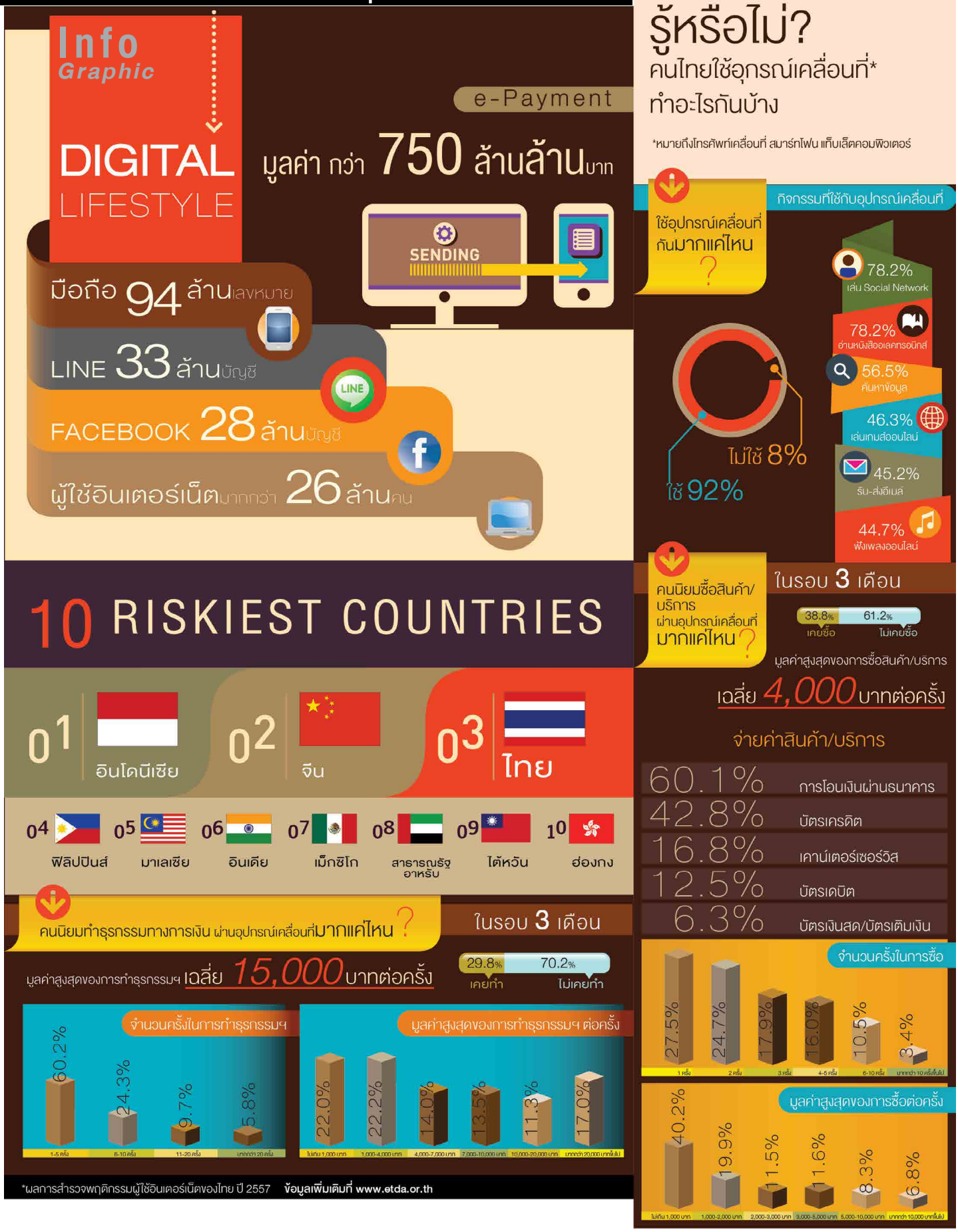
อินเทอร์เน็ตกับภัยคุกคามไซเบอร์



รู้หรือไม่?

คนไทยใช้อุปกรณ์เคลื่อนที่* ทำอะไรกันบ้าง

*หมายถึงโทรศัพท์เคลื่อนที่ สมาร์ทโฟน แท็บเล็ตคอมพิวเตอร์

ใช้อุปกรณ์เคลื่อนที่กันมากแค่ไหน?

ใช้ 92%

ไม่ใช้ 8%

กิจกรรมที่ใช้กับอุปกรณ์เคลื่อนที่

- 78.2% เล่น Social Network
- 78.2% อ่านหนังสืออิเลคทรอนิกส์
- 56.5% ค้นหาข้อมูล
- 46.3% เล่นเกมส์ออนไลน์
- 45.2% รับ-ส่งอีเมล์
- 44.7% ฟังเพลงออนไลน์

คนนิยมซื้อสินค้า/บริการผ่านอุปกรณ์เคลื่อนที่มากแค่ไหน?

ในรอบ 3 เดือน

38.8% เคยซื้อ

61.2% ไม่เคยซื้อ

มูลค่าสูงสุดของการซื้อสินค้า/บริการ เฉลี่ย 4,000 บาทต่อครั้ง

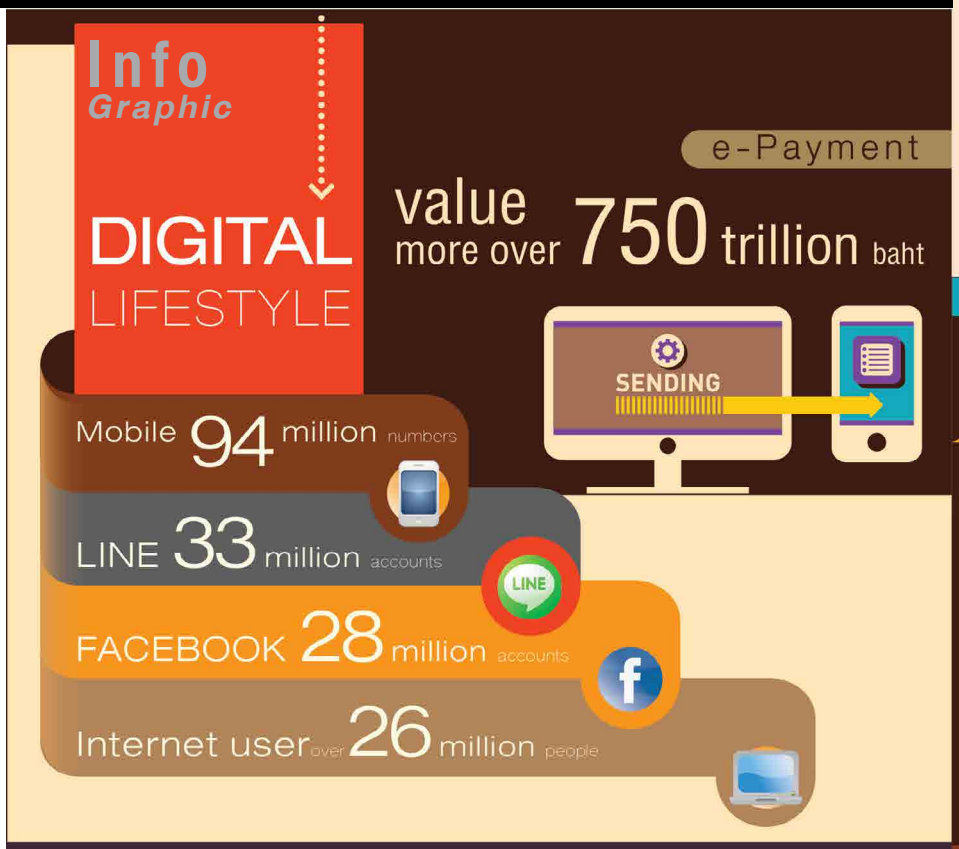
จ่ายค่าสินค้า/บริการ

- 60.1% การโอนเงินผ่านธนาคาร
- 42.8% บัตรเครดิต
- 16.8% เคาน์เตอร์เซอร์วิส
- 12.5% บัตรเดบิต
- 6.3% บัตรเงินสด/บัตรเติมเงิน

จำนวนครั้งในการซื้อ

มูลค่าสูงสุดของการซื้อต่อครั้ง

Cybersecurity



*ผลการสำรวจพฤติกรรมผู้ใช้อินเตอร์เน็ตของไทย ปี 2557 **ข้อมูลเพิ่มเติมที่ www.etda.or.th**

Cybersecurity

ปัจจุบันข้อมูลข่าวสารในโลกส่งผ่านกันอย่างรวดเร็วเพียงปลายนิ้วสัมผัส โลกเหมือนถูกย่อส่วนให้เล็กลง การติดต่อสื่อสาร และการดำเนินธุรกิจเป็นไปด้วยความรวดเร็ว ด้วยเทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันของคนในโลก ทุกคนมีอุปกรณ์สื่อสารติดตัว องค์กรที่เป็นแนวหน้านำเทคโนโลยีมาใช้ประโยชน์เพื่อแย่งชิงความเป็นหนึ่งทางธุรกิจ แม้แต่องค์กรขนาดเล็กก็มีเรื่องต้องเกี่ยวข้องกับเทคโนโลยี ทุกองค์กรใช้คอมพิวเตอร์ในการทำงานและการเก็บข้อมูล แม้ผู้ประกอบการ SMEs ก็ใช้เทคโนโลยีในการทำธุรกิจ ดังเช่นที่เราเห็นการขายสินค้าออนไลน์ที่ประสบความสำเร็จมากมาย

การที่เทคโนโลยีเข้ามามีบทบาทอย่างมากนั้น สิ่งที่เพิ่มเติมมาด้วยกันคือความเสี่ยงทางด้านเทคโนโลยีที่มีมากขึ้น ภัยคุกคามในโลกไซเบอร์ การแฮกข้อมูล การปล่อยไวรัส การใช้ประโยชน์จากข้อมูลอย่างไม่ถูกต้อง เป็นเรื่องที่หลายองค์กรไม่ได้ตระหนักถึงคณะกรรมการผู้มีบทบาทสำคัญในการกำกับดูแลองค์กรเพื่อประโยชน์สูงสุดต่อผู้มีส่วนได้เสียทุกฝ่าย จึงไม่สามารถที่จะละเลยหรือมองข้ามความเสี่ยงเกี่ยวกับเรื่องนี้ได้เลย ความเสียหายที่เกิดขึ้นอาจไม่ใช่เพียงธุรกิจหยุดชะงัก แต่เป็นความเสียหายที่คงอยู่ระยะยาวเช่นการเสียชื่อเสียง การเสียความเชื่อมั่นของผู้ถือหุ้น เป็นต้น

Boardroom ฉบับนี้จึงได้นำประเด็นเรื่องการกำกับดูแลกิจการด้านเทคโนโลยีและความปลอดภัยทางด้านเทคโนโลยีมาเป็นประเด็นที่จะให้คณะกรรมการเห็นภาพที่ชัดเจนมากขึ้น จากการที่ IOD ได้นำสมาชิกและตัวแทนจากหน่วยงานกำกับดูแลเข้าร่วมการประชุม Global Cyber Summit ที่ประเทศสหรัฐอเมริกาเมื่อเดือนเมษายนที่ผ่านมา ซึ่งจัดโดย Global Institute of Directors ซึ่งมี IOD จากทั่วโลกร่วมเป็นสมาชิก ซึ่ง IOD ประเทศไทยได้เข้าร่วมเป็นสมาชิกเมื่อปีที่ผ่านมา ในการประชุมมีคณะกรรมการจากทั่วโลกเข้าร่วมรับฟังและแลกเปลี่ยนความคิดเห็น ซึ่งเห็นว่า คณะกรรมการในต่างประเทศให้ความสำคัญกับเรื่องนี้เป็นอย่างมาก IOD จึงนำสรุปประเด็นสำคัญจากการเข้าร่วมการสัมมนา และได้ไปสัมภาษณ์หน่วยงานกำกับดูแล ผู้เชี่ยวชาญ และภาคธุรกิจ เพื่อให้คณะกรรมการเข้าใจและเห็นความสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีมากขึ้น

บทสรุปจากการสัมมนามีสาระสำคัญดังนี้

ความเสี่ยงด้านเทคโนโลยี เป็นเรื่องที่ทุกองค์กรต้องเผชิญ

ความเสี่ยงทางเทคโนโลยีนั้นไม่ใช่เพียงเรื่องของระบบเทคโนโลยีสารสนเทศ แต่รวมถึงเรื่องข้อมูลในระบบ ในโลกปัจจุบันข้อมูลได้ส่งผ่านไปทั่วโลกอย่างรวดเร็ว คณะกรรมการต้องทราบว่าอะไรเป็นข้อมูลที่สำคัญ (Critical Data) ขององค์กร ซึ่งการจัดการความเสี่ยงด้านเทคโนโลยีนั้น อาจดำเนินการตามแนวทางคือ ระบุหาสาเหตุป้องกัน ติดตามตอบสนอง และฟื้นฟู (Identify, Protect, Detect, Response and Recover) ซึ่งไม่ใช่หน้าที่ของผู้บริหารที่ดูแลเท่านั้น แต่รวมถึงคณะกรรมการและผู้บริหารของทุกหน่วยงานในเรื่องความปลอดภัยด้านข้อมูลคณะกรรมการควรถามตนเองว่า...

คณะกรรมการและผู้บริหารที่ดูแลงานด้านนี้อยู่สามารถตอบคำถามเหล่านี้ได้หรือไม่?

ทราบหรือไม่ว่าอะไรเป็นข้อมูลที่มีความสำคัญที่สุดขององค์กร?

เรามีการจัดการข้อมูลเหล่านั้นอย่างไรบ้าง?

มีการจัดระบบการควบคุมข้อมูลอย่างไร?

ถ้าเกิดเหตุผิดปกติขึ้นเรามีแผนการรับมืออย่างไร?

ใครที่สามารถเข้าถึงข้อมูลได้บ้าง?

