บทความชุด “Internal Auditing 4.0 (IA 4.0)”

ตอนที่ 3 : "คำเปลี่ยนโลก (Words to Change the World) : โอกาสและความเสี่ยงที่ Internal Auditor 4.0 (IA4.0) ต้องรู้!" (ตอนที่ 2)

นายสิริชัย สกุลแพร่พาณิชย์ (โค้ชเม้ง)
ผู้ก่อตั้ง และกรรมการผู้จัดการ CIA Coach Consulting Co., Ltd.
CIA, CRMA, C-PA, CPIAT, IAEP, EIAP, ISMS Lead Auditor
ปริญญาตรี บัญชี จุฬาฯ (Shi 58) และปริญญาโท หลักสูตร MSCG จุฬาฯ (รุ่นที่ 1)

บทความตอนที่แล้ว ผมได้เริ่มนำเสนอรายละเอียดของโอกาสและความเสี่ยงของเทคโนโลยีต่างๆ ที่ผู้ตรวจสอบภายในยุคใหม่ ที่ผมเรียกว่า Internal Auditor 4.0 (IA4.0) ต้องรู้ โดยเรียบเรียงและจัดเรียงเป็นคำศัพท์ของเทคโลยีต่างๆ ตามลำดับของตัวอักษรในภาษาอังกฤษ จาก A ถึง Z ซึ่งผมเรียกว่า “คำเปลี่ยนโลก (Words to Change the World)” โดยเมื่อตอนที่แล้ว ผมได้นำเสนอคำศัพท์ของเทคโลยีต่างๆ ตามลำดับของตัวอักษร จาก A ถึง C ไปแล้ว สำหรับบทความตอนนี้ จึงขอนำเสนอคำศัพท์ของเทคโลยีต่างๆ ตามลำดับของตัวอักษร จาก D ถึง F โดยมีรายละเอียดดังนี้

D = Data Analytics : DA (การวิเคราะห์ข้อมูล)

Data Analytics : DA (การวิเคราะห์ข้อมูล) หมายถึง กระบวนการรวบรวม จัดระเบียบ ทำความสะอาด และวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) โดยใช้เทคโนโลยีสมัยใหม่ เช่น Artificial Intelligence (AI) Machine Learning (ML) และระเบียบวิธีทางสถิติ เพื่อค้นหาข้อมูลเชิงลึก (Insights) รูปแบบ (Patterns) หรือความสัมพันธ์ที่ซ่อนอยู่ ช่วยให้องค์กรสามารถตัดสินใจบนพื้นฐานของข้อมูลได้อย่างแม่นยำแทนการใช้สัญชาตญาณ

ปัจจุบันเทคโนโลยีนี้แบ่งเป็น 4 ประเภทหลัก คือ การวิเคราะห์เชิงพรรณนา (Descriptive) การวิเคราะห์เชิงวินิจฉัย (Diagnostic) การวิเคราะห์เชิงคาดการณ์ (Predictive) และการวิเคราะห์เชิงแนะนำ (Prescriptive) **ซึ่งสร้างโอกาสมหาศาลควบคู่ไปกับความเสี่ยงที่องค์กรต้องระมัดระวัง ดังนี้**

การนำ Data Analytics ไปใช้อย่างมีประสิทธิภาพ ช่วยสร้างข้อได้เปรียบทางการแข่งขันและเพิ่มโอกาสใหม่ ๆ เช่น **เพิ่มประสิทธิภาพการตัดสินใจ (Informed Decision-Making)** เปลี่ยนจากการคาดเดาเป็นการใช้หลักฐานเชิงประจักษ์ (Traceable Evidence) และการวิเคราะห์ฉากทัศน์ (Scenario Analysis) **เข้าใจพฤติกรรมลูกค้าเชิงลึก (Customer Insights)** เชื่อมโยงข้อมูลธุรกรรม ความคิดเห็น และพฤติกรรม เพื่อสร้าง

ประสบการณ์เฉพาะบุคคล (Personalization) เช่น การแนะนำสินค้าของ Amazon ใช้ AI/ML ตรวจสอบความผิดปกติของข้อมูล (Anomaly Detection) ในระบบการเงินและการประกันภัยได้อย่างรวดเร็ว **ปรับปรุงกระบวนการทำงานและซัพพลายเชน (Process Optimization)** คาดการณ์ช่วงเวลาที่มีความต้องการสินค้าสูง (Peak Demand Forecasting) และการบำรุงรักษาเชิงคาดการณ์ (Predictive Maintenance) ช่วยลดต้นทุนการจัดการสินค้าคงคลัง **ขับเคลื่อนนวัตกรรมและโมเดลธุรกิจใหม่** นำข้อมูลมาพัฒนาเป็นผลิตภัณฑ์หรือบริการใหม่ (Data-driven Offerings) เช่น การให้คำแนะนำทางการเงินส่วนบุคคลของธนาคาร และ **สนับสนุนกลยุทธ์ความยั่งยืน (Sustainability)** ช่วยคำนวณและประเมินดัชนีชี้วัดประสิทธิภาพด้านพลังงานและการปล่อยก๊าซเรือนกระจกได้อย่างถูกต้อง เป็นต้น

