protiviti®
Face the Future with Confidence

SEC Cyber Threat Report Advises Companies to Revisit Internal Accounting Controls

October 30, 2018

On Tuesday, October 16, the U.S. Securities and Exchange Commission (SEC) issued a report advising public companies to review and recalibrate internal accounting controls to consider cyber threats. The report is based on an investigation of business email compromises (BECs), more commonly known as "spearphishing" attacks, at nine public companies across a broad range of industries that resulted in a cumulative loss of almost $100 million. The frauds lasted up to nine months and some were detected only after intervention by law enforcement or other third parties.

In this Flash Report, we summarize the report and the implications for public organizations. The SEC's release can be found here.[1]

Background

Virtually all economic activities now take place through digital technology and electronic communication, leaving business transactions and assets susceptible to a variety of cyber-related threats. This is a growing global problem, and cyber scams like the ones described in the SEC's report are an ever-increasing part of the risks faced by a wide variety of businesses, including issuers with SEC compliance obligations.

BECs are not a new phenomenon. Their proliferation has long pointed to the vital importance of the human perimeter as a complement to the technology perimeter in a cybersecurity system. Despite the efforts of companies to create awareness and manage these attacks, they continue to persist and succeed.

The effects of these frauds can be significant. According to the FBI, companies have lost more than $5 billion to BECs since 2013 – the highest estimated out-of-pocket loss from any class of cyber crime during that period. Of note, cyber threats rank consistently in a number

[1] "SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls," Press Release, October 16, 2018, www.sec.gov/news/press-release/2018-236.

of annual studies assessing the top global risks, including the World Economic Forum's Top Global Risks, as well as the *Executive Perspectives on Top Risks* survey from Protiviti and the North Carolina State University ERM Initiative.[2]

Specific provisions of the Securities Exchange Act of 1934 require public companies to adapt internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. Over the years, the SEC staff has questioned the veracity of these disclosures in terms of timing and completeness. The investigative report issued two weeks ago is just the latest effort of the SEC to focus issuers on the need to improve their disclosure controls and procedures in this area. As noted by SEC Chairman Jay Clayton:

> Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies. Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats.

As we wrote in a previous Flash Report published February 26, 2018, the SEC has identified cybersecurity as one of the most critical risks facing organizations today.[3] The SEC has published guidance regarding known threats, recommended controls and reporting obligations. That guidance is available here.[4] Other than the clear focus on BECs, the underlying message in issuing the findings of the investigative report is not new.

Key Findings

The SEC's investigation focused on internal accounting controls at companies that fell victim to spoofed or compromised emails from cyber criminals purporting to be company executives or vendors. One company made 14 wire payments requested by a fake executive over the course of several weeks – resulting in more than $45 million in losses – before the fraud was uncovered by an alert from a foreign bank. Another paid eight invoices totaling $1.5 million over several months in response to a vendor's manipulated electronic documentation for a banking change; the fraud was only discovered when the actual vendor complained about past due invoices.

The fraudulent communications typically took one of two forms:

[2] For more information, visit www.protiviti.com/toprisks.

[3] "SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures," Flash Report, February 26, 2018, www.protiviti.com/US-en/insights/sec-issues-interpretive-guidance-public-company-cybersecurity-disclosures.

[4] "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," *Federal Register*, February 26, 2018, www.sec.gov/rules/interp/2018/33-10459.pdf.

- **Emails from fake executives.** Spoofed emails, purportedly from company officials, authorized and directed finance personnel to work with an outside attorney to make wire transfers to an outside entity. These transactions typically involved foreign banks and were characterized by tight deadlines, real law firm names and some type of implied regulatory endorsement.

- **Fake vendor requests.** More technologically sophisticated than spoofed executive emails, these spoofs required infiltration of foreign vendor email accounts and changes to the payment account information in the vendor master file. Because it is common for vendors to wait several months before considering a payment delinquent, the scams, in some circumstances, were able to continue for an extended period of time.

