ประชาชาติธุรกิจ
PRACHACHAT ONLINE

วันที่ 6 กุมภาพันธ์ 2556 เวลา 13:20:34 น.
ที่มา http://www.prachachat.net/news_detail.php?newsid=1360132831&grpid=03&catid=no&subcatid=0000

ไพร้ซวอเตอร์ฯ ชี้ภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามพุ่ง แนะเอกชนไทยเตรียมรับมือ

PwC เผยผลสำรวจ Global State of Information Security ชี้ภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามพุ่ง ส่งผลต่อความเสี่ยงทางธุรกิจ แนะเอกชนไทยเร่งปรับตัวรับมือ AEC

ภาคธุรกิจทั่วโลกต้องตื่นตัวและตระหนักถึง ภัยคุกคามข้อมูลสารสนเทศ เพื่อลดปัญหาการสูญเสียของทรัพย์สินและรักษาการเติบโตของกำไร บริษัทไทยต้องเร่งปรับกลยุทธ์และมีนโยบายการรักษาความปลอดภัยของข้อมูลที่ชัดเจน เพื่อรับมือกับการเปิดประชาคมเศรษฐกิจอาเซียนที่กำลังจะมาถึง คาดแนวโน้มภัยมืดการจารกรรรมข้อมูลทะยานต่อในอีก 12 เดือนข้างหน้า

ปัญหาภัยคุกคามข้อมูลสารสนเทศ (Information security) มีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในระยะข้างหน้า หลังผลสำรวจ PwC ชี้มีบริษัททั่วโลกเพียงร้อยละ 8 ที่มีมาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศอยู่ในเกณฑ์มาตรฐานระดับสูงอย่างแท้จริง จากการสำรวจผู้บริหารกว่า 9,300 ราย ภาคธุรกิจและรัฐบาลไทยเอง ต้องหันมาตื่นตัวในการแก้ปัญหาพร้อมมีมาตรการในการรักษาความปลอดภัยของข้อมูลอย่างจริงจังและเป็นระบบ เพื่อสร้างศักยภาพในการแข่งขันและเตรียมพร้อมก่อนการเปิดประชาคมเศรษฐกิจอาเซียนในปลายปี '58

PwC ประเทศไทย (ไพร้ซวอเตอร์เฮาส์คูเปอร์ส) เปิดเผยถึงผลสำรวจ สถานะความปลอดภัยข้อมูลสารสนเทศทั่วโลก ประจำปี 2556 The Global State of Information Security® Survey 2013 ว่า มีผู้บริหารด้านไอทีทั่วโลกถึงร้อยละ 68 ที่มั่นใจว่าธุรกิจของตนมีการบริหารจัดการข้อมูลสารสนเทศที่รัดกุมและมีประสิทธิภาพ อีกทั้งมีผู้บริหารถึงร้อยละ 42 ที่หลงคิดว่าองค์กรของตนมีการประยุกต์ใช้กลยุทธ์และการวางแผนระบบรักษาความปลอดภัยข้อมูลที่ดีเลิศ อยู่ในอันดับต้นๆ หรือที่เรียกว่า Front runners

ทั้งนี้ PwC ให้คำจำกัดความของคำว่า Front runners หรือ 'องค์กรที่มีความมั่นคงด้านความปลอดภัยข้อมูล' โดยวัดจากบริษัทที่มีการดำเนินการในด้านต่าง ๆ ประกอบไปด้วย การมีกลยุทธ์การรักษาความปลอดภัยข้อมูลสารสนเทศของบริษัทที่ครอบคลุม มีผู้บริหารฝ่ายรักษาความปลอดภัยด้านข้อมูล (Chief Information Security Officer : CISO) หรือเทียบเท่ารายงานตรงต่อซีอีโอ ประธานเจ้าหน้าที่บริหารฝ่ายการเงิน ประธานเจ้าหน้าที่บริหารฝ่ายปฏิบัติการ หรือผู้ให้คำปรึกษาทางด้านกฎหมาย มีการวัดผลและประเมินประสิทธิภาพของระบบรักษาความปลอดภัยอย่างสม่ำเสมอ และมีความรู้ความเข้าใจอย่างถ่องแท้ถึงประเภทของภัยคุกคามข้อมูลสารสนเทศต่าง ๆ ที่เกิดขึ้น

