TREASURY&RISK
THE FUTURE OF FINANCE TODAY
An ALM Publication
JULY 18, 2017

A Proactive and Pragmatic Approach to Cyber Risk Management

How to use the new AICPA cybersecurity attestation reporting framework.

BY GAURAV KUMAR, JEFF SCHAEFFER

Cyberattacks are undoubtedly on the rise. Companies are no longer concerned about whether an attack will occur, but rather when and how their most valuable data will be breached. Increasing in sophistication, today's cyberattacks can impact all areas of an organization for years after the initial attack and can cost millions—if not billions—in damages.

A number of regulations focused on improving cybersecurity programs have been introduced over the past few years, including a recent regulation finalized by the New York Department of Financial Services (NYDFS) requiring banks, insurance companies, and other NYDFS-regulated entities to establish and maintain an effective cyber risk management program. Still, the magnitude of stolen information remains staggering, and the challenges associated with protecting data continue to grow.

Not all cyberattacks are made public, but it seems as though a new breach makes headlines every day. Only recently has a comprehensive framework for reporting cyber risk management activities become available: The American Institute of Certified Public Accountants (AICPA) recently released a new attestation reporting framework intended to help organizations evaluate and report on their cyber risk management programs. Designed to expand cyber-risk reporting to a broad range of internal and external users, including the C-suite and the board, the AICPA's new reporting framework aims to provide in-depth, easily consumable information about an organization's cyber risk management program.

The attestation reporting framework is voluntary. It's intended to establish a common underlying language for cyber risk management reporting and to provide corporate executives, board members, and other key stakeholders with the visibility into the organization's cyber risk management program that they need in order to improve the program's overall effectiveness and address gaps requiring remediation. The cybersecurity reporting framework allows for flexibility in the control criteria used, is appropriate for general use, and can be applicable to any entity, regardless of sector, in contrast with reporting mechanisms like a Service Organization Controls (SOC) 2 report.

Key Elements of the AICPA's Cybersecurity Framework

There are three key elements of the AICPA's cybersecurity attestation reporting framework:

1. Management's description of the entity's cybersecurity risk management program (the subject matter of the engagement);
2. Management's assertion on (a) the presentation of the description and (b) the operating effectiveness of the controls to achieve the cybersecurity objectives; and
3. Practitioners' report on (a) the presentation of the description and (b) the operating effectiveness of the controls to achieve the cybersecurity objectives.

While the decision about which description criteria is applied as part of the framework is more flexible than other types of attestation reporting (e.g., SOC 2), the description criteria are intended to promote consistency and comparability of cybersecurity information provided by different entities and to arm those charged with governance with information needed for appropriate oversight. One example criteria that organizations are able to utilize when adopting the AICPA's cybersecurity attestation reporting framework is the AICPA's Trust Services Criteria (TSC) for Security, Availability, Processing Integrity, Confidentiality, and Privacy. The TSC has been expanded and enhanced as part of the AICPA's cybersecurity attestation reporting framework and can be used when reporting on the organization's cybersecurity program.

> "As the complexity of cyber risk management continues to evolve, Practices for addressing cyber threats must evolve as well."

Since application of, and adherence to, the reporting framework is voluntary, each organization should consider the benefits to key internal and external stakeholders of receiving a report on the organization's cybersecurity risk management program. Then management can determine the best

> "Senior executives and boards are beginning to recognize cybersecurity as an issue critical to business performance, as opposed to an issue for IT to manage alone."

tool and frequency by which to address stakeholder expectations for greater transparency, as well as the need to provide in-depth information about what the company is doing to address cyber threats and improve responsiveness in the event of an incident.

For many organizations, preparing for a cybersecurity risk management examination would begin by performing a readiness assessment over their cybersecurity risk management program utilizing the AICPA's cybersecurity attestation reporting framework as the basis.

