ปาฐกถาพิเศษและการเสวนา "Cyber Security, Privacy and Data Protection"
งานสัมมนาและแสดงนิทรรศการนานาชาติ "ดิจิทัลไทยแลนด์ 2016"
วันที่ 27 พฤษภาคม 2559 ณ ห้อง Auditorium ศูนย์การประชุมแห่งชาติสิริกิติ์

1. **ปาฐกถาพิเศษ "How the Shield was Forged in Microsoft's Way" โดย Angela McKay (Director, Government Security Policy and Strategy, Microsoft)**

ในช่วง 12 ปีที่ผ่านมา มีความเปลี่ยนแปลงในด้าน Cyber Security และ Privacy ที่คนให้ความสำคัญเป็นอย่างมาก ซึ่งมีการทำงานร่วมมือกันในแวดวงของรัฐ เอกชน รวมทั้งภาคการศึกษา โดยหากจะมองในด้านเทรนด์ของผู้ใช้อินเทอร์เน็ตโลกก็มีความเปลี่ยนแปลงเป็นอย่างมาก จากปี 2005 ที่มีผู้ใช้สูงสุดที่สหรัฐอเมริกา เฟซบุ๊กเพิ่งเริ่มจากภายในมหาวิทยาลัยฮาร์วาร์ดเท่านั้น แต่เมื่อถึงปี 2025 แนวโน้มการใช้จะไปอยู่ที่จีน อินเดีย รวมทั้งสหรัฐฯ

ยุคที่ 3 ของไอทีในองค์กร

ยุคของไอทีนั้นแบ่งเป็น 3 ยุค คือ ยุคที่ 1 เป็น IT Craftsmanship ซึ่งกระบวนการทำงานยังพึ่งพากระดาษ ต่อมาเป็นยุค Industrialization ซึ่งพัฒนาให้การทำงานจากกระดาษมาสู่เทคโนโลยีที่มีประสิทธิภาพและประสิทธิผลมากขึ้น จนถึงยุคที่ 3 คือ Digitalization ที่มีนวัตกรรมทางธุรกิจดิจิทัล หรือบริการรูปแบบใหม่ ๆ เพื่อช่วยให้ชีวิตคนดีขึ้น เช่น การประกันชีวิต การดูแลสุขภาพ

Digital Transformation

เทคโนโลยีดิจิทัลสามารถนำมาประยุกต์ใช้ให้เกิดประโยชน์ทั้งต่อการสร้างอาชีพและการเพิ่มผลผลิต การปกครอง สังคมและเศรษฐกิจ การประหยัดค่าใช้จ่าย ความมั่นคงปลอดภัย ฯลฯ การใช้ไอทีหรือเทคโนโลยีดิจิทัลไม่ใช่แค่เพื่อเชื่อมต่อระหว่างรัฐกับประชาชน เช่น เรื่องจ่ายภาษี หรือร้องเรียนเรื่องการทำงานและบริการเท่านั้น หากคนอยากจะเปิดร้านอาหารซึ่งรวมทั้งร้านขายอาหารข้างทาง ไม่จำต้องจ้างทำระบบไอทีที่ซับซ้อนมากมาย เพียงเลือกวิธีการชำระเงินผ่านเครดิตการ์ด ใช้โปรแกรมทำบัญชี และร้านมีเว็บไซต์เพื่อส่งได้ 24 ชม. ซึ่งทุกสิ่งจะอยู่ในระบบต่าง ๆ เช่น ระบบคลาวด์

คลาวด์เปลี่ยนระบบดิจิทัลได้อย่างไร

ระบบคลาวด์ทำให้ภาครัฐและอุตสาหกรรมต่าง ๆ ปรับตัวได้เร็วขึ้น เพราะข้อดีในเรื่องความเร็ว ขนาด และการประหยัดทางเศรษฐกิจได้ถึง 75% เช่น การส่งมอบโซลูชันต่าง ๆ การสั่งซื้อแค่กดปุ่มครั้งหนึ่งก็ขยาย

ความสามารถได้ทันที เช่น ลูกค้ารายใหญ่ในเม็กซิโก จัดประกวดราคาสำหรับโซลูชันเทคโนโลยีใหม่ที่จะใช้เวลาในการส่งมอบ แต่การเลือกใช้ระบบคลาวด์ ทำให้ลดเวลาในการส่งมอบลง