นางสาววิไลพร ทวีลาภพันทอง หุ้นส่วนสายงานธุรกิจที่ปรึกษา PwC ประเทศไทย กล่าวว่ากระแสของภัยคุกคามข้อมูลสารสนเทศที่เพิ่มขึ้นทั่วโลก (Rise in global security incidents) การปรับลดงบประมาณเพื่อการรักษาความปลอดภัยบนระบบสารสนเทศ (Diminished budgets) และโปรแกรมการรักษาความปลอดภัยที่ไม่ได้ประสิทธิภาพ (Degrading security programmes) ล้วนเป็นปัจจัยสำคัญที่ทำให้ธุรกิจทั่วโลกส่วนใหญ่ บริหารจัดการความปลอดภัยข้อมูลสารสนเทศ อย่างไม่ตรงจุด ขาดประสิทธิภาพและเป็นที่มาของความเสี่ยงทางธุรกิจที่เพิ่มมากขึ้นในปัจจุบัน

“ผลสำรวจพบว่าองค์กรทั่วโลกส่วนใหญ่มีการประเมินตัวเองสูงเกินไป หลายๆคนคิดว่า ตนมีระบบความปลอดภัยด้านข้อมูลสารสนเทศที่เพียงพอและรัดกุมแล้ว ซึ่งในความเป็นจริงไม่ได้เป็นเช่นนั้น ยิ่งผู้ประกอบการประเมินความเสี่ยงในเรื่องนี้ต่ำเกินไป ก็จะยิ่งเป็นการเปิดช่องโหว่ให้ธุรกิจเกิดความเสี่ยงจากการประพฤติมิชอบ ไม่ว่าจะเป็นการทุจริต ฉ้อโกง การจารกรรมข้อมูลสำคัญของบริษัท ก่อให้เกิดความเสียหายเป็นมูลค่ามหาศาล ในยามที่แนวโน้มภัยคุกคามข้อมูลสารสนเทศจะพัฒนาไปในทิศทางที่รุนแรงและซับซ้อนมากขึ้นในอีก 3-4 ปีข้างหน้า,” นางสาววิไลพรกล่าว

ผลสำรวจยังพบว่า มีผู้บริหารทั่วโลกไม่ถึงครึ่งหรือ เพียงร้อยละ 45 ที่มีแผนเพิ่มงบประมาณในการลงทุนด้านระบบข้อมูลสารสนเทศในระยะ 12 เดือนข้างหน้า โดยลดลงจากร้อยละ 51 และร้อยละ 52 ในปี 2555 และ 2554 ตามลำดับ และถึงแม้ว่าจำนวนของเหตุการณ์ภัยคุกคามจะทะยานสูงขึ้นเรื่อย ๆ ก็ตาม

นางสาววิไลพรกล่าวเสริมว่า “ปัจจัยสำคัญอันดับแรกที่ดูเหมือนจะส่งผลต่อการลดหรือเพิ่มงบใช้จ่ายด้านความปลอดภัยข้อมูลสารสนเทศในความเห็นของบรรดาผู้บริหารส่วนใหญ่ หรือ 46 เปอร์เซ็นต์ ได้แก่ สภาพแวดล้อมทางเศรษฐกิจ แทนที่จะเป็นการตระหนักถึงความสำคัญของการรักษาความปลอดภัยข้อมูล จริงอยู่ว่าเราคงไม่อยากใช้จ่ายเงิน หรือลงทุนอะไรในยามที่เศรษฐกิจไม่ดี แต่อย่าลืมว่า มิจฉาชีพสมัยนี้มีกลโกงที่ซับซ้อน และไม่หยุดนิ่งอยู่กับที่ หากเรามัวแต่คิดว่าเศรษฐกิจไม่ดี ไม่ลงทุนอย่างเดียว จะยิ่งตามเขาไม่ทัน และยิ่งทำให้เกิดผลเสียในระยะยาวมากขึ้น จะได้ไม่คุ้มเสีย เพราะฉะนั้นผู้ประกอบการจำเป็นที่จะต้องจับอันดับความสำคัญในประเด็นนี้ให้ถี่ถ้วน”

