Quantum Risk: บททดสอบการรักษาความลับที่ต้องแข่งกับเวลา

(เผยแพร่เมื่อวันที่ 20 กุมภาพันธ์ 2569)

โดย ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

เมื่อปลายปีที่แล้ว ก.ล.ต. ได้ชวนท่านผู้อ่านเปิดมุมมองใหม่เกี่ยวกับ **"Quantum Risk"** หรือภัยคุกคามจากคอมพิวเตอร์ควอนตัมกันไปแล้ว และเราได้ทิ้งท้ายความสำคัญของการมี**แผนการเปลี่ยนผ่าน (Transition Plan)** เพื่อให้ธุรกิจสามารถรับมือกับคลื่นลูกใหญ่นี้ได้อย่างสมดุล ในฉบับนี้เราจะมาเจาะลึกกันต่อว่าทำไมเราต้องรีบจัดทำแผนการเปลี่ยนผ่าน และ **"เวลา"** เป็นตัวแปรที่สำคัญที่สุดในการเปลี่ยนผ่านอย่างไร

ปัจจุบันบรรยากาศของโลกตลาดทุนให้ความสำคัญกับคำว่า **ความไว้วางใจ หรือ "Trust"** มากกว่ายุคไหน ๆ และสิ่งสำคัญที่จะทำให้เกิดความไว้วางใจได้ก็คือ "การรักษาความลับ" ในการดำเนินธุรกิจให้มีความปลอดภัย ซึ่งจะทำให้ผู้ลงทุน/ประชาชนมีความเชื่อถือ เชื่อมั่น และไว้วางใจในการใช้บริการของผู้ประกอบธุรกิจในตลาดทุน โดยสิ่งเหล่านี้จะส่งเสริมให้ภาคตลาดทุนเติบโตได้อย่างยั่งยืน

ในฐานะผู้ดูแลตลาดทุน ก.ล.ต. อยากใช้โอกาสนี้ ชวนทุกท่านกลับมาสำรวจ "สุขภาพความปลอดภัย" หรือที่รู้จักกันในชื่อเป็นทางการว่า **ความยืดหยุ่นและพร้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience)** ขององค์กรอีกครั้ง ว่าในขณะที่เรากำลังวิ่งไปข้างหน้า เราได้เตรียม "รากฐาน" ให้แข็งแรงพอที่จะรองรับอนาคตแล้วหรือยัง?

หลายท่านอาจสงสัยว่า "คอมพิวเตอร์ควอนตัมยังมาไม่ถึง แล้วทำไมเราต้องรีบร้อน?"
คำตอบซ่อนอยู่ในแนวคิดที่น่ากังวลอย่าง **Harvest Now, Decrypt Later (HNDL)** หรือ **Store Now, Decrypt Later (SNDL)** ซึ่งเปรียบเสมือนการที่ผู้ไม่หวังดีกำลังแอบเก็บข้อมูลที่ท่านเข้ารหัสใส่กล่องไว้ในวันนี้ เพื่อรอเวลาที่กุญแจผี (คอมพิวเตอร์ควอนตัม) จะถูกสร้างสำเร็จ และนำกุญแจนั้นมาไขอ่านความลับได้ในที่สุด

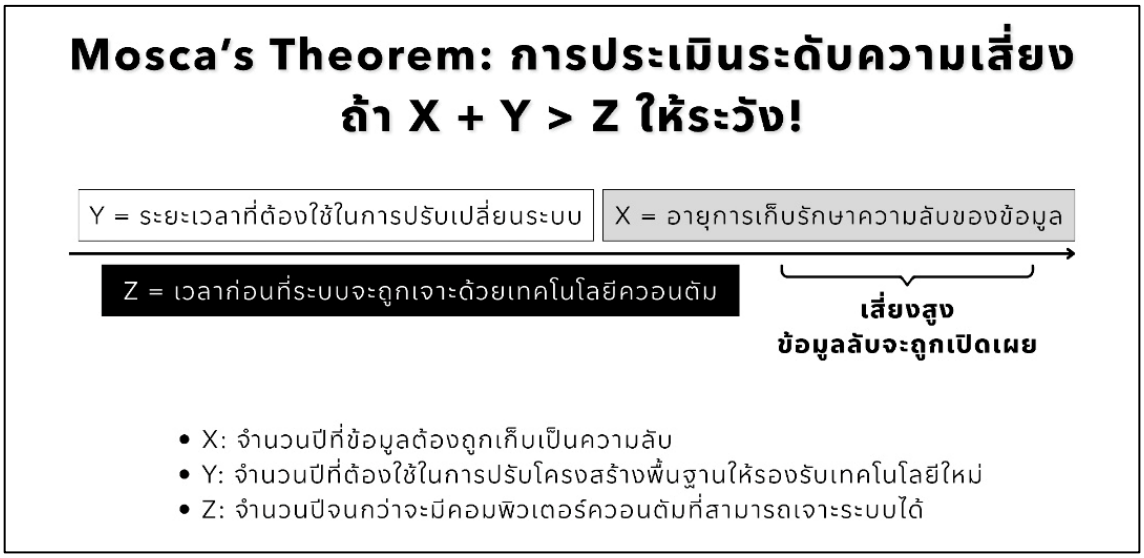
ลองจินตนาการดูว่า หากข้อมูลชีวมิติ (สแกนหน้า/ลายนิ้วมือ) ข้อมูลยืนยันตัวตนของลูกค้า (KYC) สัญญาธุรกิจระยะยาว ข้อมูลการทำ Due Diligence กับลูกค้า หรือข้อมูลพอร์ตการลงทุนของ Private Fund ที่มีอายุ 10 ปี ที่ท่านดูแลอยู่ ถูกขโมยไปในวันนี้ และถูกเปิดอ่านได้ในอีก 5 ปีข้างหน้า... ความเสียหายที่เกิดขึ้นจะไม่ใช่แค่เรื่องของค่าปรับทางกฎหมาย แต่คือ ความไว้วางใจและความเชื่อมั่นของลูกค้า ที่จะพังทลายลง ในวันที่ความลับไม่เป็นความลับอีกต่อไป

