Information Security Awareness เรื่องสำคัญที่ไม่ควรมองข้าม

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ต่อจากฉบับที่แล้ว

จบ

"Security Awareness" นั้น จะเป็นการจัดฝึกอบรมให้กับเจ้าหน้าที่ทุกระดับในองค์การให้มีความเข้าใจและตื่นตัวในเรื่องของ **"Information Security"** ให้เห็นว่าเป็นเรื่องใกล้ตัวที่ทุกคนต้องช่วยกัน โปรแกรมการฝึกอบรมนั้นอาจแตกต่างกันไปในแต่ละองค์การขึ้นกับลักษณะในการดำเนินธุรกิจขององค์การนั้นๆ ซึ่งต้องมีการปรับให้เข้ากับ "Corporate Culture" ในแต่ละองค์การ ต้องแสดงให้ทุกคนเห็นถึงความสำคัญของ Information Security ว่าคืออะไร มีรายละเอียดอย่างไรและทำไมต้องจริงจังกับเรื่องเหล่านี้ (What, How and Why) ดังนั้นรายละเอียดการฝึกอบรมจะแตกต่างกันไปขึ้นอยู่กับระดับของบุคลากรในองค์การ ซึ่งสามารถแบ่งเป็นทั้งหมด 5 กลุ่มที่มีเนื้อหาการฝึกอบรมที่แตกต่างกันไปได้ดังนี้

กลุ่มที่ 1: ผู้บริหารระดับสูง (Top Management)

โปรแกรมการฝึกอบรมควรพูดถึงภาพรวมของความสำคัญด้าน INFOSEC ผลกระทบที่จะเกิดขึ้นกับองค์การหากถูก Hacker บุกรุกระบบสารสนเทศ หรือมีการติดไวรัสในระบบ กล่าวถึงภาระหน้าที่ที่ต้องรับผิดชอบ ทั้งก่อนเกิดปัญหาและหลังจากเกิดปัญหาด้าน INFOSEC ผลกระทบกับธุรกิจ ภาพลักษณ์ขององค์การ ตลอดจนความเชื่อมั่นของผู้ถือหุ้น ซึ่งการฝึกอบรมไม่ควรจะใช้เวลามากเกินไปและไม่ควรจะลงลึกในส่วนของเนื้อหาทางด้านเทคนิคมากนัก ต้องมีการยกหรืออ้างถึง Case Study ตัวอย่างที่ผู้บริหารระดับสูงหลายท่านต้องประสบปัญหาหลังจากมีเหตุเรื่องการ Hack ระบบเกิดขึ้นกับองค์การ การฝึกอบรมผู้บริหารระดับสูงถือเป็นเรื่องที่สำคัญที่สุด เพราะผู้บริหารที่ดีต้องมีทั้ง "Due Care" และ "Due Professional" ซึ่งจำเป็นต้อง "รับผิดชอบ" และ "รู้จริง" เพื่อนำองค์การให้มีประสิทธิภาพและประสิทธิผลต่อไป

กลุ่มที่ 2: ผู้บริหารระดับกลาง (Middle Management)

ในองค์การขนาดใหญ่ โปรแกรมการฝึกอบรมด้าน INFOSEC ให้กับผู้บริหารระดับกลางควรจะมีความแตกต่างจากผู้บริหารระดับสูง ในส่วนเนื้อหาการฝึกอบรมจะต้องลงในรายละเอียดมากขึ้น ในส่วนของ Security Policies, Procedures, Standards และ Guidelines ควรจะให้สอดคล้องกับงานในแผนก หรือฝ่ายที่รับผิดชอบดูแลอยู่ รวมทั้งควรทราบถึงวิธีที่จะทำให้ระบบสารสนเทศที่ดูแลอยู่มีความปลอดภัยในระดับมาตรฐาน ตลอดจนมีการอบรมให้รู้วิธีควบคุมดูแลเจ้าหน้าที่ในบังคับบัญชาให้ปฏิบัติตามกฎเกณฑ์

ทางด้าน INFOSEC ที่ได้กำหนดไว้ใน Security Policies เป็นต้น

กลุ่มที่ 3: ผู้ดูแลระบบ (System Administrator/Network Administrator/Database Administrator)

โปรแกรมการฝึกอบรมจะมีความแตกต่างจากผู้บริหารทั้ง 2 ระดับ โดยจะมีรายละเอียดลงลึกในงานที่ต้องทำประจำวัน (Routine Tasks) และเจาะลึกในด้าน Technical กับระบบสารสนเทศที่ดูแลอยู่ เครื่องแม่ข่าย ระบบเครือข่าย และแสดงให้เห็นว่า Hacker สามารถเข้าสู่ระบบผ่านช่องโหว่ หรือจุดที่ไม่ปลอดภัยได้ง่ายดายเพียงใด เรียกว่าต้องเห็นภาพการ Hack จริงๆ ก่อนถึงจะเข้าใจและมีความตระหนักว่าเรื่องความปลอดภัยเป็นเรื่องที่ต้องดูแลกันแทบทุกวันเลยทีเดียว

