วารสารวิชาชีพบัญชี

บทความวิชาการ

กลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD

ดร.ประจิต หาวัตร*

ศรัณย์ ชูเกียรติ*

บทคัดย่อ

บทความนี้อธิบายถึงประโยชน์และความเสี่ยงของการที่องค์กรอนุญาตให้พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงานขององค์กร พร้อมทั้งกลยุทธ์การจัดการความเสี่ยงดังกล่าว

คำสำคัญ: การจัดการความเสี่ยง อุปกรณ์เคลื่อนที่

ABSTRACT

This paper describes benefits and risks of allowing employees to bring their own mobile devices to perform their tasks in the organization. The strategies to manage those risks are also mentioned.

Keywords: Risk Management, Mobile Device

* ผู้เขียนทั้งสองดำรงตำแหน่งรองศาสตราจารย์ประจำ ภาควิชาการบัญชี คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย

บทความนี้มีจุดเริ่มต้นจากความรู้ที่ได้รับจากการเข้าร่วมอบรมในการประชุม The IIA International Conference 2012 ที่ Boston, Massachusetts ประเทศสหรัฐอเมริกา เมื่อวันที่ 8–11 กรกฎาคม 2555 ด้วยการสนับสนุนจากเงินทุนพัฒนาวิชาการของภาควิชาการบัญชี และเงินทุนสนับสนุนการอบรมระยะสั้นของคณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย

Download จาก...วารสารวิชาชีพบัญชี

ในปัจจุบันแนวคิดที่องค์กรอนุญาตให้พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงานขององค์กร หรือที่เรียกย่อ ๆ ว่า BYOD (**Bring Your Own Device**) มีแนวโน้มเพิ่มขึ้นอย่างมาก ดังจะเห็นได้จากงานวิจัยของ Forrester ที่ระบุว่าในปี ค.ศ. 2012 องค์กรในสหรัฐอเมริกาประมาณร้อยละ 60 ใช้ BYOD (Werth, 2012) ส่วนในประเทศไทยก็น่าจะมีองค์กรจำนวนไม่น้อยที่พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงานขององค์กร ซึ่งมีทั้งที่ผู้บริหารขององค์กรไม่รับรู้และรับรู้พร้อมทั้งอนุญาตให้นำมาใช้อย่างเป็นทางการ ดังนั้น ผู้บริหารขององค์กรจึงควรทำความเข้าใจถึงแนวคิด BYOD ทั้งด้านประโยชน์และความเสี่ยงสืบเนื่อง พร้อมทั้งกลยุทธ์ในการจัดการความเสี่ยงของการนำแนวคิด BYOD มาใช้ในองค์กร

การนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน

BYOD หรือ Bring Your Own Device

อุปกรณ์คอมพิวเตอร์เคลื่อนที่ (Mobile Device) เป็นอุปกรณ์คอมพิวเตอร์ขนาดเล็กและน้ำหนักเบาที่รับข้อมูลผ่านจอสัมผัสหน้าหรือคีย์บอร์ดขนาดเล็ก เช่น โน๊ตบุ๊ก สมาร์ทโฟน และ แท็บเล็ต ซึ่งสามารถเชื่อมต่อกับอินเทอร์เน็ตและเครือข่ายขององค์กรผ่าน 3G หรือ Wi-Fi หรือ Bluetooth ทำให้สามารถเข้าถึงอีเมล์ ระบบงานต่าง ๆ เช่น ระบบอีอาร์พี (ERP) และข้อมูลขององค์กรได้ ที่ผ่านมาองค์กรต่าง ๆ ได้จัดซื้ออุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านี้ให้พนักงานใช้ เพื่อให้สามารถทำงานได้ในทุกที่ทุกเวลา แต่ในปัจจุบันนี้ มีแนวโน้มเพิ่มมากขึ้นที่องค์กรจะอนุญาตให้พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงานและยอมให้มีการเชื่อมต่อเข้ากับเครือข่ายไร้สายขององค์กรได้ ที่เรียกแนวคิดนี้ว่า **การนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน (BYOD: Bring Your Own Device)** การเกิดขึ้นของ BYOD ด้านหนึ่งมาจากกระแสที่พนักงานทุกคนต้องการมีอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัว อีกด้านหนึ่งเป็นความพยายามขององค์กรในการควบคุมและรักษาความปลอดภัยข้อมูลขององค์กร ดังนั้น การจัดการด้านเทคโนโลยีสารสนเทศจึงต้องหาสมดุลระหว่างสองความต้องการสองอย่างนี้

