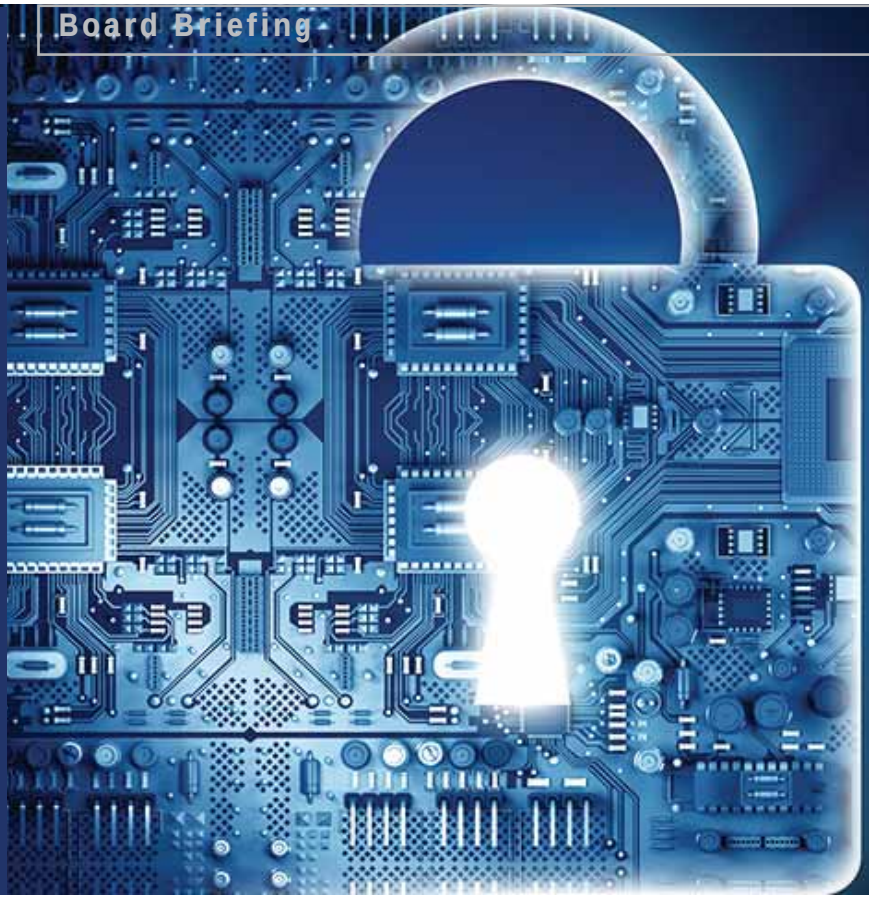

Dealing with Cyber Risk in the Boardroom

สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย ร่วมมือกับ Deloitte ได้จัดงาน IOD Director Briefing (Tea Talk) 1/2018 ในวันที่ 19 มีนาคม 2561 ณ ห้องบอลรูม โรมแรมเรเนซองส์ ราชประสงค์ โดยงานนี้ได้รับเกียรติจาก Mr. Thio Tse Gan กรรมการบริหาร ผู้นำด้านความเสี่ยงไซเบอร์เอเชียตะวันออกเฉียงใต้จาก Deloitte ในการบรรยายพิเศษในหัวข้อ "Dealing with Cyber Risk in the Boardroom" ใจความสำคัญสรุปได้ดังต่อไปนี้

Mr. Tse Gan กล่าวว่าการจัดการกับความเสี่ยงทางไซเบอร์นั้น แท้จริงแล้วเป็นหน้าที่รับผิดชอบของทุกคน มิใช่ความรับผิดชอบของฝ่าย IT, CEO หรือคณะกรรมการที่ได้รับมอบหมายให้ดูแลฝ่าย IT เท่านั้น

