Framework Offers Companies Solution for Cybersecurity Risk

Introduction

Cybersecurity attacks can threaten a business of any size and can originate from internal or external sources. A cybersecurity breach can result in both financial loss—loss of client funds, costs of litigation, disruption of business, costs associated with notification and monitoring, and fines and penalties—and reputational damage, which can result in loss of customers, vendors, and service providers. According to a 2017 study by the Ponemon Institute, the average cost of a data breach for incidents with less than 10,000 compromised records was $1.9 million.[1]

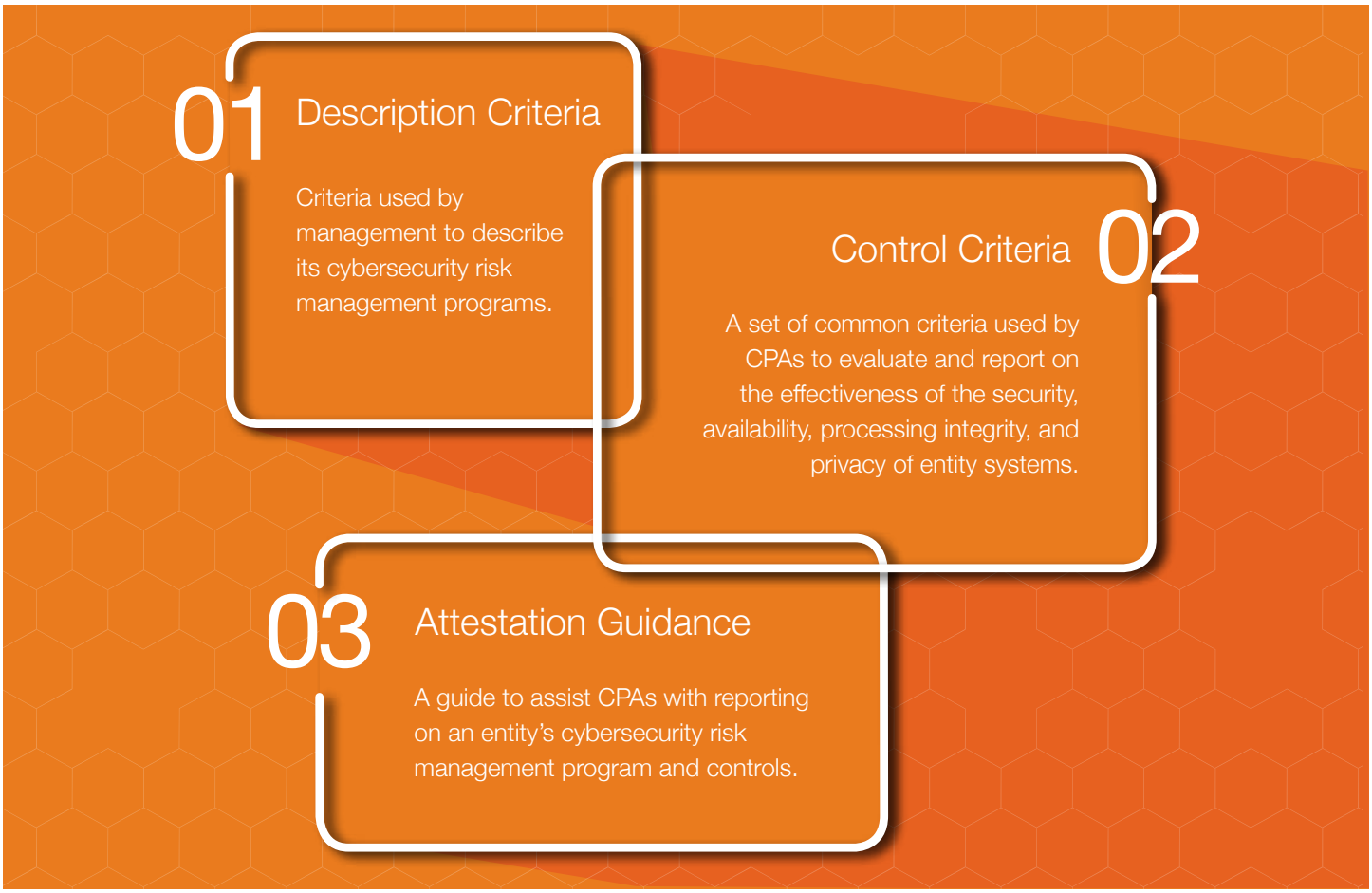
In response to these increasing cybersecurity threats throughout virtually every industry, the American Institute of Certified Public Accountants (AICPA) released a cybersecurity risk management reporting framework in April 2017. This framework allows an independent certified public accountant (CPA) to conduct a System and Organization Controls (SOC) for Cybersecurity engagement to report on the design and effectiveness of an organization's overall cybersecurity risk management program. The AICPA has stated that this examination is "designed to provide report users with information to help them understand management's process for handling enterprise-wide cyberrisks."[2]

1 Ponemon Institute, *2017 Cost of Data Breach Study* (June 2017).

2 "SOC 2® examinations and SOC for cybersecurity examinations: Understanding the key distinctions." AICPA, 2017. www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/soc-2-vs-cyber-whitepaper-web-final.pdf.

What Is the SOC for Cybersecurity and Cybersecurity Risk Management Framework?

