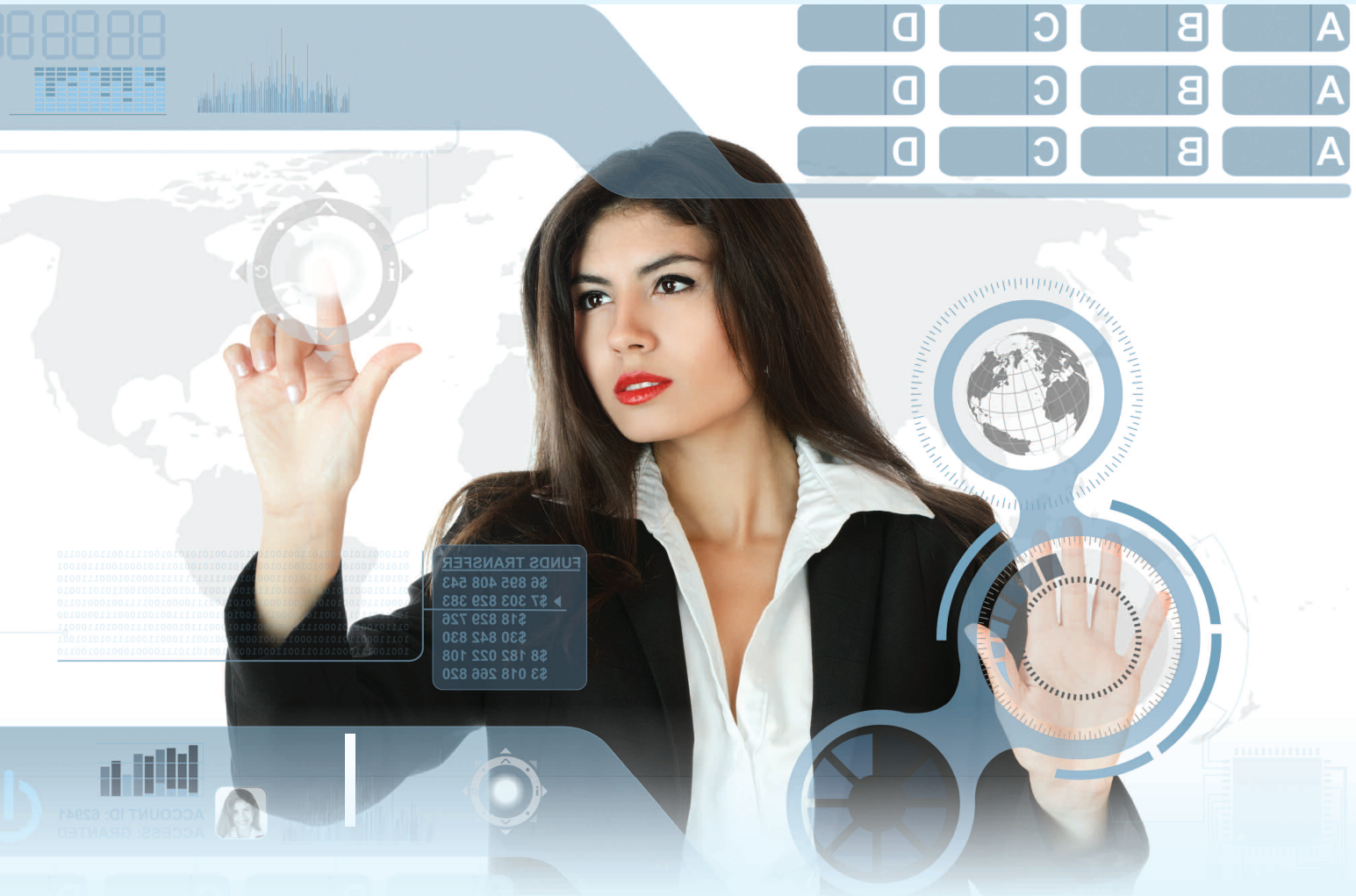

The Chief Information Security Officer

The New CFO of Information Security

By Joel Lanz

Traditionally, CPAs have considered the chief financial officer (CFO) as the guardian of a business's organizational data. It was and remains the CFO's responsibility to maintain a system of internal controls that provides reliance for the accuracy and integrity needed to prepare and attest to the financial statements. These statements and the accompanying opinion continue to be relied on by stakeholders when making financial decisions. The increasing use of rapidly developing technology, software obsolescence, and the change in user preference from desktop to mobile computing platforms have created the need for a new type of data guardian responsible for protecting all types of information in a digital world. The chief information security officer (CISO) is the person performing this role in many organizations and has become an important consideration for CPAs, both in traditional auditing and advisory services.

The Digital Environment

In the evolving digital environment, the protection of data, financial or otherwise, is considered a critical intangible asset. Consumers expect that their information will be protected, and in some industries such protection is required by law. Internally, the explosion of data avail-

ability creates innovative decision models that have changed management and created new business models (e.g., big data and data analytics). Concerns over the confidentiality, integrity, availability, and accuracy of this information, even when not used for financial reporting, continue to receive heightened attention from governance professionals and the boardroom. In some cases, the CISO functions as a point of contact for technology risk, similar to the role of CFOs in financial statement-related services.

The accounting profession has recognized that, as technology risk increasingly affects overall enterprise business objectives and risk, new risk mitigation strategies and service offerings are needed. The AICPA recently developed a cybersecurity risk management reporting framework that assists organizations in communicating the effectiveness of their cybersecurity risk management programs ("SOC for Cybersecurity," http://bit.ly/2riA0Tj). Both the Assurance Services (ASEC) and the Information Management Technology Assurance (IMTA) Executive Committees of the AICPA have issued additional guidance to facilitate CPAs' ability—whether providing