Mr. Tse Gan ได้ชี้ให้เห็นถึงการเพิ่มขึ้นอย่างน่าตกใจของสถิติอาชญากรรมในโลกไซเบอร์ ดังนี้

- โดยเฉลี่ยแล้วมีมัลแวร์ 200,000 ตัว เกิดขึ้นมาใหม่ทุกวัน
- 76% ขององค์กรต่างๆรายงานว่าตกเป็นเหยื่อของการโจมตีแบบ Phishing ในปี 2016
- 86 ประเทศขึ้นทะเบียนกับ DDos attack ใน Q2 2017 และสถิติที่ยาวนานที่สุดคือ 277 ชั่วโมง
- เกิดมัลแวร์เรียกค่าไถ่ (Ransomware Attack) มากกว่า 4,000 รายการในแต่ละวัน นับตั้งแต่ต้นปี 2016

ด้วยเหตุนี้ เขาจึงกล่าวย้ำถึงความสำคัญในการตระหนักถึงความเปลี่ยนแปลงต่างๆที่เกิดขึ้น

ดัชนีวิวัฒนาการดิจิทัล 2017 จาก HBR แสดงให้เห็นว่าหลายประเทศรวมถึงประเทศไทยนั้นกำลังก้าวเข้าสู่ Digitalization หรือการปรับระบบการทำงานเข้าสู่ระบบดิจิทัล สมาร์ทโฟนได้กลายเป็นส่วนหนึ่งของชีวิตผู้คน โดยแท้จริง อุปกรณ์อิเล็คโทรนิคนี้มีอิทธิพลต่อชีวิตเราขึ้นมากและมันกำลังเปลี่ยนแปลงวิธีการทำงานและควบคุมวิธีการแบ่งปันข้อมูลของเรา

การเปลี่ยนแปลงอีกหนึ่งอย่างที่ Mr. Tse Gan กล่าวถึง คือการที่เราให้ความสำคัญกับโซเชียลมีเดียอย่างล้นหลาม ผู้คนแชร์ทุกสิ่งทุกอย่างที่ทำจากทุกๆที่ และท้ายที่สุดแล้ว การแบ่งปันข้อมูลหรือการแชร์นี้ก็ได้กลายมาเป็นส่วนหนึ่ง

Mr. Tse Gan

ของชีวิต สิ่งที่ Mr. Tse Gan เป็นกังวลก็คือ เมื่อเวลาที่ทุกคนแชร์เรื่องราวต่างๆนั้น พวกเขาได้แชร์ข้อมูลที่เป็นความลับของทางบริษัทไปด้วยหรือไม่ สิ่งที่พึงระวังคือรูปภาพของสิ่งต่างๆในที่ทำงานนั้นสามารถเปิดเผยข้อมูลบางอย่างได้โดยที่ไม่ตั้งใจ

ความเสี่ยงทางไซเบอร์ที่มาพร้อมกับเทคโนโลยี ได้ถูกหยิบยกขึ้นมาให้เห็นในการบรรยายนี้ อย่างแรก ความเสี่ยงที่มาพร้อมกับ Cloud เป็นที่ปฏิเสธไม่ได้ว่า Cloud นั้นมีประโยชน์มากมาย แต่การที่มันสามารถถูกเข้าถึงได้จากทุกที่นั้นก่อให้เกิดความเสี่ยงจากการถูกแฮกข้อมูล นอกจากนี้การใช้ Cloud ยังมีความเสี่ยงในเรื่องของการถูกคัดลอกและส่งต่อข้อมูลโดยผู้ให้บริการ Cloud เอง เนื่องจากกรรมสิทธ์ของข้อมูลนั้นอาจเป็นของ Cloud ด้วยเช่นกัน อย่างที่สอง ความเสี่ยงที่มาพร้อมกับ Internet of Things (IoT) เทคโนโลยีที่สามารถใช้ประโยชน์ได้ในหลายๆด้าน เช่น โดรน และ RFID แต่หากอุปกรณ์ IoT ไม่ได้ถูกจัดการและควบคุมอย่างเหมาะสม อาจก่อให้เกิดหายนะขึ้นได้ ยกตัวอย่างเช่น เหตุการณ์เมื่อสองปีที่แล้ว MIRAI การโจมตีทางไซเบอร์ที่แผ่คลุมไปทั่วโลกที่ได้เจาะข้อมูลผ่านกล้องดูเด็ก (Baby Monitor) เป็นล้านๆเครื่อง อันเป็นผลทำให้บริษัทแห่งหนึ่งเกือบปิดตัวลง และสาม ความเสี่ยงที่มาพร้อมกับ Robotics จริงอยู่ที่ระบบปฏิบัติการด้วยหุ่นยนต์นั้นมีข้อดีมากมาย แต่ข้อผิดพลาดที่ก่อให้เกิดความเสียหายก็สามารถเกิดขึ้นได้เช่นกัน

