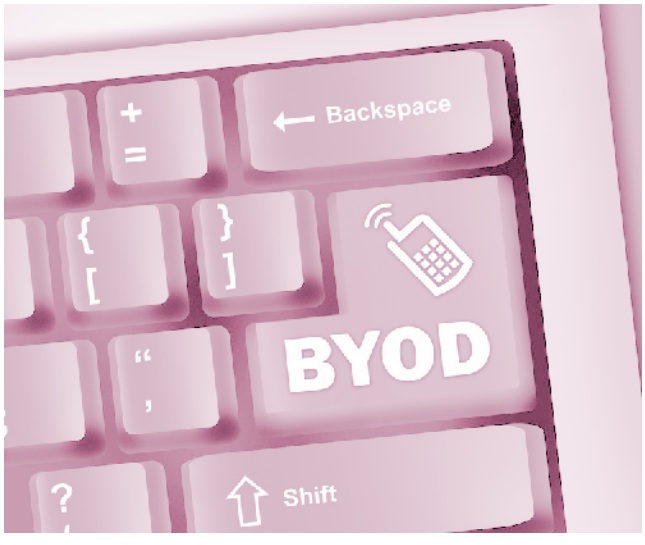
ต่อ จากฉบับที่แล้ว

วางแผนรับมือ BYOD โอกาสหรือความเสี่ยง

จบ

วิษณุศาสน์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์



7 • จัดทำข้อมูลบัญชีอุปกรณ์ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตให้เข้าถึงเครือข่ายองค์การ

เราคงไม่สามารถสร้างและใช้นโยบายการเข้าถึงเครือข่ายได้ในอากาศที่ว่างเปล่าซึ่งรวมถึงการที่จะตั้งค่าการควบคุมการบังคับใช้นโยบายการเข้าถึงเครือข่ายในอุปกรณ์และระบบสารสนเทศที่เกี่ยวข้องได้ก่อนที่รับทราบสถานการณ์ปัจจุบันของอุปกรณ์ต่างๆ ที่อยู่ในระบบ การดำเนินการเพื่อตรวจสอบความเป็นจริงในปัจจุบันของอุปกรณ์ที่เกี่ยวข้องทั้งหมดทั้งในส่วนอุปกรณ์พกพาที่ได้รับและไม่ได้รับอนุญาต และอุปกรณ์เครือข่ายและอุปกรณ์ทางสารสนเทศอื่นๆ ซึ่งสำหรับองค์การที่มีการจัดวางอุปกรณ์เครือข่ายและอื่นๆ ที่มีความซับซ้อนอย่างเช่น โรงพยาบาล มหาวิทยาลัย อาจใช้เวลาเป็นเดือนหรือเป็นปี แต่ข้อมูลเหล่านี้สามารถสร้างให้เห็นภาพจริงที่เกิดขึ้นได้อย่างสมบูรณ์เมื่อมีการเชื่อมต่อใช้งานอุปกรณ์พกพาและจำเป็นอย่างยิ่งต่อการบังคับใช้นโยบาย BYOD และควรมีการปรับปรุงบัญชีดังกล่าวให้มีความทันสมัย (เป็นปัจจุบัน) อย่างสม่ำเสมอ

8. จัดทำข้อมูลบัญชีพนักงานที่ได้รับอนุญาตและไม่ได้รับอนุญาตให้เข้าถึงเครือข่ายองค์การในแต่ละระดับ

นอกจากการจัดทำข้อมูลบัญชีอุปกรณ์แล้วสิ่งที่จำเป็นอย่างยิ่งเพื่อเชื่อมโยงข้อมูลอุปกรณ์การตัวพนักงานผู้ใช้ได้อย่างเป็นระบบนั่นคือ การจัดทำบัญชีผู้ใช้ทั้งที่ได้รับและไม่ได้รับอนุญาตให้เข้าถึงเครือข่ายองค์การในแต่ละดับตามภารกิจหรือหน้าที่รับผิดชอบ ซึ่งข้อมูลดังกล่าวเมื่อมีการใช้งานจริงอาจทำให้ได้ทราบว่าอาจมีพนักงานที่ใช้อุปกรณ์ที่ไม่ได้รับอนุญาตให้ใช้ หรือใช้อุปกรณ์ของพนักงานท่านอื่นๆ ในการเข้าถึงเครือข่าย หรือข้อมูล ขั้นตอนที่ 7 และ 8 จะทำให้เราได้มุมมองที่สมบูรณ์ของสภาพแวดล้อม BYOD ที่เป็นปัจจุบันและที่สำคัญก็ควรมีการปรับปรุงบัญชีดังกล่าวให้มีความทันสมัย (เป็นปัจจุบัน) อย่างสม่ำเสมอเช่นกัน

