SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 227

BUSINESS EMAIL COMPROMISE (BEC) AS A THREAT TO ORGANIZATIONS: A CASE STUDY

Luigi LAI

National Information Processing Institute, Warszawa; luigi.lai@opi.org.pl, ORCID: 0000-0001-9515-5109

Purpose: This analysis investigates Business Email Compromise (BEC) as a significant threat to corporate financial stability. Utilizing a paradigmatic case study of a multinational industrial enterprise, the research identifies critical organizational shortcomings and proposes risk mitigation strategies. Furthermore, the study highlights existing gaps within legal frameworks that impede effective cross-border fraud prevention and asset recovery.
Design: The research methodology employs a qualitative case study approach, integrating both legal and managerial perspectives to examine BEC intricacies. Data collection involved a detailed examination of publicly available judicial and banking records, situating the case within the broader phenomenon of cyber-enabled financial fraud.
Findings: Findings identify weaknesses in corporate payment protocols facilitating BEC: predictable workflows and limited authentication. Additionally, significant legal and organizational factors, particularly jurisdictional fragmentation, hinder timely asset recovery, notably by delaying necessary cross-border cooperation.
Research limitations/implications: Because the analysis focuses on a single case study, the generalizability of the results is inherently constrained. Future investigations should include comparative and quantitative approaches, spanning multiple jurisdictions, to evaluate the efficacy of preventive legal frameworks on a broader scale.
Practical implications: Findings support the tightening of internal security protocols, particularly through dual-channel verification and the adoption of anomaly detection tools. Continuous staff training in secure email practices and social engineering awareness is likewise essential to thwart increasingly sophisticated cyber threats. Implementing these measures can substantially reduce financial exposure and enhance overall organizational resilience.
Social implications: Although the primary focus is on corporate risk management, this research has broader societal relevance by raising awareness of digital threats and reinforcing public trust in electronic payment systems.
Originality/value: This article contributes to scholarly discourse by providing a comprehensive analysis that integrates the legal dimensions of BEC with a detailed examination of organizational vulnerabilities. The paper is therefore particularly relevant to legal scholars, management researchers, cybersecurity experts, and practitioners involved in fraud prevention.
Keywords: Business Email Compromise; Digital Fraud; Social Engineering; Cybercrime; Organizational Security.
Category of the paper: Research paper; Case study.

1. Introduction

This article is the result of an empirical analysis of a specific case of Business Email Compromise (BEC) fraud that took place in Poland; BEC fraud is a phenomenon that represents one of the most insidious threats to business management in the field of cybercrime (Cross, Gillett, 2020). The scam takes the form of a sophisticated social engineering attack that has the potential to affect all types of companies, from very small to multinational; generally speaking, the modus operandi is as follows: a group of fraudsters uses email to trick an individual or company into transferring money or revealing confidential information, often by appropriating their digital identity (Simpson, Moore, 2019).

The very nature of this type of fraud is by no means new: the tendency to manipulate and deceive others for illegal gain dates to antiquity. It is no surprise that the Latin saying 'nihil novi sub sole' (nothing new under the sun) perfectly describes this phenomenon. While in the past, attempts at fraud relied on convincing eloquence or forged documents – such as the classic example of a con artist trying to sell the Colosseum to unwary tourists – today, digital technologies have transformed and amplified these methods, making them more insidious and difficult to detect. However, the basic principle remains the same: the weak point of any security system is the human factor.

In the case in question, the fraudster managed to infiltrate the electronic correspondence between buyer and seller by adopting a sophisticated modus operandi. In a manner that can be compared to a real comedy of deception, the fraudster alternately assumed the identity of the seller and the buyer, manipulating the communication to achieve the desired result. The fraudster then tricked the buyer into making a payment to a new, apparently legitimate bank account that belonged to the cybercriminal himself.

By analysing this episode, it is possible to highlight the typical modus operandi of BEC fraud and to outline the most common vulnerabilities in the corporate sector. The aim of this article is not only to understand the mechanisms of such attacks, but also to propose concrete strategies for risk prevention and management to protect companies in an increasingly digitised and interconnected business environment.

