ไอบีเอ็มเผยผลสำรวจ CISO ผู้บริหารด้านการรักษาความปลอดภัยสารสนเทศทั่วโลก พลิกสู่ความรับผิดชอบด้านกลยุทธ์ทางธุรกิจ ตามวิวัฒนาการของ CIO และ CFO

กรุงเทพ – 11 มิถุนายน 2555 : ไอบีเอ็มเผยผลการศึกษา CISO (Chief Information Security Executives) ผู้นำและหน่วยงานด้านความปลอดภัยของระบบ มีวิวัฒนาการที่ชัดเจน โดย 25% ของการสำรวจหัวหน้าฝ่ายความปลอดภัยข้อมูลขยับจากการมุ่งเน้นด้านเทคโนโลยีสู่บทบาทการเป็นผู้นำเชิงกลยุทธ์ทางธุรกิจ

จากบทวิเคราะห์การประเมินประธานเจ้าหน้าที่บริหารด้านการรักษาความปลอดภัยสารสนเทศของไอบีเอ็มปี 2012” ของศูนย์ศึกษาเพื่อการประยุกต์ใช้บทวิเคราะห์ของไอบีเอ็ม (IBM Center for Applied Insights) ได้รวมเอาหน่วยงานที่ครอบคลุมอุตสาหกรรมที่หลากหลายและรวมข้อมูลจาก 7 ประเทศ ระหว่างไตรมาสแรกของปี 2012 ได้จัดให้มีการสัมภาษณ์ผู้บริหารด้านไอทีและธุรกิจระดับอาวุโส 138 คน ซึ่งมีหน้าที่รับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศในองค์กร เกือบ 20% เป็นผู้นำของหน่วยงานด้านการรักษาความปลอดภัยสารสนเทศในองค์กรขนาดใหญ่ที่มีพนักงานมากกว่า 10,000 คน และ 55% ปฏิบัติงานอยู่ในองค์กรขนาดใหญ่ที่มีพนักงาน 1,000-9,999 คน

นางเจษฎา ไกรสิงขร กรรมการ รองกรรมการผู้จัดการใหญ่ ธุรกิจซอฟต์แวร์ บริษัท ไอบีเอ็ม ประเทศไทย กล่าวว่า “ภาพรวมของผู้นำด้านการรักษาความปลอดภัยระบบในปัจจุบัน คือการตกอยู่ภายใต้แรงกดดันมหาศาล เพราะมีหน้าที่ต้องดูแลปกป้องสินทรัพย์ที่มีคุณค่ามากที่สุดของบริษัท ไม่ว่าจะเป็น เงิน ข้อมูลของลูกค้า ทรัพย์สินทางปัญญา และตราสินค้า เกือบสองในสามของผู้บริหารด้านการรักษาความปลอดภัยสารสนเทศระดับสูง ระบุว่าผู้บริหารระดับอาวุโส ต่างหันมาให้ความสนใจในเรื่องการรักษาความปลอดภัยข้อมูลมากกว่าเมื่อสองปีก่อน ด้วยข่าวคราวของการเจาะระบบแบบขั้นสูงและการรั่วไหลของข้อมูลทำให้พวกเขาเห็นความสำคัญว่า การรักษาความปลอดภัยระบบเป็นสิ่งที่จำเป็นต้องมีอยู่ในองค์กรธุรกิจสมัยใหม่ มากกว่าครึ่งของผู้ตอบคำถามยกให้เรื่องความปลอดภัยสำหรับอุปกรณ์สื่อสารแบบพกพาเป็นเทคโนโลยีที่ต้องให้ความสำคัญมากที่สุดในตลอดช่วงสองปีที่ผ่านมา เกือบสองในสามของกลุ่มผู้ให้ข้อมูลคาดว่าจะมีการใช้จ่ายด้านการรักษาความปลอดภัยสารสนเทศเพิ่มมากขึ้นกว่าช่วงสองปีที่

ผ่านมา และ 87% ของกลุ่มนี้คาดว่าการใช้จ่ายดังกล่าวจะเพิ่มขึ้นในอัตราที่เป็นตัวเลขสองหลัก”

นอกจากการตอบสนองต่อเหตุการณ์เฉพาะในเรื่องความปลอดภัยระบบแล้ว บทบาทของ CISO ยังขยับไปสู่เรื่องของการบริหารความเสี่ยงแบบองค์รวมและเป็นอัจฉริยะมากขึ้น – เปรียบได้กับการสู้กับเพลิงไหม้ ไปเป็นการเตรียมตัวป้องกันและบรรเทาต้นเหตุก่อนที่จะเกิดเพลิงไหม้จริง

