Cybersecurity Risk Management
Fact Sheet

Market Need
Cybersecurity is one of the top issues currently on the minds of management and boards in just about every company in the world — large and small, public and private. Managing this business issue is especially challenging because even an organization with a highly mature cybersecurity risk management program will still retain a residual risk that a material cybersecurity breach could occur and not be detected in a timely manner.

Organizations and their stakeholders need timely, useful information on cybersecurity risk management efforts. Corporate directors and senior management have begun requesting reports on the effectiveness of their cybersecurity risk management programs from independent third-party assessors. Yet today there is no widely accepted approach or professional standard for providing security assessments. Accordingly, the American Institute of CPAs (AICPA) is working to develop a voluntary, market-based solution to evaluating cybersecurity risk management that could enhance public trust in the effectiveness of a company’s cybersecurity programs.

Role of the CPA
As a profession, we have decades of experience in providing information security services. Today, four of the leading 10 information security and cybersecurity consultants are public accounting firms. Auditors are experts at risk and control assessment, and have people closest to controls who can yield efficiency gains and synergies.

Many public accounting firms are already providing cybersecurity advisory engagements, helping clients identify key risk areas, design and develop cyber risk management programs, and assess cyber-readiness. There is an opportunity for the profession to meet evolving market needs by bringing this subject matter expertise to bear, and combining it with the discipline inherent in the external audit community, through trusted, independent cybersecurity assurance services.

Foundation for Cyber Risk Management Reporting and Examination
The AICPA is proposing a reporting framework through which organizations can communicate relevant information regarding their cybersecurity risk management efforts to meet the needs of a broad range of stakeholders. We believe that an entity, its board of directors and its stakeholders will be best served if a defined set of information intended to meet their common needs addresses cybersecurity concerns.

The intent of this framework is ultimately to support voluntary examination-level cybersecurity attestation engagements that meet the informational needs of a broad range of potential report users, and leverage the core competencies of CPAs as providers of these services in accordance with Professional Standards. Most companies, however, have not yet reached the necessary level of maturity in their cybersecurity risk management to undergo an attestation engagement. In the meantime, the framework we have developed can be leveraged for cybersecurity advisory engagements, and used directly by company management in communicating with their boards and investors, establishing a common approach and language for cybersecurity risk management and reporting.
Criteria
To meet the aforementioned objective, the AICPA developed a new set of description criteria for an entity to use in designing and describing its cybersecurity risk management program. The proposed description criteria are intended to establish the policies, processes and controls that should be addressed for cybersecurity risk management, thereby giving organizations a level of comfort that they have covered all of their bases, regardless of which framework(s) they have chosen to implement internally. Accordingly, in the development of the criteria, commonly used cybersecurity risk management frameworks such as the NIST Critical Infrastructure Cybersecurity Framework and ISO 27001/27002 were considered. They are also aligned to the 2013 COSO Internal Control — Integrated Framework, to facilitate a strategic, objectives-based approach that can be integrated with companies’ broader enterprise risk management efforts.

In addition to the opinion on management’s description of its cybersecurity risk management, the examination engagement will include an opinion on the effectiveness of the cybersecurity controls. Since 1997, the AICPA has maintained a set of criteria used to evaluate the security, availability, processing integrity, confidentiality and privacy of entity systems. These control criteria, known as the Trust Services Criteria, have been updated for use in the proposed cybersecurity engagement.

Both sets of criteria are being exposed for public comment through Dec. 5, 2016, and can be accessed along with supporting materials.

 Guidance
In addition to the two sets of proposed criteria, the AICPA Assurance Services Executive Committee (ASEC) Cybersecurity Working Group is collaborating with the AICPA Auditing Standards Board (ASB) to develop a cybersecurity attestation guide for publication in the first quarter of 2017, which will provide guidance to CPAs on how to perform and report on cybersecurity examination engagements in accordance with the AICPA attestation standards.

The entity-level cybersecurity reporting framework encompasses three key sets of information that, taken together, could enhance a board’s confidence in the cybersecurity information management provides, and offers a way of communicating such confidence to stakeholders when needed. They are:

1. Management’s Description: The first component is a management-prepared narrative description of the entity’s cybersecurity risk management program. This description is designed to provide information about how the entity identifies its sensitive information and systems, the ways in which the entity manages the cybersecurity risks that threaten it and a summary of controls implemented and operated to protect the information and systems against those risks. This provides the context needed to understand the conclusions management expresses in its assertion, and by the auditor in its report, about the effectiveness of the controls included in the entity’s cybersecurity risk management program.

2. Management’s Assertion: Management also provides an assertion that the controls implemented as part of the program were effective to achieve the entity’s cybersecurity objectives.

Since 1997, the AICPA has maintained a set of criteria used to evaluate the security, availability, processing integrity, confidentiality and privacy of entity systems.
3. The Practitioner’s Opinion: The final component in this approach is a CPA’s opinion on the description of the entity’s cybersecurity risk management program (i.e., its completeness and accuracy) and the effectiveness of controls within that program to achieve the entity’s cybersecurity objectives.

Management’s description of the entity’s cybersecurity risk management program in accordance with the AICPA’s description criteria, and also management’s assertion that the controls implemented as part of the program are effective to achieve the entity’s cybersecurity objectives, can greatly facilitate management and board accountability as well as investor engagement with companies on cyber maturity. The AICPA’s guidance, however, is flexible in the sense that it does not require the use of the AICPA-developed description criteria and Trust Services Criteria, rather management and the auditor may use any suitable description criteria and controls criteria. It is also scalable to the business unit or segment level.

Related Efforts

In 2017, the AICPA will begin work on a new attestation guide for supply-chain cybersecurity risk, which will enable practitioners to provide reports to customers of manufacturers and distributors on cybersecurity risk in their supply chains and distribution networks.

The AICPA also plans to release an updated version of the SOC 2® Guide: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, following the publication of the revised Trust Services Criteria on which these engagements are based.

Both of these engagements will focus on system-level assurance, as opposed to the new cybersecurity attestation engagement described in the preceding section, which is intended to cover cybersecurity risk at the entity level.

Conclusion

Our intent is to establish a common underlying language for cybersecurity risk management and reporting — almost akin to US GAAP or IFRS for financial reporting. In doing so, we recognize that cybersecurity is not just an IT problem; it’s an enterprise risk management problem that requires a global solution, and we’ve developed robust and complete criteria from that perspective, as a tool for strategic, objectives-based cybersecurity risk management.

We believe this is a critical first step to enabling a consistent, market-based, business-based mechanism for companies to effectively communicate with key stakeholders on how they are managing cybersecurity risk. As cybersecurity maturity increases, it will also serve as the requisite foundation for high quality, independent third-party assurance services, which will necessarily evolve over time to address changing market dynamics and needs.