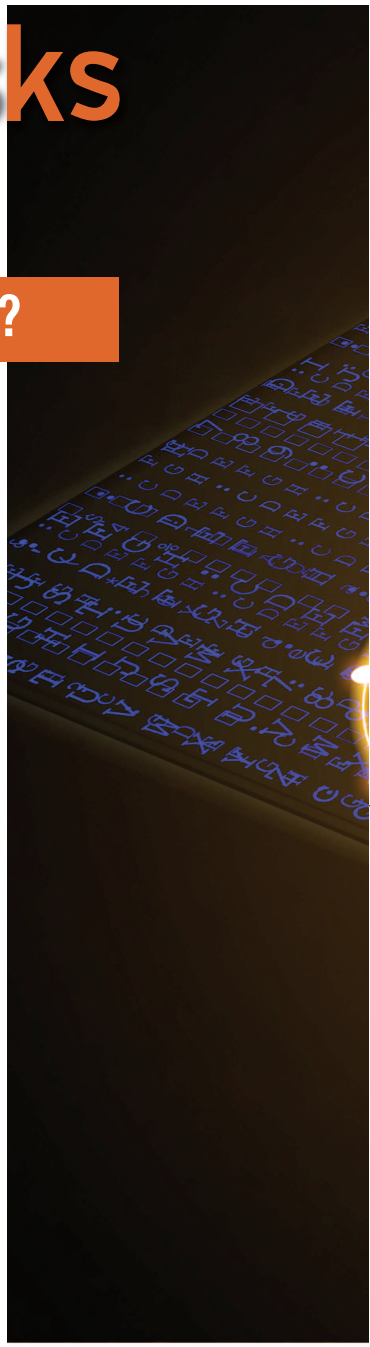
Cybersecurity Risks and Controls

Is the AICPA's SOC for Cybersecurity a Solution?



By Abdullah Al-Moshaigeh, Denise Dickins, and Julia L. Higgs

IN BRIEF

As high-profile corporate data breaches continue to occupy headline space, businesses are grappling with how to confront a serious risk that changes on an almost daily basis. In an effort to help, the AICPA has released a framework for measuring, addressing, and monitoring cybersecurity risk, called System for Organization Controls for Cybersecurity (SOC-C). This article provides a detailed discussion of SOC-C, reviewing the services and activities it prescribes and the benefits and challenges it presents to CPAs and management.

Cybersecurity is one of the biggest risks modern companies face. In 2017, the average cost of a data breach in the United States was $7.35 million, or approximately $225 for each lost or stolen electronic record. The costs include identifying the breach, notifying the affected parties, downtime, recovery, repairs, lawsuits, and customer losses (*2018 Cost of a Data Breach Study,* IBM, https://ibm.co/2WJ475C).

Cybersecurity threats are ubiquitous; they affect all businesses across all industries. Even for a small business, breaches are costly. The data suggest that the cost of a breach isolated to payroll records of a business with only five employees, bimonthly pay periods, and operating for 10 years could be nearly $300,000.

Federal and state regulators have not ignored the importance of companies protecting their electronic assets. In 2011, the SEC issued *CF Disclosure Guidance: Topic 2—Cybersecurity,* and in February 2018, it issued additional interpretive guidance about companies' cybersecurity risk and incident disclosures. These rules require that companies 1) maintain comprehensive policies and procedures related to cybersecurity risks and incidents; 2) establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity; and 3) have policies and procedures in place to thwart insider trading during the period between when a material cybersecurity incident is discovered and is publicly disclosed.

In March 2017, the New York State Department of Financial Services (DFS) issued 23 NYCRR 500, *Cybersecurity Requirements for Financial Services Companies.* With limited exceptions, entities under DFS's jurisdiction (e.g., banks, insurance companies, broker-dealers, charitable foundations) are required to specifically assess the risk of cybersecurity and design a program to address these risks in a "robust fashion," which includes the designation of a chief information security officer (CISO), staff training, establishment of multifactor access authentication, penetration testing, and timely reporting of incidents. Other states and state agencies have, or are in process of developing, cybersecurity-related rules and regulations (e.g., Massachusetts, Colorado, Vermont).

