Beware of Increased Fraud

An increasing number of companies are falling victim to external fraud, including cyber-related fraud. Scams are being perpetrated through both email and telephone contact. Victims range from large corporations to tech companies, to small businesses, to nonprofit organizations.

One of the most dangerous types of schemes being perpetrated in recent years is the business email compromise — or BEC — scheme, in which businesses that regularly perform wire transfer payments are targeted.

The FBI estimates that organizations victimized by BEC fraud attacks lose on average between $25,000 and $75,000. But some BEC fraud incidents over the past year have cost victim companies millions — if not tens of millions — of dollars. The toy maker Mattel lost $3 million in 2015 due to a BEC fraud phishing scam. In 2015, tech firm Ubiquiti disclosed in a quarterly financial report that it suffered a $46.7 million hit because of a BEC fraud scam. Also, in 2015, email con artists made off with $17.2 million from The Scoular Co., an employee-owned commodities trader.

Law enforcement received complaints from victims in every U.S. state and in at least 79 countries; between October 2013 through February 2016, law enforcement received reports from 17,642 victims. This amounted to more than $2.3 billion in losses. The overwhelming majority of victims are located in the United States. Since January 2015, the FBI has seen a 270 percent increase in identified victims and exposed loss.

Below we feature recent BEC fraud schemes, and provide recommended internal controls to mitigate the risk of loss, as well as actions to take if you suspect your company has been scammed.

Recent Fraud Trends

BEC schemes go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money through social engineering or computer intrusion techniques, and use language specific to the company they are targeting, and then request a fraudulent wire transfer using dollar amounts that lend legitimacy. BEC fraud usually begins with the thieves either phishing an executive and gaining access to that individual's inbox, or emailing employees from a look-alike domain name that is one or two letters off from the target company's true domain name. For example, if the target company's domain was "example.com" the thieves might register "examp1e.com" (substituting the letter "l" for the numeral "1" or "example.co,") and send messages from that domain.

Unlike traditional phishing scams, spoofed emails used in BEC fraud schemes rarely set off spam traps because these are targeted phishing scams that are not mass e-mailed. Also, the thieves behind them take the time to understand the target organization's relationships, activities, interests and travel and/or purchasing plans. They do this by finding employee email addresses and other information from the target's website to make the missives more convincing. When executive or employee inboxes are compromised by the thieves, the thieves will review the victim's email correspondence for certain words that might reveal whether the company routinely deals with wire transfers — searching for key words like "invoice", "deposit" and "president." The schemers conduct research to learn about the employees in a company who manage the money, as well as the protocol necessary to perform wire transfers within that business environment

On the surface, BEC scams may seem unsophisticated relative to moneymaking schemes that involve complex malicious software. But in many ways, BEC fraud is more versatile and adept at sidestepping basic security strategies used by banks and their customers to minimize risks associated with account takeovers. In traditional phishing scams, the attackers interact with the victim's bank directly, but in a BEC scam the thieves trick the victim into doing that for them.

There have been a number of versions of BEC schemes that have been identified, including the following:

Version 1:
A business, which often has a long-standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, fax or email. If an email is received, the perpetrator will spoof the email request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request.

Version 2:
The email accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y."

Version 3:
An employee of a business has his/her personal email hacked. Requests for invoice payments to Fraudster-controlled bank accounts are sent from this employee's personal email to multiple vendors identified from the employee's contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

Version 4:
Fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time sensitive matters, contact the victim either via phone or email. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam typically occurs at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.

Version 5:
Victims receive fraudulent emails requesting either all Wage or Tax Statement (W2) forms or a company list of Personally Identifiable Information (PII) prior to a traditional BEC incident, typically during tax season. These fraudulent requests are usually sent utilizing a business executive's spoofed email. The entity in the business organization responsible for the W2 and/or PII, such as HR, accounting or auditing, is the targeted recipient of the fraudulent request. Victims report they have fallen for this even if they were able to successfully identify and avoid the subsequent traditional BEC incident.

Internal Controls to Mitigate the Risk of Loss

BEC fraud attacks succeed because they rely almost entirely on tricking employees into ignoring or sidestepping some very basic security precautions. Therefore, it is important that employees are educated about these types of scams and additional security controls are implemented where deemed appropriate.

Therefore, in order to effectively mitigate the risk of loss from these types of fraud schemes, management should consider implementing a number of internal controls, including, but not limited to, the following:

- Educate employees at all levels within the organization about potential scams
- Implement effective treasury controls
  - Dual approvals for wire transfers and automated clearinghouse (ACH) payments, with appropriate segregation of duties between initiator and approver/releaser of wire transfer
  - At a minimum, dual approval for all high value wires and ACHs
  - Protect ACH transactions
    - Pre-note zero-dollar transactions to verify the recipient routing number and account number before sending a live dollar transaction
    - Designate ACH batch templates as "confidential," so only entitled users can access them
    - Establish ACH Company IDs to limit user access to specific templates, accounts or reports
    - Import ACH and wire transfer files, instead of keying them into the system
    - Limit access to ACH third party/preferred recipient list
    - Establish Universal Payment Identification Codes (UPICs), to collect ACH payments from trading partners without divulging sensitive account information

    - Secure wire transfers
        - Use bank-defined wire templates to reduce the risk of unauthorized changes to beneficiary routing information
        - Call in international wires directly to the bank if you use them infrequently
    - Phone callbacks to verify significant transactions
    - Receivers of wire requests to validate with requestor by phone
    - Limitations on daily transfers
    - User limits
    - Bank account reconciliations should be performed monthly
- Ensure effective IT security
    - Systems should be protected by commercial quality firewall and anti-virus software
    - Install a software package intended to authenticate email addresses and better protect against threats
    - Security patches need to be applied as they are made available
    - Protect users' authorization passwords by adding alphanumeric characters, never share passwords, etc.
    - Use multi-factor authentication
    - Avoid conducting online banking business activities on home computers or at publicly shared Wi-Fi locations
- Implement purchasing controls that validate changes in vendor payment information or setup of new vendors
- Take domain names similar to the one used by your organization off the market by purchasing them. For example: Fortune.com might choose to buy "F0rtune.com," where the "o" has been replaced by a zero
- Exercise restraint when publishing information about employee activities (e.g., travel plans) on company website or through social media

What To Do If You Suspect Your Company Has Been Scammed

- Contact your local FBI or U.S. Secret Service office immediately to report a "business email compromise" scheme
- Contact both your financial institution and the receiving financial institution to request they halt or unwind the transfer
- Seek advice from counsel about any legal obligations or protections you may have related to this situation, such as potential insurance coverage for any loss
- Change your controls to minimize the risk of something similar happening again
- Alert employees about the scam, how it was perpetrated, and educate them about how they can be a gateway for the scammer — these steps may motivate employees to remain vigilant