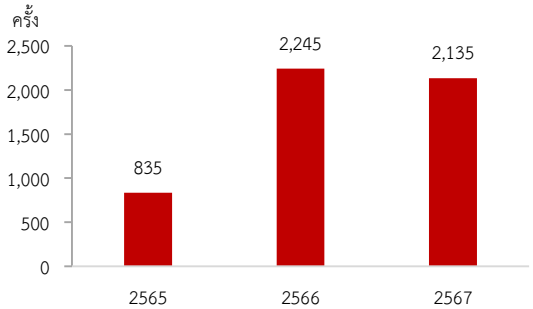
การป้องกันข้อมูลส่วนบุคคลจากภัยไซเบอร์ที่ไม่รู้ตัว

ปัญหาการละเมิดข้อมูลส่วนบุคคลเป็นภัยคุกคามที่ทั่วโลกกำลังพบเจอและมีแนวโน้มเพิ่มขึ้น ซึ่งทำให้เกิดความเสียหายมูลค่าสูงและยากต่อการรับมือ ขณะเดียวกัน รูปแบบของการละเมิดข้อมูลส่วนบุคคลยังสามารถเปลี่ยนแปลงและพัฒนาได้ตลอดเวลา ซึ่งประเทศไทยควรให้ความสำคัญในการป้องกันอย่างจริงจัง

ปัจจุบันข้อมูลส่วนบุคคล[39] เป็นทรัพยากรที่มีคุณค่าสำหรับหน่วยงานหรือองค์กรต่าง ๆ ซึ่งสามารถสร้างมูลค่าหรือการนำไปใช้ประโยชน์อื่น ๆ ไม่ว่าจะเป็นการใช้ในเชิงธุรกิจสำหรับวิเคราะห์พฤติกรรมลูกค้าเพื่อกำหนดกลยุทธ์การตลาด การต่อยอดเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) และการทำข้อมูลขนาดใหญ่ (Big Data) รวมถึงการตรวจยืนยันตัวตนของบุคคลในการใช้บริการภาครัฐ การนำไปใช้ประโยชน์ข้างต้นทำให้ข้อมูลส่วนบุคคลตกเป็นเป้าหมายของคนหลายกลุ่ม รวมถึงผู้ไม่หวังดีในการนำไปใช้ในทางที่ผิด โดยเฉพาะการละเมิดข้อมูลส่วนบุคคลที่อ่อนไหว[40] ซึ่งเป็นจุดเริ่มต้นของการก่ออาชญากรรมและสร้างความเสียหายต่าง ๆ อาทิ ถูกนำข้อมูลส่วนบุคคลไปเปิดบัญชีเพื่อฉ้อโกงผู้อื่น โดนข่มขู่จากคลิปส่วนตัว ใช้ข้อมูลบัตรเครดิตรูดซื้อสินค้า หรือถูกโอนเงินจากบัญชีธนาคาร และอาจถูกรบกวนจากการโฆษณาต่าง ๆ รวมถึงการถูกหลอกจากแก๊ง Call Center เป็นต้น โดยปัจจุบันการละเมิดข้อมูลส่วนบุคคลเป็นภัยคุกคามที่สร้างความเสียหายให้กับประเทศต่าง ๆ ทั่วโลก จากข้อมูลของ Ponemon Institute พบว่า ปี 2566 หากข้อมูลของบริษัทใดบริษัทหนึ่งรั่วไหลจะสร้างความเสียหายถึง 16.2 ล้านดอลลาร์สหรัฐต่อหนึ่งบริษัท และในปี 2567 คาดการณ์ว่า มูลค่าจะเพิ่มขึ้นเป็น 17.1 ล้านดอลลาร์สหรัฐ หรือประมาณ 630 ล้านบาท ซึ่งที่ผ่านมามีทั้งหน่วยงานรัฐ และเอกชนขนาดใหญ่ที่เคยเกิดกรณีข้อมูลรั่วไหลแล้ว อาทิ National Public Data ประเทศสหรัฐอเมริกา ซึ่งเป็นบริษัทนายหน้าข้อมูลที่ดำเนินการตรวจสอบประวัติพนักงานและรวบรวมข้อมูลประวัติอาชญากรรม ที่อยู่ เลขประกันสังคม และประวัติการทำงาน โดยมีข้อมูลรั่วไหลกว่า 2.9 พันล้านรายการ ซึ่งได้ถูกนำข้อมูลไปขายบน Dark Web และนำมาซึ่งความเสียหายต่อองค์กรด้วยการถูกฟ้องล้มละลาย หรือแม้กระทั่งบริษัทขนาดใหญ่ดังเช่น British Airways ที่หน้าเว็บไซต์ของสายการบินถูกโจมตี และโดนขโมยข้อมูลการล็อกอิน ข้อมูลการเดินทาง ชื่อที่อยู่ และข้อมูลบัตรเครดิต ซึ่งจากรายงานของ Cost of a Data Breach Report 2567 ของ IBM พบว่า ค่าเฉลี่ยของค่าใช้จ่ายที่องค์กรต้องรับผิดชอบเมื่อเกิดเหตุข้อมูลรั่วไหลหนึ่งครั้งอยู่ที่ประมาณ 4.8 ล้านดอลลาร์สหรัฐ