พนักงานที่เข้าถึงข้อมูลในองค์กรจะมีระบบในการควบคุมอย่างไรไม่ให้ข้อมูลรั่วไหล? เนื่องจากพฤติกรรมของพนักงานในปัจจุบันทุกคนมีเครื่องมือสื่อสารติดตัวตลอด (Bring your own device) ที่อาจทำให้ข้อมูลออกไปภายนอกองค์กร หรือถูกการโจมตีจากผู้ไม่ประสงค์ดี

เมื่อมีการควบรวมกิจการข้อมูลที่สื่อสารระหว่างกันควรจะมีอะไรบ้าง

ข้อมูลใดที่มีการแลกเปลี่ยนกันระหว่างคู่ค้าหรือบุคคลภายนอก

หากข้อมูลเก็บรักษาไว้นอกประเทศ มีการศึกษา กฎหมายและระเบียบที่แตกต่างกันหรือไม่ เก็บข้อมูลไว้ที่ไหน เก็บอะไรบ้าง มีความจำเป็นที่ต้องเก็บหรือไม่ และมีการประเมินความเสี่ยงของข้อมูลที่เก็บหรือไม่ เช่น อีเมล์ ภาพ เสียงบันทึกต่าง ๆ

ข้อมูลลูกค้าที่นำมาใช้ได้ปกป้องความเป็นส่วนตัวของลูกค้ามากขนาดไหน โดยถามคำถามได้ว่าทำไมจะต้องเก็บข้อมูลเหล่านั้น อะไรเป็นประเด็นเรื่องข้อมูลความเป็นส่วนตัวที่สำคัญ หน่วยงานใดที่เป็นเจ้าของข้อมูลคู่ค้าที่มีข้อมูลร่วมกันปกป้องความเป็นส่วนตัวของลูกค้าหรือไม่

ประเด็นที่น่าสนใจ คือ ในอดีตคณะกรรมการอาจมองการจัดการด้านเทคโนโลยีเป็นเรื่องค่าใช้จ่ายขององค์กร แต่ปัจจุบันควรจะปรับมุมมองเป็นเรื่องการลงทุน ว่าจะลงทุนเท่าไหร่ และลงทุนอย่างไรโดยเร็วที่สุด หลายครั้งปัญหาเรื่องความเสี่ยงด้านเทคโนโลยีไม่ใช่เรื่องเทคนิคแต่ผู้นำองค์กรขาดการให้ความสำคัญ จนเมื่อเกิดปัญหาก็ขาดการเตรียมพร้อมอย่างดี การดำเนินงานเรื่องนี้คณะกรรมการจึงต้องปรับมุมมองให้เป็นเรื่องของการคาดการณ์ล่วงหน้าและมีแผนการรองรับ

ตัวอย่างหนึ่งที่พบคือการโดนแฮกเกอร์เข้ามาโจมตีระบบ ในต่างประเทศเช่นในสหรัฐอเมริกาเจอกับกรณีนี้มาก ความท้าทายในการจัดการความเสี่ยงด้านเทคโนโลยีคือการที่เราจัดการกับสิ่งที่มองไม่เห็นด้วยตา เช่น ไวรัส การโจมตีระบบคอมพิวเตอร์ทุกตัวสามารถโดนโจมตีระบบได้ซึ่งผู้ที่โจมตีนั้นมีเป้าหมายชัดเจนว่าจะเจาะข้อมูลในระดับใด ต้องการข้อมูลอะไรบ้าง ผู้ร่วมบรรยาย ***Ms. Kim Zetter*** ผู้เขียนหนังสือ *Countdown to Zero Day: Stuxnet and the Launch of World's First Digital Weapon* ได้นำกรณีศึกษามาแบ่งปันเรื่องมัลแวร์ Stuxnet ที่เกิดขึ้นกว่าสิบปีที่แล้ว เป็นการเขียนโค้ดเพิ่ม 21 บรรทัดในโปรแกรมควบคุมระบบผลิตไฟฟ้า ซึ่งทำให้ระบบผลิตไฟฟ้าสามารถหยุดทำงานได้ มัลแวร์นี้สามารถกระจายในคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการแบบ Window เป้าหมายคือเพื่อปิดการทำงานของระบบ Protective Delay ทำให้การทำงานผิดจากปกติ ค่อย ๆ ลดประสิทธิภาพการทำงานของระบบจนกระทั่งระบบไม่สามารถทำงานต่อไปได้ ตัวอย่างชี้ให้เห็นว่าการขาดการป้องกันและให้ความสนใจเกี่ยวกับเรื่องความเสี่ยงด้านเทคโนโลยีอาจจะทำให้เกิดผลเสียกับองค์กรได้ บริษัทปัจจุบันอาจแบ่งได้เป็น 2 ประเภท คือบริษัทที่โดนขโมยข้อมูลแต่ยังไม่ทราบ กับบริษัทที่โดนขโมยข้อมูลและทราบแล้ว

ความเสี่ยงด้าน IT เป็นความเสี่ยงภาพรวมธุรกิจ

คณะกรรมการควรเล็งเห็นเรื่องความเสี่ยงด้านเทคโนโลยีเป็นหนึ่งในความเสี่ยงสำคัญของภาพรวมองค์กร (Enterprise - Wide Risk) ไม่ใช่ความเสี่ยงแค่เรื่องเทคโนโลยีหรือเรื่องทางเทคนิคที่ให้ฝ่ายไอทีเท่านั้นคอยดูแลจัดการ คณะกรรมการมองเป็นเรื่องของธุรกิจภาพรวม ไม่ใช่แยกออกมาเป็นความเสี่ยงที่ไม่เกี่ยวข้องกับธุรกิจ คณะกรรมการจึงต้องเข้าใจเรื่องของความเสี่ยงไม่ใช่เข้าใจเรื่องของเทคโนโลยี แต่เป็นส่วนหนึ่งกระบวนการทางธุรกิจ (Business Process) ทั้งหมดซึ่งอาจจะเริ่มจากการมองว่า

ควรหรือไม่ที่โครงสร้างคณะกรรมการจะมีผู้เชี่ยวชาญด้านเทคโนโลยี

เรื่องความเสี่ยงด้านเทคโนโลยีควรจะเป็นเรื่องคณะกรรมการชุดใหญ่กำกับดูแลหรือไม่ หรือให้เป็นบทบาทหน้าที่ของคณะกรรมการตรวจสอบเท่านั้น

คณะกรรมการควรจะได้รับความรู้เพิ่มเติมเกี่ยวกับเรื่องเทคโนโลยีหรือไม่?

คณะกรรมการไม่ควรที่จะกลัวในการที่จะถามคำถามที่ตนเองไม่ทราบ เช่น คำศัพท์ด้านไอทีต่างๆ ดังนั้นควรจะมีการจ้างที่ปรึกษาหรือผู้เชี่ยวชาญมาทำความเข้าใจกับคณะกรรมการมากขึ้นหรือไม่?

คณะกรรมการควรจ้างผู้เชี่ยวชาญที่มีความอิสระมาช่วยกำกับดูแลฝ่ายบริหารที่ดูแลเรื่องนี้หรือไม่?

องค์กรของเรามีทรัพยากรเพียงพอหรือไม่ ทั้งงบประมาณและบุคคลากร?

หากบริษัทเป็นเป้าหมายในการโจมตี บริษัทมีความพร้อมที่จะรับมือหรือไม่ อะไรเป็นความเสียหายที่ร้ายแรงที่สุดที่อาจเกิดขึ้นได้ จะตอบสนองต่อการโจมตีอย่างไร?

ความเสี่ยงด้านเทคโนโลยีควรเป็นความเสี่ยงระดับไม่เกิน 1-10 ของทุกองค์กรในปัจจุบัน และควรเห็นภาพที่เชื่อมกับความเสี่ยงอื่นๆ คณะกรรมการควรมองให้เห็นว่าผู้บริหารที่ดูแลเห็นความสำคัญและมีความสามารถรับมือกับความเสี่ยงนั้นได้จริงหรือไม่ ซึ่งคณะกรรมการอาจจะมีการพิจารณาแต่งตั้งคณะอนุกรรมการดูความเสี่ยงในเรื่องนี้หากเป็นความเสี่ยงที่มีความสำคัญระดับต้นๆ ขององค์กร และควรให้ทุกหน่วยงานเห็นความสำคัญและมีส่วนร่วมในการจัดการความเสี่ยงเรื่องนี้

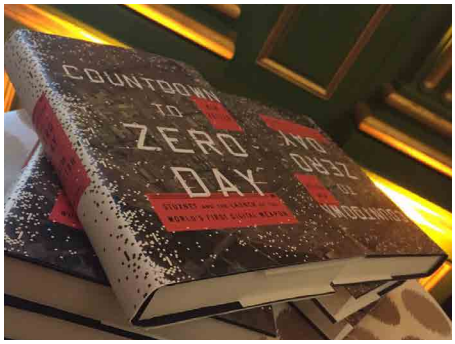
การสื่อสารมีความสำคัญ

การสื่อสารเป็นสิ่งที่สำคัญในการดำเนินงานขององค์กรทุกเรื่อง เรื่องของเทคโนโลยีก็เช่นเดียวกัน หากมีประเด็นใดที่องค์กรเป็นเป้าเสี่ยงต่อการโจมตีหรือคุกคามจะต้องสื่อสารกับหน่วยงานรัฐที่เกี่ยวข้อง การสื่อสารระหว่างภาคเอกชนและภาครัฐมีความสำคัญมากเพื่อให้ภาครัฐสามารถหาทางป้องกันได้ แต่การสื่อสารไปยังสาธารณชนผ่านสื่อมวลชนต้องมีความระมัดระวัง ควรที่จะให้ข้อมูลที่เพียงพอและจำเป็นเท่านั้น เพื่อไม่ให้เป็นเป้าหมายต่อการโจมตีของผู้ที่ไม่หวังดี

ตัวอย่างเช่น เมื่อข้อมูลรั่วไหลออกไปคณะกรรมการจะต้องเตรียมพร้อมว่า จะแจ้งลูกค้าทราบอย่างไร เมื่อไหร่ จะเปิดเผยข้อมูลมากน้อยเพียงใด และฝ่ายใดควรที่จะมาร่วมในการอธิบายกับกลุ่มลูกค้าบ้าง การให้ข้อมูลต่างๆ จะต้องระวังเรื่องความถูกต้อง ดังนั้นคณะกรรมการควรมีแผนการสื่อสารในสถานการณ์ฉุกเฉิน (Crisis Communication Plan) ควบคู่กับแผนกู้คืน (Crisis Recovery Plan) ภายในองค์กรจะต้องวางตัวขัดเจนว่าใครจะเป็นตัวแทนองค์กรที่จะสื่อสารกับสาธารณชน

นอกเหนือจากการสื่อสารภายนอก การสื่อสารกับบุคคลกรในองค์กรก็มีความสำคัญ ควรจะมีการฝึกซ้อมและอบรมให้ความรู้บุคคลากรทุกระดับ แต่ควรทำในรูปแบบที่น่าสนใจ เข้าใจง่าย เช่น การเล่นเกมส์

การสื่อสารระหว่างคณะกรรมการและผู้บริหารก็เป็นจุดที่สำคัญอย่างมาก การที่คณะกรรมการจะสามารถติดตามการดำเนินงานได้อย่างมีประสิทธิภาพ อาจจะมีการพิจารณาแต่งตั้งตำแหน่งในองค์กรได้แก่ Chief Information Officer (CIO) และ/หรือ Chief Information Security Officer (CISO) และเมื่อแต่งตั้งแล้วควรให้มีการสื่อสารและรายงานประเด็นต่างๆ ให้คณะกรรมการทราบอย่างต่อเนื่องเช่นเป็นประจำทุกเดือน หรือหากมีเหตุการณ์ที่ไม่ปรกติในเรื่องความมั่นคงปลอดภัยของไซเบอร์อาจให้มีการรายงานทุกสัปดาห์ และหากมีเหตุการณ์เกิดขึ้นคณะกรรมการควรสร้างวัฒนธรรมการยอมรับกล่าวคือไม่ต่อว่าผู้บริหารแต่รับฟังและร่วมแก้ปัญหาเพื่อให้ผู้บริหารกล้าที่จะสื่อสารสิ่งที่เกิดขึ้นอย่างแท้จริง โดยควรคิดว่า "Compliant is yesterday, resiliency is the future."



Cyber Security

Currently, all news and information in the world are sent speedily at a mere push of a button with a touch of your fingertips, as if the world have been made much smaller. Communicating with each other and conducting a business are done at a very fast pace, through technology playing a major role in the daily lives of every person in this world. Everyone has a personal mobile communications device. Leading organizations make use of technology to outcompete each other to be the number one in their businesses. Even small organizations are involved with technology, through using computers in working and storing key information. Small and medium businesses (or SMEs) make use of technology in operating their businesses - as can be seen in the great success of selling goods online.

An added aspect to technology playing such a major role is the increasing technology related risks — or 'cyber-risks'. Cyber-threats, hacking of information, release of computer viruses, or misuse of online information are all technology related risks that many organizations do not recognized. Boards of Directors have the role and responsibility for the governance and oversight of their respective organizations for the benefit of various Stakeholder groups. As such, Boards are not able to neglect or overlook the issue of these technology related risks; whereby the resulting losses and damages may not be mere interruption of business operations but may involve longer term damages — such as gaining a bad reputation or loss of confidence in the company on the part of its Shareholders.

This issue of the Boardroom brings the subjects of oversight of technology related risks (or cyber risks) and cyber-security to the attention of Board Directors, so they can have a much clearer view of these important issues. The content is based on the IOD's recent trip to the US, together with selected IOD Members and members of Regulatory authorities, to attend the Global Cyber Summit (GCS) last April, that was held by the Global Institute of Directors and attended by many member IOD organizations from around the world - including the Thai-IOD, which became a GCS member last year. Many Boards Directors participated in this global event to learn about and exchange ideas on these issues, to which, it is clear, that many Boards in other countries are placing much more importance.

Therefore, the IOD wishes to present a summary of the key ideas that were discussed at the various seminars during this event together with various viewpoints expressed at interviews conducted with various specialists, regulatory authorities and the business sector - so that Thai Board Directors can see and better understand the importance of the oversight of technology related risks.

The key points from the seminars are summarized as follows:

Technology related risks is an issue that every organization must face

Technology related risks does not only relate to the information technology (IT) systems being used but also to the information stored in these IT systems. Currently, such information can be sent around the world in an instant. Thus, Boards of Directors need to recognize what are the 'critical data' for the organization; whereby the associated risks may be managed through the structured process of: identify, protect, detect, respond, and recover). As such, it is not only the oversight responsibility of the Management Group but rather a joint responsibility of the Members the Board of Directors together with the managers of every Business Unit within the organization.

In regards to 'information security', the Board of Directors should ask itself whether the Board and the responsible members of the Management group are able answer these key questions:

Do you know what are the mission 'critical data' for the organization?

How does the company manage such set of critical information?

What sort of security measures are in place to protect such critical information?

If something abnormal or irregular occurs, what 'action plans' are in place to deal with problem?

Who are the persons able to access such 'critical data'?

What measures are in place to control and prevent intentional leaking of such critical data by those Staff authorized to access the information, since every Staff is able to bring in their own communications 'device' which may result in important information being leaked outside the organization or being vulnerable to hacking by ill-intentioned external parties?

In the event of a business merger, what sort of information should be communicated between the parties?

What sort of information is being exchanged between Business Partners or with external parties?

If the information is stored outside the country, has a study of the differing associated legal and regulatory implications been undertaken? Where is the information stored? What sort of information? Is there a necessity to store and keep the information involved?

Has a risk assessment been made in regards to the storage of the information involved - such as, emails, photographs/pictures or audio recordings?

