บทความพิเศษ

เตรียมการอย่างไรเพื่อรับมือ Internet of Things (IoT)

กสทช. ประวิทย์ ลี่สถาพรวงศา*

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

บทคัดย่อ

อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things - IoT) เป็นเทคโนโลยีที่จะนำมาซึ่งความสะดวกสบายในชีวิตประจำวัน และทำให้ประชาชนมีคุณภาพชีวิตที่ดีขึ้น แต่การจะใช้งาน IoT ได้อย่างมีประสิทธิภาพจำเป็นที่ประเทศไทยต้องเร่งจัดสรรคลื่นความถี่ให้เพียงพอกับการใช้งานในอนาคตอันใกล้ เพื่อรองรับปริมาณการสื่อสารขนาดมหาศาลและหนาแน่นในทุกพื้นที่ นอกจากนี้ ควรต้องเตรียมการรับมือภัยคุกคามจากการโจมตีทางไซเบอร์ โดยเฉพาะอย่างยิ่งการโจมตีโครงสร้างพื้นฐานที่สำคัญของประเทศ เช่น มีนโยบายกำกับดูแลด้านความปลอดภัยทางไซเบอร์ ให้มีการทดสอบและพัฒนาระบบป้องกันการโจมตี และมีมาตรการรับมืออย่างทันท่วงทีเมื่อเกิดกรณีถูกโจมตีขึ้น ในส่วนของการคุ้มครองผู้บริโภคนั้น ควรมีการฝังระบบรักษาความปลอดภัยตั้งแต่ขั้นตอนการออกแบบผลิตภัณฑ์ มีการอัปเดตเฟิร์มแวร์ในอุปกรณ์ทุกชิ้นโดยอัตโนมัติ รวมถึงการวางแนวทางในการกำหนดผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการใช้อุปกรณ์ นอกจากนี้ต้องมีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยห้ามขายต่อข้อมูล ห้ามนำข้อมูลไปใช้ผิดวัตถุประสงค์ โดยการใช้ประโยชน์อื่นใดจากข้อมูล ต้องขอความยินยอมจากเจ้าของข้อมูลเสมอ ประเด็นสุดท้ายที่สำคัญคือ ต้องรณรงค์ให้ประชาชนเกิดความตระหนักและมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อเสริมสร้างอุปนิสัยในการใช้งานอุปกรณ์ IoT ต่างๆ อย่างปลอดภัย

คำสำคัญ : อินเทอร์เน็ตของสรรพสิ่ง แผนการจัดสรรคลื่นความถี่ การเรียกคืนคลื่นความถี่และนำมาจัดสรรใหม่ การจัดประมูลล่วงหน้า การโจมตีทางไซเบอร์ ความปลอดภัยทางไซเบอร์ข้อมูลขนาดใหญ่ การคุ้มครองข้อมูลส่วนบุคคล

Abstract

Internet of things (IoT) is the technology that brings great convenience to people's daily life and enhances the quality of life. However, in order to make an efficient use of the IoT, Thailand should accelerate the spectrum assignment to be sufficient for the utilization in the imminent future, serving the massive and dense quantity of communications in all areas. Moreover, there is a necessity to prepare for coping with the threat of cyber attacks, especially for its target at the country's critical infrastructure. This can be done by stipulating the cyber security policies and regulations, testing and developing the cyber-attack prevention system, as well as specifying the countermeasures for an immediate response to the cyber attack. As for the consumer protection, matters of great concern are to make an embedded system security at the beginning of product design process that provides automatic firmware update functionalities for all devices including set up a guideline to indicate a person who is responsible for damages caused by using those devices. In addition, it is required to enact data protection law that prohibits the deeds of selling and misusing data as well as leveraging data without the permission of the data owner. The last critical concern is to raise people's awareness and understanding of the threat of cyber attacks so as to build the safety habits for using the IoT devices.