From a legal point of view, current regulations do not always guarantee effective protection against such fraud, especially in the case of cross-border transactions. The lack of uniform international standards for freezing and returning misappropriated funds further complicates the fight against this phenomenon.

The aim of this study is to analyse the susceptibility of corporate and banking systems to BEC fraud and to propose preventive strategies and risk mitigation measures. Only through increased awareness and improved cybersecurity practices can companies effectively defend themselves against this increasingly common type of threat (Federal Bureau of Investigation, 2019).

2. Theoretical framework: Digital frauds and Business Email Compromise

Digital fraud encompasses a broad spectrum of malicious activities designed to exploit technological systems, human vulnerabilities, and organizational processes for financial or informational gain. Among these, Business Email Compromise (BEC) has emerged as one of the most sophisticated forms of attack, characterized by the impersonation of high-level executives or trusted parties in an organization's email communications to manipulate employees into transferring funds or divulging confidential information. Other prevalent types of digital fraud include phishing—where attackers deceive victims into revealing credentials or financial data through counterfeit emails or websites—and vishing, which relies on telephone-based strategies to elicit sensitive information under false pretenses. These various forms of cyber-enabled fraud often share an essential mechanism: social engineering, which leverages human psychology to bypass technical security measures by tricking individuals into performing actions or sharing information.

Recent global statistics underscore the scope and severity of BEC (Europol, 2024). According to the Federal Bureau of Investigation (FBI), BEC scams were responsible for a significant portion of total reported cybercrime losses in 2022, with annual damages reaching several billion dollars worldwide (Federal Bureau of Investigation, 2023). Europol's Internet Organised Crime Threat Assessment has likewise highlighted BEC as an especially insidious threat due to its reliance on interpersonal trust and organizational knowledge, which can significantly complicate detection and response efforts (Europol, 2024). In Italy, the Clusit report has documented a similar upward trend in cybercrime, noting a steady increase in fraud attempts that target business communication channels (Clusit – Associazione Italiana per la Sicurezza Informatica, 2025). Similar concerns are echoed in the literature, with scholars stressing the operational sophistication of these attacks (Al-Musib et al., 2023; Goenka et al., 2024). These findings emphasize that BEC is not merely a localized or industry-specific threat; rather, it is an evolving global phenomenon that demands attention from both private entities and governmental bodies.

The economic and legal repercussions of BEC and other digital frauds extend well beyond immediate financial losses. Organizations victimized by BEC often suffer secondary effects such as reputational damage, reduced shareholder confidence, and disrupted business processes. On the legal front, the cross-border nature of these scams raises substantial jurisdictional challenges, as funds are frequently channeled through multiple international accounts before reaching the perpetrators. This complexity can result in delays and obstacles in asset tracing and recovery, while also complicating the pursuit of legal remedies. Data protection laws, consumer protection regulations, and contractual obligations further intertwine with the investigation and prosecution of such offenses, highlighting the need for a multi-faceted approach that spans forensic accounting, legal expertise, and cyber incident response.

Central to the concept of BEC is “communicative infiltration”, the notion that attackers skillfully infiltrate the normal flow of organizational communication to manipulate recipients who may not suspect any irregularity. This infiltration is typically achieved through deceptive emails that closely mirror legitimate corporate styles and formats, thus lowering the recipient’s guard. Coupled with social engineering, wherein adversaries exploit psychological triggers such as urgency, authority, or empathy, this tactic can lead well-intentioned employees to inadvertently participate in fraudulent transactions. The dual strategy of communication infiltration and social engineering not only undermines the trust-dependent nature of business processes but also exposes inherent vulnerabilities in corporate cultures that prioritize rapid responses to executive directives. As the threat landscape continues to evolve, companies and legal authorities alike face the challenge of implementing more robust authentication protocols, awareness training, and international legislative cooperation to curtail the increasingly pernicious impacts of BEC and related digital fraud schemes.

3. Operational Mechanics of BEC Scams

BEC frauds rely on the ability of fraudsters to infiltrate corporate communication systems and manipulate information to their advantage. The attack mechanism unfolds in several stages, characterised by a sophisticated combination of social engineering techniques and advanced technological tools. The attack starts with unauthorised access to a company email account. The criminals can obtain the credentials through phishing techniques, malware or brute force attacks. Once access has been gained, the fraudster carefully analyses the correspondence between the parties involved in financial transactions to understand the operational dynamics and internal communication patterns (Cross, Gillett, 2020).

