Lukáš Václavík

Doctoral student
University of Technology, Brno, Czech Republic
Faculty of Business and Management
E-mail: Lukas.Vaclavik1@vutbr.cz
Orcid: https://orcid.org/0000-0002-8551-9009

Jan Špatenka

Doctoral student
University of Technology, Brno, Czech Republic
Faculty of Business and Management
E-mail: Jan.Spatenka@vut.cz
Orcid: https://orcid.org/0000-0003-2024-2384

Kateřina Petrová, PhD

Assistant Professor
Brno University of Technology, Brno, Czech Republic
Faculty of Business and Management
E-mail: xphornungova@vutbr.cz
Orcid: https://orcid.org/0000-0002-6895-1238

RESILIENCE AGAINST BUSINESS EMAIL COMPROMISE: A CORPORATE CASE STUDY

UDC / UDK: 004.773:004.045.53]:658
JEL classification / JEL klasifikacija: M15, M41, K24, G32, D83
DOI: 10.17818/EMIP/2025/41
Professional paper / Stručni rad
Received / Primljeno: May 6, 2025 / 6. svibnja 2025.
Accepted / Prihvaćeno: August 28, 2025 / 28. kolovoza 2025.

Abstract

This paper presents a case study of a Business Email Compromise (BEC) attack and its impact on a company's operations. The research employed qualitative methods, including semi-structured interviews with corporate stakeholders and a literature review, to examine the state of organizational cybersecurity and identify lessons learned from cyber fraud incidents. The findings show that regular cybersecurity training, external email tagging, and robust internal communication protocols significantly reduce fraud risks. In particular, verification procedures for financial transactions and changes to banking details were identified as critical safeguards. The study highlights that cybersecurity is not merely a technical issue but a strategic business concern requiring a holistic, organization-wide approach. Human factor plays a pivotal role, and organizations must combine technical controls with employee awareness and management oversight. Practical

recommendations are provided to enhance resilience against BEC attacks, especially in international contexts where trust between business partners can be exploited.

Keywords: Cyber-attack, BEC, cybersecurity, social engineering, phishing, cyber fraud

1. INTRODUCTION

In an era where digital information is more accessible than ever, social engineering attacks have become a prominent threat to organizational security. These attacks, which exploit human psychology rather than technological vulnerabilities, can lead to significant breaches of confidential information, financial loss, and damage to reputation (Goel et al., 2017). This paper aims to present a case study of a manufacturing organization that experienced a sophisticated social engineering attack in the form of business email compromise (BEC). The authors seek to analyze the sequence of events of the attack, the organization's response, and the consequences in order to draw lessons and develop preventive strategies (Bamidele Benjamin et al., 2024).

The importance of understanding and mitigating the risks associated with social engineering threats cannot be overestimated, as the techniques used by cyber attackers evolve alongside technological developments. This is one of the reasons why it is important for organizations to adapt their mix of security measures accordingly (Jakobsson, 2016). Despite the fact that there are a number of studies in the scientific literature dealing with the issue of social engineering, including business email compromise (BEC), case studies devoted to a detailed analysis of specific attacks and appropriate countermeasures are still limited. This article aims to fill this research gap.

The main research question is: How can organizations increase their resilience to business email compromise (BEC) attacks by addressing both technical and human factors?

To answer this question, the study provides a detailed analysis of a real-world social engineering attack and offers insight into the attacker's methods, the vulnerabilities exploited, and the impact on the target organization. Through this analysis, the study seeks to inform and improve organizations' cybersecurity strategies, emphasizing the need for comprehensive security measures that include both technological and human elements. By analyzing the vulnerabilities exploited and effective recovery and prevention measures, the article contributes its findings to existing efforts to protect organizations from the evolving spectrum of cyber threats (Tahmasebi, 2024) and seeks to support the development of comprehensive cybersecurity strategies.

The study uses qualitative methodology, combining interviews with employees, management, and the IT security team, including analysis of internal

documents, emails, and security protocols related to the attack.

This article is structured as follows: The first part introduces the concept of social engineering, outlines its history, methods, and challenges it poses to organizations. The next part provides a description of the situation before the attack, the timeline of the attack, and the initial detection and response to the incident. The analysis then examines the organization's strategic response to the attack, including immediate measures taken to mitigate damage, the investigation process, and long-term security measures put in place. Finally, the document highlights key lessons learned from the incident, focusing on the importance of employee awareness and training, the role of security culture, and the integration of human factors into cybersecurity planning. The conclusion offers recommendations for organizations on how to strengthen their defenses against social engineering attacks, with an emphasis on proactive measures and continuous improvement of security practices.

2. LITERATURE REVIEW

2.1. Cybersecurity and Information Security

According to the international standard (ISO/IEC 27002:2022, 2022), information security involves implementing an appropriate set of controls – including policies, rules, processes, procedures, organizational structures, as well as software and hardware functions – to achieve the organization’s specific business objectives. Cybersecurity, as defined in (ISO/IEC 27032:2023, 2023), refers to safeguarding of people, society, organizations and nations from cyber risks. Based on these definitions, cybersecurity can be considered as a subset of information security, focusing specifically on protecting assets and information systems from cyber risks within the broader context of safeguarding information, systems, and processes.

