Cybersecurity: an IT problem?

เมื่อวันที่23 พฤศจิกายนที่ผ่านมา ดิฉันได้มีโอกาสเข้าร่วมงานสัมมนา Cyber Resilience Leadership ที่จัดขึ้นโดยธนาคารแห่งประเทศไทย ในงานนี้ ธนาคารแห่งประเทศไทยได้เชิญผู้เชี่ยวชาญด้าน Cybersecurity ที่มีประสบการณ์การทำงานกับองค์กรชั้นนำจากต่างประเทศมาบรรยายให้กรรมการและผู้บริหารระดับสูงของภาคธุรกิจการเงินที่เข้าร่วมงานกว่า 200 คน ได้ตระหนักถึงความสำคัญของการเตรียมความพร้อมให้บริษัทสามารถป้องกันตนเองและรับมือกับ Cybersecurity Risks ได้อย่างมีประสิทธิภาพ เนื่องจากในปัจจุบัน ธุรกิจจำนวนมากใช้เทคโนโลยี IT ในการดำเนินธุรกิจและสร้างโอกาสในการเติบโตมากขึ้น ทุกธุรกิจจึงมีความเสี่ยงที่จะตกเป็นเหยื่อของผู้คนที่ต้องการใช้ความก้าวหน้าทาง IT เพื่อแสวงหาประโยชน์ในทางที่ไม่ถูกต้อง จึงอาจกล่าวได้ว่าไม่มีบริษัทใดที่ไม่เคยถูก "แฮ็ก" อีกต่อไป เพราะคงมีแต่บริษัทที่รู้ตัวว่าถูกแฮ็ก กับบริษัทที่ไม่รู้ตัวว่าถูกแฮ็กเท่านั้น แต่สิ่งสำคัญคือบริษัทจะทำอย่างไรให้มี Cybersecurity เพื่อป้องกันตนเองจากผู้ประสงค์ร้ายให้ดีที่สุด และเมื่อถูกผู้ประสงค์ร้ายลักลอบเจาะเข้ามาในระบบเพื่อสร้างความเสียหาย บริษัทจะทำอย่างไรให้มี Cyber Resilience ในการรับมือและกลับมาดำเนินธุรกิจตามปกติได้เร็วที่สุด

ในงานนี้นอกจากจะได้แง่คิดเกี่ยวกับบทบาทของกรรมการและผู้บริหารระดับสูงในการสร้าง Cybersecurity และ Cyber Resilience ให้เกิดขึ้นในธุรกิจของตนแล้ว ยังมีประเด็นคำถามหนึ่งที่น่าสนใจ และผู้บรรยายกระตุ้นให้ได้ลองพิจารณาตลอดงาน คือ Cybersecurity ย่อมเกี่ยวข้องกับความพร้อมด้านเทคนิคต่างๆ ของระบบ IT ในการทำงานได้อย่างไม่ติดขัดและสามารถปกป้องข้อมูลสำคัญของบริษัทได้ ดังนั้นแล้ว ปัญหาความเสี่ยงด้าน Cybersecurity ที่มีการลักลอบเจาะหรือโจมตีระบบIT รูปแบบต่างๆ ดังที่ปรากฏอยู่ในข่าวนั้น เป็นเพียงแค่ปัญหา IT หรือไม่ สองกรณีของสองบริษัทที่เพิ่งเกิดขึ้นเมื่อไม่กี่ปีมานี้อาจช่วยตอบคำถามนี้ได้

หลายท่านคงจำกรณีลักลอบเจาะระบบเพื่อขโมยข้อมูลที่กลายเป็นข่าวดังช่วงปลายปี 2556 ของบริษัท Target ได้ ในวันที่ 19 ธันวาคม 2556 ยักษ์ใหญ่ธุรกิจค้าปลีกของสหรัฐอเมริกาได้ออกมาประกาศว่าบริษัทถูกแฮ็กเกอร์ลักลอบเจาะระบบเพื่อขโมยข้อมูลบัตรเครดิตของลูกค้าที่มาจับจ่ายช่วงเทศกาลที่ห้าง Target ทั้ง 1,797 สาขา กว่า 40 ล้านใบ แม้โลกจะได้ทราบข่าวเหตุการณ์นี้ในวันที่ 19 ธันวาคม แต่ในความเป็นจริงแล้ว แฮ็กเกอร์ได้เจาะเข้ามาในระบบของ Target เพื่อปล่อยมัลแวร์ตั้งแต่วันที่ 27 พฤศจิกายน โดยโปรแกรมตรวจจับมัลแวร์มูลค่า 1.6 ล้านเหรียญสหรัฐของ Target (ซึ่งเป็นโปรแกรมเดียวกันกับที่ CIA และกระทรวงกลาโหมสหรัฐใช้) แจ้งเตือนฝ่าย IT Security ของบริษัทว่าตรวจพบมัลแวร์ในระบบถึงสองครั้ง แต่กลับถูกมองข้ามและไม่ได้มีการดำเนินการใด จนกระทั่งในวันที่ 12 ธันวาคม เมื่อกระทรวงยุติธรรมสหรัฐแจ้งบริษัทว่าตรวจพบการทำธุรกรรมทางบัตรเครดิตที่ผิดปกติที่ห้าง Target หลายสาขา บริษัทจึงเริ่มตรวจสอบระบบ ในวันที่ 15 ธันวาคม Target จึงเพิ่งยืนยันว่ามีการลักลอบเข้ามาในระบบจริงและเริ่มกำจัดมัลแวร์ออกจากระบบแม้จะผ่านไปกว่าครึ่งเดือนแล้ว นอกจากนี้ หนึ่งเดือนต่อมาในวันที่ 10 มกราคม 2557 Target จึงเพิ่งออกมาเปิดเผยว่าจากการตรวจสอบ นอกจากข้อมูลบัตรเครดิตแล้ว ยังพบว่าข้อมูลส่วนตัวอย่างชื่อ ที่อยู่ อีเมล และเบอร์โทรศัพท์ ของลูกค้ากว่า 70 ล้านรายก็ได้ถูกขโมยไปพร้อมกันด้วย

