รายงานเผย ผลกระทบด้านการเงิน จากการรั่วไหลของข้อมูลส่วนตัว ต่อองค์กรธุรกิจในเอเชียแปซิฟิกและญี่ปุ่น

รายงานไอดีซี สนับสนุนการจัดทำโดยเดลล์ อีเอ็มซี ชี้ชัด
การรักษาความปลอดภัย ความเป็นส่วนตัว และความต่อเนื่องทางธุรกิจ
คือปัจจัยสำคัญอันดับต้น ที่ช่วยลดความเสี่ยงจากโทษปรับ

สรุปประเด็นสำคัญ
• พบความต่างในวงกว้างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศทั่วทั้งภูมิภาคเอเชียแปซิฟิกที่มีความรุนแรงแตกต่างกันไป โดยมีประเทศสิงคโปร์ ออสเตรเลีย นิวซีแลนด์ เกาหลีใต้ ไต้หวัน อินเดีย และฮ่องกง เป็นกลุ่มประเทศที่มีโทษปรับสูงสุด
• องค์กรข้ามชาติ ต้องมีความเข้าใจอย่างลึกซึ้งเกี่ยวกับการเคลื่อนย้ายข้อมูลข้ามพรมแดน รวมถึงความเป็นส่วนตัวของข้อมูล และกฎระเบียบเรื่องการรักษาความปลอดภัยในทุกตลาด หรือความเสี่ยงที่อาจจะทำให้โดนโทษปรับสำหรับการฝ่าฝืน
• ด้วยผู้ออกกฎมุ่งหวังที่จะดำเนินการตามขั้นตอนเพื่อบังคับใช้งานตามกฎระเบียบดังกล่าว ทำให้องค์กรต้องมีธรรมภิบาลด้านข้อมูล หรือการกำหนดและบังคับใช้งานด้านข้อมูลอย่างจริงจัง พร้อมกับมีกลยุทธ์ในการบริหารจัดการความปลอดภัยเพื่อตอบโจทย์ของการนำเข้าและจัดเก็บข้อมูล

ไอดีซี อินโฟบรีฟ (IDC InfoBrief) บารอมิเตอร์ด้านการบริหารจัดการความเสี่ยงข้อมูล เพื่อการประเมินศักยภาพของเอเชียแปซิฟิก จัดทำโดย ไอดีซี องค์กรที่มีความรู้ด้านการตลาดทั่วโลก สำหรับเดลล์ อีเอ็มซี เผยถึง ความรุนแรงของโทษปรับที่เป็นตัวเงินสำหรับการฝ่าฝืนกฎหมายความเป็นส่วนตัวด้านข้อมูลในตลาดสำคัญๆ ทั่วภาคพื้นเอเชียแปซิฟิกและญี่ปุ่น ซึ่งผลการรายงานจากไอดีซีที่ได้มีการเปิดเผย เน้นให้เห็นว่าทั้ง สิงคโปร์ ออสเตรเลีย และฮ่องกง เป็นตลาดหลักที่มีบทลงโทษรุนแรงที่สุดสำหรับการรั่วไหลของข้อมูล โดยคิดเป็นอัตราส่วนการปรับตามจีดีพี ในขณะที่ญี่ปุ่น อินเดีย และประเทศไทย อยู่อันดับท้ายๆ

เนื่องจากมีภัยคุกคามเกิดใหม่ในแต่ละวัน จึงทำให้กฎระเบียบและข้อบังคับเริ่มรุนแรงมากขึ้น เพื่อให้มั่นใจว่าองค์กรจะจัดการกับข้อมูลได้อย่างมีความรับผิดชอบ ในการวัดเรื่องของการบังคับใช้และโทษปรับสำหรับการรั่วไหลของข้อ

มูล IDC InfoBrief เผยให้เห็นถึงความแตกต่างอย่างมากในโทษปรับทั่วตลาดทั้ง 14 แห่งในเอเชียแปซิฟิกและญี่ปุ่น โดยได้เน้นให้เห็นถึงความสำคัญสำหรับองค์กรธุรกิจ โดยเฉพาะอย่างยิ่ง องค์กรข้ามชาติ ว่าควรตระหนักถึงข้อแตกต่างเรื่องกฎหมายความเป็นส่วนตัวของข้อมูลในแต่ละตลาดที่ทำธุรกิจ

ในตลาดเอเชียแปซิฟิกและญี่ปุ่นมีการบังคับใช้งานตามกฎหมายแตกต่างกันเป็นอย่างมาก โดยรัฐบาลประเทศสิงคโปร์ ได้กำหนดค่าปรับสูงถึง 1,000,000 ดอลลาร์สิงคโปร์ สำหรับผู้ที่ดำเนินการไม่สอดคล้องตามบทบัญญัติการคุ้มครองข้อมูล ในขณะที่ประเทศออสเตรเลีย กำหนดค่าปรับสูงถึง 1,700,000 ดอลลาร์ออสเตรเลีย ทั้งนี้ประเทศญี่ปุ่น และอินเดียมีการเรียกเก็บค่าปรับต่ำที่สุดคือ 1,000,000 เยน และ 500,000 รูปีอินเดีย ตามลำดับ สำหรับการรั่วไหลของข้อมูลส่วนตัว และเนื่องจากองค์กรทั่วภูมิภาคเริ่มก้าวสู่ระบบดิจิทัล เรื่องนี้จึงกลายเป็นประเด็นสำคัญมากยิ่งขึ้น

