งานวิจัยเดลล์ เทคโนโลยีส์ เผย การโจมตีทางไซเบอร์ และเหตุฉุกเฉินที่เพิ่มสูงขึ้น ส่งผลกระทบองค์กรในภูมิภาคเอเชียแปซิฟิกที่สำรวจถึง 84 เปอร์เซ็นต์

Dell Technologies Global Data Protection Index 2020 Snapshot ชี้ให้เห็นความท้าทายหลักที่ส่งผลต่อความพร้อมในการปกป้องข้อมูล

ประเด็นข่าวโดยสรุป

 องค์กรในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่นจัดการข้อมูลโดยเฉลี่ยเป็นจำนวน 13.31 เพตาไบท์ ซึ่งเป็นจำนวนที่เพิ่มขึ้นอย่างน่าตกใจ 693 เปอร์เซ็นต์จากปี 2016
 ค่าใช้จ่ายทั้งหมดโดยประมาณของการสูญเสียข้อมูลเพิ่มขึ้นเป็นจำนวนมากกว่า 1.3 ล้านดอลลาร์สหรัฐต่อหนึ่งองค์กรในช่วง 12 เดือนที่ผ่านมาโดยเฉลี่ย
 มากกว่าครึ่งหนึ่งขององค์กรทั้งหมดต่างพยายามที่จะค้นหาโซลูชันด้านการปกป้องข้อมูลที่เพียงพอสำหรับเทคโนโลยีเกิดใหม่ต่างๆ อาทิ 5G และโครงสร้างพื้นฐานสำหรับเอดจ์ (75 เปอร์เซ็นต์) และ AI กับ ML แพลตฟอร์ม (72 เปอร์เซ็นต์)

ผลวิจัยดัชนีการปกป้องข้อมูลทั่วโลก 2020 ของเดลล์ เทคโนโลยีส์ หรือ Global Data Protection Index 2020

Snapshot เผยให้เห็นว่าองค์กรในเอเชียแปซิฟิกและญี่ปุ่นโดยเฉลี่ยกำลังจัดการข้อมูลที่มากกว่าที่เคยเป็นในช่วงปีที่ผ่านมา 64 เปอร์เซ็นต์ ด้วยการเพิ่มสูงขึ้นของข้อมูลทำให้เกิดความท้าทายอย่างไม่อาจเลี่ยงได้ ผู้ตอบแบบสอบถามส่วนใหญ่ (77 เปอร์เซ็นต์) รายงานว่าโซลูชันการปกป้องคุ้มครองข้อมูลในปัจจุบันจะไม่สามารถตอบโจทย์ความต้องการในทางธุรกิจในอนาคตได้ทั้งหมด รายงานสรุปดังกล่าวซึ่งเป็นดัชนีการป้องกันข้อมูลทั่วโลกที่จัดทำขึ้นในทุกสองปี ได้ทำการสำรวจผู้มีอำนาจตัดสินใจด้านไอทีจำนวน 1,000 คนใน 15 ประเทศที่อยู่ในองค์กรภาครัฐ และองค์กรเอกชนที่มีพนักงานกว่า 250 คน เพื่อศึกษาเกี่ยวกับผลกระทบของความท้าทายต่างๆ และเทคโนโลยีชั้นสูงมีต่อความพร้อมในด้านการปกป้องข้อมูล จากจำนวนผู้มีอำนาจตัดสินใจด้านไอทีทั้งหมด 1,000 คน หนึ่งในสี่มาจากภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น การค้นพบในระดับภูมิภาคยังแสดงให้เห็นถึงความคืบหน้าในเชิงบวกจากจำนวน 75 เปอร์เซ็นต์ขององค์กรในภูมิภาคในปี 2019 สูงขึ้นจากจำนวน 74 เปอร์เซ็นต์ในปี 2018 – ที่มองข้อมูลในฐานะสินทรัพย์ที่มีค่า และกำลังวางแผนที่จะดึงมูลค่าของข้อมูลออกกมาหรือกำลังวางแผนที่จะทำเช่นนั้นในอนาคต