การลักลอบเจาะระบบครั้งนี้ทำให้ Gregg Steinhafel ผู้เป็น CEO ต้องออกมากล่าวขอโทษทั้งพนักงานและลูกค้าของ Target และประกาศลดราคาสินค้าในช่วงเทศกาลทุกสาขา 10% เพื่อเป็นการชดเชย อย่างไรก็ตามยอดขายของบริษัทในไตรมาสที่สี่ตกลงกว่า 50% และเมื่อเทียบกับช่วงเดียวในปีที่แล้วยังตกลง 4% นอกจากนี้ บริษัท

ยังต้องเสียค่าใช้จ่ายเพื่อชดเชยลูกค้าที่ได้รับความเสียหายรวมราว 61 ล้านเหรียญสหรัฐ อีกทั้งยังถูกฟ้องร้องและต้องจ่ายเงินชดเชยให้กับผู้เสียหายและรัฐรวมกว่า 200 ล้านเหรียญสหรัฐ ตามมาด้วยการปรับปรุงระบบการรักษาความปลอดภัยของข้อมูลลูกค้า และการลาออกของ CIO ในเดือนมีนาคม และการลาออกของ CEO ในเดือนพฤษภาคม 2557

แม้จะไม่ได้ระบุเหตุผลโดยชัดเจนว่าเหตุใด Steinhafel ผู้มีประสบการณ์ทำงานที่ Target มาถึง 35 ปีจึงตัดสินใจลาออก แต่นักวิเคราะห์จำนวนหนึ่งให้ความเห็นว่า ไม่เป็นที่น่าแปลกใจหาก CEO จะรู้สึกว่าตนเป็นผู้ที่ต้องแสดงความรับผิดชอบต่อเหตุการณ์การเจาะข้อมูลที่ส่งผลกระทบด้านการเงินและความเชื่อมั่นต่อบริษัทอย่างมาก เนื่องจากการตอบสนองของ Target ต่อเหตุที่เกิดขึ้นขาดซึ่งความเร่งด่วน และคำนึงถึงผู้ที่ได้รับความเสียหายไม่มากพอ

อีกกรณีหนึ่งที่เป็นข่าวดังเช่นกันเกิดขึ้นราวหนึ่งปีหลังกรณีของบริษัท Target และหลายท่านก็คงทราบข่าวดี คือกรณีของบริษัท Sony Pictures บริษัทในเครือของ Sony Corporation ที่ในวันที่ 24 พฤศจิกายน 2557 ถูกกลุ่มแฮ็กเกอร์ชื่อ Guardians of Peace โจมตีระบบ IT ของบริษัทให้หยุดชะงัก และลักลอบนำข้อมูลภายในที่สำคัญออกมาเผยแพร่ ไม่ว่าจะเป็นแผนกลยุทธ์ แผนการตลาด โครงสร้างเงินเดือนผู้บริหารระดับสูง ข้อมูลส่วนตัวและหมายเลข Social Security Numbers ของพนักงานทั้งอดีตและปัจจุบัน 47,426 ราย สัญญากฎหมาย อีเมลของผู้บริหารที่มีเนื้อความชวนอื้อฉาวเกี่ยวกับดารา ไปจนถึงภาพยนตร์ที่ยังไม่ได้ออกฉาย ซึ่งรวมถึงภาพยนตร์แนวตลกเสียดสีเรื่อง The Interview ที่มีเนื้อหาเกี่ยวกับการลอบสังหารผู้นำเกาหลีเหนืออีกด้วย