ลักษณะขององค์กรที่ให้ความสำคัญในการรักษาความปลอดภัย

- **มองการรักษาความปลอดภัยเป็นสิ่งจำเป็นทางธุรกิจ** หนึ่งในคุณลักษณะผู้นำของหน่วยงานชั้นนำคือ ให้ความใส่ใจในผู้นำธุรกิจและคณะกรรมการ เรื่องการรักษาความปลอดภัยไม่ใช่หัวข้อที่เร่งด่วน แต่เป็นส่วนหนึ่งในการหารือทางธุรกิจเป็นประจำ และยิ่งไปกว่านั้นคือเป็นเหมือนวัฒนธรรมขององค์กร 60% ขององค์กรที่มีความก้าวหน้ายกให้เรื่องความปลอดภัยเป็นหัวข้อประจำในการประชุมคณะกรรมการ เมื่อเทียบกับเพียง 22% ขององค์กรที่มีความก้าวหน้าน้อย ผู้นำเหล่านี้เข้าใจในความจำเป็นที่จะต้องตื่นตัวในเรื่องความเสี่ยงที่เพิ่มสูงขึ้น – และต้องให้ความสำคัญมากขึ้นในระยะยาวในเรื่องการให้ความรู้ทั่วทั้งองค์กร การประสานความร่วมมือ และการสื่อสารซึ่งกันและกัน หน่วยงานที่มีความคิดเรื่องการรักษาความปลอดภัยของระบบที่ล้ำหน้ามีความเป็นไปได้ที่จะจัดตั้งคณะทำงานด้านการรักษาความปลอดภัยระบบขึ้น เพื่อสนับสนุนการไปสู่เป้าหมายอย่างมีระบบในเรื่องนี้ ซึ่งจะขยายไปสู่เรื่องทางกฎหมาย การดำเนินธุรกิจ การเงินและทรัพยากรต่างๆ ของบริษัท 68% ขององค์กรก้าวหน้ามีคณะกรรมการด้านความเสี่ยง เทียบกับกลุ่มองค์กรที่มีความก้าวหน้าน้อยแล้วมีเพียง 26% เท่านั้นที่มีคณะกรรมการด้านนี้

- **ใช้การตัดสินใจและวัดผลจากข้อมูล:** การประเมินผลแสดงให้เห็นว่า องค์กรชั้นนำใช้ระบบการวัดผลในการตรวจสอบความก้าวหน้าคิดเป็นสองเท่า (59% เทียบกับ 26%) ทั้งนี้ การติดตามผลความตื่นตัวของผู้ใช้งาน การให้ความรู้กับพนักงาน ความสามารถในการรับมือกับการคุกคามในอนาคต และการรวมเทคโนโลยีใหม่เข้าด้วยกัน สิ่งเหล่านี้สามารถช่วยสร้างวัฒนธรรมการตื่นตัวเรื่องความเสี่ยงได้ และการตรวจสอบแบบอัตโนมัติของการวัดผลที่เป็นมาตรฐานจะช่วยให้ CISO สามารถทุ่มเทเวลาไปใส่ใจในเรื่องอื่นที่สำคัญได้แทนที่ที่จะต้องคอยดูแลในเรื่องความเสี่ยงแบบเป็นระบบอยู่ตลอดเวลา

- **การแบ่งความรับผิดชอบเกี่ยวกับงบประมาณกับผู้บริหารระดับสูง:** การประเมินแสดงผลว่าองค์กรส่วน

ใหญ่ CIO จะเป็นผู้ที่มีอำนาจการควบคุมงบประมาณด้านความปลอดภัยของระบบสารสนเทศ อย่างไรก็ตาม ในองค์กรที่ถูกจัดอยู่ในลำดับสูงนั้น การอนุมัติการลงทุนมักจะเป็นความรับผิดชอบของผู้นำทางธุรกิจมากกว่า ในกลุ่มองค์กรที่มีความก้าวหน้าสูงสุด CEO จะทำตัวเหมือน CIOในการจัดสรรและชี้นำเรื่องงบประมาณด้านการรักษาความปลอดภัยระบบสารสนเทศ ในขณะที่องค์กรที่ถูกจัดอยู่ในลำดับต่ำกว่ามักจะขาดแคลนงบประมาณ ขาดแคลนกลยุทธ์ และขาดแคลนวิธีการ แบ่งความรับผิดชอบเพื่อไปสู่เป้าหมายเรื่องการรักษาความปลอดภัย จากการศึกษาพบว่า 71% ขององค์กรก้าวหน้าจัดสรรงบประมาณสำหรับการรักษาความปลอดภัย เทียบกับกลุ่มที่องค์กรที่มีความก้าวหน้าน้อยแล้วมีเพียง 27% เท่านั้นที่จัดสรรงบประมาณในด้านนี้