Keywords : Internet of Things, IoT, Spectrum Roadmap, Refarming, Early AuctionCyber, Attack, Cyber Security, Big Data, Data Privacy

โลกยุค IoT กับการจัดสรรคลื่นความถี่

เทคโนโลยีนำมาซึ่งความสะดวกสบายในชีวิตประจำวัน ดังเช่นเทคโนโลยีการสื่อสารที่ช่วยให้เกิดการเชื่อมโยงข้อมูลจากทุกมุมโลก ทำให้ผู้คนที่แม้จะอยู่กันคนละทวีป ก็สามารถพบปะและสื่อสารกันได้บนโลกออนไลน์โดยไม่ต้องไปมาหาสู่กันจริงๆ หรือทำให้เราสามารถค้นหาสินค้าจากต่างประเทศและสั่งซื้อพร้อมชำระเงินออนไลน์ หลังจากนั้นก็เพียงรอรับสินค้าที่จะถูกส่งมาถึงบ้าน ระบบอินเทอร์เน็ตที่เชื่อมต่อข้อมูลอย่างกว้างขวางนี้จึงได้รับการขนานนามว่า *“อินเทอร์เน็ตของข้อมูลข่าวสาร”* และผู้ที่ใช้สื่อสารผ่านช่องทางอินเทอร์เน็ตนี้ก็คือ คนเรานั่นเอง

ขณะเดียวกันในช่วงหลายปีที่ผ่านมา นอกจากการเชื่อมต่ออินเทอร์เน็ตระหว่างคนกับคนแล้ว ยังเริ่มมีการสื่อสารผ่านการเชื่อมต่ออินเทอร์เน็ตระหว่างคนกับสิ่งของ และระหว่างสิ่งของกับสิ่งของด้วยกันเอง จนเรียกกันว่า *“อินเทอร์เน็ตของสรรพสิ่ง”* (Internet of Things - IoT) ตัวอย่างเช่น กล้องวงจรปิดหรือเครื่องใช้ต่างๆ ภายในบ้าน ที่เราสามารถควบคุมทางไกลด้วยอินเทอร์เน็ตผ่านโทรศัพท์มือถือ การขับเคลื่อน

รถยนต์ในลักษณะไร้คนขับ ตู้เย็นอัจฉริยะที่จะคอยรายงานเมื่อข้าวของบางอย่างในตู้ร่อยหรอลงหรือหมดอายุ และจะคอยจดรายการของที่จะต้องซื้อให้เราด้วย หรือแม้กระทั่งอุปกรณ์คอมพิวเตอร์ขนาดเล็กที่ติดตั้งใช้งานบนส่วนต่างๆ ของร่างกาย เช่น เซ็นเซอร์วัดระยะทางของการวิ่ง วัดอัตราการเต้นของหัวใจ วัดอุณหภูมิรอบๆ และคอยบอกพิกัดตำแหน่งบนโลก อุปกรณ์เหล่านี้ก็ล้วนเป็น IoT ด้วยเช่นกัน

เรื่อง IoT นี้ไม่ได้มีแค่การเชื่อมต่ออุปกรณ์พกพาหรือสิ่งของเครื่องใช้ต่างๆ ในบ้านเข้ากับอินเทอร์เน็ตเท่านั้น แต่ยังมีศักยภาพที่สามารถเปลี่ยนแปลงเมืองได้ทั้งเมืองเลยทีเดียว เช่น โครงข่ายจราจรอัจฉริยะ ซึ่งจะรายงานข้อมูลสภาพการจราจรแบบเรียลไทม์ที่ได้จากเซ็นเซอร์ตรวจจับความเคลื่อนไหว ช่วยให้ผู้ขับขี่รถยนต์สามารถตัดสินใจเลือกเส้นทางที่ประหยัดเวลาในการเดินทางได้ มีแอปพลิเคชั่นเพื่อใช้หาที่จอดรถที่ยังว่างอยู่ ในเวลากลางคืน ไฟส่องสว่างจะดับลงในกรณีที่ถนนโล่งไม่มีรถแล่นผ่าน ซึ่งจะช่วยประหยัดพลังงานไฟฟ้าให้กับเมือง หรืออย่างเช่นโครงข่ายไฟฟ้าอัจฉริยะที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารมาบริหารจัดการควบคุมการผลิต ส่ง และจ่ายพลังงานไฟฟ้า สามารถรองรับการเชื่อมต่อระบบไฟฟ้าจากแหล่งพลังงานทางเลือกที่สะอาด ซึ่งจะช่วยลดความจำเป็นในการก่อสร้างโรงไฟฟ้าแห่งใหม่ที่อาจก่อมลพิษสูง อย่างเช่น โรงไฟฟ้าที่ใช้พลังงานจากเชื้อเพลิงถ่านหิน เป็นต้น