แผนภาพ 26 สถิติการคุกคามทางไซเบอร์



ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

[39] ข้อมูลส่วนบุคคล (Personnel Data) เป็นข้อมูลเกี่ยวกับการระบุตัวบุคคลทั้งทางตรงหรือทางอ้อม ซึ่งบางส่วนสามารถเปิดเผยได้และไม่มีความเสี่ยง ไม่ว่าจะเป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยเจ้าของข้อมูล หรือข้อมูลติดต่อที่ไม่ระบุถึงบุคคลโดยเฉพาะ อาทิ อีเมลสำนักงาน หรือที่อยู่สำนักงาน

[40] ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) เป็นข้อมูลที่เป็นเรื่องส่วนตัวของแต่ละบุคคลโดยแท้จริง และมีความละเอียดอ่อนสูง อาทิ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลพันธุกรรม หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล เป็นต้น ซึ่งหากเกิดการรั่วไหลของข้อมูลหรือถูกนำไปใช้ในทางที่ผิด อาจทำให้เกิดความเสี่ยงแก่บุคคลและถูกใช้ในการเลือกปฏิบัติกับบุคคลอย่างไม่เป็นธรรมได้

สำหรับประเทศไทย แม้ว่าปัจจุบันจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่กำหนดให้ผู้จัดเก็บข้อมูลต้องได้รับการยินยอมจากเจ้าของข้อมูลก่อน และพระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่เพิ่มบทลงโทษสำหรับผู้เปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ แต่ยังพบการคุกคามทางไซเบอร์ และการรั่วไหลของข้อมูลเพิ่มขึ้นต่อเนื่อง จากสถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พบว่า ในปี 2567 มีสถิติการคุกคามทางไซเบอร์จำนวน 2,135 ครั้ง[41] เพิ่มขึ้นจากปี 2565 ที่มีจำนวน 835 ครั้ง โดยในช่วงระหว่างปี 2564 - 2567 มีข้อมูลรั่วไหลมากกว่า 26,000 ล้านรายการ อาทิ ในปี 2567 ข้อมูลที่ใช้ระบุตัวบุคคลของผู้สูงอายุเกือบ 20 ล้านรายชื่อมีการรั่วไหล หรือข้อมูลลูกค้าของร้านค้าพาณิชย์รั่วไหลจนนำมาสู่การลงโทษปรับเป็นจำนวนเงิน 7 ล้านบาท

ข้อมูลข้างต้นเป็นตัวอย่างของสถานการณ์การรั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้นแล้วในประเทศไทย ซึ่งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ แบ่งช่องทางการรั่วไหลของข้อมูลส่วนบุคคล ออกเป็น 4 ช่องทาง คือ 1) **จากตนเอง** ที่นำข้อมูลของตนเองลงบนสื่อโซเชียลต่าง ๆ หรือเก็บข้อมูลสำคัญไว้ในโทรศัพท์มือถือ 2) **จากเว็บไซต์** หรือแอปพลิเคชัน ที่มักต้องให้การยินยอมเปิดเผยข้อมูลก่อนเข้าใช้บริการ 3) **จากการโดนแฮกหรือขโมยข้อมูล** และ 4) **จากการถูกหลอกลวง** ซึ่งปัจจุบันมีการพัฒนารูปแบบให้มีความน่าเชื่อถือมากขึ้น อาทิ การทำ AI Scam Calls หรือการหลอกลวงข้อมูลทางโทรศัพท์ และ AI Deepfake หรือการปลอมใบหน้าร่วมกับน้ำเสียงในการวีดีโอคอลหาเหยื่อ ซึ่งเป็นการหลอกลวงแบบ “หลอกซ้อนหลอก” โดยใช้ AI ปลอมแปลงตัวตนให้ดูสมจริงมากขึ้น ผ่านการขโมยข้อมูลชีวภาพ (Biometric Data) ทั้งน้ำเสียงพูดและบุคลิกท่าทาง นอกจากนี้ ยังมีการหลอกลวงในรูปแบบ SpyLoan เป็นการออกแบบแอปพลิเคชันให้คล้ายกับสถาบันการเงินที่เหยื่อจะต้องระบุข้อมูลส่วนตัวเพื่อใช้งาน