ความเสี่ยงด้านไซเบอร์

การโจมตีทางไซเบอร์ที่พบเห็นทั่วไปในปัจจุบันมี 3 รูปแบบ คือ **DDos** ซึ่งเป็นการโจมตีสภาพความพร้อมใช้งานของระบบ ซึ่งระบบคลาวด์จะช่วยตรงนี้ได้ **Credential compromise** ในเรื่องข้อมูลประจำตัว ซึ่งตอนนี้มีเทคโนโลยีใหม่ ๆ ที่ช่วยป้องกันไม่ให้การโจมตีจากข้อมูลประจำตัวเหล่านี้ได้ และ **Malware exploits** ซึ่งมัลแวร์ประเภทต่าง ๆ มีการพัฒนาเป็นจำนวนมาก

ในด้านสภาพแวดล้อมของความเสี่ยงด้านไซเบอร์นั้น ประกอบด้วย **ผู้กระทำ** ซึ่งมีอยู่หลายกลุ่ม ทั้งระดับบุคคล ไปถึงระดับชาติ **วัตถุประสงค์**ในการโจมตีก็หลากหลายแตกต่างกันไป ทั้งต้องการชื่อเสียง การโจมตีความมั่นคงของประเทศ ฯลฯ โดย**เครื่องมือและเทคนิควิธีการ**เปลี่ยนแปลงไปอย่างรวดเร็ว และ**ผลกระทบ**ที่เกิดทั้งในด้านการเงิน ข้อมูลข่าวสาร หรือระบบ IP ซึ่งถือเป็นสินทรัพย์ที่มีค่าต่อองค์กรอย่างยิ่ง

เรื่องความมั่นคงปลอดภัยไซเบอร์ จึงกลายเป็นประเด็นที่ผู้บริหารระดับสูงต้องให้ความสำคัญ เพราะเป็นสิ่งที่จำเป็นต่อทั้งองค์กร

การบริหารจัดการความเสี่ยงด้านไซเบอร์

ไมโครซอฟท์ ให้ความสำคัญกับหลักการด้าน Privacy หรือความเป็นส่วนตัวที่เข้มแข็งและการปฏิบัติที่คำนึงถึงความมั่นคงปลอดภัย เพราะต้องการให้เกิดความน่าเชื่อถือของผลิตภัณฑ์ โดยมีการลงทุนทั้งในเรื่องแพลตฟอร์มและบริการที่เชื่อถือ การต่อต้านและดำเนินการเชิงรุกในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ และสนับสนุนนโยบายและการปฏิบัติที่ส่งเสริมด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยหลัก Protect-Detect-Respond

“Protect” หรือ การป้องกัน ซึ่งไม่ใช่เรื่องยากในการทำให้เกิดความพร้อม แต่สิ่งที่ยากคือ อะไรคือข้อมูลสำคัญ (Critical Information) ซึ่งต้องมองใน 2 ด้านคือ สิ่งสำคัญที่ทำให้ธุรกิจดำเนินต่อไปได้ และสิ่งที่ผู้ไม่ประสงค์ดีมุ่งหวัง ซึ่งต้องจัดลำดับความสำคัญและพิจารณาอย่างถี่ถ้วน และใช้นโยบายและการปฏิบัติในวงกว้าง เช่น การติดตั้งแพตช์ หรือการพัฒนาซอฟต์แวร์และบริการต่าง ๆ เพื่อลดระดับความรุนแรง ซึ่งองค์กรนั้นรู้วิธีในการตอบสนองกับจุดอ่อนที่เกิดขึ้นหรือไม่

“Detect” หรือ การตรวจจับ ต้องดูการทำงานแบบปกติในการรับส่งข้อมูลจากแต่ละส่วนที่แตกต่างว่าเป็นอย่างไรในสถานการณ์ปกติก่อน เพื่อได้รู้ว่าเหตุการณ์ไม่ปกติจะเป็นอย่างไร

