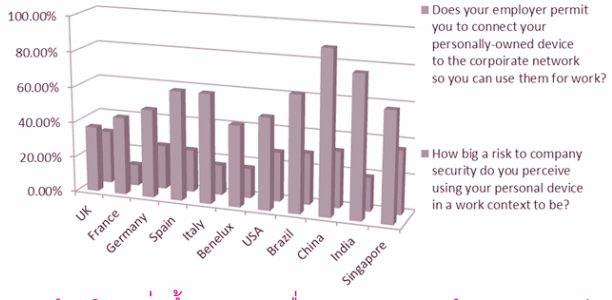
วางแผนรับมือ BYOD โอกาสหรือความเสี่ยง

วิษณ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ในปัจจุบันเราคงเลี่ยงไม่ได้ที่จะยอมรับโดยปริยายว่าเทคโนโลยีอุปกรณ์พกพาไร้สายพวก Mobile Device Handheld ทั้งหลายนั้น ได้เข้ามามีอิทธิพลต่อการดำเนินชีวิตประจำวันของเราๆ ท่านๆ เป็นอย่างยิ่ง ทั้งที่อยู่ในรูปแบบของโทรศัพท์มือถือ Smart Phone Tablet หรือแม้กระทั่งที่กำลังได้รับความนิยมแบบพวกที่เป็น Hybrid ซึ่งสามารถเปลี่ยนรูปได้ เช่นจาก Tablet สไลด์ หรือประกอบเข้ากับแผ่น Keyboard กลายเป็น Notebook และที่อยู่ในรูปแบบอื่นๆ ด้วยเหตุผลหลากหลายประการทั้งที่ใช้เป็นอุปกรณ์สำหรับติดต่อสื่อสาร เข้าถึงและสืบค้นข้อมูล จัดการงานด้านเอกสาร การทำธุรกรรม ฯลฯ ทำให้อุปกรณ์ดังกล่าวกลายเป็นของจำเป็นที่ต้องพกพาติดตัวไปทุกที่ และสามารถนำขึ้นมาใช้งานได้อย่างสะดวกรวดเร็วไม่เว้นแม้แต่ในสำนักงานขององค์การ

นอกเหนือจากนั้นส่วนสำคัญที่สนับสนุนให้เกิดการใช้งานอย่างแพร่หลายนั่นคือการพัฒนา Mobile Application ที่ทำงานบนอุปกรณ์ดังกล่าว หรือทำให้อุปกรณ์เหล่านั้นมีความสามารถและศักยภาพในการสนับสนุนการทำงานของเราได้อย่างยอดเยี่ยม การพัฒนา Mobile Application มีการเติบโตแบบก้าวกระโดด เนื่องจาก



จำนวนผู้บริโภคเพิ่มขึ้นอย่างต่อเนื่องบรรดา บริษัทผู้พัฒนาซอฟต์แวร์จึงพากันก้าวเข้าสู่ตลาด Mobile Application เกิดการพัฒนานวัตกรรมรูปแบบวิธีการ Platform ใหม่ๆ ที่มีความสามารถสูงสะดวกต่อการใช้งาน อาทิ กิจกรรมบางอย่าง ซึ่งแต่ก่อนเคยแต่พิมพ์บนแป้นพิมพ์แต่เดี๋ยวนี้ใช้วิธีสัมผัสที่หน้าจอ เลื่อน ลาก ย่อขยาย ดูทันสมัยและใช้งานง่ายขึ้น

ด้วยการมาถึงของเทคโนโลยีดังที่กล่าวข้างต้น ซึ่งมีการขยายตัวอย่างรวดเร็วจากที่เคยใช้เป็นอุปกรณ์สำหรับกิจกรรมส่วนตัว เพื่อติดต่อสื่อสาร หรือเพื่อความบันเทิง ด้วยการพัฒนาและเปลี่ยนแปลงรูปแบบของ Application ที่เกี่ยวข้องกับการทำงาน จนกระทั่งสามารถใช้บนอุปกรณ์พกพาเหล่านั้นได้อย่างสะดวก ทำให้มีหลายต่อหลายคนนำเอาอุปกรณ์ Mobile Device มาใช้ในการปฏิบัติงานในสำนักงาน ซึ่งถ้าพิจารณากันอย่างจริงจัง องค์การคงสามารถประเมินผลกระทบที่จะตามมาได้ทั้งในแง่บวก อาทิ ประสิทธิภาพในการประสานการทำงานที่ดีขึ้น ภาพลักษณ์ขององค์การที่ทันสมัย เป็นโอกาสในการพัฒนา Application ใหม่ๆ เพิ่มช่องทางการทำงาน หรือให้บริการผู้บริหารและเจ้าหน้าที่สามารถเข้าถึงข้อมูลได้อย่างรวดเร็วทุกที่ทุกเวลา เป็นต้น

