

16 มกราคม 2557

แหล่งที่มา: เว็บไซต์thailand press release news

<http://www.thailand4.com/it/2014-01-16/d8bc3e718a91c3a2b833efac806ac519/>

PwC ชี้ภัยคุกคามความปลอดภัยข้อมูลทั่วโลกพุ่ง 25% เตือนบริษัทไทยเร่งปรับกลยุทธ์ รับมืออาชญากรไซเบอร์ ก่อนเปิดเออีซี



บริษัท PwC ประเทศไทย (ไพร์ซวอเตอร์เฮาส์คูเปอร์ส) เปิดเผยถึงผลสำรวจ สถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2557 ว่า ปัญหาภัยคุกคามข้อมูลสารสนเทศ (Information security) มีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในระยะ 2-3 ปี ข้างหน้า หลังผลสำรวจระบุว่าจำนวนภัยคุกคามความปลอดภัยข้อมูลและไซเบอร์คราฟต์ทั่วโลกขยายตัวสูงขึ้นถึง 25% ในปีที่ผ่านมา แม้ภาครัฐก็จะได้มีการลงทุนเพิ่มเพื่อพัฒนาระบบฯ และมีบริษัทเพียง 17% เท่านั้นที่มีมาตรฐานการรักษาความปลอดภัยข้อมูลอยู่ในระดับสูงอย่างแท้จริง จากการสำรวจผู้บริหารกว่า 9,600 ราย

ภาครัฐกิจและรัฐบาลไทยต้องหันมาตื่นตัวในการแก้ปัญหานี้อย่างจริงจัง พร้อมมีมาตรการในการรักษาความปลอดภัยข้อมูลอย่างชัดเจนและเป็นระบบ เพื่อสร้างศักยภาพในการแข่งขันและเตรียมความพร้อมก่อนการเปิดประชาคมเศรษฐกิจอาเซียนในปลายปี '58 ผลสำรวจ สถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2557 (The Global State of Information Security® Survey 2014) พบว่า มีผู้บริหารด้านไอทีทั่วโลกถึง 74% ที่มั่นใจว่าธุรกิจของตน มีการบริหารจัดการข้อมูลสารสนเทศที่รัดกุมและมีประสิทธิภาพ ในจำนวนนี้ ยังมีผู้บริหารระดับสูงกว่าครึ่ง หรือ 50% ที่หลงคิดว่าองค์กรของตนมีการประยุกต์ใช้กลยุทธ์และการวางแผนระบบรักษาความปลอดภัยข้อมูลที่ดีเลิศ อยู่ในอันดับต้นๆ หรือที่เรียกว่า Front runners

PwC ให้คำจำกัดความของคำว่า **Front runners** หรือ ‘องค์กรที่มีความมั่นคงด้านความปลอดภัยข้อมูล’ โดยวัดจากบริษัทที่มีการดำเนินการในด้านต่างๆ ประกอบไปด้วย การมีกลยุทธ์การรักษาความปลอดภัยข้อมูลสารสนเทศของบริษัทที่ครอบคลุม มีผู้บริหารฝ่ายรักษาความปลอดภัยข้อมูล (**Chief Information Security Officer: CISO**) หรือเทียบเท่า รายงานตรงต่อซีไอโอ ประธานเจ้าหน้าที่บริหารฝ่ายการเงิน ประธานเจ้าหน้าที่บริหารฝ่ายปฏิบัติการ หรือผู้ให้คำปรึกษาทางด้านกฎหมาย มีการวัดผลและประเมินประสิทธิภาพของระบบรักษาความปลอดภัยอย่างสม่ำเสมอ และมีความรู้ความเข้าใจอย่างถ่องแท้ถึงภัยคุกคามข้อมูลสารสนเทศประเภทต่างๆ

นางสาว วิไลพร ทวีลาภพันทอง หัวหน้าส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) กล่าวว่า จำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์คราฟต์ทั่วโลกในปีที่ผ่านมา มีจำนวนเพิ่มขึ้นเป็น 3,741 เหตุการณ์ หรือเติบโต 25% จากปีก่อน ในขณะที่ความเสียหายทางการเงิน (**Financial losses**) ที่เกิดจากภัยคุกคามข้อมูลองค์กรก็เติบโตในทิศทางเดียวกัน โดยปรับตัวเพิ่มขึ้น 18% โดยเฉลี่ยในช่วงเดียวกันของปีก่อน

งบค่าใช้จ่ายด้านการรักษาความปลอดภัยข้อมูล (**Information security budget**) องค์กรทั่วโลก มีมูลค่าเฉลี่ยที่ 4.3 ล้านดอลลาร์สหรัฐฯ โดยปรับตัวสูงขึ้นอย่างมีนัยสำคัญจากปีก่อนถึง 51% แต่อย่างไรก็ดี งบลงทุนด้านนี้คิดเป็นสัดส่วนเพียง 3.8% ของงบลงทุนด้านไอทีทั้งหมด