คำถามของ Mr. Tse Gan คือ "คุณจะคำนึงถึงเรื่องความเสี่ยงเหล่านี้เมื่อใด เมื่อเกิดเหตุการณ์นั้นแล้ว หรือคุณจะให้ความสำคัญกับมันอย่างสม่ำเสมอ เพราะโดยแท้จริงแล้ว ตัวคุณเองและพนักงานทุกคนนั้นมีส่วนเกี่ยวข้องกับดิจิทัลมากกว่าที่คิด" เขาย้ำชัดอีกว่า เราต้องคำนึงถึงเรื่องความปลอดภัยและต้องเป็นกังวลถึงเรื่องความเสี่ยง เนื่องจากสิ่งเหล่านี้เป็นส่วนหนึ่งของธุรกิจที่เราดำเนินในทุกๆวัน หากเราจัดการมันได้ไม่ดี ชื่อเสียงของธุรกิจที่กำลังดำเนินอยู่อาจจะต้องถูกทำลาย

การแฮก (Hack) หรือการเจาะข้อมูลเป็นหนึ่งในภัยคุกคามที่ร้ายแรงที่สุด เมื่อเรากล่าวถึงการรับมือกับการถูกแฮกข้อมูล เรามักจะนึกถึงระเบียบข้อบังคับ การสื่อสารกับฝ่ายต่างๆ โดยเฉพาะอย่างยิ่งกับลูกค้า และสภาพแวดล้อมภายนอกอื่นๆ แต่สิ่งหนึ่งที่เรามักหลงลืมไปคือสิ่งที่ซ่อนอยู่ภายใต้พื้นผิว (Beneath the Surface) ในที่นี้คือความเสียหายอันเนื่องมาจากตัวเชื่อมที่ส่งผลกระทบต่อแก่นของบริษัท สำหรับ Mr. Tse Gan สิ่งเหล่านั้นคือทรัพย์สินทางปัญญา อันได้แก่ ชื่อทางการค้า, ค่านิยมของลูกค้าและความเชื่อมั่นที่ลูกค้ามี เราต้องใช้เวลาถึง 5-6 ปี ในการกอบกู้ความเชื่อมั่นของลูกค้าที่สูญเสียไปและมูลค่าความเสียหายของการกอบกู้ชื่อเสียงของบริษัทนั้นมหาศาลกว่าที่คาดการณ์ไว้เสมอ

Mr. Tse Gan กล่าวต่อว่า สุขลักษณะทางไซเบอร์ (Cyber Hygiene) นั้นเริ่มที่ตัวบุคคล และนี่คือ 10 สิ่งที่วิทยากรได้แบ่งปันสำหรับเป็นแนวทางในการเสริมสร้างสุขลักษณะทางไซเบอร์ที่ดี

