16 มกราคม 2557
แหล่งที่มา: เว็บไซต์ ASTV ผู้จัดการออนไลน์
http://manager.co.th/CyberBiz/ViewNews.aspx?NewsID=9570000005838

PwC เตือนบริษัทไทยเร่งปรับกลยุทธ์ รับมืออาชญากรไซเบอร์

ผลสำรวจพบ จำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามทั่วโลกขยายตัว 25% ในปีที่ผ่านมา ย้ำบริษัทไทยต้องเร่งปรับกลยุทธ์ พร้อมกำหนดนโยบายรักษาความปลอดภัยที่ทันสมัย เพื่อบริหารความเสี่ยงเพื่อรับมือกับมิจฉาชีพและการโจรกรรมข้อมูลที่ซับซ้อน รวมทั้งเตรียมตัวกับการเปิดประชาคม ศก.อาเซียนที่กำลังจะมาถึง คาดแนวโน้มภัยมืดโตต่อในอีก 2-3 ปีข้างหน้า

บริษัท PwC ประเทศไทย (ไพรซ์วอเตอร์เฮาส์คูเปอร์ส) เปิดเผยถึงผลสำรวจสถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2557 ว่า ปัญหาภัยคุกคามข้อมูลสารสนเทศ (Information security) มีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในระยะ 2-3 ปีข้างหน้า หลังผลสำรวจระบุว่าจำนวนภัยคุกคามความปลอดภัยข้อมูลและไซเบอร์ครามทั่วโลกขยายตัวสูงขึ้นถึง 25% ในปีที่ผ่านมา แม้ภาคธุรกิจจะได้มีการลงทุนเพิ่มเพื่อพัฒนาระบบฯ และมีบริษัทเพียง 17% เท่านั้นที่มีมาตรฐานการรักษาความปลอดภัยข้อมูลอยู่ในระดับสูงอย่างแท้จริง จากการสำรวจผู้บริหารกว่า 9,600 ราย

ภาคธุรกิจและรัฐบาลไทยต้องหันมาตื่นตัวในการแก้ปัญหาอย่างจริงจัง พร้อมมีมาตรการในการรักษาความปลอดภัยข้อมูลอย่างชัดเจนและเป็นระบบ เพื่อสร้างศักยภาพในการแข่งขันและเตรียมความพร้อมก่อนการเปิดประชาคมเศรษฐกิจอาเซียนในปลายปี 2558

ผลสำรวจสถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2557 (The Global State of Information Security Survey 2014) พบว่า มีผู้บริหารด้านไอทีทั่วโลกถึง 74% ที่มั่นใจว่าธุรกิจของตนมีการบริหารจัดการข้อมูลสารสนเทศที่รัดกุมและมีประสิทธิภาพ ในจำนวนนี้ยังมีผู้บริหารระดับสูงกว่าครึ่ง หรือ 50% ที่หลงคิดว่าองค์กรของตนมีการประยุกต์ใช้กลยุทธ์และการวางแผนระบบรักษาความปลอดภัยข้อมูลที่ดีเลิศ อยู่ในอันดับต้นๆ หรือที่เรียกว่า Front runners

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

นางสาววิไลพร ทวีลาภพันทอง หุ้นส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) กล่าวว่า จำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามทั่วโลกในปีที่ผ่านมามีจำนวนเพิ่มขึ้นเป็น 3,741 เหตุการณ์ หรือเติบโต 25% จากปีก่อน ในขณะที่ความเสียหายทางการเงิน (Financial losses) ที่เกิดจากภัยคุกคามข้อมูลองค์กรก็เติบโตในทิศทางเดียวกัน โดยปรับตัวเพิ่มขึ้น 18% โดยเฉลี่ยในช่วงเดียวกันของปีก่อน

งบค่าใช้จ่ายด้านการรักษาความปลอดภัยข้อมูล (Information security budget) องค์กรทั่วโลกมีมูลค่าเฉลี่ยที่ 4.3 ล้านเหรียญสหรัฐ โดยปรับตัวสูงขึ้นอย่างมีนัยสำคัญจากปีก่อนถึง 51% แต่อย่างไรก็ดี งบลงทุนฯ ด้านนี้คิดเป็นสัดส่วนเพียง 3.8% ของงบลงทุนด้านไอทีทั้งหมด