เหตุการณ์นี้เป็นข่าวใหญ่ในช่วงเวลาดังกล่าว ไม่ใช่เพียงเพราะ Guardians of Peace ขู่ให้ Sony ล้มเลิกการฉาย The Interview ไม่เช่นนั้นจะมีการก่อการร้าย ซึ่งอาจนำไปสู่ความขัดแย้งระหว่างสหรัฐอเมริกาและเกาหลีเหนือได้เท่านั้น แต่เป็นเพราะปริมาณของข้อมูลสำคัญที่ควรรักษาเป็นความลับของบริษัท (รวมไปถึงข้อมูลที่น่าอับอาย) ที่ถูกลักลอบนำออกมาเปิดเผยจนทำให้สังคมตั้งคำถามว่าเหตุใดบริษัทระดับนี้จึงหละหลวมได้เพียงนี้ อย่างไรก็ตาม นี่ไม่ใช่การถูกโจมตีโดยแฮ็คเกอร์ครั้งแรกที่บริษัทในเครือ Sony เคยเผชิญ ในปี 2554 Sony Computer Entertainment Europe ถูกแฮ็กเกอร์เจาะเข้ามาในระบบและขโมยข้อมูลส่วนตัวของลูกค้าบน PlayStation Network กว่า 77 ล้านรายทั่วโลกไป ส่งผลให้บริษัทต้องเสียค่าใช้จ่ายเพื่อซ่อมแซมแก้ไขระบบและจ่ายเงินชดเชยกว่า 170 ล้านเหรียญสหรัฐ รวมถึงถูก Information Commissioners' Office ของอังกฤษปรับ 250,000 ปอนด์ เนื่องจากตรวจพบว่าสาเหตุที่ระบบถูกเจาะเข้ามาได้โดยง่าย เป็นเพราะบริษัทไม่ได้อัพเดตซอฟต์แวร์ป้องกันการเจาะข้อมูล แต่เพียง 3 ปีถัดมาก็กลับเกิดเหตุการณ์ในลักษณะคล้ายกันขึ้นอีก ซ้ำร้าย จากการสืบสวนโดย FBI พบว่ากลุ่มแฮ็กเกอร์ได้เจาะเข้ามาในระบบตั้งแต่ 3 เดือนก่อนแล้ว และเป็นการเจาะระบบที่เปรียบได้กับการสะเดาะกลอนประตูเดียวแต่เข้าได้ทุกห้อง เนื่องจาก Sony Pictures มีระบบ IT Security ที่หละหลวม การเข้าถึงระบบไม่ได้เป็นแบบ Two-factor Authentication ที่ผู้ใช้ต้องใส่รหัสยืนยันตัวตนสองครั้ง ข้อมูลสำคัญทุกประเภท เอกสารสำคัญทุกอย่าง ไม่ว่าจะเป็นสัญญาหรือบันทึกทางธุรกิจ ก็ถูกเก็บไว้ในเซิร์ฟเวอร์กลางเดียวกัน ขณะเดียวกัน เซิร์ฟเวอร์อีเมลยังเก็บอีเมลเก่าที่สุดย้อนหลังไปได้ 7 ปีโดยไม่มีการเข้ารหัสข้อมูลแต่อย่างใด นอกจากนี้ คนทำงานยังมีพฤติกรรมที่หละหลวม เช่น เก็บรหัสที่ใช้ในการเข้าระบบไว้ในไฟล์ชื่อ "Computer Password" ในคอมพิวเตอร์ของตน

เหตุการณ์ที่เกิดขึ้นทำให้ระบบ IT ของ Sony Pictures หยุดชะงัก 1 สัปดาห์เต็ม และบริษัทต้องใช้เงินมากกว่า 35 ล้านเหรียญสหรัฐในการกู้คืนระบบ อีก 8 ล้านเหรียญสหรัฐเพื่อจ่ายเงินชดเชยให้แก่พนักงานที่ฟ้องร้องบริษัท และเงินอีกจำนวนมากเพื่อปรับปรุงระบบ IT ภายในให้แน่หนาขึ้น นอกจากนี้ ยังได้กลายเป็นชื่อบริษัทที่ผู้คนนึกถึงเมื่อกล่าวถึงการแฮ็กข้อมูลแม้เหตุการณ์แฮ็ก PlayStation Network ในปี 2554 จะเป็นบทเรียนให้บริษัทแล้วก็ตาม สาเหตุสำคัญอาจเป็นเพราะในปี 2550 Jason Spaltro ผู้บริหารฝ่าย Information Security ของ Sony Pictures ได้เคยให้สัมภาษณ์ไว้ว่าจะไม่ยอมลงทุน 10 ล้านเหรียญเพื่อป้องกันความเสี่ยงที่บริษัทจะเสียเงินเพียงแค่ 1 ล้านเหรียญ และถ้าหากบริษัทมีระบบรักษาความปลอดภัย IT ที่ยุ่งยากซับซ้อนสุดท้ายแล้วพนักงานก็จะจดรหัสลงโพสต์อิทแล้วแปะบนจอคอมพิวเตอร์อยู่ดี