ประโยชน์ของ BYOD

การนำแนวคิด BYOD มาใช้ในองค์กรนั้น มีประโยชน์หลายประการ ได้แก่

1. ประหยัดค่าใช้จ่ายการลงทุนด้านไอที (Cost Saving) เพราะพนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาเอง ทำให้องค์กรไม่จำเป็นลงทุนในอุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านั้น โดยบางองค์กรอาจใช้วิธีการเช่าอุปกรณ์คอมพิวเตอร์เคลื่อนที่ของพนักงานแทนการซื้อเป็นสินทรัพย์ขององค์กร เพื่อลดต้นทุนในการลงทุนด้านการซื้ออุปกรณ์คอมพิวเตอร์เคลื่อนที่ต่าง ๆ รวมถึงซอฟต์แวร์บางประเภทได้เช่นเดียวกัน

2. ได้ประโยชน์จากเทคโนโลยีที่ทันสมัย เนื่องจากการอนุญาตให้พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในองค์กรเป็นการเปิดโอกาสให้องค์กรมีอุปกรณ์คอมพิวเตอร์เคลื่อนที่ทันสมัยเข้ามาใช้ในการทำงานมากขึ้น ทำให้เกิดการแบ่งปันข้อมูลและความรู้เกี่ยวกับเทคโนโลยีสมัยใหม่ระหว่างพนักงานด้วยกัน

3. เพิ่มประสิทธิภาพในการทำงาน เนื่องจากเป็นอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัว ทำให้พนักงานสามารถนำติดตัวไปได้ทุกที่ทุกเวลา จึงพร้อมที่จะทำงานได้ทุกที่ทุกเวลาเช่นกัน

4. ตรงตามความต้องการของพนักงาน เนื่องจากเป็นอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัว พนักงานจึงเป็นผู้รับผิดชอบในการจัดหาและดูแลรักษาอุปกรณ์คอมพิวเตอร์เคลื่อนที่ ทำให้สามารถเลือกอุปกรณ์คอมพิวเตอร์เคลื่อนที่ที่ตรงตามความต้องการและความเหมาะสมของตนเองได้ รวมทั้งมีอิสระในการลงโปรแกรมที่อยากใช้งานได้สะดวกมากขึ้น

Download from วารสารวิชาชีพบัญชี

ความเสี่ยงสืบเนื่องของ BYOD

การนำแนวคิด BYOD มาใช้ในองค์กรนั้น มีความเสี่ยงสืบเนื่องหลายประการ ได้แก่

1. ความปลอดภัยข้อมูลองค์กร (Data Security) เนื่องจากข้อมูลของบริษัทจะถูกจัดเก็บในอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวของพนักงานซึ่งสามารถนำติดตัวไปไหนก็ได้ ดังนั้น จึงมีความเสี่ยงที่ข้อมูลจะรั่วไหล (Data Leak) ได้ในกรณีที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านั้นเกิดสูญหาย หรือข้อมูลขาดความพร้อมในการใช้งาน (Availability) ในกรณีที่ข้อมูลถูกจัดเก็บอยู่ในอุปกรณ์คอมพิวเตอร์เคลื่อนที่ของพนักงานที่ลาออก

2. การแพร่กระจายไวรัสและมัลแวร์ (Virus & Malware) เนื่องจากเป็นอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัว ดังนั้น หน้าที่ในการจัดการและการบำรุงรักษาจึงเป็นของพนักงาน หากพนักงานจัดการได้ไม่ดี จะทำให้มีความเสี่ยงต่อการที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านั้นติดไวรัสและมัลแวร์ ซึ่งเมื่อมีการนำมาใช้ในองค์กร ก็จะทำให้เกิดแพร่กระจายของไวรัสและมัลแวร์ไปยังคอมพิวเตอร์เครื่องอื่น ๆ ในองค์กรได้

3. ความยุ่งยากในการให้ความช่วยเหลือผู้ใช้งาน (User Support) เนื่องจากอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวที่พนักงานแต่ละคนนำมาใช้ในองค์กรนั้นมีความหลากหลาย ดังนั้น หากอุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านั้นเกิดปัญหาขึ้น การให้ความช่วยเหลือผู้ใช้งานจึงเป็นเรื่องที่ยุ่งยากมาก เพราะองค์กรอาจจะไม่มีพนักงานด้านไอทีที่มีความรู้ความสามารถในการแก้ปัญหาอุปกรณ์คอมพิวเตอร์เคลื่อนที่นั้น ๆ ได้ทั้งหมด

4. ความสามารถในการรองรับการใช้งานของเครือข่าย (Network Capacity) เนื่องจากการยินยอมให้พนักงานนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้งานในองค์กร ทำให้ปริมาณการใช้งานเครือข่ายเพิ่มมากขึ้น หากไม่มีการเตรียมเครือข่ายให้เพียงพอก็จะทำให้เครือข่ายขององค์กรมีปัญหาได้

กลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD

การควบคุมให้การใช้งาน BYOD เป็นไปได้อย่างมีประสิทธิผลควรมีการกำหนดกลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD ให้มีความสมดุลระหว่างความสะดวกในการใช้งานของผู้ใช้กับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรจากการใช้อุปกรณ์เคลื่อนที่ โดยกลยุทธ์ควรรวมถึงเรื่องต่อไปนี้

1. กำหนดนโยบายการใช้ BYOD

โดยทั่วไป องค์กรกำหนดนโยบายควบคุมการใช้อุปกรณ์คอมพิวเตอร์เคลื่อนที่ที่เป็นกรรมสิทธิ์ของบริษัท โดยอุปกรณ์คอมพิวเตอร์เคลื่อนที่เหล่านี้จะได้รับความคุ้มครองโดยระบบรักษาความปลอดภัยที่บริหารจัดการด้านไอทีขององค์กร อย่างไรก็ตาม การกำหนดนโยบายควบคุมอุปกรณ์คอมพิวเตอร์เคลื่อนที่ ซึ่งเป็นกรรมสิทธิ์ของพนักงานนับว่าเป็นงานที่ท้าทายอย่างหนึ่ง การกำหนดนโยบายการใช้ BYOD จำเป็นต้องอาศัยการมีส่วนร่วมของกลุ่มผู้มีส่วนได้ส่วนเสียหลายกลุ่มได้แก่ ลูกค้า ผู้บริหารฝ่ายต่าง ๆ ในองค์กร เช่น ฝ่ายไอที ฝ่ายขาย ฝ่ายกฎหมาย เป็นต้น ทั้งนี้เพื่อหลีกเลี่ยงความคลุมเครือและช่องโหว่ในนโยบาย (Ravindran et al., 2013) นอกจากนี้ การกำหนดนโยบายต้องทำอย่างระมัดระวังเพื่อให้แน่ใจว่านโยบายนี้สามารถใช้ได้เป็นเวลานานโดยนโยบายจะต้องสอดคล้องกับความต้องการของทั้งฝ่ายไอทีและผู้ใช้ นโยบายในการปกป้องสินทรัพย์สารสนเทศขององค์กรควรครอบคลุมเรื่องที่สำคัญ 4 เรื่อง ได้แก่ การควบคุมการเข้าถึง (Access Control) การใช้ที่เป็นที่ยอมรับ (Acceptable Use) การบริหารข้อมูล (Data Management) และการเข้ารหัสข้อมูล (Data Encryption) (Sullivan, 2013)

การควบคุมการเข้าถึง (Access Control) องค์กรควรระบุเรื่องของการกำหนดสิทธิและขอบเขตการใช้งานของเครือข่ายของอุปกรณ์คอมพิวเตอร์เคลื่อนที่ของพนักงาน และการติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์เพื่อป้องกันความเสี่ยงจากการแพร่กระจายจากอุปกรณ์คอมพิวเตอร์เคลื่อนที่ดังกล่าว

Download สำนักวิทยบริการฯ

> การควบคุมให้การนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน (BYOD: Bring Your Own Device) เป็นไปได้อย่างมีประสิทธิผลควรมีการกำหนดกลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD ให้มีความสมดุลระหว่างความสะดวกในการใช้งานของผู้ใช้กับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรจากการใช้อุปกรณ์เคลื่อนที่

การใช้ที่เป็นที่ยอมรับ (Acceptable Use) เพื่อป้องกันการที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่บางชนิดที่ใช้งานอยู่จะไม่ได้รับการสนับสนุนการใช้งาน (Support) โดยหน่วยงานไอทีขององค์กร องค์กรควรกำหนดนโยบายให้มีการทำรายละเอียดว่าอุปกรณ์คอมพิวเตอร์เคลื่อนที่ประเภทใดบ้างที่องค์กรรองรับและสนับสนุนให้นำมาใช้ได้ในองค์กร เพื่อให้พนักงานทราบและใช้เฉพาะอุปกรณ์คอมพิวเตอร์เคลื่อนที่ตามที่ระบุไว้เท่านั้น แม้จะเป็นการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการปฏิบัติงานก็ต้องลงทะเบียนไว้กับองค์กรว่าเป็นอุปกรณ์คอมพิวเตอร์เคลื่อนที่ที่อนุญาตให้นำมาใช้อย่างเป็นทางการ (Official Device) ได้

การบริหารข้อมูล (Data Management) ควรมีการแบ่งระดับของข้อมูล (Data Classification) ที่พนักงานสามารถเข้าถึงได้โดย (หรือจัดเก็บใน) อุปกรณ์คอมพิวเตอร์เคลื่อนที่ และกำหนดให้มีการควบคุมที่สอดคล้องกับระดับของข้อมูลซึ่งจะช่วยลดความเสี่ยงจากการรั่วไหลของข้อมูลที่เป็นความลับ นอกจากนี้ ในการเตรียมพร้อมเผื่อกรณีที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่สูญหาย แล้วองค์กรต้องการลบข้อมูลที่จัดเก็บก็ควรกำหนดนโยบายให้มีการติดตั้งและใช้การลบจากระยะไกล (Remote Wipe) เช่น Mobile Defense และ Android Lost เป็นต้น

