ถึงเวลาของ จบ IT Security Awareness

วิชญ์คุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

➲ Cyber Security Architecture

สำหรับ IT Security นั้นหลายคนอาจมองว่าเป็นการดำเนินงานภายใต้เขตของงานด้านเทคโนโลยีสารสนเทศ และการสื่อสาร แต่ปัจจุบันมีการขยายขอบเขตครอบคลุมองค์ประกอบอื่นๆ ที่เกี่ยวข้อง เนื่องจากปัจจัยภายนอกต่างๆ ล้วนแล้วแต่ส่งผลกระทบต่อการจัดการ Security แทบทั้งสิ้น จึงมีการใช้คำว่า Cyber Security แทนเมื่อจะกล่าวถึงการดำเนินงานเรื่อง Security ในบริบทของ IT และเมื่อพูดถึงการบริหารจัดการองค์การ EA จะเข้ามามีบทบาทสำคัญในการอธิบายโครงสร้าง สำหรับ Cyber Security ก็เช่นเดียวกัน เนื่องจากต้นตอของปัญหา Security นั้น เกิดจากการขาดแนวคิด และแนวทางปฏิบัติที่เหมาะสมตั้งแต่เริ่มต้น ดังนั้น องค์การควรต้องมีการออกแบบระบบการรักษาความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบโครงสร้างองค์การ ผลผลิต และบริการต่างๆ รวมถึงโครงสร้างด้านทรัพยากรเทคโนโลยีสารสนเทศ และการสื่อสาร ทั้งในส่วนของ Hardware และ Software

➲ The risk of service providers

การ “Outsource” ทางด้าน IT เพื่อให้ผู้เชี่ยวชาญเฉพาะทางมาดูแล และให้คำปรึกษาแก่องค์การนั้น ได้รับความนิยม และมีการดำเนินการอย่างแพร่หลาย ซึ่งการ Outsource ด้าน Cyber Security องค์การมักจะว่าจ้าง MSSP (Managed Security Service Provider) เข้ามาดำเนินการเฝ้าระวังการโจมตี ในรูปแบบของ SOC (Security Operation Center) เพราะถ้าหากองค์การดำเนินการเองอาจไม่คุ้มค่าในการลงทุน รวมถึงขาดแคลนบุคลากรผู้เชี่ยวชาญ เนื่องจากองค์การส่วนใหญ่ไม่ได้มีพันธกิจหลักในงานด้าน IT ประกอบกับเป็นการบริหารความเสี่ยงในลักษณะโอนถ่ายความเสี่ยงไปสู่ Outsource แต่ปัญหาที่อาจเกิดขึ้นก็คือ การที่ Outsource ไม่ปฏิบัติงานตามที่ตกลงกันไว้ในสัญญา หรือตาม SLA (Services Level Agreement) ทำให้อาจมีช่องโหว่จากการดำเนินงานของ Outsource ดังนั้นองค์การควร

พิจารณาเลือกใช้บริการ Outsource อย่างรัดกุม และมีการบริหารความเสี่ยงร่วมกันอย่างเหมาะสม

➲ Big data will lead to big problems

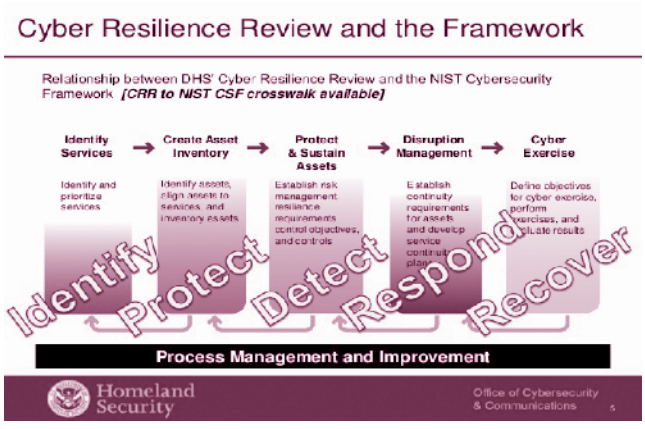
การนำเทคโนโลยี "Big Data" เข้ามาใช้ในการวิเคราะห์ข้อมูลจำนวนมหาศาลที่ปริมาณขึ้นอย่างต่อเนื่องขององค์การ (โดยเฉพาะอย่างยิ่งถ้าองค์การใช้ Social Network เป็นเครื่องมือในการสร้างความสัมพันธ์ทางด้านการตลาด ลูกค้า คู่ค้า หรือการประสานการทำงานภายใน) ทั้งข้อมูลด้านการตลาด เทคโนโลยี กระบวนการปฏิบัติงาน การให้บริการ รวมถึงข้อมูลที่เกี่ยวข้องกับการเฝ้าระวัง และรักษาความมั่นคงปลอดภัยมีความจำเป็นต่อองค์การเป็นอย่างมาก ซึ่งปัจจุบันระบบบริหารจัดการข้อมูลในรูปแบบเดิมๆ ไม่สามารถรองรับได้ และมีบางส่วนเป็นข้อมูลที่องค์การไม่สามารถบริหารจัดการ และควบคุมได้ ดังนั้นองค์การจึงควรมีเครื่องมือ กระบวนการบริหารจัดการและบุคลากรผู้เชี่ยวชาญทำหน้าที่บริหารจัดการกับข้อมูลขนาดใหญ่ขององค์การอย่างเป็นระบบ และรัดกุม เพราะข้อมูลบางอย่างมีนัยสำคัญ จนอาจกลายเป็นเป้าหมายของผู้ไม่ประสงค์ดีอย่างหลีกเลี่ยงไม่ได้

