



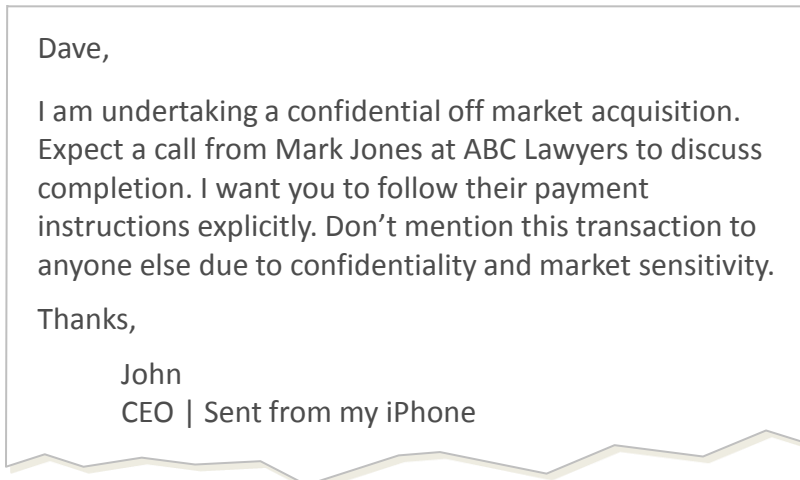
BUSINESS EMAIL COMPROMISE FRAUD

How to Develop Risk-Reduction and
Recovery Strategies

Companies are being targeted by social engineering fraudsters, circumventing traditional IT security controls and preying on the natural tendency of employees who want to be helpful. Awareness is the first step to reducing risk exposure.

The Touchpoint: what is Business Email Compromise?

A fraudster's email may look something like the one depicted below:



This kind of scam is called Business Email Compromise ("BEC") Fraud, and while it might initially seem easy to identify, it is in fact an expansive and mounting problem that is costing companies billions of dollars in stolen funds and trade secrets. BEC is problematic because it involves social engineering, which circumvents traditional IT security by exploiting employees' natural tendency to "want to help." The two partners in the

BEC example above would likely know each other well, the instructions *John* gives *Dave* would follow normal company procedures and the email would appear completely ordinary, as if the real CEO had sent it.¹

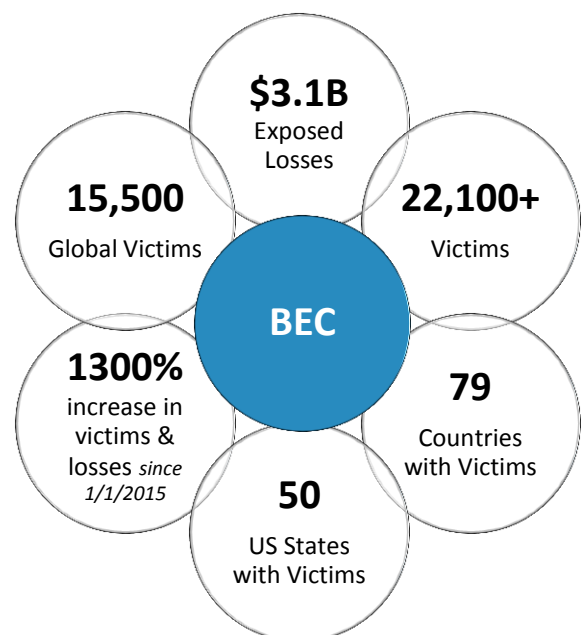
BEC tests the strength of a company's finance and accounting departments, and internal controls; BEC takes general business email security beyond reliance on most employees' common sense and initial email screening. Even companies with excellent IT security can be potentially vulnerable.