จากกรณีที่เกิดขึ้นจะเห็นได้ว่าTarget และ Sony Pictures ได้รับความเสียหายอย่างมากทั้งด้านตัวเงินและชื่อเสียง อีกทั้ง ยังส่งผลกระทบต่อการดำเนินธุรกิจโดยตรง ในกรณีของ Target ความไม่ไว้วางใจในความปลอดภัยของระบบที่เกิดขึ้นทำให้ลูกค้าจำนวนมากไม่กล้าที่จะกลับมาจับจ่ายใช้สอย จนบริษัทต้องปรับปรุงระบบความปลอดภัยครั้งใหญ่ ขณะที่ Sony Pictures นอกจากการทำงานต้องหยุดชะงักแล้ว ข้อมูลที่มีผลต่อความได้เปรียบในการแข่งขัน และทรัพย์สินทางปัญญาของบริษัทถูกนำเปิดเผยหมด แม้ IT จะเป็นองค์ประกอบหลักที่ทำให้เกิด Cybersecurity Risks แต่ธุรกิจก็ควรถือความเสี่ยงประเภทนี้เป็น Business Risks ที่มีความสำคัญเชิงกลยุทธ์เพื่อที่จะได้บริหารจัดการได้อย่างเหมาะสม เพราะหากมอง Cybersecurity ว่าเป็นเพียงปัญหาด้าน IT แล้ว การจัดการความเสี่ยงและการแก้ปัญหาก็จะเป็นเพียงเรื่องของฝ่าย IT ไม่ใช่เรื่องของฝ่ายธุรกิจ

นอกจากนี้ ทั้งสองกรณียังแสดงให้เห็นว่าแท้จริงแล้ว Cybersecurity ไม่ใช่ปัญหาด้านเทคนิค แต่เป็นปัญหาด้านคน และผู้นำคือผู้ที่มีบทบาทสำคัญในการสร้างวัฒนธรรมที่คนทำงานตระหนักถึงความสำคัญของ Cybersecurity ต่อธุรกิจ Target มีโปรแกรมป้องกันการเจาะระบบคุณภาพสูงในระดับเดียวกับที่ CIA และกระทรวงกลาโหมสหรัฐใช้ แต่สาเหตุที่โปรแกรมราคาแพงปกป้องข้อมูลสำคัญของบริษัทจากแฮ็กเกอร์ไม่ได้ก็คือความหละหลวมของคนทำงานเอง การมองข้ามสัญญาณเตือนการขาดซึ่งความเร่งด่วนในการตรวจสอบและแก้ไขปัญหา ชี้ให้เห็นว่าคนทำงานไม่ตระหนักว่าความเสี่ยงมีผลกระทบต่อธุรกิจในระดับไหน จึงเป็นที่น่าสนใจว่าผู้นำมีบทบาทในการสร้าง

ความตระหนักให้แก่คนทำงานมากน้อยเพียงใด ขณะที่ Sony Pictures มีการรักษาความปลอดภัยของข้อมูลที่หละหลวมจนน่าตกใจ จนอาจกล่าวได้ว่าการไม่คำนึงถึงความปลอดภัยของข้อมูลเป็นวัฒนธรรมของบริษัท และผู้ที่มีส่วนสำคัญในการปล่อยให้วัฒนธรรมนี้ดำรงอยู่ก็คือตัวผู้บริหารระดับสูงเอง ดังจะเห็นได้ว่าไม่ได้มีความสนใจที่จะเปลี่ยนทัศนคติของคนทำงาน เพราะผู้นำเองก็ไม่ได้ให้ความสำคัญกับ Cybersecurity แม้จะมีบทเรียนจากบริษัทในเครือมาแล้ว