ตาราง 19 จำแนกข้อมูลที่รั่วไหลและผลกระทบ

ช่องทาง	ลักษณะของการหลอกลวง	ข้อมูลที่ถูกขโมย
ตนเอง	• แชร์ข้อมูลลงโซเชียลโดยไม่ตั้งค่าความเป็นส่วนตัว • เก็บข้อมูลสำคัญ อาทิ เบอร์โทรศัพท์ ที่อยู่	• ข้อมูลถูกนำไปใช้โดยบุคคลอื่น
เว็บไซต์หรือแอปพลิเคชัน	• ต้องกดยินยอมให้เข้าถึงข้อมูลก่อนใช้บริการ • เว็บไซต์หรือแอปพลิเคชันใช้ข้อมูลเพื่อวัตถุประสงค์อื่น	• ถูกติดตามพฤติกรรมออนไลน์ • ข้อมูลถูกนำไปขาย
แฮกหรือขโมยข้อมูล	• แฮกเกอร์เจาะระบบขององค์กร • ใช้วิธีฟิชชิ่ง (Phishing) หลอกให้ผู้ใช้กรอกรหัสผ่าน	• ข้อมูลถูกนำไปขายบน Dark Web • ถูกขโมยตัวตน (Identity Theft)
การถูกหลอกลวง	AI Scam Calls, Deepfake, SpyLoan	• เสียเงินจากการหลอกลวง • ข้อมูลถูกนำไปใช้ก่ออาชญากรรม

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

จะเห็นได้ว่าปัจจุบันข้อมูลส่วนบุคคลสามารถรั่วไหลได้หลากหลายรูปแบบและหลายช่องทาง ซึ่งเมื่อประเมินความเสี่ยงของประเทศไทย พบประเด็นที่น่ากังวลที่อาจทำให้ข้อมูลรั่วไหล ดังนี้

1. **คนไทยบางส่วนยังไม่ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลอย่างแท้จริง** โดยคนไทยบางส่วนยินยอมให้ข้อมูลส่วนบุคคลแลกกับสิทธิประโยชน์จากสินค้าและบริการ เพราะคิดว่าผู้ให้บริการมีความน่าเชื่อถือ กล่าวคือ จากรายงาน Digital Live Decoded 2024[42] ประเทศไทย พบว่า แม้ภาพรวมคนไทยจะมีความกังวลเกี่ยวกับการรั่วไหลของข้อมูล หรือการถูกหลอกเพื่อเอาข้อมูลมากถึงร้อยละ 75 ซึ่งสูงกว่าประเทศอื่น ๆ

