ถึงเวลาของ IT Security Awareness

วิชญ์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ในช่วงต้นเดือนมิถุนายนที่ผ่านมา ผมได้รับเชิญจากหน่วยงานภาครัฐ และรัฐวิสาหกิจให้ทำหน้าที่วิทยากรฝึกอบรมในเรื่องของการปฏิบัติตามมาตรฐาน ISO 27001:2013 ซึ่งหลายท่านอาจคุ้นเคยในชื่อของ ISMS (Information Security Management System) โดยมาตรฐานดังกล่าว เป็นกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสารขององค์การ การกำหนดแนวทาง และแนวปฏิบัติเพื่อการควบคุมในมิติต่างๆ โดยมีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยในด้านดังกล่าว ดังนั้นการฝึกอบรมที่นำเอา ISO มาตรฐานสากลเป็นที่ตั้งนั้น เพื่อให้เกิดประโยชน์ต่อผู้เข้าอบรมที่ส่วนใหญ่เป็นเจ้าหน้าที่ทางด้านเทคนิค และผู้บริหารระดับกลางขององค์การที่เข้าใจงานรวมถึงปัญหาเป็นอย่างดี การอบรมจึงเน้นเชิงปฏิบัติเพื่อให้สามารถสะท้อนเหตุการณ์ กรณีที่เกี่ยวข้องกับปัญหา หรือความเสี่ยงด้านความมั่นคงปลอดภัยขององค์การที่เกิดขึ้นจริง และที่อาจเกิดขึ้นในอนาคต รวมถึงภัยคุกคามในแง่มุมต่างๆ ทั้งที่คาดถึง และคาดไม่ถึง ซึ่งในฐานะของวิทยากรทำให้ได้มีโอกาสแลกเปลี่ยนประสบการณ์ ร่วมระดมสมองและเสนอแนะแนวทางในการป้องกัน การบริหารจัดการความเสี่ยง การกำหนดแผนเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บนสถานการณ์จริงขององค์การ

โดยจากการฝึกอบรมทำให้มองเห็นแนวโน้มของการให้ความสำคัญเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของทั้งภาครัฐ และเอกชน ที่เพิ่มมากขึ้นทั้งในแง่ของนโยบาย และการปฏิบัติอย่างจริงจัง ทั้งนี้สืบเนื่องจากการที่หน่วยงานต่างๆ โดนโจมตีทางอิเล็กทรอนิกส์จากผู้ไม่ประสงค์ดีในรูปแบบต่างๆ ในปริมาณ และความถี่ที่มากขึ้น รวมถึงผลกระทบจากการโจมตีแต่ละครั้งยิ่งทวีความรุนแรงมากขึ้นเป็นเงาตามตัว ประกอบกับการพัฒนาเทคโนโลยีใหม่ๆ ทำให้การเข้าถึงข้อมูลสารสนเทศที่เป็นหัวใจสำคัญขององค์การทำได้ง่าย และหลากหลายวิธีการทั้งที่ได้รับอนุญาต และที่ไม่พึงประสงค์ การมาถึงของ IOT (Internet of Things), Big Data, Social age, Mobile technology ทำให้หลายองค์การต้องปรับตัวเพื่อรับมือกับสถานการณ์ดังกล่าว

Gartner ได้ทำนายไว้ใน “Top Security Trends 2016-2017” ว่า Mega Trends ทั้ง 4 อันได้แก่ Social, Mobile Cloud และ Big Data จะมีอิทธิพลทำให้ปัญหาด้าน Cyber Security ทวีความรุนแรงมากยิ่งขึ้น (Cyber Security ถูกนิยามขึ้นเพื่อให้ครอบคลุมขอบเขตที่มากกว่า “Information Security” ซึ่งเริ่มจะมีคนใช้คำนี้เพื่อกล่าวถึงเรื่อง Security มากขึ้นในปัจจุบัน) ทำให้วิธีการจัดการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศแบบเดิมๆ อาจไม่สามารถนำมาใช้ได้อย่างมีประสิทธิภาพ จำเป็นต้องปรับกลยุทธ์ในการบริหารจัดการให้เหมาะสม และทันต่อสถานการณ์ ซึ่งแนวโน้มของ Cyber Security ที่น่าสนใจจาก “Responsive Security” ของ Dr. Meng-Chow Kang และบทความจาก ACIS Professional Center มีดังนี้