Cybersecurity at the Organization's Highest Levels

As the complexity of cyber risk management continues to evolve, practices for addressing cyber threats must evolve as well so that organizations are prepared to respond to cybersecurity events faster and more effectively. Data at risk from today's cyber threats includes far more than the personal identifiers (like Social Security numbers), payment data, and personal health information that are commonly front and center in discussions of cybersecurity. In fact, the greatest damage to companies often comes from the less obvious—and sometimes undetected—cyber threats, such as theft of intellectual property, espionage, destruction of data, attacks on core operations, or attempts to disable critical infrastructure. While more difficult to understand and quantify, these business impacts can cause long-lasting damage to a company's brand and reputation, not to mention significant financial damages across the entire organization.

Senior executives and boards are beginning to recognize cybersecurity as an issue critical to business performance, as opposed to an issue for IT to manage alone. As breaches increase in volume, and as the time and cost that it takes to identify, mitigate, and recover from them escalates, cybersecurity has risen to the top of the business agenda, leaving boards demanding greater visibility into their organization's cyber risk management program and expecting to see proof of the program's effectiveness.

Active involvement and oversight from the board can ensure that an organization is paying adequate attention to cyber risk management. The board can help shape expectations for reporting on cyber threats, while also advocating for greater transparency and assurance around the effectiveness of the program.

In companies that implement the AICPA's new attestation reporting framework, boards will have access to information from an independent third-party firm that they can use to objectively evaluate and report on the effectiveness of the company's cyber risk management program to key stakeholders, including investors, analysts, customers, business partners and regulators. By leveraging this information, boards can challenge management's assertions around the effectiveness of their cyber risk management programs while also credibly communicating any related findings to other key stakeholders.

Cyber Risk Management Examination

A cyber-risk management examination engagement conducted by an independent, AICPA-licensed audit firm can help a company improve the transparency of its approach to cybersecurity, as well as improving operational efficiency by using a single, standardized reporting mechanism.

Because of the rapidly evolving nature of cyber risks and the varying levels of maturity of corporate cyber risk management programs, an organization should consider performing an internal assessment of its readiness for the cyber risk management examination prior to transitioning to an independent third-party attestation. The internal assessment should include the following:

- Selection of an appropriate cyber control framework such as NIST CSF, ISO 27001, or the AICPA's Trust Services Criteria;
- Identification of the company's most critical IT assets;

> "Ultimately, building a strong foundation for addressing cybersecurity — before regulatory mandates or a crisis demands it-can provide a strategic competitive advantage."

- Evaluation of the effectiveness of current-state internal controls included within the company's cyber risk management program, leveraging the cyber control framework adopted by management;
- Identification of potential gaps in, and enhancement opportunities for, key cyber risk processes and related internal controls; and
- Development of a remediation plan and subsequent execution of key remediation activities.

With the pressure and scrutiny continuing to mount on organizations to report on the effectiveness of their cyber risk management programs and related controls, this type of report can be vital in helping the board effectively fulfill their cybersecurity oversight responsibilities.

Ultimately, building a strong foundation for addressing cybersecurity—before regulatory mandates or a crisis demands it—can provide a strategic competitive advantage for a company by enhancing its brand and reputation. The time to act is now.

Gaurav Kumar *is a principal in Deloitte & Touche LLP, where he advises clients on managing risk and internal controls, including those around IT risk management, identity access management, and management's corresponding compliance with Sarbanes-Oxley/Model Audit Rule regulations. Kumar currently leads Deloitte's Risk and Financial Advisory services, supporting companies' implementations of the revised COSO framework for the insurance industry, and serves on the American Institute of Certified Public Accountants (AICPA) task force for the development of the cybersecurity risk management attestation reporting framework.*

Jeff Schaeffer *is a managing director in Deloitte & Touche LLP with more than 14 years of experience specializing in risk management, corporate governance and compliance, and controls transformation within the financial services industry. In this role, Jeff leads efforts to design companywide processes and controls to support various complex global transformation programs, including working with clients to perform risk assessments across in-scope business processes and systems, design and validate internal control frameworks, identify gaps requiring remediation, and help design governance structures to sustain internal controls programs.*