“Respond” หรือ การตอบสนอง เช่นจะตอบสนองอย่างไรถ้าพบว่าซอฟต์แวร์ที่ใช้มีช่องโหว่ หรือถ้าตรวจพบว่ามีสิ่งผิดปกติเกิดขึ้น จะต้องสืบสวนและวิเคราะห์อย่างรวดเร็ว เพื่อบรรเทาความเสี่ยง องค์กรต้องจัดการโดยมีแผนการรับมือกับภัยคุกคามที่ชัดเจน ทีมงานต้องมีวิธีการทำงานที่ชัดเจน เช่น ทีมประชาสัมพันธ์จะสื่อสารกับสาธารณะอย่างไร ทีมกฎหมายจะจัดการกับเหตุการณ์หรือคดีอย่างไร สุดท้ายคือ ด้าน Forensics ต้องตรวจพิสูจน์พยานหลักฐาน เพื่อที่จะดำเนินคดีกับผู้ที่ก่อเหตุ ไม่ใช่ปล่อยให้เขาหนีไป ต้องพิสูจน์ว่ามัลแวร์มีการเคลื่อนที่เคลื่อนไหวอย่างไร ซึ่งสามารถให้ข้อมูลของเขาได้

ความสำคัญของระบบคลาวด์

เนื่องจากการเติบโตของภัยคุกคามที่มากขึ้น ทำให้จำเป็นต้องมีสถาปัตยกรรมทางเทคโนโลยีไฮบริด (Hybrid Technology Architecture) โดยไมโครซอฟท์มีทางเลือกของรูปแบบในการใช้ให้เหมาะสม ทั้งในแบบส่วนตัว แบบสาธารณะ และแบบไฮบริด และรูปแบบของบริการ ที่มีทั้งโครงสร้างพื้นฐาน แพลตฟอร์ม และซอฟต์แวร์ โดยมีหลักการของคลาวด์ที่เชื่อถือได้ (Trusted Cloud Principles) โดยเน้น**ความมั่นคงปลอดภัย ความเป็นส่วนตัว และการควบคุม** ซึ่งมีทางเลือกในการเก็บข้อมูล **การปฏิบัติตามข้อกำหนดต่าง ๆ** ซึ่งต้องปฏิบัติตามแต่ละภูมิภาคที่อยู่ และ**ความโปร่งใส** ในการทำงานกับตัวแทนในท้องถิ่นต้องแสดงให้เห็น

ความร่วมมือ

การต้องพึ่งพากันและความเสี่ยงจะขับเคลื่อนนโยบายสาธารณะ ซึ่งผู้วางนโยบายต้องดูทั้งระบบ สังคม และอธิปไตย ซึ่งเทคโนโลยีมาท้าทายในเรื่องนี้ โดยความกดดันของบทบาทและการเป็นผู้ออกกฎของรัฐบาล จะต้องมีการพูดคุย ซึ่งบางครั้งอาจจะมีจุดอ่อนที่ต้องปกป้องข้อมูล ซึ่งจากการติดตามมีอย่างน้อย 95 ประเทศ ที่มีการริเริ่มในเรื่องการพัฒนาด้านกฎหมาย ซึ่งการเพิ่มขึ้นของความไม่มั่นคงปลอดภัยในระดับนานาชาติและความกดดันในการออกกฎระเบียบข้อบังคับ ทำให้นวัตกรรมอยู่ในความเสี่ยงไปพร้อม ๆ กัน

สุดท้ายการเปลี่ยนโฉมหน้าไปสู่ดิจิทัล เป็นความท้าทายที่จะต้องพร้อมต่อสู้กับความเสี่ยง โดยต้องใช้แนวทางในการบริหารจัดการความเสี่ยง การแชร์ข้อมูล การจัดการกับความเปราะบาง การปกป้องโครงสร้างพื้นฐานที่สำคัญ รวมทั้งบรรทัดฐาน ในบทบาทที่สอดประสานกัน

2. **การเสวนา “Learn from the Giants, How They Lift Cybersecurity and Privacy Obstacles”** โดย
   - **Philipp Dupuis (Minister Counselor, Head of the Trade and Economic Section of the EU Delegation to Bangkok)**
   - **Ssu-Han Koh (Sales Engineer Manager – South East Asia Intel Security)**
   - **Jimmy Low (Pre-Sales Manager, Kaspersky Lab SEA)**
   - **อาทิตย์ สุริยะวงศ์กุล (Coordinator, Thai Netizen Network)**
   - **ดร.ชาลี วรกุลพิพัฒน์ (NECTEC)**
   - **ดร.ชัยชนะ มิตรพันธ์ (รองผู้อำนวยการ ETDA)** ดำเนินรายการ