"เราจะเห็นได้ว่าจำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามทั่วโลกมีการปรับตัวเพิ่มขึ้นเรื่อยๆ แม้ว่าภาคธุรกิจจะได้มีการลงทุนในด้านนี้เพิ่มเติมในช่วงที่ผ่านมา สะท้อนให้เห็นว่าการรักษาความปลอดภัยที่ไม่ได้ประสิทธิภาพ ประกอบกับการใช้กลยุทธ์ที่ล้าสมัย ถือเป็นปัจจัยถ่วงที่ทำให้องค์กรทั่วโลกส่วนใหญ่มีการบริหารจัดการความปลอดภัยข้อมูลอย่างไม่ตรงจุด และเป็นที่มาของความเสี่ยงทางธุรกิจที่เพิ่มขึ้น"

ผู้บริหารบริษัททั่วโลกส่วนใหญ่ที่เราทำการสำรวจยังคงมีการประเมินตัวเองที่สูงเกินไป หลายๆ คนคิดว่าตนมีระบบความปลอดภัยข้อมูลที่รัดกุมและเพียงพอ เป็นที่น่าสนใจว่ามี 30% ของผู้บริหารเหล่านี้ล้วนมาจากองค์กรขนาดใหญ่ที่มีรายได้มากกว่า 1 พันล้านเหรียญทั้งสิ้น

นางสาววิไลพรกล่าวต่อว่ายิ่งผู้ประกอบการประเมินความเสี่ยงในเรื่องนี้ต่ำเกินไป ก็จะยิ่งเป็นการเปิดช่องโหว่ให้ธุรกิจเกิดความเสี่ยงจากการประพฤติมิชอบ ก่อให้เกิดความเสียหายเป็นมูลค่ามหาศาล

ผลสำรวจยังพบว่าจำนวนของบริษัทที่ไม่รู้ว่ามีภัยคุกคามข้อมูลเกิดขึ้นกับบริษัทของตน ปรับตัวเพิ่มขึ้นเป็น 2 เท่าในช่วง 2 ปีที่ผ่านมา สะท้อนให้เห็นว่ามีบริษัทอยู่เป็นจำนวนมากที่ใช้กลยุทธ์ในการป้องกันความปลอดภัยข้อมูลที่ล้าสมัย และมีผู้บริหารที่ทำการสำรวจทั่วโลกเพียง 17% เท่านั้นที่มีคุณสมบัติเข้าข่ายการเป็นผู้นำความปลอดภัยข้อมูลอย่างแท้จริง (True information security leaders)

*****'แฮกเกอร์' แชมป์วายร้ายจารกรรมข้อมูลนอกองค์กร**

ผลจากการสำรวจระบุว่า อินไซเดอร์ (Insider) หรือบรรดากลุ่มผู้ใช้ข้อมูลภายใน ได้แก่ พนักงานบริษัทในปัจจุบัน (31%) และพนักงานเก่าของบริษัท (27%) มีแนวโน้มที่จะประกอบการโจรกรรมข้อมูลภายในองค์กรมากที่สุด ในขณะเดียวกัน ผู้บริหารถึง 32% มองว่า แฮกเกอร์ (Hacker) เป็นอาชญากรข้อมูลนอกองค์กรอันดับ 1 ตามด้วยคู่แข่ง (14%), อาชญากรรมแบบมีการวางแผนและจัดการล่วงหน้า หรือออร์แกไนซ์คราม (12%), กลุ่มนักเคลื่อนไหว นักต่อต้าน (10%), ผู้ก่อการร้าย (8%) และอื่นๆ

*****อเมริกาใต้, เอเชียแปซิฟิกขึ้นแท่นผู้นำด้านงบลงทุนความปลอดภัยข้อมูลปี 2557**

อย่างไรก็ดี เมื่อมองแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศ (Information security spending) ในแต่ละภูมิภาคทั่วโลกพบว่า เทรนด์การใช้จ่ายเพื่อลงทุนด้านความปลอดภัยข้อมูลของผู้บริหารในทวีปอเมริกาใต้ และเอเชียแปซิฟิกมีความร้อนแรงแซงหน้าธุรกิจในแถบอเมริกาเหนือ และยุโรป ที่ยังคงเผชิญกับการชะลอตัวทางเศรษฐกิจและการฟื้นตัวอย่างช้าๆ จากปัญหาวิกฤตหนี้