In some cases, it is not necessary to compromise the target's account directly: it may be enough to spoof email addresses to make the sender's identity appear credible. This allows fraudsters to join the communication flow without arousing suspicion. Once they have gained access to the communication, the criminal carefully monitors the emails exchanged between administrative departments or between the company and its suppliers/customers. The aim is to identify the key moments when payments are authorised and to determine how payment instructions are issued. Fraudsters may wait weeks or even months before taking action to gather enough information to organise the fraud as effectively as possible. During this observation period, the criminal may also send test emails to gauge the recipients' reactions and find out if there are any verification procedures in the payment processes.

When the criminal sees a suitable moment, they modify existing communication or create fake communication, assuming the identity of one of the parties involved. Usually, the fraudster pretends to be a company supplier and sends an email containing new payment instructions,

indicating a different bank account than the original one. To make the request appear more legitimate, the language is often adapted to the victim's language, and the style and tone of the authentic e-mail are reproduced. In addition, the fraudsters may attach forged company signatures or forged documents to strengthen the credibility of the request.

If the victim does not recognise the scam and follows the new instructions, the payment will be made and the funds will be transferred to a bank account controlled by the fraudster. These accounts are often located in countries with less strict money laundering regulations, making it difficult to recover the misappropriated funds. After receiving the money, fraudsters quickly move it between different bank accounts, using layering techniques to hide its origin. In many cases, the funds are converted into cryptocurrencies or withdrawn in cash, making it almost impossible to trace and return them to the victim (Bakarich, Baranek, 2020). The fraud is usually detected when the actual beneficiary of the payment – the original supplier – demands the agreed payment, indicating that they have not received the money. At this point, the defrauded company realises their mistake and tries to stop the payment or recover the funds through banking and judicial authorities. However, time works in the criminal's favour: once the money has been transferred and settled through a network of accounts and transactions, it is extremely difficult for financial authorities to intervene effectively. This highlights the importance of implementing effective security systems and strict verification procedures to prevent the risk of BEC fraud (Susanti et al., 2023).

4. Case Study Analysis: Infiltration and Money Laundering Techniques

The case analysed here is a paradigmatic example of Business Email Compromise (BEC) fraud, which highlights certain weaknesses in corporate payment processes and critical regulatory issues in the recovery of misappropriated funds. The case involved a European multinational industrial company that, as a result of fraudulent manipulation of its electronic communications, made payments of several hundred thousand euros to a bank account in the name of a Polish front company set up for money laundering purposes.

The attack used a repetitive and well-established transaction, which facilitated the fraud. Company A, operating in the high-tech industry, periodically purchased spare parts for high-value machinery from its regular supplier, company B. The continuous use of these machines required regular purchases. The continuous use of these machines required regular replacement of components, with large payments every six months. This predictability in financial flows was exploited by fraudsters who analysed the communication between the two companies, identifying the purchase cycle in order to infiltrate the transactions. By manipulating the exchange of emails between the parties, they were able to change the payment instructions, causing the funds to flow into a fraudulent account.

The scam consisted of several stages. After determining the exact time when Company A was to make the transfer, the fraudsters sent a seemingly authentic email with the new bank details. Convinced of the legitimacy of the request, the financial directors of company A authorised the transfer by paying the amount into an account controlled by the fraudsters and held in the name of a fictitious Polish company. The money was immediately transferred through a network of intermediary accounts, using offshore banks and institutions with less stringent control regulations, which made it much more difficult to recover the embezzled amounts.

Analysis of this episode shows how the predictability of financial transactions and the lack of cross-checking of payment details can become critical weaknesses. This case highlights the importance of stronger security protocols, including independent verification of bank details changes, multi-factor authentication and tools to detect anomalies in financial flows. Only a preventive and integrated approach can reduce the risk of BEC fraud, preventing companies with established payment processes from becoming the main targets of cybercriminals.