In addition to ISO/IEC standards, frameworks and guidelines developed by the National Institute of Standards and Technology (NIST) in the United States, particularly the NIST Special Publication 1800 series (NIST Technical Series Publication List: SP1800, 2022) provide practical guidance for implementing cybersecurity measures. Together, the ISO/IEC 27000 family and NIST SP 1800 series represent internationally recognized standards for managing and improving cybersecurity practices.

2.2. Cybersecurity and Information Security in Organizations

In the context of the digital era, cybersecurity and information security have become critical components of organizational resilience against cyber threats. An effective cybersecurity strategy involves not only technical defenses (e.g. intrusion detection systems, firewalls, encryption), but also organizational,

procedural, and human-centric measures. Cybersecurity activities should no longer be perceived as the exclusive responsibility of IT or security dedicated departments. Instead, cybersecurity must become and organization-wide holistic effort where every employee is playing an active role (Spremić & Šimunic, 2018).

Soomro et al. (2016) and Tang et al. (2015) emphasize that cybersecurity governance should begin at the board level, framing it as a core component of business strategy rather than treating it as a purely technical concern. The high cost of damage caused by cyber-attacks to organizations is due to the failure of the human factor, in addition to inadequate cybersecurity infrastructure. Based on analysis of cyber incident data, human error can be identified as the leading cause of cyber incidents (Georgiadou et al., 2021). Since the cybersecurity landscape is highly dynamic, cybersecurity management has become a discipline in which organizations must be prepared to respond operationally to unplanned and evolving threats (Limba et al., 2017). Although there is growing awareness of the financial implications of cyber incidents for organizations, existing cost estimates are likely to significantly underestimate the true overall impact (Romanosky, 2016).

2.3. Social Engineering Attack

Social engineering attacks represent a sophisticated spectrum of cyber threats that target the least predictable element of security systems, namely human psychology and inattention. Gupta et al. (2016) describes phishing as a combination of social engineering and technical tactics aimed at persuading users to hand over their personal data. Unlike traditional cyber-attacks, which target software and hardware vulnerabilities, social engineering attacks focus on manipulating individuals into revealing confidential information, granting unauthorized access, or performing actions that compromise security (Hadnagy, 2018). These attacks are based on the attacker's understanding of human behavior and use techniques of deception, abuse of trust, and manipulation.

Phishing, one of the most widespread forms of social engineering, involves sending fraudulent messages that attempt to evoke a sense of legitimacy or reputation of the source, often via email, with the aim of persuading individuals to provide sensitive data (Mitnick et al., 2002). Spear phishing, a more targeted version, personalizes attacks on specific victims, increasing the likelihood of success. Vishing (voice phishing) and smishing (SMS phishing) expand the arsenal, using phone calls and text messages, respectively, to elicit valuable information directly from the target (Granger, 2001). According to Khonji et al. (2013), phishing mitigation techniques include detection, offensive defense, correction, and prevention. We believe it is essential to clarify where phishing detection techniques fit within the broader mitigation process.

Another common tactic is pretexting, where the attacker fabricates scenarios or assumes roles to obtain information under pretenses. This could involve impersonating co-workers, police, bank officials, or any authority figure

trusted by the victim (Stajano & Wilson, 2011). These attacks seek to deceive individuals or organizations into taking actions that benefit the attackers or into disclosing sensitive information, such as social security numbers, health records, or passwords (Salahdine & Kaabouch, 2019). Tailgating and baiting are physical variants, with the former involving following someone into a restricted area without proper authentication, and the latter offering a physical reward, like a USB drive labeled "Confidential," left in a place where the target will find and use it, unwittingly compromising their system.

The effectiveness of social engineering lies in exploiting human instincts and social behaviors, such as the desire to be helpful, fear of trouble, or the tendency to trust authority figures (Hadnagy, 2018). Attackers thoroughly research their targets and often use information available on social platforms or other publicly available sources to create convincing and manipulative narratives.

Defense against social engineering attacks requires an emphasis on both technological solutions, such as spam filters and secure authentication processes, and the human factor. Increasing employee resilience involves conducting regular training and awareness programs (Mitnick et al., 2002) with the aim of promoting a culture of security, suspicion, and skepticism among users.

Social engineering attacks reinforce the need for comprehensive cybersecurity strategies that address not only the technological aspects but also the human elements of the information security domain. As attackers continually refine their methods, the need for ongoing education and vigilance remains paramount in mitigating the risks associated with these tactics.

2.4. Business Email Compromise

Business email compromise (BEC) attacks are a sophisticated type of cyber fraud that primarily targets organizations that conduct banking transactions and have business partners abroad. Attackers may pose as senior executives of the organization or international suppliers in order to illegally and unlawfully obtain funds or sensitive information from unsuspecting employees (FBI, 2019). BEC scams are carefully crafted to appear completely legitimate and often exploit compromised senior management email accounts or use domain spoofing techniques to mimic business partner accounts (Hadnagy, 2018).