9. ควบคุมการเข้าถึงบนพื้นฐานของความจำเป็นในการใช้งาน

เมื่อเราได้สร้างนโยบายการเข้าถึงเครือข่ายและได้มีการศึกษาเกี่ยวกับพฤติกรรมของพนักงานความเห็นที่มีต่อนโยบาย BYOD สามารถมองเห็นการถึงและใช้งานของอุปกรณ์ที่มีการจัดทำบัญชีข้อมูลและผู้ใช้งานที่เป็นปัจจุบันบนเครือข่ายขององค์การเป็นที่เรียบร้อยแล้ว ตอนนี้ก็ถึงเวลาที่จะเริ่มต้นการบังคับใช้การเข้าถึงเครือข่ายด้วยนโยบายการควบคุมที่ว่าด้วย ใคร ทำอะไร ที่ไหนและเมื่อไหร่ บนพื้นฐานของการจำกัดสิทธิ์การเข้าถึงตามความจำเป็นในการใช้งานเป็นสำคัญ ทั้งนี้การวางแนวนโยบายดังกล่าวต้องมีการเชื่อมโยงความสัมพันธ์ของพนักงาน อุปกรณ์ และสิทธิได้อย่างเหมาะสม ซึ่งสำหรับใน Solution ด้านความปลอดภัยบางระบบสามารถกำหนดให้เป็นข้อมูลพื้นฐาน โดยสามารถที่จะทำการจำกัดสิทธิอัตโนมัติได้ในกรณีที่มีการใช้งานที่นอกเหนือสิทธิ์ที่ได้รับ หรือฝ่าฝืน โดยการใช้งานอุปกรณ์ที่ไม่ได้รับอนุญาต

10. การประเมินความเสี่ยงอย่างต่อเนื่องและการปรับปรุงนโยบายอย่างเหมาะสม

เราคงไม่สามารถสร้างนโยบาย BYOD ขององค์โดยอาศัยข้อมูลภาพรวมของความเสี่ยงที่ส่งผลกระทบต่อความปลอดภัยทางสารสนเทศและความต้องการของพนักงานเพียงช่วงเวลาหนึ่ง แต่จำเป็นต้องดำเนินการปรับปรุงอย่างต่อเนื่อง การตรวจสอบช่องโหว่และความต้องการที่เปลี่ยนแปลงของพนักงานอาจส่งผลให้เกิดการปรับเปลี่ยนนโยบายเพื่อตอบสนองความต้องการที่เปลี่ยนแปลงไปของพนักงานรวมทั้งภัยคุกคามความปลอดภัยขององค์การ การพัฒนา

แบบก้าวกระโดดของเทคโนโลยี รูปแบบการบังคับใช้นโยบายจึงจำเป็นต้องมีความยืดหยุ่นและเอื้อประโยชน์ทั้งแก่พนักงานและองค์การอย่างเหมาะสมและยอมรับได้

นโยบายถือเป็นสิ่งที่สำคัญกว่าเทคโนโลยีการรักษาความปลอดภัย เนื่องจากเป็นการสื่อสารการทำความเข้าใจสร้างข้อตกลงร่วมกัน ระหว่างองค์การกับพนักงาน ซึ่งเมื่อได้ข้อสรุปที่เหมาะสมจึงนำมาประยุกต์ให้เข้ากับเทคโนโลยีที่องค์การมี หรือพอที่จะจัดหาได้ เนื่องจากเทคโนโลยีสารสนเทศเป็นแค่เครื่องมือที่นำมาประยุกต์ใช้งานเพื่อสนับสนุนให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพเพียงเท่านั้น ซึ่งไม่จำเป็นต้องดีที่สุดแต่ต้องเหมาะสมกับองค์การที่สุดเป็นสำคัญ

แม้ว่าแนวคิดในเรื่อง BYOD ยังคงต้องการการพัฒนาอีกพอสมควร แต่ผู้บริหารองค์การจำนวนหนึ่งก็พยายามเดินหน้านโยบายที่เกี่ยวข้องอย่างต่อเนื่อง ด้วยเหตุผลที่หลากหลาย อาทิ ในหลายองค์การสามารถคำนวณความคุ้มค่าในการลงทุนกับระบบบริหารจัดการอุปกรณ์ส่วนตัวของบุคลากรได้ค่อนข้างชัดเจน โดยมีความมั่นใจพอสมควรว่าในระยะยาวจะสามารถประหยัดการลงทุนในอุปกรณ์และค่าใช้งานในการดูแลรวมถึงบริการซ่อมบำรุงต่างๆ ได้