แม้จะมีประโยชน์สูง แต่การบริหารจัดการข้อมูลที่ไม่รัดกุมอาจนำมาซึ่งความเสี่ยงร้ายแรง เช่น **คุณภาพของข้อมูลต่ำ (Poor Data Quality)** หากวิเคราะห์ข้อมูลที่ผิดพลาด ซ้ำซ้อน หรือไม่สมบูรณ์ (Garbage In, Garbage Out) จะนำไปสู่การตัดสินใจที่ผิดพลาดทางธุรกิจ **ความปลอดภัยของข้อมูลและความเป็นส่วนตัว (Cybersecurity & Privacy)** การรวบรวมข้อมูลส่วนบุคคลจำนวนมาก เสี่ยงต่อการถูกโจมตีทางไซเบอร์และการละเมิดกฎหมายความเป็นส่วนตัว (เช่น PDPA หรือ GDPR) **ความซับซ้อนเกินความจำเป็น (Overcomplicating Analytics)** การเลือกใช้โมเดลที่ซับซ้อนเกินไปหรือเน้นเครื่องมือล้ำสมัย โดยไม่ได้คำนึงถึงข้อมูลเชิงลึกที่นำไปปฏิบัติได้จริง (Actionable Insights) **การทำงานแบบแยกส่วน (Siloed Approach)** แต่ละแผนกใช้คำนิยามตัวชี้วัด (Metrics) ต่างกัน ขาดการแชร์ข้อมูลข้ามสายงาน ทำให้ภาพรวมการวิเคราะห์คลาดเคลื่อน **การต่อต้านการเปลี่ยนแปลง (Neglecting Change Management)** ความล้มเหลวในการสร้างวัฒนธรรมขับเคลื่อนด้วยข้อมูล (Data-Driven Culture) หรือพนักงานขาดความรู้ความเข้าใจ (Data Literacy) ทำให้ไม่นำระบบไปใช้งานจริง และ **ความลำเอียงของอัลกอริทึม (Algorithmic Bias)** โมเดล AI/ML อาจเรียนรู้จากข้อมูลในอดีตที่มีอคติ ส่งผลให้การคาดการณ์หรือการตัดสินใจขาดจริยธรรมและเกิดการเลือกปฏิบัติ เป็นต้น

E = Encryption (การเข้ารหัสลับ)

Encryption (การเข้ารหัสลับ) คือ กระบวนการแปลงข้อมูลจากรูปแบบปกติที่อ่านได้ (Plaintext) ให้เป็นรหัสลับ (Ciphertext) โดยอาศัยอัลกอริทึมทางคณิตศาสตร์และกุญแจรหัส (Cryptographic Keys) เพื่อป้องกันไม่ให้บุคคลที่ไม่มีสิทธิ์เข้าถึงสามารถอ่านหรือแก้ไขข้อมูลได้ ถือเป็นรากฐานสำคัญสูงสุดของความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบัน

เทคโนโลยีการเข้ารหัส สร้างโอกาสและการเติบโตอย่างมหาศาลให้กับโลกดิจิทัลในมิติต่าง ๆ เช่น **สร้างความปลอดภัยในการประมวลผลบน Cloud** ช่วยให้องค์กรจัดเก็บข้อมูลบนระบบ Cloud Storage ได้

