GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

13 พฤษภาคม 2024

ความคิดเห็นของ GDA ต่อคณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติของประเทศไทย

มาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระบบคลาวด์

Global Data Alliance (GDA)[1]
ยินดีที่ได้มีโอกาสแสดงความคิดเห็นต่อประกาศของคณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ
เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระบบคลาวด์ (*ต่อไปนี้เรียกว่า* "นโยบายการรักษาความปลอดภัยบนคลาวด์")[2]

GDA เป็นกลุ่มพันธมิตรข้ามอุตสาหกรรม ซึ่งมีสำนักงานใหญ่ทั่วเอเชีย ยุโรป และซีกโลกตะวันตก
โดยมีความมุ่งมั่นต่อมาตรฐานความรับผิดชอบด้านข้อมูลในระดับสูง
และอาศัยความสามารถในการเข้าถึงและถ่ายโอนข้อมูลข้ามพรมแดนเพื่อสร้างนวัตกรรมและสร้างงานต่าง ๆ GDA
สนับสนุนนโยบายที่ช่วยปลูกฝังความไว้วางใจในเศรษฐกิจดิจิทัล ในขณะเดียวกันก็ปกป้องความสามารถในการถ่ายโอนข้อมูลข้ามพรมแดน
และระงับการเรียกร้องข้อกำหนดด้านการเก็บข้อมูลไว้ในประเทศที่จำกัดการค้า

บริษัทสมาชิกของ GDA มีบทบาทในหลายภาคส่วนของเศรษฐกิจประเทศไทย สมาชิก GDA
ร่วมกันสนับสนุนการจ้างงานหลายแสนตำแหน่ง การลงทุนหลายร้อยล้านดอลลาร์ รวมถึงกิจกรรมเพื่อพัฒนานวัตกรรม
และการพัฒนาเศรษฐกิจในประเทศไทย

GDA สนับสนุนนโยบายการรักษาความปลอดภัยบนคลาวด์ของประเทศไทยในหลายแง่มุม
แต่แนะนำให้ประเทศไทยทำการสำรวจแนวทางอื่นสำหรับโครงสร้างพื้นฐานคลาวด์และข้อบังคับการเก็บข้อมูลไว้ในประเทศที่พบในที่นี้[3]

ความคิดเห็นและข้อเสนอแนะโดยรวม

GDA
สนับสนุนเป้าหมายของประเทศไทยในการปรับปรุงการรักษาความปลอดภัยและความสมบูรณ์บนคลาวด์ผ่านนโยบายการรักษาความปลอดภัยบนคลาวด์ GDA ยังสนับสนุนการนำมาตรฐานสากลของประเทศไทยไปปรับใช้ในนโยบายการรักษาความปลอดภัยบนคลาวด์ GDA
ยื่นเสนอให้พิจารณาด้วยความเคารพว่านโยบายการรักษาความปลอดภัยบนคลาวด์จะมีประสิทธิภาพสูงสุด
หากสะท้อนถึงความรับผิดชอบร่วมกันระหว่างลูกค้าที่ใช้บริการคลาวด์ของรัฐบาลไทยและผู้ให้บริการคลาวด์ในด้านการใช้แนวทางปฏิบัติที่ดีที่สุดเพื่อจัดการความเสี่ยงและปรับปรุงความยืดหยุ่นของคลาวด์

ในเวลาเดียวกัน GDA
กังวลว่านโยบายการรักษาความปลอดภัยบนคลาวด์ดูเหมือนจะมีข้อบังคับในการจัดเก็บข้อมูลในเครื่องที่จะขัดต่อเป้าหมายที่ระบุไว้ของนโยบายในการปรับปรุงการรักษาความปลอดภัย GDA ยังกังวลเกี่ยวกับข้อกำหนดที่ระบุว่าเซิร์ฟเวอร์สำรองควรอยู่ใน: (1) ประเทศไทย (2) ที่อื่น ๆ ในเอเชียตะวันออกเฉียงใต้ หรือ (3) ฮ่องกง จีน

ดัชนีชี้วัดระบบการประมวลผลแบบคลาวด์ (รายงานระดับโลกที่จัดอันดับความพร้อมของประเทศต่าง ๆ
สำหรับการนำไปปรับใช้และการเติบโตของบริการประมวลผลแบบคลาวด์) อธิบายว่า:

