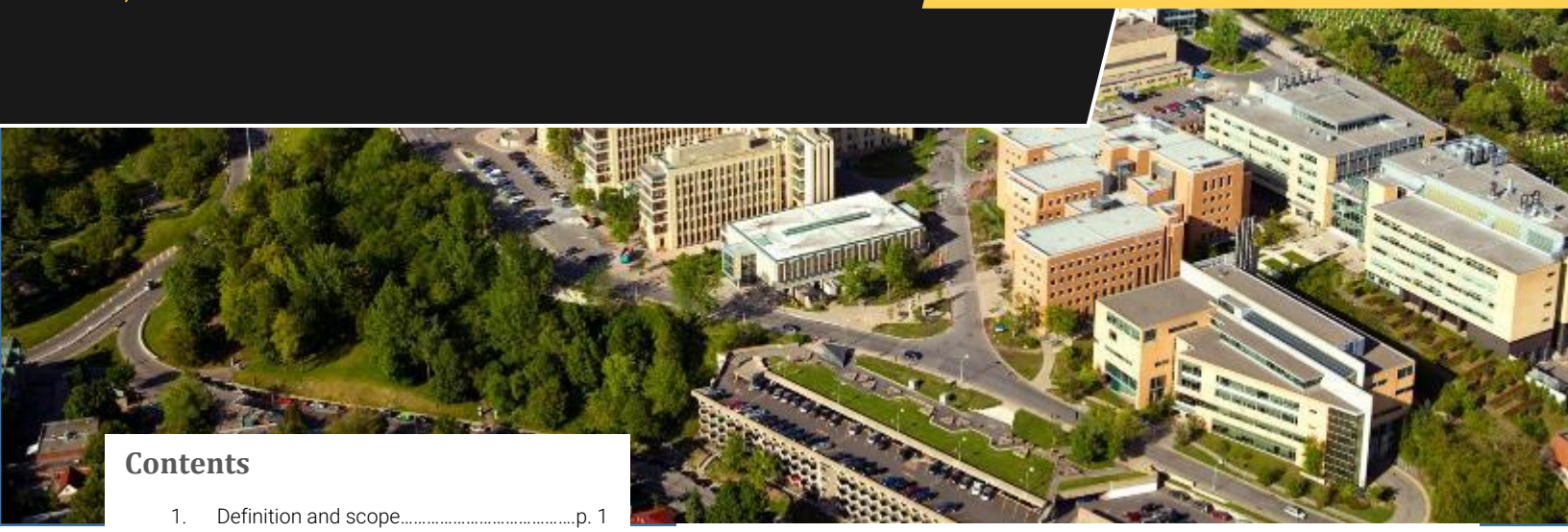
Business Email Compromise

Claire Gagnon, Master's Candidate

RCCP Research Chair in Cybercrime Prevention

Briefing Note
Vol. 2, No. 3



Contents

The Research Chair in Cybercrime Prevention was established on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Definition and scope

First reported around 2005, **Business Email Compromise (BEC) began as a cyberattack by hackers impersonating company executives (chief executive officer or chief financial officer) and tricking employees into making unauthorized funds transfers.**[1, 2] BEC now extends to requests for confidential information, gift card purchases and masquerading as suppliers.[3, 4] To give the impression that the request is legitimate, fraudsters initiate the interaction from an organization's hacked email address or a quasi-identifiable email address.[5]

Requiring little effort and technology, BEC has significant advantages over other types of online fraud.[6] It's highly profitable for fraudsters, the victim response rate is higher than for other types of attacks and although fraudsters must research into the organization, the duration of the attack from contact to completion is three days on average.[6]

While this type of fraud is not the most significant in terms of the number of victims, it causes considerable financial losses. According to the Internet Crime Complaint Center (IC3), losses from BEC in 2019 were 3.7 times higher than for any other type of fraud.[3] Total estimated global losses reported between June 2016 and July 2019 were more than US$26 billion for more than 166,000 reported incidents.[4]

Victim profile

Financial losses, often considerable, can amount to several million dollars for a single company.[7] During the last three months of 2019, fraudsters obtained $2,500 to $680,000 per bank transfer request, or about $55,000 on average.[8] In the case of gift cards, the requested amounts were much more modest, ranging from $250 to $10,000, for an average of $1,600.[8]

From July 2018 to June 2019, **the countries most affected by CEO fraud were English-speaking**: The United States (39%), the United Kingdom (26%) and Australia (11%).[9] Next in line were Belgium (3%), Germany (3%) and Canada (2%).[9] In total, more than 177 countries were targeted.[4] The bulk of the attacks originate in Nigeria, but fraudulent organizations have also been detected in Russia, Ghana, Kenya and Israel.[6, 10]