These examples underscore the importance of devising and maintaining a system of internal accounting controls attuned to cyber-related fraud, as well as the critical role of training in implementing controls to protect assets in compliance with federal securities laws.

The victims in this investigation, for instance, had procedures requiring authorization for payment requests, management approval for outgoing wires and verification of any changes to vendor data. Yet they still fell victim to attack because electronic communications, alone, were deemed sufficient to process significant wire transfers and changes to vendor data. The frauds were able to go undetected due to inadequate outgoing payment notification and account reconciliation procedures.

The efficacy of accounting controls depends on the personnel that implement, maintain and follow them. These frauds succeeded, at least in part, because the responsible personnel did not sufficiently understand the company's existing controls or did not recognize indications in the emailed instructions that those communications might not be reliable. Underscoring this point, in a recent global survey conducted by ESI ThoughtLab, 87 percent of organizations cited untrained staff as their greatest cyber risk.[5] Furthermore, we observe many companies relying on immature processes dependent on manual procedures and human decisions, which lack metrics, measures and monitoring, and often fail over time, leading to losses such as these.

In one instance, the accounting employee who received a spoofed email did not follow the company's dual-authorization requirement for wire payments, directing unqualified subordinates to serve as second signatory. In another, the accounting employee

[5] *The Cybersecurity Imperative – Managing Cyber Risks in a World of Rapid Digital Change*, ESI ThoughtLab, October 2018, www.protiviti.com/US-en/insights/cybersecurity-imperative.

misinterpreted the company's authorization matrix as giving him approval authority at a level reserved for the CFO. This is a clear example where the process is still manual and not enforcing system-level access controls.

There also were numerous examples where the recipients of the fraudulent communications asked no questions about the nature of the supposed transactions, even where such transactions were clearly outside of the recipient employee's domain and even where the employee was asked to make multiple payments over days and even weeks. In two instances the targeted recipients were themselves executive-level employees — chief accounting officers — who initiated payments in response to fake executive emails.

The SEC chose not to charge any victimized companies or personnel in conjunction with its investigations, but chose to publish its findings as an advisory to all publicly traded companies, urging them to reassess internal accounting controls and calibrate them to the current risk environment, concluding that, "Given the prevalence and continued expansion of these attacks, issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks."

Our Point of View

Obviously, the failure to prevent business email and cyber-related vulnerabilities can expose public companies to significant risk. As a reminder, the Sarbanes-Oxley Act of 2002 requires a registrant's key executives (typically the CEO and CFO) to attest that the company maintains adequate internal controls over financial reporting (ICFR), including those related to cybersecurity, for disclosure into the public domain on a periodic (i.e., quarterly as well as annual) basis in their SEC filings.

Thus, cybersecurity should be an important part of an issuer's diligence in conjunction with its ICFR design and processes for evaluating their operating effectiveness. To amplify the importance of the above, if a registrant's key executives directly or negligently certify in periodic filings that the organization's controls are "adequate" and the company then experiences a negative cyber event, those executives may be at risk of SEC discipline for those certifications.

Therefore, we strongly recommend that all public companies (and those aspiring to be public companies) should regularly reassess all elements of their existing ICFR for preventing and addressing the risks of increasingly creative cyber-related intrusions and/or frauds. This review should include:

- Rigorously assessing the current state of relevant policies, procedures and employee training protocols, and prompt remediation of any identified exposure areas;
- Maturing and automating controls that currently rely on manual processes, including integrating technology-enforced controls that are less apt to fail due to human error; and
- Consulting counsel on how certifying officers can best demonstrate the appropriate diligence to protect themselves from enforcement actions.

Issuers should take note that the SEC has been focusing on improving cybersecurity disclosures for several years. Lax controls over BECs have always been the root cause of embarrassing incidents. The SEC's investigative report is sobering in that its attendant messaging raises the stakes for issuers and their certifying officers.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®