The essence of BEC fraud is the manipulation of human psychology, whereby attackers conduct extensive analysis of their targets to understand the organizational hierarchy, financial operations, and relationships between business partners in order to create convincing fraudulent communications (APWG, 2020). The fraud itself takes place via email communication, the aim of which is to build trust between the parties without raising doubts about the legitimacy of the request or demand for a subsequent financial transaction.

The primary types of BEC include fake invoice schemes, CEO fraud,

attorney impersonation, and data theft. Fake invoice schemes involve the impersonation of suppliers requesting fund transfers for payments to a fraudulent account. CEO fraud targets employees with the authority to make transfers, with emails appearing to come from the CEO or another top executive requesting urgent wire transfers. Attorney impersonation scams often involve requests for secretive or urgent transactions purportedly needed for legal reasons. Data theft focuses on obtaining confidential information that can be used for further attacks or identity theft (SANS Institute, 2016).

Based on a report by the Internet Crime Complaint Center (IC3), which is part of the FBI's cybercrime investigation division, in 2023 this organization recorded more than 21,000 reports of Business Email Compromise in its reporting effort. Estimated losses from this type of fraud were over 2.9 billion USD (FBI, 2023). In its report, company IBM confirms that phishing is widely used by cybercriminals, and according to the IBM Cost of a Data Breach report, phishing is the most common vector of data breaches and accounts for 15% of their total number. Based on their data, phishing breaches cost organizations an average of $4.88 million (IBM, 2024). In the following Figure 1, we can observe the development of incidents of the entire set of phishing attacks at organizations, a subset of which is the Business Email compromise fraud. In individual years, we can observe growth, especially between 2019, 2020 and 2021, where the worldwide SARS-CoV-2 pandemic had an indisputable influence on this growth (Monteith et al., 2021).

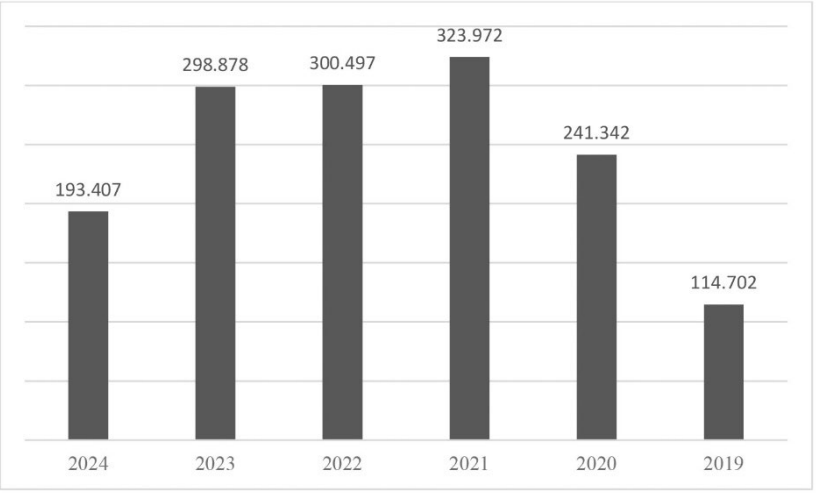

Figure 1 Phishing attacks statistics

Source: Own processing based on FBI (2023), FBI (2024).

2.5. Mitigation Strategies and Security Controls

Defending against BEC requires a combination of technical measures and employee education. Organizations are advised to implement email authentication protocols such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) to help prevent email spoofing. In addition, measures such as two-factor authentication of financial transactions or policies for verifying payment requests through alternative communication channels can help in reducing the likelihood of this threat (Krebs, 2017).

Another important aspect is regular employee training, as employees are the first line of defense. Regular training simulating phishing and BEC attacks can prepare employees to recognize and respond appropriately to suspicious emails (Angafor et al., 2024). Prevention is essential to foster an organizational culture where employees can be critical of suspicious and unusual requests, even from their managers. The common approach to ensuring security against phishing attacks in general is through updated training programs, as the techniques used by attackers are constantly improving. The rise of generative artificial intelligence plays undoubtedly an important role and may contribute to the development of even more sophisticated attack techniques in the future (Loh et al., 2024).

3. METHODOLOGY AND DATA COLLECTION

The qualitative part of the research was conducted in the form of interviews within the organization analyzed to assess the current situation in the field of cybersecurity. The findings contributed to defining lessons learned from cyber fraud incidents.

The collected qualitative data serves as an effective tool for revealing the depth of human experiences, emotions, and interactions within the organization. This methodology emphasizes the importance of context and allows researchers to delve deeper into more complex phenomena.

As Creswell (2013) outlines, qualitative research seeks to interpret phenomena in terms of the meanings that people attach to them. In doing so, it emphasizes subjective truth over objective facts. This approach is particularly valuable in the social sciences, where understanding the nuances of human behavior and social interactions is key. Inductive reasoning plays a key role in qualitative research, which involves research and data analysis without predefined hypotheses. Through iterative data processing, the researcher identifies patterns and themes based on information obtained from its participants. This process not only increases the authenticity of the research but also contributes to the development of a richer theoretical understanding of the phenomena under study.