The fraudulently obtained amounts were transferred to no fewer than 140 countries, **the main destinations being Hong Kong and China**. The United Kingdom, Mexico and Turkey are increasingly frequently mentioned.[4] Some of these countries act as temporary havens where the money is laundered before being sent to fraudsters. In addition, according to FinCEN, 73% of incidents reported in the US also involved local transfers, made possible through mule networks.[11] Mules are fraud middlemen whose role is to "lend" their bank account to criminal organizations. Money from victim organizations is deposited in mule accounts and transferred to a foreign bank account.[6] Transfer requests are less likely to arouse the suspicions of victims and the anti-fraud units of financial institutions if they come from the countries of the victim organizations. Mules may be unaware that these transactions are being used for illegal purposes and may themselves fall victim to employment opportunity or romance scams.[6]

BEC targets businesses and organizations and **can affect any industry**. For example, educational and academic institutions, manufacturing or service companies, financial institutions and even non-profit organizations can be targets.[4, 5, 6, 12] An Ohio church, for example, lost nearly US$1.8 million as a result of BEC.[13] While all sectors can be targeted, some are more at risk than others, with manufacturing and construction at the top of the list, accounting for 25% of all attempts, for an average of $54,000, followed by the retail sector (18%) and the real estate sector (16%).[11] The latter has seen a variation of BEC in which the scammer impersonates a real estate agent, changes the agent's banking account information held by the client and demands payment for the property purchased.[14] The average amount requested is $179,001,[11] which is higher than for other identity theft cases. Given the huge potential rewards, fraud attempts in the real estate industry have increased dramatically over the past three years.[11]

Within organizations, **anyone with the authority to make or authorize a bank transfer or disclose confidential information may be a potential target**.[15] In most cases, scammers look at the organization chart, particularly the information posted online, and even hack email accounts. By infiltrating the company's key internal communications, they can obtain signatures, ascertain customary transfer protocols, identify loopholes in authorization and authentication protocols, and send fraudulent emails without fear of them being detected as suspicious.[5, 16]

Scammers adapt to the business hours of the organizations they target to ensure that fraudulent email messages take time zone differences into account and are received during business hours.[14,17] As a result, 91% of attacks are carried out on weekdays.[17] Lastly, scammers use grammar and spell checkers to avoid making spelling or punctuation mistakes in English emails.[6]

Risk factors

Given the targeted nature of BEC, cybercriminals need to be familiar with the organizational structure of the victim institutions and identify the reporting relationship between the

target and the person whose identity they plan to steal.[18] It's important to personalize the cyberattack to make the request appear legitimate.[2, 18] Several risk and protection factors at the organizational and individual level are associated with this fraud.

Organizational factors

Companies with high billing volumes or international business are prime targets for BEC[11, 18, 19] A business that is accustomed to making large transfers will also be more lucrative for fraudsters than a company that makes only smaller transfers.

According to the FinCEN, the business line of the target organization plays an important role. For example, in 2017, financial firms were more targeted than others.[11]

Organizations with **publicly available information on their reporting structure and partners** are particularly at risk. In fact, the more the fraudsters know about their target, the better their chances of success.[20]

The time of year plays into BEC trends. For example, **gift card purchase attempts increase during the lead-up to the holiday season**.[17] Educational institutions are more targeted in September, at the start of the school year. This is a busy time for schools when many purchases are made and new employees start their jobs.[17] Tax season is also an attractive time for fraudsters.[17] Conversely, some periods, such as the July 4 (US national holiday) and Labour Day weekends, see decreases in the number of BEC attempts.[17]

Individual factors

Work overload, urgency and lack of fraud awareness are risk factors.[22, 23] Fraudsters can also rely on the zeal of a new employee who, wishing to look good, won't question requests from the CEO and will reply quickly.