“ข้อมูลคือสิ่งที่มีความสำคัญอย่างยิ่งต่อธุรกิจและเป็นกุญแจที่จะไขไปสู่การปฏิรูปทางดิจิทัลขององค์กร” เบธ ฟาเลน ประธาน ด้านการปกป้องข้อมูลของ เดลล์ เทคโนโลยีส์ กล่าว “เมื่อเราเข้าสู่ทศวรรษหน้าของข้อมูล (next data decade) กลยุทธ์การปกป้องข้อมูลที่ยืดหยุ่น เชื่อถือได้และทันสมัย คือสิ่งสำคัญที่ช่วยให้ธุรกิจสามารถตัดสินใจได้อย่างชาญฉลาดยิ่งขึ้น รวดเร็วมากขึ้น รวมทั้งจัดการกับผลกระทบจากการดิสรัปชั่นที่มีราคาแพง”

“การเติบโตอย่างมหาศาลของข้อมูลผสานเข้ากับมูลค่าของข้อมูลที่เพิ่มสูงขึ้นกำลังสร้างให้เกิดโอกาสต่างๆ ขึ้นเป็นจำนวนมาก แต่ก็ยังสร้างความเสี่ยงใหม่ๆ ให้เกิดขึ้นจากการที่องค์กรต้องรับมือกับการที่ว่าจะปกป้องข้อมูลได้อย่างน่าเชื่อถือและยั่งยืนได้อย่างไร อเล็กซ์ เล่ย รองประธาน โซลูชันด้านการปกป้องข้อมูล เดลล์ เทคโนโลยีส์ ภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น กล่าว “จากการที่มูลค่าข้อมูลขององค์ กรระดับเอนเทอร์ไพรส์เพิ่มสูงขึ้น มูลค่าของการสูญเสียข้อมูลก็เพิ่มมากขึ้นอย่างเห็นได้ชัด ในปี 2020 และปีถัดไปๆ องค์กรที่ใช้ประโยชน์จากความสามารถในการจัดการข้อมูลและการป้องกันที่ครอบคลุมในสภาพแวดล้อมแบบมัลติ-แพลตฟอร์ม และมัลติ-คลาวด์ จะได้รับการเตรียมพร้อมเพื่อลดความเสี่ยงใหม่ๆ ที่เกิดขึ้น กระตุ้นการพัฒนานวัตกรรม รวมทั้งลดต้นทุนรวมในการเป็นเจ้าของ (TCO) ตลอดจนเพิ่มประสิทธิภาพสูงสุดให้กับผลลัพธ์ในการดำเนินธุรกิจ

เหตุฉุกเฉินและภัยภิบัติที่เพิ่มสูงขึ้นในอัตราที่น่าตกใจ
จากการศึกษาพบว่าองค์กรในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น กำลังจัดการข้อมูลจำนวนถึง 13.31 เพตาไบต์ (PB)ซึ่งเพิ่มขึ้น 64 เปอร์เซ็นต์จากจำนวนเฉลี่ย 8.13 เพตาไบต์ (PB) ในปี 2018 และเป็นจำนวนเพิ่มขึ้น 693 เปอร์เซ็นต์จากการจัดการข้อมูลจำนวน 1.6 เพตาไบต์ขององค์กรในปี 2016 ภัยคุกคามที่ใหญ่ที่สุดต่อข้อมูลทั้งหมดนี้ดูเหมือนจะเป็นการเพิ่มจำนวนสูงขึ้นของเหตุฉุกเฉินและภัยพิบัติ (disruptive events) ต่างๆ ทั้งจากการโจมตีทางไซเบอร์ไปจนถึงการสูญหายของข้อมูล และการเกิดการหยุดการทำงานของระบบ (system downtime) องค์กรส่วนใหญ่ (84 เปอร์เซ็นต์ในปี 2019 เมื่อเทียบกับ 80 เปอร์เซ็นต์ในปี 2018) ได้รับความเสียหายจากเหตุฉุกเฉินเหล่านี้ในช่วง 12 เดือนที่ผ่านมา นอกจากนี้ จำนวนอีก 70 เปอร์เซ็นต์หวาดกลัวว่าองค์กรของพวกเขาจะประสบเหตุ