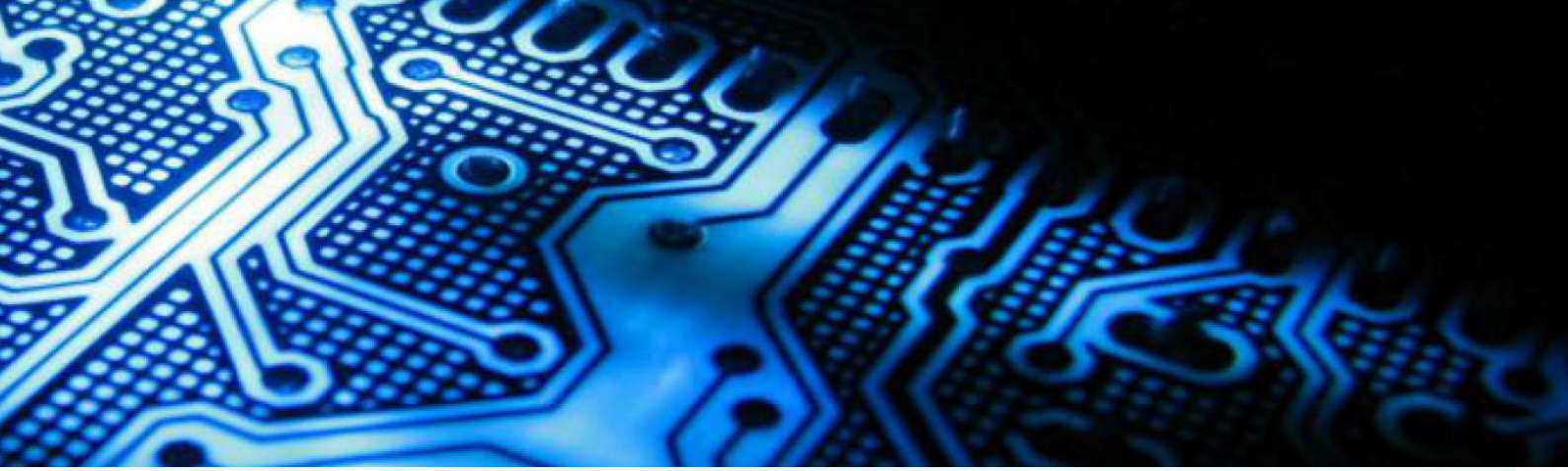
ลองมาพิจารณาอีกหนึ่งเหตุการณ์ที่เพิ่งเกิดขึ้นเร็วๆ นี้ ในวันที่ 27 มิถุนายนที่ผ่านมา เมื่อบริษัท Maersk คองโกลเมอเรตสัญชาติเดนมาร์กที่ทำธุรกิจขนส่งทางเรือของบริษัทมีขนาดใหญ่ที่สุดในโลก ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ที่พัฒนามาจากโค้ดตัวเดียวกันกับ WannaCry ชื่อ Petya ที่ล็อคเครือข่ายคอมพิวเตอร์ที่โจมตีเพื่อเรียกค่าไถ่มูลค่า 300 บิทคอยน์ มีหลายบริษัทในหลายอุตสาหกรรมในยุโรปและอเมริกาที่ตกเป็นเป้าการโจมตีของ Petya โดยพบมากที่สุดในประเทศยูเครน สำหรับ Maersk ที่ดูแลการขนส่งทางเรือทั้งหมด 15% ของโลก ผลกระทบที่เกิดขึ้นรุนแรงจนทำให้บริษัทต้องปิดระบบ IT ทั้งหมดเพื่อกันไม่ให้มัลแวร์แพร่กระจาย การขนส่งทางเรือทั้งหมดต้องหยุดนิ่งเนื่องจากไม่สามารถใช้ระบบ GPS ได้ ท่าเรือของบริษัท 76 แห่งทั่วโลกที่เชื่อมต่อกันผ่านเครือข่ายอินเทอร์เน็ตหยุดชะงัก บุคลากรในบริษัทต้องติดต่อกันทางโทรศัพท์มือถือผ่าน WhatsApp เนื่องจากไม่สามารถใช้ระบบอีเมลได้ และงานบางส่วน เช่น การรับจองบริการขนส่ง ต้องกลับไปเป็นแบบ Manual เพื่อไม่ให้การดำเนินธุรกิจหยุดนิ่ง 100%

ในวันถัดมาหลังเกิดเหตุ Maersk ได้ออกมาชี้แจงว่าแม้ปัญหาที่เกิดขึ้นจะทำให้การดำเนินงานทุกส่วนเกิดความล่าช้าอย่างมาก แต่ไม่มีข้อมูลสำคัญใดของลูกค้ารั่วไหลจากการถูกโจมตีครั้งนี้ 2 วันหลังเกิดเหตุ Maersk ก็ได้ออกมารายงานว่าบริษัทสามารถจำกัดมัลแวร์ในระบบที่โดนโจมตีได้แล้ว และสามารถกลับมารับจองบริการขนส่งได้ตามปกติ และได้ดำเนินการกำจัดมัลแวร์และกู้คืนระบบที่เหลือจนระบบสำคัญทยอยกลับมาเป็นปกติภายใน 5 วัน ในเดือนสิงหาคมที่ผ่านมา Maersk จึงได้ออกมาสรุปยอดความเสียหายจากการโจมตีครั้งนี้ว่าอาจส่งผลกระทบต่อยอดขาดทุนในไตรมาสที่สาม เป็นมูลค่า 300 ล้านเหรียญสหรัฐ

