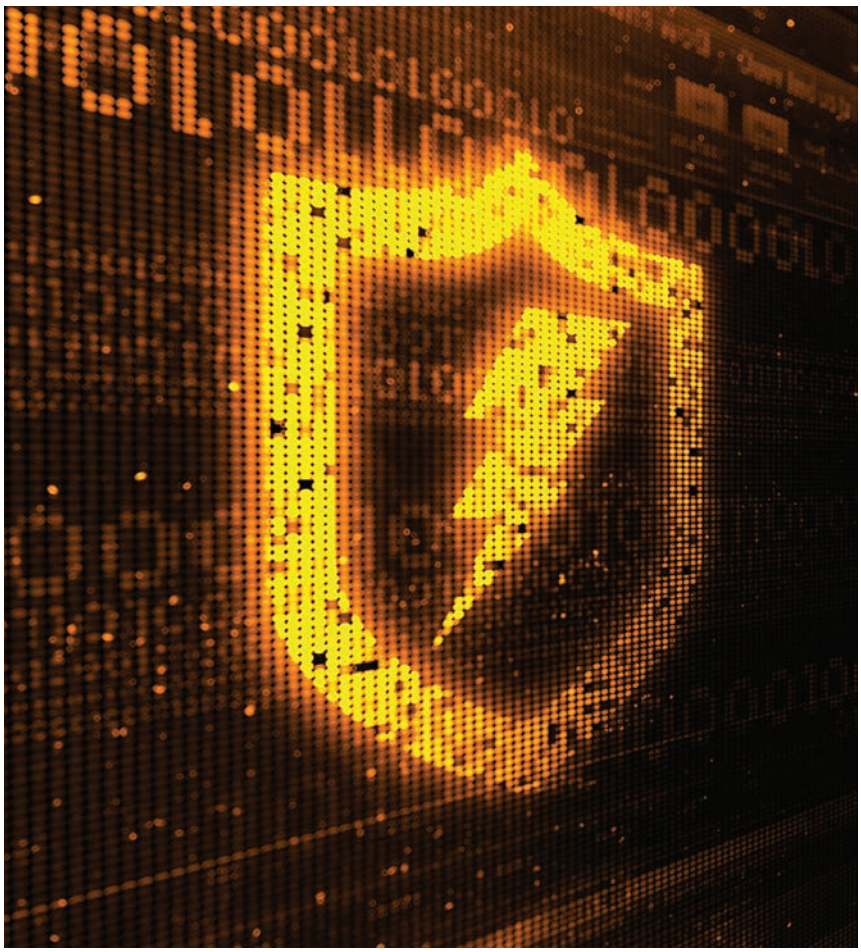
SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement

By Gerry H. Grant and C. Terry Grant

As companies turn to digital technologies for business solutions, the risk of a security breach continues to rise. For the last 11 years, the security of information technology and data has been rated as a top technology initiative in surveys conducted and published by the AICPA. In addition to concerns about the loss of data and sensitive information, the AICPA surveys identify controls for mobile devices and cloud computing as ongoing concerns.

In the fall of 2011, the SEC issued enhanced financial statement disclosure guidance that has led to a higher level of cybersecurity awareness, monitoring, and scrutiny by SEC registrants ("CF Disclosure Guidance: Topic 2," Oct. 13, 2011). The guidance, issued by the SEC's Division of Corporation Finance, is in response to more frequent and severe cybersecurity incidents experienced by SEC registrants. The required new disclosure obligations focus on cybersecurity risks and actual cyber attack incidents.



Nature of Cyber Attacks

The SEC guidance states that cyber attacks can be deliberate or can result from unintended events, and they can be carried out by outside hackers or by internal agents (e.g., employees, contractors, vendors). Attacks can be executed in a variety of ways to achieve different objectives. Examples of specific attacks mentioned by the SEC include—

- unauthorized access to sensitive data;
- industrial espionage;
- sabotage of hardware and software;
- infection of hardware and software with malicious software;
- theft of computer time and other denial of service attacks; and
- theft of mobile devices, such as laptops, notebooks, and cell phones.

