

17 มกราคม 2557

แหล่งที่มา: Prachachat Turakij Online

http://www.prachachat.net/news_detail.php?newsid=1389859641

PwC ชี้ภัยคุกคามความปลอดภัยข้อมูลทั่วโลกพุ่ง 25% เตือนรับมืออาชญากรไซเบอร์ก่อนเปิดเออีซี

บริษัท PwC ประเทศไทย (ไพร์ซฮอเวอร์เฮาส์คูเปอร์ส) หนึ่งในเครือข่ายบริษัทผู้ให้บริการด้านการตรวจสอบบัญชี บริการให้คำปรึกษาด้านภาษี และบริการให้คำปรึกษาทางธุรกิจรายใหญ่ของโลก เผยผลสำรวจ The Global State of Information Security® Survey 2014 —ผลสำรวจสถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลกประจำปี 2557 ทั้งนี้ผลสำรวจประจำปีครั้งที่ 16 ถูกจัดทำขึ้นระหว่างวันที่ 1 กุมภาพันธ์ ถึง 1 เมษายน 2556 โดยความร่วมมือกันระหว่าง PwC, CIO Magazine และ CSO Magazine ผ่านการสำรวจความคิดเห็นทางอีเมลล์จากบรรดานักธุรกิจและ ผู้นำบริษัทไอทีชั้นนำทั่วโลกกว่า 9,600 ราย ครอบคลุม 115 ประเทศ โดยแบ่งเป็นผู้ถูกสำรวจจากทวีปอเมริกาเหนือ (36%), ยุโรป (26%), เอเชียแปซิฟิก (21%), อเมริกาใต้ (16%) และ ตะวันออกกลาง และแอฟริกาใต้ (2%)

ผลจากการสำรวจที่น่าสนใจ ได้แก่

จำนวนภัยคุกคามความปลอดภัยข้อมูลทั่วโลก (Information security) ขยายตัวสูงขึ้นถึง 25% มาที่ 3,741 เหตุการณ์ในปี 2556 และมีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในระยะ 2-3 ปีข้างหน้า ในขณะที่ความเสียหายทางการเงิน (Financial losses) ที่เกิดจากภัยคุกคามข้อมูลก็เติบโตในทิศทางเดียวกัน โดยปรับตัวเพิ่มขึ้นเฉลี่ย 18% ในช่วงเดียวกันของปีก่อน

ภาคธุรกิจต้องหันมาตื่นตัวในการแก้ปัญหาพร้อมมีมาตรการ ในการรักษาความปลอดภัยของข้อมูลอย่างจริงจังและเป็นระบบ เพื่อสร้างศักยภาพในการแข่งขัน และขยายฐานลูกค้าใหม่ๆ หลังผลสำรวจระบุว่า มีบริษัททั่วโลกเพียง 17% ที่มีมาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศอยู่ในเกณฑ์มาตรฐานระดับสูงอย่างแท้จริง ส่วนทางกับความมั่นใจของผู้บริหารส่วนใหญ่ที่เข้าใจผิด คิดว่าตนมีระบบความปลอดภัยด้านข้อมูลสารสนเทศที่รัดกุมเพียงพอแล้ว

กระแสของภัยคุกคามข้อมูลสารสนเทศที่เพิ่มขึ้นทั่วโลก (Rise in global security incidents) และกลยุทธ์การรักษาความปลอดภัยระบบข้อมูลที่ล้าสมัย (Outdated strategies) ถือเป็นปัจจัยหลักที่ทำให้ธุรกิจทั่วโลกส่วนใหญ่ บริหารจัดการความปลอดภัยข้อมูลสารสนเทศ อย่างไม่ตรงจุด ขาดประสิทธิภาพและเป็นที่มาของความเสียหายทางธุรกิจที่เพิ่มมากขึ้น ในปัจจุบัน

ผู้บริหารทั่วโลกเกือบครึ่ง (50%) คาดจะขยายการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลองค์กรของตนในอีก 12 เดือนข้างหน้าดีขึ้นกว่าปีก่อนที่ 45%

ในระดับทวีป ผู้บริหารบริษัทในอเมริกาใต้ (66%) และเอเชียแปซิฟิก (60%) คาดจะมีการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลสารสนเทศในอีก 12 เดือนข้างหน้ามากที่สุด นำหน้าตลาดที่พัฒนาแล้วอย่างยุโรปที่ 46% และอเมริกาเหนือที่ 38%

ในยุคที่นวัตกรรมไอทีไม่ว่าจะอุปกรณ์สื่อสารที่ทันสมัย สื่อสังคมออนไลน์ (Social media) คลาวด์คอมพิวติ้ง (Cloud computing) และแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring your own device: BYOD) เข้ามามีบทบาทต่อการดำเนินธุรกิจในปัจจุบัน ความเสี่ยงทางธุรกิจที่พบมากขึ้นอันดับต้นๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่ได้นำถึงถึงการรักษาปลอดภัยของข้อมูลในระดับที่เพียงพอควบคู่กันไปด้วย

ผู้บริหารที่ทำการสำรวจเกือบครึ่ง หรือ 47% กล่าวว่าองค์กรของตนมีการใช้คลาวด์คอมพิวติ้ง (Cloud computing) แต่มีบริษัทเพียงแค่ 18% ที่มีโซลูชันการรักษาความปลอดภัยข้อมูลบนระบบคลาวด์

บริษัทส่วนใหญ่มีการนำระบบป้องกันความปลอดภัยข้อมูลที่รู้จักกันดีมาใช้อย่างแพร่หลาย ไม่ว่าจะเป็นการใช้พีเอ็น (VPN), การตั้งค่าไฟร์วอลล์ (Firewall) หรือ การป้องกันข้อมูลด้วยการเข้ารหัสบนเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Encryption of desktop PCs) แต่ในความเป็นจริง มีบริษัทเพียงน้อยรายเท่านั้น ที่มีการนำเอาเครื่องมือตรวจสอบข้อมูลและเครือข่ายที่สามารถวิเคราะห์ความเสี่ยงแบบเรียลไทม์ (Real-time) มาใช้ควบคู่ไปด้วย

อุปสรรคสำคัญในการปรับปรุงระบบความปลอดภัยของข้อมูลองค์กรทั่วโลกมีอยู่ด้วยกัน 3 ประการ ได้แก่ ความขาดแคลนของแหล่งเงินทุน ความเข้าใจที่ไม่เพียงพอของภาคธุรกิจที่มีผลกระทบต่อความปลอดภัยข้อมูลสารสนเทศในระยะยาว และการขาดวิสัยทัศน์หรือการสนับสนุนอย่างจริงจังจากผู้นำ ได้แก่ ซีอีโอ ผู้บริหารระดับสูง ไปจนถึงคณะกรรมการบริษัท

ภาคธุรกิจไทยต้องทบทวนบทบาทการนำกลยุทธ์ความปลอดภัยข้อมูลสารสนเทศมาใช้กับองค์กร เพื่อสร้างรายได้เปรียบทางธุรกิจ ขยายฐานลูกค้า และตลาดใหม่ๆ ในยามที่ประเทศกำลังเตรียมความพร้อมก่อนการเปิดประชาคมเศรษฐกิจอาเซียน