> บริการคลาวด์จะให้บริการข้ามพรมแดนระดับชาติ
> และความสำเร็จขึ้นอยู่กับการเข้าถึงตลาดระดับภูมิภาคและระดับโลก
> นโยบายเข้มงวดที่สร้างอุปสรรคทางการค้าที่เกิดขึ้นจริงหรือที่อาจเกิดขึ้นจะขัดขวางหรือชะลอวิวัฒนาการของการประมวลผลแบบคลาวด์[4]

เราขอแนะนำด้วยความเคารพว่าควรปรับปรุงนโยบายการรักษาความปลอดภัยบนคลาวด์เพื่อรองรับศักยภาพสูงสุดของการประมวลผลแบบคลาวด์โดยใช้แนวทางที่มีความยืดหยุ่น ส่งเสริมความเป็นส่วนตัวและการรักษาความปลอดภัย ตลอดจนช่วยให้องค์กรต่าง ๆ
ในประเทศไทยได้รับประโยชน์จากการเข้าถึงข้ามพรมแดนในโครงสร้างพื้นฐานและเทคโนโลยีที่ดีที่สุดที่ให้บริการบนคลาวด์
โดยเฉพาะอย่างยิ่ง เราขอแนะนำให้ประเทศไทยทำการสำรวจแนวทางอื่นในข้อบังคับการจัดเก็บข้อมูลที่พบในร่างนโยบาย

การอภิปราย

นโยบายการรักษาความปลอดภัยบนคลาวด์ประกอบด้วยข้อกำหนดต่อไปนี้ที่กำหนดให้มีการจัดตั้ง “ศูนย์ข้อมูลหลัก” ในประเทศไทย และ “ศูนย์ข้อมูลสำรอง” ในประเทศไทย เขตบริหารพิเศษฮ่องกง หรือที่อื่น ๆ ในเอเชียตะวันออกเฉียงใต้ โดยเฉพาะอย่างยิ่ง ข้อย่อย 5.2.5 มีการระบุไว้ดังต่อไปนี้:

> 5.2.5 การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม
> 5.2.5.1 ตำแหน่งที่ตั้งของศูนย์ข้อมูล (ตำแหน่งที่ตั้งศูนย์ข้อมูล)
>
> ผู้ใช้บริการคลาวด์
>
> ก) ควรใช้ศูนย์ข้อมูลหลักในประเทศไทย (การเก็บข้อมูลไว้ในประเทศ)
>
> ผู้ให้บริการคลาวด์
>
> ก) ควรจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (การเก็บข้อมูลไว้ในประเทศ)
>
> ข) ควรจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (การเก็บข้อมูลไว้ในประเทศ)
> หรือในเอเชียตะวันออกเฉียงใต้ที่ใกล้เคียงกับการใช้งานหลักของผู้ใช้บริการคลาวด์มากที่สุด รวมถึงเขตปกครองพิเศษฮ่องกง

GDA
มีความกังวลหลายประการเกี่ยวกับความเสี่ยงด้านการปฏิบัติงานและการรักษาความปลอดภัยที่เกี่ยวข้องกับโครงสร้างพื้นฐานนี้และข้อบังคับการเก็บข้อมูลไว้ในประเทศ โดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับวัตถุประสงค์ด้านการรักษาความปลอดภัยทางไซเบอร์ของประเทศไทย
และความสนใจในโครงสร้างพื้นฐานการประมวลผลแบบคลาวด์ที่ปลอดภัย
และการเริ่มต้นใช้งานเทคโนโลยีที่ผู้ให้บริการคลาวด์ให้การสนับสนุน

ข้อจำกัดด้านข้อมูลข้ามพรมแดนในร่างนโยบายอาจเป็นอุปสรรคสำหรับเป้าหมายนโยบายสาธารณะที่เกี่ยวข้องกับสุขภาพ ความเป็นส่วนตัว และการรักษาความปลอดภัยของบุคคลในประเทศไทย โดยเราจะกล่าวถึงหัวข้อเหล่านี้ด้านล่าง[5]