กลุ่มที่ 4: ผู้ดูแลระบบความปลอดภัยคอมพิวเตอร์โดยตรง (Security Administrator)

องค์การที่มีการจัดการด้าน IT ที่ดีควรจะมีการแยกแผนก หรือฝ่าย INFOSEC ออกจากแผนก หรือฝ่าย IT เพราะหน้าที่การดูแลด้าน INFOSEC โดยเฉพาะจำเป็นที่จะต้องมีความรู้ในขั้นสูงและมีเวลามากพอที่จะดูแลเรื่องของ INFOSEC อย่างเพียงพอ เช่น มีเวลาดูเรื่องช่องโหว่ใหม่ๆ ของระบบ Windows หรือ Unix อยู่เป็นประจำ รวมทั้งทราบถึงวิธีการแก้ปัญหาที่ถูกต้อง เพื่อจะได้แนะนำเจ้าหน้าที่ในกลุ่มที่ 3 ให้ปฏิบัติงานต่อไปได้ตรงจุด โปรแกรมการฝึกอบรมต้องอยู่ในระดับ “Advanced Technical/Advanced Knowledge” รวมทั้งการทราบถึงและนำเอาเทคโนโลยีใหม่ๆ ของ Hacker รวมถึงเทคโนโลยีที่ใช้ในการป้องกันรูปแบบใหม่ๆ มาประยุกต์ใช้ด้วยและพูดถึงเรื่อง “Incident Response” หรือเวลาที่มีปัญหาด้าน INFOSEC จะต้องทำตัวเป็นหน่วย 191 หรือหน่วย FBI ที่จะต้องรับผิดชอบในการตรวจจับ Hacker และกู้ระบบสารสนเทศที่ถูกโจมตี หรือได้รับผลกระทบจากสิ่งแวดล้อมและภัยธรรมชาติให้กลับคืนสภาพขึ้นมาให้บริการได้ตามปกติโดยเร็วที่สุด (Disaster Recover Planning)

กลุ่มที่ 5: ผู้ใช้งานคอมพิวเตอร์ทั่วไป (Users)

กลุ่มนี้เป็นกลุ่มของเจ้าหน้าที่ผู้มีความรู้ด้าน INFOSEC น้อยมาก เช่น เจ้าหน้าที่คีย์ข้อมูล เจ้าหน้าที่ฝ่ายขายที่ต้องใช้คอมพิวเตอร์ในการทำ Quotation ให้ลูกค้า เป็นต้น ควรจะต้องเรียนรู้วิธีการใช้งาน Internet ที่ถูกต้อง วิธีการป้องกันไวรัสและการแก้ไขปัญหาเบื้องต้น รู้วิธีการป้องกันตัวเองด้วยการใช้ Personal Firewall Program การใช้งานโปรแกรม e-mail ที่ถูกต้อง เป็นต้น เรื่องต่างๆ เหล่านี้จำเป็นต้องมีการจัดฝึกอบรมแก่เจ้าหน้าที่ผู้ใช้งานคอมพิวเตอร์ทั่วไปให้มีความเข้าใจในระดับหนึ่งเพื่อลดปัญหาต่างๆ ที่อาจเกิดขึ้นให้น้อยลง รวมทั้งฝึกอบรมให้เข้าใจศัพท์ต่างๆ ทางด้าน INFOSEC เช่น คำว่า Threat, Exploit หรือ Vulnerability เมื่อมีความเข้าใจแล้วการอ่าน Security Policies และการปฏิบัติตามก็จะมีประสิทธิภาพมากขึ้น

โดยสรุปแล้ว การฝึกอบรมด้าน INFOSEC นั้น ควรมีการฝึกอบรมเป็นระยะๆ อย่างต่อเนื่อง อย่างน้อย 2-3 ครั้งในหนึ่งปี เป้าหมายของการฝึกอบรมนั้นไม่ใช่เพียงแต่สร้างให้เกิดความเข้าใจด้าน INFOSEC ที่ดีขึ้นเท่านั้น แต่จะทำให้เจ้าหน้าที่ทุกคนรู้ว่า “ทำไม” ถึงต้องใส่ใจและช่วยกันป้องกันระบบสารสนเทศขององค์การ สร้างความปลอดภัยให้กับคอมพิวเตอร์ขององค์การอย่างจริงจังในสภาพแวดล้อมที่มีการแข่งขันสูงในยุคปัจจุบันซึ่ง “IT” มีส่วนสำคัญอย่างมากในการดำเนินธุรกิจและธุรกรรมต่างๆ ขององค์การ TPA news