➲ Hacking Industry

จากความสำเร็จของ Ransomware หรือโปรแกรมเรียกค่าไถ่ สามารถสร้างรายได้ให้ Hacker ได้อย่างมากมาย ทำให้อาชญากรเหล่านี้สร้าง Malware ในรูปแบบของ Ransomware อย่างจริงจัง กลายเป็นอาชญอุตสาหกรรมไปโดยปริยาย กล่าวคือมีการทำงานร่วมกันในรูปแบบของ Organized Crime รวมถึงกรณีที่หน่วยงานของภาครัฐในบางประเทศได้จัดตั้งทีม Hacker เพื่อให้ทำการเจาะระบบในงานจารกรรมต่างๆ และมีความร่วมมือระหว่างประเทศที่มีเป้าประสงค์ร่วมทางการเมือง และเศรษฐกิจ ทำให้รัฐบาลในหลายประเทศต้องออกกฎหมายรองรับ และจัดให้มีองค์การที่มีหน้าที่บริหารจัดการ และกำหนดนโยบายด้าน Cyber Security อย่างจริงจัง

➲ Undefined Unknown Threat

ความจริงที่ว่าเราไม่สามารถสร้างให้มีการรักษาความมั่นคงปลอดภัยที่ใช้งานในทางปฏิบัติได้เต็ม 100% ทั้งนี้เนื่องมาจากว่าปัจจุบันองค์การกำลังต่อสู้กับภัยที่มองไม่เห็น มีข้อมูลจำนวนมากที่อยู่ในอีกด้านหนึ่งของโลก internet ที่ซึ่งผู้ไม่ประสงค์ดีจนกระทั่งถึงอาชญากรทางอิเล็กทรอนิกส์ใช้เป็นเครื่องมือสนับสนุนการกระทำที่ไม่พึงประสงค์ มีการปลอมแปลง ปกปิดร่องรอยการกระทำผิด การยึดหรือฝังโปรแกรมในเครื่องแม่ข่าย/เครื่องลูกข่ายของผู้อื่นแล้วนำไปใช้กระทำความผิด ทำให้การสืบค้นเพื่อหาผู้กระทำผิดทำได้อย่างยากลำบาก ตลอดจนเรายังไม่ทราบว่าผู้ที่ไม่หวังดีต่อองค์การของเราที่แท้จริงแล้วเป็นใคร เกิดปัญหาที่เรียกว่า “Attack Attribution” คือ การหาตัวจริงของผู้กระทำผิดไม่พบ พบแต่เพียง IP Address ของเป้าหมายที่ถูกยึดเครื่องมาใช้โจมตี ดังนั้นการบริหารจัดการกับ Undefined Unknown Threat จำเป็นต้องเปลี่ยนแนวคิดจากการวางแผนเพื่อป้องกันเป็นการเตรียมพร้อมรับมือกับการถูกโจมตีอยู่ตลอดเวลาด้วยการเฝ้าระวังแบบ Real Time และต้องมีความยืดหยุ่นเพียงพอต่อการปรับเปลี่ยนแนวทางการปฏิบัติเมื่อถูกโจมตี

➲ Internet of Trust

จากการพัฒนา Internet of thing ที่ก้าวหน้าอย่างรวดเร็ว ทำให้การเข้าถึง และแบ่งปันข้อมูลสารสนเทศทำได้ง่ายหลายหลายรูปแบบ หลากหลายวิธีการ ทั้งที่ตั้งใจ และรู้เท่าไม่ถึงการณ์ ก่อให้เกิดความสัมพันธ์ที่ซับซ้อนระหว่าง “Thing”, “Threat” และ “Information” ทั้งในแง่ของผู้ใช้งาน และผู้ให้บริการรวมถึงในระดับขององค์การจำเป็นต้องมีการรักษาความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เกิดความน่าเชื่อถือโดยเฉพาะในมิติขององค์การ เนื่องจากความเสี่ยงที่สำคัญอันดับต้นๆ เมื่อเกิดการรั่วไหลของข้อมูลสารสนเทศ นั่นคือความเสี่ยงจากการเสื่อมเสียชื่อเสียง ภาพลักษณ์ขององค์การที่ยากจะหลีกเลี่ยงผลกระทบที่รุนแรง จำเป็นต้องให้ความสำคัญมีการควบคุมการใช้งาน การให้บริการ และบริหารจัดการความน่าเชื่อถือที่เหมาะสม

อ่านต่อฉบับหน้า