"จะเห็นได้ว่ามีผู้บริหารฯ บริษัทในเอเชียถึง 60% ที่ยังคงความมั่นใจในการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลองค์กรในระยะข้างหน้า เปรียบเทียบกับ 61% ในปีก่อน ซึ่งถึงแม้จะลดลงนิดหน่อย แต่ก็ยังถือว่าเป็นทวีปที่มีอัตราสูงสุดเป็นอันดับสอง รองจากทวีปอเมริกาใต้ที่ 46% และนำหน้ายุโรปที่ 46% และอเมริกาเหนือที่ 38% ตามลำดับ"

ด้านนายศิระ อินทรกำธชัย ประธานกรรมการบริหาร บริษัท PwC ประเทศไทย กล่าวเสริมว่า ในยุคที่นวัตกรรมไอทีไม่ว่าจะอุปกรณ์สื่อสารที่ทันสมัย สื่อสังคมออนไลน์ (Social media) คลาวน์คอมพิวติ้ง (Cloud computing) และแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring your own device : BYOD) เข้ามามีบทบาทต่อการดำเนินธุรกิจในปัจจุบัน ความเสี่ยงทางธุรกิจที่พบมากเป็นอันดับต้นๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่ได้คำนึงถึงการรักษาความปลอดภัยของข้อมูลในระดับที่เพียงพอควบคู่กันไปด้วย

"การใช้งานระบบสารสนเทศอย่างแพร่หลายในชีวิตประจำวันทำให้เกิดการคาบเกี่ยวของการใช้งานอุปกรณ์ไอทีสำหรับการทำงานและเรื่องส่วนตัว ซึ่งถือเป็นโจทย์ใหญ่ขององค์กรหลายแห่งทั่วโลกในปัจจุบัน ว่าจะมีวิธีบริหารจัดการอย่างไรเพื่อให้การทำงานแบบเคลื่อนที่ หรือแนวคิดแบบ BYOD ที่สามารถเรียกใช้ข้อมูลจากที่ไหน เมื่อไหร่ก็ได้ ตามที่ต้องการ มีความปลอดภัยและป้องกันการสูญหายของข้อมูลได้มากที่สุด"

ผลสำรวจพบว่า มีบริษัทมากเกือบครึ่ง หรือ 47% ทั่วโลกที่มีการใช้ระบบคลาวน์คอมพิวติ้ง แต่ในทางตรงกันข้าม มีเพียง 18% ที่มีโซลูชันรักษาความปลอดภัยข้อมูลบนระบบคลาวด์

"จริงอยู่ที่เราจะเห็นบริษัทส่วนใหญ่มีการนำระบบป้องกันความปลอดภัยข้อมูลที่รู้จักกันดีมาใช้ในปัจจุบัน ไม่ว่าจะเป็นการใช้วีพีเอ็น (VPN), การตั้งค่าไฟร์วอล (Firewall) หรือการป้องกันข้อมูลด้วยการเอนคริปชันเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Encryption of desktop PCs) แต่นั่นยังไม่เพียงพอ มีบริษัทเพียงน้อยรายเท่านั้นที่มีการนำเอาเครื่องมือตรวจสอบข้อมูลและเครือข่ายที่สามารถวิเคราะห์ความเสี่ยงแบบเรียลไทม์ (Real-time) มาใช้ควบคู่ไปด้วย"

ขณะที่มองว่าอุปสรรคสำคัญในการปรับปรุงระบบความปลอดภัยของข้อมูลองค์กรทั่วโลกมีอยู่ด้วยกัน 3 ประการ ได้แก่ ความขาดแคลนของแหล่งเงินทุน ความเข้าใจที่ไม่เพียงพอของภาคธุรกิจที่มีผลกระทบต่อความปลอดภัยข้อมูลสารสนเทศในระยะยาว และการขาดวิสัยทัศน์หรือการสนับสนุนอย่างจริงจังจากผู้นำ ได้แก่ ซีอีโอ ผู้บริหารระดับสูง ไปจนถึงคณะกรรมการบริษัท

ส่วนแนวโน้มที่จะเกิดขึ้นเร็วๆ นี้คือ ภาคธุรกิจไทย ต้องทบทวนบทบาทและหยุดนำแนวคิดเก่าๆ ในการรักษาความปลอดภัยข้อมูลมาใช้กับองค์กรของตน เอกชนไทยต้องมีการปรับกลยุทธ์โดยหันมาให้ความสำคัญต่อเทคโนโลยีสารสนเทศเพื่อสร้างความได้เปรียบทางธุรกิจ ขยายฐานลูกค้า และหาตลาดใหม่ๆ ในยามที่ทุกคนกำลังเตรียมความพร้อมก่อนการเปิดเออีซี