An investigation by the Polish Regional Prosecutor's Office revealed a complex financial structure involving several legal entities, resulting in the embezzlement of a total of more than 2.1 million euros. The fraud was based on a multi-layered money laundering model with three main stages: (1) setting up front companies through letterbox companies, (2) layering and transferring funds (layering), and (3) transforming into assets that are difficult to trace. The fraudsters took over inactive companies and changed their ownership structure using fictitious letters of credit, which allowed them to open company bank accounts without immediately attracting the attention of financial regulators. After receiving the money, the criminals set up multiple transactions between different bank accounts, splitting the amounts in order to avoid the banks' automatic monitoring systems (smurfing technique). Within 48 hours, funds were transferred between different jurisdictions, taking advantage of less strict banking regulations, while some amounts were converted into cryptocurrencies or withdrawn in cash via anonymous credit cards issued by foreign financial institutions.

From a legal point of view, the preventive seizure of funds triggered interpretative doubts regarding their distribution, and several victims filed competing claims. An international industrial company contested the claim of another defrauded company, which demanded a full refund of the seized funds, arguing that they originated exclusively from its own transaction and should not be distributed among several injured parties. The dispute became complicated due to the transnational nature of the fraud and differences in banking and criminal law, in particular with regard to the legal qualification of frozen funds and their return in accordance with the principle of priority of the original creditor (Wawrzyniak, 2024; Gwoździewicz, Tomaszycki, 2017).

The investigation was initiated by a Polish banking institution that received a SWIFT warning about a fraudulent transfer. The bank cooperated with the authorities, repeatedly providing information on the accounts involved in the fraud. Among the identified accounts, the most significant was the alpha account, in the name of a front company, to which an international industrial company made a payment. This account was blocked by BNP Paribas and then by the public prosecutor's office, freezing the final balance of several million euros.

An analysis of the transactions revealed that the money was quickly redirected through multiple transactions before it was frozen, in order to make it more difficult to trace the money and facilitate money laundering. The account received funds from another company and was then emptied through foreign transfers to accounts in the name of unknown entities. However, a few days later, another transfer from an international industrial company restored the positive balance, which was then completely frozen by the bank and the prosecutor's office.

From a legal point of view, the main dispute concerned the claim made by the second defrauded company, which demanded the entire frozen amount. This company claimed that the accounts involved were managed by a single criminal organisation and that the seized funds should be used primarily for its own compensation. However, thanks to timely bank-based freezing, the funds of the multinational industrial company did not mix with the funds of other defrauded companies, thus preventing them from being categorised as separate criminal assets.

This circumstance allowed the international corporation to more forcefully demand full reimbursement of the seized amounts, without having to compete with other victims in the process of recovering the illegally embezzled funds.

5. Legal framework of BEC fraud in Polish criminal law

From the perspective of Polish law, BEC (Business Email Compromise) fraud generally involves a number of related crimes, including fraud, document forgery, money laundering and, in some cases, unauthorised access to computer systems. Their legal configuration is based on several provisions of the Polish Penal Code, which regulate criminal behaviour typical of these fraudulent schemes.

The main offence is fraud (Article 286 of the Polish Penal Code), which punishes anyone who, for the purpose of financial gain, misleads a person or exploits their weakness to induce them to take actions resulting in economic loss. The penalty is between six months and eight years imprisonment, depending on the severity of the damage caused.

In addition to fraud, the BEC structure often involves document forgery (Section 270), which punishes anyone who alters or uses forged documents with the intention of passing them off as genuine with up to five years' imprisonment. In cases where the forgery also involves public officials or specialists authorised to certify documents, the offence of false certification

(Article 271) may be committed, punishable by imprisonment for a period of three months to eight years in the event of financial gain resulting from the offence. This offence is punishable by imprisonment for a period of six months to ten years, with the penalties being more severe if the person in question acts in cooperation with others or obtains a particularly significant advantage. In the case of money laundering involving financial entities such as banks or credit institutions, the regulations provide for an aggravating circumstance for those who facilitate the transfer or conversion of suspicious amounts.

