Quantum Risk: ภัยคุกคามใหม่ในโลกดิจิทัล ที่ไม่ควรมองข้าม

(เผยแพร่เมื่อวันที่ 5 พฤศจิกายน 2568)

โดย ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

"Quantum Risk" ไม่ใช่เรื่องไกลตัวอีกต่อไป เพราะอาจทำให้ระบบ**การเข้ารหัส (Cryptography)**[1] ที่ใช้ปกป้องข้อมูลส่วนบุคคลถูกทำลายในอนาคต ซึ่งภัยคุกคามนี้เกิดขึ้นได้กับทุกข้อมูลที่พึ่งพาการเข้ารหัส ตั้งแต่รหัสผ่านแอปพลิเคชันการลงทุนไปจนถึงข้อมูลสำคัญเกี่ยวกับการลงทุน โดยผลกระทบฝั่ง**ผู้ใช้บริการ** มีทั้งข้อมูลส่วนบุคคลและความมั่งคั่งของพวกเขาจะถูกเปิดเผยหรือถูกขโมยไป ส่วนฝั่ง**ผู้ให้บริการ** ย่อมถูกกระทบในเรื่องชื่อเสียง ความน่าเชื่อถือ และความเสียหายทางการเงินที่อาจประเมินค่าไม่ได้ จึงถือเป็นความท้าทายต่อธุรกิจการเงินในปัจจุบัน

ด้วยความสามารถของ Quantum Computing อาจนำมาซึ่งภัยคุกคามในการทำลายกลไกการเข้ารหัสแบบ Public Key Cryptography ที่องค์กรส่วนใหญ่ใช้ เช่น RSA และ ECC[2] ซึ่งเป็นหัวใจของการทำธุรกรรมที่ปลอดภัยบนอินเทอร์เน็ตและการปกป้องข้อมูลที่ละเอียดอ่อน และเมื่อใดที่ Quantum Computing สามารถเข้าถึงได้ในเชิงพาณิชย์ การเข้ารหัสด้วย algorithms ใด ๆ ที่ไม่สามารถทนทานต่อการถอดรหัสด้วยเทคโนโลยี Quantum (Quantum-resistant algorithms หรือที่เรียกว่า Quantum-Safe) การเข้ารหัสเหล่านั้นจะเปราะบางไม่ต่างจากการใช้ตู้เซฟที่ไม่ปิดประตู

ความเสี่ยงจากควอนตัมเป็นปัญหาระดับโลก หน่วยงานสากลด้านความปลอดภัยไซเบอร์ จึงได้เตรียมแนวทางการรับมือไว้ 2 รูปแบบหลัก ดังนี้

1. Post-Quantum Cryptography (PQC) เป็นการป้องกันเชิงซอฟต์แวร์ที่สร้างระบบเข้ารหัสใหม่ด้วยหลักการทางคณิตศาสตร์ ที่แม้แต่ Quantum Computing ก็อาจต้องใช้เวลาหลายพันปีในการถอดรหัส เช่น เทคนิค Multivariate ที่ใช้สมการหลายตัวแปรและมีความซับซ้อนมาก เป็นต้น

2. Quantum Key Distribution (QKD) เป็นการป้องกันเชิงฮาร์ดแวร์ โดยใช้หลักการของ Physic Quantum เพื่อสร้างช่องทางการสื่อสารที่ปลอดภัยอย่างสมบูรณ์ระหว่างผู้ส่งและผู้รับ นั่นจึงทำให้ QKD สามารถตรวจจับการแอบลักลอบดักข้อมูลได้ทันที หากมีใครพยายามทำ อย่างไรก็ตาม QKD ต้องใช้โครงสร้างพื้นฐานแบบเฉพาะและมีข้อจำกัดด้านระยะทาง จึงเหมาะสำหรับการใช้งานเฉพาะกรณีที่ต้องการความปลอดภัยสูงสุด

---

[1] กระบวนการเข้ารหัสที่ใช้กุญแจแบบคู่ คือ (1) private key ซึ่งจะต้องเก็บเป็นความลับมีเจ้าของคนเดียวเท่านั้นที่รู้ และ (2) public key ที่เปรียบเสมือนบ้านเลขที่ ซึ่งเปิดเผยให้ผู้อื่นสามารถส่งข้อมูลมาหาเราได้