Some psychological factors, such as **attention deficit, fatigue, and sensitivity to the fraudster's manipulation techniques** may also be risk factors.[22, 24] Perpetrators of BEC use social engineering techniques, particularly those that exert psychological pressure on the victim owing to the urgency of the request. This sense of urgency is reflected in the emails sent to the victim that use keywords, like "have a moment," "transaction request," "important" and "urgent"[9, 17, 25] and the fact that the email is deliberately sent near the end of office hours.[26]

Some fraudsters will try to make contact with the victim before giving them all the information needed to reply to the request. For example, "are you at your desk or available to do a rush transaction?", a person replying to such an email is ten times more likely to become a victim.[6]

Employees can also disclose sensitive information. For example, an employee's LinkedIn profile may provide information on the employee's corporate finance responsibilities.[20]

Recommendations

The consequences of succumbing to BEC can be numerous and substantial. **Financial loss** is the most direct consequence. A drop in equity values and **reputational damage** can also occur when BEC is disclosed to the public.[24, 27] The impact of these negative consequences is such that some businesses don't report being fraud victims.[28] In more serious cases, some companies have to dismiss their employees or declare bankruptcy.[24, 27] At the individual level, the employee responsible for the fraudulent transaction may suffer psychological harm, lose the organization's trust, have responsibilities taken away or even be fired.[22, 24, 27, 29]

Technology-based prevention

Several characteristics of this type of fraud make technology-based detection complex. The targeted nature of email and the use of email services with a high reputation score are constraints on technology-based prevention.[17, 18] Because these fraudulent emails are rarely sent with malicious links or files, **they are not**

considered dangerous by anti-virus software.[30] In addition, fraudulent email is only sent to a maximum of six people within a company and therefore cannot be considered spam.[17] Lastly, if the email comes from a hacked email account, the likelihood of the fraud attempt being detected is low.

To prevent the hacking of email accounts, it's important to be aware of basic protective measures, such as using unique and complex passwords.[31] Also recommended is the use of multi-factor authentication (MFA) technologies, which prevent accounts from being compromised by requiring several forms of identification at each login. There are many low-cost, easy-to-use solutions to protect against email account hacking. An intrusion detection system can be installed to supplement basic protections.[24] The organization must also assess its internal security controls on a regular basis or even hire a cybersecurity consultant or develop a dedicated inhouse unit, depending on the size of the company.[21, 24]

The DMARC email authentication protocol detects and limits consumer exposure to fraudulent emails, such as spam and phishing emails. Observations from the Cosmic Lynx study show that this crime group specifically selects companies that do not have DMARC[10] standards in place.

Corporate liability

Transfer requests must be doubly confirmed, using two different methods to verify their legitimacy, for example, replying to an email from a new message thread and then calling the person concerned using the phone number provided by the organization.[18, 24] However, the best solution is in-person confirmation or videoconference confirmation, if necessary. Cases of BEC using artificial intelligence have been noted.[35] To confirm the CEO's stolen identity or send an oral confirmation from the CEO, fraudsters have used existing videos to reproduce the company CEO's voice.[36] The transmission of sensitive information and changes to an employee's or partner's banking information must be subject to similar controls.[18, 24]

An additional protection is to prohibit emergency payments within the company.[32]

Finance employees must be limited in number and have differentiated tasks.[33] For example, one employee handles invoices, another prepares payments and a third confirms transfers.[32] All players in the payment chain must be made aware of various types of fraud and their consequences.[5] Online fraud awareness training, including for BEC, is available to organizations free of charge or for purchase.[34] Employee training must be comprehensive, cover the various methods used by fraudsters and increase employee vigilance during risk periods.

Given that fraud is more likely to succeed the more fraudsters know about a company, it is necessary to monitor the public information available on an organization's internal and external operations.[12, 20]

Companies must also have a fraud action plan so they can respond quickly if fraud occurs.[32] Despite the high percentage of businesses fearing an increase in fraud and cybercrime, only half have a contingency plan in place if a threat materializes.[32]

Other recommendations

The scientific literature on BEC is limited and rarely deals with targeted employees and specific risk factors. From a prevention and awareness perspective, specific attention should therefore be given to this aspect. Police institutions and victims must continue to be proactive, particularly by encouraging fraud reporting, freezing mule bank accounts, closing accounts used fraudulently and making strategic arrests through international cooperation.[6]

BEC and several other types of fraud are closely linked, which suggests that BEC should be analyzed from a holistic perspective. For example, mules may be recruited through

online romance or employment opportunity scams.[6] In addition to these scams, BEC is often conducted in conjunction with online vehicle sales, rental and lottery scams.[19]

Lastly, in the United States, money recovery programs, such as the FBI's Recovery Asset Team, have been set up specifically for BEC victims.[37] Although the money can be recovered only if it was sent locally, 75% of the US$258 million obtained through fraud has been returned to the affected businesses[9]—much more than would be recovered otherwise. In fact, if fraud is not detected within 24 hours and payment was made using gift cards or sent internationally, there is little chance of recovering the money.[5] Given this program's encouraging results, it's important to develop it and even implement it in other targeted countries.