- **ผลกระทบต่อนโยบาย ICT:** นโยบาย ICT สามารถช่วยประสานงานการเจรจาระหว่างภาครัฐและเอกชน สนับสนุนการลงทุน และเพิ่มสิทธิประโยชน์สูงสุดของเทคโนโลยี ICT ทั่วทั้งเศรษฐกิจ
  ข้อจำกัดด้านข้อมูลข้ามพรมแดนมักจะเป็นอุปสรรคสำหรับนโยบายเหล่านี้ ตัวอย่างเช่น
  สิทธิประโยชน์ของนโยบายการประมวลผลแบบคลาวด์มีแนวโน้มที่จะเกิดขึ้นในบริบทข้ามพรมแดนที่ช่วยให้สามารถให้บริการทรัพยากรการประมวลผลได้อย่างยืดหยุ่นและปรับขนาดได้ สร้างสมดุลการโหลดที่รวดเร็ว
  และมีความพร้อมในการเข้าถึงเทคโนโลยีที่ดีที่สุดจากทั่วทุกมุมโลก
  การใช้ข้อบังคับการเก็บข้อมูลไว้ในประเทศและข้อจำกัดการถ่ายโอนเพื่อห้ามการเข้าถึงโครงสร้างพื้นฐานและเทคโนโลยีการประมวลผลแบบคลาวด์ข้ามพรมแดน จะตัดสิทธิองค์กรในท้องถิ่น (รวมถึง MSME) และผู้ใช้ดังนี้
    - การเข้าถึงทรัพยากรไอทีข้ามพรมแดนที่จัดตั้งขึ้นในต่างประเทศ
    - ความร่วมมือและสื่อสารข้ามพรมแดนกับพันธมิตรทางธุรกิจต่างประเทศ
    - การทำธุรกรรมต่างประเทศและโอกาสทางธุรกิจ ตลอดจน
    - การปรับปรุงความยืดหยุ่นซึ่งเป็นผลมาจากการจัดเก็บข้อมูลในตำแหน่งที่ตั้งทางภูมิศาสตร์หลายแห่ง[6]

- **ผลกระทบต่อการรักษาความปลอดภัยทางไซเบอร์**:
  บางคนแย้งว่าข้อจำกัดด้านข้อมูลข้ามพรมแดนมีความจำเป็นเพื่อรับรองการรักษาความปลอดภัยทางไซเบอร์ อย่างไรก็ตาม
  *วิธีการ*ปกป้องข้อมูลมีความสำคัญต่อการรักษาความปลอดภัยมากกว่า *สถานที่*จัดเก็บ
  และข้อจำกัดในการถ่ายโอนมักส่งผลให้การรักษาความปลอดภัยทางไซเบอร์*เปราะบางมากขึ้น* ไม่ได้*รัดกุมยิ่งขึ้น*
  การถ่ายโอนข้อมูลข้ามพรมแดนช่วยปรับปรุงการรักษาความปลอดภัยทางไซเบอร์
  เนื่องจากการถ่ายโอนเหล่านี้ทำให้เครื่องมือการรักษาความปลอดภัยทางไซเบอร์สามารถตรวจสอบรูปแบบการรับส่งข้อมูล
  ระบุความผิดปกติ และเปลี่ยนทิศทางภัยคุกคามที่อาจเกิดขึ้นในรูปแบบที่ขึ้นอยู่กับการเข้าถึงข้อมูลแบบเรียลไทม์ทั่วโลก
  การรักษาความปลอดภัยทางไซเบอร์ที่รัดกุมยิ่งขึ้นเกิดขึ้นได้จากการวิเคราะห์ข้อมูลข้ามพรมแดน
  ซึ่งเป็นแนวทางการป้องกันทางไซเบอร์โดยเฉพาะที่มีการประสานงานทั่วทั้งเครือข่ายไอทีและขอบเขตระดับชาติ[7]
  เมื่อรัฐบาลควบคุมการเก็บข้อมูลไว้ในประเทศหรือจำกัดความสามารถในการถ่ายโอนและวิเคราะห์ข้อมูลแบบเรียลไทม์
  จะทำให้เกิดช่องโหว่โดยไม่ได้ตั้งใจ[8] โปรดดูภาคผนวก I สำหรับข้อมูลเพิ่มเติม