Reputational and out-of-pocket cybersecurity costs create significant pressure on entities to ensure that information shared with customers, vendors, employees, and investors is safe and to comply with regulations. This article describes how entities might address these objectives by engaging a CPA to perform the services pre-

scribed by the AICPA's recently issued System for Organization Controls for Cybersecurity (SOC-C) and discusses the benefits and limitations of SOC-C services.

Addressing Cybersecurity Risks

The impetus to establish and evaluate the design and operating effectiveness of controls intended to address an entity's risks is not new to managers and accountants. Companies often use the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management (ERM)—Integrated Framework to identify important risks that may adversely affect the achievement of business strategies, as well as to design controls to address and monitor these risks. Managers and auditors use COSO's Internal Control—Integrated Framework to evaluate the design and operating effectiveness of systems of internal control over financial reporting (ICFR).

Frameworks designed to address information technology risks have been developed by the Information Systems Audit and Control Association (ISACA) and the

Exhibit
SOC for Cybersecurity Description Criteria

Category	Description Criteria
Nature of business and operations	**DC1:** The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed.
Nature of information at risk	**DC2:** The principal types of sensitive information created, collected, transmitted, used, or stored by the entity.
CRMP objectives (cybersecurity objectives)	**DC3:** The entity's principal CRMP objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing. **DC4:** The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives.
Factors that have a significant effect on inherent cybersecurity risks	**DC5:** Factors that have a significant effect on the entity's inherent cybersecurity risks, including the 1) characteristics of technologies, connection types, service providers, and delivery channels used by the entity, 2) organizational and user characteristics, and 3) environmental, technological, organizational, and other changes at the entity and in its environment during the period covered. **DC6:** For security incidents that 1) were identified during the 12-month period preceding the period-end date of management's description and 2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: a) nature of the incident; b) timing surrounding the incident; and c) extent (or effect) of those incidents and their disposition.
Cybersecurity risk governance structure	**DC7:** The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the CRMP. **DC8:** The process for board oversight of the entity's CRMP. **DC9:** The established cybersecurity accountability and reporting lines. **DC10:** The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities.
Cybersecurity risk assessment process	**DC11:** The process for 1) identifying cybersecurity risks and environmental, technological, organizational, and other changes that could have a significant effect on the entity's CRMP and 2) assessing the related risks to the achievement of the entity's cybersecurity objectives. **DC12:** The process for identifying, assessing, and managing the risks associated with vendors and business partners.
Cybersecurity communications and quality of cybersecurity information	**DC13:** The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's CRMP, including 1) objectives and responsibilities for cybersecurity and 2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both. **DC14:** The process for communicating with external parties regarding matters affecting the functioning of the entity's CRMP.
Monitoring of the CRMP	**DC15:** The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity. **DC16:** The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors.
Cybersecurity control processes	**DC17:** The process for developing a response to assessed risks, including the design and implementation of control processes. **DC18:** A summary of the entity's IT infrastructure and its network characteristics. **DC19:** The key security policies and processes implemented to address the entity's cybersecurity risks, including the following: a) Prevention of intentional and unintentional security events; b) detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents; c) management of processing capacity to provide for continued operations during security, operational, and environmental events; d) detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability; e) identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period.

Source: AICPA (http://www.aicpa.org) CRMP=Cybersecurity Risk Management Program

International Organization for Standardization (ISO) [Control Objectives for Information and Related Technologies (COBIT) and ISO 27001 Information Security Management, respectively]. The National Institute of Standards and Technology (NIST) describes a continuous improvement process framework designed to specifically assist companies in developing a robust process to identify and address cybersecurity risks. The NIST framework includes the following control criteria:

- Identify—develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- Protect—develop and implement appropriate safeguards to ensure delivery of critical services
- Detect—develop and implement appropriate activities to identify the occurrence of a cybersecurity incident
- Respond—develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- Recover—develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Just as COSO's internal control framework helps managers design and evaluate controls intended to address financial reporting risks, the NIST framework can help managers and board members reduce the risk of security breaches and comply with federal and state regulations by serving as a guideline to design and evaluate controls intended to address cybersecurity risks. The AICPA also has a cybersecurity risk framework that, as described below, was developed to be used in conjunction with a SOC-C engagement.