This study used semi-structured interviews as the primary qualitative research tool, valued for its flexibility and depth. This method combines a predetermined set of open-ended questions with the further exploration possibility

of specific topics or answers. This approach facilitates a comprehensive understanding of the respondent's perspective and allows the researcher to steer the conversation toward areas of interest to the research objective while maintaining flexibility given the dynamic nature of the interaction (Kvale, 2007). According to Bryman (2012), semi-structured interviews are suitable for allowing respondents to discuss their answers more in depth, which can reveal connections and insights that strictly structured interviews might not reveal.

Secondary data was collected through a systematic review of relevant scientific publications focusing on aspects of cyber and information security, particularly strategies and methodologies used to mitigate cyber risks. The scope of the literature included discussions of critical factors influencing user awareness and their ability to withstand cyber-attacks, as well as case studies describing the experiences of organizations after cyber-attacks in professional journals over a five-year period from 2018 to 2024.

The main research question is: How can organizations increase their resilience to Business Email Compromise (BEC) attacks by addressing both technical and human factors?

To achieve this research goal, semi-structured interviews were conducted in the fall of 2024 with 13 key stakeholders in the analyzed manufacturing organization. The participants included IT security personnel, members of management, and accounting staff in order to identify lessons learned after a business email compromise attack. These interviews were designed to explore the company’s preparation for and response to the BEC attack. The insights gained from the interviews enhance the understanding of organizational vulnerabilities and support the refinement of strategies for the future prevention and mitigation of such cybersecurity threats. The findings contribute significantly to identifying lessons learned from Business Email Compromise (BEC) incidents.

4. CASE STUDY

4.1. Organizational profile

The analyzed organization is localized within the Czech Republic in the sector of high-tech instrumentation, which is used for research in various primarily scientific fields or specialized high-tech production. The production of scientific equipment and instruments is localized in the Czech Republic, and the manufactured equipment is exported worldwide through an extensive network of distribution partners, who gain a unique representation for the country or region. The company exports 95% of its production abroad to its customers. The company has a turnover of CZK 2.5 billion and employs over 650 people. In addition to the production itself, its activities include servicing purchased instrumentation and systems. In addition to the service and production departments, the company also has a sales and product and software development department. The present paper

focuses on the analysis of this organization, which was hit by a social engineering attack, specifically a type of business email compromise that targeted and attacked the trust between the organization and one of its distributors.

4.2. The Organization's Approach to Safety and Prevention

The analyzed organization employs IT specialists primarily for the development of supporting software systems for interaction and control of instruments, work with measured data, and their further analysis, which contributes to the organization's revenue. The organization has a team of 20 employees responsible for this R&D area. The operations of the organization, including cybersecurity, are handled by the IT department, which, apart from cybersecurity, covers day-to-day operations such as system administration (CRM, ERP, etc.), employee support, and configuration of network infrastructure and workstations. This team consists of 5 employees and is responsible for the IT operation of the entire organization.

Operational data are stored on dedicated on-premises data storage facilities due to their sensitivity and volume; third-party cloud services are not used for processing or storage.

The security measures in place were identified through interviews with relevant employees. According to the interviews, regular employee training is not conducted, although the benefits are recognized. Instead, employees receive regular messages warning about different types of cyber threats.

As a precautionary measure, employees are required to change their passwords regularly, and passwords must meet complexity and entropy requirements.

The organization records various types of attacks targeting its assets. Monitoring systems and implemented measures aim to protect the organization from attackers breaching infrastructure or stealing sensitive data, including know-how. Attempts by attackers to exploit infrastructure vulnerabilities are managed through patch management and regular system updates.

Among the attacks, some target the human factor, including social engineering attempts. Within the last ten years, the organization has experienced two successful Business Email Compromise (BEC) attacks.

4.3. Business Communication Procedure Between Distributor and Manufacturer

Communication between the parties usually occurs as follows: the distributor, based on an order from an end customer in its area of operation, sends the order − including device or system specifications − to the analyzed

organization. The organization, based on this order, creates a production request in its ERP system. Following this request, the device is put into production, and the organization informs the distributor of the final price for the goods and services ordered, including the expected delivery date.

Subsequently, the shipping method and other financing conditions are negotiated. Once the product is manufactured, the organization requests payment from the distributor for the ordered goods. The distributor then collects payment from the end customer and reimburses the organization accordingly. The organization sends the ordered and paid-for goods either to the distributor or directly to the end customer, based on prior agreement.

The relationship between the distributor and the organization is generally based on trust due to long-term cooperation and ongoing collaboration, although risks exist for all parties.

4.4. Course in Attacks

Both attacks followed a similar course. Due to the distributor network, the attackers focused on the communication channels between the distributors and the analyzed organization. Although the attack itself cannot be classified as a supply chain attack, it nevertheless shares certain similarities with such attacks.