การเรียนรู้จากภาคเอกชน

ในเรื่องความเป็นส่วนตัวของทาง **Intel** นั้น เริ่มจากการป้องกันทรัพย์สินของบริษัท มีอะไรบ้างที่เป็นความลับ วิธีการทำงานคือ แยกแยะ จัดกลุ่ม และดูระดับการควบคุม สิ่งไหนที่อ่อนไหวก็ให้ความสำคัญสูงกว่า โดยดูที่ปัจจัย เช่นในเรื่องคน อยากปกป้องข้อมูล แต่ก็ต้องให้ข้อมูลด้วย ซึ่งหากจำเป็นต้องแลกในเรื่องความเป็นส่วนตัว ก็ให้ได้เพียงระดับหนึ่ง ซึ่งในสิงคโปร์เอง มีกฎหมายเรื่องความเป็นส่วนตัว หรือในเรื่องกระบวนการและนโยบายในการแชร์ข้อมูล ต้องดูว่าการพูดคุยอยู่ในระดับไหนและสามารถแชร์ข้อมูลได้ในระดับไหน ส่วนในการควบคุม คือการอนุญาต จะให้ระดับไหน เช่น การแชร์รูป แชร์ได้ในระดับไหน มีตัวเลือกว่าใช้ หรือไม่ให้ใช้ระดับไหน

ด้าน **Kaspersky** ในฐานะแลบที่ทำงานมา 18 ปีแล้ว ในเรื่องความเป็นส่วนตัว ต้องมีความรับผิดชอบในเรื่องข้อมูลที่เผยแพร่ออกไป ต้องดูบทบาทในองค์กรในเรื่องการกระจายข้อมูล ข้อมูลบางชนิดสามารถไปพูดคุยในที่สาธารณะได้ แต่บางเรื่องต้องดูเรื่องการตลาด เรื่องแผนกอื่น ซึ่งเป็นการควบคุมโดยตำแหน่งหน้าที่ และเมื่อพูดถึงภัยคุกคาม ก็มีการแยกระหว่างฝ่ายปฏิบัติการ ฝ่ายพัฒนาองค์กร ถ้ามีการเจาะระบบ ก็จะปกป้องได้ง่ายขึ้น เพราะมีการแยกส่วนการทำงาน

มุมมองจากภาครัฐ

ทางฝั่ง **สหภาพยุโรป** หรือ **EU** มองว่า โลกกำลังร้อนเรื่องความมั่นคงปลอดภัยไซเบอร์ โดย EU จะบังคับใช้กฎหมายเกี่ยวกับการปกป้องข้อมูล ซึ่งมีความท้าทายเพราะ EU มีถึง 28 ประเทศ ซึ่งโครงสร้างทางกฎหมายต่างกัน แต่มีตลาดร่วมที่เคลื่อนไหวไปสู่ดิจิทัลซึ่งมีจุดอ่อนด้วย โดยมีความพยายามในการกำหนดกฎหมายให้เป็นแนวเดียวกัน

ความเป็นส่วนตัวและข้อมูลส่วนบุคคลเป็นหลักการพื้นฐาน (Fundamental Rights) ที่กำหนดในกฎหมายของ EU อยู่แล้ว แต่เนื่องจากช่วงที่ผ่านมา กฎในการรักษาความเป็นส่วนตัวและข้อมูลส่วนบุคคลของ EU มีการเปลี่ยนแปลง (General Data Protection Regulation) โดยให้การคุ้มครองแก่ปัจเจกชนมากขึ้น ทั้งเรื่อง Right to Be Forgotten ที่เจ้าของข้อมูลมีสิทธิขอให้ผู้ให้บริการ Search Engine ลบข้อมูลของตนออกจากระบบ (แต่สิทธินี้ไม่ใช้กับอาชญากรหรือนักการเมือง) และเรื่อง Right of Data Portability ที่เจ้าของข้อมูลมีสิทธิในการขอให้โอนหรือส่งต่อข้อมูลของตนเพื่อใช้กับบริการอื่น ๆ ด้วยได้