To what extent have measures been taken to protect the confidentiality of the personal information of the

customers/clients; whereby it should be asked why such personal information are necessary and required? What constitutes genuine important personal information?

Which Business Unit owns such personal information? And do the Business Partners, who have the same personal information, also have measures in place to protect the personal confidentiality of your customers/clients and their personal information?

An interesting issue is that in the past the Board of Directors may view the management of technology as an 'expense' for the company, but currently this viewpoint should be changed to seeing the matter of technology as more of an 'investment' to be made by the organization — namely; how much investment is required and how fast can the investment be made. Often, the issue of technology related risks is not really a technical issue but rather that corporate leaders often do not give this matter much importance, whereby when a problem occurs there is a lack of real readiness or of being well-prepared. With regards to this issue, Boards of Directors need to change their existing viewpoints to that of anticipating negative events in advance and then of having in place effective plans to preempt or deal with such events.

An interesting example is hacking of information systems overseas - such as in the USA, where it happens quite frequently. A challenge in managing technology related risks is to manage those risks we cannot see, such as computer viruses. Attacking a computer system can be done easily through the attackers having a clear aim of attacking the information in the system at a specific level and of what information they want to access. A seminar participant, *Ms. Kim Zetter*, author of the book **"Countdown to Zero Day: Stuxnet and the Launch of World's First Digital Weapon"**, presented and shared the case study about Stuxnet Malware that occurred about 10 years ago. By adding 21 new lines of code into a software program that controls electricity power generation, it was possible to shutdown the entire power generating system. This 'malware' was able to be spread into computers using the Windows operating system, with the aim of shutting down the 'protective delay system' through causing the normal power generating operation to gradually become abnormal and to reduce the efficiency of the power generating system until it was not able to operate any further. This example shows how the lack of any protective measures or interest in technology related risk issues may result in losses and damages to the organization; whereby companies can be categorized into 2 types: namely, companies that have had their critical information stolen but does not know about it; and companies that have had their critical information stolen and know about it.

Information technology related risks are 'enterprise-wide' risks.

Boards of Directors should view technology related risks as being a key part of its 'enterprise wide risks' and not only related specifically to technology or technical matters to be managed and the sole responsibility of the IT Department. The Board should see it as being an enterprise wide operational matter and not as a separate risk issue that does not involve the overall business operations. As such, the Board of Directors needs to understand this matter from the point of view of being a key risk factor rather than a purely technology matter, whereby it is an integral part of the overall business processes. Such an understanding can be achieved by starting to take the following points of view:

Should or should not the composition of the Board of Directors include someone with IT expertise and knowhow?

Should IT related risks also be an oversight responsibility of the main Board, or a role and responsibility for the Audit Committee only?

Should the Board of Directors receive additional knowledge about technology or not?

The Board of Directors should not be afraid to ask questions about matters that it does not know — such as, various technology terminologies.

As such, should the Board engage an IT consultant or IT specialist to provide it with a better understanding of IT matters or not?

Should the Board of Directors engage an independent IT specialist to oversee the members of the Management Group responsible for IT matters or not?

Does our organization have sufficient associated resources or not - in terms of people and budgets?

In the event that the company is subject to a cyber-attack, it it well prepared - or not - to deal with it? And what would be the most serious extent of damages or losses to the company, which would meet the objectives of such a cyber-attack?

Technology related risks should be ranked at beyond more than the current top 1 to 10 risks within any organization; and such risks should also be viewed as being connected to other types of risks. The Board of Directors should ensure that those members of Management directly responsible for IT matters should also realize the importance of technology related risks as well as are regarded as fully and genuinely capable of meeting such risks. As such, the Board of Directors may consider establishing a Risk Management Sub-Committee responsible for overseeing such key and important risks for the organization, as well as should ensure that every operational unit within the company also sees the importance of the various technology related risks and be involved in managing such risks.

Communications are important

Good communications are vital for the overall effective conduct of all business aspects of the organization. As such, technology is also an important aspect; whereby if there are any related issues that make the organization at risk of being a vulnerable target of any cyber-attacks, these should be informed to the involved Public Authorities. Good communications between the Private and Public Sectors are important to enable the Public Sector to determine effective preventive and protective measures. However, informing the general public, via the public media, must be done with care. Any such public disclosures of information should be adequate and only as necessary, so that the organization will not be a target for any cyber-attacks by any ill-intentioned external parties — such as, in the event of a leak of important information,

the Board of Directors should be well-prepared in regards to when and how to inform customers/clients and with how much or how little information should be given. The Board should also determine who, within the organization, should be involved and responsible for disclosing the information to the customers/clients, with close attention also being given to the accuracy of the information being disclosed. As such, the Board of Directors should have in place a 'Crisis Communication Plan' together with a 'Crisis Recovery Plan'. Further, it should be clearly identified who, within the organization, will be the official 'representative' of the organization responsible for communicating with and informing the general public.

In addition to external communications, communicating internally with the organization's staff is also important. Regular training and practice in regards to internal communications should take place; but this must be done in an interesting manner that can be easily understood — such as, through role playing.

Good communications between the Board of Directors and the Management Group is also a vital and important aspect. So as to enable the Board of Directors to oversee and monitor the company's business operations in an effective manner, it may consider appointing a Chief Information Officer (CIO) and/or a Chief Information Security Officer (CISO) within the organization; whereby once such an appointment is made, regular updates of various ongoing issues should be made to the Board - on a monthly basis or on a weekly basis in the event that a irregular incident or crisis occurs relating to cyber-security or cyber threats. Further, in the event of such crisis situations, the Board of Directors must create a positive corporate culture of accepting the situation — namely, not blaming the Management Group and listen to all the facts as well as closely collaborating together to quickly resolve the problem. This is so that the Management Group will always be open and willing enough to inform the Board of the real facts and situation; whereby the Board should keep in mind this saying "Compliance is yesterday, resilience is the future".

CyberSecurity: ความมั่นคงปลอดภัยในโลกไซเบอร์

คุณจีราวรรณ บุญเพิ่ม
ประธานคณะกรรมการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Mrs. Jirawan Boonperm
Chairpreson
Electronic Transactions Development Agency (Public Organization) - ETDA

เมื่อก้าวเข้าสู่ยุค Digital Economy หรือเศรษฐกิจดิจิทัล นั้นหมายถึง เศรษฐกิจและสังคมที่ใช้ข้อมูลข่าวสารและITเป็นกลไกสำคัญในการขับเคลื่อนการปฏิรูปกระบวนการผลิต การดำเนินธุรกิจ การค้า การบริการ การศึกษา รวมถึงกิจกรรมต่างๆ ทางเศรษฐกิจและสังคมอื่นๆ ที่ส่งผลต่อการพัฒนาทางเศรษฐกิจ และการพัฒนาคุณภาพชีวิตของคนในสังคม

แน่นอนเมื่อมีการใช้ข้อมูลข่าวสาร มีการรับส่งหรือส่งต่ออย่างอิสระและรวดเร็ว การรั่วไหลของข้อมูลย่อมเกิดขึ้นได้ หลายประเทศได้ตระหนักถึงความไม่มั่นคงปลอดภัยที่อาจเกิดขึ้นนี้ และให้ความสำคัญกับ Cybersecurity หรือการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก

สำหรับประเทศไทย รัฐบาลได้ให้ความสำคัญกับ Cybersecurity เช่นเดียวกันเพื่อเป็นการสร้างความเชื่อมั่นให้กับภาคธุรกิจและสังคมในการทำธุรกรรมออนไลน์ ซึ่งเป็นเครื่องจักรหนึ่งในการขับเคลื่อนระบบเศรษฐกิจของไทย หน่วยงานหลักที่รับภารกิจที่สำคัญนี้โดยเฉพาะ คือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ที่ดำเนินงานอยู่ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) และกำลังอยู่ในระหว่างการเสนอเพื่อพิจารณาร่างกฎหมายปรับปรุงกระทรวงโดยมีการเปลี่ยนชื่อ เป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

Boardroom ฉบับนี้ ได้รับเกียรติจาก *คุณจีราวรรณ บุญเพิ่ม* ประธานคณะกรรมการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ให้สัมภาษณ์เรื่อง Cybersecurity พร้อมชี้ให้เห็นถึงผลลัพธ์ที่อาจเกิดขึ้น เมื่อองค์กรขาดความตระหนักรู้และไม่มีมาตรการหรือระบบป้องกันข้อมูลอย่างเพียงพอขององค์กร

เรื่องหลักที่ต้องเร่งทำ

เริ่มแรก*คุณจีราวรรณ*เล่าให้ฟังถึงพันธกิจที่ สพธอ. ต้องดำเนินการ คือ การพัฒนา การทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศทั้งในระดับผู้ประกอบการอุตสาหกรรม ระดับองค์กร และระดับประชาชน ให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ ซึ่งมีองค์ประกอบสำคัญ 3 ด้าน คือ

1. เครื่องมือในการทำธุรกรรมออนไลน์ต้องมีความมั่นคงปลอดภัย ไม่ว่าจะเป็นคอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต หรือเครือข่ายอินเทอร์เน็ตเองต้องมีกลไกในการดูแลให้ใช้งานได้ถูกต้อง
2. มีมาตรฐานในการทำธุรกรรมออนไลน์เพื่อลดความซ้ำซ้อน ลดข้อผิดพลาด และเพิ่มประสิทธิภาพ และ
3. มีกฎหมายรองรับการทำธุรกรรมออนไลน์ไม่ว่าจะเป็นด้านการรับส่งข้อมูล การดูแลข้อมูลส่วนบุคคล ตลอดจนป้องปรามการกระทำความผิดโดยใช้ IT เป็นเครื่องมือ

สิ่งที่คุณจีราวรรณบอกว่าเป็นเรื่องสำคัญเร่งด่วนที่ต้องทำคือการสร้างความตระหนักรู้ให้กับผู้ประกอบการทุกระดับ รวมถึงประชาชนทั่วไปเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ทั้งนี้เพราะปัจจุบันทุกคนมีอุปกรณ์ที่สามารถเข้าถึงข้อมูลต่างๆ ผ่านทางอินเทอร์เน็ตได้อย่างง่ายดาย ไม่ว่าจะเป็นเรื่องส่วนตัวหรือเรื่องงาน จนเกิดเป็น trend ที่เรียกว่า Bring your own device คือการนำอุปกรณ์ส่วนตัวมาใช้ทำงาน ซึ่งผู้ใช้อาจขาดความรู้ ความเข้าใจถึงการป้องกันอย่างเพียงพอ ซึ่งโอกาสที่ข้อมูลสำคัญๆ ของหน่วยงานจะเกิดความเสียหายได้นั้นมีมากทีเดียว แม้ว่าปัจจุบันทาง สพธอ. จะมีไทยเซิร์ตที่คอยเฝ้าระวังและติดตามภัยคุกคามบนอินเทอร์เน็ตตลอด 24 ชั่วโมง แต่ประเทศไทยยังคงเป็นพื้นที่ที่ถูกโจมตีและมีความเสี่ยงด้านอินเทอร์เน็ตมากแห่งหนึ่ง และกลายเป็นฐานในการแฮกข้อมูล หรือกระจายมัลแวร์ไปยังประเทศต่างๆ

IT Governance

เนื่องด้วย IT เป็นหัวใจสำคัญของการดำเนินธุรกิจ การกำกับดูแลเรื่องนี้จึงมีความสำคัญเหมือนกับความเสี่ยงทางธุรกิจอื่นๆ คณะกรรมการควรให้ความเข้าใจ สนใจ เรื่องระบบดูแลความมั่นคงปลอดภัย ติดตาม เฝ้าระวัง ป้องกัน ความมั่นคงปลอดภัยด้านไซเบอร์ที่จะเกิดขึ้น เพื่อเป็นการป้องกันความเสียหายที่จะเกิดขึ้นกับองค์กร เช่น การเสียหายด้านชื่อเสียงซึ่งประเมินมูลค่าไม่ได้รวมทั้งจัดให้มีวาระการประชุมเรื่องนี้อย่างชัดเจนในการประชุมคณะกรรมการ เพื่อให้แน่ใจว่าระบบต่างๆ มีความโปร่งใส ตรวจสอบได้ และสามารถเปิดเผยรายงานการรั่วไหลของข้อมูล รวมถึงมีวิธีการในแก้ไขปัญหาเพื่อการพัฒนาและสร้างระบบป้องกันให้มีประสิทธิภาพมากขึ้น ถ้ากรรมการขาดความรู้ความเชี่ยวชาญควรจะมีการเชิญผู้เชี่ยวชาญจากภายนอกเข้ามาเป็นที่ปรึกษาในเรื่องนี้

นอกจากนี้ *คุณจีราวรรณ* ยังฝากอีกว่า การทำหน้าที่ดังกล่าวไม่ใช่หน้าที่ของหน่วยงาน IT ขององค์กรเพียงอย่างเดียว หรือหน่วยงานใดหน่วยงานหนึ่ง หากแต่เป็นเรื่องของทุกคนในองค์กรที่ต้องช่วยกัน โดยเริ่มต้นจากระดับคณะกรรมการลงไป ซึ่งในส่วนนี้ทาง สพธอ. มีการจัดเตรียมผู้เชี่ยวชาญ ด้าน IT ที่พร้อมให้คำแนะนำและความรู้ด้าน IT แก่หน่วยงานหรือประชาชนทั่วไป หรือหากองค์กรใด ต้องการสรรหาบุคคลที่มีความเชี่ยวชาญด้าน IT เข้าเป็นส่วนหนึ่งของการพัฒนาและดำเนินงาน ทาง สพธอ. มีรายชื่อให้บริการเช่นกัน

เอกชนขานรับ

คุณจีราวรรณ กล่าวว่า ในการดำเนินงานที่ผ่านมา ภาคเอกชนให้ความสนใจอย่างต่อเนื่องในเรื่องการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ โดยเฉพาะในกลุ่มธุรกิจการเงิน เนื่องด้วยมีความเกี่ยวข้องโดยตรงในการทำธุรกรรมผ่านอินเทอร์เน็ต แต่อย่างไรก็ดี สพธอ. อยากให้ภาคเอกชนในอุตสาหกรรมอื่นๆ ให้ความสำคัญเกี่ยวกับเรื่องนี้ขึ้นเช่นเดียวกัน และร่วมกับ สพธอ. ในการพัฒนาระบบ และแบ่งปันประสบการณ์ที่เผชิญมา เพื่อให้เป็นกรณีศึกษาและร่วมกันหาทางป้องกันต่อไป

นอกจากนี้ ทาง สพธอ. ได้มีการจัดทำ Leading Practice เพื่อใช้เป็นแม่แบบในการสร้างระบบในแต่ละองค์กร และพัฒนาให้เข้ากับองค์กรต่อไปได้ สำหรับองค์กรภาครัฐมีพรบ.ธุรกรรมทางอิเล็กทรอนิกส์ที่เขียนกรอบไว้แล้ว ซึ่งอาจนำมาปรับใช้ในภาคเอกชนได้ต่อไป ซึ่งทางสพธอ. จะต้องทำงานร่วมกับองค์กรอื่นๆ เช่น IOD ในการสอบถามความคิดเห็นภาคเอกชนและจัดทำ Leading Practice ที่เหมาะสมกับภาคเอกชน และอาจจะมีการออกเป็นกฎหมายอีกครั้งในอนาคต ซึ่งก่อนที่จะทำจะต้องมีการให้ความรู้กับภาคเอกชนอย่างชัดเจนก่อน

Cybersecurity

As we move towards the digital era — or specifically the Digital Economy — this means that the economy and society as a whole will make full use of information technology and communications

media as an important means to drive the modernization of manufacturing and production processes, business opertions, trade, services, and education together with various other economic and social activities that have an impact on the development of the economy and the overall quality of life for everyone in the society.