อย่างไร้กังวล และเปิดโอกาสให้เกิดเทคโนโลยีใหม่อย่าง Homomorphic Encryption ที่ช่วยให้เราสามารถประมวลผลหรือวิเคราะห์ข้อมูลได้ทั้งที่ยังถูกเข้ารหัสอยู่ **ขับเคลื่อนเศรษฐกิจดิจิทัลและการเงินไร้เงินสด** รองรับความปลอดภัยในระบบธนาคารออนไลน์ การชำระเงินผ่านอีคอมเมิร์ซ และเป็นกลไกหลักในการทำงานของ Blockchain และสินทรัพย์ดิจิทัล (Cryptocurrency) **ยกระดับความเป็นส่วนตัวในการสื่อสาร** แทคโนโลยี End-to-End Encryption (E2EE) เปิดโอกาสให้ผู้ใช้งานทั่วไปสามารถคุยโทรศัพท์ ส่งข้อความ หรือประชุมวิดีโอได้อย่างปลอดภัย โดยไม่มีบุคคลที่สามรวมถึงผู้ให้บริการแอปพลิเคชันเข้ามาแอบดูได้ **เพิ่มความน่าเชื่อถือและการปฏิบัติตามกฎหมาย** ช่วยให้ธุรกิจปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA ของไทย หรือ GDPR ของยุโรป) ได้อย่างสมบูรณ์ สร้างความเชื่อมั่นและภาพลักษณ์ที่ดีให้แก่แบรนด์ และ **การเปลี่ยนผ่านสู่ Post-Quantum Cryptography (PQC) การ**เร่งพัฒนาอัลกอริทึมที่ทนทานต่อคอมพิวเตอร์ควอนตัม กลายเป็นโอกาสทางธุรกิจใหม่สำหรับบริษัทไอทีและผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ในการอัปเกรดระบบรักษาความปลอดภัยทั่วโลก เป็นต้น

แม้จะมีประโยชน์สูง แต่การเข้ารหัสก็นำมาซึ่งความเสี่ยงและสิ่งท้าทายใหม่ ๆ เช่นกัน เช่น ภัยคุกคามจากคอมพิวเตอร์ควอนตัม (Quantum Threat) คอมพิวเตอร์ควอนตัมในอนาคตมีขีดความสามารถที่จะถอดรหัสลับแบบเดิม (เช่น RSA หรือ ECC) ได้อย่างง่ายดาย ก่อให้เกิดความเสี่ยงแบบ "Harvest Now, Decrypt Later" ซึ่งแฮกเกอร์จะขโมยและเก็บข้อมูลที่เข้ารหัสในปัจจุบันไว้ เพื่อรอไปถอดรหัสเมื่อเทคโนโลยีควอนตัมพร้อมใช้งาน **ปัญหาการจัดการกุญแจรหัส (Key Management)** หากองค์กรเก็บรักษากุญแจถอดรหัสไม่ดีพอจนถูกขโมย ระบบที่วางไว้จะล้มเหลวทันที หรือในทางกลับกัน หากกุญแจรหัสสูญหายหรือเสียหาย องค์กรจะไม่สามารถกู้คืนข้อมูลสำคัญนั้นกลับมาได้อีกเลย **การถูกนำไปใช้ในทางที่ผิดโดยอาชญากร** แฮกเกอร์มักใช้เทคโนโลยี Encryption ในการทำ Ransomware (มัลแวร์เรียกค่าไถ่) โดยแอบเข้ารหัสข้อมูลของเหยื่อเพื่อล็อกระบบและเรียกเงินค่าไถ่ นอกจากนี้ ระบบสื่อสารที่เข้ารหัสอย่างมิดชิด (E2EE) ยังกลายเป็นช่องทางให้ผู้ก่อการร้ายหรือผู้ค้าสิ่งผิดกฎหมายใช้หลบเลี่ยงการตรวจสอบของเจ้าหน้าที่รัฐ และ **ความเสี่ยงจากการตั้งค่าและข้อผิดพลาดในการติดตั้ง (Cryptographic Failures)** การเลือกใช้อัลกอริทึมที่ล้าสมัย (เช่น SHA-1 หรือ MD5) หรือการเขียนโค้ดติดตั้งระบบเข้ารหัสที่ผิดพลาด ถือเป็นหนึ่งในความเสี่ยงสูงสุดที่ทำให้ระบบไอทีมีช่องโหว่ เป็นต้น

F = Firewall (ด่านกันบุกรุก)

Firewall (ด่านกันบุกรุก) แปลตรงตัวในภาษาไทยว่า "กำแพงไฟ" แต่ในทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ศัพท์บัญญัติราชบัณฑิตยสภาเรียกว่า "ด่านกันบุกรุก" หรือที่นิยมทับศัพท์และเรียกกันทั่วไปว่า "ไฟร์วอลล์" **เทคโนโลยี Firewall** ในยุคปัจจุบันได้วิวัฒนาการจากระบบกรองพอร์ตพื้นฐาน (Stateful

Inspection) ไปสู่ Next-Generation Firewall (NGFW) และรูปแบบ Cloud-Native / Hybrid Mesh Firewall ที่ผสานระบบปัญญาประดิษฐ์ (AI) เพื่อปกป้องระบบเครือข่ายที่กระจายตัวอย่างไร้ขอบเขต

