สรุปสาระสำคัญของการบรรยายเรื่อง Cyber Security and Cyber Forensics โดย Mr.Andre Arnes (Chief Security Officer, Telenor Group)

† Cyber Security คือการป้องกันระบบที่เชื่อมต่อกับอินเตอร์เน็ต ทั้งส่วนของ hardware, software และ data จากภัยคุกคามทางไซเบอร์ ซึ่งต้องอาศัยความมั่นคงปลอดภัยด้านข้อมูลและด้านอุปกรณ์ Physical

† Cyber Attack ถือเป็นภัยระดับสากลที่ผู้นำต้องให้ความสำคัญอย่างสูงสุดในขณะนี้

† แนวโน้ม Cyber Attack มีเพิ่มขึ้นจากกระแส digital transformation โดยพัฒนารูปแบบที่หลากหลาย เช่น ransomeware, malware, virus, phishing, spear phishing เป็นต้นรวมทั้งทวีความรุนแรงยิ่งขึ้น

† ผู้ที่ก่อเหตุ Cyber Attack อาจจัดกลุ่มได้ตามระดับความอันตรายจากมากไปน้อยได้ดังนี้

1. Nation
2. Contractors
3. Organized Crime
4. Hacktivism
5. Crime & Fraud

† การป้องกันภัยไซเบอร์

- ผู้รับผิดชอบในการป้องกันภัยไซเบอร์ คือทุกคนในองค์กร เริ่มตั้งแต่คณะกรรมการ ผู้บริหาร จนถึงผู้ปฏิบัติงานทุกคน มิใช่แค่ฝ่ายเทคโนโลยีสารสนเทศเท่านั้น
- หน่วยงานต้องมีการวิเคราะห์ว่าสิ่งมีค่าใดในองค์กรที่อาจถูกคุกคาม ใครจะเป็นผู้คุกคาม ผ่านช่องทางใด เพื่อจะได้เตรียมการรับมือไว้แต่เนิ่นๆ
- การเตรียมการทั้งเรื่องบุคลากร กระบวนการ ระบบงาน ให้คำนึงถึงความเสี่ยง และคิดมาตรการควบคุมประกอบกันไป โดยควรเตรียมการแบบ proactive (เชิงป้องกัน)ดีกว่า reactive (เชิงบรรเทา) ทั้งนี้ Human Firewall เป็นสิ่งสำคัญที่สุด แม้องค์กรจะมีอุปกรณ์และระบบป้องกันที่ล้ำสมัย แต่หากบุคลากรขาดความตระหนักรู้ ขาดความใส่ใจ ก็ส่งผลให้องค์กรตกเป็นเหยื่อของภัยไซเบอร์ได้

- องค์กรอาจนำมาตรฐานสากลที่เกี่ยวข้องมาใช้ในการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น GSMA, NIST, ISO 27001

- ตัวอย่างแผนกลยุทธ์ในการจัดการความมั่นคงปลอดภัยของ Telenor

2016 เริ่มสร้างพื้นฐานการมีส่วนร่วมโดยสื่อสารให้ผู้ปฏิบัติงานในโครงการสำคัญเข้าใจเรื่องการรักษาความมั่นคงปลอดภัย
2017 ทยอยลด gap ในด้าน capability & governance
2018 สร้าง mindset ในการทำธุรกิจที่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัย
2019 เน้นการบริหารจัดการความมั่นคงปลอดภัยที่มีประสิทธิผลและ scalable
2020 มุ่งสู่การเป็นผู้นำด้านการบริหารจัดการความมั่นคงปลอดภัย

† Cyber Forensics คือการนำวิธีการทางวิทยาศาสตร์ที่ผ่านการรับรองแล้วมาใช้เพื่อรักษา จัดเก็บ พิสูจน์ ระบุ วิเคราะห์ แปลความ จัดทำเอกสารและการนำเสนอ หลักฐานดิจิทัลที่มาจากแหล่งข้อมูลดิจิทัล เพื่อช่วยในการสืบหาผู้กระทำความผิด ซึ่งต้องดำเนินการสืบสวนอย่างรวดเร็ว โดยคำนึงถึงการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้วย

† ข้อเสนอแนะในการพัฒนา Cyber Security

- การสร้างความร่วมมือ : เนื่องจากการที่แต่ละหน่วยงานลงทุนสร้างระบบป้องกันภัยไซเบอร์เองจะมีต้นทุนสูงมาก ภาครัฐจึงควรเป็นผู้ดำเนินการในการสร้างหน่วยงานกลางโดยอาศัยความร่วมมือระหว่างภาครัฐและเอกชนมาดำเนินการและให้การสนับสนุนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ตัวอย่างเช่น ใน Norway ภาครัฐจัดตั้ง Cyber Security Center เพื่อธุรกิจ SME โดยไม่คิดค่าบริการ หรือคิดในอัตราที่ถูกมาก รวมทั้งควรส่งเสริมการแลกเปลี่ยนข้อมูลระหว่างองค์กรเพื่อให้รู้ทันและดำเนินการจัดการภัยไซเบอร์ได้
- การพัฒนาศักยภาพ : สร้างคนที่มีความรู้ความสามารถในการบริหารจัดการ Cyber Security รวมทั้งส่งเสริมความรู้ความเข้าใจของสาธารณชนเกี่ยวกับเรื่องดังกล่าว เพื่อสร้างความตระหนักรู้
- การออกกฎระเบียบ : หน่วยงานกำกับดูแลควรออกกฎที่มีความยืดหยุ่นเพียงพอเพื่อให้ธุรกิจสามารถปรับตัวได้อย่างรวดเร็วตามสถานการณ์ที่เปลี่ยนแปลงไปได้ เนื่องจากการพัฒนาเทคโนโลยีสารสนเทศใหม่ๆ ต้องอาศัยกลไกที่ dynamics นอกจากนี้ ต้องมีการวิเคราะห์ความเสี่ยงของเทคโนโลยีที่สร้างใหม่ เพื่อรับมือกับความเสี่ยงด้วย รวมทั้งส่งเสริมการปฏิบัติตามมาตรฐานสากลด้าน Cyber Security ตลอดจนสร้างกรอบแนวทางในการเตรียมความพร้อมรองรับ cyber security, cyber attack และการทำ cyber forensics ให้ชัดเจน