Published on *The National Law Review* https://natlawreview.com

BEC/FBI Tech Hacking Advisory – Doing Business with Foreign Suppliers/Businesses

Article By:

Basileios "Bill" Katris

It was not so long ago that in the cyberspace realm businesses only needed to worry about having a good firewall and spam filter to prevent fraud. Now, as technology has advanced so have the fraudsters and the government is warning businesses, especially those conducting business with foreign suppliers and/or businesses, of a new and escalating scam called the Business Email Compromise, the BEC. Earlier this year, the FBI issued its first public service announcement ("PSA-Alert")about the BEC, out of its Internet Crime Complaint Center (IC3). Then, in August 2015, the FBI updated the BEC PSA-Alert in order to further warn businesses and to provide up-to-date statistics. The statistics published show that between October 2013 to August 2015 there have been more than 7,000 U.S. victims with losses estimated close to $750 million. Worldwide, the BEC losses are estimated at more than $1.2 billion.

What Businesses Need to Look Out For

Per the FBI PSA-Alert, the BEC **is a scam that targets businesses working with foreign suppliers and/or other businesses that regularly perform wire transfer payments**. The FBI has identified four main versions of the BEC scam. Version 1 typically involves 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 is sometimes made via e-mail in which the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Version 2 usually involves e-mail accounts of high-level business executives (CFO, CTO, etc) being compromised. The account may be spoofed or hacked and may result in a request for a wire transfer from the compromised account being made to a second employee within the company or a financial institution who is normally responsible for processing such requests. Version 3 typically involves personal e-mail of an employee being hacked and results inrequests for invoice payments to fraudster-controlled bank accounts sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. In August 2015, the FBI alerted the public to Version 4 of the BEC, which it described as victims "being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions."

How to Protect Your Business

The FBI has advised businesses to take the following protective measures (Alert I-082715a-PSA) :

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

While the measures above will provide some level of security, it is important to analyze your individual business's unique manner and methods of operations (i.e. IT security, conducting financial transactions, etc..), which may require additional security measures or protocols.

National Law Review, Volume V, Number 302