Open Journal of Applied Sciences, 2023, 13, 803-812
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Business Email Compromise Challenges to Medium and Large-Scale Firms in USA: An Analysis

Okechukwu Ogwo-Ude[1,2]

[1]Department of Computer Information Systems, Prairie View A&M University, Prairie View, TX, USA
[2]Association for the Advancement of Artificial Intelligence, Bellevue, WA, USA
Email: okeyogwoude@gmail.com

How to cite this paper: Ogwo-Ude, O. (2023) Business Email Compromise Challenges to Medium and Large-Scale Firms in USA: An Analysis. *Open Journal of Applied Sciences*, **13**, 803-812.
https://doi.org/10.4236/ojapps.2023.136064

Received: May 9, 2023
Accepted: June 6, 2023
Published: June 9, 2023

Abstract

Business Email Compromise (BEC) attacks have emerged as a significant cybersecurity threat, leading to substantial financial losses for organizations. According to the FBI's Internet Crime Complaint Center (IC3), BEC attacks resulted in financial losses exceeding $1.8 billion in the USA in 2019 alone. Business Email Compromise (BEC) attacks have emerged as a significant cybersecurity threat, leading to substantial financial losses for organizations. According to the FBI's Internet Crime Complaint Center (IC3), BEC attacks resulted in financial losses exceeding $1.8 billion in the USA in 2019 alone. BEC attacks target a wide range of sectors. No industry is immune to these attacks, which emphasizes the need for increased vigilance across all sectors. Attackers often impersonate high-level executives or vendors to gain credibility and manipulate employees into complying with fraudulent requests. BEC attacks have a global reach, with threat actors operating from various countries, including Nigeria, Russia, China, and Eastern European nations. We will examine the unique difficulties SMEs encounter in relation to BEC attacks. This study provides a more excellent knowledge of the severity of the problem and offers ideas for efficient mitigation solutions through an investigation of attack characteristics, tactics, and impacts.

Keywords

SMEs, Vulnerability, Threat, Business Email Compromise (BEC), Email Security, Fraud

1. Introduction

Business Email Compromise (BEC) has emerged as a significant and rapidly evolving cybersecurity threat, impacting organizations of various sizes and industries globally. While much attention has been given to the challenges faced by small and medium-sized companies (SMEs) in relation to BEC attacks, the vulnerabilities and complexities experienced by medium and large-scale companies in the USA have garnered less research focus. This article aims to address this research gap by examining the specific challenges posed by BEC to medium and large-scale companies in the USA and exploring the implications for their financial stability, operational continuity, and overall cybersecurity resilience.

Medium and large-scale companies play a critical role in the US economy, often possessing substantial financial resources, extensive operational infrastructure, and a larger employee base. However, these very attributes can attract the attention of sophisticated threat actors who seek to exploit vulnerabilities within these organizations' communication channels and financial processes. The impact of successful BEC attacks on medium and large-scale companies can be severe, leading to substantial financial losses, reputational damage, and disruptions to critical business operations.

While SMEs are often targeted due to their limited cybersecurity resources and awareness, medium and large-scale companies face distinct challenges stemming from their organizational complexity, broader attack surface, and potential interconnectedness with global supply chains. The sophistication of BEC attacks targeting these companies has evolved, encompassing tactics such as spear-phishing, social engineering, domain impersonation, and compromising executive accounts to deceive employees and initiate unauthorized transactions or disclose sensitive information.

Financial losses resulting from BEC attacks on the medium and large-scale companies can reach staggering amounts, often running into millions or even billions of dollars per incident. These substantial financial impacts not only affect the bottom line but also jeopardize longterm investment strategies, shareholder confidence, and overall business viability.

Operational disruptions resulting from successful BEC attacks can cripple medium and large-scale companies, impacting supply chains, customer relationships, and internal processes. The subsequent delays in financial transactions, compromised data integrity, and operational downtime can have far-reaching consequences for the organization's competitiveness and market position.

Furthermore, medium and large-scale companies face complex legal and regulatory challenges in the aftermath of BEC attacks. Compliance with industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in healthcare or the Payment Card Industry Data Security Standard (PCI DSS) in finance, poses additional hurdles in managing the fallout from these incidents.