“เราจะเห็นได้ว่าจำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์คราฟต์ทั่วโลกมีการปรับตัวเพิ่มขึ้นเรื่อยๆ แม้ว่าภาคธุรกิจจะได้มีการลงทุนในด้านนี้เพิ่มเติมในช่วงที่ผ่านมา สะท้อนให้เห็นว่าการรักษาความปลอดภัยที่ไม่ได้ประสิทธิภาพประกอบกับการใช้กลยุทธ์ที่ล้าสมัย ถือเป็นปัจจัยฉนวนที่ทำให้องค์กรทั่วโลกส่วนใหญ่ มีการบริหารจัดการความปลอดภัยข้อมูลอย่างไม่ตรงจุด และเป็นที่มาของความเสียหายทางธุรกิจที่เพิ่มขึ้น” นางสาว วิไลพร กล่าว

“ผู้บริหารบริษัททั่วโลกส่วนใหญ่ที่เราทำการสำรวจ ยังคงมีการประเมินตัวเองที่สูงเกินไป หลายคนคิดว่า ตนมีระบบความปลอดภัยข้อมูลที่รัดกุมและเพียงพอ เป็นที่น่าสนใจว่ามี 30% ของผู้บริหารเหล่านี้ล้วนมาจากองค์กรขนาดใหญ่ที่มีรายได้มากกว่า 1 พันล้านเหรียญฯทั้งสิ้น”

นางสาววิไลพร กล่าวต่อว่า ยิ่งผู้ประกอบการฯ ประเมินความเสี่ยงในเรื่องนี้ต่ำเกินไป ก็จะเป็นการเปิดช่องโหว่ให้ธุรกิจเกิดความเสียหายจากการประหลาดใจชอบ ก่อให้เกิดความเสียหายเป็นมูลค่ามหาศาล

ผลสำรวจยังพบว่า จำนวนของบริษัทที่ไม่รู้ว่ามีภัยคุกคามข้อมูลเกิดขึ้นกับบริษัทของตน ปรับตัวเพิ่มขึ้นเป็น 2 เท่าในช่วง 2 ปีที่ผ่านมา สะท้อนให้เห็นว่า มีบริษัทอยู่เป็นจำนวนมากที่ใช้กลยุทธ์ในการป้องกันความปลอดภัยข้อมูลที่ล้าสมัย และมีผู้บริหารที่ทำการสำรวจทั่วโลกเพียง 17% เท่านั้นที่มีคุณสมบัติเข้าข่ายการเป็นผู้นำความปลอดภัยข้อมูลอย่างแท้จริง (**True information security leaders**)

‘แฮ็กเกอร์’ แชนปี วาฬร้ายจารกรรมข้อมูลนอกองค์กร

ผลจากการสำรวจระบุว่า อินไซด์เดอร์ (**Insider**) หรือ บรรดากลุ่มผู้ใช้ข้อมูลภายใน ได้แก่ พนักงานบริษัทในปัจจุบัน (31%) และ พนักงานเก่าของบริษัท (27%) มีแนวโน้มที่จะประกอบการโจรกรรมข้อมูลภายในองค์กรมากที่สุด ในขณะเดียวกัน ผู้บริหารถึง 32% มองว่า แฮ็กเกอร์ (**Hacker**) เป็นอาชญากรข้อมูลนอกองค์กรอันดับ 1 ตามด้วยคู่แข่ง (14%), อาชญากรรมแบบมีการวางแผนและจัดการล่วงหน้า หรือ ออร์แกนไครม (12%), กลุ่มนักเคลื่อนไหว นักต่อต้าน (10%), ผู้ก่อการร้าย (8%), และอื่นๆ

อเมริกาใต้, เอเชียแปซิฟิกขึ้นแท่นผู้นำด้านงบประมาณความปลอดภัยข้อมูลปี '57

อย่างไรก็ดี เมื่อมองแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศ (Information security spending) ในแต่ละภูมิภาคทั่วโลกพบว่า เทรนด์การใช้จ่ายเพื่อลงทุนด้านความปลอดภัยข้อมูลของผู้บริหารในทวีปอเมริกาใต้ และ เอเชียแปซิฟิกมีความร้อนแรง แซงหน้าธุรกิจในแถบอเมริกาเหนือ และยุโรป ที่ยังคงเผชิญกับการชะลอตัวทางเศรษฐกิจและการฟื้นตัวอย่างช้าๆ จากปัญหาวิกฤตหนี้

“จะเห็นได้ว่าผู้บริหารบริษัทในเอเชียถึง 60% ที่ยังคงความมั่นใจในการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลองค์กรในระยะข้างหน้า เปรียบเทียบกับ 61% ในปีก่อน ซึ่งถึงแม้จะลดลงเล็กน้อย แต่ก็ยังถือว่าเป็นทวีปที่มีอัตราสูงสุดเป็นอันดับสองรองจากทวีปอเมริกาใต้ที่ 66% และนำหน้ายุโรปที่ 46% และอเมริกาเหนือที่ 38% ตามลำดับ” นางสาว วิไลพร กล่าว