แต่ในแง่ลบนั้นจะเป็นประเด็นของความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานที่หละหลวมของพนักงาน หรือเจ้าหน้าที่ที่เป็นเจ้าของอุปกรณ์ ช่องโหว่ของเครือข่ายสารสนเทศ การถูกโจมตีทางสารสนเทศ การนำเข้า หรือส่งออกข้อมูลสำคัญ การรั่วไหลของข้อมูล เหล่านี้คือสิ่งที่ควรคำนึงถึง หากจะมีการปรับวัฒนธรรมองค์การในเรื่องการใช้งาน Mobile Device ของผู้บริหารและพนักงานเพื่อการทำงานในองค์การ

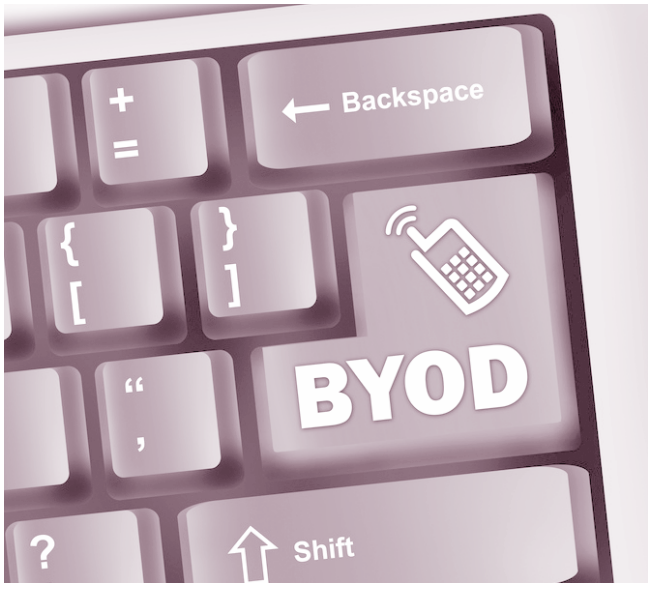
ทำความรู้จักกับ BYOD

BYOD มาจาก Bring Your Own Device แปลตรงตัวก็หมายถึง "นำอุปกรณ์ของคุณมาเอง" เป็นการอธิบายถึงแนวโน้มทางเทคโนโลยี ที่เจ้าหน้าที่ หรือพนักงานขององค์การนำอุปกรณ์พกพาของตนเองมาที่ที่ทำงานและใช้อุปกรณ์ดังกล่าวเพื่อเข้าถึงทรัพยากรที่มีการควบคุมการเข้าถึงขององค์การ อาทิ e-Mail ขององค์การ File Server (เครื่องแม่ข่ายที่ใช้จัดเก็บข้อมูลขององค์การ) รวมถึงฐานข้อมูล BYOD มีความสำคัญมากขึ้นเรื่อยๆ ต่อโลกของธุรกิจในปัจจุบัน ประมาณ 90% ของพนักงาน ใช้อุปกรณ์ของตนเองอยู่แล้วในที่ทำงาน แม้ว่าจะมีการใช้งานอย่างจำกัดก็ตาม ซึ่งส่วนใหญ่องค์การธุรกิจต่างๆ ไม่สามารถห้ามแนวโน้มดังกล่าวได้

บางคนเชื่อว่า BYOD อาจช่วยให้พนักงานมีผลิตภาพในการทำงานมากขึ้น แต่ถ้าหากปล่อยไว้โดยไม่บริหารจัดการวิธีปฏิบัติงานดังกล่าวอาจนำไปสู่การรั่วไหลของข้อมูล ตัวอย่างเช่น ถ้าพนักงานคนหนึ่งใช้ Smart Phone เพื่อเข้าถึงเครือข่ายขององค์การและต่อมาอุปกรณ์ดังกล่าวสูญหาย ข้อมูลที่เป็นความลับขององค์การที่เก็บอยู่ในอุปกรณ์ดังกล่าวก็อาจจะถูกอ่าน หรือนำไปใช้โดยบุคคลที่ไม่พึงประสงค์ ซึ่งประเด็นปัญหาที่สำคัญประการหนึ่งที่อาจดำเนินการได้ยากในการบริหารจัดการ BYOD นั่นก็คือ การติดตามและควบคุมการเข้าถึงเครือข่ายขององค์การและเครือข่ายส่วนตัว