To address the unique challenges faced by medium and large-scale companies in the USA, this article aims to delve into the characteristics, impacts, and mitigation strategies associated with BEC attacks. By examining real-world case studies, industry reports, and relevant research, this study seeks to provide insights into the evolving nature of BEC attacks on medium and large-scale companies, highlight the potential financial and operational consequences, and offer actionable recommendations to enhance cybersecurity resilience.

The findings of this research will contribute to the existing body of knowledge on BEC and provide practical guidance for medium and large-scale companies in the USA to fortify their defenses against this pervasive threat. By understanding the specific challenges, they face and adopt appropriate risk management strategies, and these companies can better protect their financial interests, maintain operational continuity, and safeguard their reputation in an increasingly complex cybersecurity landscape.

2. Literature Review

Business Email Compromise (BEC) has emerged as a significant and evolving threat, targeting organizations of all sizes across various industries globally. While extensive research has been conducted on BEC challenges faced by larger enterprises, limited attention has been given to the specific challenges encountered by small and medium-sized companies (SMEs) in the USA. This literature review aims to provide an overview of the existing knowledge, key findings, and relevant research projects regarding BEC challenges to SMEs, while also highlighting the gaps in current research.

Several studies have explored the tactics and techniques employed by threat actors in BEC attacks. [1] revealed that BEC attacks commonly exploit human vulnerabilities through spear-phishing and social engineering, with emails designed to trick employees into disclosing sensitive information or initiating unauthorized financial transactions. Additionally, according to [2] research project on BEC highlighted the increasing use of advanced techniques such as email spoofing and compromised vendor accounts.

Financial losses resulting from BEC attacks on SMEs have been a significant concern. As stated in [3] that BEC attacks led to losses exceeding $1.8 billion in 2019 in the USA alone. Moreover, research by [4] highlighted that SMEs are particularly vulnerable to financial losses due to their limited resources and cybersecurity investments.

Operational disruptions caused by BEC attacks have also been highlighted in the literature. [5], BEC incidents can disrupt business operations, leading to loss of productivity, delays in financial transactions, and potential reputational damage. The absence of robust incident response plans and backup systems exacerbates the impact of these disruptions on SMEs.

Furthermore, legal and regulatory implications associated with BEC incidents pose challenges to SMEs. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), and reporting requirements following a breach can be particularly burdensome for SMEs. Non-compliance can result in legal consequences and significant financial penalties [5].

Despite the growing prevalence of BEC attacks on SMEs [6], there remains a gap in research specifically addressing the challenges faced by SMEs in the USA. While studies conducted in other countries provide valuable insights, the unique context of the US business landscape, regulatory environment, and specific challenges faced by American SMEs warrant a focused investigation.

In conclusion, the literature review demonstrates the vulnerabilities of SMEs to BEC attacks, including limited resources, financial losses, operational disruptions, and legal implications. The existing research provides a foundation for understanding these challenges but falls short in addressing the specific context of SMEs in the USA. This study aims to bridge this gap by conducting an in-depth analysis of the BEC challenges faced by SMEs in the USA, contributing to the knowledge base and providing practical recommendations to enhance the resilience of SMEs against BEC threats.

3. Methodology

In this research study, an online survey using Google Forms was conducted during the 2020 cybersecurity virtual meeting of the Institute of Electrical and Electronics Engineers (IEEE). The purpose of the survey was to investigate the difficulties and problems faced by technology professionals and researchers regarding Business Email Compromise (BEC) attacks in their respective organizations. The target population for the survey included university researchers, small and medium-sized enterprises (SMEs), government agencies, and technology specialists from Fortune 500 firms. The sample population consisted of practitioners in the field with varying levels of experience, ranging from senior systems administrators to lower-level IT staff members who manage security-related issues in their organizations. The participating organizations ranged in size from medium-sized to Fortune 500 companies.