ทั้งนี้ คาดกันว่าปัจจุบันทั่วโลกมีอุปกรณ์ IoT ที่เชื่อมต่ออินเทอร์เน็ตกว่า 13,000 ล้านชิ้น และจะได้รับความนิยมใช้งานเพิ่มขึ้น โดยบริษัท SAP ซึ่งเป็นผู้ผลิตซอฟต์แวร์รายใหญ่ของโลกสัญชาติเยอรมัน คาดการณ์ว่าภายในปี ค.ศ. 2020 ทั่วโลกจะมีอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตจำนวนเกิน 50,000 ล้านชิ้น เรียกว่ามีจำนวนมากกว่าประชากรทั้งโลก ขณะที่คาดว่า IoT จะสร้างรายได้จากการเชื่อมต่ออินเทอร์เน็ตให้กับผู้ให้บริการอินเทอร์เน็ตราว 8,100 ล้านยูโร

จากตัวเลขประมาณการข้างต้นสะท้อนให้เห็นว่า การใช้งาน IoT จะขยายตัวเพิ่มขึ้นอย่างรวดเร็วในช่วงเวลาไม่กี่ปีข้างหน้านี้ แต่ด้วยเทคโนโลยีการสื่อสารไร้สายในปัจจุบันที่ยังมีข้อจำกัด ทำให้การเชื่อมต่อสิ่งของต่างๆ มักทำได้ดีเฉพาะการเชื่อมต่อเครื่องใช้ประจำที่ผ่านอินเทอร์เน็ตประจำ ที่ซึ่งวางสายเข้าสู่บ้านหรือสำนักงาน หากจะมีการเชื่อมต่อสิ่งของต่างๆ มากมายจริงๆ ก็ต้องออกแบบโครงข่ายไร้สายให้รองรับปริมาณการสื่อสารขนาดมหาศาลและหนาแน่นในทุกพื้นที่ รวมทั้งต้องรองรับการตอบสนองได้อย่างฉับไว เพราะการใช้งานอินเทอร์เน็ตในวันข้างหน้าต้องการความเร็วสูงขึ้นเรื่อยๆ ซึ่งเทคโนโลยี 4G ไม่สามารถรองรับความต้องการในลักษณะนี้ได้ แต่ 5G ที่กำลังจะมาถึง ได้รับการออกแบบเพื่อตอบสนองความต้องการดังกล่าว กล่าวคือ หากเราควบคุมรถยนต์ผ่านระบบ 4G ซึ่งมีความหน่วงในการตอบสนอง (Latency) ก็จะเกิดอุบัติเหตุวุ่นวายมากมายบนท้องถนน แต่ผลการทดลอง 5G ในปัจจุบันสามารถลดความหน่วงของสัญญาณไปกลับหนึ่งรอบเหลือเพียงสองในพันส่วนของวินาที ทำให้สามารถควบคุมอุปกรณ์ทางไกลได้ฉับไว เกือบเหมือนควบคุมด้วยมือของเราเอง เช่นเดียวกับการผ่าตัดทางไกล การกู้ภัยในพื้นที่อันตรายก็จะปลอดภัยยิ่งขึ้นกว่าในปัจจุบัน

จากการศึกษาของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union - ITU) พบว่า ความต้องการจำนวนคลื่นความถี่ของแต่ละประเทศในการใช้งาน เพื่อให้บริการโทรคมนาคม

จะเพิ่มเป็นจำนวน 1340 MHz ถึง 1960 MHz ในปี ค.ศ. 2020 ดังนั้น ประเด็นการจัดสรรทรัพยากรคลื่นความถี่ให้เพียงพอกับการใช้งานของเทคโนโลยี จึงถือเป็นหัวใจสำคัญ โดยประเทศไทยควรมีการกำหนดแผนการจัดสรรคลื่นความถี่ (Spectrum Roadmap) เพื่อรองรับการก้าวเข้าสู่ยุค IoT ซึ่งนอกจากการจัดทำให้เป็นไปตามมาตรฐานสากลแล้ว ขณะเดียวกันกับดักสำคัญที่ประเทศไทยติดหล่มอยู่หลายสิบปี คือปัญหาคลื่นความถี่จำนวนมากยังอยู่ในมือของรัฐวิสาหกิจเจ้าของเดิมไม่ยอมคืน เพราะฉะนั้นจึงจำเป็นต้องเร่งดำเนินการเรียกคืนคลื่นความถี่และนำมาจัดสรรใหม่ (Refarming) นอกจากนี้สิ่งสำคัญอีกประการหนึ่งคือ การกำหนดให้มีการจัดประมูลล่วงหน้า (Early Auction) เนื่องจากการประมูลล่วงหน้าจะทำให้ไม่เกิดช่องว่างในการใช้งานคลื่นความถี่ อีกทั้งผู้ให้บริการโทรคมนาคมมีระยะเวลาในการเตรียมการและสามารถเปลี่ยนแปลงเทคโนโลยีได้ทัน