4.5. Case No. 1

In 2017, routine communication was ongoing between the organization's distributor partner covering the Singapore area. The end customer placed an order for instrumentation through the distributor. The manufacturing organization accepted the order, and the counterparties agreed on the delivery method to the end customer, including the arrangement of the final price and delivery date. Once the goods were ready, the organization contacted the distributor to inform them and enclosed an invoice for payment.

During the production period, however, the distributor's email account was compromised by an attacker. By exploiting a password vulnerability due to low complexity and weak security practices, the attacker gained access to all of the distributor's email communications, as multi-factor authentication or other protective measures were not in place. This allowed the attacker to obtain a complete overview of ongoing correspondence and current business activities.

When an email from the organization arrived with an attached invoice, the attacker deleted it from the distributor’s inbox to prevent the distributor from seeing it. The attacker then created a fake email account mimicking the organization's domain, differing by only a single character, and replicated the account of the person the distributor normally communicated with. Although the original email was deleted, the attacker retained its text, including the invoice, but modified the

payment details to redirect funds to a bank account in Warsaw. To maintain credibility, the attacker preserved the full previous thread of communication.

Aware of the risk that the distributor might attempt verification, the attacker also attached a fraudulent statement of bank account change to the invoice, including the signature of the organization's CEO. The signature was later discovered to have been extracted from the organization's publicly available annual report. Due to the distributor's long-standing trust in the organization, no suspicion was raised regarding the authenticity of the communication.

The attacker then pressured the distributor to transfer the requested funds promptly to enable shipment of the goods. Communication with the organization was delayed because the attacker continued to control the distributor's email account and deleted incoming messages. Consequently, the distributor transferred the payment to the attacker's account in Warsaw, and the funds were promptly withdrawn.

After noticing the unusual delay in payment, the organization contacted the distributor, who confirmed the payment. Upon reviewing the organization's bank account, both parties discovered that fraudulent activity had occurred. Following negotiations, the organization offered a small discount on the goods provided, but the distributor, being responsible for the incident, had to cover the damage incurred.

4.6. Case No. 2

In 2023, a specialized university unit located in Europe placed an order for instrumentation from the organization analyzed based on a previous tender. The financing of the instrumentation was carried out in phases according to the source of funding, provided as subsidies from European funds. An email thread was established between the university and the manufacturing organization based on these payments.

After all refinement discussions, the matter reached the point of making the actual payment. On March 16, the payment method was agreed upon between the relevant departments of both parties, and an invoice with payment details was sent for the transaction, scheduled for Friday, March 24.

Shortly thereafter, on March 22, the university was contacted by an individual claiming to represent another department of the manufacturing organization. This person referred to the contacts involved in the initial communication and signed the email as "Chief Office Manager," pointing out an error in the original invoice. A corrected invoice with an apology and a new account number was attached, allegedly reflecting a recent change in the organization's bank details. However, the individuals mentioned in the email were not copied on the message, which did not raise any suspicion on the part of the university at the time.

On Monday, March 29, the organization did not receive the funds and contacted the university to request payment. The university responded that the payment had already been made and attached the original conversation with the attacker. The university immediately reported the incident to its banking institution, which was able to stop the flow of funds in cooperation with the Slovenian National Bank.

Further investigation revealed that the fraudulent message had been sent from a domain closely resembling the organization's original domain, employing typo squatting (also known as URL hijacking). It was also discovered that the attacker's account listed on the altered invoice was with a Chinese bank operating in England. However, the account owner could not be traced.

4.7. Other Cases

In addition to the above-mentioned cases, the organization has observed an increasing trend of attempts to carry out similar types of attacks, particularly since 2017, when it was acquired by a large investor. There have been frequent attempts to pressure accounting personnel, sometimes impersonating the CEO of the organization, to pay invoices or to disclose lists of invoices. The organization has also recorded numerous phishing attacks targeting employees across all departments.

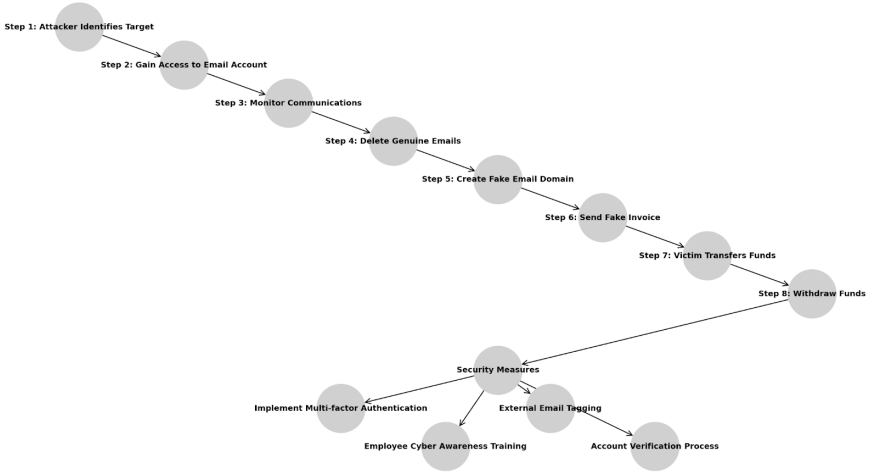

Figure 2 Structured cyber-attack Flowchart and security measures

Source: Own Processing.