➲ Generation C: Digital Lifestyle in Digital Economy

ในยุค Generation C นั้น ผู้คนจะมีความผูกพันกับการเชื่อมต่อ internet แบบ Always Online ตลอดเวลา สังเกตได้จากพฤติกรรมการใช้ Smart Phone, Smart Mobile Device และ Social Network กลุ่มผู้ไม่ประสงค์ดีจึงหันมาโจมตีไปที่ช่องโหว่ของระบบปฏิบัติการ Mobile อาทิ Android, iOS มากขึ้น และมุ่งเป้าหมายการโจมตีไปยัง Social Network ยอดนิยมทั้ง Facebook, Twitter, LINE, instagram ฯลฯ โดยผู้ไม่ประสงค์ดีจะเจาะเข้าสู่ข้อมูลส่วนบุคคล และโจมตีต่อเนื่องเพื่อเชื่อมโยงถึงเครือข่ายภายในขององค์การในขั้นตอนต่อไป โดยอาศัยข้อมูลส่วนบุคคลเป็นวัตถุดิบ ดังนั้น องค์การควรทำความเข้าใจกับพฤติกรรมของบุคลากรในยุค Generation C และต้องสร้างความเข้าใจ และความตระหนักให้เห็นถึงความเสี่ยง ผลกระทบที่อาจเกิดขึ้น ผ่านการจัดฝึกอบรมในเรื่องที่เกี่ยวข้องกับ Information Security Awareness และควรมีการเตรียมความพร้อมรับสถานการณ์การโจมตี (Cyber Drill) เพื่อให้บุคลากร และผู้บริหารในองค์การมีความเข้าใจ และตระหนักถึงภัยจากการโจมตีทางอิเล็กทรอนิกส์ที่อยู่ใกล้ตัว เพราะเมื่อการโจมตีเกิดขึ้นจะได้ไม่ตกเป็นเหยื่อโดยรู้เท่าไม่ถึงการณ์

➲ Cyber Security Centric and Cyber Resilience in Action

การบริหารความมั่นคงปลอดภัยขององค์การในอนาคตต้องมีรูปแบบเป็น "Cyber Resilience" ซึ่งหมายถึงระบบต้องมีความสามารถในการรองรับการโจมตี และจะต้องสามารถทำงานหรือให้บริการได้อย่างต่อเนื่อง ไม่ทำให้เกิดความเสียหายต่อภารกิจ และภาพลักษณ์ขององค์การ ภาพลักษณ์ของผู้บริหาร ดังนั้นแนวคิดของ Information Security Management ในรูปแบบเดิมๆ จึงไม่ครอบคลุมเพียงพอ จำเป็นที่ต้องนำแนวคิด Cyber Security Resilience Framework มาประยุกต์ใช้

