Introduction

Business email Compromise (BEC), also known as email Account Compromise or CEO Fraud, is a scam targeting businesses globally and is a growing threat. BEC fraud schemes are among the fastest-growing cyber-enabled crime threats, causing billions of dollars in losses worldwide. In 2018, the Federal Bureau of Investigation’s (FBI) Internet Crime Compliance Centre received 20,373 BEC complaints, representing losses of more than USD1.2 billion, almost double those of 2017. Based on the US Financial Crimes Enforcement Network’s (FinCEN) analysis of information contained in Suspicious Activity Reports, it was revealed that the total value of attempted BEC thefts reached an average of USD301 million per month in 2018 (i.e. more than USD3 billion annually). BEC scams continue to grow and evolve, targeting businesses of all sizes. Victims are spread across the globe, although funds stolen through BEC fraud are often initially sent to mule accounts in Hong Kong and China.

What is BEC Fraud and How Does It Work?

Step 1 Targeting
Fraudsters target companies and local government departments globally.

Step 2 Reconnaissance
Fraudsters scrutinise publicly-available information for potential targets through professional and social media websites such as LinkedIn, Facebook, and Google.

Step 3 Compromise
Fraudsters may hack the email accounts of a target company, using social engineering tactics, such as phishing emails, which induce the victim to click on a malicious link that then downloads malware. This malware gives fraudsters access to the company’s email accounts or reveals information such as passwords, enabling them to monitor communications within the company and identify the parties who regularly initiate fund transfers.

Step 4 Impersonation
Once fraudsters have access to an email account, they can send emails from that account impersonating a trusted party (e.g. CEO or supplier). These instructions might be sent to the finance department or other staff with financial authority with the objective of making them think a request to remit funds or change beneficiary account details is for a legitimate business purpose. For example, fraudsters may pose senior manager within the company (CEO Fraud) or a supplier (Supplier) to initiate fund transfers.

Step 5 Transferring Money
Fraud), requiring an urgent payment to solve a cash flow issue or to procure goods or services. Email accounts for vendors, lawyers, and other sectors (such as real estate) may also be spoofed.

Fraudsters do not always need to compromise a target email account directly in order to carry out an impersonation. Slight variations on legitimate email addresses and web domains may be used, which at first glance might appear genuine, making the victim believe the email comes from someone they trust. Closer inspection would reveal that the email address is different from the legitimate account (e.g. a fraudster may use Richard.Chan@abcbanking.com to impersonate legitimate account Richard.Chan@abcbank.com).

Fraudsters may also use malware to direct email replies to an account under their control, and the victim is induced to believe they are responding to an email from a trusted party.

BEC Fraud Evolves

In order to accomplish a deception, According to FinCEN, BEC scam methods evolve over time. For example, impersonating senior managers accounted for 33% in 2017, declining to 12% in 2018, while using fraudulent vendor or client invoices grew from 30% in 2017 to 39% in 2018.

“Cybercrime has become increasingly financially motivated; banks and the financial sector are a key target for cybercriminals, with some of the main threats being banking Trojans, ATM malware, DDoS attacks, card-present and card-not-present fraud, CEO or Business email Compromise (BEC) fraud and ransomware. The crime-as-a-service business model which underpins cybercrime provides access to cybercrime tools and services that allow even entry-level cybercriminals to conduct attacks hugely disproportionate their skill level, often for negligible costs.”

Steve Wilson | Head of the Europol Cybercrime Centre

References:
1. Bulletin on Business Email Compromise Fraud issued by the Egmont Group on 30 July 2019 (link)
2. FBI Internet Crime Report 2018 (link)
3. FinCEN Financial Trend Analysis: Manufacturing and Construction Top Targets for Business Email Compromise July 2019 (link)
4. News article “Tackling cybercrime is a major challenge for Europe” (link)
Best Practice

BEC fraud is usually successful for three main reasons: lack of staff awareness, social engineering, and insufficient security protocols. Below are some suggested solutions that may help to safeguard against BEC fraud:

✓ Train and educate staff to increase their awareness of BEC fraud and ensure they feel empowered to speak up if they receive an unusual communication. For example, the cyber security team or other internal team(s) within the company might undertake tests of staff awareness and response by sending emails simulating “phishing”.

✓ Stress the importance of vigilance and prompt reporting of any potential incidents of fraud, even if there is only a suspicion. Ensure staff do not open suspicious links or attachments received by email. Staff should be particularly careful when checking private emails on the company’s computers (if the company allows its staff to do so).

✓ Staff should be alert to unusual requests by senior managers or other persons who might not normally send such emails.

✓ Staff should be alert to requests which are described as urgent or which request confidentiality or secrecy, particularly where they contradict internal procedures or practices, or involve a fund transfer to a country / bank / account that would not usually receive such a transfer. In case of doubt on a transfer order, staff should consider consulting a competent colleague.

✓ Implement internal protocols concerning fund transfers, including appropriate documentation and approvals. For example, for large or unusual fund transfers, a requirement for secondary confirmation of the transfer request could be considered (e.g. by using telephone verification as part of such two-factor authentication). Only previously verified telephone numbers should be used, rather than those provided in the email request (which could be controlled by the fraudster).

✓ Detection systems that use artificial intelligence (AI) and machine learning to enhance overall cyber defense against BEC should be considered. These can help flag invalid email addresses (e.g. for a company where their legitimate email format is abc_company.com, variations such as abc-company.com would be flagged as fraudulent). A rule should also be implemented to flag email communications where the “reply to” email address is different from the “from” email address shown. Additionally, staff should check email addresses when dealing with sensitive information and fund transfers.

✓ Email systems can also be configured to colour-code emails so that employee / internal accounts are one color and emails from non-employee / external accounts are another. Alternatively, emails from external accounts can be flagged or annotated as “External”.

✓ AI and machine learning can help to analyse email behavior, email authorship (e.g. checking the sender’s writing style), and email intention (e.g. payment or urgency). When the AI detects indications that an email sender is impersonating a senior manager within the company, a warning can be sent to the implied sender (i.e. the senior manager being impersonated), the recipient, and the internal team(s) responsible for action, such as Information Security.

✓ Review information posted on the company’s website to minimise the risk of social engineering and encourage staff to show caution on social media. Avoid sharing information of the company’s hierarchy, security or procedures.

✓ Reinforce the importance of data security, encrypt sensitive data, and ensure that the company anti-malware / anti-virus systems are always up to date.

Here for Good

At Standard Chartered, we are committed to tackling all the financial crime threats we face. Where we identify red flags and typologies based on accounts used to receive the proceeds of fraud, we share these with regulators and our industry peers.

“We work together with regulators, our fraud risk management team, global associations to communicate the education message not only to our clients locally but also other parts of the world.”

Paddy O’Hara | Head of Financial Crime Compliance, GCNA, Standard Chartered Bank