BDO KNOWS:

CYBERSECURITY

CYBERSECURITY & THE CFO: MONETIZING RISK

Gone are the days when it was breaking news that a cybersecurity breach had occurred. We've become accustomed – even desensitized – to cyber events, even as significant losses in our capital markets continue. Not only are cybersecurity attacks and breaches here to stay for the foreseeable future, but the frequency in which they occur, as well as the sophistication levels of the incidents, continue to increase at a rapid pace. Managing these risks is daunting, as is keeping up with new legislation and regulation designed to help standardize the ways in which data security and cybersecurity breaches are managed and reported. That's the bad news. The good news? Addressing cybersecurity risk is a higher priority now more than ever before, with the C-suite and boards of directors becoming more and more involved. Since cybersecurity is an entity-wide issue impacting many areas within an organization, it is important that it is "owned" by a person or group with the appropriate line-of-sight, authority and access to the board. So, what, exactly, is the role of the CFO when it comes to cybersecurity?

CONTACTS:

JEFF WARD
Third-Party Attestation
National Managing Partner
314-889-1220
jward@bdo.com

JOSH AYERS
Assurance Partner
314-889-1173
jayers@bdo.com

C-suite executives and board members are more and more finding themselves in a cybersecurity risk oversight role, and as such, are increasing their involvement in management's development, implementation, and monitoring of comprehensive, enterprise-wide cybersecurity risk management programs. Clearly, the CFO is responsible for the financial matters of the company, including evaluating the processes and controls that are implemented to ensure information is produced in a reliable manner. Cybersecurity is often considered by the CFO, but typically only for purposes limited to the amounts in the financial statements and related disclosures. However, in addition to financial processes and disclosures, the CFO – a role that is becoming increasingly involved in their organization's overall digital transformation – must be in tune with the company's cybersecurity risk management program, a program that should encompass an organization's overall IT environment, including systems, networks, and related data – not only addressing financial reporting needs but also operational and compliance needs – all of which are susceptible to a cyber event. Given that cybersecurity is an entity-wide endeavor, and that a breach occurring in operations will cause an organization financial loss – potentially a significant one, the CFO must find a better way to more accurately monetize the cyber risks in the enterprise.

Enter SOC for Cybersecurity. In April 2017, the AICPA introduced a new cybersecurity risk management examination – SOC for Cybersecurity – designed to help organizations meet the growing challenge of communicating to interested parties, both internally and externally, the design and effectiveness of their cybersecurity risk management programs. In a SOC for Cybersecurity examination, an entity's cybersecurity risk management program is defined 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.

A SOC for Cybersecurity examination assesses management's description of their cyber risk management program against the following areas:

- Nature of Operations
- Nature of Information at Risk
- Cybersecurity Risk Management Program Objectives
- Inherent Risks Related to the Use of Technology
- Cybersecurity Risk Governance Structure
- Cybersecurity Risk Management Process
- Cybersecurity Communications and Quality of Cyber Information
- Monitoring of the Cybersecurity Risk Management Program
- Cybersecurity Control Activities

A SOC for Cybersecurity report enables a better understanding of how the entity identifies its information assets, the ways in which the entity manages cybersecurity risks, and the key security policies and processes implemented and operated to protect the entity's information assets against these risks.

Once completed, the SOC for Cybersecurity report provides clear, concise, and relevant cybersecurity information to relevant stakeholders and provides the needed information in a transparent manner, yet maintains the necessary security and confidentiality of the system. For instance, senior management, as well as others within the entity, receive information about the effectiveness of the entity's cybersecurity risk management program, including the controls designed, implemented, and operated to mitigate threats against the entity's sensitive information and systems. Boards of directors receive information about the cybersecurity risks facing the entity, as well as the cybersecurity risk management program implemented by management and designed to help fulfill oversight responsibilities. SOC reports also include information from independent third-party assessors that help evaluate management's effectiveness in mitigating cybersecurity risks – all of which better position stakeholders to make informed decisions. And as for the CFO? They now have a tool to help monetize cybersecurity risk.