ประชาชาติธุรกิจ

23 มกราคม 2557
แหล่งที่มา: เว็บไซต์ Prachachart Turakij
http://www.prachachat.net/news_detail.php?newsid=1390448479

ภัยคุกคามข้อมูลทั่วโลกพุ่ง 25% เตือนองค์กรไทยรับมืออาชญากรไซเบอร์

บริษัท PwC ประเทศไทย (ไพร้ซวอเตอร์เฮาส์คูเปอร์ส) เปิดเผยถึงผลสำรวจจากผู้บริหารกว่า 9,600 ราย เกี่ยวกับสถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2557 ว่า ปัญหาภัยคุกคามข้อมูลสารสนเทศ (Information Security) มีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในระยะ 2-3 ปีข้างหน้า

หลังผลสำรวจพบว่าจำนวนภัยคุกคามความปลอดภัยข้อมูล และไซเบอร์ไครมทั่วโลกขยายตัวสูงขึ้นถึง 25% ในปีที่ผ่านมา แม้ภาคธุรกิจจะมีการลงทุนเพิ่มเพื่อพัฒนาระบบ และมีบริษัทเพียง 17% เท่านั้นที่มีมาตรฐานการรักษาความปลอดภัยข้อมูลอยู่ในระดับสูงอย่างแท้จริง

“วิไลพร ทวีลาภพันทอง” หุ้นส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) กล่าวว่า จำนวนภัยคุกคามข้อมูลสารสนเทศ และไซเบอร์ไครมทั่วโลกในปีผ่านมามีจำนวนเพิ่มขึ้นเป็น 3,741 เหตุการณ์ หรือเติบโต 25% จากปีก่อน

"ในขณะที่ความเสียหายทางการเงิน (Financial Losses) ที่เกิดจากภัยคุกคามข้อมูลองค์กรก็เติบโตในทิศทางเดียวกัน โดยปรับตัวเพิ่มขึ้น 18% โดยเฉลี่ยในช่วงเดียวกันของปีก่อน"

“งบฯลงทุนค่าใช้จ่ายด้านการรักษาความปลอดภัยข้อมูล (Information Security Budget) องค์กรทั่วโลก มีมูลค่าเฉลี่ยที่ 4.3 ล้านเหรียญสหรัฐ โดยปรับตัวสูงขึ้นอย่างมีนัยสำคัญจากปีก่อนถึง 51% อย่างไรก็ดี งบฯลงทุนด้านนี้คิดเป็นสัดส่วนเพียง 3.8% ของงบฯลงทุนด้านไอทีทั้งหมด”

“เราจะเห็นได้ว่าจำนวนภัยคุกคามข้อมูลสารสนเทศ และไซเบอร์ไครมทั่วโลกมีการปรับตัวเพิ่มขึ้นเรื่อย ๆ แม้ว่าภาคธุรกิจจะมีการลงทุนทางด้านนี้เพิ่มเติมในช่วงที่ผ่านมา ที่ไม่เพียงจะสะท้อนให้เห็นว่าการรักษาความปลอดภัยที่ไม่ได้ประสิทธิภาพ ประกอบกับการใช้กลยุทธ์ที่ล้าสมัย ถือเป็นปัจจัยถ่วงที่ทำให้องค์กรทั่วโลกส่วนใหญ่มีการบริหารจัดการความปลอดภัยข้อมูลอย่างไม่ตรงจุด และเป็นที่มาของความเสี่ยงทางธุรกิจที่เพิ่มขึ้น”

นอกจากนั้น “วิไลพร” ยังกล่าวอีกว่า ผู้บริหารบริษัททั่วโลกส่วนใหญ่ที่เราทำการสำรวจ ยังคงมีการประเมินตัวเองที่สูงเกินไปหลาย ๆ คนคิดว่าตนมีระบบความปลอดภัยข้อมูลที่รัดกุมเพียงพอ แต่เป็นที่น่าสนใจว่ามี 30% ของผู้บริหารเหล่านี้ล้วนมาจากองค์กรขนาดใหญ่ที่มีรายได้มากกว่า 1 พันล้านเหรียญทั้งสิ้น