ความเสี่ยงของ IoT กับการคุ้มครองผู้บริโภค

ดูเหมือนอนาคตอันใกล้ในโลกยุค IoT ชีวิตความเป็นอยู่ของคนเราจะสะดวกสบายและมีคุณภาพชีวิตที่ดีขึ้น ต่อไปเราจะถูกแวดล้อมด้วยระบบอัจฉริยะ ไม่ว่าอุปกรณ์เครื่องใช้อัจฉริยะ บ้านอัจฉริยะ โครงข่ายการจราจรอัจฉริยะ เมืองอัจฉริยะ จนหลายคนเฝ้ารอการมาถึง แต่ทุกเรื่องราวย่อมมีทั้งข้อดีข้อเสีย ที่ผ่านมาอินเทอร์เน็ตของข้อมูลทำให้เยาวชนเข้าถึงการพนันออนไลน์ แหล่งยาเสพติด และสื่อลามก ผู้ก่อการร้ายเข้าถึงความรู้ในการสร้างอาวุธทำลายล้างชีวิต คนบางกลุ่มใช้อินเทอร์เน็ตเพื่อสร้างข่าวลวงหรือใส่ร้ายคนอื่น มิจฉาชีพสวมรอยเพื่อแฮ็กบัญชีธนาคารหรือบัญชีเครือข่ายสังคมออนไลน์ ในปัจจุบันการหลอกลวงและการฉ้อโกงผ่านอินเทอร์เน็ตเป็นข่าวที่พบได้ทุกวัน ฉันใดฉันนั้น อินเทอร์เน็ตของสรรพสิ่งที่ไม่มีระบบการรักษาความปลอดภัยที่ดีพอก็ย่อมมีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ และอาจส่งผลกระทบในวงกว้างได้ ลองคิดดูว่าหากมีผู้ประสงค์ร้ายเจาะระบบอุปกรณ์ทางการแพทย์เพื่อขโมยข้อมูลด้านสุขภาพ หรือเปลี่ยนแปลงการทำงานของอุปกรณ์ทางการแพทย์ ผลเสียที่เกิดขึ้นก็อาจร้ายแรงถึงการรักษาพยาบาลและชีวิตของผู้ป่วยได้

ในการประชุม Mobile World Congress 2017 ที่ประเทศสเปน เมื่อเดือนมีนาคมที่ผ่านมา มีการพูดถึงระบบรักษาความปลอดภัยของอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตทั่วโลก ผู้บริหาร SoftBank เล่าว่า พนักงานของบริษัทคนหนึ่งนัดทานอาหารเที่ยงกับภรรยา ขณะนั่งรอภรรยาในร้านก็ใช้เวลาว่างทดสอบระบบรักษาความปลอดภัยของกล้องวงจรปิดสาธารณะ เพียงแค่ช่วงเวลาก่อนภรรยาเดินทางมาถึง ปรากฏว่าเขาสามารถแฮ็กกล้องวงจรปิดได้ถึงหนึ่งล้านสองแสนตัว

และในการประชุมดังกล่าวยังได้มีการสาธิตการแฮ็ก BabyCam (กล้องวงจรปิดเฝ้าดูทารก) กาต้มน้ำและเครื่องทำกาแฟ โดยใช้เวลาเพียงไม่กี่วินาที ซึ่งผู้เชี่ยวชาญระบุว่า เราเตอร์อินเทอร์เน็ตตามบ้านหลายร้อยล้านเครื่องทั่วโลกถูกแฮ็กได้ง่ายมาก โดยเฉพาะเราเตอร์ที่ติดตั้งมานานและไม่มีการอัปเดตเฟิร์มแวร์เพื่ออุดช่องโหว่เรื่องความปลอดภัย ทำให้คนร้ายแฮ็กอุปกรณ์ทุกชิ้นที่เชื่อมต่อได้ไม่ยาก