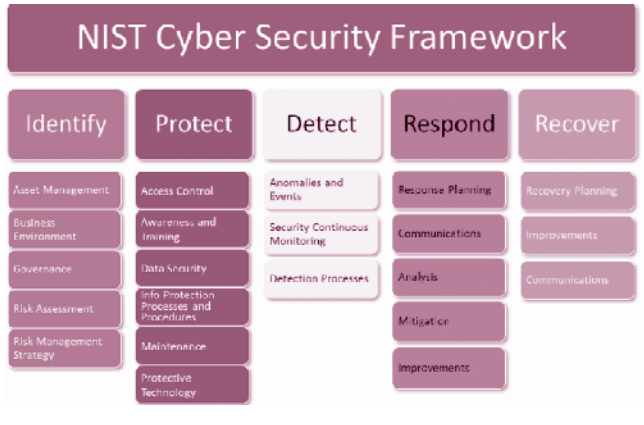


➲ Increasing in Cyber Security Capabilities and Competency

ปัญหาการขาดแคลนผู้เชี่ยวชาญด้าน Cyber Security ขององค์การนั้น เกิดขึ้นทั่วโลก ทั้งในสหรัฐอเมริกา ยุโรป และประเทศในแถบเอเชีย ซึ่งประเทศชั้นนำในเอเชียตะวันออกเฉียงใต้อย่างสิงคโปร์ก็ขาดแคลนบุคลากรในด้านนี้เช่นกัน การขาดองค์ความรู้ และประสบการณ์ ทำให้หลายองค์การไม่สามารถที่จะป้องกันตัวเองจากการโจมตีทางอิเล็กทรอนิกส์ได้ ดังปรากฏให้เห็นเป็นข่าวอย่างต่อเนื่อง ซึ่งแนวทางการแก้ปัญหาขององค์การส่วนใหญ่นั่นคือ การ Outsource โดยเฉพาะการเฝ้าระวังตลอด 24 ชั่วโมง (24×7 Real-time Monitor) และการตอบสนองต่อเหตุการณ์อันไม่พึงประสงค์ (Incident Respond) โดยทีมผู้เชี่ยวชาญ การปิดช่องโหว่ กู้คืนข้อมูล และการวางมาตรการเพื่อป้องกันไม่ให้เหตุการณ์ดังกล่าว เกิดขึ้นอีกในอนาคต โดยที่บุคลากรขององค์การจะทำหน้าที่ควบคุม ประสานงาน และตรวจสอบการทำงานของ Outsource อย่างเป็นระบบ

➲ Integrated Risk-Based Approach Standards & Best Practices

การสร้างความยั่งยืนให้กับ Cyber Security ขององค์การชั้นนำจะอ้างอิงมาตรฐาน และแนวทางในการปฏิบัติ (Standard and Best Practice) อาทิ NIST Cyber Security Framework, แนวทางปฏิบัติของ ISO27001:2013 ที่เน้นการบริหารความเสี่ยงเป็นพื้นฐานสำคัญ มาประยุกต์ใช้ในการบริหารจัดการด้านความมั่นคงปลอดภัยขององค์การอย่างเหมาะสม และสอดคล้องกับวัฒนธรรมในการทำงาน

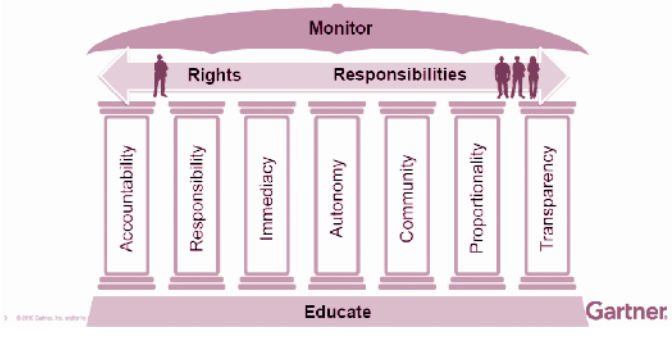


จากแนวทางของ Cyber Security ข้างต้นเป็นสิ่งที่องค์การควรต้องคำนึงถึง ซึ่งสำหรับการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารขององค์การนั้น ถึงแม้ว่าจะมีแนวทางที่ถูกพัฒนาอย่างต่อเนื่องซึ่งสอดคล้องกับสถานการณ์ให้นำไปประยุกต์ใช้ รวมถึงมีเทคโนโลยี และเครื่องมือจำเป็น ตลอดจนผู้ให้บริการที่มีทีมงานผู้เชี่ยวชาญทั้งใน และต่างประเทศเป็นทางเลือกในการบริหารจัดการความเสี่ยงขององค์การ เพื่อรับมือกับภัยจากการโจมตีทางอิเล็กทรอนิกส์ที่ไม่สามารถคาดการณ์หรือแม้กระทั่งการประเมินความเสียหายที่จะเกิดขึ้นได้ ประกอบกับมีการดำเนินงานร่วมกับ Outsource หรือผู้เชี่ยวชาญ อาทิ การติดตามเฝ้าระวังสถานการณ์ การวางแผนเพื่อให้ระบบ และสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องถึงแม้จะถูกโจมตี หรือเกิดสถานการณ์ที่ไม่พึงประสงค์ การวางแผนเมื่อเผชิญสถานการณ์ในลักษณะของ Crisis Management