เพราะสมการความเชื่อมั่นนั้นเรียบง่าย หาก "ความลับ" รั่วไหล "Trust" ย่อมพังทลาย และเมื่อ Trust หายไป การเติบโตอย่างยั่งยืนของตลาดทุนก็ไม่อาจเกิดขึ้นได้

แล้วเราจะสามารถประเมินว่า องค์กรของเรามีความเสี่ยงจาก Harvest Now, Decrypt Later (HNDL) หรือ Store Now, Decrypt Later (SNDL) หรือไม่

ศาสตราจารย์ Michele Mosca ได้เสนอทฤษฎีที่ชื่อว่า Mosca's Theorem ซึ่งมี "สมการแห่งเวลา (Mosca's Inequality)[1]" ที่เรียบง่ายแต่ทรงพลัง ให้เราลองคำนวณเล่น ๆ ดูครับ

[1] Michele Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," *Cryptology ePrint Archive*, Report 2015/1075, (2015)



ภาพแสดงตัวอย่างการคำนวณตามทฤษฎีของ Mosca (Mosca' Theorem Level of Risk Determination)

จากสมการ "If (X + Y) > Z, then worry" **ท่านลองแทนที่ตัวเลขลงในสมการ โดยถามตัวเองด้วย 3 คำถามนี้**

1. **ข้อมูลนี้ต้องเป็นความลับนานแค่ไหน? (X)** เช่น ข้อมูลส่วนบุคคลลูกค้าอาจต้องเก็บรักษาตลอดอายุการใช้งาน (10 ปี+)
2. **ต้องใช้เวลากี่ปีในการเปลี่ยนกระบวนการเข้ารหัส เพื่อรักษาความปลอดภัยทั้งองค์กร? (Y)** สำหรับสถาบันการเงินขนาดใหญ่ การรื้อถอนระบบเก่า (Legacy) และติดตั้งระบบเข้ารหัสใหม่ที่ทนทานต่อควอนตัม (Quantum Resistance) อาจใช้เวลามากขึ้นกว่าการเจาะรหัสปัจจุบัน (Post-Quantum Cryptography) อาจกินเวลา 5-7 ปี
3. **คาดการณ์ว่าคอมพิวเตอร์ควอนตัมจะเก่งพอจะเจาะรหัสได้เมื่อไหร่? (Z)** ผู้เชี่ยวชาญจากหลายภูมิภาคเริ่มคาดการณ์ตรงกันว่า เทคโนโลยีนี้กำลังพัฒนาแบบก้าวกระโดด **และอาจนำมาใช้จริงได้ในอีก 5 ปีข้างหน้า หรืออาจจะเร็วกว่านั้น หากนำ AI เข้ามาช่วย**

โจทย์สำคัญคือ หาก Z ซึ่งเป็นระยะเวลาที่ภัยคุกคามมาถึง ลดเหลือเพียง 5 ปี ในขณะที่ Y ซึ่งเป็นระยะเวลาเปลี่ยนแปลงระบบหรือการเปลี่ยนแปลงการเข้ารหัสข้อมูลที่อาจใช้เวลา 5-7 ปี
เมื่อนำมาเข้าสูตรคำนวณแล้วจะเห็นว่า X+Y>Z !!! ... นั่นแปลว่า "เราไม่มีเวลาเหลือให้รอแล้ว" และข้อมูลของท่านอาจอยู่ในภาวะ "เสี่ยง" ตั้งแต่ยังไม่เริ่มทำอะไรเลย