The Facts


BEC is a complex, refined scam, manifesting strategy in genuine but jeopardized business email accounts and utilizing computer intrusion techniques and social engineering to prompt unauthorized transfers of funds. Social engineering is defined as coaxing, threatening or simply deceiving people into either giving up information or performing an action that aids the fraudster in criminal activity.²

BEC most often occurs within businesses that frequently wire-transfer funds globally, but it can be done using checks, administrative expense codes or other means. Fraudsters use methods consistent with a company's standard practices. According to the latest FBI BEC Public Service Announcement June 14, 2016, this activity is a Global problem and it is growing exponentially. The statistics reflect losses from October 2013 to May 2016.³

BEC by the Numbers⁽³⁾



How BEC Fraudsters Operate



The fraudster team is sophisticated; its targets are selected deliberately

Fraudsters do their homework. They check publicly available information such as web pages, press releases and social media to obtain information on relevant company operating details:

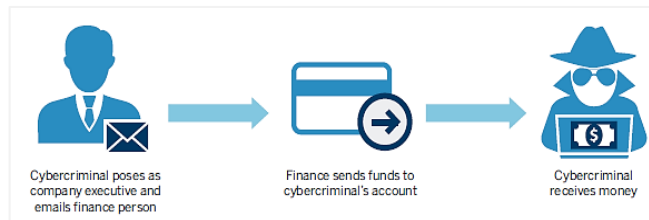
- Where the company operates and with whom
- Names and titles of company officers
- Individuals with wire transfer/monetary transaction responsibility
- Management organizational structure and reporting lines
- Changes to executive personnel
- Funding rounds
- New products and services or patents
- Product or geographic expansion plans
- Travel plans (e.g., CEO, CFO, conference attendance)
- Spoofing domain names

Fraudsters then prepare an email: spoofing or typosquatting, which makes the email domain appear legitimate although it contains a subtle error,⁴ the email is written using an urgent tone, uses an excuse like travel or a meeting to explain the style of request, states a realistic amount of money to be transferred according to standard procedures and is signed informally, or even with a default device signature such as “Sent from my iPhone.”

There are numerous variations of the BEC fraud methodology, and while consistently relying on social engineering, can take several forms.⁵

There are two frequent types of BEC fraud.

1. CEO Fraud | “Masquerading”

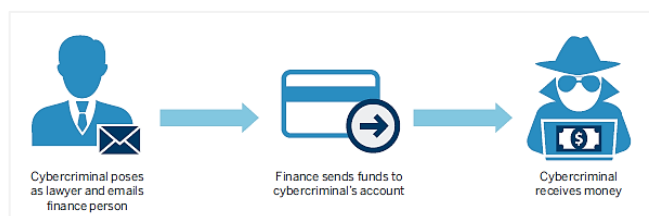


Email accounts of senior business executives (routinely the CEO, CFO, CTO) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instruction to send funds to “X” bank for reason “Y.”⁶ According to Trend Micro, the most imitated company positions for fraudsters are:

- CEO 31%
- President 17%
- President and CEO 13%
- Managing Director 15%

CEO Fraud | “Masquerading” method is also called “business executive scam” and “financial industry wire frauds.”⁷