[2] RSA และ ECC เป็นวิธีเข้ารหัสข้อมูลแบบกุญแจสาธารณะที่ใช้กันอย่างแพร่หลาย โดย RSA (Rivest-Shamir-Adleman) เป็นวิธีที่เก่าแก่และถูกใช้อย่างแพร่หลายกว่า ส่วน ECC (Elliptic Curve Cryptography) เป็นวิธีที่ใหม่และมีประสิทธิภาพมากกว่า

“ความตึงเครียดทางภูมิรัฐศาสตร์” (Geopolitical Tension) หรือแรงจูงใจด้านความมั่นคงของชาติ เป็นอีก**ปัจจัยที่เร่ง**ให้ Quantum Computing อาจมาถึงเร็วกว่าที่คิด เนื่องจากชาติมหาอำนาจต่างเร่งลงทุนและผลักดันการพัฒนาเทคโนโลยีดังกล่าวอย่างเต็มที่ เพื่อช่วงชิงความได้เปรียบ หากชาติใดสร้าง Quantum Computing ที่ถอดรหัสคู่แข่งได้ก่อน ก็จะกุมความได้เปรียบ ทั้งในมิติเศรษฐกิจ ความมั่นคง และข่าวกรองอย่างสมบูรณ์ ปัจจัยเร่งนี้อาจทำให้ “อนาคต” มาถึงเร็วกว่าที่คาดไว้ เราจึงไม่สามารถประเมินความเร็วของการมาถึงของ Quantum Computing โดยดูแค่ปัจจัยเชิงพาณิชย์เพียงอย่างเดียว แม้ว่ามีหลายองค์กรมองว่า Quantum Computing ยังอยู่ในห้องทดลองและเป็นเรื่องไกลตัว บางฝ่ายบอกว่า อีก 10-20 ปี กว่าที่ Quantum Computing จะพร้อมใช้งานในเชิงพาณิชย์

ความก้าวหน้าของ AI ส่งผลต่อการพัฒนา Quantum Computing เช่นกัน เพราะช่วยเพิ่มศักยภาพของเทคโนโลยีนี้ให้สามารถนำมาใช้ในเชิงพาณิชย์ได้รวดเร็วยิ่งขึ้น เช่น การเปิดตัวของ Microsoft’s QPU (Quantum Processing Unit) ที่มีชื่อรุ่นว่า Majorana 1 ซึ่งมีขนาดเล็ก แต่มีประสิทธิภาพในการประมวลผลสูงกว่า Super computer หลายเท่า แม้ QPU รุ่นนี้ยังไม่ได้ถูกนำมาใช้งานจริงในเชิงพาณิชย์ แต่ก็แสดงให้เห็นถึงความก้าวหน้าและกำลังจะเกิดขึ้นในไม่ช้า

หลายองค์กรอาจตั้งคำถามว่า “Quantum Computing ยังอยู่ระหว่างการพัฒนา ทำไมต้องรีบสนใจหรือกังวลตอนนี้?” คำตอบคือแนวคิดที่เรียกว่า **“Harvest Now, Decrypt Later (HNDL)”** หรือ ดักเก็บข้อมูลไว้ก่อน แล้วรอเวลาที่ Quantum Computing จะถอดรหัสข้อมูลเหล่านั้นได้ในอนาคต นั่นหมายความว่า ข้อมูลที่ปลอดภัยในวันนี้ ไม่ว่าจะเป็นข้อมูลลูกค้า เอกสารทางกฎหมาย ธุรกรรมการเงินย้อนหลัง หรือแม้รหัสผ่าน (key algorithm) อาจไม่ปลอดภัยอีกต่อไปในวันหน้า องค์กรจึงควรรีบประเมินความเสี่ยง และวางแผนการปกป้องข้อมูลตั้งแต่วันนี้ ไม่ใช่รอให้ Quantum Computing มีใช้อย่างแพร่หลายในเชิงพาณิชย์ แล้วค่อยเริ่ม