The survey aimed to collect responses from experts and researchers in the field of internet security who attend the conference and publish cybersecurity research for federal agencies, colleges, and institutions. A total of 182 survey responses were received and completed, representing a representative sample of researchers and industry experts in the field of internet security. The questionnaire used in the survey consisted of 15 items. Each item utilized a Likert scale, where respondents were asked to rate their agreement or disagreement on a scale from 1 to 5, with "strongly disagree" and "strongly agree" as anchors. The Likert scale allowed participants to express their opinions on the difficulties and challenges they faced regarding BEC attacks. In addition to the Likert scale items, the questionnaire also included categorical options for respondents to answer questions related to their gender and high-level IT experience. The gender options were represented by the numbers 1 (male) and 2 (female), while the high-level IT experience question likely had a binary option, such as 1 (yes).

By using this survey methodology and collecting responses from a diverse group of technology professionals and researchers, the study aimed to gain insight into the specific difficulties and problems encountered in relation to BEC assaults in various organizations.

4. Result of Statistical Analysis

The results of the statistical analysis are shown in Table 1.

1) Survey Question 1. On a scale of 1 to 5, how secure do you believe your company's network is, according to the study? The response analysis to the survey question is displayed in Table 2. This suggests that 17% of the sample gave the answers 1 and 2, while 83% gave the answers 3, 4, and 5. It also suggests that 83 percent of the sample believed their organization was secure.

This conclusion was further supported by a test of the hypothesis (single proportion) that the population proportion of workers in the relevant industries who believe that their organizations are secure at the 5% level of significance is less than or equal to 50%. Po should represent the percentage of workers in various industries that believe they are secure. Ho (Null Hypothesis): Po 0.50 who believe their business is secure; Ha (Alternative Hypothesis): Po 0.50 who believe their business is secure. (Level of Significance) = 5%. Since 182.50 > 0 and 182.50 > 10 (or considering that the number of successes and failures are 91 and 91, respectively) are at least 10, the study can employ the Z-test statistic if $np \geq 10$ and $n(1- p) \geq 10$. This study estimates the test statistic by: $Z = P' - Po = pPo(1 - Po)/n$ Here, $P' = 0.83$ (sample proportion); $Po = 0.50$ (population proportion); $N = 182$; $Zc = 8.92$; $Zt = 1.65$ (5% level of significance) critical value = 0.05.

Our analysis rejected the null hypothesis and supported the alternative because $Zc > Zt$. The examination is important. It demonstrates that more than half (83%) of the workforce in the sector believe their organization is secure. This judgment is made in light of the sample outcome, which is a representative sample that accurately predicts the population. With a very small margin of error, sample statistics can accurately predict population parameters at point estimate or interval estimate.

Table 1. Primary Statistics: used to gather feedback directly from targeted audience.

Sample of Size (n)	182	Sample of size (n)	182
No of Women	82	No of IT-Admin	154
No of Men	100	No of Non-IT-Admin	28
Percent-age of women	45	Percentage of IT-Admin	85
Percent-age ofMen	55	Percentage of Non-IT-Admin	15

Table 2. Response analysis of Survey Question 1.

1	Never (1)	7
2	Rarely (2)	24
3	Sometimes (3)	79
4	Often (4)	52
5	Always (5)	20

2) Survey Question 2. On a scale of 1 to 5, the survey questioned participants how useful they found the network scanning technologies their company employed for threat mitigation. The response analysis to the survey question is displayed in Table 3. 15% of the sample's replies were 1, 2, and 3 totals; 85% of the sample's responses were 4 and 5.