ความเห็นจากภาคประชาสังคม

ในมุมมองของตัวแทนประชาชนจาก **Thai Netizen Network** เห็นว่า ข้อมูลเป็นอำนาจ มีมากเท่าไหร่ ก็สามารถตัดสินใจเกี่ยวกับเรื่องต่าง ๆ ได้ดีขึ้น และสำหรับข้อมูลส่วนตัว ถ้าใครมีข้อมูลส่วนตัวของเรา เขาก็สามารถควบคุมชีวิตเราได้ การให้สิทธิอย่าง EU ในการควบคุมข้อมูลของตัวเราเองก็เป็นสิ่งที่น่าสนใจ

หากจะดูในเรื่องโครงสร้างของ Content-Platform-Network ทุกรัฐบาลในโลกต้องการให้ประชาชนมีความมั่นคงปลอดภัยมากขึ้น ซึ่งหมายถึง การควบคุมกำกับดูแล การหามาตรการปกป้องพลเมือง เริ่มจาก Content หรือเนื้อหา ในอดีตเรามีสถานีวิทยุโทรทัศน์ไม่กี่สถานี ถ้าสถานีนั้นมีเนื้อหาไม่ดี ก็ไปที่สถานีนั้น เพื่อหยุดการเผยแพร่เนื้อหานั้นก็สามารถทำได้ เพราะมีน้อย แต่เมื่อเข้าสู่ยุคอินเทอร์เน็ต ทุกคนคือผู้สร้างเนื้อหา การกำกับดูแลจึงเคลื่อนไปสู่ผู้ให้บริการแพลตฟอร์ม (Platform) แต่ปัญหาคือ ในบางบริบท ความรับผิดใช้ไม่ได้ เพราะผู้ให้บริการไม่ได้อยู่ในเมืองไทย เมื่อรัฐบาลไม่สามารถควบคุมแพลตฟอร์ม ก็ไปถึงเน็ตเวิร์ก (Network) ผลที่เกิดขึ้นคือ คนที่ได้รับผลคือเจ้าของเนื้อหา การไปปิดเว็บไซต์ที่มีเนื้อหาเสียแค่เรื่องเดียว อาจกระทบต่อเนื้อหาที่เป็นประโยชน์ด้วย การลงมาถึงเน็ตเวิร์กมากเท่าไหร่จึงส่งผลที่ไม่พึงประสงค์มากขึ้น

ข้อคิดจากฝ่ายนโยบายและนักวิจัย

ด้านนักวิจัยซึ่งเป็นหนึ่งในคณะอนุกรรมการมั่นคงปลอดภัย ภายใต้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ ด้วยมองว่า การจะทำให้เกิดความสมดุลระหว่างการปกป้องข้อมูล หนึ่งคือนโยบาย สองคือโซลูชันด้านไอที ซึ่งภาคเอกชนนั้นช่วยได้ในการจัดทำนโยบาย ต้องดึงผู้มีส่วนได้ส่วนเสียทุกภาคส่วนเข้ามาร่วมมือกัน ถ้ามีเฉพาะเจ้าหน้าที่ทางด้านเทคนิคการกำหนดนโยบายก็จะไม่ได้ผล ส่วนในด้านไอทีนั้น การพัฒนาโซลูชันไอทีขึ้นมาชิ้นหนึ่งต้องเน้นทุกส่วนในนโยบาย เช่นใน **NECTEC** ดูทั้งการควบคุม การสำรอง และการบริหารจัดการความเสี่ยง ซึ่งต้องระบุว่าจะควบคุมการเข้าถึงข้อมูลอย่างไร อาจต้องอยู่ในเครือข่ายต่างหาก เช่น อินเทอร์เน็ต อันที่สองคือหลายองค์กร อนุญาตให้พนักงานนำอุปกรณ์ของตัวเองมาใช้ ซึ่งอุปกรณ์เคลื่อนที่มีความละเอียดอ่อน จะต้องควบคุมการเข้าถึง ซึ่งเป็นสิ่งสำคัญ เช่น ถ้าหาย สามารถสั่งการจากระยะไกลให้ข้อมูลถูกลบออกไปได้ ซึ่งคิดในแง่

ความเป็นส่วนตัวของข้อมูลขององค์กร แต่ก็ทำให้ความเป็นส่วนตัวของผู้ใช้หายไป ซึ่งแต่ละองค์กรก็มีระดับการยอมรับแตกต่างกันไป