เทคโนโลยีนี้มอบโอกาสในการยกระดับความปลอดภัย แต่ในขณะเดียวกันก็มาพร้อมกับความเสี่ยงใหม่ ๆ ที่องค์กรต้องเผชิญ ดังนี้

โอกาสทางเทคโนโลยีและธุรกิจ (Opportunities) เช่น **การตรวจจับภัยคุกคามอัจฉริยะด้วย AI (AI-Driven Threat Detection)** Firewall ยุคใหม่สามารถดึงข้อมูล Threat Intelligence จากคลาวด์ มาวิเคราะห์พฤติกรรมทราฟฟิกที่ผิดปกติ (Behavioral Analytics) ช่วยให้องค์กรตรวจจับและระงับการโจมตีทางไซเบอร์ที่เกิดขึ้นอย่างรวดเร็วในรูปแบบวินาทีได้ เช่น มัลแวร์เรียกค่าไถ่แบบ Zero-Day **การรักษาความปลอดภัยทราฟฟิกเข้ารหัส (Encrypted Traffic Security)** ในปัจจุบันข้อมูลบนเว็บมากกว่า 90% ถูกเข้ารหัส (TLS/SSL) ซึ่งเป็นช่องโหว่ให้ผู้ไม่หวังดีซ่อนมัลแวร์เข้ามา เทคโนโลยี NGFW มอบโอกาสในการทำ Deep Packet Inspection (DPI) เพื่อถอดรหัสและตรวจสอบสิ่งแปลกปลอมโดยไม่กระทบต่อความเป็นส่วนตัวของผู้ใช้งาน **รองรับการทำงานแบบไฮบริดและการขยายตัวผ่านคลาวด์ (Cloud-Native & Hybrid Mesh)** ช่วยให้องค์กรสามารถควบคุมนโยบายความปลอดภัยจากศูนย์กลาง (Centralized Management) ครอบคลุมทั้งพนักงานที่ทำงานแบบ Remote Work, ระบบ On-Premises และ Multi-Cloud ได้อย่างต่อเนื่อง **ขับเคลื่อนสถาปัตยกรรม Zero Trust (Identity-First Security)** เปลี่ยนจากการป้องกันแค่ขอบเขตเครือข่ายเดิม ๆ มาเป็นการตรวจสอบสิทธิ์ตามตัวตนของผู้ใช้ (User Identity) และอุปกรณ์อย่างต่อเนื่อง "ไม่ไว้วางใจใครจนกว่าจะยืนยันตัวตน" และ **ตอบสนองเกณฑ์การปฏิบัติตามกฎหมาย (Regulatory Compliance)** ช่วยให้อัตโนมัติในการสร้างรายงานและบันทึก Log ที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA, GDPR) และมาตรฐานสากล เป็นต้น

ความเสี่ยงและความท้าทาย (Risks & Challenges) เช่น **ความผิดพลาดจากการตั้งค่าโดยมนุษย์ (Configuration Errors)** การกำหนดกฎ (Rules) หรือนโยบายที่ซับซ้อนเกินไปมักนำไปสู่ช่องโหว่ที่แฮกเกอร์ใช้เจาะระบบได้ หรืออาจส่งผลกระทบย้อนกลับไปบล็อกทราฟฟิกปกติขององค์กรเอง (False Positives) **ภัยคุกคามจากภายในที่ Firewall ตรวจจับไม่ได้ (Insider Threats)** Firewall ส่วนใหญ่เน้นคัดกรองทราฟฟิกเข้า-ออกระหว่างภายนอกกับภายในเครือข่าย หากพนักงานในองค์กรนำอุปกรณ์ที่ติดมัลแวร์มาเสียบเข้าระบบ หรือตั้งใจขโมยข้อมูล เทคโนโลยี Firewall ทั่วไปจะไม่สามารถตรวจจับการเคลื่อนไหวในแนวราบ (Lateral Movement) นี้ได้ดีพอ **ช่องโหว่บนตัวอุปกรณ์ Firewall เอง (Vulnerabilities & Exploits)** ตัวอุปกรณ์หรือซอฟต์แวร์ Firewall ก็มีโอกาสเกิดช่องโหว่ระดับซีโร่เดย์ (Zero-day vulnerabilities) ที่แฮกเกอร์จ้องจะโจมตีเพื่อยึดสิทธิ์ผู้ดูแลระบบ (เช่น เคสช่องโหว่ร้ายแรงที่มักถูกค้นพบในระบบปฏิบัติการของแบรนด์ชั้นนำ) **ปัญหาคอขวดและประสิทธิภาพระบบ (Latency & Resource Consumption)** การเปิดฟังก์ชันความปลอดภัยขั้นสูง เช่น การถอดรหัส SSL/TLS หรือการสแกนเชิงลึก (DPI) ต้องใช้พลังงานในการประมวลผลสูงมาก (High