Obviously, with the increased communcations of information and data together with the increase in the free and fast flow of information being sent, received or forwarded on to other parties, incidents of information leaks will be bound to occur. Many countries have recognized this unsecure and potential leak of such information ows, and have also given importance to the issue of safeguarding the security of information — or cyber security.

As for Thailand, the Government is also giving the issue of cyber security much importance, in order to create confidence on the part of the business sector and society in undertaking online transactions that are considered to be a vital engine to drive the development of Thailand's economy. The government authority assigned with this key responsibility is the Electronics Transactions Development Agency (or ETDA), which is a Public Sector organization within the Ministry of Information Technology (ICT Ministry) that is currently in the process of drafting proposed new laws to be re-designated as the Ministry of Digital Technology for the Economy and Society.

This issue of the BOARDROOM magazine is honored to be able to interview *Mrs. Jirawan Boonperm, Chairperson of the Electronic Transactions Development Agency (ETDA)* on the subject of 'cybersecurity' as well as to hear her views on the potential resulting impact for an organization that lacks an awareness of this matter and that does not have in place any measures to protectits important information.

Key and urgent actions to be undertaken

At the start of the interview, *Mrs. Jirawan* told us that the key mission of the ETDA is to develop the system for electronic or online transactions of the country for the operational level of key industries, for the activities of key organizations, and for the people in general, so that there is full security and trustworthiness on the part of everyone. This mission consists of 3 elements: *1) The tools and devices used for undertaking such online transactions must be safe and secure — whether it is a mobile phone, tablet/PC and the internet network system itself, there must be measured to oversee and ensured that all such devices can be used in a proper and correct manner. 2) There must be standards of operations in undertaking online transactions, in order to reduce complexities, minimize errors and enhance overall effectiveness. 3) There must be laws to regulate and support online transactions — whether it is sending/receiving information, control of personal information, and prevention/protection against the misuse of IT as a tool for wrongdoings.*

Mrs. Jirawan also stated that one matter that must be urgently undertaken is to educate and communicate to business operators at all levels together with the general public about information security — or cyber security. This is because nowadays everyone is able to easily access various types of information via the internet — regardless of whether it is personal or business related information. In this regard, it has now become a common trend for people 'to bring your own device' — or make use of their personal communications device to work. As such, users may still not sufficiently understand about security and protection of information, and thus there is significant risk that damage will be caused to important data of the organization. Despite the fact that the ETDA, through its 'Thai-CERT' keeps a constant and 24 hour watch on potential cyber threats to the internet network, but Thailand is still vulnerable to cyber attacks, and to being a site with significant internet related risks where information hacking has often occurred or from which 'malicious' malware is released to various other countries.

IT Governance

Given that IT systems is at the heart of all business operations, oversight and governance of such systems is as essential as other potential business risks. As such, Boards of Directors need to fully understand as well as be concerned with systems to control the security and safety of IT systems in use. Boards must also monitor and be mindful about cyber security, and protect against potential cyber threats to the organization — such as, loss of reputation the full value of which cannot be assessed. Further, specific consideration of this key issue must be undertaken on a regular basis at Board Meetings, in order to ensure that the various associated operational systems are transparent and have full accountability, as well as it is possible to disclose information about information leaks together with relevant corrective measures against them - with the aim of establishing a more effective information security and protection system. In the event that the Board Directors does not have full knowledge on this issue, the Board should engage an outside expert or specialist to advise the Board on these matters.

Furthermore, *Mrs. Jirawan* added that this duty is not only the responsibility of the IT Department or any other specific internal business unit, but rather is the duty of everyone within the organization to help with these responsibilities; whereby it should start from the very top - at the Board level - and go downwards. With regard to this responsibility, the ETDA has IT experts available to provide advice to and educate any business organization or even the general public about IT issues. Also, should any organization seek to recruit IT specialists to join it in develop and operate its IT operations, then the ETDA can also provide a list of potential candidates for consideration.

Positive response from the general public

Mrs. Jirawan also stated that from past activities, the general public has continually shown keen interest in the development of electronic transactions — especially within the finance sector, since this business sector is directly involved with undertaking their transactions via the internet. However, the ETDA also wants private sector groups within other industry/business sectors to give importance to this matter through cooperating together with the EDTA in developing IT systems and in sharing relevant past experiences and problems, as well as in collaborating to ffiind ongoing effective ways of protecting information.

Additionally, the ETDA has determined and established *some* 'leading practices'

that can be used as a template for establishing a cyber security system that can then be developed further within each respective organization. For Public Sector organizations, there is the Electronics Transactions Act that includes a framework, which Private Sector organizations could possibly adopt and adapt for their own specific use. As such, the ETDA needs to collaborate with other organizations — such as the IOD — in surveying Private Sector organizations' views in order to help determine other 'leading practices' suitable for the Private Sector in the future. These views may also be used to establish additional legal requirements, whereby the Private Sector needs to be further informed and educated about specific issues beforehand.

CyberSecurity: การกำกับดูแลด้านไอที

คุณเมธา สุวรรณสาร
อุปนายกสมาคม
Information Systems Audit
and Control Association (ISACA)
Mr. Metha Suvanasarn
Vice President
Information Systems Audit and Control Association
(ISACA)

อีกหนึ่งหน่วยงานที่ทำงานด้านระบบสารสนเทศที่น่าสนใจ คือ สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ ที่เป็นเครือข่ายจาก Information Systems Audit and Control Association (ISACA) จากประเทศสหรัฐอเมริกา ซึ่งเป็นหน่วยงานที่ส่งเสริม สนับสนุนเผยแพร่ข่าวสารด้านการตรวจสอบและการควบคุมงานด้านคอมพิวเตอร์ และเน้นให้ผู้บริหารและผู้ประกอบวิชาชีพด้านคอมพิวเตอร์ ได้เห็นความสำคัญในระบบควบคุม เพื่อสร้างเสริมประสิทธิภาพขององค์การและดูแลให้การใช้ทรัพยากรมีประโยชน์สูงสุด ซึ่งทาง ***คุณเมธา สุวรรณสาร*** *อุปนายกสมาคม Information Systems Audit and Control Association (ISACA)* ให้เกียรติสัมภาษณ์ถึงความสำคัญและบทบาทหน้าที่ของกรรมการในการกำกับดูแลด้านไอที

การกำกับดูแลด้านไอที (IT Governance) คืออะไร

อาจารย์เมธา สุวรรณสาร เป็นผู้เชี่ยวชาญด้านการกำกับดูแลด้านไอที (IT Governance-ITG) ได้ให้คำจำกัดความเกี่ยวกับ ITG ว่าคือ "กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร" หรือ GEIT-Governance of Enterprise IT ซึ่งเป็นไปตามวัตถุประสงค์ในการกำกับดูแล คือการสร้างคุณค่าเพิ่มให้กับผู้มีส่วนได้เสีย และมั่นใจว่าองค์กรจะได้รับผลประโยชน์ ในขณะเดียวกันมีการบริหารความเสี่ยงที่เหมาะสม และการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด เพื่อให้การดำเนินงานขององค์กรบรรลุเป้าประสงค์ในทุกมิติและทุกบริบท โดยสอดคล้องกับมาตรฐานและกรอบการจัดการที่ดีที่เป็นสากล หรือจะพูดให้ง่ายก็คือ ITG คือ **"การกำกับดูแลกิจการที่ดีระดับองค์กร ที่เป็นหน้าที่และความรับผิดชอบของคณะกรรมการ เพื่อสร้างคุณค่าเพิ่ม สนองตอบความต้องการของผู้มีส่วนได้เสีย"**

หลักการที่นำมาใช้ในการกำกับดูแลด้านไอที

อาจารย์เมธา แนะนำหลักการหนึ่งที่เรียกว่า COBIT ซึ่งย่อมาจาก Control Objectives for Information and Related Technology ที่มีวิวัฒนาการมายาวนานกว่า 46 ปี ของสมาคม ISACA สากล ที่ย่อมาจาก Information Systems Audit and Control Association ภายใต้กรอบ IT Governance Institution ได้ศึกษาและพัฒนาการควบคุมการตรวจสอบสู่การบริหารไอที การกำกับดูแลไอที และการดำเนินทางธุรกิจที่ผสมผสานกันระหว่างการกำกับดูแลและการบริหารธุรกิจเป็นหนึ่งเดียวแบบบูรณาการ ซึ่ง COBIT5 มีหลักการโดยย่อ ดังนี้

- เป็นการตอบสนองต่อความต้องการของผู้มีมีส่วนได้เสีย
- มีกรอบการการดำเนินงานทางธุรกิจที่ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร
- ประยุกต์ใช้กรอบการดำเนินงานที่บูรณการเป็นหนึ่งเดียว
- มีปัจจัยเอื้อที่ก่อให้เกิดความสำเร็จ
- ให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล
- แยกการกำกับดูแลหรือ Governance ให้เป็นบทบาทของคณะกรรมการที่แยกจากการบริหารจัดการ

หลักการทั้ง 5 ของ COBIT5 มีขั้นตอน มิติ ขอบเขต แนวทาง การนำไปใช้ บทบาทของผู้เกี่ยวข้องที่แตกต่างกันไป ที่ควรพิจารณาถึงปัจจัยแวดล้อม เทคโนโลยี ศักยภาพของบุคลากรอย่างลึกซึ้ง

การกำกับดูแลด้านไอทีสำคัญอย่างไร

อาจารย์เมธา เน้นย้ำว่าเรื่องนี้มีความสำคัญมาก จากการสำรวจไม่เป็นทางการพบว่าวาระการประชุมของคณะกรรมการไม่ค่อยมีเรื่องหรือเป้าหมายเกี่ยวกับไอทีควบคู่กับเป้าหมายระดับองค์กรอย่างมีนัยสำคัญและเมื่อมีการพิจารณาเรื่องไอทีก็เป็นการพิจารณาเรื่องไอทีแยกจากเป้าหมายและกลยุทธระดับองค์กร ซึ่งไม่สอดคล้องกับหลักการที่เป็นสากลที่การกำกับดูแลด้านไอทีต้องเป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี ทำให้ระดับองค์กรที่ไม่สามารถตอบสนองต่อการขับเคลื่อน และความต้องการของผู้มีส่วนได้เสียได้อย่างเต็มที่

หากเรื่องไอทีไม่ได้เป็นส่วนหนึ่งของธุรกิจแบบบูรณาการตามความหมายและหลักการของ IT Governance หรือ GEIT- Governance of Enterprise IT จะส่งผลกระทบต่อองค์กรและความรับผิดชอบของคณะกรรมการในหลายด้าน โดยเฉพาะอย่างยิ่งด้าน Performance คือผลสัมฤทธิ์ และ Conformance คือการกำกับดูแลให้เป็นไปตามมาตรฐาน โดยมีการประเมินผล สั่งการ และเฝ้าติดตาม ซึ่งหากเป็นเช่นนั้นจะเกิดความเสี่ยงเกินกว่าที่องค์กรจะยอมรับความเสียหายได้ อันจะทำให้เกิดผลทางลบตามมามากมาย หากองค์กรใดให้ความสำคัญในเรื่องนี้องค์กรและคณะกรรมการนั้นก็จะมั่นใจได้ว่าได้รับความเชื่อถือความเชื่อมั่น ความไว้วางใจ จากผู้มีส่วนได้เสียและกรรมการสามารถตอบคำถามภายใต้ "Fiduciary duty" ได้ในทุกมิติและทุกบริบทของการกำกับดูแลกิจการที่ดี

บทบาทของคณะกรรมการ

อาจารย์เมธา ให้ความเห็นว่าการเริ่มต้นขององค์กรเป็นส่วนที่สำคัญมาก ซึ่งนโยบายในองค์กรทุกอย่างเริ่มต้นที่คณะกรรมการ คณะกรรมการอาจเริ่มต้นในการดำเนินงานเรื่องนี้โดยการทบทวนบทบาทของกรรมการชุดต่างๆ ให้สอดคล้องกับหลักการของ IT Governance ภายใต้กรอบ COBIT5 หากการปรับเปลี่ยนโครงสร้างขององค์กร ต้องใช้เวลา และทรัพยากรนานเกินควร การสื่อสาร สร้างความเข้าใจในเรื่องและประโยชน์ของการกำกับและบริหารแบบบูรณาการ และการปรับปรุงกฎบัตรของคณะกรรมการชุดต่างๆ น่าจะเป็นเรื่องที่ทำได้ก่อน หลังจากนั้นจึงมีการประเมินเพื่อพัฒนาและนำหลักการฯมาใช้และปรับปรุงประยุกต์อย่างเหมาะสม

ในเรื่องหนึ่งที่กรรมการควรให้ความสำคัญในการกำกับดูแลคือเรื่อง ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Risk) ซึ่งเป็นเรื่องหนึ่งของความเสี่ยงด้านไอที (IT Risk) ที่เป็นสาเหตุของปัญหาที่สำคัญยิ่ง ที่มีผลกระทบต่อ Performance และ Conformance ระดับองค์กร การวิเคราะห์ความเสี่ยงและการป้องกันความเสี่ยงระดับองค์กรในเรื่อง Cybersecurity นั้น ควรใช้ผู้เชี่ยวชาญที่เป็นมืออาชีพเฉพาะเรื่องโดยเริ่มจากการกำหนดความเสี่ยงที่องค์กรยอมรับได้ และมีการกำกับดูแลโดยคณะกรรมการ ตามหน้าที่หลัก นั่นคือการประเมินผล การสั่งการ และการเฝ้าติดตามอย่างเป็นกระบวนการ

อาจารย์เมธา แนะนำว่าหากท่านใดต้องการทราบรายละเอียดเพิ่มเติมเกี่ยวกับเรื่องการกำกับดูแลได้ไอที ตัวอย่างการนำไปประยุกต์ใช้จริงของ COBIT5 เช่น เรื่อง เศรษฐกิจดิจิตอล สามารถอ่านได้เพิ่มเติมจากบทความในเว็บไซต์ www.itgthailand.com

IT Governance

Another organization of interest, involved with information technology systems, is the Information Systems Audit and Control Association (ISACA) for the Bangkok region, which is part of the US-based ISCA. It is responsible for supporting, promoting and informing relevant news and information relating to the audit and control of computer systems. ISACA's main aim is to promote that corporate Management and IT Professionals give greater importance to the control and monitoring of computer system, in order to enhance their organization's effectiveness and to ensure that its resources are utilized for the maximum benefit possible. The IOD was honored to be able to interview *Mr. Metha Suvanasarn, Vice President of the Information Systems Audit and Control Association (ISACA)* for the Bangkok region, about the importance of IT Governance as well as the role and responsibility of Board Directors relating to IT Governance.

