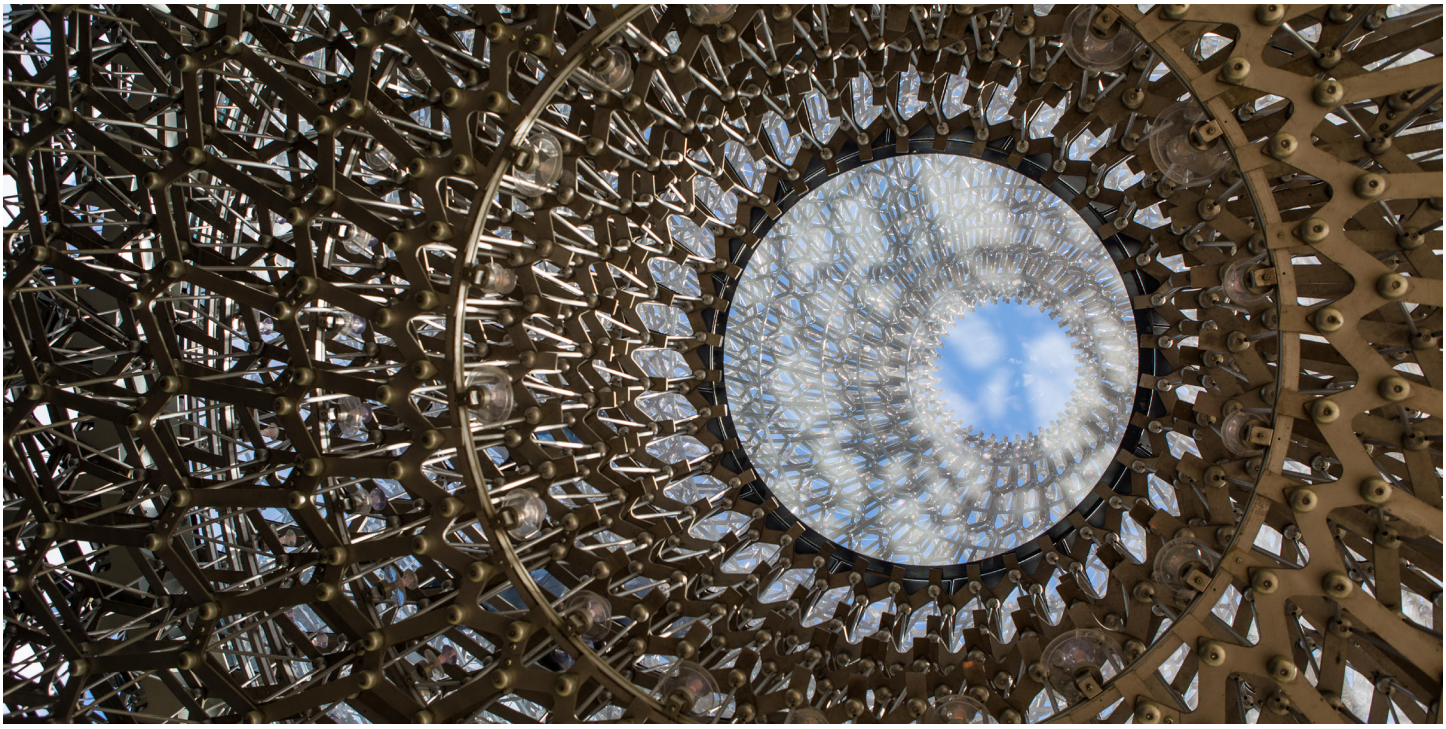
Deloitte.

Heads Up | Volume 25, Issue 18
October 30, 2018



In This Issue


- What Is a BEC Scam?
- How Does a BEC Scam Occur?
- How Can BEC Scams Be Identified and Avoided?
- What Controls May Help Companies Prevent or Detect These Types of Cybercrimes?
- Key Takeaways
- SEC's Focus on Cybersecurity


# Cyber Threat Considerations Related to Implementation of Internal Accounting Controls

*by Jim Burya and Sandy Herrygers, Deloitte & Touche LLP*

In response to the continued increase in cybercrime, the SEC issued an investigative report[1] on October 16, 2018, that cautioned companies to consider cyber threats when they are implementing their internal accounting controls. The report focuses on the internal accounting controls of nine issuers in a range of sectors "that were victims of one of two variants of schemes involving spoofed or compromised electronic communications from persons purporting to be company executives or vendors," commonly referred to as business e-mail compromise (BEC) scams. The SEC considered whether the companies affected by the BECs complied with the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934, under which certain issuers are required to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization." Further, the report emphasized that "[w]hile the cyber-related threats posed to issuers' assets are relatively new, the expectation that issuers will have sufficient internal accounting controls and that those controls will be reviewed and updated as circumstances warrant is not."