SOC for Cybersecurity

SOC-C was developed to "enhance public trust in entity-prepared communications about the effectiveness of their cybersecurity risk management programs" (*Cybersecurity Risk Management Reporting Fact Sheet,*

http://bit.ly/2Hj1wdC). SOC-C's process is similar to evaluating and reporting on the design and effectiveness of ICFR (required for publicly traded companies by PCAOB Auditing Standard 2201, *An Audit of Internal Control over Financial Reporting*) in that it gives management the responsibility to design and implement a cybersecurity risk management program (CRMP) and to evaluate whether program controls are effective to achieve management's objectives. A CRMP is defined by SOC-C as "the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented." It is also management's responsibility to identify and document important information assets, possible threats to those assets, controls that reduce the likelihood of threats, and security breach response plans. CPAs may then independently provide positive assurance about whether controls are designed and operating effectively.

SOC-C describes two services: a nonattest consulting engagement and an examination of the design and operating effectiveness of cybersecurity controls. In a SOC-C consulting engagement, CPAs provide guidance to an entity developing a CRMP, helping to identify control deficiencies and making recommendations for improvement using the AICPA's cybersecurity risk framework. This framework serves as a tool for both management and CPAs in preparing for and conducting a SOC-C engagement. It includes 19 description criteria that, along with implementation guidance, are summarized in nine categories (see the *Exhibit*).

In a SOC-C examination, the CPA forms a conclusion about the design of an entity's CRMP and the operating effectiveness of its program controls based on an independent evaluation and testing. Like an auditor's reporting on the design and operating effectiveness of ICFR, which commonly uses the COSO internal control framework as a basis for evaluation, the basis for the CPA's conclusion about a client's CRMP should be grounded in a framework with specific, relevant control criteria like those described by NIST, or the AICPA's Trust Services Criteria (http://bit.ly/2WQVTIE). Management may select any description or control criterion as the basis for its assertion about the entity's CRMP and program controls, so long as the criterion selected is relevant, objective, measurable, and does not omit factors that could reasonably be expected to impact users' decisions.

The SOC-C examination report includes three sections: 1) management's description of its CRMP, 2) management's assertion

about whether the description is in accordance with the description criteria and the program controls are effective based on given control criteria, and 3) the CPA's conclusion about the CRMP and program controls. The report is intended for general use.

In comparison, before SOC-C, CPAs could be engaged to provide companies with positive assurance that certain controls of service organizations were designed or operating effectively; these services are commonly referred to as SOC 1, 2 or 3. CPAs are typically engaged to perform SOC services by companies who want to provide their customers with an independent opinion about the adequacy of their internal controls. For example, Amazon Web Services provides SOC reports to clients who purchase website hosting services. The reports describe the controls Amazon has in place and include attestation by a CPA as to whether the controls meet control criteria described by Amazon. A comparison of the purpose and intended users of SOC services is provided on the AICPA's website (http://bit.ly/2EhFN3A).

Benefits and Limitations

SOC-C benefits apply equally to all entities, be they privately held, publicly traded, for-profit, or not-for-profit. Arguably, the greatest benefit of SOC-C is derived from its requirement that management identify, document, and evaluate its CRMP. If an entity has dedicated little time to cybersecurity risks, the description and control criteria provide a framework that CPAs can use to help management develop a robust CRMP. If the entity is sophisticated in identifying and responding to cybersecurity risks, the description and control criteria will help identify gaps in its CRMP. This comparison process is similar to when the COSO internal control framework was updated in 2013 to include a heightened focus on fraud, IT, and outsourcing risks, and many entities found control gaps in these areas. To accomplish either a start-from-scratch or critical evaluation of CRMP, CPAs should recommend that employees with the appropriate skills and influence be included in the process. These might include the CFO, CISO, IT staff, and internal auditors.

> SOC-C describes two services: a nonattest consulting engagement and an examination of the design and operating effectiveness of cybersecurity controls.

