Cybersecurity and the AICPA Cybersecurity Attestation Project

Chris Halterman
Executive Director EY

Chair AICPA Trust Information Integrity Task Force

Agenda Item 8-D

IAASB Meeting, September 21-25, 2015

New York, USA

Increasing awareness of cybersecurity exposure for business and other entities

- Increased dependence on interconnected IT
  - Transaction processing
  - Increased value of information
  - Acceptance of proof of identify in electronic form
- Cyber attacks have become more organized, profitable, and persistent
- Cybersecurity has evolved into a critical business issue

Effective cybersecurity programs are a now a necessity for most entities

- Goal of cybersecurity
  - Supports integrity of system processing and the information stored on systems, including but not limited to systems and information significant to financial reporting
  - Helps ensure systems and information are available when needed
  - Reduces the risk of compromise of confidential information, including
    - confidential personal information addressed by privacy laws and regulations
    - intellectual property and proprietary business data

Functions potentially involved in a cybersecurity program

- Board/those charged with governance
- CEO
- Senior management
- Risk management and compliance
- General counsel
- CFO/finance
- COO/operations
- CIO
- IT security
- Privacy office
- Others

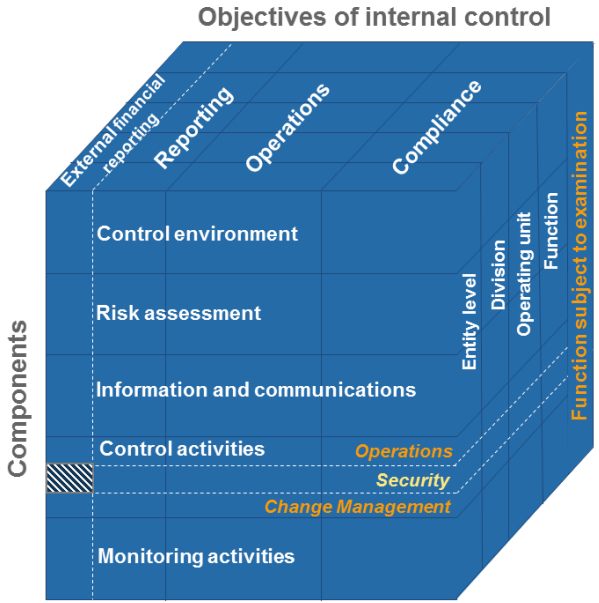
Information regarding cybersecurity at an entity is needed

- Decision makers include
  - Those charged with governance
  - Investors
  - Customers
  - Business partners
  - Regulators
- The information needed is mostly unique from what is needed for financial reporting purposes

Two distinct needs for cybersecurity information

- As it relates to financial reporting of entities
  - Impact of business risks on financial audit
  - Impact of cybersecurity incident's on an entity's financial position and results
- As it relates to the business operations and compliance of entities
  - Evaluation of users' risks
  - Evaluation of the impact of entity's operations on users' operations

Internal control and cyber security at an entity



Security controls addressed as part of a financial audit

Controls addressed as part of a cybersecurity attestation engagement

AICPA/CAQ response

- Response of the profession in the US:
  - Center for Audit Quality has been leading a discussion on the effect of cybersecurity on financial audits
    - Separate and distinct from the AICPA cybersecurity attestation project
    - Communication to firms
  - AICPA has initiated a project to develop subject matter and attestation guidance for reporting on cybersecurity as it relates to the operations and compliance of an entity

CAQ communications to firms

Auditor responsibilities

- Identifying and assessing the risk of material misstatement
  - Understanding the nature of the entity and its environment
  - Understanding of the effect of IT on financial reporting and ICFR
  - Consideration of financial statement misstatement risk
- Assess the impact of any breaches on financial reporting and ICFR