2. Attorney Impersonation



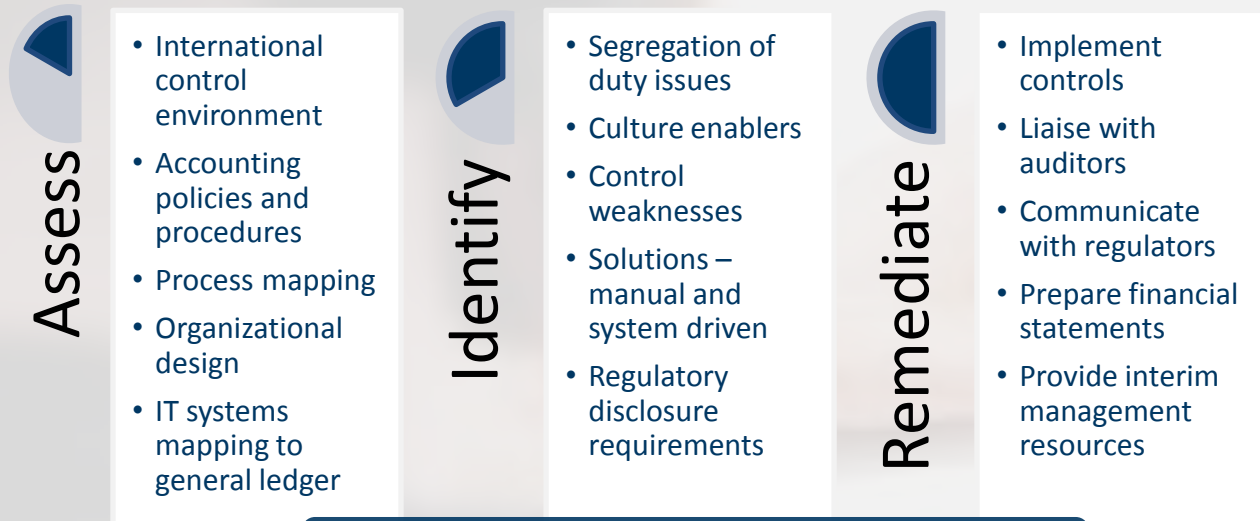
Victims are contacted by fraudsters by phone or email, claiming they are law firm representatives or lawyers. Then the fraudsters typically pressure the victim to keep the request confidential and/or to take action quickly when transferring the funds. Effective ways to make this technique work is to contact the finance person just before close of business, at the end of the work week and/or at close of business for international financial institutions. Primary positions targeted in BEC frauds are CFOs, finance directors and finance controllers – employees in charge of a company’s finance and accounting department, including duties responsible for transferring funds, vendor setup and accounts payable.

Strategies to Deal with BEC

BEC challenges the fabric of the internal control environment in the finance and accounting departments. Companies either face the threat of BEC or face the aftermath of its activities, but either situation will benefit from enhanced existing internal controls.

The Risk-Reduction Strategy

Three activities can help to reduce the risk of exposure to BEC:



Awareness is the best way to prevent BEC Fraud

Assessing internal control environments and **identifying** weaknesses that could enable fraudsters to perpetuate a BEC event is critical.

Not only will assessing controls and identifying weaknesses help safeguard a company's assets, but it will also reduce the chances of a potential misstatement of financial results arising from material weaknesses in internal controls over financial reporting.

Creating detailed action plans to **remediate** identified internal control weaknesses, whether system or manually driven, and preparing analyses to corroborate that these weaknesses have been addressed will mitigate the likelihood of a BEC event (or of it being repeated).

Social engineering exposes deficiencies in internal control-environment contributors including:

- Accounting policies and procedures
- Process functionality and mapping
- Segregation of duties
- Organizational structure
- Communication and training
- Integration of accounting IT systems
- Cybersecurity protocols

The Recovery Strategy

If you or your client falls victim to a BEC event, it is essential that a team quickly mobilizes to investigate the incident thoroughly, safeguard the evidence for future litigation and tactics for recovery that will endure into the future:



Investigate

- Conduct computer forensic examinations and data collections to uncover vital evidence
- Identify participants
- Conduct Witness Interviews
- Reconstruct records



Litigate

- Preserve evidence
- Prepare formal reports for regulators and law enforcement in conjunction with counsel and electronic evidence services



Recover

- Assist law enforcement with investigations
- Trace the movement of assets
- Assess viability of recovering funds
- Recommend remediation tactics, regulator investigation responsiveness

In a post-BEC event scenario, the outcome will be heavily dependent on a comprehensive global forensic solution. Responding quickly, both domestically and internationally, to investigate the source of the BEC fraud, identify the perpetrators, quantify the extent of the losses and damages, move swiftly to provide support for recovery actions and collaborate with counsel to address regulatory, litigation and disclosure risks is essential for a smooth and rapid recovery.

The BEC Impact

BEC wire transfers are predominantly made to Chinese and Hong Kong banks⁸, and as companies' awareness grows and security measures increase to counter the bold and direct wire transfer method, fraudsters are trying another, more surreptitious technique. Using the same fake email method, fraudsters seek to perform tax refund fraud using W-2 forms, collected from junior accounting or human resource employees. While stealing tax refunds is less lucrative than large wire transfer requests, this method demonstrates the increasing diversity of the BEC scam⁹: BEC does not discern between small or large corporations, it pursues various sums and targets numerous industries.