What is IT Governance?

Mr. Metha, who is an expert and specialist on IT Governance (ITG), defined IT Governance as being "the business operation's framework for governance and management of its IT systems on an enterprise-wide basis - or GEIT (Governance of Enterprise IT). This is in accordance with the goals of its overall corporate governance practices - namely, creating value added for all Stakeholders and ensuring that the organization will achieve maximum benefits; while at the same time, appropriate management of risks will also be undertaken together with making effective use of all its resources to gain full benefit, so that the overall organization will achieve its stated objectives and goals in every operational dimension or context. As such, this corresponds to the internationally accepted good management standards and framework; or simply put: "good governance at the corporate level is the role and responsibility of the Board of Directors, in order to create value added, and to meet the requirements of the Stakeholders"

Key principles used in regards to IT Governance *Mr. Metha* recommended one key principle relating to IT Governance, namely: "Control Objectives for Information and Related Technology" (or COBIT), that was innovated and initiated more 46 ago by ISACA — or the international Information Systems Audit and Control Association, under the auspices of the IT Governance Institution, that studied and developed control and monitoring procedures for the auditing the management of IT systems, the control procedures for IT systems, and the business operational procedures that combines both the governance and management of the overall business in one integrated system.

As such, COBIT 5 incorporates the following principles:

1) Meeting the requirements of the Stakeholders
2) Having an enterprise-wide operational framework in an comprehensive or integrated manner
3) Adapting the operational framework into one integrated system
4) Incorporating together various factors, in order to enable successful achievements and to facilitate integrated organizational-wide performance results.
5) Separating out governance related activities, that is the duty of the Board of Directors, from those management/operational activities

The above 5 key principles of the COBIT 5 system incorporates and includes: various steps, dimensions/aspects, scope of coverage, operating guidelines, and the defined respective roles of involved parties that need to be taken into consideration, as well as details regarding environmental factors, technology systems and the potential capability of associated people resources.

How important is IT Governance?

Mr. Metha emphasized that this is a very important matter. From an informal assessment of the agenda items of Board Meetings, it was found that there were not many significant discussions dealing with information technology matters or objectives that related to corporate objectives; and that whenever there were discussions on IT matters, it was separate to the discussions on corporate objectives or strategies. This does not correspond to international principles, in which IT Governance is an integral part of the overall good corporate governance practices; and thus results in governance at the corporate level not being able to fully meet the ongoing requirements of the Stakeholders.

If matters relating to IT are not fully integrated as part of or within the overall business operational systems, as required by the principles of IT Governance or the principles Governance of Enterprise IT (GEIT), it will have an impact for the organization as well as on the Board of Directors responsibility for the various aspects of the organization — especially in regards to overall 'performance' (ie: performance results) and 'conformance' (ie: overall governance practices that are in accordance with accepted standards which incorporates evaluation, direction and monitoring). As such, if this is the case, then it would result in greater risks and potentially greater damages or losses than would be considered acceptable by the organization, which will lead to significantly greater negative impacts and consequence. However, if any organization does give importance to this issue, then both that organization and its Board of Directors would be able to feel sure of receiving both the trust and confidence from its Stakeholders. Further, the Board of Directors will be able to respond to a key question that it has fully discharged its 'fiduciary duty' in every aspect and context relating to good corporate governance practices.

Role of the Board of Directors

Mr. Metha expressed the view that initial activities of any organization are very important; whereby any policies of the organizations are normally initiated by the Board of Directors. Thus, the Board may initiate this issue through reviewing the role and responsibilities of the various Board Committees so that they correspond to the principles of IT Governance within the framework of COBIT 5. If the restructuring of the organization requires a significant amount of time and resources than expected, perhaps one thing that could be undertaken initially is to communicate and inform those within the organization about the issues of and associated benefits to be derived from having in place fully integrated corporate governance and Management systems together with a redefined Charter for each respective Board Committee. This action would achieve a better understanding on their part. Thereafter, an assessment of the principles to be applied should be made, in order to develop and adapt them, as appropriate, for further application within the organization.

One matter to which that the Board should give importance in regards to overall corporate governance is

the issue of **'cyber security' risk,** which relates to overall IT risks and is a ***key issue*** that will have an impact on *both* ***'performance'*** and **'conformance'** at a *corporate level.*

The assessment and prevention of risks, at a corporate level, relating to cyber security should be assigned to professional experts and specialists, and should start with determining what level of risks are acceptable (ie: risk appetite), and should also be overseen by the Board of Directors in accordance with their core role — namely: evaluation, direction, and monitoring results in a structured process.

Mr. Metha recommended that if anyone wishes to learn more about IT Governance and examples of actual situations of how COBIT 5 has been adapted and applied — such as, in regards to the digital economy, further details can seen in related articles through accessing the ITG website: www.itgthailand.com.

Cybersecurity:

ความก้าวหน้าทางเทคโนโลยี VS ความเสี่ยงที่เกี่ยวข้อง

ดร.นฤมล สิงหเสนี
รองกรรมการผู้จัดการใหญ่กลุ่มงานการเงินและสนับสนุนธุรกิจ
บริษัท แม็คกรุ๊ป จำกัด (มหาชน)
Dr. Narumol Sinhaseni
Deputy Managing Director of Finance and Business Support Department
Mc Group Plc.

เรื่องเทคโนโลยีเข้ามามีบทบาทในการทำธุรกิจอย่างมาก เช่น การติดต่อสื่อสารของผู้บริหารปัจจุบันใช้อีเมล์เป็นช่องทางสื่อสารหลัก องค์กรต้องปฏิสัมพันธ์กับลูกค้าตลอดเวลา ระบบงานภายในองค์กรแบบธุรกิจค้าปลีกใช้เทคโนโลยีตั้งแต่ติดบาร์โคด การทำบัญชีการรายงานยอดขาย ในต่างประเทศการทำธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ได้รับความสนใจอย่างมาก ซึ่งประเทศไทยก็มีการทำเรื่องนี้มากยิ่งขึ้น การที่เทคโนโลยีเข้ามามีบทบาทมากขนาดนี้ ความเสี่ยงในการใช้งานก็ยิ่งมีมากขึ้น ทั้งเรื่องของตัวระบบ และข้อมูลที่อยู่ในระบบ ดังนั้นคณะกรรมการและผู้บริหารจึงไม่สามารถที่จะเพิกเฉยและไม่ให้ความสำคัญเกี่ยวกับเรื่องนี้

อาจารย์นฤมล ยกตัวอย่างของการทำธุรกิจพาณิชย์อิเล็กทรอนิกส์ว่าเมื่อมีการใช้งานมากขึ้นการรักษาความปลอดภัยยิ่งจะต้องเพิ่มมากขึ้น การติดต่อของผู้บริหารที่มีข้อมูลที่สำคัญของบริษัทจะต้องระมัดระวังมากยิ่งขึ้น "ปัจจุบันสั่งงานกันผ่านทางไลน์ หรือส่งอีเมล์โดยใช้เมล์สาธารณะ เช่น Gmail ทางองค์กรได้มีการตั้งกูญแจเมล์หรือไม่ ว่าให้ใครเปิดดูข้อมูลได้บ้าง และมั่นใจได้อย่างไรว่าข้อมูลจะไม่รั่วไหล" นอกจากนั้นข้อมูลลูกค้าในระบบก็มีความสำคัญมากที่จะปกป้องความเป็นส่วนตัวของลูกค้า องค์กรต่างๆ ได้ให้ความสำคัญกับเรื่องนี้มากน้อยเพียงใด

อาจารย์นฤมล แนะนำว่าทุกองค์กรควรวางนโยบายเรื่องระบบการกู้ข้อมูล (Data Recovery System) คือเมื่อข้อมูลในระบบล่มองค์กรจะต้องกู้ข้อมูลให้ได้ภายในระยะเวลาเท่าไหร่ ซึ่งขึ้นอยู่กับว่าบริษัทมีความจำเป็นในการใช้ข้อมูลมากน้อยแค่ไหน เช่น โรงพยาบาลอาจจะต้องกู้ให้ได้ภายใน 1 ชั่วโมง ในธุรกิจค้าปลีกเช่นบริษัท แมคกรุ๊ป จำกัด (มหาชน) มีการกำหนดว่าจะต้องกู้ข้อมูลให้ได้ภายใน 1 วัน ทุกบริษัทควรจะมีแผนรองรับอย่างชัดเจนว่าหากระบบล่มหรือข้อมูลสูญหายจะมีการจัดการอย่างไร ควรจะมีซ้อมเพื่อเตรียมการหากเหตุการณ์ที่ไม่คาดหมายเกิดขึ้น

กรณีศึกษาด้านความเสี่ยงทางเทคโนโลยีที่เกิดขึ้นในบริษัทที่อาจารย์นฤมลยกตัวอย่างเช่น การนำซอฟท์แวร์ที่ผิดกฎหมายมาใช้ในบริษัท พนักงานแต่ละคนมีคอมพิวเตอร์พกพาเป็นของตนเอง หลายครั้งนำไปลงซอฟท์แวร์ที่ผิดกฎหมาย ซึ่งถ้าตรวจจับเจออาจก่อให้เกิดความเสียหายต่อองค์กรเช่น ติดไวรัส ต้องจ่ายค่าปรับและส่งผลภาพลักษณ์ต่อองค์กร ทางบริษัทจึงต้องมีการออกนโยบายที่ชัดเจน สื่อสารกับพนักงาน และลงโปรแกรมในคอมพิวเตอร์ทุกเครื่องที่ป้องกันไม่ให้พนักงานนำไปดาวน์โหลดโปรแกรมได้เอง เป็นต้น

โครงสร้างองค์กรที่เอื้ออำนวย

การจัดการความเสี่ยงด้านเทคโนโลยีได้อย่างมีประสิทธิภาพนั้นอาจารย์นฤมลแนะนำให้ทุกองค์กรมีการวางตัวผู้รับผิดชอบอย่างชัดเจน ที่แมคกรุ๊ปมีการแต่งตั้ง Chief Information Technology Officer (CIO) เพื่อดูแลเรื่องนี้โดยตรง สำหรับองค์กรอื่นๆ *อาจารย์นฤมล* แนะนำว่าหากไม่มีผู้เชี่ยวชาญภายในอาจจัดหาผู้เชี่ยวชาญจากภายนอก ซึ่งผู้เชี่ยวชาญนั้นจะต้องวางระบบภายในองค์กรทั้งด้านโครงสร้าง และการวางระบบการทำงานที่ชัดเจน เช่น คนมาทำงานวันแรกจะต้องมีอีเมล์ของบริษัททันที หน่วยงานนี้ตามจริงแล้วควรที่จะรายงานตรงกับคณะกรรมการความเสี่ยง

สำหรับงบประมาณก็ขึ้นอยู่กับความจำเป็นในการใช้เทคโนโลยีภายในองค์กรมากน้อยเพียงใดซึ่งคณะกรรมการจะต้องมีส่วนร่วมในการตัดสินใจและติดตามการใช้งบประมาณที่ได้อนุมัติไป มีวาระประจำในที่ประชุมคณะกรรมการทุกครั้ง คณะกรรมการต้องเป็นผู้เริ่มต้นตั้งแต่การวางนโยบาย ซึ่งหากขาดความเข้าใจควรจะเชิญผู้เชี่ยวชาญมาให้ความรู้ ซึ่งไม่ได้จำกัดแค่ระดับผู้บริหารแต่ลงไปถึงพนักงานทุกระดับ รวมทั้งหาความรู้เพิ่มเติมผ่านการอ่านการเข้าร่วมอบรมสัมมนาต่างๆ เพื่อให้มีความเข้าใจมากยิ่งขึ้น

ต่างประเทศกับประเทศไทย

เนื่องด้วย *อาจารย์นฤมล* เป็นท่านึงที่ได้ไปร่วมประชุม Global Cyber Summit ที่ประเทศสหรัฐอเมริกา อาจารย์จึงเห็นมุมมองที่แตกต่างบางอย่าง อาจารย์เห็นว่าคณะกรรมการและผู้บริหารให้ความสนใจกับเรื่องนี้มาก เพราะเห็นว่าเป็นจุดเสี่ยงที่อาจนำความเสียหายมาสู่องค์กรได้ ในขณะที่ประเทศไทยยังพูดคุยเรื่องนี้ไม่มากนักวิทยากรท่านหนึ่งที่อเมริกาได้แบ่งปันว่าไม่มีระบบใดที่สมบูรณ์แบบ แต่เราต้องมีอย่างน้อยเท่าเทียมกับคนอื่นๆ เพื่อที่เราจะไม่เป็นเหยื่อ "เราอาจไม่ต้องวิ่งเร็วเท่าหมี แต่ต้องเท่ากับหรือเร็วกว่าคนรอบข้าง" ในประเทศสหรัฐอเมริกาพัฒนาไปไกลมีตำแหน่งใหม่ๆ เกิดขึ้นในองค์กรเช่น Chief Information Security Officer (CISO)

ในประเทศไทยอาจารย์นฤมลเห็นว่ารัฐบาลควรวางเรื่องโครงสร้างพื้นฐานให้ดีและรวดเร็ว เช่น เรื่องบอร์ดแบนด์ที่ควรรวดเร็วและมีเสถียรภาพกว่านี้ และการออกกฎหมายเรื่องการป้องกันความปลอดภัยควรมีความชัดเจนมากยิ่งขึ้นหากรัฐบาลให้ความสำคัญเรื่องนี้อย่างจริงจังภาคเอกชนก็จะสามารถใช้ประโยชน์จากเทคโนโลยีได้อย่างเต็มที่และปลอดภัย

Technology progress VS Relevant risk

Technology plays an important role in business such as, communication of the executives that currently use e-mail as a main communication channel, the organization has to interact with the customers at all time, internal system of the retail business relies on technology ranging from, barcoding, accounting to sale reporting. For international business, electronic commerce (e-commerce) has been in the trend. Thailand also sees more e-commerces as well. The more important role of technology inevitably results in more risks, including the system itself and data in the system. Thus, the Board of Directors and executives inevitably could not ignore this issue.