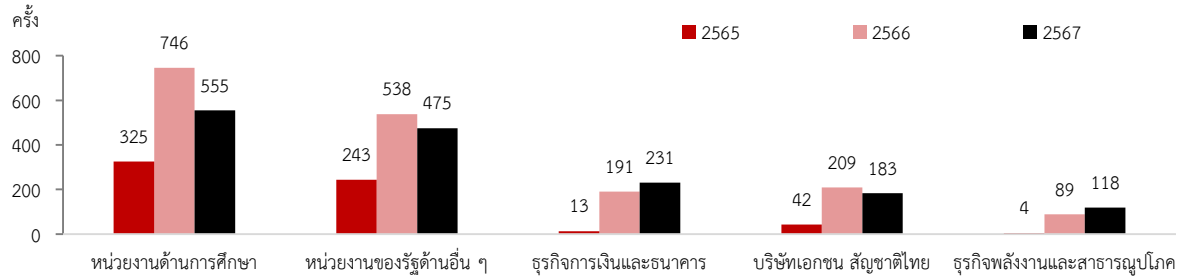
[41] รูปแบบที่มีการคุกคามมากที่สุด 3 รูปแบบ ได้แก่ รูปแบบ Intrusion Attempts (ความพยายามจะบุกรุกเข้าถึงระบบ) มีการกระทำความผิดจำนวน 913 ครั้ง คิดเป็นร้อยละ 42.7 ของการกระทำความผิด รูปแบบ Fraud (การฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์) จำนวนการกระทำความผิดทั้งหมด 525 ครั้ง คิดเป็นร้อยละ 24.5 ของภัยคุกคามทางไซเบอร์ โดยเป็นประเภทของการฉ้อโกงที่พบได้บ่อย และรูปแบบ Investment Fraud (การฉ้อโกงการลงทุน)

[42] Digital Lives Decoded 2024 ซึ่งทำการสำรวจผู้ใช้งานผู้ใช้งานอินเทอร์เน็ต 1,002 ราย อายุระหว่าง 16-64 ปี ในประเทศไทย โดยบริษัท เทเลนอร์ เอเชีย (Telenor Asia)

ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่มีค่าเฉลี่ยอยู่ที่ร้อยละ 68 แต่คนไทยกว่าร้อยละ 60 ยินยอมให้บริษัทเข้าถึงข้อมูลส่วนบุคคล เพื่อให้ได้มาซึ่งสิทธิพิเศษ ส่วนลดสินค้า หรือของสมนาคุณจากบริษัท ขณะเดียวกัน ร้อยละ 38 ของคนไทยยังรู้สึกไม่กังวล เนื่องจากมีความเชื่อใจว่าผู้ให้บริการจะสามารถรักษาข้อมูลส่วนบุคคลได้ นอกจากนี้ ยังพบว่าการเข้าถึงสินค้าและบริการหลายประเภทเริ่มกำหนดให้ผู้ใช้บริการต้องให้ข้อมูลส่วนบุคคลอื่นที่นอกเหนือความจำเป็น ซึ่งผู้ใช้บริการไม่ได้มีการตรวจสอบว่ายินยอมให้ข้อมูลประเภทใดบ้าง นอกจากนี้ คนไทยและหน่วยงานต่าง ๆ ยังมีการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ ซึ่งมีความเสี่ยงต่อการถูกละเมิดข้อมูลส่วนบุคคล โดย BSA[43] พบว่า ในปี 2566 การละเมิดลิขสิทธิ์ซอฟต์แวร์จากองค์กร 104 แห่ง สร้างมูลค่าความเสียหายกว่า 100 ล้านบาท โดยร้อยละ 24 ของการใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์โดนละเมิดข้อมูลส่วนบุคคลจากแรนซัมแวร์[44]

2. **ภาครัฐและเอกชนของไทยยังขาดแนวทางรองรับภัยคุกคามทางไซเบอร์ที่ชัดเจน** โดยข้อมูลของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. พบว่า ร้อยละ 75 ของหน่วยงานรัฐไม่มีแผนสำหรับรองรับคุกคามทางไซเบอร์ ซึ่งจากสถิติการคุกคามทางไซเบอร์ ระหว่างปี 2565 - 2567 หน่วยงานด้านการศึกษาเป็นองค์กรเป้าหมายในการโจมตีสูงสุด เนื่องจากมีการเก็บข้อมูลที่มีความอ่อนไหวจำนวนมาก อาทิ ข้อมูลประวัตินักเรียน ข้อมูลผู้ปกครอง และที่อยู่ ส่วนด้านภาคเอกชน โดยเฉพาะธุรกิจ SMEs ไม่มีการป้องกันหรือมีการป้องกันที่ไม่เพียงพอ โดยผลสำรวจของ CISCO ในปี 2567 SMEs ไทยกว่าร้อยละ 67 เคยถูกโจมตีทางไซเบอร์ และทำให้การดำเนินงานของธุรกิจร้อยละ 56 หยุดชะงัก ซึ่งร้อยละ 49 ระบุว่า เกิดจากแนวทางการรักษาความปลอดภัยทางไซเบอร์ไม่มีประสิทธิภาพเพียงพอที่จะตรวจจับ หรือป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์