ที่สำคัญ ผลสำรวจยังพบข้อมูลที่น่าสนใจอีกว่าจำนวนของบริษัทที่ไม่รู้ว่ามีภัยคุกคามข้อมูลเกิดขึ้นกับบริษัทของตน ปรับตัวเพิ่มขึ้นเป็น 2 เท่าในช่วง 2 ปีผ่านมา สะท้อนให้เห็นว่ามีบริษัทอยู่เป็นจำนวนมากที่ใช้กลยุทธ์ในการป้องกันความปลอดภัยข้อมูลที่ล้าสมัย และมีผู้บริหารที่ทำการสำรวจทั่วโลกเพียง 17% เท่านั้นที่มีคุณสมบัติเข้าข่ายการเป็นผู้นำความปลอดภัยข้อมูลอย่างแท้จริง (True Information Security Leaders)

ผลจากการสำรวจระบุว่า อินไซเดอร์ (Insider) หรือบรรดากลุ่มผู้ใช้ข้อมูลภายใน ได้แก่ พนักงานบริษัทในปัจจุบัน (31%) และพนักงานเก่าของบริษัท (27%) มีแนวโน้มที่จะประกอบการโจรกรรมข้อมูลภายในองค์กรมากที่สุด

ขณะเดียวกัน ผู้บริหารถึง 32% มองว่าแฮกเกอร์ (Hacker) เป็นอาชญากรข้อมูลนอกองค์กรอันดับ 1 ตามด้วยคู่แข่ง (14%), อาชญากรรมแบบมีการวางแผน และจัดการล่วงหน้า หรือออร์แกไนซ์ไครม (12%), กลุ่มนักเคลื่อนไหว นักต่อต้าน (10%), ผู้ก่อการร้าย (8%) และอื่น ๆ

ผลจากการสำรวจระบุว่า อินไซเดอร์ (Insider) หรือบรรดากลุ่มผู้ใช้ข้อมูลภายใน ได้แก่ พนักงานบริษัทในปัจจุบัน (31%) และพนักงานเก่าของบริษัท (27%) มีแนวโน้มที่จะประกอบการโจรกรรมข้อมูลภายในองค์กรมากที่สุด

ขณะเดียวกัน ผู้บริหารถึง 32% มองว่าแฮกเกอร์ (Hacker) เป็นอาชญากรข้อมูลนอกองค์กรอันดับ 1 ตามด้วยคู่แข่ง (14%), อาชญากรรมแบบมีการวางแผน และจัดการล่วงหน้า หรือออร์แกไนซ์ไครม (12%), กลุ่มนักเคลื่อนไหว นักต่อต้าน (10%), ผู้ก่อการร้าย (8%) และอื่น ๆ

ดังนั้น เมื่อมองแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศ (Information Security Spending) ในแต่ละภูมิภาคทั่วโลกพบว่าเทรนด์การใช้จ่ายเพื่อการลงทุนด้านความปลอดภัยข้อมูลของผู้บริหารในทวีปอเมริกาใต้ และเอเชีย-แปซิฟิก มีความร้อนแรง แซงหน้าธุรกิจในแถบอเมริกาเหนือและยุโรป ที่ยังคงเผชิญกับการชะลอตัวทางเศรษฐกิจ และการฟื้นตัวอย่างช้า ๆ จากปัญหาวิกฤตหนี้

ดังจะเห็นว่ามีผู้บริหารบริษัทในเอเชียถึง 60% ที่ยังคงความมั่นใจในการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลองค์กรในระยะข้างหน้า เปรียบเทียบกับ 61% ในปีก่อน แม้ตัวเลขจะลดลงนิดหน่อย แต่ยังถือว่าเป็นทวีปที่มีอัตราสูงสุดเป็นอันดับสองรองจากทวีปอเมริกาใต้ที่ 66% และนำหน้ายุโรปที่ 46% และอเมริกาเหนือที่ 38% ตามลำดับ

ทางด้าน "ศิระ อินทรกำธรชัย" ประธานกรรมการบริหาร บริษัท PwC ประเทศไทยกล่าวเสริมว่า ในยุคที่นวัตกรรมไอทีไม่ว่าจะอุปกรณ์สื่อสารที่ทันสมัย สื่อสังคมออนไลน์ (Social Media) คลาวด์คอมพิวติ้ง (Cloud Computing) และแนวคิดของการนำอุปกรณ์สื่อสารส่วนตัวมาใช้ในการทำงาน (Bring Your Own Device : BYOD) เข้ามามีบทบาทต่อการดำเนินธุรกิจในปัจจุบัน