Søren Skou CEO ของ Maersk ผู้มีประสบการณ์การทำงานกับบริษัท 34 ปี แต่เพิ่งเข้ามาดำรงตำแหน่ง CEO ได้เพียง 12 เดือนก่อนเกิดเหตุ ยอมรับว่าไม่เคยมีประสบการณ์การบริหารในสภาวะวิกฤตแบบนี้มาก่อน แต่สิ่งที่ Skou ลงมือทำทันทีคือเข้าร่วมการประชุมรับมือกับวิกฤตที่มีฝ่าย IT เข้าร่วมด้วย เพื่อให้เข้าใจว่าเกิดอะไรขึ้น และตัดสินใจว่าระบบ IT ของส่วนงานใดที่สำคัญกับธุรกิจที่สุดและควรกลับมาใช้ได้ก่อน Skou ยังดูแลให้แน่ใจว่ามีการสื่อสารทั้งภายนอกและภายในถึงข้อเท็จจริงที่เกิดขึ้นและความคืบหน้าในการแก้ไขปัญหาอย่างสม่ำเสมอ โดยเฉพาะการส่งข่าวสถานะการทำการของท่าเรือและระบบรับจองบริการขนส่ง สุดท้าย Skou ได้ให้อำนาจการตัดสินใจแก่บุคลากรหน้างานใน 130 ประเทศที่บริษัทดำเนินธุรกิจอยู่ เพื่อให้ Maersk ยังสามารถให้บริการลูกค้าได้โดยไม่ต้องรอคำสั่งจากสำนักงานใหญ่หรือกังวลเรื่องต้นทุน Skou ยังกล่าวว่าคงไม่มีทางป้องกันการโจมตีแบบนี้ได้ จึงต้องพิจารณาว่าหากเกิดเหตุการณ์เช่นนี้ขึ้นอีก Maersk จะทำอย่างไรเพื่อเรียกคืนระบบกลับมาให้เร็วกว่านี้ และจะป้องกันความเสี่ยงจากการถูกโจมตีให้มีประสิทธิภาพกว่านี้ได้อย่างไร

กรณีของ Maersk แสดงให้เห็นภาพที่ต่างออกไปจาก Target และ Sony Pictures ความรวดเร็วของบริษัทในการรับมือและเข้าจัดการกับปัญหา การมีแผนสำรองในการดำเนินธุรกิจเมื่อเกิดเหตุที่ทำให้ระบบใช้งานไม่ได้ การให้ความสำคัญกับการรักษาข้อมูลของลูกค้า แสดงให้เห็นว่า Maersk มองว่า Cybersecurity เป็นสิ่งสำคัญต่อการดำเนินธุรกิจ และเป็นความเสี่ยงที่สำคัญของบริษัท จึงมีมาตรการจัดการเพื่อให้เกิดความเสียหายน้อยที่สุดและธุรกิจยังสามารถดำเนินต่อไปได้ นอกจากนี้ CEO ของ Maersk ยังแสดงให้เห็นคุณลักษณะของผู้นำที่เห็นความสำคัญของ Cybersecurity ต่อการดำเนินธุรกิจของบริษัท และเป็นแบบอย่างให้บุคลากรในบริษัทเห็นความสำคัญนี้ ดังจะเห็นได้จากการเข้าไปทำความเข้าใจและมีส่วนร่วมในการแก้ไขปัญหา ความพร้อมที่จะปรับปรุงการรับมือและการบริหารจัดการความเสี่ยงด้าน Cybersecurity ให้เข้มแข็งยิ่งขึ้น และการให้คนทำงานมีส่วนร่วมในการรับรู้ข้อมูลที่สำคัญและมีอำนาจตัดสินใจ เพื่อช่วยกันทำให้บริษัทยังสามารถดำเนินงานต่อไปได้

Target, Sony Pictures และ Maersk ล้วนตกเป็นเหยื่อของกลุ่มคนที่ใช้ความก้าวหน้าทาง IT แสวงหาประโยชน์ในทางที่ผิด แม้จะแสดงให้เห็นภาพที่น่ากลัวของความเสี่ยงในการดำเนินธุรกิจในยุคนี้ แต่ทั้งสามกรณีก็แสดงให้เห็นว่าธุรกิจจะสามารถรับมือกับปัญหา Cybersecurity รูปแบบใดก็ตามได้ หากมีความเข้มแข็งทางระบบ IT และ "Mindset" ของผู้นำและคนทำงานที่ตระหนักถึงความสำคัญของ Cybersecurity ต่อการดำเนินธุรกิจ ไม่ใช่เพียงแค่ปัญหาสำหรับฝ่าย IT เท่านั้น และมอง Cybersecurity Risks เป็นความเสี่ยงของธุรกิจที่สามารถบริหารจัดการได้ ท่านกรรมการและผู้บริหารระดับสูงในฐานะผู้นำของบริษัท จึงควรลองกลับไปพิจารณาว่าธุรกิจของท่านในตอนนี้มี Mindset ต่อ Cybersecurity อย่างไร ยังเป็นเพียงแค่ปัญหาด้าน IT หรือไม่ แต่แน่นอนว่าในการสร้างหรือปรับเปลี่ยน Mindset ของคนทำงานเพื่อก่อให้เกิดวัฒนธรรมองค์กรแบบใดก็ตาม ปัจจัยที่สำคัญที่สุดก็คือ Mindset ของตัวผู้นำเอง



On November 22, I had the opportunity to attend the Cyber Resilience Leadership seminar organized by the Bank of Thailand (BoT). In the event, BoT invited experts in cyber security from leading international organizations to give a talk for more than 200 directors and senior executives from financial sector to realize the importance of preparing their organizations to protect themselves and deal with cyber risks effectively. Nowadays, many businesses used IT to run the business and create more growth. Thus, every business had a risk of being victimized by people who wanted to make the most of their advance in IT in the wrong way. It could be said that no company had ever been hacked anymore because there were only the companies that were aware of being hacked and those that were not aware that they were hacked. It was important how the company afforded cyber security to protect themselves from the hackers and when they hacked into the system and cause damage. How did the company afford Cyber Resilience to cope with the hackers and resume normal business operations as soon as possible?