- **ผลกระทบต่อความเป็นส่วนตัว**: บางคนแย้งว่าข้อจำกัดข้อมูลข้ามพรมแดนมีความจำเป็นด้วยเหตุผลด้านความเป็นส่วนตัว กล่าวคือ เพื่อให้แน่ใจว่าบริษัทต่าง ๆ ประมวลผลและใช้ข้อมูลที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลของประเทศ ในความเป็นจริง
  องค์กรที่ถ่ายโอนข้อมูลทั่วโลกมักจะใช้ขั้นตอนต่าง ๆ เพื่อตรวจสอบให้แน่ใจว่าข้อมูลได้รับการคุ้มครอง
  แม้ว่าจะถ่ายโอนออกนอกประเทศก็ตาม ด้วยเหตุนี้ องค์กรต่าง ๆ มักจะใช้กลไกการถ่ายโอนข้อมูลที่ได้รับการอนุมัติที่หลากหลาย[9]

- **ผลกระทบต่อการปฏิบัติตามกฎระเบียบ**:
  บางคนอ้างว่าข้อจำกัดข้อมูลข้ามพรมแดนทำให้รัฐบาลสามารถเข้าถึงข้อมูลเพื่อวัตถุประสงค์ด้านกฎระเบียบหรือการสืบสวน
  อย่างไรก็ตาม ตำแหน่งของข้อมูลไม่ใช่ปัจจัยกำหนด ในทางตรงกันข้าม “ข้อกำหนดการเก็บข้อมูลไว้ในประเทศสามารถเพิ่ม...
  ความเสี่ยงด้านการดำเนินงาน ขัดขวางการบริหารความเสี่ยงและการปฏิบัติตามข้อกำหนด
  และขัดขวางการเข้าถึงข้อมูลด้านกฎระเบียบและการกำกับดูแลทางการเงิน” [10] ดังนั้น
  หน่วยงานกำกับดูแลในหลายประเทศจึงสนับสนุนให้มีการถ่ายโอนข้อมูลข้ามพรมแดนอย่างมีความรับผิดชอบ[11] ในทำนองเดียวกัน
  การถ่ายโอนข้อมูลมีความสำคัญต่อลำดับความสำคัญของนโยบายสาธารณะอื่น ๆ รวมถึงการติดตามและป้องกันการฉ้อโกงทางการเงิน
  การป้องกันการฟอกเงิน การต่อต้านการทุจริต และวัตถุประสงค์ด้านการปฏิบัติตามกฎหมายอื่น ๆ

นอกจากนี้ เราทราบว่าตารางที่หน้า 6 มีกรอบแนวคิดที่จัดประเภทบริการคลาวด์เป็นผลกระทบระดับต่ำ ปานกลาง และสูง อย่างไรก็ตาม ไม่มีคำแนะนำที่ชัดเจนว่าแต่ละหน่วยงานจะพิจารณาลักษณะการจัดประเภทที่เหมาะสมอย่างไร
การสร้างความโปร่งใสมากขึ้นเกี่ยวกับวิธีการจัดประเภทดังกล่าวจะเป็นประโยชน์อย่างมาก

เพื่อให้แน่ใจว่าการจัดประเภทมีความสอดคล้องกัน และเพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นในการจัดประเภทที่ต่ำหรือสูงเกินไป นอกจากนี้ เรายังแนะนำให้มีช่องทางในการขอให้ทบทวนหรือพิจารณาการตัดสินใจเกี่ยวกับการจัดประเภทตามข้อมูลที่ได้รับ

เมื่อพิจารณาถึงการจัดประเภทแล้ว การพิจารณาแยกแยะข้อกำหนดการเก็บข้อมูลไว้ในประเทศตามระดับการจัดประเภทอาจมีประโยชน์ ตัวอย่างเช่น ระบบที่อยู่ในกลุ่มการจัดประเภทที่มีผลกระทบต่ำอาจได้รับการยกเว้นสำหรับข้อกำหนดด้านการเก็บข้อมูลไว้ในประเทศ ควรพิจารณาเพื่อจำแนกความแตกต่างของการดูแลที่แตกต่างกันตามประเภทของผู้ให้บริการคลาวด์ (เช่น Infrastructure-as-a-Service, Platform-as-a-Service) โดยอาจไม่จำเป็นต้องควบคุม Software-as-a-Service ซึ่งอาจรวมถึงบริการที่นำเสนอทางอินเทอร์เน็ตอย่างกว้าง ๆ ภายในขอบเขตของข้อกำหนดการเก็บข้อมูลไว้ในประเทศ