Dr. Narumol raises an example of e-commerce that when there are more usages, the security has to be raised as well. The executives' communication with important information has to be more careful. "Nowadays, there are communications through Line or public e-mail such as Gmail, does the organization set a password and how can they be sure that there is no data leakage?" In addition, customers' data in the system is very important to protect their privacy. How much do the organizations emphasize on this issue?

Dr. Narumol also suggests every organization should set a data recovery system. It is the case when the system fails, how much time the organization is able to recover the data? It depends on the necessity of the data such as, the hospital should recover data within 1 hour, in the retail business such as Mc Group Plc. has determined to recover data within 1 day. Every organization should have a clear plan how to take an action in case of system failure or data lost. There should be a rehearsal to prepare for unexpected incidence.

Dr. Narumol raises a case study about the technological risk that might occur in the company such as, the usage of illegal software of the employee. Every employee has his/her own computer installed illegal software. If they are checked, there might be a damage to the organization such as viruses. The organization has to pay the ffiine and have the bad reputation. Therefore, the company has to have a clear policy, communicate with the employee and install a program in the every computer to prevent the employees to download or install the software by themselves.

Favorable organization structure

Regarding of effective technological risk management, *Dr Narumol* suggests every organization to place the responsible person clearly. At Mc Group, there is a Chief Information Technology Officer (CIO) to be responsible for this issue directly. For other organizations, she suggests them to look for external expert to set a system in the organization, including a clear structure and operational system such as a new employee must have the company e-mail instantly. Actually, this department should report to the Risk Committee.

The budget depends on the necessity to use technology in the organization. The Board of Directors have to participate in decision making and monitoring the approved budget. Importantly, it should be a regular agenda of the Board meeting. The Board have to be the initiators themselves from setting a policy. If they do not understand, they should learn from the expert. Moreover, the executives and employees at all levels should learn more through attending the seminars.

Thailand and aboard

As *Dr. Narumol* was one of the attendants of Global Cyber Summit in the United States of America, she has different viewpoints in some issues. She has an opinion that the Board of Directors and executives should pay attention to this issue because it is a risk that might cause damage to the organization. While it is not an interesting issue in Thailand, an American expert has shared that there is not such a perfect system, but we have to have a system at the same level as the other to prevent us from being a prey "we do not have to run as fast as a bear but, we have run as fast or equal as the others" In the United States of America, there are new positions in the organization such as Chief Information Security Officer (CISO)

In Thailand, *Dr. Narumol* has an *opinion* that the government should invest in a good and *fast infrastructure*

such as a faster and more stable broadband and a new law to protect security should be clearer. If the Thai government seriously take it, the private sector would benefit fully and safely from the technology.

พลตำรวจตรี ดร. สุพิศาล ภักดีนฤนาถ
ประธานกรรมการ
บริษัท คอมมิวนิเคชั่น แอนด์ ซิสเต็มส์ โซลูชั่น จำกัด (มหาชน)
Pol. Major General Dr. Supisarn Bhakdinarinath
Chairman
Communication & System Solutions Pcl.

CyberSecurity: การเตรียมพร้อมของทุกองค์กร

ปัจจุบันนี้มีเทคโนโลยีเกิดขึ้นใหม่และเปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้น เทคโนโลยีสารสนเทศ หรือ IT ในโลกของไซเบอร์นี้ จึงเป็นส่วนสำคัญสำหรับธุรกิจทุกแขนง ไม่ว่าบริษัทใดต่างมีความจำเป็นเร่งด่วนที่ต้องคอยปรับเปลี่ยนพัฒนาระบบ IT ของบริษัทให้สอดคล้องกับกระแส IT อยู่เสมอ และสิ่งสำคัญที่สุด คือ การรับมือกับความเสี่ยงที่อาจเกิดขึ้นจากโลกของไซเบอร์ Boardroom ฉบับนี้จึงขอสัมภาษณ์ *พลตำรวจตรี ดร. สุพิศาล ภักดีนฤนาถ ประธานกรรมการบริษัท คอมมิวนิเคชั่น แอนด์ ซิสเต็มส์ โซลูชั่น จำกัด (มหาชน)* ในฐานะของคณะกรรมการบริษัทที่ดำเนินงานด้านเทคโนโลยีสารสนเทศโดยตรง ทั้งยังมีความรู้และประสบการณ์ทางด้านเทคโนโลยีจากทั้งภาครัฐอีกด้วย

ความเสี่ยงด้าน IT

เริ่มแรก*พลตำรวจตรี ดร. สุพิศาล* เล่าให้ฟังถึงความเสี่ยงต่างๆ ที่เกิดขึ้นในระบบ IT เช่น การเจาะข้อมูลระยะไกล (Remote Hacker) โดยผู้ก่อการร้าย การใช้ระบบ IT ในการแทรกซึมลงถึงเครื่องจักรกลให้เกิดเหตุขัดข้องและสร้างความเสียหายให้กับองค์กร หรือการใช้ IT ในการตรวจสอบและจัดเก็บข้อมูล พยานหลักฐาน ข้อมูล VDO และภาพของคู่ความในการต่อสู้ทางคดี การดำเนินงานต่างๆ ที่ต้องใช้คอมพิวเตอร์เข้ามามีส่วนร่วม แม้แต่การเรียนการสอนในระดับประถมก็มีการใช้คอมพิวเตอร์เช่นกัน หากมีการถูกเจาะระบบเข้ามาเปลี่ยนแปลงข้อมูล ก็สามารถสร้างความเสียหายได้มากทีเดียว

แนวทางรับมือ

สำหรับ *พล.ต.ต. ดร. สุพิศาล* มองว่ากระแส IT จะเข้ามามีบทบาท และมีแนวโน้มเพิ่มสูงขึ้นเรื่อยๆ องค์กรต้องปรับตัวเพื่อรับมือให้ได้ เริ่มจากการจัดตั้งหน่วยงานหรือผู้ดูแลเฉพาะด้านอย่าง Unit IT ที่มี CIO (Chief Information Offiicer or Information Technology (IT) Director) ดูแลโดยตรง เพราะมีความสำคัญต่อบริษัทมาก เนื่องจากเป็นหน่วยงานที่สามารถช่วยลดต้นทุนในเรื่องต่างๆ ได้จากการวางระบบที่ดี และจะต้องมีการรายงานความปลอดภัยของระบบต่อคณะกรรมการและผู้บริหารอย่างต่อเนื่อง เพื่อดูแนวโน้มและปรับปรุงระบบอย่างต่อเนื่อง และมีการพัฒนาบุคคลากรภายในให้มีศักยภาพควบคู่กันไปการสร้างความสัมพันธ์กับลูกค้า ถือเป็นอีกส่วนหนึ่งที่ต้องดำเนินการ เพราะในโลกไซเบอร์ ลูกค้าเป็นส่วนสำคัญในการผลักดันการดำเนินงานของบริษัทให้เติบโต และช่วยในเรื่องของภาพลักษณ์ได้ดี

การใช้บริการจัดเก็บข้อมูลที่มีมาตรฐาน เช่น การใช้ Clouds หรือ Application ที่ถูกพัฒนาโดยบริษัทขนาดใหญ่ เพื่อการจัดเก็บข้อมูลแทนวิธีเดิมที่เก็บข้อมูลที่เป็นความลับของบริษัท บน server และทำการ Back up ด้วยตัวบริษัทตนเองถือว่ามีความเสี่ยง หากบริษัทไม่มีการป้องกันที่มีประสิทธิภาพ ดังนั้น การลงทุนแบบนี้สามารถครอบคลุมความปลอดภัยทุกๆ ด้าน ไม่ว่าจะเป็นความปลอดภัยทางด้านผู้ดูแล การตรวจสอบการ Upgrade ฉะนั้นการว่าจ้างให้บริษัทที่มีความเชี่ยวชาญทางด้าน IT เข้ามาบริหาร จึงเป็นหนึ่งหลักการที่ดีและมีประสิทธิภาพในการสร้างความปลอดภัยของไซเบอร์

บทบาทของกรรมการ และการป้องกันการเกิดผลเสียทาง IT

กรรมการต้องมีการพัฒนาตัวเองให้ทันต่อกระแสที่เปลี่ยนไป *พล.ต.ต.ดร.สุพิศาล* มองว่ากรรมการควรต้องปลูกฝังการใช้ IT ลงไปใน DNA ขององค์กร เพื่อสร้างให้ทุกแผนกเกิดการใช้งานจริง และตกผลึกลงไปจากรุ่นสู่รุ่นโดยใช้ IT เป็นเครื่องมือสื่อสาร จนหล่อหลอมให้เป็นภาพลักษณ์ขององค์กร

พล.ต.ต. ดร.สุพิศาล กล่าวเพิ่มเติมว่าการพัฒนาและวางแผนในเรื่องการป้องกันความเสี่ยงที่จะเกิดขึ้นต้องอาศัยปัจจัยหลายด้าน ยกตัวอย่างที่ CSS เลือกใช้บุคลากรภายในองค์กรเป็นหน่วยขับเคลื่อนหลักเพื่อให้มีความเข้าใจในพื้นฐานของข้อมูลและรับรู้ถึงการเปลี่ยนแปลงของเครื่องมือทาง IT ที่เกิดขึ้นในทุกเวลา รวมถึงการพัฒนาองค์กรให้สอดคล้องกับนโยบายรัฐบาล แต่เหนืออื่นใด การดำเนินการทุกอย่างล้วนต้องคำนึงถึงผู้มีส่วนได้ส่วนเสียขององค์กรเป็นสำคัญ ต้องมีการรายงานและแสดงข้อมูลอย่างเปิดเผย

สรุปได้ว่ากรรมการสามารถจัดการกับความเสี่ยงด้านความปลอดภัยของไซเบอร์ได้ด้วยการ

1. สร้างโครงสร้างและผลักดันให้มีหน่วยงานด้าน IT โดยเฉพาะ และให้กรรมการทุกท่านรวมไปถึงพนักงานทุกคนตระหนักและตื่นตัวในเรื่อง IT อย่างจริงจัง
2. จัดเตรียมเครื่องมือ หรืออุปกรณ์ให้เหมาะสมกับการดำเนินงาน
3. วางกฎกติการ่วมกัน และกำหนดใช้ในทุกระดับทุกแผนก
4. ใช้ระบบที่มีมาตรฐานในการควบคุมความเสี่ยง

Preparation by Every Organization

Currently, launch of new technology systems as well as technological changes are happening all the time; and, therefore, in this 'cyber world' information technology (IT) systems have become essential for every type of business. Regardless, all companies need to urgently change and develop their technology systems to be in line with the current most IT trend on a regular basis; and, thus, one of the most important issue is: Meeting the potential risks within the cyber world.

This issue of the BOARDROOM, therefore, includes an interview with *Pol. Major General Dr. Supisarn Bhakdinarinath Chairman, Communication & System Solutions Pcl.*, in his capacity as a Board Director of a company that is directly involved with information technology as well as in being an expert with extensive experiences in technology matters and in the Public Sector.

IT related risks

Pol. Major General Dr. Supisarn stated that the various types of risks relating to IT systems — such as: the risk from remote hackers or hacking by terrorists using IT systems that infiltrate into various types of machinery or mechanical systems to cause a breakdown or interruption of their operations that result in damages and losses to the affected organization; or making use of IT systems to review and compile written evidence or information in VDO and photographic formats of the other parties for use in legal disputes. All such activities require the use of computers; and even teaching in primary schools also needs the use of computers. If the computer system can be hacked to change the existing information or data stored, it will result in significant damages for the affected party.

Directions in meeting such risks

From his viewpoint, *Pol. Major General Dr. Supisarn* sees that IT trends and associated systems will play an increasing role going forward. Organizations must adapt themselves to be able to meet such trends. They can begin by creating an internal unit specifically responsible for IT matters — such as an IT Unit/Department headed by the CIO/IT Director (ie: Chief Information Officer or Information Technology (IT) Director). The IT Unit has a significant degree of importance for the overall organization, since it is an internal unit that can help reduce costs in various operational aspects through implementing effective IT systems. It is also required to report on the security of the systems to the Board of Directors on a regular basis, so that possible trends can be predicted and continuous improvements can be made together with ongoing development of internal people resources to enable them to have the corresponding required capabilities.

Establishing relations with customers is an other required operational aspect, since in the cyber world customers are an important componentin driving the company's development and growth as well as in helping to create a positive corporate image.

Make use of a standard information storage system — such as, cloud or an application developed by large companies — instead of storing confidential company data on its existing server system together with its own data backup system, which is considered to be a major risk if the company does not have an effective security system in place. Therefore, making such an investment will incorporate a comprehensive security system — whether it is security relating to peoplen responsible for oversight, to audit, to the systems upgrade. Thus, engaging IT experts and specialists to be responsible for the management of the IT systems is a core and effective principle in creating cyber security.

Role of Board Directors and protecting from IT related losses or damages

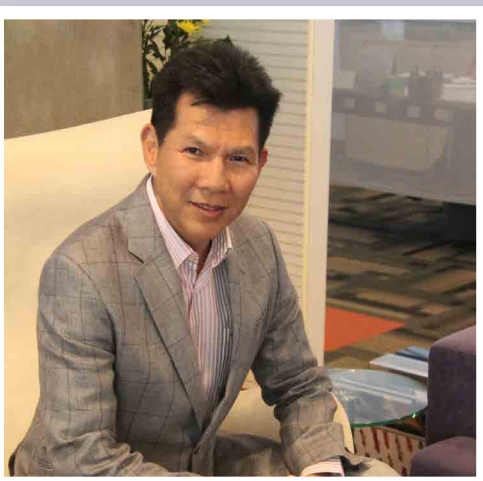
Pol. Major General Dr. Supisarn said that Board Directors need to develop themselves to be attuned to the latest ever-changing IT trends, as well as embed the use of IT systems into the corporate DNA, so that every Department make full use of them and hand down this corporate culture from generation to generation through the use of IT as a means of communications, until it becomes molded as an integral component of its corporate image.

***Pol. Major General Dr. Supisarn* also added that the development and planning of prevention measures against possible risks must depend on various factors** — for example, CSS chose to use outside resources to primary party for the implementation of its system, in order to achieve a basic understanding of the information and to be fully aware of the changes in IT tools that occurs at every point. Also, the development of the organization needs to be aligned with Government policies. But most important of all, every activity needs to take into consideration the Stakeholders and to report and disclose all relevant information in a open manner.

In summary, Board Directors can tackle the issue of managing risks relating to cyber security through as follows:

1. Determining a structure for and pushing to create a dedicated internal IT Unit/Department, as well as encouraging all Board Directors and every Staff member to become aware of and actively alert to IT related issues,
2. Making available all the required tools and equipments appropriate to its operations and activities,
3. Jointly determining the rules and regulations to be used at every level and Department,
4. Using systems that incorporate standards relating to controlling risks.