4.8. Key Vulnerabilities

The analysis identified several vulnerabilities in the organization's cybersecurity posture, including a lack of multi-factor authentication for external email communications and insufficient employee training. The attack exploited the trust between the organization and its distributors, manipulating the email communication process to divert financial transactions to fraudulent accounts.

4.9. Lessons Learned

Based on these experiences, the organization has made several changes to its internal processes to prevent the recurrence of similar incidents. After the attack, the organization implemented several key measures:

First, among the main measures taken since the initial attack was training the entire distribution network on the practices employed by attackers, including the introduction of a reporting process in case a similar situation occurs in the future cooperation.

Second, the organization implemented external email tagging, whereby any sender not on the trusted list is flagged as suspicious. While such an email may not necessarily be malicious, it provides the recipient with a signal to be vigilant and verify the legitimacy of the other party. This system also creates a need to verify the authenticity of the sender before initiating financial transactions.

Third, the organization has implemented regular training for accountants and key financial staff to recognize suspicious signs in email communications, with a focus on detecting phishing attempts and BEC scams. Accountants are also trained to respond immediately when such an attack is suspected.

Finally, the organization has informed its distributors that any changes to bank accounts will be officially notified to the organization and amended in the form of a mutually agreed contractual amendment. It will therefore not be possible to change them solely through ordinary email communication. This information is also included on all invoices issued. Similarly, suppliers are required to provide a bank account statement indicating their own account for payments.

5. DISCUSSION

The study's findings validate the key role of the human factor in cybersecurity. While technological solutions (multi-factor authentication, external email labeling) are an essential part of security, human awareness and behavior are equally important (Arbanas et al., 2021). Cybercriminals often exploit trust, time pressure, and coercion to trick employees into bypassing security protocols, as confirmed by Angafor et al. (2024).

Based on lessons learned from incidents, organizations can adopt security

strategies to raise awareness and strengthen their defenses against cyberattacks and fraud. One important milestone is to conduct comprehensive training for accountants and other staff on cyber fraud practices in accordance with Abdulla et al. (2023) and standards such as ISO/IEC 27002:2005 (2005). By learning about common attack tactics such as phishing and BEC, accountants will be better equipped to recognize warning signs early on. Training should include instructions on verifying the legitimacy of email senders, such as checking domain information, viewing unusual attachments, and questioning requests for urgent suspicious activities (e.g., making or verifying a payment). Accountants must also be trained to immediately report suspicious activity through designated processes and channels, enabling a rapid response to prevent or mitigate damage. (Sakib et al., 2023) similarly identified human error as a primary factor in the spread of ransomware and emphasized the importance of user support and training.

Another appropriate measure is the introduction of external email flagging. Emails from unknown senders are flagged as potentially suspicious, even if they do not appear to be obviously malicious based on their content. This system provides an additional layer of protection by alerting the recipient to verify the legitimacy of the sender or mark the email as spam before taking any action (Gangavarapu et al., 2020). Advanced approaches may also use NLP-based phishing detection techniques (Egozi and Verma, 2018) or machine learning methods to identify fraudulent emails (Abdulnabi et al., 2024). Accountants, as the direct point of contact for financial transactions, can benefit from these tools in detecting and preventing fraudulent emails that might otherwise be mistaken for legitimate communications. Combining these technological measures with regular training increases vigilance when handling sensitive financial information and flows.

In addition, organizations should establish clear communication protocols regarding changes to financial accounts, both with customers and suppliers. Both parties must be aware that any change in bank account details will be communicated through official channels, and this process should be reflected in all invoices and contracts to increase awareness and transparency. Requiring suppliers to provide bank account statements and mandating formal contract amendments for any changes ensures that all financial transactions remain secure and verifiable. When consistently applied, these proactive measures can significantly reduce the likelihood of successful cyberattacks targeting financial processes (AL-Hawamleh, 2023).

Although the organization has implemented several important measures, these steps represent a necessary foundation for further development in the area of cyber and information security. Findings from Nisha et al. (2021) suggest that additional steps, such as regular security audits, advanced email filtering, user behavior analysis, and formal cyber incident response planning, reduce vulnerability and improve organizational resilience. In addition, in line with the guidelines NIST Technical Series Publication List: SP1800 (2022), organizations are encouraged to implement user activity analysis and system logging to detect anomalies, monitor potential threats, and assist in subsequent incident investigations.

The integration of these additional protective measures could complement existing procedures, address potential gaps in current cybersecurity, and mitigate risks that may arise as a result of evolving social engineering and sophisticated BEC threats.

Overall, the results confirm that responsibility for cybersecurity in modern commercial organizations is no longer the sole domain of IT departments, but rather involves organizations at all levels, including management.

The study's findings are consistent with existing literature on social engineering attacks, highlighting the manipulation of trust and the exploitation of human psychology (Del Pozo et al., 2018) or (Siddiqi et al., 2022). Previous studies have emphasized the importance of employee training in cyber fraud prevention, and this study expands on these findings with specific recommendations, not only for accounting departments.