คำแนะนำโดยละเอียด

เราขอเสนอคำแนะนำโดยละเอียดดังต่อไปนี้

- **คำแนะนำหลักของเรา** คือให้คณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติของประเทศไทยลบข้อย่อย 5.2.5.1 (ตำแหน่งที่ตั้งศูนย์ข้อมูล) ออกจากนโยบายการรักษาความปลอดภัยบนคลาวด์
- **คำแนะนำทางเลือกของเรา**
  คือให้คณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติของประเทศไทยชี้แจงว่าศูนย์ข้อมูลภายใต้หัวข้อย่อยนี้อาจตั้งอยู่ในเขตเศรษฐกิจใดก็ได้ที่ผู้ให้บริการระบบคลาวด์สามารถดำเนินการได้ตามข้อกำหนดด้านการรักษาความปลอดภัยทางไซเบอร์ ทั้งด้านการดำเนินงานและด้านเทคนิคของคณะกรรมการฯ โดยอ้างอิงตามแผนการจัดการความเสี่ยงที่แสดงให้เห็น

ไม่ว่าในกรณีใด ๆ เราขอเรียกร้องให้คณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติลบการอ้างอิงถึงเขตบริหารพิเศษฮ่องกง เนื่องจากมีความกังวลอย่างกว้าง ๆ เกี่ยวกับการรักษาความปลอดภัยและความสมบูรณ์ของข้อมูล ทั้งจากมุมมองด้านการรักษาความปลอดภัยทางไซเบอร์และจากมุมมองของกระบวนการทางกฎหมาย ซึ่งอยู่ภายใต้เขตอำนาจศาลของสาธารณรัฐประชาชนจีน

บทสรุป

โดยสรุป
เราขอแนะนำด้วยความเคารพให้ประเทศไทยลบโครงสร้างพื้นฐานในท้องถิ่นของร่างนโยบายและข้อบังคับการเก็บข้อมูลไว้ในประเทศออกจากนโยบายการรักษาความปลอดภัยบนคลาวด์ เราขอขอบคุณที่ได้มีโอกาสแบ่งปันมุมมองเหล่านี้ และหวังว่าจะเป็นประโยชน์ในขณะที่ประเทศไทยพิจารณาขั้นตอนถัดไปในร่างนโยบาย โปรดอย่าลังเลที่จะติดต่อเรา หากมีข้อสงสัยใด ๆ เกี่ยวกับการเสนอให้พิจารณานี้

ภาคผนวก

ความสัมพันธ์ระหว่างการรักษาความปลอดภัยทางไซเบอร์และข้อบังคับด้านโครงสร้างพื้นฐานในท้องถิ่น ข้อกำหนดการเก็บข้อมูลไว้ในประเทศ และข้อจำกัดด้านการถ่ายโอนข้อมูลข้ามพรมแดน

ความสามารถในการค้นหาและถ่ายโอนข้อมูลในลักษณะที่ปลอดภัยตามการใช้งานมากที่สุด
คือแนวทางปฏิบัติที่ดีที่สุดในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
ส่วนหนึ่งเป็นเพราะการมองเห็นข้อมูลที่เกี่ยวข้องกับไซเบอร์ข้ามพรมแดนช่วยให้เครื่องมือการรักษาความปลอดภัยทางไซเบอร์สามารถตรวจสอบรูปแบบการรับส่งข้อมูล ระบุความผิดปกติ
และเปลี่ยนทิศทางภัยคุกคามที่อาจเกิดขึ้นในรูปแบบที่ขึ้นอยู่กับการเข้าถึงข้อมูลแบบเรียลไทม์ทั่วโลก นอกจากนี้
บริษัทอาจเลือกที่จะจัดเก็บข้อมูลไว้ในสถานที่ที่มีความหลากหลายทางภูมิศาสตร์เพื่อปิดบังตำแหน่งของข้อมูลและลดความเสี่ยงจากการโจมตีทางกายภาพ เพื่อให้บริษัทสามารถลดเวลาแฝงของเครือข่าย และเพื่อรักษากข้อมูลสำรอง
และการกู้คืนข้อมูลสำคัญหลังจากเกิดความเสียหายทางกายภาพในสถานที่จัดเก็บ ในทางกลับกัน
เมื่อรัฐบาลควบคุมการเก็บข้อมูลไว้ในประเทศหรือจำกัดความสามารถในการถ่ายโอนและวิเคราะห์ข้อมูลแบบเรียลไทม์
จะทำให้เกิดช่องโหว่โดยไม่ได้ตั้งใจ ตามที่สรุปไว้ด้านล่าง