แผนภาพ 27 สถิติการคุกคามทางไซเบอร์ จำแนกตามประเภทหน่วยงานที่ถูกโจมตีสูงสุด 5 ลำดับแรก



ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

3. **หลายหน่วยงานยังขาดบุคลากรทั้งจำนวนและทักษะด้านความปลอดภัยทางไซเบอร์** โดยข้อมูลของบริษัทฟอร์ติเน็ต ผู้นำด้านความปลอดภัยทางไซเบอร์ ระบุว่า องค์กรในประเทศไทยร้อยละ 92 เคยถูกละเมิดข้อมูล และร้อยละ 72 ระบุว่าขาดแคลนทักษะด้านความปลอดภัยทางไซเบอร์ ซึ่งในกรณีของภาครัฐ สำนักงานคณะกรรมการข้าราชการพลเรือน พบว่า ในปี 2566 หน่วยงานของรัฐมีข้าราชการที่มีความสามารถในการรับมือภัยทางไซเบอร์เพียง 3,888 คน (ข้อมูล ณ วันที่ 27 มกราคม 2568) จากจำนวนข้าราชการในระบบ 1.7 ล้านคน เช่นเดียวกับภาคเอกชนที่ประสบปัญหาขาดแคลนบุคคลกรเช่นกัน โดยการสำรวจของสถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI)[45] พบว่า ประเทศไทยขาดบุคลากรที่มีทักษะด้านความปลอดภัยทางไซเบอร์[46] โดยมีความต้องการมากถึง 13,683 ตำแหน่ง คิดเป็นร้อยละ 36.6 ของความต้องการแรงงานในกลุ่ม STEM ทั้งหมด นอกจากนี้ ตำแหน่งของบุคลากรที่มีทักษะด้านความปลอดภัยทางไซเบอร์ในบริษัทเอกชนส่วนใหญ่จะมีตำแหน่งเฉพาะ

[43] BSA หรือ กลุ่มพันธมิตรซอฟต์แวร์ เป็นสมาคมการค้าที่ได้รับการสนับสนุนโดยบริษัทซอฟต์แวร์ระดับโลก มีกิจกรรมหลักในการส่งเสริมการใช้งานซอฟต์แวร์ถูกลิขสิทธิ์และยับยั้งการใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์

[44] ไวรัสคอมพิวเตอร์รูปแบบการล็อกไฟล์หรือระบบของเหยื่อ แล้วเรียกค่าไถ่ เพื่อปลดล็อก

[45] โครงการพัฒนาระบบวิเคราะห์ข้อมูลด้วย Large Language Models (LLMs) เพื่อการใช้ประโยชน์ในการพัฒนากำลังคนสมรรถนะสูงฯ

[46] อาทิ นักเขียนโปรแกรม นักวิเคราะห์ระบบ วิศวกรซอฟแวร์ เป็นต้น

ในองค์กรขนาดใหญ่ หรือธุรกิจที่มีความสัมพันธ์กับต่างประเทศที่มีการกำหนดมาตรฐานด้านความปลอดภัยของข้อมูล ขณะที่ธุรกิจขนาดกลางและขนาดย่อมมักไม่ค่อยให้ความสำคัญกับบุคลากรตำแหน่งนี้ เนื่องจากต้องใช้ต้นทุนสูงในการพัฒนาระบบเทคโนโลยีสารสนเทศและจ้างบุคลากรเพื่อรองรับความปลอดภัยของข้อมูล

4. **การขาดความร่วมมือระหว่างภาครัฐและเอกชน** รวมถึงการประสานงานระหว่างประเทศ โดยการโจมตีทางไซเบอร์บางส่วนเกิดขึ้นในแพลตฟอร์มของเอกชนทั้งในประเทศและต่างประเทศ ซึ่งภาครัฐต้องอาศัยความร่วมมือกับเอกชนในการจัดการปัญหา อย่างไรก็ตาม เนื่องจากภาคเอกชนให้ความสำคัญกับการรักษาข้อมูลของลูกค้า จึงไม่ค่อยเปิดเผยข้อมูลต่อ ส่งผลให้เกิดความล่าช้าไม่ว่าจะเป็นการยับยั้งเหตุและการแจ้งเตือนต่อหน่วยงานหรือองค์กรเอกชนที่เกี่ยวข้องได้อย่างทันท่วงที ขณะที่ภาคเอกชนต่างประเทศ ยังมีข้อจำกัดเพิ่มเติมในการบังคับใช้กฎหมายในการดำเนินการขอข้อมูลของผู้กระทำความผิดที่มีฐานที่ตั้งอยู่ในต่างประเทศ