1. ติดตั้งซอฟต์แวร์รักษาความปลอดภัยจากผู้ให้บริการที่เชื่อถือได้และหมั่นอัพเดตอยู่เสมอ
2. ใช้เว็บไซต์และแอปพลิเคชั่นบนมือถือที่น่าเชื่อถือเท่านั้น
3. ระมัดระวังในการเลือกรับเพื่อนบนโซเชียลมีเดียและข้อมูลที่คุณแชร์
4. ระวังป๊อปอัพต่าง ๆ และอย่าไว้ใจทุกสิ่งที่ฟังดูดีเกินจริงบนอินเตอร์เน็ต
5. ตั้งรหัสผ่านที่หลากหลาย และแข็งแรงสำหรับแต่ละบัญชี
6. เปิดเฉพาะไฟล์แนบที่คุณรู้แน่ชัดว่าคืออะไร แม้ว่าไฟล์นั้นจะถูกส่งมาจากคนที่คุณรู้จักก็ตาม
7. เก็บข้อมูลสำคัญให้ปลอดภัย เอกสารลับหรือ USBs ควรถูกเก็บไว้ในที่ปลอดภัย และหลีกเลี่ยงการเขียนรหัสผ่านลงบนกระดาษ
8. ระวังคนแปลกหน้าที่เข้าไปในที่ทำงานของคุณ
9. ระมัดระวังเมื่อเชื่อมต่อกับระบบเครือข่ายไร้สายสาธารณะ (Public Wireless Networks) การอยู่บนระบบที่ปลอดภัยไม่ได้การันตีว่าคุณจะปลอดภัยจากผู้ใช้งานร่วมเครือข่ายที่ประสงค์ร้าย
10. ตระหนักถึงแนวโน้มด้านความปลอดภัยและภัยคุกคามในปัจจุบัน

นอกจากนี้เขายังได้เสนอแนวทางในการลดความเสี่ยงจากการถูกคุกคามที่อาจเกิดขึ้นเมื่อนำเทคโนโลยีใหม่ ๆมาใช้ แนวทางนั้นได้แก่ 1) การวางกลยุทธ์สำหรับไซเบอร์ สามารถทำได้โดยการจัดตั้งโปรแกรมสำหรับความเสี่ยงทางไซเบอร์ที่สอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์และความเสี่ยงขององค์กร 2) การวางความมั่นคงและปลอดภัย คือมีกระบวนการจัดการความเสี่ยง เพื่อป้องกันภัยจากการคุกคามที่คาดการณ์ไว้และที่เกิดขึ้นอย่างกะทันหัน 3) มีความระมัดระวังและตื่นตัวอยู่เสมอ คือการมีความรอบรู้ด้านภัยคุกคามและรอบรู้สถานการณ์ เพื่อที่จะคาดการณ์และระบุพฤติกรรมที่เป็นอันตราย และ 4) มีความยืดหยุ่นเพื่อฟื้นคืนสภาพ คือมีการเตรียมความพร้อมและความสามารถที่จะแก้ไขและกอบกู้สถานการณ์จากเหตุการณ์คุกคามและลดผลกระทบให้เหลือน้อยที่สุด

พึงระลึกไว้เสมอว่า การโจมตีทางไซเบอร์นั้นไม่เคยเป็นหายนะที่เกิดเพียงครั้งเดียว ดังนั้นทุก ๆฝ่าย นับตั้งแต่ผู้บริหารระดับสูงไปจนถึงพนักงานต้องมีความพร้อม หนึ่งในแง่มุมที่ยากที่สุดคือเรื่องของบุคลากร คุณต้องแน่ใจว่าวัฒนธรรมขององค์กรนั้นได้ถูกรวมเรื่องนี้เข้าไปด้วยเหตุนี้การฝึกสอนและอบรบจึงเป็นเรื่องที่สำคัญมาก

Mr. Tse Gan ได้ส่งท้ายการบรรยายด้วย 10 ขั้นตอนสำคัญเพื่อการเตรียมความพร้อมสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ดังนี้