ความร่วมมือเป็นสิ่งสำคัญ

ทาง **Intel** ให้ความเห็นว่าความเป็นส่วนตัวและความมั่นคงปลอดภัยนั้นแตกต่างกัน ซึ่งเป็นเรื่องความร่วมมือทั้งบุคคล รัฐบาล กิจการต่าง ๆ ในทั้งกระบวนการ โดย Intel มีการทำงานร่วมกับพาร์ทเนอร์ ที่มีการแบ่งปันข้อมูล แม้เป็นคู่แข่งก็มีการร่วมมือแชร์ข้อมูลเพื่อให้เกิดประโยชน์ โดยในปีที่แล้ว สามารถช่วยเหลือเจ้าหน้าที่ปราบปราม Botnet มีการทำงานร่วมกันภายในองค์กร ดูว่าจะต้องช่วยเหลือองค์กรอย่างไรภายในสภาพแวดล้อม ซึ่งมีโครงสร้างพื้นฐานที่ไม่เพียงปกป้องไม่ใช่เฉพาะของ Intel เท่านั้น แต่ให้ธุรกิจในภาพรวมดำเนินต่อไปได้

ด้าน **Kaspersky** เสริมเรื่องความร่วมมือกับเจ้าหน้าที่รักษากฎหมายในการต่อต้านอาชญากรรมทางอินเทอร์เน็ต ซึ่งทำโดยฝ่ายเดียวไม่ได้ โดยจุดที่อ่อนแอที่สุดคือ “คน” ดังนั้น คนต้องมีความรู้ในเรื่องของความเสี่ยง

ฝ่าย **EU** นั้น เห็นว่า รัฐบาลไม่ใช่ผู้รู้ทุกอย่าง ต้องอาศัยความร่วมมือในการทำงาน การมีร่างกฎหมายหรือกฎระเบียบต่าง ๆ ต้องรับฟังความคิดเห็นและข้อกังวล ซึ่งต้องใช้ความเชี่ยวชาญจากทุกฝ่ายเข้ามามีส่วนร่วม

ด้าน **NECTEC** กล่าวว่า วิธีที่ดีที่สุดที่จะให้เกิดความร่วมมือคือ การสร้างชุมชนแบบไม่เป็นทางการ ข้อดีคือความคุ้นเคยจากการได้มาแลกเปลี่ยนมุมมองที่แตกต่างกัน เช่น มี TISA ที่มีบุคคลจากหลายสาขามาร่วมกัน ชุมชนลักษณะนี้ทำให้เกิดการจัดอบรม สร้างอาสาสมัคร ให้ความรู้ทั้งที่เป็นทางการและไม่เป็นทางการ หรือ ETDA ก็มีเวทีพูดคุยเช่นกัน (ETDA Open Forum)

ส่วน **Thai Netizen Network** พูดถึงหลักการของระดับสากล เช่น หลักการมะนิลา ซึ่งเป็นร่วมมือระหว่างภาคเอกชนกับภาคประชาสังคมที่กำหนดความรับผิดของคนกลาง (Intermediary Liability) เพื่อให้ภาครัฐเห็นชอบและยอมรับ หรือของ UN ที่กำหนดเรื่องแนวทางในการดำเนินการให้กับธุรกิจและการคุ้มครองสิทธิมนุษยชน นอกจากกฎระเบียบเหล่านี้ ก็มีความร่วมมือระหว่างธุรกิจและการพูดคุยผ่านเวทีต่าง ๆ เช่น Telecommunication Industry Dialogue, Global Network Initiative ฯลฯ

ดร.ชัยชนะ จาก ETDA ทิ้งท้ายว่า การพูดคุยวันนี้อยู่บนพื้นฐานของการขับเคลื่อนเศรษฐกิจดิจิทัล ในฐานะหน่วยงานรัฐ ETDA ได้จัดเวทีนี้ให้เป็นอีกเวทีหนึ่งที่สะท้อนถึงความร่วมมือของทุกภาคส่วน เพื่อร่วมกันหาความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยบนโลกออนไลน์ อีกทั้งยังเพื่อสร้างความเชื่อมั่นในการทำธุรกรรมทางออนไลน์ ซึ่งเป็นปัจจัยสำคัญที่จะช่วยให้เศรษฐกิจและสังคมดิจิทัลเดินหน้าต่อไป