การฉุกเฉินนี้ในอีก 12 เดือนข้างหน้า

ยิ่งไปกว่านั้นคือการค้นพบว่าองค์กรที่ใช้ผู้ให้บริการปกป้องข้อมูลมากกว่าหนึ่งรายนั้นมีความเสี่ยงมากกว่าเกือบสี่เท่าด้านความปลอดภัยบนไซเบอร์ที่ป้องกันการเข้าถึงข้อมูล (42 เปอร์เซ็นต์ขององค์กรที่ใช้ผู้ให้บริการสองรายหรือมากกว่ากับ 11 เปอร์เซ็นต์ของผู้ใช้ผู้ให้บริการเพียงรายเดียว) แต่การใช้ผู้ให้บริการด้านการปกป้องข้อมูลจำนวนหลายหลายกำลังเพิ่มขึ้น 83 เปอร์เซ็นต์จากการที่องค์กรเลือกที่จะใช้โซลูชันด้านการปกป้องข้อมูลจากผู้ให้บริการมากกว่าสองราย คิดเป็นจำนวนเพิ่มขึ้น 25 เปอร์เซ็นต์จากปี 2016

ค่าใช้จ่ายของดิสรัปชั่นยังเพิ่มขึ้นในอัตราที่น่าตกใจ ต้นทุนโดยเฉลี่ยของการหยุดทำงานหรือ downtime ในช่วง 12 เดือนที่ผ่านมาพุ่งสูงขึ้นขึ้น 61% จากปี 2018 ถึง 2019 ส่งผลต่อการประมาณมูลค่าต้นทุนรวมอยู่ที่ 794,308 ดอลลาร์สหรัฐในปี 2019 เพิ่มขึ้นจาก 494,869 ดอลลาร์สหรัฐในปี 2018 ขณะเดียวกัน ค่าใช้จ่ายโดยประมาณของการสูญเสียข้อมูลเพิ่มขึ้นจาก 939,703 ดอลลาร์สหรัฐในปี 2018 เป็น 1,301,524 ดอลลาร์สหรัฐในปี 2019 โดยเฉลี่ย โดยค่าใช้จ่ายเหล่านี้เพิ่มสูงขึ้นอย่างมีนัยยะสำคัญสำหรับองค์กรที่ใช้ผู้ให้บริการปกป้องข้อมูลมากกว่าหนึ่งรายโดยมีค่าใช้จ่ายที่เกี่ยวข้องกับการหยุดทำงานของระบบสูงขึ้นเกือบสี่เท่า และเกือบ 12 เท่าสำหรับค่าใช้จ่ายในการสูบเสียของข้อมูลโดยเฉลี่ย

เทคโนโลยีเกิดใหม่ ความท้าทายสำหรับโซลูชันการปกป้องข้อมูล
จากการที่เทคโนโลยีเกิดใหม่ หรือ emerging technologies ยังคงก้าวหน้าและเป็นตัวกำหนดภูมิทัศน์ดิจิทัล องค์กรต่างกำลังเรียนรู้วิธีการใช้เทคโนโลยีเหล่านี้เพื่อผลลัพธ์ทางธุรกิจที่ดีขึ้น การศึกษาระบุว่าองค์กรผู้ตอบแบบสอบถามในภูมิภาคเอเชียแปซิฟิกเกือบทั้งหมดกำลังลงในเทคโนโลยีใหม่หรือเทคโนโลยีที่กำลังจะเกิดขึ้นในห้าอันดับแรก (top 5) ดังนี้ 1) แอปพลิเคชันคลาวด์ หรือ cloud-native applications (64 เปอร์เซ็นต์) 2) ซอฟต์แวร์ในรูปแบบการบริการ (software-as-a-service: SaaS) (58 เปอร์เซ็นต์) 3) ปัญญาประดิษฐ์ (AI) และแชชีน เลิร์นนิ่ง (ML) (50 เปอร์เซ็นต์) 4) 5G และโครงสร้างพื้นฐานคลาวด์ เอดจ์ (49 เปอร์เซ็นต์) และ 5) อินเทอร์เน็ต ออฟ ธิงส์/เอ็นด์ พ้อยต์ (end point) (45 เปอร์เซ็นต์)