In addition to the ideas about the role of directors and senior executives in creating cyber security and cyber resilience for their businesses, there was also an interesting issue and questions that the guest speaker encouraged us to consider throughout the event, namely the cyber security was concerning the IT system to work smoothly and be able to protect the company data, thus the risk of cyber security that the IT system was hacked or attacked in various forms, were they merely the problem of IT? Recent 2 cases from 2 companies might answer the question.

Many of us might remember the case of hacking the system to steal data at the end of 2013 of Target Company. On December 19, 2013, a giant company in retail of the United States revealed that its system was hacked to steal the data of more than 40 million credit cards of the customers that shopped during the festival at 1,797 branches of Target. Although it was known to the world on December 19, in fact, the hackers had hacked the system of Target to release a malware since November 27. It was detected by a program that worthed 1.6 million US dollars of Target (the same program as CIA and Ministry of Defence). The program sent warnings to the IT Security Department of the company for 2 times but it was ignored and there was no action taken. It was until December 12, that the Ministry of Justice sent a notice to the company that there were many unusual transactions at many branches of Target. Then, the company started to investigate the system. After that, on December 15, Target confirmed that the system was hacked and started to eliminate malwares from the system, although it had been half month already. One month later, on January 10, 2014, Target just revealed that in addition to credit card data, some personal data such as address, e-mail and telephone number of more than 70 million customers was also hacked at the same time.

As a consequence of hacked system, Gregg Steinhafel, company CEO had to apologize employees and customers of Target and discounted the products at all branches for 10% as a compensation. However, the sale in the fourth quarter fell more than 50% and 4% when compared with the same period last year. Furthermore, the company also had to pay a compensation for 61 million US dollars for the customers. It was also accused and had to pay for the sufferers and the state for 200 million US dollar followed by the improvement of cyber security and resigning of CIO in March and resigning of CEO in May 2014.

Although, there was no a clear reason why Steihafel who had worked at Target for 35 years resigned, some analysts had an opinion that it was not surprising if the CEO would have a feeling to show his responsibility to the incident that had a great impact on finance and credit of the company because the response of Target to the incident was not immediate and it did not consider sufferers sufficiently.

Another case was also a headline a year after the incident of Target and many of us might have known very well. It was a case of Sony Pictures, a company under Sony Cooperation. On November 24, 2014, a group of hackers name Guardians of Peace attacked the IT system of the company causing the system to stop working. The hackers also released the important internal data of the company, including strategic plan, marketing plan, salary structure of the senior executive, personal data and social security numbers of present and former 47,426 employees, law contracts, e-mails of the executives with shaming message concerning the stars, unreleased movies,

including The Interview which was a parody movie about assassination of North Korea leader.

This incident was a headline at that time. It was not because the Guardian of Peace required Sony to cancel the release of The Interview that could bring terrorism and lead to the conflict between United States and North Korea but the quantity of important data that should be confidential (including shaming data) that was revealed. The society questioned how a world class company like Sony was so careless. However, this was not the first time that the company was attacked by the hackers. In 2011, Sony Computer Entertainment Europe was attacked by the hackers and they stole personal data of 77 million customers worldwide on PlayStation Network. This case, the company had to pay for reparation of the system and compensation for 170 million US dollars. Besides, it was fined 250,000 pounds by Information Commissioners' Office of England because it was found that the system was hacked easily because the company did not update anti-hacking software. Only 3 years later, the similar incident happened again. Even worse, the investigation of FBI found that the hackers had entered the system 3 months ago and it could be compared with using a key to open a door that could go to every room because Sony Pictures had a careless IT security. To enter the system was not two-factor authentication that the user had to fill in password for authentication for 2 times. All Important data and documents, including contracts and business minutes were stored at a central server, while e-mail server still kept old e-mails dating back for 7 years without encryption Furthermore, the workers also worked carelessly such as keeping the password for authenticating the system in a file name "Computer Password" in their computers.