Specific SEC Disclosures

The SEC guidance is consistent with other disclosure requirements mandated by federal securities laws associated with any significant business risk. But the risks associated with cybersecurity go beyond generic risks that could apply to all SEC registrants. The new guidance suggests disclosures should focus on the unique facts and circumstances related to specific, material cybersecurity risk factors. For example, SEC financial statement disclosure obligations can arise from the following:

- Cybersecurity risks and costs associated with a registrant's operations
- Cybersecurity risks arising from outsourcing activities
- Cybersecurity incidents that have occurred during the past year and that are individually or collectively material in nature
- Cybersecurity risks that may go undetected for an extended period
- Cybersecurity risks that give rise to relevant insurance coverage.

In addition to these potential risks, actual cyber attacks should be disclosed as

to the nature, occurrence, and the potential cost of the attack, as well as the related consequences of the attack. Disclosing information about prior attacks can often help users understand the risk the company is facing and how the company is remediating past security breaches.

Potential and actual cyber attacks present unique risks and costs to companies. Costs for actual security breaches can often be determined, but costs of potential breaches are very difficult to estimate. The SEC offered guidance on costs that should be considered, indicating that cyber attacks can expose companies to the following:

- Remedial costs associated with a loss of data and information and the loss of business after an attack
- Costs of cybersecurity
- Loss of revenues due to a loss of data or customers
- Regulatory fines
- Litigation costs
- Reputational damage that can lead to loss of customers and reduced investor confidence.

The SEC disclosure guidance acknowledges that registrants have been devoting additional resources to cybersecurity. These include hiring additional IT security personnel, training existing internal agents, upgrading IT hardware and software, and hiring IT security consultants.

Six Companies Attracted SEC Attention and Letters

For obvious reasons, companies are reluctant to disclose the details of cyber attacks. Security breaches often harm a company's reputation, spawn litigation, and expose vulnerabilities to competitors. In early 2012, the SEC sent letters to six companies—Amazon.com, American International Group Inc. (AIG), Eastman Chemical Co., Google, Hartford Financial Services Group Inc., Quest Diagnostics Inc.—noting the inadequacies of cybersecurity risk disclosures in their annual reports. Surprisingly, five of the six companies cited by the SEC reported effective internal controls from 2005 to their current filing. AIG reported early ineffective controls, during 2005–2007, but the material weaknesses reported did not include IT deficiencies.

> The SEC disclosure guidance requires management to explain the costs and other consequences of material cybersecurity incidents.

Internal control audits are governed by Auditing Standard (AS) 5, *An Audit of Internal Control over Financial Reporting that Is Integrated with an Audit of Financial Statements*. The standard requires auditors to use a "top-down approach" that begins at the financial statement level to identify controls that present a "reasonable possibility" of material financial statement misstatement. Interestingly, the SEC's enhanced disclosure guidance could be interpreted as an expansion of the scope of the integrated audit of internal control over financial reporting and the financial statements. IT controls, including those that are not directly related to the financial statement assertions, arguably fall under the scope of the integrated audit.

Disclosures in the 2012 annual reports of five of the six companies (all except Eastman Chemical) strongly stressed the risks of cyber attacks. The companies stated that cybersecurity measures were in place to help prevent system interruption and the loss of sensitive data. But the disclosures also revealed that these measures cannot provide absolute assurance that a cybersecurity breach can be prevented.

In spite of the disclosures made by these six companies, the SEC determined that they did not go far enough to alert investors to the risks of cyber attacks and did not disclose the fact that such attacks had occurred. The SEC requested that Amazon disclose a cyber attack that stole millions of addresses and credit card information from its Zappos unit. Amazon eventually complied with the SEC's request, but only after arguing that the disclosure was not required because Zappos did not contribute material revenue. Hartford presented a materiality argument as well, but the SEC responded that any cyber attack should be disclosed. Google announced in 2010 a hacker raid on the company's source code, but was asked to include the cyber attack disclosure in a recent filing to provide a better understanding of their cybersecurity risk factor. All six companies have complied, or will comply in upcoming financial statements, with the SEC's request.