The companies below have experienced BEC Fraud, through either wire-transfer or W2-form fraud¹⁰:

Company	Type of Fraud	Loss	Date
The Scoular Co.	Wire-Transfer	\$17.2 million	June 2014
SnapChat	W2	Data Leak	March 2016
Seagate Technology	W2	Data Leak	March 2016
AFGlobal Corp.	Wire-Transfer	\$480,000	May 2014
Medidata Solutions Inc.	Wire-Transfer	\$4.8 million	Feb. 2015
Ubiquiti Networks Inc.	Wire-Transfer	\$46.7 million	June 2015
Mansueto Ventures	W2	Data Leak	March 2016
Sprouts Farmer's Market	W2	Data Leak	March 2016
Pivotal Software	W2	Data Leak	March 2016
Xoom	Wire-Transfer	\$30.8 million	Jan. 2015

A Success Story

The following case study is a real life example of the problems confronted by a NASDAQ listed \$4B global data communications equipment and Tech Hardware manufacturer during 2016.

Situation

The company experienced a Business Email Compromise incident which resulted in a loss of \$39.1 million. The BEC incident and resultant investigation led to the identification and disclosure of more than a costly, one-time mistake. The investigation pointed out three material weaknesses in internal controls over financial reporting at financial year end, with other areas of improvement, particularly in the FP&A function, also identified. Much of the prior management had left, and the company required interim management to ensure timely financial reporting and Internal Control Remediation following the BEC incident.

The principal tasks the company needed to complete included:

- Fill multiple management positions: CAO, Assistant Controller, SEC Reporting Manager, International Controller and AP Manager
- Obtain someone to become the principal accounting authority for SEC quarterly and annual reporting and overseeing of the external audit function
- Remediate of internal control deficiencies, documentation of accounting policies and procedures and IT systems mapping
- Redesign and rebuild the Finance and Accounting Organization, including recruitment, transitioning of new hires and geographic relocation
- Implement improved financial reporting and projection capabilities

Outcome

The recovery was an overwhelming success. The company recovered \$8.1 million of the initial loss, issued its delinquent financial statement, rebuilt and significantly improved the Finance & Accounting Organization to be able to comply with SEC reporting in a timely and accurate manner.

The company now has risk-reduction strategies in place and is prepared for any future threats.

Sources

1. <https://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/#more-33617>
2. <https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business>
3. FBI Internet Crime Complaint Center (IC3), June 2016
4. <http://fraudwatchinternational.com/expert-explanations/what-is-a-bec-scam/>
5. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise>
6. Federal Bureau of Investigation, Public Service Announcement I-061416-PSA, June 14, 2016; <https://www.ic3.gov/media/2016/160614.aspx>
7. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise>
8. <http://www.chinalawblog.com/2016/08/the-china-bank-scam-its-growing.html>
9. <https://threatpost.com/fbi-social-engineering-hacks-lead-to-millions-lost-to-wire-fraud/114453/>

10. Table Sources:

1. <http://www.cso.com.au/article/595279/what-ceo-spoofing-attack-snapchat-looked-like/>
2. <https://krebsonsecurity.com/tag/the-scoular-co/>
3. <https://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/#more-33617>
4. http://www.omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html
5. <https://www.law360.com/articles/770108/medidata-insurer-denied-wins-in-4-8m-fraud-coverage-suit>
6. <http://www.thedenverchannel.com/money/sprouts-farmers-markets-employee-information-compromised-in-phishing-scam>



Mark Spragg

Senior Managing Director
mark.spragg@fticonsulting.com

Nathan Landrey

Senior Managing Director
nathan.landrey@fticonsulting.com

Edward Westerman

Senior Managing Director
edward.westerman@fticonsulting.com

The views expressed herein are those of the authors and not necessarily the views of FTI Consulting, Inc., its management, subsidiaries, affiliates, or other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on [Twitter \(@FTIConsulting\)](#), [Facebook](#) and [LinkedIn](#).