อย่างไรก็ตามองค์การยังคงต้องมีการเตรียมความพร้อมในลักษณะของการป้องกันอยู่อย่างต่อเนื่อง และสม่ำเสมอ เช่น การสื่อสารสร้างความเข้าใจให้กับบุคลากร การสร้างความตระหนักถึงภัยที่อาจเกิดขึ้น การร่วมกันจัดทำ และทบทวน Risk Management ให้ทันต่อการเปลี่ยนแปลงขององค์การ และปัจจัยภายนอก บนพื้นฐานความเข้าใจของบุคลากรที่เกี่ยวข้องเพื่อให้เกิด “IT Security Awareness” ขึ้นในแนวคิดของบุคลากร เพราะแม้ว่าจะมีการวางนโยบายที่รัดกุมเพียงใด หรือมีระบบรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพสูงมีทีมงานผู้เชี่ยวชาญมากแค่ไหน จุดอ่อนที่เป็นความเสี่ยงสำคัญของทุกองค์การก็คือ ความไม่ตระหนักถึงภัย การไม่ให้ความสำคัญ การปล่อยปละละเลย ความประมาทของบุคลากร ฯลฯ เหล่านี้เป็นดัชนีชี้วัดในเรื่องความปลอดภัยที่สำคัญยิ่งกว่าการมีระบบ Security ที่ทันสมัย มีราคาแพง

ดังนั้น องค์การควรให้ความสำคัญที่บุคลากรเป็นหลัก ควรมีการกำหนดมาตรการที่เหมาะสม เพราะองค์การอาจไม่ต้องลงทุนในเรื่อง Security มากนักโดยทำเฉพาะในส่วนที่ไม่สามารถทำเองได้ แต่อาจจะได้ระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพในระดับสูงที่เหมาะสมกับวัฒนธรรมขององค์การก็เป็นได้ ทั้งนี้สอดคล้องกับหลักการของ Gartner ในเรื่อง People-Centric Security

People-Centric Security



ปัญหาเรื่องความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ส่งผลกระทบโดยตรงต่อความเชื่อมั่น ความน่าเชื่อถือขององค์การ เป้าหมายของการโจมตี คือ ข้อมูลสารสนเทศ ทรัพยากรด้านเทคโนโลยีสารสนเทศ กระบวนการทางธุรกิจที่สำคัญขององค์การ รวมถึงภาพลักษณ์ทั้งขององค์การ และผู้บริหารแล้วแต่ว่าเป้าหมายคืออะไร ซึ่งการโจมตีที่เกิดจากภายนอกองค์การอาจสามารถเฝ้าระวังและปกป้องสิ่งสำคัญเพื่อลดความเสียหายได้ แต่การโจมตีจากภายในองค์การที่น่าจะป้องกันได้กลับกลายเป็นความเสี่ยงสำคัญ และอาจส่งผลกระทบที่รุนแรง (ตัวอย่างเช่น เพียงแค่ Thumb Drive ส่วนตัว 1 อัน เสียบเข้าเครื่องลูกข่ายที่เชื่อมเข้ากับระบบเครือข่ายองค์การชั้นในที่ไม่ได้มีการป้องกัน และไม่ได้มีการ Scan เพื่อป้องกันโปรแกรมไม่พึงประสงค์ หากเกิดความเสียหายขึ้นอาจไม่สามารถประเมินได้) ดังนั้น องค์การควรเริ่มต้น “IT Security Awareness” ที่เหมาะสม ทำความเข้าใจ และดำเนินการอย่างตรงจุดก่อนจะสายเกินไป หากเปรียบกับภาพยนตร์เรื่อง Star Wars แล้ว ในกรณีของ Cyber War อาจจะต้องกล่าวว่า **“ขอ Awareness จงสถิตอยู่กับองค์การของท่าน...”** แทน TPA news

ข้อมูลอ้างอิง

- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
- US-CERT, Department of Homeland Security
- CERT, Software Engineering Institute, Carnegie Mellon University
- ACIS Professional Center
- “Responsive Security” by Dr. Meng-Chow Kang
- “Top security trends for 2016-2017” by Gartner