traditional assurance or new risk advisory services—to help businesses meet concerns over information protection. ASEC has issued a series of white papers forecasting the changing nature and impact of technology on the future of auditing (e.g., Paul Byrnes, Tom Criste, Trevor Stewart, and Miklos Vasarhelyi, "Reimagining Auditing in a Wired World," August 2014, http://bit.ly/2pgpoXP). IMTA continues to publish cybersecurity workpapers and presentations, such as "Top Cybercrimes Whitepaper: How CPAs Can Protect Themselves and Their Clients" (Jeff Streif, Lisa Traina, and Steven J. Ursillo Jr., 2017, http://bit.ly/2pvKRI8).

As the profession has ventured into these new services, it has also recognized that the CFO no longer maintains a monopoly over data protection. In order to advise businesses on taking advantage of the opportunities created by technology, CPAs must pay proper attention to and effectively manage the corresponding technology risks. In addition, an effective and independent information security function is needed as customer relationships become more automated. Website unavailability, data breaches, defacement of websites, and improperly coded and updated e-commerce sites represent some of the technology risks faced by digital businesses. For all these reasons, a qualified and effective CISO is essential.

In some cases, the CISO functions as a point of contact for technology risk, similar to the role of CFOs in financial statement-related services.

Evolution of the Role

The CISO did not always have such an important and prominent role, and in some organizations did not have any role at all. Originally, and still in many smaller companies, the information security function was viewed as a responsibility of all employees and distributed as such. This strategy relied on each business function knowing best how to protect the information assets for which it was responsible. Unfortunately, this meant security was never a primary responsibility for any individual or department, and, as a result, seldom received the attention and budget it needed. Many departments did not view security strategically and managed requirements in an ad hoc manner. A second problem was that security was not represented on an organization-wide basis, including making appropriate budgeting investments and having representation when enterprise-wide decisions were made. As customers seldom came into contact with security functions, this scenario persisted in many organizations until the advent of e-commerce.