BEC fraud can also involve the offence of unauthorised access to computer systems (Article 267), which applies to anyone who unlawfully obtains confidential information by breaching computer security measures. The penalties for this offence range from an administrative fine to two years' imprisonment, depending on the severity of the violation. This offence is particularly relevant when fraudsters infiltrate company mailboxes using phishing techniques or exploiting computer vulnerabilities.

Another important legal aspect is the possibility for Polish judicial authorities to order the confiscation of criminal assets (art. 299, §7), ordering the return of misappropriated funds to the victims if these funds can be clearly identified. However, in situations where the illegal amounts have been ‘mixed’ with other financial resources, these funds can be considered part of the criminal assets, which complicates their recovery.

Finally, the Polish Penal Code contains provisions on the concurrence of offences (Articles 11 and 12), according to which several frauds committed within a short period of time and for the same purpose may be treated as a single offence with enhanced severity, for which more severe penalties may be imposed. In particular, if a criminal group organises several fraudulent transfers, Polish case law tends to treat these activities as a single offence, aggravated by the continuity of the transactions.

6. Conclusions

From a corporate management perspective, preventing BEC fraud and other cyber threats relies on one key element: continuous employee training and the implementation of clear and strict security protocols. Experience shows that the human factor is the most vulnerable link in the corporate security chain, as employees, subjected to a high pace of work and intense cognitive load, are more prone to making mistakes that can be exploited by fraudsters. To limit this risk, companies must adopt structured prevention strategies, including both raising employee awareness through regular training programmes and introducing a rigorous internal vademecum for handling financial communications and sensitive information (Birla, Parwani, 2024; Ogwo-Ude, 2023).

Companies should establish strict rules of 'communication hygiene' by enforcing a two-factor confirmation system whenever a change of bank details is required for paying suppliers or sending confidential data. This mechanism, in combination with direct verification through independent channels, drastically reduces the risk of fraudulent manipulation. The creation of standardised procedures, supported by advanced technological tools, not only ensures a higher level of security, but also constitutes an effective barrier against vulnerabilities resulting from human error, thus protecting the company's financial and operational integrity (Caldarola et al., 2023).

Finally, this case suggests the need for a stricter regulatory approach, with the introduction of more stringent payment traceability standards and the harmonisation of procedures for blocking and returning illegally transferred funds, in order to mitigate the risks arising from a financial system that is increasingly vulnerable to digital fraud. Furthermore, there is a need to strengthen the control of procedures for opening corporate bank accounts, imposing stricter checks on the real ownership of companies and directors to prevent the use of fictitious entities as money laundering tools. Adopting a more proactive approach to preventing these frauds, based on cooperation between regulators, banks and businesses, is a key step towards reducing the vulnerability of the financial system to these increasingly sophisticated types of attacks (Susanti et al., 2023; Lazarus, 2025).

This research presents some inherent limitations. First, it is based on a single case study, which limits the generalizability of the findings. Furthermore, the analysis was constrained by partial access to banking and judicial data due to confidentiality and procedural limitations.

For future research, it would be valuable to conduct quantitative studies involving multiple cases of BEC fraud in diverse industries and legal contexts. Comparative legal analysis across jurisdictions would also shed light on regulatory inconsistencies and best practices. Finally, future research should explore the role of artificial intelligence in the early detection and prevention of BEC scams, including predictive modelling and anomaly detection in financial communication patterns.

References

1. Al-Musib, N.S., Al-Serhani, F.M., Humayun, M., Jhanjhi, N.Z. (2023). Business email compromise (BEC) attacks. *Materials Today: Proceedings*, *Vol. 81, Part 2*, pp. 497-503, doi: 10.1016/j.matpr.2021.03.647
2. Atlam, H.F., Oluwatimilehin, O. (2023). Business email compromise phishing detection based on machine learning: A systematic literature review. *Electronics*, *Vol. 12, Iss. 1,* p. 42, doi: 10.3390/electronics12010042