As a result, it can be inferred that 85% of the sample believes the scanning technologies are effective at reducing threats. To further support this finding, we tested the hypothesis (single proportion) that, at the 5% level of significance, the population proportion of industry personnel who believe that scanning technologies are beneficial in minimizing dangers is less than or equal to 50%. Let Po represent the percentage of industry personnel who believe that scanning tools are helpful in reducing dangers. Ho (Null Hypothesis): $Po > 0.50$ believes that scanning tools can help reduce threats; Ha (Alternative Hypothesis): $Po > 0.50$ believes that scanning tools can help reduce threats. Here, 5% (level of Significance) is the value. If $np \geq 10$ and $n(1 - p) \geq 10$ then I can use Z-test statistic and since 182*0.50 > 0 and 182*0.50 > 10 (or considering that the number of success and failures are 91 and 91 respectively are at least 10. We calculate the test statistic by: $Z = P' - Po = pPo(1 - Po)/n$ Here, $P' = 0.85$ (sample proportion); $Po = 0.50$ (population proportion); $N = 182$; $Zc = 9.5$; $Zt = 1.65$ (5% level of significance) critical value = 0.05. Since $Zc > Zt$, we rejected the Null hypothesis (Ho) and accepted the alternate hypothesis (Ha). The test is significant. It confirms that more than 50 percent (85%) of the industries workers' population think that the scanning tools are useful in mitigating threats. This conclusion is based on the sample result (a representative sample) which is reliably predictive of the population. Sample statistics predict population parameters at point estimate or interval estimate within negligible margin of errors.

3) Survey Question 3. On a scale of 1 to 5, how frequently do your businesses perform a network security defense as you look for threats on your network, was the question posed by the study. The response analysis to the survey question is displayed in Table 4. A total of 7.7% of the sample's replies were 1 and 2, while 92.3% of the sample's responses were 3, 4, and 5.

This implies that 92.3% of the sample thinks that their organizations run a network security defensive when searching for threats on the network. To further validate this result, we conducted a test of hypothesis (single Proportion) that the population proportion of industries workers who think that their organizations run a network security defensive as they search for threats on the network at 5% level of significance is less or equal to 50% (hypothetical population proportion). Let Po be the population proportion of industries workers who think that their organizations run a network security defensive while searching the network for threats. Ho (Null Hypothesis): $Po \leq 0.50$ think that their company runs a network security defensive; Ha (Alternative Hypothesis): $Po \geq 0.50$ think that their company runs a network security defensive. Here, $\alpha = 5\%$ (level of Significance). If $np \geq 10$ and $n(1 - p) \geq 10$ then the study can use Z-test statistic

Table 3. Response analysis of Survey Question 2.

1	Very Unhelpful (1)	0
2	Somewhat Unhelpful (2)	13
3	Neither helpful nor Unhelpful (3)	14
4	Somewhat helpful (4)	97
5	Very Secure (5)	58

Table 4. Response analysis of Survey Question 3.

1	Never (1)	7
2	Rarely (2)	7
3	Sometimes (3)	58
4	Often (4)	86
5	Always (5)	24

and 182*0.50 > 0 and 182*0.50 > 10 (or considering that the number of success and failures are 91 and 91 respectively are at least 10. The study estimates the test statistic by: $Z = P' - Po = pPo(1 - Po)/n$ Here, $P' = 0.923$ (sample proportion); $Po = 0.50$ (population proportion); $N = 182$; $Zc = 11.4$; $Zt = 1.65$ (5% level of significance) critical value = 0.05. Since $Zc > Zt$, we reject Null hypothesis (Ho) and accept the alternate hypothesis (Ha). The test is significant. It confirms that more than 50 percent (92.3%) of the industries workers' population think that their organization runs network security defensive while on threat hunting. This conclusion is based on the sample result (a representative sample) which is reliably predictive of the population. Sample statistics predict population parameters at point estimate or interval estimate within negligible margin of errors.

5. Conclusions

The challenges presented by Business Email Compromise (BEC) to medium and large-scale companies in the United States of America (USA) are significant and require immediate attention [7]. This article has examined the specific vulnerabilities and complexities faced by medium and large-scale companies in relation to BEC attacks in the US context. The findings have revealed that these companies are particularly susceptible to BEC due to their size, complexity, and broader attack surface. The financial impact of successful BEC attacks can be devastating, posing a threat to the financial stability, shareholder confidence, and long-term viability of medium and large-scale companies. Operational disruptions resulting from BEC incidents can lead to supply chain disruptions, customer dissatisfaction, and reputational damage. Additionally, legal and regulatory challenges arise as these companies navigate compliance with industry-specific regulations and reporting requirements.