[1] SEC Investigative Report Release No. 84429, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements.*

## What Is a BEC Scam?

As described in the SEC's report, a BEC scam occurs when attackers use compromised or fraudulent e-mail addresses to target specific employees within organizations and ask them to participate in what appear to be legitimate transactions or to make changes to key payment or vendor information. The scam typically involves the hacking of an individual's e-mail account, which is then used to send e-mails to other individuals within an organization or outside of it (e.g., to customers). This occurs more commonly in hosted e-mail solutions that are not protected by multifactor authentication (MFA). It also occurs in scenarios in which hackers are able to set up rules for e-mail forwarding and deleting to monitor and remove communications that may be used to detect the unauthorized use of the e-mail address. Fraudulent or spoofed e-mails commonly look similar to or have domain names that are similar to legitimate correspondence.

## How Does a BEC Scam Occur?

Cyber criminals use publicly available information from company Web sites, directories, databases, and social media platforms to target company executives as well as specific employees in organizational areas such as finance or human resources. The following six types of BEC scams are prevalent:

| | |
|---|---|
| Changed vendor payment details | A fraudulent e-mail sent from an attacker posing as a company vendor with new payment or bank routing information used to falsely redirect vendor invoice payments. |
| Changed employee payroll details | A fraudulent e-mail sent from an attacker posing as an employee with advice about new payment or bank routing information used to falsely redirect payroll checks or deposits. |
| E-mail replication | Hacked or replicated e-mail domains of managers or directors used to send out requests to the finance team to make an urgent payment. |
| Fraudulent e-mail request | Fraudulent e-mail requesting that employees transfer funds related to a fictitious invoice or transaction. This can be done by hacking, by using social engineering (i.e., use of deception to manipulate individuals into divulging confidential or personal information), or by using domain names that resemble legitimate ones. |
| Executive/attorney impersonation | The impersonation of lawyers or executives requesting the urgent or immediate transfer of funds related to confidential matters. |
| Data theft | Using a compromised e-mail to target human resources or finance departments to fraudulently request employee records. This information can then be used for further BEC scams or for identity fraud. |

## How Can BEC Scams Be Identified and Avoided?

A pervasive theme in BEC scams is that an individual employee gives the hacker access to an e-mail account, generally by clicking a link in an e-mail or by downloading a file through a phishing attack. A BEC scam can also occur when an employee completes a requested action on the basis of a fraudulent or spoofed e-mail. Companies should consider enhancing their security awareness programs with improved employee training to prevent these attacks and should remind employees of the following BEC scam characteristics:

- *Content* — Does the e-mail ask you to click an unfamiliar link or download an attachment, does the e-mail contain errors, or is its language or the request illogical or unusual?
- *Hyperlinks* — If you hover the mouse over a hyperlink, does the content match the actual link?

- *Attachments* — If the e-mail contains an attachment, is the title or format of the attachment unfamiliar or different from the information in the request?
- *Address* — Does the business name noted in the e-mail match the business name? If it claims to be from an internal source, are there discrepancies in the spelling or order of the name, or is it from an outside source that is suspicious?
- *Subject* — Is the text in the subject line irrelevant or different from the content of the e-mail? For example, it may state that it is a reply to an e-mail that you have not sent.

## What Controls May Help Companies Prevent or Detect These Types of Cybercrimes?

In addition to raising the general security awareness of employees, companies should evaluate the design and operation of those controls that may help prevent or detect successful BEC scams. The following are some examples of general information technology (IT) and business process controls that companies should consider as part of a layered defense strategy regarding BEC:

| General IT Controls | | |
|---|---|---|
| **Type** | **Purpose** | **Summary** |
| MFA — IT access | MFA is implemented to validate that authorized users are authenticated before gaining access to the system. | A frequently used control is the implementation of application-based MFA for hosted e-mail solutions. MFA can help prevent a hacker from accessing a hosted e-mail solution that would then be used by the hacker to send e-mails from a compromised company e-mail address. |
| Virtual private network (VPN) | Controls are implemented to restrict VPN access to authorized and appropriate users. | Many organizations already use VPN to authenticate users who attempt to gain access to an organization's internal network from a remote location. Applications and infrastructure are placed behind the organization's firewall and therefore are unable to be accessed until the user connects to the VPN. |
| Secure e-mail gateways | Controls are implemented to encrypt and decrypt e-mail to prevent unauthorized disclosure of information. | Strong security controls associated with inbound and outbound e-mail traffic are necessary to help prevent unauthorized disclosure of information. |
| URL filtering | Controls are implemented to restrict malicious material from being delivered over a Web browser or e-mail. | Preventing users from accessing malicious Web addresses helps avoid unauthorized disclosure of sensitive information such as the username and password an employee uses for authentication. Preventive controls in the e-mail gateway further reduce the likelihood that a malicious e-mail is delivered to an inbox. |
| Endpoint security | Endpoint protection (e.g., antivirus, anti-malware) is implemented to prevent malicious software from running. | If enterprise-wide preventive controls fail to detect and mitigate the threat before a user sees it, endpoint protection may add an additional mitigation step to prevent unauthorized use of computer resources. |