6. CONCLUSION

This study highlights the key role of human factors in cyber and information security, particularly in accounting departments, where employees are the primary target of business email compromise (BEC) attacks. While technical measures such as email flagging and multi-factor authentication provide essential protection, the incidents analyzed suggest that human behavior and awareness are a significant link in fraud prevention.

The findings also confirm that organizations should incorporate ongoing training programs focused on recognizing phishing attempts, verifying financial requests, and immediately reporting suspicious activity. Complementary technical solutions, such as advanced email filtering and anomaly detection, can further strengthen these efforts.

By documenting a real-world BEC attack in a Central European context, this study provides empirically grounded insights into technical and organizational measures that are underrepresented in the current literature. It emphasizes the importance of integrating cybersecurity responsibilities at all organizational levels, incorporating security awareness into daily operations, and establishing clear communication and verification protocols for financial transactions.

The limitations of this study may be its focus on a single company and the limited number of incidents, which may restrict the generalizability of the findings to any organization.

Future research should examine a broader range of organizations and contexts, allowing for a more comprehensive understanding of the effectiveness of both technical and behavioral cybersecurity measures.

Future research should also explore not only technical safeguards but also organizational culture and behavioral strategies that strengthen resilience against evolving social engineering threats.

Author Contributions: Conceptualization, L.V. and K.P.; Methodology, J.S.; Software, L.V.; Validation, L.V. and J.S. Analysis, J.S.; Investigation, X.X.; Resources, J.S. and L.V.; Data Curation, K.P.; Writing – Original Draft Preparation, J.S.; Writing – Review & Editing, L.V.; Visualization, J.S.; Supervision, K.P.; Project Administration, J.S.; Funding Acquisition, J.S.

Funding: The research was funded by Brno University of Technology junior specific internal grant no. FP-J-23-8224, FP-J-24-8504 and FP-S-25-8736.

Conflict of Interest: The authors declare no conflict of interest.

Acknowledgements: The authors would like to express their gratitude to all company respondents for their willingness to share their experience in the researched area.

REFERENCES

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of Social Engineering Awareness Among Students and Lecturers. *IEEE Access*, *11*, 101098-101111. https://doi.org/10.1109/ACCESS.2023.3311708

Abdulnabi, I., Yaseen, Q., Ablel-Rheem, D. M., Ibrahim, A. O., & Ismail, M. A. (2024). Arabic Phishing Email Detection: A Hybrid Machine Learning Based on Genetic Algorithm Feature Selection. *International journal of advanced computer science and applications*, *15* (8), 312-325. https://www.webofscience.com/wos/alldb/full-record/WOS:001312983900001; https://doi.org/10.14569/IJACSA.2024.0150832

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *14* (2), 801-809. https://doi.org/10.14569/IJACSA.2023.0140292

Angafor, G. N., Yevseyeva, I., & Maglaras, L. (2024). Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. *International Journal of Information Security*, *23* (3), 1679-1693. https://doi.org/10.1007/s10207-023-00809-5

APWG. (2020). *Phishing Activity Trends Report*. https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf; https://doi.org/ 10.1016/S1361-3723(19)30025-9

Arbanas, K., Spremic, M., & Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management*, *73* (5), 699-719. https://doi.org/10.1108/ajim-02-2021-0037

Bamidele Benjamin, L., Enoch Adegbola, A., Amajuoyi, P., Daniel Adegbola, M., & Bukola Adeusi, K. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19* (2), 134-153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Bryman, A. (2012). *Social research methods* (4th ed). Oxford University Press.

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (Third). SAGE Publications.

Del Pozo, I., Iturralde, M., & Restrepo, F. (2018). Social Engineering: Application of Psychology to Information Security. *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 108-114. https://doi.org/10.1109/W-FiCloud.2018.00023

Egozi, G., & Verma, R. (2018). Phishing Email Detection Using Robust NLP Techniques. *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, 7-12. https://doi.org/10.1109/ICDMW.2018.00009

FBI (2019). *Business Email Compromise The $26 Billion Scam*. Federal Bureau of Investigation. Retrieved October 24, 2024, from https://www.ic3.gov/PSA/2019/PSA190910

FBI (2023). *Internet Crime Report*. IC3. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53* (7), 5019-5081. https://doi.org/10.1007/s10462-020-09814-9

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35* (2), 486-505. https://doi.org/10.1057/s41284-021-00286-2

Goel, S., Williams, K., Dincelli, E., & (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, *18* (1), 22-44. https://doi.org/10.17705/1jais.00447

Granger, S. (2001). *Social engineering fundamentals, part I: hacker tactics*. Symantec Connect Community. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4182f6b99e9ca2efe6d3f3e9f3fd59ded36333dd

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537-540. https://doi.org/10.1109/CCAA.2016.7813778

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (Second). Wiley. https://doi.org/10.1002/9781119433729

IBM (2024). *What is phishing?*. https://www.ibm.com/topics/phishing

ISO/IEC 27002:2005. (2005). ISO copyright office.

