SOC for Cybersecurity: Reporting on Your Cybersecurity Risk Management Program

CYBERGUARD COMPLIANCE

Table of Contents

Introduction of SOC for Cybersecurity Reports

Cybersecurity is a major concern amongst organizations of all sizes. Stakeholders need critical information about how companies are managing cybersecurity threats and whether companies have effective processes and controls in place in order to prevent and detect breaches that could disrupt their business, result in financial losses, or destroy their reputation. According to the results of a survey of 591 IT and IT security practitioners, companies experience an average of more than one cyber-attack per month, and incur annual costs of approximately $3.5 million as a result of those attacks. The survey, sponsored by BrandProtect and conducted by the Ponemon Institute, also found that fully 79 percent of respondents said they lack comprehensive strategies to identify and mitigate those attacks.

While 59 percent of respondents said the protection of intellectual property from external threats is essential or very important to the sustainability of their companies, 64 percent of security leaders said they lack the tools and resources required to monitor, 62 percent lack the tools and resources required to analyze and understand, and 68 percent lack the tools and resources required to mitigate external threats.

Managing cybersecurity threats is especially challenging because even a company with a highly mature Cybersecurity Risk Management Program is susceptible to breaches that may not be detected in a timely manner. In 2017, the American Institute of CPAs (AICPA) developed a cybersecurity risk management reporting framework. The SOC for Cybersecurity framework facilitates communication between companies and their various stakeholders who have a vested interest in their Cybersecurity Risk Management Program. Additionally, since SOC for Cybersecurity is an examination report which must be performed by a licensed CPA firm, the stakeholders can rest assured the Cybersecurity Risk Management Program was examined by an independent third party.

Need for SOC for Cybersecurity Reports

There have been numerous high-profile cybersecurity attacks compromising critical data of major corporations, governments, non-profits, and small-to-medium sized organizations over the past few years. The effects of these breaches include:

- Reputational damage
- Loss of intellectual property
- Disruption of key business operations
- Fines and penalties assessed by regulatory bodies
- Litigation and remediation costs

- Exclusion from strategic markets

These embarrassing and costly effects of cybersecurity attacks has led to increased scrutiny on a company's Cybersecurity Risk Management Program. Increasingly, various stakeholders (e.g. investors, customers, business partners, regulators, board of directors, etc.) are demanding proof of the preparedness and effectiveness of the company's Cybersecurity Risk Management Program.

Managing this business issue is especially challenging because even an organization with a highly mature cybersecurity risk management effort will still retain a residual risk that a material cybersecurity breach can occur and not be detected in a timely manner. Furthermore, the need for cybersecurity risk management is ever-increasing because of a combination of factors, including:

- A company's dependency on information technology;
- The complexity of information technology networks;
- The extensive reliance on third parties; and
- Human nature (e.g., susceptibility to social engineering).

Overview of the SOC for Cybersecurity Report

SOC for Cybersecurity is an examination engagement performed by a licensed CPA firm on a company's Cybersecurity Risk Management Program. In a SOC for Cybersecurity examination, there are two distinct subject matters: (a) the description of the company's Cybersecurity Risk Management Program and (b) the effectiveness of controls within that program to achieve the company's cybersecurity objectives. A cybersecurity risk management examination results in the issuance of a cybersecurity risk management examination report that is for general use. The term general use applies to attest reports that are not restricted to specified parties. In an engagement to achieve a high level of assurance (an examination), the practitioner's conclusion should be expressed in the form of an opinion. When attestation risk has been restricted only to a moderate level (a review), the conclusion should be expressed in the form of negative assurance.

The cybersecurity risk management examination report includes the following three key components:

1. ***Management's description of the company's Cybersecurity Risk Management Program***. The first component is a management-prepared narrative description of the company's Cybersecurity Risk Management Program (description). This description is designed to provide information about how the company identifies its information assets, the ways in which the company manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the company's information assets against those risks. The description provides the context needed for users to understand the conclusions,

expressed by management in its assertion and by the CPA firm in the practitioner's report. Management uses the description criteria to prepare and evaluate a company's Cybersecurity Risk Management Program.

2. ***Management's assertion***. The second component is an assertion provided by management, which may be as of a point in time (think "Type I" audit) or for a specified period of time (think "Type II" audit). Specifically, the assertion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the company's Cybersecurity Risk Management Program were effective to achieve the company's cybersecurity objectives based on the control criteria. The AICPA has developed control criteria for use when evaluating whether the controls within the program were effective to achieve the company's cybersecurity objectives. CPA firms must use a well-established risk management and control framework when assessing the effectiveness of controls within the Cybersecurity Risk Management Program to achieve the company's cybersecurity objectives. Examples of such frameworks include:
    - Trust Services Criteria for Security, Availability, and Confidentiality (SOC 2)
    - NIST Critical Infrastructure Cybersecurity Framework
    - ISO 27001/27002
3. ***Practitioner's report***. The third component is a practitioner's report, which contains an opinion, addressing both subject matters in the examination. Specifically, the opinion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the company's Cybersecurity Risk Management Program were effective to achieve the company's cybersecurity objectives based on the control criteria.