นอกจากนี้พบด้วยว่า อุปกรณ์ IoT จำนวนมากถูกติดตั้งโดยใช้รหัสผ่านที่มาจากโรงงาน หรือใช้ช่องทางการเชื่อมต่ออินเทอร์เน็ตที่ไม่มีการเข้ารหัสลับข้อมูลที่รับส่ง ทำให้ผู้ประสงค์ร้ายสามารถดักรับรหัสผ่านได้

ทั้งนี้ การแฮ็กโดยทั่วไปมีเป้าหมายสองกลุ่ม หนึ่งคือกลุ่มบุคคลสำคัญ มีชื่อเสียง หรือฐานะดี เพื่อล้วงความลับหรือเจาะข้อมูลลับต่างๆ หรือขโมยทรัพย์สินทางออนไลน์ อย่างเช่นกรณีวิกิลีกส์เผยแพร่ข้อมูลว่าหน่วยสืบราชการลับบางประเทศบันทึกเสียงสนทนาภายในบ้านของเหยื่อผ่านสมาร์ตทีวีที่ปิดอยู่ และจริงๆ แล้วในกรณี BabyCam คนร้ายสามารถบันทึกวิดีโอได้ด้วย

เนื่องจากการแฮ็กแต่ละครั้งต้องใช้ทรัพยากรและเวลา คนร้ายจะไม่เสียเวลาทำแบบนี้กับประชาชนทั่วไป เพราะประโยชน์ตอบแทนไม่คุ้มค่า แต่คนทั่วไปก็เป็นเป้าหมายกลุ่มที่สอง เพราะระบบรักษาความปลอดภัยมีช่องโหว่ โดยหลักแล้วคนร้ายจะแฮ็กอุปกรณ์อะไรก็ได้ชิ้นแรก แล้วใช้เป็นเกตเวย์ในการแฮ็กอุปกรณ์ที่เหลือทั้งหมดในบ้าน แล้วสร้างทราฟฟิกไปโจมตีเซิร์ฟเวอร์หรือเว็บไซต์เป้าหมายอีกชั้นหนึ่ง ซึ่งเรียกการโจมตีแบบนี้ว่า ดีดอส (Distributed Denial of Service - DDos) ทำให้สามารถโจมตีเป้าหมายพร้อมๆ กันจากอุปกรณ์ทั่วโลกหลายล้านชิ้น ยากต่อการหาต้นตอการโจมตี

คำถามคือ เมื่อเกิดการโจมตีทางไซเบอร์ในลักษณะเช่นนี้ แล้วใครต้องเป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้น

ในอดีตเวลาเครื่องคอมพิวเตอร์ติดไวรัสเราจะโทษผู้ใช้งาน ไม่มีใครกล่าวโทษผู้ผลิตคอมพิวเตอร์หรือกล่าวโทษเจ้าของระบบปฏิบัติการ เพราะความเสี่ยงในการติดไวรัสมักจะมาจากพฤติกรรมการใช้งาน ผู้บริโภคต้องติดตั้งโปรแกรมตรวจฆ่าไวรัสเอง แต่ในกรณีเครื่องทำกาแฟอัจฉริยะ หรือเครื่องใช้ไฟฟ้าอื่นๆ ผู้บริโภคก็เพียงแต่ใช้งานตามคู่มือการใช้งานตามปกติ หรือกรณีรถยนต์อัจฉริยะไร้คนขับ ผู้โดยสารก็เพียงนั่งเฉยๆ ไม่ได้ควบคุมรถ หรือมีพฤติกรรมแผลงๆ แต่อย่างใด จะให้เป็นผู้แบกรับความผิดแบบเดิมๆ คงไม่เป็นธรรม