ดังนั้น เพื่อให้ประเทศไทยสามารถป้องกันการรั่วไหลของข้อมูลส่วนบุคคลได้ดียิ่งขึ้น อาจต้องมีการดำเนินการตั้งแต่**การสร้างความตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล** โดยการรณรงค์ผ่านสื่อต่าง ๆ การสร้างความเข้าใจเกี่ยวกับการให้ข้อมูลส่วนบุคคล รวมถึงการสร้างความตระหนักรู้ทางไซเบอร์โดยวิธีการปฏิบัติ อาทิ การจำลองฟิชชิง (Phishing Simulations) เพื่อช่วยฝึกซ้อมการรักษาความปลอดภัยทางไซเบอร์ **อีกทั้งยังต้องส่งเสริมให้หน่วยงานต่าง ๆ กำหนดแนวทางและพัฒนาบุคลากรเพื่อรับมือภัยคุกคามทางไซเบอร์ที่ชัดเจน** โดยหน่วยงานรัฐและเอกชนที่มีการเก็บข้อมูลที่มีความอ่อนไหว ควรจัดทำแผนการป้องกันและตั้งทีมเฝ้าระวังความปลอดภัยทางไซเบอร์ (CSIRT) เพื่อตรวจจับและเตรียมรับมือภัยคุกคาม รวมทั้งมีการส่งเสริมให้มีแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างภาครัฐและเอกชน และพัฒนาบุคลากรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) เพื่อตรวจสอบการใช้ข้อมูลของหน่วยงานในการประเมินความเสี่ยง (Risk Assessment) ของการรั่วไหลข้อมูลส่วนบุคคล รวมถึง ต้องส่งเสริมให้ทุกภาคส่วนใช้โปรแกรมที่ถูกลิขสิทธิ์ เพื่อป้องกันการโจมตีจากแฮกเกอร์

ตัวอย่างแนวทางป้องกันข้อมูลส่วนบุคคลจากต่างประเทศ

1	การแจ้งเตือน สิงคโปร์	การแจ้งเตือนเมื่อเกิดการรั่วไหลของข้อมูลผ่านทางเว็บไซต์ และในบางกรณีอาจมีการออกคำเตือนให้กับผู้ใช้งานที่ได้รับผลกระทบ รวมทั้งบังคับให้แพลตฟอร์มออนไลน์แสดงข้อความเตือนในโฆษณาประเภทการเงินหรือการลงทุน	
2	การออกมาตรการ สหรัฐอเมริกา	ข้อกำหนด CCPA ในรัฐแคลิฟอร์เนีย กำหนดให้บริษัทต้องแจ้งให้ผู้ใช้ทราบถึงการเก็บข้อมูลส่วนบุคคล และสิทธิในการขอให้หยุดใช้หรือขายข้อมูล รวมถึงมีการป้องกันการนำข้อมูลส่วนบุคคลไปใช้โดยกำหนดให้หน่วยงานรัฐต้องใช้ระบบยืนยันตัวตนแบบ Multi-Factor Authentication (MFA)	
3	การใช้เทคโนโลยี สวิตเซอร์แลนด์	การใช้เทคโนโลยี Blockchain เพื่อจัดเก็บข้อมูลภาครัฐและการทำธุรกรรมของรัฐและเอกชน ซึ่งทำให้ข้อมูลมีความปลอดภัยมากขึ้นจากคุณสมบัติที่สามารถป้องกันการแอบดัดแปลงข้อมูล และควบคุมการเข้าถึงข้อมูลด้วยเจ้าของข้อมูลเอง	
4	การพัฒนา/ฝึกอบรม สหราชอาณาจักร	การให้ทุนเพื่อฝึกอบรมแก่นักเรียนระดับมัธยมและอุดมศึกษาสำหรับเตรียมพร้อมบุคลากรด้านไซเบอร์ในอนาคต