Eventually organizations adopted the role of the information security officer (ISO). This professional, although recruited and employed by the information technology department, frequently served as both a liaison to business units and as a technical security specialist. In pre-Internet days, the ISO would typically be someone with network management or system software experience and would frequently focus efforts on access controls at the user, system, and network levels. Frequently, the ISO served a defensive purpose that primarily kept intruders from accessing mainframe and related assets while helping to enforce automated segregation of duty controls over insiders. GAAS and early versions of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) publications were directed at this type of control environment.

With the advent of e-commerce, customers increasingly came to expect that a business would provide a safe and secure digital environment. These expectations went beyond securing a particular transaction, also including the protection of personal data entrusted to the company. In addition, the defacement of a website was now visible to customers. Cybercrimes, including distributed denial-of-service attacks, Internet-facilitated frauds, and identity theft, only increased the cost of inability to sufficiently protect digital assets began to impact both business and their customers (see Gordon M. Snow, "Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit," Sept. 14, 2011, http://bit.ly/2q0mtBB).

The need to master information security practices and overcome digital threats to business elevated the ISO position to a more senior, and in some cases executive, level. Larger organizations recognized the importance of risk management, and professional associations began to promote the "three lines of defense" model. Under this model, operational responsibilities (first line) were differentiated from activities relating to risk management and compliance functions (second line). Operational information security responsibilities, including user access administration, configuration management, and detailed monitoring of network traffic, remained within the information technology function or were outsourced. More strategic functions, including governance, policy development, board reporting, and business continuity, became the purview of the CISO. This segregation of responsibilities enabled the independence of internal auditors (third line), who could then "provide assurance to senior management and the board over both the first and second lines' efforts consistent with the expectations of the board of directors and senior management" (Douglas J. Anderson and Gina Eubanks, "Leveraging COSO across the Three Lines of Defense," Institute of Internal Auditors, July 2015, http://bit.ly/2pvr5g8).

> Realistically, the role of the CISO and the ability to successfully protect the enterprise must now be a critical control for those responsible for governance, investors, and other stakeholders.

What Does the CISO Do?

Many organizations and commercial enterprises have published white papers and consulting studies trying to both identify current CISO practices and projected CISO roles. As the budget authority and purchasing power of the CISO has increased, many security vendors and consultancies have increased their emphasis on investing in the CISO role and the technology products needed to support it. As important as budget numbers and potential expenses are, however, they should not be the only impetus for financial professionals to understand more about the CISO role. Realistically, the role of the CISO and the ability to successfully protect the enterprise must now be a critical control for those responsible for governance, investors, and other stakeholders.

Among the various published guidance on the role of the CISO, many of the more reputable sources focus on larger organizations. "Structuring the Chief Information Security Officer Organization" describes and defines a CISO team structure and functions for a large, diverse U.S. national organization using input from CISOs, policies, frameworks, maturity models, standards, codes of practice, and lessons learned from major cybersecurity incidents (Julia Allen, Gregory Crabb, Pamela Curtis, Brendan Fitzpatrick, Nader Mehravari, and David Tobar, Software Engineering Institute, Carnegie Mellon University, October 2015, http://bit.ly/2qYdrDl). The report identifies four primary functions of the CISO. These four functions are consistent with how reputable organizations view the information security function (see, e.g., Kevin M. Stine, Kim Quill, and Gregory A. Witte, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Feb. 19, 2014, http://bit.ly/2qWfRkZ). More importantly, each of these functions directly affects the work of the financial professional, whether as an external auditor or a management accountant (including risk managers and internal auditors).

Many financial professionals who believe that the CISO's role is limited to cybersecurity and other technology-related issues are surprised to learn that the CISO is also responsible for critical controls frequently relied on by external auditors and management accountants.