ถึงกระนั้นสามในสี่ (75 เปอร์เซ็นต์) ของผู้ตอบแบบสอบถามเชื่อว่าเทคโนโลยีเกิดใหม่เหล่านี้สร้างความซับซ้อนในการป้องกันข้อมูลให้มากขึ้นในขณะที่ 72 เปอร์เซ็นต์ระบุว่าเทคโนโลยีเกิดใหม่ก่อให้เกิดความเสี่ยงต่อการปกป้องข้อมูล นอกจากนี้ มากกว่าครึ่งของผู้ที่ใช้เทคโนโลยีเกิดใหม่ต่างพยายามค้นหาโซลูชันการปกป้องข้อมูลที่เพียงพอสำหรับเทคโนโลยีทั้งหลายเหล่านี้ อันได้แก่

- 5G และโครงสร้างพื้นฐานคลาวด์ เอดจ์ (75 เปอร์เซ็นต์)
- แพลตฟอร์ม AI และ ML (72 เปอร์เซ็นต์)
- คลาวด์-เนทิฟ แอปพลิเคชัน (64 เปอร์เซ็นต์)
- อินเทอร์เน็ต ออฟ ธิงส์/เอ็นด์ พ้อยต์ (59 เปอร์เซ็นต์)

- กระบวนการอัตโนมัติในหุ่นยนต์ (56 เปอร์เซ็นต์)

การศึกษายังพบว่า 77 เปอร์เซ็นต์ของผู้ตอบแบบสอบถามเชื่อว่าโซลูชันการปกป้องข้อมูลที่มีอยู่เดิมขององค์กรของพวกเขาจะไม่สามารถตอบสนองความท้าทายทางธุรกิจในอนาคตได้ทั้งหมด โดยผู้ตอบแบบสอบถามระบุความไม่มั่นใจในส่วนต่างๆ ดังนี้:

- การ กู้คืนข้อมูลจากการโจมตีบนไซเบอร์ (70 เปอร์เซ็นต์)
- การกู้คืนข้อมูลจากเหตุการณ์การสูญหายของข้อมูล (66 เปอร์เซ็นต์)
- การทำตามกฎระเบียบของการกำกับดูแลข้อมูลในระดับภูมิภาค (65 เปอร์เซ็นต์)
- การทำตามวัตถุประสงค์ตามระดับการให้บริการสำรองและกู้คืนข้อมูล (60 เปอร์เซ็นต์)

การปกป้องข้อมูลผนึกกำลังเข้ากับคลาวด์

องค์กรธุรกิจตอบรับรูปแบบการผสมผสานการใช้งานคลาวด์รูปแบบต่างๆ เข้าด้วยกันเมื่อมีการใช้งานแอปพลิเคชันทางธุรกิจใหม่ๆ และเพื่อปกป้องเวิร์กโหลดต่างๆ อาทิ คอนเทนเนอร์ แอปพลิเคชันคลาวด์-เนทิฟและแอปพลิเคชันซอฟต์แวร์ในรูปแบบการบริการ (SaaS) ผลการวิจัยแสดงให้เห็นว่าองค์กรผู้ตอบแบบสอบถามในภูมิภาคเอเชียแปซิฟิคชื่นชอบการใช้งานพับบลิคคลาวด์/SaaS (46 เปอร์เซ็นต์), ไฮบริดคลาวด์ (38 เปอร์เซ็นต์) และไพรเวทคลาวด์ (36 เปอร์เซ็นต์) เนื่องจากสภาพแวดล้อมการใช้งานแอปพลิเคชันที่ใหม่กว่าเช่นนี้ ขณะเดียวกัน 76 เปอร์เซ็นต์ขององค์กรที่สำรวจระบุว่าเป็นข้อบังคับหรือเป็นสิ่งที่สำคัญอย่างยิ่งสำหรับผู้ให้บริการการปกป้องข้อมูลที่จะให้การปกป้องแอปพลิเคชันคลาวด์-เนทิฟ

จากการที่มีการเคลื่อนย้ายของข้อมูล ทั้งที่ผ่านไปจากหรืออยู่โดยรอบสภาพแวดล้อมของเอจด์ ผู้ตอบแบบสอบถามจำนวนมากกล่าวว่าต้องการการสำรองข้อมูลบนระบบคลาวด์มากกว่า โดย 60 เปอร์เซ็นต์ระบุเป็นไพรเวทคลาวด์ และ59 ต้องการพับบลิคคลาวด์เนื่องจากแนวทางในการจัดการและปกป้องข้อมูลของพวกเขาสร้างขึ้นในพื้นที่ของเอจด์ (edge locations)