| Business Process Controls | | |
|---|---|---|
| **Type** | **Purpose** | **Summary** |
| Authorization verification controls | Controls to validate that users are authorized to request changes to bank routing or other payment information. | These controls can be used to prevent unauthorized changes to payroll or payment bank routing information. They include authenticating an e-mail request, calling the authorized vendor representative or the employee, or requesting physical verification through a cancelled check. |
| Review of vendor or employee master file changes | Management reviews all changes to the vendor or payroll master file. | The review of all vendor master file changes by a supervisor or manager may help reduce the risk of fictitious or fraudulent changes to the vendor master file, including changes to vendor payment bank routing information. Such a review would include verification of the change to authenticated requests. |
| Change confirmation | Controls to confirm payment information with vendor or employee. | A confirmation message is sent to a vendor or employee when a change to bank routing information is made so that the vendor or employee can verify the authentication of the change. |

## Key Takeaways

Bear in mind the following:

- The cybersecurity landscape continues to evolve, and schemes like the ones described above and in the SEC's report are increasing as more economic activities take place through digital technology and electronic communications.
- The BEC examples described above underscore the importance of devising and maintaining a system of internal accounting controls to address this kind of cyber-related fraud.
- Training and user security awareness play critical roles in both the implementation and operating effectiveness of controls.

While the SEC's report states that "the Commission is not suggesting that every issuer that is the victim of a cyber related scam is, by extension, in violation of the internal accounting controls requirements of the federal securities laws," it also emphasized that companies must "calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly." The above considerations, while not intended to be comprehensive, may be useful in a company's evaluation of its internal controls for preventing BEC scams.

## SEC's Focus on Cybersecurity

The SEC's release of the investigative report is consistent with the Commission's focus on the evolving risks associated with cybersecurity. Cybersecurity remains a priority for the SEC Enforcement Division's recently created Cyber Unit, which continues to target cyber-related misconduct.

In addition, on February 21, 2018, the SEC issued interpretive guidance[2] (the "release") in response to the pervasive increase in digital technology as well as the severity and frequency of cybersecurity threats and incidents. The release largely refreshes existing SEC staff guidance related to cybersecurity (e.g., CFDG Topic 2[3]) and, like that guidance, does not establish any

[2] SEC Interpretation No. 33-10459, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.
[3] SEC CF Disclosure Guidance: Topic No. 2, *Cybersecurity*.

new disclosure obligations but rather presents the SEC's views on how its existing rules should be interpreted in connection with cybersecurity threats and incidents. However, the release does address topics not discussed in previously issued SEC releases, such as (1) disclosures about a corporate board's risk oversight, (2) insider trading policies, and (3) SEC Regulation FD (on fair disclosure) and selective disclosure. For more information, see Deloitte's February 23, 2018, *Heads Up*.

Further, in its recently issued strategic plan for fiscal years 2018–2022, the SEC identified an initiative to "focus on ensuring that the market participants we regulate are actively and effectively engaged in managing cybersecurity risks and that these participants and the public companies we oversee are appropriately informing investors and other market participants of these risks and incidents." Accordingly, registrants should consider evaluating both their controls and disclosures related to cybersecurity as risks evolve and update them as needed.

## *Dbriefs* for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy and tax.
- Controllership perspectives.
- Driving enterprise value.
- Financial reporting.
- Governance, risk, and compliance.
- Tax accounting and provisions.
- Transactions and business events.

*Dbriefs* also provides a convenient and flexible way to earn CPE credit — right at your desk.

## Subscriptions

To subscribe to *Dbriefs*, or to receive accounting publications issued by Deloitte's Accounting Services Department, please register at My.Deloitte.com.

## DART and US GAAP Plus

Put a wealth of information at your fingertips. The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, IASB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and navigation system that, together with its powerful search and personalization features, enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's *FASB Accounting Standards Codification Manual*, and can also elect to receive *DART Weekly Roundup*, a weekly publication that highlights recent additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.

In addition, be sure to visit US GAAP Plus, our free Web site that features accounting news, information, and publications with a U.S. GAAP focus. It contains articles on FASB activities and those of other U.S. and international standard setters and regulators, such as the PCAOB, AICPA, SEC, IASB, and IFRS Interpretations Committee. Check it out today!