- **การวางแผนการรักษาความปลอดภัยทางไซเบอร์แบบบูรณาการ** ข้อจำกัดด้านการถ่ายโอนข้อมูลและข้อกำหนดการเก็บข้อมูลไว้ในประเทศบังคับให้องค์กรต่าง ๆ ปรับใช้แนวทางแบบไซโลกับข้อมูล ซึ่งมักจะจำกัดตำแหน่งของข้อมูลบางอย่าง แต่ไม่ใช่ทั้งหมด ความแตกต่างนี้ทำให้เกิดความซับซ้อนทางเทคนิคที่ไม่จำเป็น โดยไม่เกิดประโยชน์ใด ๆ ต่อการรักษาความปลอดภัย พูดง่าย ๆ ก็คือ ข้อกำหนดเชิงประดิษฐ์ในการจัดเก็บข้อมูลภายในขอบเขตทำให้บุคลากร กระบวนการ
และเทคโนโลยีที่องค์กรต้องการใช้เพื่อจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ต้องประสบกับปัญหา

- **ความตระหนักรู้ด้านการรักษาความปลอดภัยทางไซเบอร์** ข้อจำกัดด้านการถ่ายโอนข้อมูลและข้อกำหนดการเก็บข้อมูลไว้ในประเทศเป็นอุปสรรคต่อการมองเห็นความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ ไม่เพียงแต่ในระดับภายในและระหว่างองค์กรเท่านั้น แต่ยังรวมถึงระดับชาติและระดับนานาชาติอีกด้วย หากผู้ปกป้องทางไซเบอร์ไม่สามารถเข้าถึงตัวบ่งชี้ภัยคุกคามหรือข้อมูลการรักษาความปลอดภัยทางไซเบอร์อื่น ๆ ที่รวบรวมในเขตอำนาจศาลเดียว การจัดการกับกิจกรรมทางไซเบอร์ที่เป็นอันตรายในเขตอำนาจศาลอื่นจะทำได้ยากขึ้น

- **ความร่วมมือด้านการรักษาความปลอดภัยทางไซเบอร์** ข้อจำกัดด้านการถ่ายโอนข้อมูลและข้อกำหนดการเก็บข้อมูลไว้ในประเทศสามารถขัดขวางการทำงานร่วมกันข้ามพรมแดน การแบ่งปันข้อมูล และการป้องกันเครือข่ายที่มีการประสานงานอื่น ๆ เมื่อข้อจำกัดและข้อกำหนดดังกล่าวแยกผู้ปกป้องเครือข่ายออกจากกัน พวกเขาไม่สามารถใช้ท่าทีการป้องกันที่เป็นเอกภาพและประสานงานกันเพื่อต่อต้านผู้ไม่หวังดีที่ไม่ให้ความสนใจในพรมแดนของประเทศ กล่าวโดยสรุป ข้อจำกัดด้านการถ่ายโอนข้อมูลอาจทำให้ผู้ไม่หวังดีที่ไม่สนใจข้อกำหนดทางกฎหมายในท้องถิ่นมีความได้เปรียบทางโครงสร้างอย่างยั่งยืนมากกว่าผู้ปกป้องทางไซเบอร์ที่จะทำเช่นนั้น