นอกจากนี้ สิ่งน่ากังวลอีกประการหนึ่งที่พบจากผลสำรวจ คือ ความเข้มงวดในการใช้เทคโนโลยีเพื่อปกป้องระบบสารสนเทศจากสิ่งที่ไม่พึงประสงค์ต่างๆ อาทิ สปายแวร์ (Spyware) แอดแวร์ (Adware) มัลแวร์ (Malware) โทรจัน (Trojan) หรือไวรัสต่างๆ ที่ลดจำนวนลงอย่างเห็นได้ชัด ซึ่งคาดว่า เป็นผลมาจากการประหยัดงบประมาณ เพื่อให้สอดคล้องกับสภาพเศรษฐกิจในช่วงที่ผ่านมา

เอเชียขึ้นแท่นผู้นำด้านงบลงทุนความปลอดภัยข้อมูลปี ’56

อย่างไรก็ดี เมื่อมองแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศ (Information security spending) ในแต่ละภูมิภาคทั่วโลกจะพบว่า เทรนด์การใช้จ่ายเพื่อลงทุนด้านความปลอดภัยข้อมูลสารสนเทศของผู้บริหารในภูมิภาคเอเชียมีความร้อนแรง แซงหน้าธุรกิจในแถบอเมริกาเหนือ และยุโรป ที่ยังคงเผชิญกลับการชะลอตัวทางเศรษฐกิจและวิกฤตหนี้

“บริษัทในเอเชียถึง 61 เปอร์เซ็นต์ที่ทำการสำรวจคาดจะมีการลงทุนเพิ่มเพื่อพัฒนาความปลอดภัยข้อมูลสารสนเทศในอีก 12 เดือนข้างหน้า เปรียบเทียบกับ 74 เปอร์เซ็นต์ในปีก่อน ซึ่งถึงแม้จะลดลง แต่ก็ยังถือว่าเป็นทวีปที่มีอัตราสูงสุดเป็นอันดับสองรองจากทวีปอเมริกาใต้ที่ 63 เปอร์เซ็นต์และนำหน้ายุโรปที่ 43 เปอร์เซ็นต์และอเมริกาเหนือที่ 34 เปอร์เซ็นต์ ตามลำดับ,” นางสาววิไลพรกล่าว

“นอกจากนี้ เรายังพบว่า บริษัทในเอเชียยังมีแนวโน้มที่จะเพิ่มงบด้านความปลอดภัยข้อมูลสารสนเทศในเรื่อง Business continuity และการฟื้นฟูธุรกิจหลังเกิดภัยพิบัติมากกว่าประเทศเพื่อนบ้านอีกด้วย”

ท่ามกลางกระแสของยุค ‘บิ๊ก ดาต้า’ (Big data) หรือ การผสมผสานเทคโนโลยีระดับสูงเพื่อบริหารจัดการข้อมูลองค์กรที่มีขนาดใหญ่และมีความซับซ้อน ให้สามารถจัดเก็บและสำรองข้อมูล รวมทั้งนำข้อมูลดังกล่าวมาใช้ให้เกิดประโยชน์กับธุรกิจได้อย่างมีประสิทธิภาพ ผลจากการสำรวจพบว่า องค์กรส่วนใหญ่ทุกวันนี้มีระบบการจัดเก็บข้อมูลที่หละหลวม ไม่มีประสิทธิภาพเปรียบเทียบกับปีที่ผ่านมา ยกตัวอย่าง เช่น มีผู้ทำการสำรวจเพียงร้อยละ 35 ที่มีการจัดเก็บข้อมูลส่วนตัวของพนักงานและลูกค้าอย่างถูกวิธี และมีเพียงร้อยละ 31 ที่มีการกำหนดความสามารถในการเข้าถึงและการใช้งานกับฐานข้อมูลอย่างเป็นระบบ

