร์
เรื่องที่คณะกรรมการไม่ควรมองข้าม

ปัจจุบันมนุษย์ดำเนินชีวิตโดยมีเทคโนโลยีเป็นส่วนประกอบของชีวิตประจำวันอย่างแยกออกจากกันไม่ได้ จากการสำรวจล่าสุด ประชาชน 85.1% ของประเทศ ใช้งานอินเตอร์เน็ตเฉลี่ย 6-10 ชั่วโมงต่อวัน[1] โดยในภาคการผลิตเองก็ไม่ต่างกัน จากการคาดการณ์ของ McKinsey พบว่าการลงทุนใน IoT ของกลุ่มอุตสาหกรรมทั่วโลก ภายในช่วงปี 2020-2025 มีแนวโน้มสูงขึ้น 12 % ต่อปี[2] ซึ่งยิ่งแสดงให้เห็นว่าสังคมมนุษย์กำลังหลอมรวมเข้ากับเทคโนโลยีอย่างขาดกันไม่ได้

อย่างไรก็ตามอินเตอร์เน็ตก็ไม่ได้มีเพียงแค่ข้อดี แต่ยังนำมาซึ่งการฉกฉวยโอกาสข้อผู้ไม่ประสงค์ดีโดยอาศัยช่องโหว่ของระบบด้วยเช่นกัน ยกตัวอย่างเช่น กรณีโรงพยาบาลสระบุรีที่ถูก Ransomware ทำให้ไม่สามารถเข้าถึงข้อมูลต่างๆ ของคนไข้ หรือในกรณีของบริษัทในตลาดหลักทรัพย์ฯ อย่าง บริษัท สตาร์ ปิโตรเลียม รีไฟน์นิ่ง จำกัด (มหาชน) ที่ถูก Phishing email ทำให้ Hacker ได้ข้อมูลจนทำให้บริษัทสูญเงินไปกว่า 700 ล้านบาท เป็นต้น

เห็นได้ว่ากรณีที่ยกตัวอย่างมานั้นก่อให้เกิดความเสียหายต่อองค์กรทั้งทางการเงินและชื่อเสียงอย่างมาก จึงปฏิเสธไม่ได้เลยว่าบริษัทจดทะเบียนในตลาดหลักทรัพย์ฯ นั้นจำเป็นที่จะต้องให้ความสำคัญกับเรื่องนี้ โดยเฉพาะผู้ที่มีหน้าที่กำหนดทิศทางของบริษัทอย่างคณะกรรมการ ควรศึกษาและให้ความสำคัญกับ Cybersecurity เป็นอย่างยิ่ง

จากการเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็วส่งผลให้หลาย**ธุรกิจต้องเร่งปรับตัว (Transformation)** ทั้งในเรื่องรูปแบบการทำธุรกิจ, กระบวนการทำงาน และระบบภายในของบริษัท ซึ่งถูกกดดันจากทั้งเรื่องของเวลาและงบประมาณจนอาจทำให้คณะกรรมการหรือผู้บริหารละเลยที่จะนำ Cybersecurity เข้าไปเป็นส่วนหนึ่งในการพิจารณาแผนการปรับตัวของบริษัท ทั้งนี้ จากการสำรวจของ Ernst & Young พบว่าผู้บริหารกว่า 81%[3] ยอมรับว่า COVID-19 ทำให้บริษัทต้องปรับตัวอย่างรวดเร็ว โดยทำให้ต้องข้ามขั้นตอนทาง Cybersecurity ต่างๆ ที่บริษัทมี ก่อเกิดความเสี่ยงทางไซเบอร์สูงขึ้นเป็นอย่างมาก รวมไปถึงมีผู้บริหารเพียง 9%[4] เท่านั้นที่มั่นใจว่าระบบ Cybersecurity ของบริษัทสามารถป้องกัน Cyberattack ในโลกยุคใหม่ได้เป็นอย่างดี ซึ่งความเชื่อมั่นนี้ลดลงจากการสำรวจเมื่อปี 2020 ถึง 11%

ภาครัฐเองก็ตระหนักถึงความสำคัญของ Cybersecurity โดยได้ออก พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 โดยสาระสำคัญคือแนวทางในการจัดการ การป้องกัน การรับมือ และการลดความเสี่ยงทางไซเบอร์ ซึ่งจะเป็นจุดเริ่มต้นในการผลักดันให้เกิดการพัฒนา Cybersecurity ในด้านต่างๆ ที่ขยายผลไปถึงภาคเอกชนด้วยเช่นกัน

สำหรับบริษัทจดทะเบียน ตาม CG Code ปี 2560 ได้มีการบรรจุเรื่องความปลอดภัยทางไซเบอร์เอาไว้ โดยแนะนำให้คณะกรรมการดูแลให้การบริหารความเสี่ยงขององค์กรครอบคลุมถึงเรื่องเทคโนโลยีสารสนเทศ และจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

นอกจากนี้เกณฑ์**การประเมินรายงานการกำกับดูกิจการที่ดีสำหรับบริษัทจดทะเบียนฉบับใหม่** ที่จะมีผลในปี 2566 ได้มีการประเมินการเปิดเผยข้อมูลนโยบายทางด้าน IT Security และ การติดตามการปฏิบัติ เช่น แผนงานผลการปฏิบัติ การจัดสรรทรัพยากร เป็นต้น

สำหรับตัวบริษัทเองนั้นสามารถเริ่มต้นปรับตัว เพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยีได้จากการกำหนดนโยบาย Cybersecurity ซึ่งควรมีเนื้อหาครอบคลุมตั้งแต่ จุดมุ่งหมายของการจัดทำนโยบาย มีใครที่เกี่ยวข้องกับนโยบายบ้าง กระบวนการป้องกันต่างๆ ที่บริษัทจะนำมาใช้ การประเมินความเสี่ยงด้านไซเบอร์ที่จะส่งผลต่อตัวกิจการ การตรวจสอบระบบรักษาความปลอดภัย การจัดตั้งหน่วยงานรับผิดชอบ จนถึงวิธีการสื่อสารให้พนักงานได้รับทราบ เป็นต้น ทั้งนี้การมี **นโยบายด้าน Cybersecurity อย่างเดียวยังไม่เพียงพอ** องค์กรควรจัดตั้งให้มีหน่วยงานรับผิดชอบในการติดตามดูแลด้าน Cybersecurity ขึ้นมาเป็นการเฉพาะ เพื่อวิเคราะห์การดำเนินงานขององค์กรเทียบกับกฎหมายและข้อบังคับต่างๆ ตรวจสอบและวัดระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร และจัดอบรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงาน

ถ้าองค์กรของท่านยังไม่ได้เนินการใดๆ เลย อย่านิ่งนอนใจ **เรื่องความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่เรื่องเล็กๆ ต่อไปสำหรับยุคดิจิทัลวิถีใหม่นี้แล้ว**

1: https://workpointtoday.com/internet01/

2: McKinsey & Company (February 2021)

3: https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

4: https://www.ey.com/en_gl/global-board-risk-survey