Although SEC guidance is not technically a ruling, sanctions and fines can be imposed if SEC requests are not met. A June 2013 white paper by corporate compliance resource provider Intelligize revealed an increase of 106% in cybersecurity disclosures by SEC registrants in the first six months of 2013 (http://info.intelligize.com/june2013whitepaper). In essence, SEC comment letters to registrants on specific topics often have the effect of de facto rulings.

Practical Guidance on Disclosures

The SEC disclosure guidance requires management to explain in the management's discussion and analysis (MD&A) section of quarterly and annual reports the costs and other consequences of material cybersecurity incidents as they relate to the financial condition of the registrant and the results of its operations. The MD&A discussion should also address potential cybersecurity costs and risks. For example, if an actual cybersecurity incident, such as data theft, has occurred, management should discuss the likelihood of the incident having a material impact on the financial condition of the company, or, if a cyber attack compromised trade secrets related to a new product development, how might this impair the future viability of the product. Other examples of disclosure discussions would include material litigation costs, such as costs associated with stolen sensitive customer information that could lead to identity theft. Other MD&A disclosures should address the costs of preventing cyber attacks. Such costs could include costs to maintain business rela-

tionships, loss of business and future cash flows, as well as impairment of goodwill and long-lived assets.

Disclosures might also be needed as part of management's assessment of internal controls. If cybersecurity risks could affect a company's information system and impact the integrity of financial reporting, management should include this as an internal control deficiency and seek remedies. In addition, disclosures should be included in the company's "description of business" section if the cyber attack affects products or services, and in the company's "legal proceedings" section if material litigation is pending.

Cyber attacks occurring after the balance sheet date but before the financial statements are issued should be considered a subsequent event. If material, the nature of the attack and related potential cost should be disclosed.

Both internal and external auditors are involved with the adequacy of existing cybersecurity controls. The process of evaluating security controls has become more complicated, necessitating expanded use of IT equipment. The *Computer Security Handbook* notes that today's auditors may need special training to understand and test security controls in a digital system (Seymour Bosworth, Michael E. Kabay, Eric Whyne, 6th Ed., Wiley, 2014).

Internal auditors need applicable skills in order to be able to analyze the risks associated with data security, perform routine and regular security audits, help select security systems, evaluate whether security goals have been met, and monitor compliance with security procedures. External auditors must have the special technical skills necessary to ensure that financial statements are fairly and accurately presented. From a security perspective, external auditors should have necessary skills to identify sources of computer security information, understand the client's computer security environment, identify critical controls within the system, conduct an actual security review with appropriate testing, report the audit findings to management and include recommendations for reducing and eliminating material weaknesses in the client's security environment, and identify both strength and weaknesses in a client's security system and test strengths for consistency and weaknesses to determine if monetary losses have been incurred.

Auditors should not assume that cyber attacks are limited to high-tech companies. All businesses could be at risk of having customer credit card numbers and other personal information stolen. Auditors should consider the SEC's new cybersecurity disclosures for private companies as well, because private companies are subject to some of the same requirements as SEC registrants.

When in doubt, auditors are advised to seek the help of an external specialist. Information system auditors and security experts can be a valuable source of information on security risks and remedial modifications to internal control systems that can help bolster them and help companies comply with the expanded cybersecurity disclosures expected by the SEC. ❑

Gerry H. Grant, PhD, CPA, *is an assistant professor of accounting at the College of Charleston, Charleston, S.C.* ***C. Terry Grant, PhD, CPA,*** *is a professor of accounting at the University of South Alabama, Mobile, Ala.*