ผู้สอบบัญชี กับ Cybersecurity

Cybersecurity คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหาย ส่งผลต่อความปลอดภัยของข้อมูลข่าวสารในรูปแบบอิเล็กทรอนิกส์ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ การเข้าถึง การประมวลผล และการกระจายข้อมูลในระบบออนไลน์ ทั้งนี้ Cybersecurity ยังรวมถึงการระวังป้องกันต่อการโจมตี และการจารกรรมต่อระบบสารสนเทศ (IT)

ในปัจจุบันมีการทำงานผ่านระบบออนไลน์เพิ่มมากขึ้น พาดหัวข้อข่าวซึ่งทำให้กิจการและหน่วยงานกำกับดูแลตื่นตัวอย่างยิ่งเป็นเรื่อง Cybersecurity กิจการต้องให้ความสำคัญและสนใจในเรื่องนี้ เพราะหากข้อมูลความลับทางธุรกิจถูกขโมยหรือหายไป ก็อาจเป็นผลเสียต่อธุรกิจ ชื่อเสียงของกิจการ และกระทบความเชื่อมั่นของนักลงทุนที่มีต่อกิจการ ผลการสำรวจโดยสำนักงานสอบบัญชีชั้นนำสองแห่ง โดยสอบถามผู้บริหารและผู้ที่รับผิดชอบด้าน IT ในปี 2013 พบว่ามีอัตราการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตเพิ่มสูงขึ้น **Center for Audit Quality (CAQ)**[i] ซึ่งเป็นองค์กรในประเทศสหรัฐอเมริกาเห็นความความสำคัญในเรื่องนี้ จึงได้เผยแพร่บทความเรื่อง **Cybersecurity and the External Audit**[ii] โดยมีเนื้อหาเกี่ยวกับงานของผู้สอบบัญชีที่เกี่ยวข้องกับ cybersecurity สามารถสรุปได้ดังนี้

- มาตรฐานการสอบบัญชีกำหนดให้ผู้สอบบัญชีต้องทำความเข้าใจเกี่ยวกับระบบ IT ของกิจการที่ตรวจสอบ และผลกระทบของระบบ IT ที่มีต่อรายงานทางการเงิน
- ผู้สอบบัญชีต้องทำความเข้าใจระบบควบคุมอัตโนมัติ (Automated Control) ในส่วนที่มีความเกี่ยวข้องกับรายงานทางการเงิน รวมถึงทำความเข้าใจระบบการควบคุมทั่วไปของระบบสารสนเทศ (IT General Control) ซึ่งมีผลต่อประสิทธิภาพของการควบคุมอัตโนมัติ อีกทั้งผู้สอบบัญชีต้องตรวจสอบความเชื่อถือได้ของข้อมูลและรายงานจากการประมวลผลด้วยระบบ IT
- ผู้สอบบัญชีควรทำความเข้าใจในระบบและการควบคุมด้าน IT ของกิจการ โดยเป็นปัจจัยหนึ่งในการประเมินความเสี่ยงในการแสดงข้อมูลที่อาจจะขัดต่อข้อเท็จจริงอย่างเป็นสาระสำคัญต่อรายงานทางการเงิน ซึ่งรวมถึงประเมินความเสี่ยงที่อาจเกิดจากเข้าถึงระบบ IT โดยบุคคลที่ไม่ได้รับอนุญาต (Unauthorized Access)
- ระบบและข้อมูลที่อยู่ในขอบเขตของการตรวจสอบบัญชีนั้นเป็นเพียงแค่ส่วนหนึ่งของระบบและข้อมูลทั้งหมดที่กิจการใช้ในการดำเนินการ งานของผู้สอบบัญชีจะมุ่งเน้นการตรวจสอบการเข้าถึงและการเปลี่ยนแปลงของระบบและข้อมูลที่จะส่งผลต่อประสิทธิผลของการควบคุมภายในที่เกี่ยวกับรายงานทางการเงิน (Internal Control Over Financial Reporting) เช่น ตรวจสอบระบบ Enterprise Resource Planning (ERP) หรือระบบที่จัดทำขึ้นเพื่อวัตถุประสงค์เฉพาะ เช่น ระบบทะเบียนสินทรัพย์ถาวร (Fixed Asset System) เป็นต้น ซึ่งเป็นขอบเขตที่แคบมากกว่าการตรวจสอบระบบ IT โดยทั่วไปของกิจการ

- ดังนั้น ขอบเขตของการตรวจสอบงบการเงินและการตรวจสอบการควบคุมภายในที่เกี่ยวกับรายงานทางการเงินตามมาตรฐานวิชาชีพจึงอาจมิได้รวมถึงการตรวจสอบการกระทำผิดที่เกี่ยวข้องกับ Cybersecurity ซึ่งมักจะเกิดจากการเจาะข้อมูลมาจากภายนอก อย่างไรก็ตาม หากเกิดการกระทำผิดดังกล่าวอย่างมีสาระสำคัญ ผู้สอบบัญชีจะต้องประเมินผลกระทบที่มีต่อรายงานทางการเงินการเปิดเผยข้อมูล เช่น เรื่องหนี้สินที่อาจจะเกิดขึ้น และผลกระทบต่อระบบการควบคุมภายในที่เกี่ยวข้องด้วย

---

[i] http://www.thecaq.org/about-us

[ii] http://www.thecaq.org/docs/alerts/caqalert_2014_03.pdf?sfvrsn=2