ดังนั้น ในโลกยุค IoT อุปกรณ์ทุกชิ้นต้องถูกฝังระบบรักษาความปลอดภัยตั้งแต่ขั้นตอน การออกแบบผลิตภัณฑ์ (Security by Design) และกรณีที่พบช่องโหว่ต้องมีการออกแพตช์ (Patch) หรืออัปเดตเฟิร์มแวร์อัตโนมัติ เพราะในอนาคตแต่ละบ้านอาจมีอุปกรณ์ไอโอทีนับร้อยชิ้น การจะให้ผู้บริโภคคอยอัปเดตเฟิร์มแวร์เองทุกชิ้นในแต่ละเดือนก็คงไม่เหลือเวลาไปทำอะไรอื่นอีก นอกจากนี้อาจต้องมีการทำประกันภัยที่เกิดจากการใช้งานอุปกรณ์ต่างๆ อีกด้วย และต้องวางแนวทางในการกำหนดผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้น เพราะอุปกรณ์ชิ้นหนึ่งเกี่ยวข้องกับหลายบริษัท เช่น ผู้ผลิตชิพ ผู้ผลิตตัวอุปกรณ์ ผู้ผลิตซอฟต์แวร์หรือแอปพลิเคชัน ผู้รับผิดชอบระบบสื่อสาร และผู้เป็นเจ้าของแบรนด์ เป็นต้น

นอกจากเรื่องการป้องกันการโจมตีทางไซเบอร์แล้ว ประเด็นที่ต้องคุ้มครองผู้บริโภคยังมีเรื่องการรักษาข้อมูลส่วนบุคคล เพราะปัจจุบันมีแนวโน้มอย่างชัดเจนว่า ภาคธุรกิจจะใช้การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analysis) เพื่อตอบสนองความต้องการของผู้บริโภค ทำให้สามารถวิเคราะห์โพรไฟล์ของผู้บริโภค

แต่ละคนว่านิยมบริโภคอะไร หรือมีความต้องการจับจ่ายใช้สอยในเรื่องอะไรบ้าง จนบางครั้งรู้ดีกว่าตัวผู้บริโภคคนนั้นเสียอีก

เคยมีกรณีตัวอย่างเกิดขึ้นที่กรุงลอนดอน ประเทศอังกฤษ ซึ่งมีการติดตั้ง *"ถังขยะอัจฉริยะ"* ในย่านการเงิน แล้วใช้ข้อมูลจากโทรศัพท์เคลื่อนที่มาประมวลเพื่อแสดงโฆษณาที่ถูกต้องตรงใจให้กับคนที่สัญจรไปมาผ่านถังขยะได้เห็น รายงานของผู้ผลิตเทคโนโลยีดังกล่าวระบุว่า มีการเก็บข้อมูลจากโทรศัพท์มากกว่า 4 ล้านเครื่อง อย่างไรก็ดี เมื่อผู้คนชาวลอนดอนทราบเรื่องนี้ ระบบดังกล่าวจึงถูกถอดออก

ในส่วนประเด็นความเป็นส่วนตัว ต่อไปเราอาจจะพบเห็นโดรนบินเต็มท้องฟ้าหากไม่มีการกำกับดูแล โดรนจะสามารถรุกล้ำความเป็นส่วนตัวของแต่ละบ้านได้ไม่ยาก และอุปกรณ์เซ็นเซอร์ต่างๆ ในบ้านที่เราติดตั้งเพื่อดูแลความปลอดภัย ก็ใช้เป็นเครื่องมือระบุว่ามีใครอยู่ในห้องไหนหรือบ้านไหนหรือไม่ กำลังนั่ง ยืน หรือนอนอยู่ หรือแม้แต่มิเตอร์อัจฉริยะก็อาจบอกได้ว่าในบ้านมีคนอยู่หรือไม่ ส่วนอุปกรณ์พกพาติดตัว (Wearable Device) ก็ใช้ระบุตำแหน่งผู้ใช้งานได้ คนร้ายจึงสามารถใช้ข้อมูลเหล่านี้ติดตามเรา หรือใช้ตัดสินใจบุกเข้าบ้านเราเวลาปลอดคนก็ได้

ตัวอย่างเหล่านี้ล้วนเป็นความเสี่ยงที่จะเกิดขึ้นในยุค IoT ที่ทุกฝ่ายในสังคมต้องเตรียมการรับมืออย่างรอบคอบและรัดกุม