The IT system of Sony Pictures was halted for a week by this incident and the company had to spent more than 35 million US dollar to restore the system and another 8 million US dollar as a compensation of the employees that accused of the company and much more to improve internal IT system to be more complex. Moreover, the company was well known when people talked about hacking data, although the incident in 2011 of hacking PlayStation Network was a lesson for the company already. The important cause might be because in 2007, Jason Spaltro, an executive Department of Information Security of Sony Pictures had interviewed that he would not invest 10 million US dollars to prevent the risk of the company that cost only 1 million US dollar. If the company had a complex IT security system but the employees would write down their passwords on post-it and put it on the computer anyway.

From these examples, you will see that Target and Sony Pictures were affected greatly for their finance and image. It also had a direct impact on the business operation. In case of Target, the customers did not trust the system security and did not go shopping at Target. As a consequence, the company had to greatly improve its security system. For Sony Pictures, the IT system was halted and the important data and intellectual properties that had an effect on advantages of the company were revealed. Although IT was a key component for cyber security risks, the business should consider this kind of risk as business risk with strategic importance in order to manage properly because if the company considered it as it was only IT problem, the risk management and problem solving would be only the affair of IT department not the business sector.

In addition, these 2 cases have shown us that cyber security was actually not a

technical problem but people and a leader had an important role in creating a culture that the workers realized the importance of cyber security to the business. Target had a high quality program against hacking with the same standard as CIA and Ministry of Defence but the cause that expensive program could not protect important data of the company from the hackers was the carelessness of the workers themselves that ignored the warning and did not take immediate action to check and solve the problem. It indicated that the workers did not realize how much the risk had an impact on the business. It was interesting how much a leader had a role in creating awareness for the workers. Surprisingly, Sony Pictures had a very careless security for its data that we could say it was an organization culture. The person that allowed this this culture to exist in the organization was the senior executives. Thus, it was not interesting to change the attitude of the workers because the leaders did not pay much attention to cyber security, although there had been a lesson from the affiliates already.

Let's take another look at what happened recently on June 27, when Maersk, the Danish-based Conglomerate company, the largest shipping company in the world was attacked by a ransom malware developed from the same code as WannaCry, called Petya that locked up the attacked computer network for a 300 bitcoins ransom. There were many companies in many industries in Europe and America that were targeted of Petya, mostly in Ukraine. For Maersk that managed 15% of the world's shipping, the impact was so severe that the company had to shut down its IT system in order to keep malware from spreading. All shipments were stopped because the GPS did not work. The operation of 76 ports of the companies worldwide that were interconnected via the Internet were halted. Company personnel had to contact each other via their mobile phone via WhatsApp, because they could not use the email system and some jobs, such as transportation service booking was done manually in order to prevent the business to completely stop operating.

The next day after the incident, Maersk came out and explained that despite the operations were delayed, there was no leakage of customers' important data from this attack. Two days after the incident, Maersk also reported that the company was able to limit the malware on the attacked system and return to normal booking service. It removed the malware and restored the system to return to normal within 5 days. On August recently, Maersk summarized the damage from this attack that might have an impact on the third quarter of 300 million dollar.

Søren Skou, CEO of Maersk, had 34 years of experience with the company, but had been the CEO for 12 months before the incident., admitted that he had no experience in managing this kind of crisis. Skou took action immediately by attending a meeting with IT department to cope with the crisis to understand what was going on and decided which system was the most important and should be resumed first. Besides, he also ensured that there was both internal and external communication about the truth and progress to solve the problem regularly, especially updating the status of ports and transportation service booking system. Lastly, Skou has empowered decision-makers in 130 countries that the company was operating to allow them to provide services to the customers without waiting for order from the central office or worrying about the cost. Skou also said that there was no way to prevent this kind of attack. We had to consider what to do if this happened again, what Maersk would do to restore the system faster and how to protect against the risk of being attacked more effectively.

The case of Maersk has shown us a different image from Target and Sony Pictures, such as the speed of the company to deal with the problem, having a backup plan for the business when the incident caused the system to fail and emphasis on the importance of customers' data. These have shown that Maersk considered cyber security as important issue for doing a business and the major risk of the company. Thus, it had measures to minimize the damage and the business could keep operating. Moreover, CEO and Maersk also showed leadership qualities that realized the importance of cyber security on business operation of the company and they were the example for other employees as could be seen from the understanding and participation in solving the problem, readiness to strengthen handling and risk management in cyber security and workers were involved in acknowledging important information and decision power to keep the company working.

Target, Sony Pictures and Maersk were all the victims to the misuse of IT. Although it has shown a dreadful picture of the risk in running business at the present, all three cases show that businesses are able to cope with cyber security problem in any forms if there is a strong IT system and mindset of leaders and workers who realize the importance of cyber security on the business not only the problem for IT department and cyber security risk is a business risk that can be managed. Directors and executives as leaders of the company should consider how your business has a mindset toward cyber security and if it is only IT problem. Certainly, creating or changing mindset of the workers to create a corporate culture, the most important factor is the mindset of the leader itself.

นางสาวจารัรวี จิระมะกร
Ms. Charawi Chiramakara

Senior CG Analyst
Curriculum Development
Thai IOD