ยิ่งไปกว่านั้น **ความเสียหายไม่ได้เกิดขึ้นเพียงวันที่ข้อมูลเข้ารหัสถูกขโมยไป** แต่ข้อมูลเข้ารหัสเหล่านั้นอาจกลายเป็นหนังสือที่ถูกเปิดอ่านได้อีก 5-10 ปีข้างหน้า คำถามสำคัญที่ผู้บริหารต้องเข้าใจ จึงไม่ใช่ “ข้อมูลขององค์กรถูกเข้ารหัสแล้วหรือไม่?” แต่ต้องเป็น **“การเข้ารหัสที่องค์กรใช้อยู่ในปัจจุบันแข็งแกร่งพอที่จะทนทานต่อศักยภาพของ Quantum Computing ในอนาคต (Quantum-Safe) หรือไม่?”** หากคำตอบคือ “ไม่” นั่นแปลว่า ข้อมูลทั้งหมดที่เชื่อว่าปลอดภัย อาจมีวันหมดอายุรออยู่ เพราะมีโอกาสที่จะถูกถอดรหัสได้ในอนาคตนั่นเอง

การเปลี่ยนผ่านสู่ยุค Quantum อาจดูเป็นเรื่องใหญ่และน่ากังวล เปรียบเหมือนสมัย Y2K แต่จุดเริ่มต้นที่ทำได้ทันทีและสำคัญที่สุด คือ การประเมินความเสี่ยงของข้อมูล (Data Risk Assessment) โดยมีมิติของ “เวลา” เป็นหัวใจสำคัญ โดยต้องเริ่มต้นจากการทำความเข้าใจข้อมูลที่มีและจัดลำดับความสำคัญของข้อมูล ดังนี้

1. สำรวจและจัดทำบัญชีข้อมูล (Data Inventory): จัดเก็บข้อมูลอะไรบ้าง? จัดเก็บไว้ที่ไหน? และมีการป้องกันอย่างไร?

2. ประเมินความปลอดภัยของอายุข้อมูล (Security Shelf-Life): องค์กรควรพิจารณาว่า “ข้อมูลแต่ละประเภทต้องคงความลับไปอีกนานแค่ไหน?” “หากข้อมูลที่บริษัทเก็บรักษา กำลังจะพบความเสี่ยงจากการถูกถอดรหัสได้ในอีก 10 ปีข้างหน้า จะกระทบต่อองค์กรหรือไม่?” “หากข้อมูลขององค์กรที่เคยพบว่ารั่วไหลในอดีต แม้เข้ารหัสไว้แล้ว แต่หากถูกถอดรหัสได้ในอนาคต จะกระทบต่อองค์กรและลูกค้าหรือไม่” หากคำตอบคือ “ใช่” นั่นคือจุดที่ควรเริ่มวางกลยุทธ์ป้องกัน

- ข้อมูลการทำธุรกรรมรายวัน อาจมีความเสี่ยงต่ำจากมิติเวลา เพราะหมดความสำคัญภายในระยะเวลาสั้น อาจต้องการความปลอดภัยเพียง 3-5 ปี
- ข้อมูลส่วนบุคคลของลูกค้า (PII), ข้อมูล KYC/CDD, ข้อมูล biometrics หรือสัญญาทางการเงินระยะยาว อาจต้องการความปลอดภัยนานถึง 10-20 ปี หรือตลอดชีวิตของลูกค้า

การจัดลำดับความสำคัญของข้อมูลนี้ จะช่วยให้องค์กรสามารถวางแผนการลงทุนในระบบรักษาความปลอดภัยแบบ Post-Quantum ได้อย่างมีประสิทธิภาพ โดยข้อมูลที่มีความเสี่ยงสูงจากมิติเวลาควรได้รับการปกป้องด้วยระบบการเข้ารหัสที่ทนทานต่อ Quantum ในลำดับแรก (Quantum-Safe) ขณะที่ข้อมูลที่มีความเสี่ยงต่ำอาจใช้ระบบเดิมต่อไปได้อีกสักระยะ

บทความนี้ ก.ล.ต. มุ่งสร้างความตระหนักให้องค์กรไม่ควรรอให้เทคโนโลยี Quantum มาถึงก่อน แต่**ควรเตรียมแผนการเปลี่ยนผ่าน (Transition Plan) ที่ช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงและการลงทุนในการป้องกันได้อย่างสมดุล** ซึ่งจะเป็นปัจจัยสำคัญที่จะทำให้องค์กรสามารถอยู่รอดและเติบโตได้ในยุค Quantum ที่กำลังจะมาถึง

****