ดังนั้น สิ่งแรกที่ทำได้ทันทีโดยยังไม่จำเป็นต้องทุ่มงบประมาณมหาศาลซื้อเครื่องมือใหม่ในวันนี้ เพื่อลดความเสี่ยงจากหนักเป็นเบา คือ การเริ่มบริหารจัดการ Data & Cryptographic Control ใน 2 ส่วนสำคัญคือการทำ **"บัญชีคุมสินทรัพย์การเข้ารหัส" (Cryptographic Inventory)** และ **"บัญชีคุมสินทรัพย์ประเภทข้อมูล" (Data Inventory)**

การรู้ว่าจุดอ่อนอยู่ตรงไหน คือก้าวแรกของการสร้างภูมิคุ้มกันที่สำคัญ เหมือนการเดินสำรวจบ้านเพื่อดูว่ากลอนประตูหน้าต่างแต่ละบานเป็นแบบไหน เก่าหรือใหม่ ถึงเวลาต้องเปลี่ยนหรือยัง แล้วตอนนี้มีกุญแจอยู่ที่ใครบ้าง รวมถึงในบ้านของเรามีทรัพย์สินอะไรที่สำคัญหรือต้องดูแลบ้างเก็บไว้ในห้องที่ล็อกดีแล้วรึเปล่า ซึ่งในโลกดิจิทัลก็เช่นกัน

ช่วงไตรมาสแรกของปีเป็นช่วงที่องค์กรจะทบทวน/ประเมินความเสี่ยงด้านไอที (IT Risk Assessment) นี่จึงเป็นจังหวะที่ดีในการเริ่มสำรวจดูว่า

- คณะกรรมการบริษัทได้เริ่มพูดคุย ประเมินความเสี่ยงภัยคุกคามจากคอมพิวเตอร์ควอนตัมบ้างแล้วหรือยัง
- ระบบสำคัญ ๆ ของเราใช้อัลกอริทึมอะไรล็อกกุญแจอยู่ เช่น RSA, ECC หรือ AES และอัลกอริทึมเหล่านั้นจะป้องกันภัยคุกคามจากคอมพิวเตอร์ควอนตัม (Quantum Safe Cryptography) ได้หรือไม่
- มีกุญแจดอกไหนบ้างที่ถูกฝังอยู่ในโปรแกรม (Hard-coded) ทำให้เปลี่ยนได้ยาก
- ข้อมูลสำคัญชุดไหนบ้างที่มีระยะเวลาที่ข้อมูลต้องเก็บรักษาเป็นความลับ (Security Shelf-Life) ยาวนานเกิน 5 ปี
- ข้อมูลต่าง ๆ ถูกจัดสรรและแบ่งประเภทตามระดับความสำคัญ ครบถ้วนแล้วหรือไม่
- ฝ่ายงานที่เกี่ยวข้องด้านความเสี่ยง หรือด้านเทคโนโลยี ภายในองค์กรได้มีการศึกษา หรือตระหนักถึงความเสี่ยงของคอมพิวเตอร์ควอนตัมบ้างแล้วหรือยัง

หากคำตอบจากคำถามข้างต้น คือ “ไม่รู้” “ไม่ทราบ” “ไม่แน่ใจ” ก็น่าจะเป็นสัญญาณที่พอจะบอกได้แล้วว่า องค์กรยังไม่มีความพร้อม และจำเป็นจะต้องเตรียมการ หรือหารือเรื่องนี้ภายในกันอย่างจริงจัง

ภายใต้ยุทธศาสตร์ **“Building Trust, Powering Growth”** ของ ก.ล.ต. ปี 2569-2571 เราเชื่อมั่นว่า “ความปลอดภัย” คือรากฐานสำคัญและไม่ใช่ภาระที่เป็นต้นทุน แต่เป็น “สินทรัพย์” ที่มีค่าที่สุด ในวันที่โลกกำลังเปลี่ยนผ่าน ผู้ที่ตระหนักรู้และเริ่มขยับตัวก่อน ไม่เพียงแต่จะปกป้องตนเองจากภัยคุกคามในอนาคต แต่ท่านกำลังส่งสัญญาณบอกผู้ใช้บริการของท่าน หรือผู้มีส่วนได้เสีย ว่า “เราใส่ใจและพร้อมดูแลทรัพย์สินหรือข้อมูลของท่านในทุกสถานการณ์” นอกจากนี้ การมีระบบ Cyber Resilience ที่พร้อมรับมือควอนตัม คือ หนึ่งใน **“เครื่องหมายแห่งความเชื่อมั่น” ที่สะท้อนถึงความตั้งใจจริงขององค์กร**

ยิ่งปล่อย (เวลา) ยิ่งเสี่ยง (ภัย) เริ่มใส่ใจตั้งแต่วันนี้ ผลดีต่อ Trust ขององค์กรและตลาดทุน