1. สร้างบรรยากาศร่วม ให้ผู้นำได้มีส่วนร่วมในการจัดการความเสี่ยงทางไซเบอร์
2. ประเมินความเสี่ยงโดยครอบคลุมดูภาพรวมในองค์กร, ICD และผลิตภัณฑ์ที่เกี่ยวข้อง
3. ให้คนมีส่วนร่วมในแฟ้มความเสี่ยง (Risk Profile) แบ่งปันผลข้อมูลกับผู้นำและคณะกรรมการบริษัท
4. สร้างความปลอดภัย โดยการประสานการลงทุนและโปรแกรมจัดการความเสี่ยงทางโลกไซเบอร์เข้าด้วยกัน
5. จำไว้เสมอว่าข้อมูลคือทรัพย์สินเชื่อมต่อมูลค่าทางธุรกิจเข้ากับข้อมูลและกลยุทธ์เพื่อปกป้องข้อมูลบริษัท
6. ประเมินความเสี่ยงจากบุคคลที่สาม อันได้แก่ การประเมินความเสี่ยงของผู้ให้บริการด้านความเสี่ยงด้านไอทีและผู้ให้บริการเครือข่ายและบุคคลอื่น ๆ
7. รอบคอบในการเฝ้าระวังตรวจสอบ ระบุให้แน่ชัดว่าช่องโหว่ในส่วนสำคัญของบริษัทนั้นจะถูกตรวจสอบพบหรือไม่และรวดเร็วเพียงใด
8. เตรียมพร้อมอยู่เสมอ โฟกัสกับการเตรียมการรับมือเหตุการณ์ต่าง ๆและช่องโหว่ที่อาจเกิดขึ้น โดยใช้หลักการจำลองสงคราม
9. แบ่งหน้าที่ความรับผิดชอบในองค์กรให้ชัดเจนหาคำตอบให้ได้ว่าเรื่องไซเบอร์นี้อยู่ในความรับผิดชอบของฝ่าย IT ฝ่ายเดียวหรือเป็นหน้าที่ของทุกคน
10. เสริมสร้างความตระหนัก ให้พนักงานทุกคนได้มีส่วนร่วมและรับรู้บทบาทหน้าที่ตนเองในการปกป้องค์กรอย่างแน่ชัด

The Thai Institute of Directors, in partnership with Deloitte, organized the IOD Director Briefing (Tea Talk) 1/2018 on 19 March 2018, at the Renaissance Bangkok Ratchaprasong Hotel. The special guest speaker was Mr. Thio Tse Gan, Executive Director, Southeast Asia Cyber Risk Services Leader, Deloitte who gave a presentation on dealing with cyber risk in the boardroom. Highlights of the presentation are given below:

Mr. Gan began by pointing out that cyber risk management is, in fact, everybody's responsibility, and not just an issue for the information telecommunications (IT) department the CEO, or the directors that has been assigned to oversee the IT department to deal with.

He noted that there has been an alarming escalation in cybercrime and cited the following statistics:

- 200,000 new malwares emerge on average everyday
- 76% of organizations have reported being victim of a phishing attack in 2016
- 86 countries registered with DDSs attack in second quarter of 2015, with longest recorded duration being 277 hours
- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016

These rising figures emphasize the need to fully recognize the importance in recognizing the changes that are taking place.

Mr. Gan noted that one change, as indicated by the digital evolution index 2017 from HBR, is that many countries, including Thailand, are moving rapidly into digitalization. Smart-phones have become an important part of people's lives. This device has become significantly more powerful, and it is heavily influencing the way people operate and the way information is shared.

Another change he mentioned is how society is embracing social media. People share everything they do from any location. Basically, sharing has become part of people's lives. His concern with this is that when people share, they may also be sharing sensitive information of the company and noted that people must bear in mind that pictures of things around the office could unintentionally reveal some information.