- **บริการรักษาความปลอดภัยทางไซเบอร์ของบุคคลที่สาม** องค์กรหลายแห่งขยายการบริหารความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ของตนเองผ่านผู้ให้บริการด้านการรักษาความปลอดภัยทางไซเบอร์บุคคลที่สาม บริการที่ดีที่สุดจะขึ้นอยู่กับการเข้าถึงข้อมูลทางไซเบอร์จากทั่วโลก หากไม่มีการเข้าถึงนี้ บริการเหล่านี้และผู้ใช้จะเสี่ยงต่อการถูกบุกรุกมากขึ้น

- **ความยืดหยุ่นด้านการรักษาความปลอดภัยทางไซเบอร์** ไม่ว่าพื้นที่ทางภูมิศาสตร์เฉพาะจะมีความเสี่ยงสูงต่อภัยพิบัติทางธรรมชาติหรือในเขตสงครามที่อาจเกิดขึ้นในอนาคต การกระจายข้อมูลอย่างมีประสิทธิภาพถือเป็นองค์ประกอบสำคัญของความยืดหยุ่น

ความเข้าใจผิดที่ว่าการเก็บรักษาข้อมูลไว้ภายในขอบเขตของประเทศเท่านั้นจะช่วยเพิ่มความปลอดภัยได้ จริง ๆ แล้วเป็นการสร้างความเสี่ยงที่เพิ่มมากขึ้นอย่างมาก

- **การปกป้องในนามของการรักษาความปลอดภัยทางไซเบอร์** การเก็บข้อมูลไว้ในประเทศหรือการบล็อกการถ่ายโอนข้อมูลนั้นไม่มีประโยชน์ด้านการรักษาความปลอดภัยทางไซเบอร์
การรักษาความปลอดภัยถูกกำหนดขึ้นตามการป้องกันทางเทคนิคและการดำเนินงานที่มาพร้อมกับข้อมูล ไม่ใช่ตำแหน่งที่ตั้ง ข้อจำกัดด้านการถ่ายโอนและข้อกำหนดการเก็บข้อมูลไว้ในประเทศมักใช้เพื่อบรรลุวัตถุประสงค์อื่น ๆ
บางทีปัญหาที่เป็นระบบมากที่สุดที่มีการใช้กฎหมายการรักษาความปลอดภัยทางไซเบอร์เพื่อต้องมีการเก็บข้อมูลไว้ในประเทศ คือการลดบทบาทของกฎหมายและนโยบายที่ออกแบบมาเพื่อปรับปรุงการรักษาความปลอดภัยอย่างแท้จริง

---

[1] บริษัทสมาชิกของ GDA ดำเนินธุรกิจด้านการบัญชี เกษตรกรรม ยานยนต์ การบินและอวกาศและการบิน ชีวเภสัชภัณฑ์ สินค้าอุปโภคบริโภค พลังงาน ภาพยนตร์และโทรทัศน์ การเงิน การดูแลสุขภาพ งานบริการ ประกันภัย การผลิต อุปกรณ์ทางการแพทย์ ทรัพยากรธรรมชาติ สิ่งพิมพ์ เซมิคอนดักเตอร์ ซอฟต์แวร์ ห่วงโซ่อุปทาน โทรคมนาคม และการขนส่ง บริษัทสมาชิกของ GDA มีการดำเนินงานและการจ้างงานหลายล้านตำแหน่งใน 50 รัฐของสหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติม โปรดดู https://www.globaldataalliance.org

[2] https://www.law.go.th/listeningDetail?survey_id=MzcyNURHQV9MQVdfRlJPTlRFTkQ=

[3] สมาชิก GDA มีมุมมองที่หลากหลายเกี่ยวกับร่างนโยบายการรักษาความปลอดภัยบนคลาวด์ในแง่มุมต่าง ๆ ซึ่งอาจกล่าวถึงในการเสนอให้พิจารณาผ่านองค์กรต่าง ๆ เพื่อให้สอดคล้องกับการให้ความสำคัญในนโยบายข้อมูลข้ามพรมแดนของ GDA การเสนอให้พิจารณาของ GDA จะให้ความสำคัญกับการเก็บข้อมูลไว้ในประเทศ และในแง่มุมการถ่ายโอนข้อมูลของนโยบายเพียงอย่างเดียว

[4] BSA, *ดัชนีชี้วัดระบบการประมวลผลแบบคลาวด์, หน้า* 1 (2018) ที่ https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