CyberSecurity: ไซเบอร์ป้องกันได้ด้วยการแชร์



คุณระเทียร ศรีมงคล
ประธานเจ้าหน้าที่บริหาร
บริษัท บัตรกรุงไทย จำกัด (มหาชน)
Mr. Rathian Srimongkol
Chief Executive Officer
Krungthai Card Plc.

อีกหนึ่งธุรกิจที่ต้องส่งผ่านข้อมูลต่างๆ ตลอดเวลา คงจะหนีไม่พ้นธุรกิจบัตรเครดิต ที่มีการทำธุรกรรมผ่านอินเตอร์เน็ต และไม่ใช่จำกัดเฉพาะแค่ประเทศไทยเท่านั้น แต่หมายถึงการส่งผ่านข้อมูลไปทั่วโลก การป้องกันที่ดีและรัดกุมเป็นเรื่องที่ท้าทายอย่างมาก *คุณระเทียร ศรีมงคล ประธานเจ้าหน้าที่บริหาร บริษัท บัตรกรุงไทย จำกัด (มหาชน)* ได้สละเวลาพูดคุยเรื่องความเสี่ยงในโลกไซเบอร์ รวมไปถึงการป้องกันได้อย่างน่าสนใจ

IT เข้ามามีบทบาทอย่างไร

เป็นที่ทราบกันดีแล้วว่า KTC ให้ความสำคัญกับความทันสมัยและนวัตกรรม จึงไม่แปลกใจที่ KTC ได้นำเทคโนโลยีสารสนเทศที่ทันสมัยเข้ามาเป็นส่วนสำคัญในการพัฒนาธุรกิจ เรียกได้ว่าเป็น Back Bone ขององค์กรเลยก็ว่าได้ ที่ KTC มีการจัดโครงสร้างด้าน IT เป็น 3 ระดับ คือ Plan จะเป็นหน่วยงานที่มีหน้าที่วางแผนการดำเนินงาน Build ที่เน้นการลงทุนเท่าที่จำเป็น และสุดท้ายคือ Run เป็นการดำเนินธุรกิจให้เดินไปอย่างต่อเนื่อง และมีประสิทธิภาพ โดยทั่วไปแล้วองค์กรอื่นๆ ในขั้นตอน Plan และ Build มักจะเป็นการใช้บุคคลภายนอกมาดำเนินงาน ทั้งการวางระบบ คิดโครงสร้าง แต่สำหรับ KTC เป็นการสร้างจากบุคลากรภายในองค์กร นั่นหมายถึงการเข้าใจตัวตนและลักษณะงานขององค์กร ทำให้สามารถวางแผนและสร้างระบบที่สามารถตอบทุกความต้องการได้อย่างลงตัว

KTC มองว่าการลงทุนงบประมาณเรื่องระบบไม่ใช่ประเด็นสำคัญ แต่ที่สิ่งสำคัญคือการพัฒนาบุคลากรขององค์กรให้เข้าใจและสามารถออกแบบระบบให้เหมาะสมกับองค์กร และจะต้องสามารถอธิบายให้ทุกคนเข้าใจได้เหมือนกัน ด้วยภาษาที่เข้าใจง่าย ไม่ใช่ศัพท์เทคนิค การพัฒนาจะเป็นไปในลักษณะที่ก้าวเดินไปพร้อมๆ กันทั้งองค์กร ซึ่งความรู้ตรงนี้ที่เป็นตัวแปรด้านมูลค่าในการพัฒนาระบบ ซึ่งอาจหมายถึงมูลค่าสูงจนแทนค่าไม่ได้เลยนั่นเอง สำหรับคณะกรรมการตรวจสอบ หรือคณะกรรมการที่มีหน้าที่บริหารความเสี่ยง ไม่จำเป็นต้องมีความเชี่ยวชาญด้าน IT แต่ควรจะมีพื้นฐานด้าน IT อยู่บ้างและให้ผู้เชี่ยวชาญมาอธิบายเพิ่มเติม นับเป็นแนวทางหนึ่งที่ช่วยให้คณะกรรมการทำหน้าที่ได้อย่างมีประสิทธิภาพมากขึ้น

แนวทางป้องกัน

ที่อเมริกามีการให้ความสนใจด้าน IT อย่างชัดเจน มีการตั้งหน่วยงานเกี่ยวกับ IT ขึ้นมาโดยเฉพาะ มีผู้บริหารชัดเจน หรือที่เรียกว่า Chief Information Security Officer - CISO มีการเสนอรายงานต่อผู้บริหารและคณะกรรมการอย่างสม่ำเสมอ มีการวางแผนงานเมื่อเกิดเหตุการณ์ แต่ในประเทศไทย *คุณระเทียร* คิดว่ามีการให้ความสนใจไม่มากเท่าที่ควร มักจะเป็นการแฝงอยู่ในหน่วยงานต่างๆ และมีการรายงานต่อผู้บริหาร เช่น Head of ERM (Enterprise Risk Management) หรือ CEO โดยจะรายงานเชิงสถิติ ตัวเลข รายละเอียดของ Transaction ต่างๆ ต่อ ERM แต่จะรายงานเพียงกรณีที่พบเจอความผิดปกติต่อ CEO ซึ่งเป็นสิ่งที่ไม่ค่อยถูกต้องเท่าที่ควร การรายงานที่ดีควรจะรายงานให้ทราบเหมือนกันทั้งฝ่าย ERM และ CEO รวมไปถึงคณะกรรมการ เพราะทุก Incident สามารถเป็นสัญญาณที่บ่งบอกถึงอะไรสักอย่างในอนาคต ทำให้เกิดการเฝ้าระวังและหาทางป้องกันได้บ่อยครั้งที่ผู้บริหารได้รับรายงานว่าพบการพยายามเจาะข้อมูล (Hack) ทั้งที่ทำสำเร็จและไม่สำเร็จ แต่นั่นหมายถึงจำนวนครั้งที่ถูกค้นพบ แต่ครั้งที่ไม่สามารถตรวจจับได้ว่ามีการพยายามเจาะข้อมูล มีจำนวนมากน้อยเท่าใดเราไม่มีทางทราบได้เลย ดังนั้น การเฝ้าระวังจากรายงาน Incident จะช่วยให้ให้คณะกรรมการและฝ่ายบริหารหาทางป้องกันได้อย่างทันท่วงที

คุณระเทียร บอกอีกว่าสิ่งที่สำคัญประการหนึ่งเมื่อเกิดเหตุการณ์ทาง Cyber ให้คิดว่าเราจะมีแผนอย่างไรในการแก้ไขปัญหา เริ่มแรกต้องคาดการณ์ความเสี่ยงต่างๆ ที่จะเกิดขึ้นให้ได้ว่ามีอะไรบ้าง แล้วแต่ละเหตุการณ์เราจะแก้ไขอย่างไร และป้องกันอย่างไร

Case Study

คุณระเทียร ยกตัวอย่างเหตุการณ์ที่เกิดขึ้นจริงว่ามีบริษัทหนึ่งได้รับการติดต่อจากคู่ค้า (Supplier) ว่าให้ทำการชำระเงินตามใบแจ้งหนี้หมายเลขที่ระบุ แต่ขอเปลี่ยนบัญชีที่รับชำระเงินเป็นเลขบัญชีใหม่ เมื่อบริษัทโอนเงินไปเรียบร้อยแล้ว ปรากฏว่าคู่ค้าตัวจริงมาทวงถามเงินที่ต้องทำการชำระ ทำให้รู้ว่าบริษัทโดนเจาะอีเมล์ นับเป็นความเสียหายอย่างมาก

สำหรับกรณีนี้ *คุณระเทียร* มองว่าการป้องกันไม่ใช่แค่เรื่องของเทคโนโลยี แต่เป็นเรื่องของระบบการดำเนินงานภายในองค์กร เช่นในกรณีนี้น่าจะมีระบบให้ตรวจสอบข้อมูลก่อนที่จะดำเนินการตามอีเมล์ เช่น มีการโทรศัพท์เพื่อตรวจสอบซ้ำอีกครั้งก่อนที่จะดำเนินการ จึงสรุปได้ว่าการจัดการความเสี่ยงด้านเทคโนโลยีต้องเป็นส่วนหนึ่งของการจัดการความเสี่ยงภาพรวมขององค์กร

ป้องกันได้ด้วยการแบ่งปันประสบการณ์

การมีแนวปฏิบัติที่ชัดเจนจะช่วยให้บริษัทมีโอกาสตรวจสอบขั้นตอนต่างๆ ที่วางไว้ว่ามีความปลอดภัยมากเพียงพอหรือไม่ และสิ่งสำคัญอีกประการที่ช่วยเรื่องการป้องกันได้อย่างดี คือ ควรจะมีการแบ่งปันประสบการณ์ในสิ่งที่เกิดขึ้น เพราะจะช่วยให้บริษัทอื่นๆ สามารถวางแนวทางการป้องกันความเสียหายที่จะเกิดขึ้นได้ โดยไม่ต้องเกิดความเสียหายก่อน

ในช่วงท้ายของการสัมภาษณ์ *คุณระเทียร* พูดถึงความแตกต่างระหว่างประเทศไทย และต่างประเทศในเรื่องการเปิดเผยข้อมูลในเรื่องความปลอดภัยของไซเบอร์ว่าในต่างประเทศมีการเปิดเผยข้อมูลต่างๆ รวมถึงความผิดปกติที่เกิดขึ้นอย่างชัดเจน เพื่อให้บริษัทอื่นเกิดความตื่นตัวและสามารถวางแนวทางป้องกันได้ และวิธีคิดของผู้บริหารของต่างประเทศเมื่อเกิดความผิดพลาดขึ้นจะมองว่ามันคือการเรียนรู้ เป็น Learning Curve เป็นสิ่งที่ต้องรับมือ และหาวิธีการแก้ไขป้องกัน สิ่งเหล่านี้คือจุดเด่นที่เราควรนำมาปรับใช้ให้เกิดประโยชน์ต่อไป

Cyber could be protected by sharing

The credit card business involves the transfer of large amounts of date at all times. The data transfer is not just limited to Thailand, but is global. A good and strict prevention of crimes in the cyber world is a challenge for businesses. *Mr. Rathian Srimongkol, Chief Executive Officer of Krungthai Card Plc.* granted us an interview to discuss risk in the cyber world and preventive approaches.

What was the role of information technology?

It was well known that KTC focused heavily on technology and innovation and not surprising that KTC had adopted state-of-art information technology as a key component in business development. The technology served as the backbone of the organization. KTC had an IT structure consisting of three levels, Plan, Build and Run. Plan was the departmen responsible for making an operational plan. Build focused on necessary investment. Run was the ongoing and effective operation. Most organizations had outsourced external experts in Plan and Run, including setting a system and creating a structure, while KTC had relied on personnel in the organization, as they better understood the identity and characteristics of the organization. As a consequence, they could plan and create a system that meets the bank's requirements.

KTC was not overly concerned about the investment budget in the system. The key issue was to develop personnel in the organization to understand and design a proper system for the organization. Importantly, the personnel needed to be able to explain to others how the system works and ensure that there was a clear understanding and that simple language not jargon was used. The development involved a concerted effort by the whole organization. This knowledge was a valued variable in the system development. The value might be so high and priceless. The Audit Committee or Risk Management Committee was not required to have the IT expertise, but it should have basic knowledge of it, with experts available to provide detailed explanations. This was one approach to enhance the effectiveness of the Board of Directors.

Protective approach

In the United States, there was clearly an interest in IT. Companies set up IT departments with executives and the top post being Chief Information Security Officer (CISO), who reported to the management and Board of Directors regularly. Interest in this issue in Thailand was minimal. In various Thai organizations, staff members overseeing IT operations tended to report to the Head of ERM (Enterprise Risk Management) or CEO by reporting statistic data, number and details of transactions to ERM. They would only report IT-related cases that seemed abnormal, which was not thorough enough. All suspicious cases should be reported to the ERM and CEO, including the Board of Directors, because every incident could be a sign of something in the future that needs to be monitored and prevented. Often, the cases reported to management pertaining to successful and unsuccessful of hacking of data, but only some of the cases were detected. It is now known how many of them went undetected. Thus, monitoring from the incident report could help the Board of Directors and the management to prevent hacking from occurring.

Mr. Rathian added that when there was a cyber incidence, the bank had to think what the best resolution is. First, it had to anticipate the risks that could occur, which would then allow it to solve and prevent the problem from occurring again. .

Case Study

Mr. Rathian raised a case study, which involved a company that was approached by a supplier to pay its bill to a new bank account. The company paid the bill as requested, but soon after received a payment request form the real supplier. Finally the company's email had been hacked, which resulted in extensive damages.

That case proved that a company not only should be protected technologically, but the organization should be protected as well. The company should have checked the information before acting according to the e-mail. For example it could have rechecked the bill. In conclusion, risk management in technology must be a component in the overall risk management of the organization.

Protection by sharing experience

A clear guideline would help an organization to recheck every procedure if it was suffificiently safe. Importantly, sharing an experience contributes to good protection because it could help other organizations to prepare an approach to prevent the damage beforehand.

At the end of the interview, *Mr. Rathian* talked about the difference between Thailand and other countries regarding information disclosure pertaining to the security of the cyber world. In other countries, information disclosure is more readily used, including abnormalities to raise awareness of other organization and plan a preventive approach.

Moreover, in the mindset of the executive, **mistakes were considered to be part of the learning curves** for dealing with **and preventing damage in the cyber world. By highlighting those mistakes, everyone can learn and adapt in the context of Thailand.**

CyberSecurity: เข้าใจไอที เข้าใจความเสี่ยง

คุณธีรนันท์ ศรีหงส์
กรรมการผู้จัดการ
ธนาคารกสิกรไทย จำกัด (มหาชน)
Mr. Teeranun Srihong
Managing Director
Kasikornbank Plc.