Mr. Gan illustrated several cyber risks associated with technology in the presentation. First, risks that comes with the Cloud. It is undeniable that the Cloud is very beneficial, but because it can be accessed anywhere, there is strong potential risk of being hacked. Additionally, Cloud users do not know if their data would be replicated and forwarded by the Cloud service provider as they may claim that they also own the data. Second, there are the risks associated with the Internet of Things – a useful technology that can be used for a

number of things, such as drones and RFID. There could be disaster, however, if the Internet of Things devices are not operated properly; for example, Mirai, a malware, compromised millions of baby monitors two years ago globally and almost forced one company to close down. Third, there are risks related to robotics. Although robotics are very helpful and are very cost efficient, chances of mistakes also exist.

Mr. Gan posed a key questions for the audience: When do you seriously take action to deal with cyber risk? Is only after there is an incident that directly affects you or do you monitor it regularly, which is necessary, because we are more digitalized than we actually realize?. He further highlighted that is necessary to consider the security aspects related to the risk. If they are not handled well, the reputations of ongoing businesses can be ruined.

Hacking is one of the greatest threats, Mr. Gan said. When talking about an implication of a hack, people often think about regulations and communications, especially with customers and other external environment, but the factors "beneath the surface", such as the cost relating to the effects on the core of the organization, includes intellectual property: trade names, the value of customers, and the confidence that customers have. It could take five to six years to regain customers' confidence after harm it done to its reputation, he said, adding that the cost for an organization to recover its reputation is always much greater than what is initially expected.

Mr. Gan said that cyber hygiene starts with the individual and then he provided 10 things to use as guideline for good cyber hygienic.

1. Install security software from a reputable provider and update it regularly.
2. Stay with reputable websites and mobile applications.
3. Be careful of your selection of friends and information you share on social media.
4. Beware of pop-ups. Be cautious of anything on the Internet this is a "sure win".
5. Make sure that you have various and strong passwords for each account.
6. Only open attachments when you are expecting them and know what they contain, even if you know the sender.
7. Keep sensitive information safe. Confidential document or USBs should always be kept in safe places and avoid writing passwords on paper.
8. Be careful of strangers in your office.
9. Be careful when using public wireless networks. Being on a secure connection does not guarantee safety from other malicious users on the same network.
10. Consciously keep up with current security trends and threats.

In addition, he suggested four approaches to minimize the risk of being compromised with adoption of new technology. The approaches are to be strategic, secure, vigilant, and resilient. To be strategic, one needs to look at the strategy in place relating to cyber. The cyber risk program must be in line with the strategic objectives and risk appetite of the organization. To be secure the means to have risk prioritized controls to defend critical asserts against known and emerging threats. To be vigilant is to have threat intelligence and situational awareness to anticipate and identify harmful behavior. To be resilient is to be prepared and to have the ability to recover from cyber incidents and minimize their impacts.

Mr. Gan stated that one must remember that a cyber-attack is never a single event disaster; accordingly, all company staff members, starting from the top management to the staff in the organization, needs to be prepared to tackle such an incident. One of the most difficult aspects is the people. The people culture must be addressed, which entails coaching and training.

Mr. Gan ended the presentation with a list of 10 steps for organizations to take to prepare for cyber risks:

1. Set the tone — engage leadership in managing cyber risks.
2. Assess risk broadly — include enterprise, ICS and connected product.
3. Socialize the risk profile — share the results with leadership and the board.
4. Build in security — harmonize investments with a cyber risk program.
5. Remember data are assets — connect business value with data and strategies to protect them.
6. Assess third party risk — assess the risks of the information telecommunications risk provider, the network provider and others
7. Be vigilant with monitoring — determine whether and how quickly a breach in key areas of the company would be detected
8. Always be prepared — focus on incident and breach preparedness, using war games simulation.
9. Clarify organizational responsibilities — is it just the information technology departments or all departments.
10. Encourage increased awareness — get employees on board and ensure they know their role in protecting the organization.

Event Supported by

Deloitte.