“การขับเคลื่อนด้วยข้อมูล เป็นสิ่งที่หลีกเลี่ยงไม่ได้สำหรับองค์กรที่กำลังปฏิรูปไปสู่ดิจิทัล องค์กรธุรกิจต่างตระหนักดีถึงโอกาสในการนำข้อมูลมาใช้ได้อย่างมีประสิทธิภาพเพื่อปฏิรูปสินค้า การบริการ รวมถึงกลยุทธ์ แต่ในขณะที่องค์กรเหล่านี้ ได้ประโยชน์จากการใช้ข้อมูลสร้างโอกาสใหม่ๆ ขณะเดียวกันก็มีความเสี่ยงมากขึ้น เพราะพื้นที่การโจมตีขยายตัวมากขึ้น รวมถึงข้อเรียกร้องให้องค์กรต้องมีการบริหารจัดการข้อมูลที่ดี” ดมิทริ เฉิน รองประธานฝ่ายขายประจำภาคพื้นเอเชียแปซิฟิกและญี่ปุ่น เดลล์ อีเอ็มซี “ประเด็นนี้ก่อให้เกิดการสร้างสภาพแวดล้อมด้านไอทีที่ปลอดภัยและขยายขีดความสามารถได้ รวมถึงการใช้ระบบโครงสร้างพื้นฐานได้อย่างเหมาะสมตามข้อเรียกร้องที่องค์กรปัจจุบันไม่สามารถหลีกเลี่ยงได้”

บารอมิเตอร์ของ ไอดีซี ยังเน้นให้เห็นถึงการเปลี่ยนแปลงกฎระเบียบอันนำมาซึ่งโอกาสสำหรับธุรกิจในการขับเคลื่อนไปสู่การบริหารจัดการข้อมูลได้ดียิ่งขึ้น ไซมอน พิฟฟ์ รองประธาน ฝ่ายธุรกิจด้านการรักษาความปลอดภัยไอที ของไอดีซี เอเชียแปซิฟิก ได้ให้ความเห็นว่า “กฎระเบียบด้านความเป็นส่วนตัวของข้อมูลนับเป็นแรงกระตุ้นไปสู่การพัฒนากลยุทธ์ด้านการจัดการข้อมูลที่ดียิ่งขึ้น อย่างเช่น ช่วยลดช่องว่างการปกป้องข้อมูลในระบบโครงสร้างแบ็กอัพที่ใช้อยู่ ทั้งนี้ ตลอดระยะเวลาที่ผ่านมา หลายประเทศในภูมิภาคจะดำเนินการตามขั้นตอนในเชิงรุกเพื่อสร้างความแข็งแกร่งให้กับระบบโครงสร้างข้อมูลสำคัญ และร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปก็จะยังคงกระตุ้นเรื่องนี้ต่อไป”

เนื่องจากกฎระเบียบต่างๆ ได้พัฒนาเพื่อสะท้อนให้เห็นถึงความเปลี่ยนแปลงในภาพรวมเกี่ยวกับภัยคุกคาม ไอดีซี อินโฟบรีฟ จึงได้ชี้ให้เห็นถึง 3 ประเด็นหลักที่การบริหารจัดการข้อมูลที่ดีช่วยลดความเสี่ยงได้ คือการรักษาความปลอดภัย ควาเป็นส่วนตัว และความต่อเนื่องทางธุรกิจ ทั้งนี้ในการรักษาความปลอดภัยต้องมั่นใจได้ว่าจะมีการนำเข้าและจัดเก็บข้อมูลอย่างปลอดภัยเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูล (data integrity) ส่วนเรื่องความเป็นส่วนตัวต้องมั่นใจได้ว่าข้อมูลที่ใช้ระบุตัวตนนั้นมีความปลอดภัย ให้ความสามารถในการเข้าถึง และให้ความสามารถในการลบทิ้งได้ในระดับที่เหมาะสม ตามที่กฎระเบียบในร่างต่างๆ ได้กำหนดไว้ การวางแผนเรื่องความ

ต่อเนื่องทางธุรกิจและการบริหารจัดการความเสี่ยงควรต้องอำนวยความสะดวกในการเข้าถึงข้อมูลได้ตลอดเวลาเช่นกัน ดั้งนั้นการพิจารณาระบบโครงสร้างไอทีต้องให้ความสำคัญกับเรื่องเหล่านี้เพื่อมั่นใจถึงการดำเนินการที่สอดคล้องตามกฎระเบียบ

แหล่งข้อมูลเพิ่มเติม

- ไมโครไซต์: Data Risk Management Barometer
- เดลล์ อีเอ็มซี บล็อก: Shifts in Legislative Compliance and Its Impact to Enterprise IT
- ข้อมูลผลิตภัณฑ์: Dell EMC Data Protection and Security solutions