Notable functions identified in the *Exhibit* include the following:

- Facilitating the maintenance of customer relationships and increasing retention by ensuring the protection of confidential customer information and company reputation.
- Developing and monitoring compliance with policies and procedures, ranging from enforcing segregation of duties in end user functions to specifying controls for cybersecurity protections.
- Monitoring and evaluating the organization's technology activities to help ensure and provide assurance that technology-related risks are managed in accordance with organization risk appetite and tolerances.
- Ensuring compliance with technology-related regulations, including serving as the primary contact with regulators on issues relating to business continuity, information/cybersecurity, privacy, vendor management, e-business, IT operations, and IT management.
- Developing tests and reports on business resiliency, including business continuity and computer crime response, to ensure that the company can continue operating during crisis situations and breaches.
- Managing organization-wide oversight over third-party service providers, including reviewing SOC reports, coordinating due diligence, and monitoring security-related service level agreements.
- Leading management investigations involving the use of technology, including cybersecurity and insider thefts.
- Serving as the primary contact with law enforcement and sometimes, depending on the industry, conferring with clients on how to improve security postures (especially in the banking industry).

Organizational Placement of the CISO

Despite the importance of the CISO's role in IT governance and promoting an organization's internal control structure, the organizational placement of the CISO continues to generate controversy. While regulated industries, including financial services, recognize the benefits of an independent CISO reporting to a

EXHIBIT

Functions of the Chief Information Security Officer

Software Engineering Institute at Carnegie Mellon University	National Institute of Standards and Technology Cybersecurity Framework	Representative Expectations	External Auditor Concerns	Management Accountant Concerns
Protect, shield, defend, and prevent	Identify Protect	Access control software User awareness Proactive security testing Configuration management Service level agreements Patch management	Preventive controls	Appropriate funding Regulatory compliance Asset protection Insurance
Monitor, detect, and hunt	Detect	Monitor adherence to policies and procedures Monitor and review activity logs Security (e.g., penetration) testing	Detective controls Elevation of issues that may require financial statement disclosure	Governance, risk, and compliance technology updates Key performance indicators Balanced scorecards
Respond, recover, and sustain	Respond Recover	Incident response Computer forensics Emergency management Law enforcement coordination	SEC disclosures Audit opinion Adequacy of financial reserves and liability establishment	Business resiliency Claim processing Regulatory disclosures Accounting for the incident
Govern, manage, comply, educate, and manage risk	N/A	Technology risk appetite and tolerances Policies and procedures Board reporting IT governance Regulatory compliance	Audit committee IT audit	Board-level reporting Management certifications Risk assessment and management

THE MAKING OF A CISO

In assessing the role and contribution of a CISO, it is helpful to understand the education and experience requirements typically expected for the role. As with other executive positions, many paths can be taken to become a CISO, and they are not all technical. Former military cybersecurity officers, law enforcement personnel, technology risk consultants, and even former CIOs are popular choices. But with the increased outsourcing of day-to-day security operations, lawyers, researchers, and even financial practitioners (especially those with governance and risk management experience) are chosen to fill this critical role. Relationship management, leadership, and effective execution of risk management strategies are critical components of executive success, no matter the function managed.

Whether it is best to have a technical or businessperson as the CISO depends upon a variety of issues, including the type of business, reliance on vendors, and composition of the existing team members. For example, a technology startup whose existence relies on the ability to maintain security and has limited staff may prefer a more technical skilled professional who can easily identify application weaknesses. A more mature company with various divisions, a strong IT department, technical information security staff, and significant use of third parties to manage security may find an information security professional with a legal or financial background best.

Experienced CPAs possess the fundamental skill set required become a CISO, but typically require additional training and experience. Hands-on interaction with the existing information security team—whether as an information security liaison for the finance department, a part of the technology risk management team, or an IT auditor or outside security consultant—is critical, as is experience with corporate governance practices, regulatory compliance, corporate relationship management, financial and business process controls, and vendor management oversight.