ในประเทศไทยธุรกิจธนาคารนับว่าเป็นธุรกิจที่มีความก้าวไกลในเรื่องการใช้ระบบเทคโนโลยีสารสนเทศและการป้องกันความเสี่ยงที่อาจเกิดขึ้น จากการใช้งาน Boardroom ฉบับนี้จึงขอสัมภาษณ์ *คุณธีรนันท์ ศรีหงส์ กรรมการผู้จัดการธนาคารกสิกรไทย จำกัด (มหาชน)* เกี่ยวกับแนวทางที่ทางธนาคารได้นำเทคโนโลยีไปใช้ประโยชน์และการจัดการกับความเสี่ยงที่อาจเกิดขึ้น เพื่อเป็นประโยชน์กับภาคธุรกิจอื่นๆ ที่ต้องการใช้เทคโนโลยีสารสนเทศให้เป็นประโยชน์ในการธุรกิจและมีแผนการจัดการความเสี่ยงอย่างเหมาะสม

IT กับงานธนาคาร

คุณธีรนันท์ เล่าให้ฟังว่าทางธนาคารได้นำเทคโนโลยีมาใช้ในการดำเนินงานในองค์กรมากกว่า 30 ปีแล้ว ในช่วงแรกเป็นการนำมาใช้งานเพื่อเพิ่มประสิทธิภาพของกระบวนการทำงานต่างๆ ภายในองค์กร แต่ต่อมาเทคโนโลยีได้ขยายบทบาทออกไปมากกลายเป็นเครื่องมือสำคัญที่ใช้สร้างความภักดีกับลูกค้า นำระบบของธนาคารและระบบของลูกค้ามาผูกกันเพื่อความพึงพอใจสูงสุดของลูกค้า เทคโนโลยีกลายเป็นเครื่องมือทางกลยุทธ์ทั้งในการบริหารงานลูกค้าและเพิ่มประสิทธิภาพการทำงานขององค์กร การขยายขอบเขตไปสู่ Social Media และเทคโนโลยีมือถือในปัจจุบันกลายเป็นเครื่องมือในการทำธุรกิจที่สำคัญขององค์กร

จากการใช้เทคโนโลยีมากทำให้ความเสี่ยงมากขึ้นตามไปด้วย ธนาคารจะต้องมั่นใจว่าเทคโนโลยีที่ใช้อยู่นั้นสามารถใช้ได้อย่างต่อเนื่องไม่หยุดชะงัก ข้อมูลที่มีในระบบไม่ได้รับการใช้ในทางที่ไม่เป็นประโยชน์ มีการป้องกันข้อมูลลูกค้าอย่างดีให้ปลอดภัยจากทั้งอาชญากรรมทางอีเลคทรอนิคส์ (Crime) และการทุจริต (Fraud) ต่างๆ

คุณธีรนันท์ กล่าวว่าใช้เทคโนโลยีแล้วต้องคุมให้ได้ ไม่ให้เป็นเครื่องมือที่มาทำร้าย ถ้าอาศัยเทคโนโลยีในการทำงานก็จะต้องชัดเจนว่าการทำงานเทคโนโลยีนั้นมีความต่อเนื่องและมีความปลอดภัย

การจัดการความเสี่ยงด้านเทคโนโลยี

คุณธีรนันท์ แบ่งปันให้ฟังว่าทางธนาคารได้มีการจัดวางโครงสร้างที่ดูแลเรื่องนี้โดยเฉพาะมีการจัดตั้งคณะอนุกรรมการบริหารความเสี่ยงด้านปฏิบัติการโดยกรรมการผู้จัดการเป็นประธานของคณะฯ ซึ่งมีเรื่องเทคโนโลยีสารสนเทศเป็นเรื่องที่ใหญ่และสำคัญในคณะฯ นี้ การรายงานขึ้นตรงต่อคณะกรรมการความเสี่ยงซึ่งมีคณะกรรมการชุดใหญ่เป็นสมาชิกในคณะนี้โดยมีกรรมการผู้จัดการอยู่ด้วย ภายใต้คณะกรรมการความเสี่ยง มีคณะกรรมการที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศโดยเฉพาะจึงสามารถให้มุมมองและคำแนะนำที่เป็นประโยชน์ และหลายครั้งท่านคณะกรรมการได้มีการพูดคุยกับ Chief Information Officer (CIO) โดยตรงเป็นการส่วนตัว โดยคณะกรรมการความเสี่ยงจะกลั่นกรองเรื่องที่จะนำเสนอคณะกรรมการชุดใหญ่อีกครั้ง

การจัดการความเสี่ยงนั้นต้องเริ่มจากการทำความความเข้าใจความเสี่ยงที่มีอยู่ ทางธนาคารได้มีจัดหมวดหมู่ความเสี่ยงด้านเทคโนโลยีออกมาเป็น 10 ด้าน และทำการประเมินความเสี่ยงความเสี่ยงแต่ละด้าน โดยร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยี (IT Key Risk Indicator) ที่สำคัญเพื่อจัดลำดับผลกระทบที่เกิดขึ้นจากความเสี่ยง หลังจากนั้นได้จัดทำแผนเพื่อป้องกันความเสี่ยง (Risk Treatment Plan) การทำตามแผน และการติดตามแผนอย่างต่อเนื่องโดยมีการจัดให้ทำรายงานความเสี่ยง (Risk Reporting) เป็นประจำ โดยทางธนาคารได้หมวดหมู่ความเสี่ยง 10 ด้านได้แก่

ด้านความปลอดภัยของเทคโนโลยีสารสนเทศ (IT security risks) ทั้งข้อมูลและระบบในเรื่องการรักษาความลับ ความถูกต้อง ความพร้อมในการใช้งาน

ด้านข้อมูล (Data risks) เช่น ข้อมูลสูญหาย รั่วไหล ถูกปลอมแปลง หรือทำลาย

ด้านผู้ขายและผู้ให้บริการงานเทคโนโลยีสารสนเทศ (IT Vendor/ Supplier risks) เพื่อจะมั่นใจว่าผู้ให้บริการสามารถทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง

ด้านการปฏิบัติการงานเทคโนโลยีสารสนเทศ (IT Operational risks) เช่น การวางแผนพัฒนาการออกแบบระบบ และ**โครงสร้างด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware risks)** ที่อาจเกิดการทำงานผิดพลาดหรือไม่ทำงาน

ด้านโปรแกรมเทคโนโลยีสารสนเทศ (Software risks) ที่อาจเกิดการทำงานผิดพลาดหรือไม่พร้อมใช้งาน

ด้านการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project management risks) ที่อาจล่าช้า หรือไม่สำเร็จจากสาเหตุต่างๆ เช่น การวางแผนที่ไม่รัดกุมและการจัดสรรทรัพยากรที่ไม่เพียงพอ

ด้านบุคคลากร (Personnel risks) ที่อาจขาดความรู้และทักษะ การจัดคนที่ไม่เหมาะสมกับงานรวมไปถึงการทุจริตต่างๆ

ด้านการกู้ระบบจากเหตุการณ์ฉุกเฉินและการบริหารความต่อเนื่องของการให้บริการงานเทคโนโลยีสารสนเทศ (Disaster Recovery and IT Continuity risks)

ด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎหมาย (Compliance risk)

คุณธีรนันท์ เสริมเพิ่มเติมว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องเริ่มจากนโยบายขององค์กรที่ชัดเจนจากคณะกรรมการและผู้บริหารว่าจะให้ความสำคัญเกี่ยวกับเรื่องนี้ และมีการกำหนดผู้รับผิดชอบที่ชัดเจนที่จะมองภาพรวมและติดตามให้เป็นไปตามแผน แต่ในรายละเอียดความเสี่ยงแต่ละตัวหน่วยงานที่เกี่ยวข้องต้องเข้ามามีส่วนร่วม และการป้องกันความเสี่ยงต้องเข้าใจว่าเทคโนโลยีเป็นเรื่องที่เปลี่ยนแปลงเป็นรายวัน หน่วยงานทุกหน่วยงานต้องมีวินัยในการบริหารประจำวัน ติดตามผลและทบทวนแผนงานเป็นประจำ เพราะเห็นว่ากรณีที่เกิดขึ้นส่วนมากมาจากภายในองค์กรทั้งความสามารถที่ไม่เพียงพอของบุคคลากรและการทุจริตของบุคคลากรมากกว่าจะเป็นคนภายนอกที่เข้ามาจารกรรมข้อมูล จึงต้องมีระบบในการติดตามการปฏิบัติงานด้านต่างๆ อย่างสม่ำเสมอ ความเสี่ยงต้องได้รับการประเมินได้ว่าเป็น incident คือ เกิดขึ้นครั้งเดียวหรือเป็น problem คือ ปัญหาระยะยาวขององค์กร

ความร่วมมือเพื่อพัฒนา

คุณธีรนันท์ ให้ความคิดเห็นว่าการพัฒนาการดำเนินงานด้านเทคโนโลยีสารสนเทศในประเทศไทยในส่วนของภาครัฐควรจะมีนโยบายและวิธีการที่ทำให้บริษัทต่างๆ ลดต้นทุนในการบริหารความเสี่ยงเรื่องนี้ได้ เช่น การให้ข้อมูลกับประชาชน เพราะหลายครั้งอาชญากรรมทางไซเบอร์เกิดจากความไม่รู้ของผู้ใช้งาน อีกด้านหนึ่งคือ การออกกฎหมายที่มีบทลงโทษที่เหมาะสมสำหรับผู้ที่ทำผิดและลงโทษ

อย่างรวดเร็ว หน่วยงานต่างๆ ของรัฐควรที่จะร่วมมือกันในการวางแผนป้องกันอาชญากรรมไซเบอร์อย่างบูรณาการ และมีช่องทางให้ร้องเรียนได้หากเกิดกรณีที่ผิดปกติ

ภาคธนาคารมีธนาคารแห่งประเทศไทยที่ทำงานอย่างเข้มแข็งในการวางแนวนโยบายเกี่ยวกับเรื่องการใช้เทคโนโลยีสารสนเทศ มีการแนะนำเพื่อให้ธนาคารปรับปรุงอย่างต่อเนื่อง และมีการทำทดสอบเช่นการเจาะข้อมูลอย่างต่อเนื่องในระหว่างธนาคารเองมีการวางมาตรฐานกลางร่วมกันเมื่อต้องมีการเชื่อมระบบระหว่างกัน ในบริษัทจดทะเบียนในธุรกิจอื่นๆ อาจจะยังให้ความใส่ใจในเรื่องนี้น้อยเพราะยังเน้นเรื่องการสร้างผลประกอบการมากกว่า

คุณธีรนันท์ จึงแนะนำว่าคณะกรรมการและผู้บริหารจะต้องให้ความสำคัญกับเรื่องนี้ก่อน เชื่อว่าความเสี่ยงเรื่องนี้มีอยู่จริง ถ้าบริษัทใดไม่มีการพูดคุยเรื่องนี้ในที่ประชุมคณะกรรมการเลยอาจเป็นเรื่องที่ผิดปกติ เมื่อผู้นำองค์กรให้ความสำคัญและเริ่มดำเนินการเรื่องนี้ก็น่าจะร่วมกับบริษัทอื่นๆ ในการให้ความรู้กับลูกค้าเกี่ยวกับเรื่องนี้เพื่อขยายวงความเข้าใจให้กว้างขวางมากยิ่งขึ้น

The Risk from Information Technology

The banking industry in Thailand is increasing its use of advancing information technology (IT) and along with this is the need for risk management associated with using that technology. For this issue of Boardroom, we have interviewed *Mr. Teeranun Srihong, Managing Director of Kasikornbank Plc.* about his bank's approach for adopting information technology and managing the potential risk from it for the benefit of other businesses that would like to use IT in their business and set a proper risk management plan.

Information technology and banking

Mr. Teeranun told us that the bank began adopting IT for its operations more than 30 years. It fifirst used IT to enhance the effectiveness of the working process in the organization. Then, it was used for more functions, especially as a tool to build customer loyalty. He explained that the bank integrated the system of customers and the bank together to attain the highest satisfaction of the customers. Technology became a strategic tool in administrating customer affairs and enhancing effectiveness of the organization. Currently, the bank is expanding its scope to social media and mobile phone technology, which has become an important business tool of the organization The use of more technology has resulted in more risks, said *Mr. Teeranun*. The bank had to be sure that the technology was using which could be used constantly and the he data in the system were not abused. Customer data had to be well protected from electronic crimes and frauds.

Mr. Teeranun said that when the banks adapts new technology, it must be able to control the technology to prevent it from becoming counterproductive to the operations. In line with becoming more dependent on the technology, the bank must ensure that it functions consistently and is secure.

Technological risk management

Mr. Teeranun shared the experience Kasikorn Bank had with a particular structure for technological risk management. An operational risk management subcommittee was set up with the Managing Director assuming the role as its chairman. IT was the new big issue for the subcommittee, which reported directly to the Risk Committee. The Risk Committee consisted of some member of the Board of Directors and the Managing Director and had several experts in technology at its disposal, particular those who could provide a general overview and useful recommendations. Sometimes, the committee also had a meeting with Chief Information offifficer (CIO) directly. The Risk Committee would review the key issues to report to the Board of Directors again.

Risk management must begin with understanding the existing risks. The bank had categorized technological risks into 10 categories and assessed the risk in each category. It also cooperated with relevant organizations to make IT key risk indicators in order to rank the impact from the risks. Then, it developed a risk treatment plan and an implementation and monitoring plan, which entailed submitting risk reports on a regular basis. The bank had categorized risks into 10 categories, as follows, IT security risks, including data and security system, accuracy and readiness of operation; Data risks, such as data loss, data leakage and data that was forged or destructed;
IT vendor/supplier risks to ensure that the supplier could work effectively and constantly;
IT operational risks, such as development plan, system design and structure;
Hardware risks, hardware that may malfunctioned or out of order;
Software risks, software that may be malfunctioned or unavailable;
IT project management risks, projects what miss their deadline or be unsuccessful because of various causes, such as weak planning and insuffifficient resource allocation;
Personnel risks that employees may lack knowledge or skills, bad personnel management and corruption;
Disaster recovery and IT continuity risks;
Compliance risks.

Mr. Teeranun added that technological risk management had to begin with a clear policy of the organization that the Board of Directors and management would focus on this issue and assign a capable person to review the plan and take charge of implementing it. Then, the relevant department was responsible for each risk. Risk management relied on the understanding that technology changed daily. Every department had to be responsible for daily administration and monitoring and reviewing the implementation plan on a regular basis because most problems were caused by internal factors, such as insufficient expertise and corruption of personnel rather than by hacking from outsiders. Therefore, the company needed a system to monitor the operations regularly. Each risk had to be evaluated as an incident, or a long-term problem of the organization.

Cooperation for development

Mr. Teeranun noted that regarding to IT development in Thailand, the public sector should have a policy and approach that enabled companies to reduce cost in technological risk management, such as providing information to the public because cybercrimes could sometimes be the result of ignorance by the users. He explained that legislation with appropriate penalties for those who committed cyber-crimes should be in place. Public agencies should cooperate with each other to build a defense against cyber-crime and provide a complaint channel when there is an unusual case.

In the banking sector, the Bank of Thailand had worked hard in the area of policy orientation on the use of information technology. Staff members were constantly recommended to enhance their knowledge and expertise in that area. In addition, there was a penetration test on the banking system and a central standard was imposed for connections among banks. Other listed companies might have less interest in technological risk management because they were more interested in the company performance. But, he stated that this should not be the case. All Boards of Director must realize the existence of technological risk. It was unusual if the company did not discuss this issue in the Board meeting. When the organization leaders started to take a serious interest in this issue,

the company should cooperate with other companies ***to*** **educate** **the *customers*** **with the objective to widen** the scope **of understanding on this important issue.**