“ข้อมูลกลายเป็น commodity ที่สำคัญขององค์กร ซึ่งเทรนด์นี้จะยิ่งเติบโตและมีความซับซ้อนมากขึ้น ทำให้บริษัทต่างๆต้องเริ่มมองหาระบบที่เข้ามาช่วยจัดการกับสตอเรจ สิ่งที่ธุรกิจหลายแห่งเผชิญเหมือนกัน คือมีปริมาณข้อมูลมากขึ้น แต่งบประมาณสำหรับการบริหารข้อมูลกลับไม่สูงตามไปด้วย” นางสาววิไลพรกล่าว “บิ๊ก ดาต้า จะยิ่งส่งผลให้ผู้ประกอบการโดยเฉพาะบ้านเรา ต้องทบทวนบทบาทของระบบวิเคราะห์ข้อมูล เพื่อกลั่นกรองข้อมูลเชิงลึก เพื่อสร้างความได้เปรียบทางธุรกิจ และหาตลาดใหม่ ๆ ในยามที่ทุกภาคส่วนต่างเตรียมความพร้อม ก่อนการเปิดประชาคมเศรษฐกิจอาเซียน” นางสาววิไลพรกล่าว

ผลสำรวจยังระบุว่า ความเสี่ยงที่พบในยุคที่นวัตกรรมไอทีมีผลต่อการดำเนินธุรกิจขององค์กรส่วนใหญ่ในปัจจุบัน คือ การรับเอาเทคโนโลยี ไม่ว่าจะเป็น อุปกรณ์สื่อสารที่ทันสมัย สื่อสังคมออนไลน์ (Social media) และคลาวน์คอมพิวติ้ง (Cloud computing) มาใช้เร็วเกินไปโดยไม่ได้คำนึงถึงความปลอดภัยของข้อมูลสารสนเทศเป็นอันดับแรก มีผู้บริโภคถึงร้อยละ 88 ที่มีการใช้โทรศัพท์เคลื่อนที่เพื่อประโยชน์ของหน้าที่การงานและเรื่องส่วนตัว แต่ในทางตรงกันข้าม มีธุรกิจไม่ถึงครึ่ง (ร้อยละ 45) ที่สามารถจำแนกการใช้โทรศัพท์ส่วนตัวออกจากเรื่องงาน นอกจากนี้ มีเพียงร้อยละ 37 ที่มีการติดตั้งเทคโนโลยีเพื่อป้องกันภัยคุกคามประเภทมัลแวร์ (Malware) ในเครื่องมือถือ

“หากจะให้มองแนวโน้มในระยะข้างหน้า เรามองว่า แนวคิดเก่าๆในการรักษาความปลอดภัยข้อมูลบนโลกไอทีนั้นใช้ไม่ได้อีกต่อไป ผู้ประกอบการจำเป็นที่จะต้องหันมาพิจารณาความปลอดภัยของธุรกิจของตนให้มากขึ้น โดยเฉพาะอย่างยิ่ง sector ที่ต้องอาศัย high level of trust อย่างภาคการเงินการธนาคาร และภาคบริการที่ต้องรักษาข้อมูลของลูกค้าหรือความลับทางธุรกิจ เอกชนไทยบ้านเราต้องมีการปรับกลยุทธ์องค์กร โดยหันมาให้ความสำคัญกับเทคโนโลยีสารสนเทศ และหาประโยชน์จากการใช้เทคโนโลยีเหล่านี้เพื่อสามารถวิเคราะห์ข้อมูลได้อย่างถูกต้อง สิ่งเหล่านี้ล้วนเป็นปัจจัยที่ผู้บริหารต้องคิด และ มองไปข้างหน้าพร้อมๆ กัน”