อยู่อย่างไรให้ปลอดภัยในยุค IoT

บางท่านอาจคิดว่าอาวุธไซเบอร์ที่ทรงอานุภาพจะทำให้เราเป็นฝ่ายชนะ แต่แท้จริงแล้วภัยของการคุกคามทางไซเบอร์คือการถูกโจมตี ซึ่งสามารถเกิดขึ้นเวลาใดก็ได้ การพัฒนาระบบรับมือการโจมตีจึงถือเป็นสิ่งสำคัญ ทั้งนี้ ในการปกป้องโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งรัฐมิได้ควบคุมด้วยตนเอง เป็นเรื่องที่รัฐต้องขบคิดให้ชัดเจนว่าจะเลือกนโยบายเสรีให้ต่างคนต่างรับผิดชอบตนเอง หรือต้องมีนโยบายกำกับดูแล (Market forces vs Regulation) เนื่องจากโครงสร้างพื้นฐานในยุคดิจิทัลล้วนเชื่อมต่อออนไลน์และเสี่ยงต่อภัยคุกคาม เช่น ด้านการผลิตพลังงานหรือกระแสไฟฟ้า ด้านการขนส่งทั้งทางบก ทางน้ำ ทางอากาศ ด้านการเงินการธนาคาร ด้านโรงพยาบาลหรือบริการทางการแพทย์ ด้านการสื่อสาร หรือกระทั่งตลาดหลักทรัพย์ ซึ่งล้วนแล้วแต่มีความสำคัญอย่างยิ่งยวด แต่การพัฒนาระบบรับมือภัยคุกคามนั้นไม่อาจปฏิเสธได้ว่าต้องมีต้นทุน และในบางครั้งเอกชนก็เน้นการควบคุมหรือลดต้นทุนของตนเอง แต่ผลกระทบจากภัยคุกคามต่อสังคมนั้นมีมูลค่าสูงมากกว่าหลายเท่าตัว เช่น หากระบบไฟฟ้าของประเทศล่ม ก็เท่ากับเศรษฐกิจหยุดชะงัก จึงจำเป็นต้องมีการกำกับดูแล โดยการออก Smart Regulation ตามด้วยการตรวจสอบการปฏิบัติตามกติกา การทดสอบการโจมตีทางไซเบอร์ และการปรับปรุงพัฒนาระบบ ตลอดจนมีความยืดหยุ่นในการรับมือ กล่าวคือเมื่อมีผู้บุกรุกเข้ามาในระบบ จะตีวงจำกัดขอบเขตของปฏิบัติการโจมตีได้ในระดับใด และหากเกิดผลกระทบแล้วจะฟื้นฟูระบบให้กลับสู่ปกติโดยเร็วได้อย่างไร เช่น การกู้ระบบไฟฟ้าของประเทศให้กลับคืนมา

ในเวลานับเป็นชั่วโมง ไม่ใช่เป็นวันหรือเป็นสัปดาห์ หมายความว่าแต่ละระบบต้องมีข้อมูลสำรองและระบบสำรอง และต้องมีการฝึกซ้อมการกู้ระบบอย่างสม่ำเสมอ ไม่ต่างจากการซ้อมรับอัคคีภัยในอาคาร

ขณะที่ในส่วนของอุปกรณ์ IoT ก็ควรมีการกำหนดมาตรฐานแนวทางการพัฒนาอุปกรณ์และการรับรองมาตรฐานอุปกรณ์ให้มีความมั่นคงปลอดภัยที่ดีพอ และกำหนดแนวทางความรับผิดชอบหากเกิดปัญหาจากการใช้งานอุปกรณ์เหล่านี้ รวมทั้งควรมีการบูรณาการอำนาจหน้าที่ระหว่างหน่วยงานภาครัฐกันเองหรือแบ่งขอบเขตงานให้ชัดเจน ตัวอย่างเช่น การนำเข้ารถแทรกเตอร์ที่ใช้เทคโนโลยี IoT จะต้องขออนุญาตนำเข้าจากผู้ใด เข้าหลักเกณฑ์การนำเข้าเครื่องวิทยุคมนาคมของ กสทช. หรือไม่ ซึ่งจะเห็นได้ว่ากฎเกณฑ์ที่มีอยู่ในปัจจุบันไม่รองรับเทคโนโลยีที่เกิดขึ้นใหม่นี้เสียแล้ว