"ความเสี่ยงทางธุรกิจที่พบมากเป็นอันดับต้น ๆ คือการรับเอาเทคโนโลยีมาใช้โดยไม่คำนึงถึงการรักษาความปลอดภัยของข้อมูลในระดับที่เพียงพอควบคู่กันไปด้วย โดยการใช้งานระบบสารสนเทศอย่างแพร่หลายในชีวิตประจำวัน ทำให้เกิดการคาบเกี่ยวของการใช้งานอุปกรณ์ไอทีสำหรับการทำงานและเรื่องส่วนตัว"

"ซึ่งถือเป็นโจทย์ใหญ่ขององค์กรหลายแห่งทั่วโลกในปัจจุบันว่าจะมีวิธีบริหารจัดการอย่างไร เพื่อให้การทำงานแบบเคลื่อนที่หรือแนวคิดแบบ BYOD ที่สามารถเรียกใช้ข้อมูลจากที่ไหน เมื่อไหร่ก็ได้ ตามที่ต้องการ มีความปลอดภัย และป้องกันการสูญหายของข้อมูลได้มากที่สุด"

นอกจากนั้น ผลสำรวจยังพบว่ามีบริษัทเกือบครึ่ง หรือ 47% ทั่วโลกมีการใช้ระบบคลาวด์คอมพิวติ้ง แต่ในทางตรงกันข้าม มีเพียง 18% ที่มีโซลูชั่นรักษาความปลอดภัยข้อมูลบนระบบคลาวด์

"จริงอยู่ที่เราจะเห็นบริษัทส่วนใหญ่มีการนำระบบป้องกันความปลอดภัยข้อมูลที่รู้จักกันดีมาใช้ในปัจจุบัน ไม่ว่าจะเป็นการใช้วีพีเอ็น (VPN), การตั้งค่าไฟร์วอล (Firewall) หรือการป้องกันข้อมูลด้วยการเอ็นคริปชั่นเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Encryption of Desktop PCs) แต่นั่นยังไม่เพียงพอ เพราะมีบริษัทเพียงน้อยรายเท่านั้น ที่มีการนำเอาเครื่องมือตรวจสอบข้อมูลและเครือข่าย ที่สามารถวิเคราะห์ความเสี่ยงแบบเรียลไทม์ (Real-time) มาใช้ควบคู่กันไปด้วย"

ดังนั้น เมื่อมองไปข้างหน้า "ศิระ" จึงบอกว่าอุปสรรคสำคัญในการปรับปรุงระบบความปลอดภัยของข้อมูลองค์กรทั่วโลกมีอยู่ด้วยกัน 3 ประการ ได้แก่ ความขาดแคลนของแหล่งเงินทุน, ความเข้าใจที่ไม่เพียงพอของภาคธุรกิจที่มีผลกระทบต่อความปลอดภัยข้อมูลสารสนเทศในระยะยาว และการขาดวิสัยทัศน์ หรือการสนับสนุนอย่างจริงจังจากผู้นำ ได้แก่ ซีอีโอ, ผู้บริหารระดับสูง ไปจนถึงคณะกรรมการบริษัท

"ผมจึงมองว่าเรื่องนี้เป็นเรื่องจำเป็นสำหรับภาคธุรกิจไทย ที่จะต้องทบทวนบทบาท และหยุดนำแนวคิดเก่า ๆ ในการรักษาความปลอดภัยข้อมูลมาใช้กับองค์กรของตน ขณะที่ภาคเอกชนไทยต้องมีการปรับกลยุทธ์ โดยหันมาให้ความสำคัญกับเทคโนโลยีสารสนเทศเพื่อสร้างความได้เปรียบทางธุรกิจ เพื่อขยายฐานลูกค้า และหาตลาดใหม่ ๆ ในยามที่เราทุกคนกำลังเตรียมความพร้อมก่อนการเปิดเออีซี"

“นอกจากนี้ ผู้บริหารระดับสูงยังจะต้องเร่งสร้าง Awareness ในเรื่องการรักษาความปลอดภัยข้อมูลให้เกิดแก่พนักงาน, ลูกจ้าง และ Stakeholder อื่น ๆ รวมถึงการปลูกฝังจริยธรรมในการเผยแพร่ข้อมูล ซึ่งถือเป็นต้นทุนที่สำคัญของบริษัทออกไปภายนอก”

ถึงจะทำให้องค์กรต่าง ๆ รับมือกับอาชญากรไซเบอร์ในอนาคตได้