3. Bakarich, K.M., Baranek, D. (2020). Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise. *Current Issues in Auditing*, *Vol. 14, Iss. 1,* pp. A1-A9.
4. Birla, M.A., Parwani, B. (2024). Digital forensic issues in cloud accounting: A comprehensive review. *Towards Excellence*, *Vol. 16, Iss. 1*.
5. Caldarola, B., Mazzilli, D., Napolitano, L., Patelli, A., Sbardella, A. *Economic complexity and the sustainability transition: A review of data, methods, and literature*. Retrieved from: https://publications.jrc.ec.europa.eu/repository/handle/JRC137954, 29.01.2025.
6. Cross, C., Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *Vol. 27, Iss. 3*, pp. 871-884. Retrieved from: https://ideas.repec.org/a/eme/jfcpps/jfc-02-2020-0026.html, 04.05.2025.
7. Federal Bureau of Investigation. *Business Email Compromise: The $50 Billion Scam*. Retrieved from: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise, 29.01.2025.
8. Financial Times. *The Rise of AI-Powered Email Fraud: Why Companies Need to Act Fast.* Retrieved from: https://www.ft.com/content/d60fb4fb-cb85-4df7-b246-ec3d08260e6f, 29.01.2025.
9. Goenka, R., Chawla, M., Tiwari, N. (2024). A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. *International Journal of Information Security*, *Vol. 23, Iss. 2,* pp. 819-848.
10. Gwoździewicz, S., Tomaszycki, K. (2017). *Prawne i społeczne aspekty cyberbezpieczeństwa*. Warszawa: Międzynarodowy Instytut Innowacji.
11. Kanj, S., Garcia, P., Rosés, O., Pegueroles, J. (2025). A review of tactics, techniques, and procedures (TTPs) of MITRE framework for business email compromise (BEC) attacks. *IEEE Access*, *vol. 13,* pp. 50761-50776. Retrieved from: https://www.ft.com/content/d60fb4fb-cb85-4df7-b246-ec3d08260e6f, 29.01.2025.
12. Lazarus, S. *How do the cybercriminals behind business email compromise (BEC) fraud operate?* Retrieved from: https://www.lse.ac.uk/social-policy/research/Research-clusters/Mannheim/News, 04.05.2025.
13. Michalecki, D. (2023). Przestępstwa internetowe – zapobieganie i zwalczanie – obywatele bez ochrony. *Kontrola Państwowa*, *Vol. 68, Iss. 5,* p. 412.
14. Ministry of Digital Affairs of the Republic of Poland. *Oszustwa typu BEC*. Retrieved from: https://www.gov.pl/web/cyfryzacja/oszustwa-typu-bec, 04.05.2025.
15. Ogwo-Ude, O. (2023). Business Email Compromise Challenges to Medium and Large-Scale Firms in USA: An Analysis. *Open Journal of Applied Sciences*, *Vol. 13,* pp. 803-812, doi: 10.4236/ojapps.2023.136064.
16. Okumu, D., Omollo, R., Raburu, G. (2024). Human firewall simulator for enhancing security awareness against business email compromise. *Journal of Global Humanities and Social Sciences*, *Vol. 5*, doi: 10.61360/BoniGHSS242016800708

17. Puczyńska, J., Podhajski, M., Wojtasik, K., Michalak, T.P. (2024). Duże modele językowe i możliwości ich wykorzystania w terroryzmie dżihadystycznym i przestępczości. *Terrorism – Studies, Analyses, Prevention*, *Vol. 5, Iss. 5,* pp. 133-164.
18. Simpson, G., Moore, T. (2019). Empirical analysis of losses from business-email compromise. *APWG Symposium on Electronic Crime Research* (eCrime) (pp. unknown). Retrieved from: https://docs.apwg.org/ecrimeresearch/2020/85_BEC_Loss_Distribution.pdf, 04.05.2025.
19. Susanti, D., Subandi, F., Failasufa, N., Putri, W. (2023). Business email compromise (BEC) fraud and how to prevent it. *Asia Pacific Fraud Journal*, *Vol. 8,* p. 269, doi: 10.21532/apfjournal.v8i2.307
20. Wawrzyniak, P. (2024). Wybrane aspekty cyberbezpieczeństwa polskiego systemu bankowego z perspektywy bezpieczeństwa Rzeczypospolitej Polskiej. *Cybersecurity & Cybercrime*, *Vol. 1, Iss. 6 (Numer specjalny)*, pp. 1-290.