สำหรับองค์การที่แสวงหานวัตกรรมและเทคโนโลยีใหม่ในการสนับสนุนการดำเนินงานมีแนวโน้มที่จะมอง BYOD ไปในทางบวก ทั้งนี้ เพราะการขยายกรอบการควบคุมออกไม่ให้บีบรัดมากจนเกินไปย่อมนำไปสู่อิสรภาพทางความคิด การได้รับประสบการณ์ในการทำงานใหม่และความคิดสร้างสรรค์ที่มากขึ้นของพนักงาน รวมทั้งการให้อิสรภาพในการเลือกใช้อุปกรณ์ซึ่งมีความเป็นส่วนตัวสูง (Style or Character) จะมีผลต่อการดึงดูดให้บุคลากรรุ่นใหม่ ระดับคุณภาพสนใจเข้าร่วมงานกับองค์การ อีกทั้งยังอาจช่วยให้พวกเขาทำงานอย่างมีความสุขและอยู่กับองค์การได้นานขึ้น

ผู้บริหารรุ่นใหม่มองเห็นขีดความสามารถของ Mobile Application บนระบบปฏิบัติการ Android และ iOS ว่า อาจจะเป็นปัจจัยสำคัญในการเพิ่ม Productivity ให้กับองค์การทั้งในระดับหน่วยงานและพนักงาน เพราะความหลากหลายของ Application ที่ราคาไม่สูงนักเหล่านี้จะส่งผลให้พนักงานได้ใช้เครื่องมือที่ถนัดและใช้เท่าที่จำเป็นไม่ต้องได้รับผลกระทบจากการที่ต้องใช้ระบบงานที่ซ้ำซ้อนเกินไปอย่างที่ผ่านมา

และสำหรับองค์การขนาดกลางและขนาดย่อม หรือ SMEs ซึ่งมีจำนวนอุปกรณ์พกพาไม่มากนัก แม้จะไม่ได้ประโยชน์ในแง่ของการลดเงินลงทุนแต่องค์การเหล่านี้จะมองว่าสำหรับจำนวนอุปกรณ์และบุคลากรที่ไม่มากมายนี้ ทำให้การจัดการแนวคิด BYOD กลายเป็นเรื่องที่ไม่ยุ่งยากเท่ากับการดูแลบำรุงรักษาอุปกรณ์ที่องค์การเป็นเจ้าของที่ให้เงินลงทุนและยุ่งยากกว่า

โดยสรุปแล้ว การใช้อุปกรณ์พกพาส่วนตัวของพนักงานในที่ทำงานเป็นแนวโน้มทางเทคโนโลยีและการบริหารจัดการที่เป็นทั้งโอกาสซึ่งจะนำคุณประโยชน์บางประการมาสู่องค์การและพนักงาน และในขณะเดียวกันก็นำพาความเสี่ยงโดยเฉพาะภัยคุกคามที่มีต่อเครือข่ายสารสนเทศและข้อมูลที่สำคัญขององค์การ เทคโนโลยีที่พัฒนาขึ้นแทบทุกชนิดมีทั้งข้อดีและข้อเสียซึ่งก็ไม่มีข้อยกเว้นสำหรับ BYOD เช่นกัน ดังนั้น องค์การที่คิดจะนำนโยบาย BYOD มาใช้อย่างเหมาะสมนั้น สามารถก่อให้เกิดประโยชน์สูงสุดต่อองค์การและพนักงาน โดยสิ่งสำคัญ คือ การใช้งานภายใต้การบริหารจัดการและการควบคุมการเข้าถึงระบบเครือข่ายสารสนเทศและข้อมูลที่มีประสิทธิภาพ เพื่อที่จะไม่สร้างผลกระทบต่อความมั่นคงขององค์การนั่นเอง TPA news

แหล่งข้อมูลอ้างอิง

- TEN STEPS TO SECURE BYOD, Bradford Networks, 2012
- BYOD Risks and Rewards, Gerhard Eschelbeck, Chief Technology Officer and David Schwartzberg, Senior Security Engineer, Sophos Ltd., 2012
- Bring Your Own Device (BYOD) Policy Guidebook, ZAP, 2012
- Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems, Fortinet, 2012
- Good Technology State of BYOD Report, Good Technology, 2011
- Good Technology's 2nd Annual State of BYOD Report, Good Technology, 2012
- A SANS Whitepaper: SANS Mobility/BYOD Security Survey, Kevin Johnson, 2012
- Bring Your Own Device (BYOD), ม.ล.ลือศักดิ์จักรพันธุ์ ผู้อำนวยการเทคโนโลยีสารสนเทศและผู้จัดการฝ่ายพัฒนาธุรกิจ บริษัท เอสแอนด์พี ซินดิเคท จำกัด (มหาชน), 2012
- http://www.itmanagerdaily.com/byod-policy-template/
- http://www.zdnet.com/topic-byod-and-the-consumerization-of-it/
- http://www.itnewsafrica.com/2013/03/byod-where-does-the-control-actually-lie/
- http://www.icpnetworks.co.uk/blog/index.php/tag/bring-your-own-device-statistics/
- http://www.zenprise.com/solutions/bring-your-own-device/