A SOC-C consulting project provides an objective assessment of an entity's residual cybersecurity risk, helps establish a tone at the top that prioritizes cybersecurity risk, and helps demonstrate compliance with federal and state cybersecurity regulations. A SOC-C examination adds credibility to an entity's CRMP and signals external stakeholders that management intends to maintain a strong system of cybersecurity controls. A SOC-C examination may even reduce an entity's cybersecurity insurance premiums.

On the other hand, the examination does not guarantee that a security breach will not occur or will be detected in a timely manner. Like all internal controls, CRMP controls reduce the likelihood of errors and fraud, but they cannot prevent them. In addition, the form and origination of security threats is constantly changing. A well-controlled technology environment today could be at risk of being breached tomorrow. The evaluation of all control systems must be continuous, not one-and-done.

Of concern is management's selection of the criteria against which the entity's CRMP is to be evaluated; management may choose to include all, or omit some, specific criteria. For example, the AICPA's Trust Services' control criteria are security, availability, processing integrity, confidentiality, and privacy. If management chooses to omit evaluation of the privacy criteria, the SOC-C report would be silent with respect to the design adequacy and operating effectiveness of privacy program controls, possibly creating an expectations gap regarding CPAs' responsibilities. Users of SOC-C reports must carefully evaluate the extent of services performed when determining whether their needs are met and not overrely on the results of a SOC-C examination. Just as importantly, CPAs should evaluate engagement risk before agreeing to undertake SOC-C services.

As an example, Ernst & Young (EY) certified certain IT security controls of Equifax using ISO Standard 27001 prior to Equifax's 2017 security breach (Francine McKenna, "Unit of Equifax's Auditor EY Certified the Information Security That Was Later Breached," MarketWatch, Dec. 20, 2018, https://on.mktw.net/2VzURUU). Although Ernst & Young may not ultimately be held liable in ensuing shareholder lawsuits against Equifax, it is highly likely that its costs of information production alone will far exceed the fees billed for the provided certification services. It is important that CPAs identify the potential expectations of users of the results of SOC-C engagements, as well as have the relevant skills to perform SOC-C services.

For CPAs who decide to offer SOC-C services, IT skills and current experi-

ence are important. Credentials like the Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP) can help deepen relevant skills. In addition, the AICPA offers a Cybersecurity Advisory Certificate. The program, which takes 15.5 hours to complete, is described as for "practitioners who are interested in providing cybersecurity advisory services and want to build their competencies in and understanding of these types of services." It also cautions, "Participants must have either IT expertise or access to IT professionals who possess the skills to perform this work." Given the pace of change in cybersecurity risk, CPAs who want to build a practice in SOC-C should consider hiring individuals with specialized IT and cybersecurity skills.

Solving Problems before They Become Problems

The result of a cybersecurity breach can, on a proportionate basis, be equally as costly to a small nonprofit as it is to a large, publicly traded company. Building and maintaining a robust CRMP is a continuous effort that requires the commitment of board members and senior management, as well as investment in capital and human assets. Using SOC-C's description and control criteria as part of a consulting engagement to help an entity design, implement, and evaluate the operating effectiveness of its CRMP can be valuable to management and board members, while performing an independent examination of the design and operating effectiveness of an entity's cybersecurity controls can enhance public trust in its communications about the effectiveness of its CRMP.

While there are other cybersecurity-related certification options (e.g., ISO 27001, HITRUST), SOC-C may be a more cost-effective solution in many contexts. SOC-C's common criteria for disclosure and evaluation of an entity's CRMP cover a broad range of stakeholders' cybersecurity information needs and concerns, thereby reducing the number of certifications that might otherwise be required. In addition, management selects the control criteria to be evaluated, which increases flexibility. Importantly, SOC-C services can only be provided by independent CPAs acting in accordance with the AICPA's Code of Professional Conduct. ❑

***Abdullah Al-Moshaigeh, PhD**, is an adjunct professor of accounting at Florida Atlantic University, Boca Raton, Fla. **Denise Dickins, PhD, CPA, CIA,** is a professor of accounting at East Carolina University, Greenville, N.C. **Julia L. Higgs, PhD, CPA,** is a professor of accounting at Florida Atlantic University.*