การเข้ารหัส (Encryption) การเข้ารหัสข้อมูลจะช่วยรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งระหว่างการส่งไปยังอุปกรณ์หรือระบบอื่นและระหว่างที่จัดเก็บอยู่ในอุปกรณ์คอมพิวเตอร์เคลื่อนที่ จะช่วยลดความเสี่ยงจากการรั่วไหลของข้อมูลได้เป็นความลับได้เช่นเดียวกับการบริหารข้อมูลที่กล่าวมาข้างต้น การที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่ใช้เชื่อมต่อกับ Public Wi-Fi และเครือข่ายเคลื่อนที่ ทำให้มันมีความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยมากกว่าการใช้งานในระบบ LAN ขององค์กร ดังนั้นจึงควรมีการควบคุมข้อมูลระหว่างส่งโดยอาศัยการเข้ารหัสข้อมูลระหว่างส่งผ่านอุปกรณ์เครือข่ายโดยใช้ Secure Socket Layer (SSL) Virtual Private Network (VPN) ส่วนการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์เคลื่อนที่นั้นมีความยากกว่าการดูแลข้อมูลระหว่างส่ง เนื่องจากอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนใหญ่ไม่มีการเข้ารหัสในตัวอุปกรณ์ (Device Encryption) หรือมีแต่การเข้ารหัสอาจถูกแฮ็คได้ ซึ่งการตรวจให้พบการแฮ็คนี้ก็ต้องมีการติดตั้งระบบที่จะช่วยตรวจจับ iOS jailbreaking หรือ Android Rooting อย่างไรก็ตาม ในปัจจุบันมีผู้คิดค้นและเผยแพร่ apps ที่ใช้ block jailbreak detection และ root detection

2. ตรวจสอบการใช้ BYOD

เพื่อให้แน่ใจว่าการใช้อุปกรณ์คอมพิวเตอร์เคลื่อนที่ของพนักงานนั้นเป็นไปตามนโยบายที่องค์กรกำหนดตามที่กล่าวถึงในข้อ 1 และตามมาตรฐานการใช้งานเทคโนโลยีสารสนเทศทั่วไป เช่น การอัพเดทอุปกรณ์และเครือข่ายด้วย Security Patch ล่าสุด การอบรมเกี่ยวกับนโยบาย (Password Policy) เป็นต้น

Download จาก กรมวิชาชีพบัญชี

3. จัดประเมินและฝึกอบรมเพิ่มทักษะการใช้อุปกรณ์คอมพิวเตอร์เคลื่อนที่ใหม่ ๆ ให้กับพนักงาน

เพื่อให้พนักงานสามารถนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่มาใช้ภายในองค์กรได้ถูกวิธี มีความมั่นคงปลอดภัย และเกิดประสิทธิภาพสูงสุด

บทสรุป

กระแสการนำอุปกรณ์คอมพิวเตอร์เคลื่อนที่ส่วนตัวมาใช้ในการทำงาน (BYOD: Bring Your Own Device) กำลังได้รับความนิยมและถูกนำไปใช้อย่างแพร่หลายมากยิ่งขึ้นทุกที ซึ่งแน่นอนว่าย่อมก่อให้เกิดประโยชน์อย่างมากมายกับองค์กร ในขณะเดียวกันก็เป็นความท้าทายที่สำคัญขององค์กรที่จำเป็นจะต้องมีการบริหารจัดการด้านเทคโนโลยีสารสนเทศให้เหมาะสม ซึ่งต้องอาศัยความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีสารสนเทศและแนวคิด BYOD ทั้งด้านประโยชน์และความเสี่ยงสืบเนื่องที่ตามมา เพื่อกำหนดกลยุทธ์การจัดการความเสี่ยงจากการใช้ BYOD ให้เหมาะสม

บรรณานุกรม

Ravindran, S., Sadana, R., and D. Baranwal, "BYOD in the Enterprise—A Holistic Approach," *ISACA Journal*, Vol. 1, 2013.

Sullivan, D. "MDM software: Why it's important and what it should include" http://searchconsumerization.techtarget.com/tip/MDM-software-Why-its-important-and-what-it-should-include accessed on June 13, 2013

Werth, W.W. "Bitzer Mobile Solves BYOD Security and Usability Clash for Enterprise Mobility," March 2012, www.bitzermobile.com/press-release-9/

Download จาก วารสารวิชาชีพบัญชี