Computational Overhead) ซึ่งหากอุปกรณ์มีประสิทธิภาพไม่เพียงพอ จะทำให้เครือข่ายเกิดความล่าช้า (Latency) และกระทบต่อการดำเนินธุรกิจ และ **ภัยคุกคามแห่งอนาคต (Post-Quantum Threats)** การมาถึงของคอมพิวเตอร์ควอนตัม (Quantum Computing) อาจทำให้ระบบการเข้ารหัสข้อมูลที่ Firewall ใช้อยู่ในปัจจุบันถูกถอดรหัสได้ในเวลาอันรวดเร็ว องค์กรจึงมีความเสี่ยงหาก Firewall ไม่ได้รับการอัปเกรดเป็น Post-Quantum Cryptography (PQC) เป็นต้น

โปรดติดตามรายละเอียดของโอกาสและความเสี่ยงของเทคโนโลยีต่างๆ ที่ผมเรียบเรียงเป็นคำศัพท์ทางเทคโนโลยี ซึ่งผมเรียกว่า "คำเปลี่ยนโลก (Words to Change the World)" ได้ในตอนต่อไปนะครับ

ข้อมูลอ้างอิง :

- Big Data Institute (BDI): รายละเอียดการประยุกต์ใช้ Data Analytics ในภาคธุรกิจและการจัดการความเสี่ยง จากบทความ Data Analytics คืออะไร ? และมีอะไรบ้าง ? ทำไมทุกองค์กรถึงให้ความสำคัญ
- Dataforest AI (2026): แนวโน้มเทคโนโลยี ปี 2026 ประโยชน์ต่อธุรกิจ และข้อผิดพลาดทั่วไป จากบทความ Business Data Analytics: Uses, Risks & Trends in 2026
- Disrupt Ignite: แนวคิดการสร้างข้อได้เปรียบทางการแข่งขันและประเภทของการวิเคราะห์ จากบทความ Data Analytics คืออะไร ศาสตร์การวิเคราะห์ในยุค Disruption
- Oracle Corporation: ความท้าทายในการวิเคราะห์ข้อมูลและการใช้ Machine Learning จากคู่มือ 10 Data Analytics Challenges & Solutions
- ResearchGate (2025): การวิเคราะห์แนวโน้ม นวัตกรรมรายอุตสาหกรรม และประเด็นด้านจริยธรรม จากงานวิจัย The Future of Data Analytics: Trends, Challenges, and Opportunities
- Sangfor Technologies (2025): Data Encryption ถอดรหัสเทคโนโลยีปกป้องข้อมูลจากภัยคุกคามยุคดิจิทัล ค้นหาจาก Sangfor Blog
- Fortinet (2025): What is Encryption? Definition, Types & Benefits ค้นหาจาก Fortinet Cyber Glossary
- Google Cloud (2025): What is encryption and how does it work? ค้นหาจาก Google Cloud Learn
- The Silicon Review (2024): The Role of Encryption in Protecting Large Files During Corporate Exchanges (ระบุถึงแนวโน้ม Quantum Computing และเทรนด์ความเสี่ยงปี 2025-2026) ค้นหาจาก The Silicon Review
- Advace Cybersecurity (2026): Top three trends shaping the security of encrypted communications in 2026 ค้นหาจาก Adva Security Blog
- Invicti (2025): Cryptographic Failures: 2025 OWASP Top 10 Risk ค้นหาจาก Invicti Web Security Risk
- Palo Alto Networks: What Are the Benefits of a Firewall? สืบค้นจาก Palo Alto Networks Cyberpedia
- Check Point Software Technologies (2025): 6 Main Firewall Threats & Vulnerabilities, and How to Mitigate Them สืบค้นจาก Check Point Cyber Hub
- Fortinet (2026): Cybersecurity trends 2026: Defending against agentic & AI threats สืบค้นจาก Fortinet Cyberglossary
- World Economic Forum (2026): Global Cybersecurity Outlook 2026: The trends reshaping cybersecurity สืบค้นจาก World Economic Forum Publications
- Nomios Group (2026): Top 5 NGFW solutions for 2026 สืบค้นจาก Nomios News & Blog
- Cibersafety (2024): Potential Firewall Risks and Challenges สืบค้นจาก Cibersafety Blog