References

[1] Competition Bureau Canada. (2018). Faits sur la fraude — Détecter, contrer et signaler la fraude.

[2] Sûreté du Québec. (2017). Fraude du président, soyez vigilant.

[3] Federal Bureau of Investigation (FBI). (2019). Internet Crime Report.

[4] Internet Crime Complaint Center (IC3). (2019). Business Email Compromise: The $26 Billion Scam.

[5] Financial Crimes Enforcement Network (FinCEN). (2019). Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business.

[6] Jakobsson, M., Wilson, J. and Linton, J .(2018). Behind the "From" Lines: Email Fraud on a Global Scale.

[7] Larouche, V.(2017). Comment un escroc a volé 5,5 millions à La Coop fédérée. *La Presse*.

[8] Agari Cyber Intelligence Division (ACID). (2020). Q1 2020: Email Fraud & Identity Deception Trends.

[9] Symantec Security Response. (2019). BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly.

[10] Agari Cyber Intelligence Division (ACID). (2020). Cosmic Lynx Threat Dossier: The Rise of Russian BEC.

[11] Financial Crimes Enforcement Network/FinCEN. (2019). Manufacturing and Construction Top Targets for Business Email Compromise.

[12] Federal Bureau of Investigation (FBI). (2017). Business E-mail Compromise. E-mail Account Compromise: The 5 Billion Dollar Scam.

[13] Muncaster, P. (2019). US Church Hit in $1.8m BEC Scam. Infosecurity Magazine.

[14] Remorin, Lord, Flores, R. & Matsukawa, B. (2018). Tracking Trends in Business Email Compromise (BEC) Schemes. Trend Micro 26.

[15] Federal Bureau of Investigation (FBI). (2017). Business E-Mail Compromise.

[16] Abbasi, F. Advanced Deception with BEC Fraud Attacks. (2018). Trustwave.

[17] Barracuda. (2019). Spear Phishing: Top Threats and Trends. Defending against business email compromise attacks.

[18] Canadian Center for Cyber Security. (2017). Campagnes de fraudes par nom de sosie de domaine et par virement bancaire.

[19] US Justice Department. (2019). 281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes.

[20] Mansfield-Devine, S.(2016). The imitation game: how business email compromise scams are robbing organisations. Computer Fraud Security, 5–10.

[21] Zweighaft, D. (2017). Business email compromise and executive impersonation: are financial institutions exposed? *J. Invest. Compliance*, *18*, 1–7.

[22] knowbe4. (2017). CEO FRAUD: Prevention Manual.

[23] Proofpoint. (2016). Qu'est-ce que le Business Email Compromise (BEC) ?

[24] Carlier, L. (2018). Fraude au président : vous êtes une cible, ne devenez pas une victime. *Richter*.

[25] Cidon, A., Gavish, L., Bleier, I., Korshun, N., Schweighauser, M. and Tsiking, A. (2019). High Precision Detection of Business Email Compromise. Proceedings of the 28th USENIX Security Symposium.

[26] Kikerpill, K. and Siibak, A. (2019). Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails. *Masaryk Univ. J. Law Technol.*, *13*(45).

[27] Agazzi, A. E. (2020). Business Email Compromise (BEC) and Cyberpsychology. *ArXiv Cornell Univ*.

[28] Berthier, T. (2017). Attaques par HoaxCrash et par Faux Ordres de Virement : la puissance du leurre cognitif.

[29] Cross, C. and Gillett, R. (2020). Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. *J. Financ. Crime*, 1–14.

[30] Barracuda. (2019). Spear Phishing: Top Threats and Trends. Email account takeover: Defending against lateral phishing. *Barracuda*.

[31] AIG. (2019). Cyber Claims: GDPR and business email compromise drive greater frequencies.

[32] Boullier, C., Gicquel, F., Goy, O., Hager, S. and Chauffert-Yvart, V.(2019). 5e baromètre DFCG / Euler Hermes sur la fraude et la cybercriminalité.

[33] Competition Bureau Canada. (2018). Le petit livre noir de la fraude 2e édition.

[34] Association Internationale des Douaniers Francophones (AIDF). (2019). E-learning destiné à la prévention de la fraude au changement de coordonnées bancaires. Association Internationale des Douaniers Francophones.

[35] Radio-Canada. (2019). L'IA utilisée pour recréer la voix d'un PDG et voler 320 000 $ à une entreprise.

[36] Pindrop. (2018). Voice Intelligence Report.

[37] Halpern, M. and Gregory, D. (2019). FBI, This Week: Recovery Asset Team Helps Return Stolen Funds to Victims.