For some, an advanced degree in information assurance may help provide some of the requisite knowledge. Fortunately, many well-respected and accredited universities offer online or combination executive degrees in cybersecurity (e.g., Brown University). Online certificate courses are available alternatives [e.g., individual courses through Open SUNY (State University of New York)].

As with professional accounting, potential CISOs can differentiate themselves through attainment of professional certification. The Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM), both sponsored by ISACA, are a natural next step for financial professionals, as the programs focus on IT auditing and management challenges of an information security function. Those choosing a more technical foundation should consider the Certified Information Systems Security Professional (CISSP) sponsored by $(ISC)^2$. The SANS Institute is another source for technical security training.

Whether seeking to become a CISO or reviewing the effectiveness of the CISO function, CPAs should review the above factors. The ability to remain current with new technology and to demonstrate its impact on business objectives is critical to the success of the function and the individual.

chief risk officer, some industries, notably higher education, continue to place the CISO in the IT department under the direction of the CIO. Some experts argue that given the importance of the role, the CISO should report directly to the CEO, others that the CIO and CISO should share the responsibility for protecting the organization's digital assets, and still others believe that organizational placement does not matter at all.

While experts debate the organization role of the CISO, boards of directors and audit committees continue to exercise increased attention and oversight over cybersecurity and technology in general. A recent study by the University of Indiana considered the role of the CISO and the need for independence in order to provide the board with accurate information outside the politics of day-to-day corporate operations:

> Many organizations that are very focused on the integrity of their information, especially in the government sector, seek to preserve the CISO's independence and position the CISO outside the IT department on a level on par with the CIO. This provides independence, but it can also become problematic with regards to the CISO's accountability and reliance on its IT underpinning. (Val Hooper and Jeremy McKissack, "The Emerging Role of the CISO," Business Horizons, November–December 2016, http://bit.ly/2qWlCiv)

Despite the above considerations, an ISACA and RSA Conference Survey of 461 cybersecurity managers and practitioners found that the cybersecurity/information security function continues to report to the CIO for 63% of survey participants, to the CEO for 14%, and directly to the board for 8% ("State of Cybersecurity Implications for 2016," March 2016, http://bit.ly/2pvCuwB). In the author's experience, placement of the CISO function is very dependent on the type of business and overall security

knowledge of the organization. More technology-dependent and digital businesses appear to better appreciate the importance and need for an independent CISO and place that individual accordingly. CISOs tend to continue to report to CIOs when management or the board are technophobes, IT is considered a commodity, and the impulse is to rely on the CIO to interpret cybersecurity issues and ensure that the technical issues are taken care of.

Traditional Obstacles Remain

Companies of all sizes recognize the increasing importance of the CISO; however, no matter the size of the organization or how well supported or funded a CISO is, classical impediments to the success of the function remain. The National Association of Corporate Directors published a blog post that contained various thoughts on the CISO position (Kathryn Cave, "Does the CISO Role Need to Be Formalized?" NACD in the News, Feb. 23, 2017, http://bit.ly/2qnB8aZ). One contributor commented: "The position of CISO is a difficult one though. The business importance of this individual has changed rapidly over the last few years and some see the position as a classic short-term fall guy—ready to be fired with the first breach." Realistically, the odds are against the CISO; even if the CISO can control all technology-related risks, hackers can take advantage of the human factor—the employees, vendors, and customers who sometimes fail to heed the advice of the CISO and place the organization at unnecessary risk.

If CPAs and financial executives want to reap the benefits that a CISO can provide, they should aggressively support the position's independence and facilitate the resources needed to get the job done. Employing knowledgeable staff that can competently assess the effectiveness of the CISO's role in promoting an appropriate internal control environment and can make the necessary recommendations to change corporate behavior is critical in ensuring success. ❑

Joel Lanz, CPA/CGMA/CITP/CFF, CISA, CISM, CISSP, CFE, *is the founder and principal of Joel Lanz, CPA, P.C., Jericho, N.Y. He is a member of* The CPA Journal *editorial board.*