ISO/IEC 27002:2022. (2022). Information security, cybersecurity and privacy protection – Information security controls. International Organization for Standardization.

ISO/IEC 27032:2023. (2023). Cybersecurity – Guidelines for Internet security. International Organization for Standardization.

Jakobsson, M. (2016). Case Study: Business Email Compromise. *Understanding Social Engineering Based Scams*, 115-122. https://doi.org/10.1007/978-1-4939-6457-4_11

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey, *15* (4), 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

Krebs, B. (2017). *The Essentials of DMARC*.

Kvale, S. (2007). *Doing Interviews. Series: The SAGE Qualitative Research Kit*. SAGE Publications. https://doi.org/10.4135/9781849208963

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4* (4), 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a Hybrid Security Framework for Phishing Awareness Education and Defense. *Future Internet*, *16* (3). https://doi.org/10.3390/fi16030086

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23* (4). https://doi.org/10.1007/s11920-021-01228-w

Nisha, T. N., Bakari, D., & Shukla, C. (2021). Business E-mail Compromise – Techniques and Countermeasures. *2021 International Conference on Advance Computing and Innovative Technologies in*

Engineering (ICACITE), 217-222. https://doi.org/10.1109/icacite51222.2021.9404587

NIST Technical Series Publication List: SP1800. (2022). https://pages.nist.gov/NIST-Tech-Pubs/SP1800.html

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Sakib, S., Raiaan, M. A. K., Fahad, N. M., Mukta, M. S. H., Al Mamun, A., & Chowdhury, S. (2023). A Review of the Evaluation of Ransomware: Human Error or Technical Failure?. *2023 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*, 393-397. https://doi.org/10.1109/ICICT4SD59951.2023.10303580

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11* (4). https://doi.org/10.3390/fi11040089

SANS Institute. (2016). *SANS 2016 State of ICS Security Survey*. SANS. https://paper.vulsee.com/icsmaster/doc/%E5%9B%BD%E5%A4%96/ICS-2016-Belden-Survey.pdf

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12* (12). https://doi.org/10.3390/app12126042

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36* (2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spremić, M., & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. *Proceedings of the World Congress on Engineering*, *1*, 341-346.

Stajano, F., & Wilson, P. (2011). Understanding scam victims. *Communications of the ACM*, *54* (3), 70-75. https://doi.org/10.1145/1897852.1897872

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. *Journal of Information Security*, *15* (2), 106-133. https://doi.org/10.4236/jis.2024.152008

Tang, M., Li, M. 'gang, & Zhang, T. (2015). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17* (2), 179-186. https://doi.org/10.1007/s10799-015-0252-2

Lukáš Václavík
Doktorand
Tehnološko sveučilište u Brnu, Češka Republika
Fakultet za poslovanje i menadžment
E-mail: Lukas.Vaclavik1@vutbr.cz
Orcid: https://orcid.org/0000-0002-8551-9009

Jan Špatenka
Doktorand
Tehnološko sveučilište u Brnu, Češka Republika
Fakultet za poslovanje i menadžment
E-mail: Jan.Spatenka@vut.cz
Orcid: https://orcid.org/0000-0003-2024-2384

Dr. sc. Kateřina Petrová
Docentica
Tehnološko sveučilište u Brnu, Češka Republika
Fakultet za poslovanje i menadžment
E-mail: xphornungova@vutbr.cz
Orcid: https://orcid.org/0000-0002-6895-1238

OTPORNOST NA KOMPROMITIRANJE POSLOVNE E-POŠTE: STUDIJA SLUČAJA KORPORACIJE

Sažetak

Ovaj rad predstavlja studiju slučaja napada kompromitiranjem poslovne e-pošte (BEC) i njegov utjecaj na poslovanje tvrtke. U istraživanju korištene su kvalitativne metode, uključujući polustrukturirane intervjue s korporativnim dionicima i pregled literature, kako bi se ispitalo stanje organizacijske kibernetičke sigurnosti i identificirale pouke iz incidenata kibernetičkih prijevara. Nalazi pokazuju da redovita obuka o kibernetičkoj sigurnosti, vanjsko označavanje e-pošte i robusni interni komunikacijski protokoli značajno smanjuju rizike od prijevare. Postupci provjere financijskih transakcija i promjene bankovnih podataka prepoznati su kao ključne zaštitne mjere. U istraživanju se naglašava da kibernetička sigurnost nije samo tehničko pitanje, već strateška poslovna briga koja zahtijeva holistički pristup na razini cijele organizacije. Ljudski faktor igra ključnu ulogu, a organizacije moraju kombinirati tehničke kontrole s osviještenošću zaposlenika i nadzorom uprave. Daju se praktične preporuke za poboljšanje otpornosti na BEC napade, posebno u međunarodnim kontekstima, gdje se povjerenje između poslovnih partnera može zloupotrijebiti.

Ključne riječi: Kibernetički napad, računovodstvo, kibernetička sigurnost, društveni inženjering, krađa identiteta, kibernetička prijevara.

JEL klasifikacija: M15, M41, K24, G32, D83.