Benefits and Potential Users of the SOC for Cybersecurity Reports

There are numerous benefits to undergoing the SOC for Cybersecurity report, including:

- Developing a competitive advantage against similar companies who have not completed a SOC for Cybersecurity engagement
- Potentially reduced premiums on your Cybersecurity policy.
- Providing detailed information to stakeholders who have a vested interest in your company's Cybersecurity Risk Management Program, including:
    - **Senior management:** A cybersecurity risk management examination report provides senior management with information about the effectiveness of an organization's Cybersecurity Risk Management Program, including the controls designed, implemented

and operated to mitigate threats against the company's sensitive information and systems.

- **Boards of directors:** A cybersecurity risk management examination report provides board members with information about the cybersecurity risks the company faces and the program that management has implemented to help them fulfill its oversight responsibilities. It also helps them evaluate management's effectiveness in managing cybersecurity risks.
- **Analysts and investors:** A cybersecurity risk management examination report provides analysts and investors with information about a company's Cybersecurity Risk Management Program. This information is intended to help them understand the cybersecurity risks that could threaten the achievement of the company's operational, reporting, and compliance (legal and regulatory) objectives and, consequently, have an adverse impact on the company's value and stock price.
- **Business partners:** A cybersecurity risk management examination report provides business partners with information about the company's Cybersecurity Risk Management Program as part of their overall vendor risk management process. This information may help determine matters such as whether there is a need for multiple suppliers for a good or service and the extent to which they choose to extend credit to the company. Some business partners may need a detailed understanding of controls implemented by the company and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose information technology (IT) systems are interconnected with systems at the company may need to understand the specific logical access protection over the interconnected systems implemented by the company.

- Providing transparency to key elements of the entity's Cybersecurity Risk Management Program
- Enhancing confidence in the integrity of the information presented within the Cybersecurity Risk Management Program

For additional information regarding SOC for Cybersecurity, contact us today.

About CyberGuard Compliance

CyberGuard Compliance is based in the United States, but serves clients around the globe. The firm's leadership team has over 150 years of combined business management, operations and related information technology (IT) experience. CyberGuard Compliance has performed over 1,000 SOC audits, and unlike most traditional CPA firms which focus on financial statement auditing and tax compliance,

CyberGuard Compliance focuses on cybersecurity and compliance related engagements. These engagements include, but are not limited to, SOC 1 Audits, SOC 2 Audits, SOC 3 Audits, SOC Readiness Assessments, ISO 27001 Assessments, PCI Compliance, HIPAA Compliance, HITRUST Compliance, Vulnerability Assessments, and Penetration Testing.

CyberGuard Compliance was founded with the goal of providing clients with top professional talent from a boutique-style professional services firm. Each of their professionals has over 10 years of relevant experience at "Big 4" and other large international or regional accounting firms, and most carry the designation of Certified Public Accountant ("CPA"), Certified Information Systems Auditor ("CISA"), Certified Information Systems Manager ("CISM"), or Certified Internal Auditor ("CIA"). CyberGuard Compliance treats its staff as valued and highly talented peers, while omitting avoidable layers of management and associated costs.

CyberGuard Compliance has a diverse client base, ranging from Fortune 50 clients to government agencies to start-ups in Silicon Valley. Many of their clients are companies undertaking the audit for the first time. They pride themselves in working closely and collaboratively with their clients to ensure all service related risks are addressed with appropriate criteria and control activities. Their detailed approach helps to identify opportunities for improvement within their clients' operations. CyberGuard Compliance's proven methodology, flexible delivery methods, efficient economic operating model, and focus on adding value for their clients has enabled the firm to be one of the most highly sought after Cybersecurity, SOC Audit, and IT compliance-focused CPA firms in the United States.

As a Public Accounting Oversight Board (PCAOB) registered and licensed public accounting firm, CyberGuard Compliance is subject to an independent peer review on their auditing practice by a recognized and approved peer review program. This ensures the firm is held to the strictest of audit standards.

Contact CyberGuard Compliance

CyberGuard Compliance has assembled top tier leadership to help their clients through the SOC for Cybersecurity process. For further information regarding SOC reports, or to request a fee proposal from CyberGuard Compliance, please visit their "Contact Us" page to submit an informational form or call 866.480.9485 today. Or, feel free to contact the SOC Practice Leader directly:

Tim Roncevich, CISA | SOC Practice Leader

T/ 866.480.9485

E/ ContactUs@CGCompliance.com