เพื่อที่จะสร้างหน่วยงานด้านการรักษาความปลอดภัยระบบที่มีฝีมือและเป็นที่เชื่อมั่น ผู้นำด้านงานรักษาความปลอดภัยระบบต้องสร้างแผนปฏิบัติงาน (action plan) บนพื้นฐานของความสามารถที่มีอยู่และสิ่งที่จำเป็นมากที่สุดในปัจจุบัน รายงานให้คำแนะนำไว้จากการค้นพบว่า องค์กรสามารถก้าวไปข้างหน้าบนพื้นฐานของระดับวุฒิภาวะในปัจจุบันของตัวองค์กรได้อย่างไร

การรักษาความปลอดภัยระบบในยุคนี้จึงมีความท้าทายใหม่ๆ ให้เห็น แต่เราสามารถแก้ปัญหาสิ่งเหล่านี้ได้ด้วยการจัดทำวิธีปฏิบัติที่เป็นนวัตกรรม และนำเอาวิธีการที่ผสมผสานและเป็นองค์รวมมาใช้งาน CISO ที่ให้ความสำคัญกับกับปัจจัยเหล่านี้เป็นอันดับต้นๆ สามารถช่วยให้องค์กรพัฒนากระบวนการทางธุรกิจให้ดีขึ้นได้เป็นอย่างมาก และบรรลุเป้าหมายการวัดผลความสำเร็จในความก้าวหน้าเรื่องการสร้างวัฒนธรรมความตื่นตัวด้านความเสี่ยง ซึ่งทำให้สามารถรับมือกับการคุกคามในอนาคตได้อย่างว่องไวและครบครัน

ไอบีเอ็มมีระบบการรักษาความปลอดภัยแบบครบวงจร (End-to-end) ที่เตรียมการรักษาความปลอดภัยแบบอัจฉริยะเอาไว้ เพื่อช่วยองค์กรธุรกิจให้ปกป้องบุคลากร ข้อมูล แอพลิเคชั่น และโครงสร้างพื้นฐานได้แบบองค์รวม ไอบีเอ็มมีผลิตภัณฑ์ที่เกี่ยวข้องกับการรักษาความปลอดภัย สำหรับบริหารจัดการการเข้าถึงและระบุตัวตน การจัดการเหตุการณ์และความปลอดภัยสารสนเทศ ความปลอดภัยของฐานข้อมูล การพัฒนาแอพลิเคชั่น การบริหารความเสี่ยง การจัดการเครื่องปลายทาง ความปลอดภัยบนระบบเครือข่าย รวมทั้งบริการที่เกี่ยวข้องทั้ง บริการการจัดการความปลอดภัย (Managed Security Services) บริการให้คำปรึกษา (Consulting Security Services) และงานวิจัยไอบีเอ็มเอ็กซ์-ฟอร์ซ (IBM X-Force) ซึ่งเป็นรายงานประจำปีที่ทำอย่างต่อเนื่องเพื่อประเมินภาพรวมสถานการณ์ด้านความปลอดภัยต่อภัยคุกคามทางออนไลน์ นอกจากนี้ไอบีเอ็มยังมีหน่วยงานที่เป็นศูนย์ปฏิบัติการงานวิจัยและพัฒนาด้านการรักษาความปลอดภัยระบบที่ใหญ่ที่สุดในโลกและมีหน่วยงานในการส่งมอบ ซึ่งประกอบไปด้วยศูนย์ปฏิบัติการด้านการรักษาความปลอดภัย 9 แห่ง ศูนย์วิจัยไอบีเอ็ม 9 แห่ง ห้องทดลองเพื่อพัฒนา

ซอฟต์แวร์ด้านการรักษาความปลอดภัย 11 แห่ง และสถาบันด้านการรักษาความปลอดภัยขั้นสูงอยู่ในสหรัฐอเมริกา ยุโรป และเอเชียแปซิฟิก ไอบีเอ็มคอยตรวจสอบเหตุการณ์ด้านความปลอดภัยถึง 13 พันล้านรายการต่อวันในกว่า 130 ประเทศทั่วโลก และเป็นเจ้าของสิทธิบัตรด้านความปลอดภัยมากกว่า 3,000 รายการ ด้วยพัฒนาการและนวัตกรรมด้านการรักษาความปลอดภัยมานานกว่า 40 ปี ไอบีเอ็มจึงเปี่ยมไปด้วยความรอบรู้และเชี่ยวชาญอย่างลึกซึ้งในด้านการวิจัย การบริการ และการให้คำปรึกษาในด้านการรักษาความปลอดภัย เพื่อช่วยให้องค์กรต่างๆมีความเข้าใจและสามารถป้องกันภัยคุกคามในธุรกิจได้ดียิ่งขึ้น

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยระบบของไอบีเอ็ม สามารถเข้า ไปเยี่ยมชมได้ที่: www.ibm.com/security.