[5]สำหรับข้อมูลเพิ่มเติม *โปรดดู* https://www.globaldataalliance.org/downloads/02112020[]crossborderdata.pdf

[6] *โดยทั่วไปแล้ว* ให้ดู BSA, *การย้ายสู่ระบบคลาวด์ – บทเริ่มต้นสำหรับการประมวลผลแบบคลาวด์* (2018) ที่ https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf

[7] *ดู ไอดี* บริการคลาวด์ที่ให้บริการข้ามพรมแดนมีข้อได้เปรียบด้านการรักษาความปลอดภัยมากกว่าแนวทางการให้บริการด้านไอทีรูปแบบอื่น (บริการคลาวด์ภายในองค์กรหรือในพื้นที่):

- การรักษาความปลอดภัยทางกายภาพ: เจ้าหน้าที่ที่ผ่านการรับรองสามารถตรวจสอบเซิร์ฟเวอร์อย่างระมัดระวังทุกวันตลอด 24 ชั่วโมง เพื่อป้องกันการละเมิดทางกายภาพ และสามารถใช้โปรโตคอลที่สอดคล้องกันกับสถานที่จำนวนไม่มากได้
- การรักษาความปลอดภัยของข้อมูล: CSP สามารถรับประกันความสมบูรณ์ของข้อมูลผ่านการใช้โปรโตคอลการเข้ารหัสที่ล้ำสมัยสำหรับข้อมูลที่จัดเก็บไว้และระหว่างส่ง CSP สามารถสร้างการสำรองข้อมูลที่ซ้ำซ้อนในศูนย์ข้อมูลที่กระจัดกระจายตามภูมิศาสตร์ ซึ่งช่วยลดความเสี่ยงของการสูญหายในกรณีไฟฟ้าดับ หรือภัยพิบัติทางธรรมชาติ หรือสิ่งที่มนุษย์สร้างขึ้น
- การตรวจหาภัยคุกคามขั้นสูง: CSP ใช้ประโยชน์จากข่าวกรองด้านการรักษาความปลอดภัยที่ได้รับการปรับปรุงอันล้ำสมัย โดยใช้การทดสอบการเจาะระบบปกติเพื่อจำลองการโจมตีในโลกแห่งความเป็นจริง และประเมินโปรโตคอลการรักษาความปลอดภัยต่อภัยคุกคามที่เกิดขึ้นใหม่
- การปรับใช้แพตช์แบบอัตโนมัติ: การปรับใช้แพตช์แบบอัตโนมัติและแบบรวมศูนย์ รวมถึงการอัปเดตแบบเรียลไทม์สำหรับการทำงานของโปรโตคอลการรักษาความปลอดภัยเครือข่ายเพื่อปกป้องระบบจากช่องโหว่ใหม่ที่ระบุได้
- การจัดการและการตอบสนองต่อเหตุการณ์: CSP จะดูแลทีมงานผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ทั่วโลก เพื่อตอบสนองและบรรเทาผลกระทบของการโจมตีและกิจกรรมที่เป็นอันตราย
- การรับรอง: โดยทั่วไปแล้ว CSP จะต้องได้รับการรับรองตามมาตรฐานการรักษาความปลอดภัยสากล และมีการตรวจสอบอย่างสม่ำเสมอเพื่อต่ออายุใบรับรอง

[8] *ดู ไอดี* หน้า 1.

[9] *โดยทั่วไปแล้ว ให้ด*ูเชิงอรรถ 8 *อินฟรา* กลไกการถ่ายโอนข้อมูลเหล่านี้อาจรวมถึงการตัดสินใจที่เพียงพอ การรับรอง จรรยาบรรณ กฎเกณฑ์ขององค์กรที่มีผลผูกพัน (BCR) และข้อสัญญามาตรฐาน (SCC) ที่มีการป้องกันคุ้มครองข้อมูลในตัว

[10] *โปรดดู เช่น* แถลงการณ์ร่วมระหว่างสหรัฐอเมริกาและสิงคโปร์เกี่ยวกับการเชื่อมต่อข้อมูลบริการทางการเงิน ที่: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity;

[11] *ดูไอดี,* พรบ. USMCA 17.2.1; พรบ. FTA ของสหรัฐอเมริกา-ญี่ปุ่น (PPC)