New AICPA Standards Aim to Take a Bite Out of Cybercrime

By C. William (Bill) Thomas, CPA, Ph.D.

Adapting to business in cyber space has been both terrific and terrifying. From automobiles to air conditioner thermostats, things are going digital. Horror stories of foreign and domestic hackers stealing identities, account numbers, information and even elections have awakened us to a whole new world of potential threats, as well as the need for taking new actions for data protection. Given the reputation of CPAs as trusted business professionals, it is logical for business to turn to us for help.

SOC for Cybersecurity

To help businesses meet the growing challenges of cyber risk, the Assurance Services Executive Committee (the Committee) of the American Institute of CPAs (AICPA) has introduced a market-driven, flexible and voluntary cybersecurity risk management reporting framework. The framework is a key component of a new System and Organization Controls (SOC) for Cybersecurity engagement, through which a CPA reports on an organization's enterprise-wide cybersecurity risk management program. This framework will enable all organizations in a wide variety of industries to take a proactive and agile approach to cybersecurity risk management and to communicate with stakeholders regarding those activities.

The framework contains roles for both financial management of the entity and the CPA practitioner. Management is responsible for preparing information about the entity's cybersecurity risk management program. This information includes a narrative description of the program that describes how the entity identifies its most sensitive information, ways in which the entity manages its cybersecurity threats and the key security policies designed to protect the entity's information assets against those threats. It also includes management's assertion about whether the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives. The CPA practitioner is responsible for performing an attestation examination and providing a report that expresses an opinion on management's description and on the effectiveness of controls within the program.

Criteria for Describing and Evaluating Controls

The Committee has developed two distinct, but complimentary sets of criteria for use in the description and examination of the cybersecurity risk management program. Use of common criteria enhances comparability between reporting entities with regard to cybersecurity matters. The two sets of criteria include: (1) description criteria for use in management's narrative description of its program and (2) control criteria for the CPA practitioner's use in a consulting or attestation engagement.

Description criteria are a set of benchmarks for use when preparing the entity's description of its cybersecurity risk management program. The entity's program consists of the policies, processes and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives, as well as how it detects, responds to, mitigates and recovers from such events. Description criteria include (1) nature of the business and operations; (2) nature of the information at risk; (3) objectives of the entity's cybersecurity risk management program; (4) factors that affect the entity's cybersecurity risk; (5) the entity's cybersecurity risk governance structure; (6) the entity's risk assessment process; (7) processes by which risks are communicated; (8) ways the entity monitors risk; and (9) the entity's cybersecurity control processes.

Control criteria are used in either consulting or attestation engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality or privacy of information and systems. AICPA has revised a set of Trust Services Criteria for this purpose that may be used by the CPA practitioner. These criteria align with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2013 *Internal Control – Integrated Framework*, to better address cybersecurity risks and increase flexibility in application across an entire entity, including at a subsidiary, division or operating unit level within a function relevant to an entity's operational, reporting or compliance objectives. Organizations may also use other criteria, as long as they are appropriate for the engagement.

Attestation Guide Coming Soon

The Committee is developing an attestation guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, expected later this year. In addition to providing guidance in performing attestation engagements, this guide may be helpful to CPAs engaged to provide cybersecurity advisory services to an organization that may help them improve their cybersecurity risk management programs. In addition, use of the description criteria and control criteria may assist management of various entities in establishing a common approach and language to use when communicating with their boards and other stakeholders about the entity's cybersecurity risk management efforts. To read further, consult https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx. ■

C. William Thomas, CPA, Ph.D. is the J.E. Bush professor of accounting in the Hankamer School of Business at Baylor University in Waco. Thomas can be reached at Bill_Thomas@baylor.edu.