ด้านนายศิระ อินทรกำแหง ประธานกรรมการบริหาร บริษัท PwC ประเทศไทย กล่าวเสริมว่า ในยุคที่นวัตกรรมไอทีไม่ว่าจะอุปกรณ์สื่อสารที่ทันสมัย สื่อสังคมออนไลน์ (Social media) คลาวด์คอมพิวติ้ง (Cloud computing) และแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring your own device: BYOD) เข้ามามีบทบาทต่อการดำเนินธุรกิจในปัจจุบัน ความเสี่ยงทางธุรกิจที่พบมากขึ้นอันดับต้นๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่ได้นิ่งถึงการรักษาปลอดภัยของข้อมูลในระดับที่เพียงพอควบคู่กันไปด้วย

“การใช้งานระบบสารสนเทศอย่างแพร่หลายในชีวิตประจำวัน ทำให้เกิดการคาบเกี่ยวของการใช้งานอุปกรณ์ไอทีสำหรับการทำงานและเรื่องส่วนตัว ซึ่งถือเป็นโจทย์ใหญ่ขององค์กรหลายแห่งทั่วโลกในปัจจุบันว่าจะมีวิธีบริหารจัดการอย่างไรเพื่อให้การทำงานแบบเคลื่อนที่ หรือแนวคิดแบบ BYOD ที่สามารถเรียกใช้ข้อมูลจากที่ไหน เมื่อไหร่ก็ได้ ตามที่ต้องการ มีความปลอดภัยและป้องกันการสูญหายของข้อมูลได้มากที่สุด” นาย ศิระ กล่าว

ผลสำรวจพบว่า มีบริษัทมากเกือบครึ่ง หรือ 47% ทั่วโลกที่มีการใช้ระบบคลาวด์คอมพิวติ้ง แต่ในทางตรงกันข้าม มีเพียง 18% ที่มีโซลูชันรักษาความปลอดภัยข้อมูลบนระบบคลาวด์

“จริงอยู่ที่เราจะเห็นบริษัทส่วนใหญ่มีการนำระบบป้องกันความปลอดภัยข้อมูลที่รู้จักกันดีมาใช้ในการใช้งาน ไม่ว่าจะเป็นการใช้วีพีเอ็น (VPN), การตั้งค่าไฟร์วอลล์ (Firewall) หรือ การป้องกันข้อมูลด้วยการเข้ารหัสบนเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Encryption of desktop PCs) แต่นั่นยังไม่เพียงพอ มีบริษัทเพียงน้อยรายเท่านั้น ที่มีการนำเอาเครื่องมือตรวจสอบข้อมูลและเครือข่าย ที่สามารถวิเคราะห์ความเสี่ยงแบบเรียลไทม์ (Real-time) มาใช้ควบคู่ไปด้วย”

เมื่อมองไปข้างหน้า นายศิระกล่าวว่า อุปสรรคสำคัญในการปรับปรุงระบบความปลอดภัยของข้อมูลองค์กรทั่วโลกมีอยู่ด้วยกัน 3 ประการได้แก่ ความขาดแคลนของแหล่งเงินทุน ความเข้าใจที่ไม่เพียงพอของภาคธุรกิจที่มีผลกระทบต่อความปลอดภัยข้อมูลสารสนเทศในระยะยาว และการขาดวิสัยทัศน์หรือการสนับสนุนอย่างจริงจังจากผู้นำ ได้แก่ ซีอีโอ ผู้บริหารระดับสูง ไปจนถึงคณะกรรมการบริษัท

“ถือเป็นเรื่องที่น่าเป็นห่วงอย่างยิ่งที่ภาคธุรกิจไทย ต้องพบพานบทบาทและหุ้มนำแนวคิดเก่าๆ ในการรักษาความปลอดภัยข้อมูลมาใช้กับองค์กรของตน เอกชนไทยต้องมีการปรับกลยุทธ์โดยหันมาให้ความสำคัญกับเทคโนโลยีสารสนเทศเพื่อสร้างความได้เปรียบทางธุรกิจ ขยายฐานลูกค้า และหาตลาดใหม่ๆ ในยามที่เราทุกคนกำลังเตรียมความพร้อมก่อนการเปิดเออีซี นอกจากนี้

ผู้บริหารระดับสูงยังจะต้องเร่งสร้าง **Awareness** ในเรื่องการรักษาความปลอดภัยข้อมูลให้เกิดแก่พนักงานลูกค้าและ **Stakeholder** อื่นๆ รวมทั้งปลูกฝังจริยธรรมในการเผยแพร่ข้อมูลซึ่งถือเป็น **Asset** ที่สำคัญของบริษัทออกไปภายนอกอีกด้วย”