นอกจากนี้ ต่อไปในอนาคต อุปกรณ์ IoT จะสร้างและเก็บข้อมูลจำนวนมากอยู่ตลอดเวลา ประเด็นสำคัญจึงต้องมีการคุ้มครองข้อมูลส่วนบุคคล ห้ามขายต่อข้อมูล และห้ามนำข้อมูลไปใช้ผิดวัตถุประสงค์ โดยกำหนดมาตรฐานขั้นต่ำในการดูแลและใช้ประโยชน์ข้อมูลส่วนบุคคล และยึดหลักการพื้นฐานว่า การใช้ประโยชน์อื่นใดจากข้อมูล ต้องขอความยินยอมจากเจ้าของข้อมูลเสมอ และเจ้าของข้อมูลมีสิทธิร้องขอให้ลบข้อมูลของตนเองได้ โดยภาคอุตสาหกรรมต้องใช้ข้อมูลอย่างมีความรับผิดชอบและมีจริยธรรมเพื่อให้เกิดนวัตกรรมที่เหมาะสม

ที่กล่าวมาทั้งหมดนี้ ไม่ได้หมายความว่าผู้บริโภคไม่ต้องรับผิดชอบอะไร เพราะต่อให้ระบบรักษาความปลอดภัยดีเพียงใด หรือมีการซื้อซอฟต์แวร์รักษาความปลอดภัยมาใช้งาน แต่หากเราเป็นผู้มอบกุญแจหรือเป็นผู้ไขประตูให้คนร้ายเข้ามาในระบบเสียเอง ระบบรักษาความปลอดภัยทั้งหลายก็ช่วยอะไรไม่ได้ ดังนั้นผู้บริโภคย่อมต้องรับผิดชอบตัวเองด้วย สิ่งที่ผู้บริโภคต้องตระหนักคือการสร้างนิสัยในการใช้งานอย่างปลอดภัยและไม่เปิดเผยข้อมูลสำคัญแก่ใครๆ ซึ่งในปัจจุบันคนร้ายนิยมใช้เทคนิค Social Engineering มากกว่าการแฮ็กข้อมูล เพราะการหลอกให้เราเปิดเผยข้อมูลนั้น ใช้หลักจิตวิทยาในการหลอกลวงโดยไม่ต้องเชี่ยวชาญด้านเทคนิคเหมือนการแฮ็ก การส่งอีเมลหลอกลวง การสร้างหน้าเว็บปลอม การสวมรอยเป็นคนที่เรารู้จัก การสร้างข้อมูลข่าวสารเท็จ หรือแม้แต่การโทรมาหลอกแบบแก๊งคอลล์เซ็นเตอร์ คือรูปแบบต่างๆ ที่จะหลอกลวงให้เราเปิดเผยข้อมูลออกไปด้วยตัวเราเอง กรณีการเจาะภาพลับของดาราฮอลลีวู้ดที่เก็บบนระบบคลาวด์นั้น ส่วนใหญ่เกิดจาก Social Engineering ไม่ใช่การแฮ็กขั้นเทพแต่อย่างใด หรือตัวอย่างการรั่วไหลของข้อมูลสำคัญอย่างง่ายๆ ที่คนทั่วไปไม่ทันระวัง เช่น การเปิดเผยวันเดือนปีเกิดในสื่อสังคมออนไลน์ ซึ่งจะพบว่าข้อมูลนี้เป็นข้อมูลที่ทางเจ้าหน้าที่ธนาคารมักใช้เป็นคำถามเพื่อพิสูจน์ตัวตนของเราเวลาที่ติดต่อกับธนาคารทางโทรศัพท์

ในยุคที่ IoT กำลังมีบทบาทมากขึ้น และไม่มีอะไรมาฉุดรั้งเทคโนโลยีนี้ได้ จึงจำเป็นต้องสร้างความตระหนักและความรู้ความเข้าใจแก่สังคมอย่างจริงจัง โดยทุกฝ่ายต้องร่วมรับผิดชอบและร่วมมือกันเพื่อให้การใช้งานเกิดความปลอดภัยมากที่สุด เพราะการไม่มีนโยบายและมาตรการรับมือในเรื่องเหล่านี้สุดท้าย IoT ก็อาจนำพาหายนะมาสู่สังคมและประเทศชาติได้ด้วยเช่นกัน