สถานการณ์ของ BYOD

หลังจากที่ทราบแล้วว่า BYOD คืออะไร คราวนี้เรามามองในมุมที่เป็นภาพรวมของสถานการณ์ BYOD โดย Fortinet องค์การชั้นนำด้าน Solution ประสิทธิภาพสูงสำหรับความปลอดภัยเครือข่ายได้ประกาศผลการสำรวจทั่วโลกที่เผยให้เห็นว่าผู้ที่ใช้อุปกรณ์ของตนเองในที่ทำงาน หรือเพื่อการทำงาน นำมาซึ่งประเด็นท้าทายของระบบเทคโนโลยี สารสนเทศองค์การ โดยที่พนักงานให้ความสำคัญด้านความปลอดภัยของข้อมูลองค์การในระดับที่ค่อนข้างต่ำ แต่ยังคาดหวังที่จะใช้อุปกรณ์ของตัวเอง ในการทำงานต่อไป และพบว่าส่วนใหญ่พนักงานชาวเอเชียมีความรู้สึกขัดขืนกับนโยบาย การรักษาความปลอดภัยขององค์การที่ห้ามใช้อุปกรณ์ส่วนบุคคลของพวกเขาในที่ทำงาน หรือเพื่อการทำงาน ทำให้เรามองเห็นถึงความจำเป็นเร่งด่วนที่องค์การควรจะพัฒนากลยุทธ์ การรักษาความปลอดภัย เพื่อรองรับการใช้อุปกรณ์ของตนเองในที่ทำงาน หรือเพื่อการทำงานของพนักงาน จากการสำรวจภูมิภาค 15 เขตทั่วโลก ซึ่งได้แก่ อินเดีย เกาหลี จีน ไต้หวัน ฮ่องกง สิงคโปร์ ญี่ปุ่น สหรัฐอเมริกา สหราชอาณาจักร ฝรั่งเศส เยอรมนี อิตาลี สเปน โปแลนด์และสหรัฐอาหรับเอมิเรตส์



ในช่วงพฤษภาคม - มิถุนายน พ.ศ.2555 ที่ผ่านมาได้มีการสอบถามพนักงานที่ใช้อุปกรณ์ของตนเองเพื่อทำงานมากกว่า 3,800 คน (โดยมี 1,443 เป็นผู้ตอบในเอเชีย) อายุระหว่าง 21-31 ถึงมุมมองของพวกเขาในด้าน BYOD และผลกระทบต่อสภาพแวดล้อมการทำงาน วิธีการรักษาความปลอดภัยส่วนบุคคลของตนเอง รวมถึงทัศนคติด้านเทคโนโลยีสารสนเทศขององค์การ

ในกลุ่มของประชากรที่ได้ทำการสำรวจแสดงให้เห็นว่า BYOD จะเป็นที่นิยมต่อไป กว่าสามในสี่ (85%) ของผู้ตอบแบบสอบถามในเอเชียตอบว่า ใช้เป็นประจำอยู่แล้ว จากมุมมองของผู้ใช้งานเห็นว่า BYOD เป็นที่นิยมเนื่องจากผู้ใช้งานสามารถเข้าถึง Application ที่ตนเองเคยชินและชื่นชอบได้ โดยเฉพาะอย่างยิ่ง Social Media ต่างๆ การสื่อสารเฉพาะกลุ่ม (Personal communications)

ทั้งนี้ 59% ของผู้ตอบแบบสอบถามในเอเชียยอมรับว่าการสื่อสารส่วนบุคคลที่มีอิทธิพลมาก ไม่มีวันไหนที่พวกเขาไม่มีการเข้าถึงเครือข่ายทางสังคมและ 67% จะหยุดส่ง SMS ได้ไม่ถึง 1 วันและเมื่อเปรียบเทียบกับค่าเฉลี่ยทั่วโลกแล้ว จะเห็นว่าพนักงานในเอเชียให้ความสำคัญกับอุปกรณ์พกพาของพวกเขาอย่างมีนัยสำคัญสูงกว่าถึง 35% และให้ความสำคัญกับเครือข่ายทางสังคมและ SMS สูงกว่าถึง 47%

ความเข้าใจที่หละหลวมด้านความเสี่ยงทางธุรกิจอาจเกิดความขัดขืนต่อนโยบายองค์การได้ จากกลุ่มคนใช้งาน BYOD รุ่นแรกๆ ในโลกนั้นเข้าใจว่า การนำอุปกรณ์ส่วนตัวมาใช้เพื่อทำงานอาจจะนำพาซึ่งความเสี่ยงให้กับองค์การของพวกเขา ทั้งนี้ร้อยละสี่สิบสองของกลุ่มตัวอย่างการสำรวจในเอเชียเชื่อว่าสามารถก่อให้เกิดปัญหาข้อมูลสูญหายและความเสี่ยงต่อภัยคุกคามทางสารสนเทศที่เป็นอันตรายได้จริง แต่ถึงแม้ว่าจะเห็นความเสี่ยงและนโยบายขององค์กรด้านเทคโนโลยีสารสนเทศอยู่ ก็ไม่สามารถหยุดการนำอุปกรณ์ส่วนตัวมาใช้ได้ ยิ่งไปกว่านั้น เกือบครึ่งหนึ่งของผู้ตอบแบบสอบถามในเอเชีย (47%) ยอมรับว่าพวกเขาได้ขัดขืนหรือจะขัดขืนต่อนโยบายของบริษัทที่ห้ามการใช้อุปกรณ์ส่วนตัวเพื่อการทำงานด้วยซ้ำ

อ่านต่อฉบับหน้า