The cybersecurity risk management framework serves as the backbone of this new type of SOC report. The framework was developed collaboratively by the AICPA Assurance Services Executive Committee and the Auditing Standards Board, with a goal of creating a broad-range, cross-industry common language for communicating and reporting on an organization's cybersecurity risk management approach. The framework consists of these three facets:



The framework around which the SOC for Cybersecurity is designed can be used by CPAs to assist their clients in two ways. First, based on the framework criteria, CPAs can work with their clients to evaluate and improve their cybersecurity risk management programs. CPAs can provide an array of services, depending upon the stage of the client's program development. These services range from assisting management with the development of the cybersecurity risk management program to providing a pre-assessment to identify potential weaknesses and gaps in the program before undergoing a full examination. Second, an independent CPA can be engaged to provide a cybersecurity risk management examination once the client is confident that his or her cybersecurity risk management program is fully developed and free of gaps.

What Is Included in the SOC for Cybersecurity Report?

A cybersecurity risk management examination allows a CPA to provide an opinion, via the SOC for Cybersecurity Report, on an entity's cybersecurity risk management program. The report includes three areas of an entity's cybersecurity policies, procedures, and plans. The first area is management's description of the entity's cybersecurity risk management program. The AICPA has identified nine items to be included in management's description, as follows:[3]

01 **Nature of Business and Operations** – Information about the nature of the entity's business and operations.

02 **Nature of Information at Risk** – The principle types of sensitive information susceptible to cybersecurity risk.

03 **Cybersecurity Risk Management Program Objectives** – The entity's objectives related to the availability, confidentiality, and integrity of data, as well as the integrity of processing the data.

04 **Factors That Have a Significant Effect on Inherent Cybersecurity Risks** – Including technologies, connection types, use of service providers, delivery channels, and organizational characteristics specific to the entity.

05 **Cybersecurity Risk Governance Structure –** The process for establishing, maintaining, and communicating integrity and ethical values; providing board oversight; establishing accountability; and ensuring the use of qualified personnel.

06 **Cybersecurity Risk Assessment Process –** The process of identifying, assessing, and managing cybersecurity risks.

07 **Cybersecurity Communications and the Quality of Cybersecurity Information –** The entity's process for communicating cybersecurity objectives, expectations, and responsibilities to internal and external parties.

08 **Monitoring of the Cybersecurity Risk Management Program –** By what means the entity assesses how effectively cybersecurity controls are operating.

09 **Cybersecurity Control Processes –** The processes used for developing a response to assessed risks.

The second area included in the SOC for Cybersecurity Report is management's assertion that its description is prepared in accordance with the aforementioned description criteria, and that the controls identified in the description were effective in meeting the entity's cybersecurity objectives. The third area is the independent CPA's opinion on management's description of the controls, and their effectiveness, for meeting the entity's objectives.

3 "Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program." AICPA Assurance Services Executive Committee (April 15, 2017). www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/description-criteria.pdf.

How Does the SOC for Cybersecurity Differ from the SOC 2?

Many readers may be familiar with the AICPA's SOC 2 examination, which also involves a CPA's testing of the operating effectiveness of controls. Although the SOC 2 may initially appear to be a similar engagement to the SOC for Cybersecurity, there are some significant differences. Depending on the organization undergoing the examination, there are important considerations for determining the appropriate SOC engagement.

The first consideration is the type of entity eligible for each kind of SOC examination. The SOC 2 is limited to service organizations, or business units or specific service lines within a service organization. Generally, any entity can obtain a SOC for Cybersecurity Report. Under a SOC 2 examination, the service organization's management has an option to include, or carve out, a subservice organization in the description of its services. The SOC for Cybersecurity does not present this option, and any subservices organizations or third party with access to company data must be included in the entity's cybersecurity risk management program.

The SOC 2 covers controls over the security, availability, and processing integrity of a system, or the privacy or confidentiality of information processed by the system. In evaluating controls during the SOC 2 examination, a CPA must test the controls against the Trust Services Criteria. As mentioned previously, in a SOC for Cybersecurity examination, controls—as outlined within the AICPA's description criteria— are measured against a control criterion. The SOC for Cybersecurity allows several control criteria (including the Trust Services Criteria, the International Organization for Standardization's 27001 Information Security Standard, and the National Institute of Standards and Technology's Cybersecurity Framework) for use in evaluating controls. The SOC for Cybersecurity permits management to select a control criterion that is most suitable to the specific entity and the entity's cybersecurity risk management program.

The distribution of a SOC 2 report is restricted to specified users who have explicit knowledge and a thorough understanding of the service organization and its system. This is because the SOC 2 reports on details of the controls tested by the CPA and the specific results of the testing. During a SOC for Cybersecurity examination, the CPA tests controls in a similar manner to the SOC 2 examination, but the details of each test performed are not included in the report. As a result, the SOC for Cybersecurity Report is appropriate for general, unrestricted distribution and can be disseminated to a wider audience and used for sales and marketing purposes. It could be used to provide current and prospective customers insight into a company's cybersecurity controls.

How PYA Can Help

With cybersecurity proving to be of paramount concern, organizations are compelled to demonstrate their internal controls and processes can effectively address detection, response, mitigation, and recovery following a cybersecurity attack or breach. PYA, a nationally ranked certified public accounting firm, assists organizations by conducting both SOC cybersecurity and SOC 2 examinations. We can also perform a gap analysis to determine if your organization is ready for SOC or SOC 2.

Our IT Risk Management team, under the direction of a former hospital CIO, works to diagnose IT risks to mitigate regulatory, financial, and reputational dangers.

For more information about SOC, SOC 2, or risk mitigation, contact:

Mike Shamblin
Managing Principal of Audit & Assurance Services
mshamblin@pyapc.com
(800) 270-9629

Barry Mathis
Principal
bmathis@pyapc.com
(800) 270-9629