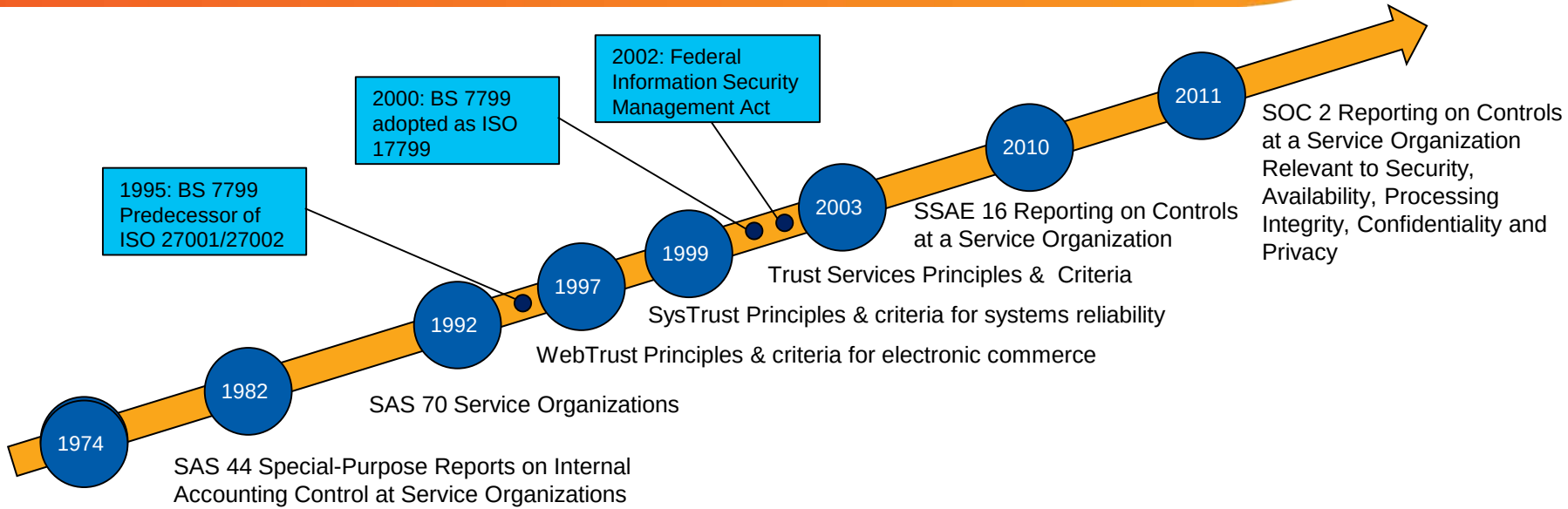
AICPA cybersecurity attestation project

- Working group under the Assurance Services Executive Committee
- Support from the CAQ
- Member firm support
- Outreach to users and industry as the project develops

AICPA cybersecurity attestation project

- Goal
  - Identify the information needed by users for decision making
  - Develop cybersecurity information subject to engagement
  - Identify suitable criteria for evaluating the subject matter
  - Develop practitioner guidance

Timeline of AICPA IT Security Auditing



Key considerations for practitioners

- Cybersecurity is a business issue with financial statement implications, affecting customers, business partners, investors and the public
- Entities of all sizes and in all industries are affected
- Practitioners need to be able to support stakeholder by:
  - Assessing the impact of a cybersecurity incident on financial statements
  - Providing independent assessments of cybersecurity risk management to concerned stakeholders
  - Providing an independent perspective regarding the entity's cybersecurity risks and risk management program to those charged with governance and senior management

Near term developments in cybersecurity—some thoughts

Considerations going forward

- Standards potentially affected by further cybersecurity developments
  - ISA 315 – Identifying and Assessing the Risks of Material Misstatement through understanding the Entity and its Environment
  - ISA 330 – The Auditor's Responses to Assessed Risks
  - ISA 402 – Audit Considerations Relating to an Entity Using a Service Organization
  - ISA 620 – Using the Work of an Auditor's Expert
  - ISAE 3402 – Assurance Reports on Controls at a Service Organization
- Standards used to report on cybersecurity program
  - ISAE 3000 -- Assurance Engagements Other Than Audits or Reviews of Historical Financial Information

Questions?

www.iaasb.org