To address these challenges, effective mitigation strategies must be implemented. Medium and large-scale companies should prioritize robust cybersecurity measures, including employee training programs, to enhance awareness and response to BEC attempts. Implementing advanced email authentication protocols, implementing multi-factor authentication, and establishing incident response plans are vital steps to strengthen defenses and minimize the impact of BEC attacks. Collaboration among industry peers, cybersecurity organizations, and law enforcement agencies can foster information sharing and collective efforts to combat BEC threats. Furthermore, staying updated on emerging attack techniques and leveraging technological solutions to detect and prevent BEC attacks are crucial for maintaining cybersecurity resilience.

While this article has provided valuable insights into the BEC challenges faced by medium and large-scale companies in the USA, further research is needed to explore industry-specific vulnerabilities, sector-wise variations, and the effectiveness of mitigation strategies. By continuing to investigate and address the unique challenges faced by medium and largescale companies in the context of BEC, stakeholders can work collaboratively to strengthen cybersecurity resilience, protect critical assets, and foster a secure business environment for these companies in the USA. Ultimately, the collective efforts of medium and large-scale companies, policymakers, researchers, and cybersecurity professionals are essential in mitigating the impact of BEC and ensuring the sustained growth and success of these organizations in the dynamic and evolving cyber landscape.

6. Recommendations

Based on the challenges posed by Business Email Compromise (BEC) to medium and large-scale companies in the United States of America (USA), the following recommendations are proposed to enhance their cybersecurity resilience and effectively counter BEC threats:

- Implement Robust Security Measures: Medium and large-scale companies should invest in robust cybersecurity measures, including advanced email authentication protocols (e.g., DMARC, SPF, DKIM) to prevent email spoofing and domain impersonation [8]. Additionally, multi-factor authentication should be implemented for all critical systems and accounts to add an extra layer of protection against unauthorized access.
- Conduct Regular Employee Training: Employees should receive regular training on BEC awareness and best practices. This training should educate employees on how to identify suspicious emails, recognize common BEC tactics (e.g., social engineering, spear-phishing), and verify the authenticity of email requests before taking any action. By improving employee awareness, the risk of falling victim to BEC attacks can be significantly reduced.
- Establish Incident Response Plans: Medium and large-scale companies should develop and regularly update comprehensive incident response plans specifically tailored to address BEC incidents. These plans should outline clear procedures for reporting and handling suspected BEC attacks, involve key stakeholders from IT, legal, finance, and communications departments, and include steps for

promptly notifying law enforcement agencies and affected parties.

- Foster Collaboration and Information Sharing: Companies should actively participate in industry collaborations, such as Information Sharing and Analysis Centers (ISACs), to share insights, threat intelligence, and best practices related to BEC attacks. Collaborative efforts can help identify emerging trends, tactics, and techniques used by threat actors, enabling proactive mitigation and defense strategies.
- Implement Advanced Threat Detection Systems: Deploying sophisticated threat detection systems, such as AI-powered anomaly detection and behavior-based analytics, can enhance the capability to detect and respond to BEC attacks in real-time. These systems can identify suspicious patterns, unusual account behaviors, and indicators of compromise, allowing organizations to take swift action and prevent further damage.
- Strengthen Vendor and Partner Relationships: Medium and large-scale companies should establish strong relationships with their vendors and partners, emphasizing the importance of cybersecurity measures. Regular communication and shared best practices can create a mutually beneficial environment that promotes the exchange of security-related information and strengthens collective defenses against BEC attacks.

Acknowledgements

I would like to express my sincere appreciation to all those who have contributed to the successful completion of this research paper. Special thanks go to my colleagues and other experts in technology whose invaluable insights were integral to the foundation of this research. I am also grateful to my family and friends for their support throughout the course of this work.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Gupta, P., *et al.* (2018) A Survey on Deep Learning-Based Email Spam Filtering. *Journal of Network and Computer Applications*, **125**, 91-105.

[2] Bromium (2019) Behind the Scenes of BEC. https://www.bromium.com/resource/behind-the-scenes-of-bec/

[3] A Study by the Federal Bureau of Investigation, FBI (2020). https://www.fbi.gov/news/press-releases/fbi-releases-2020-incident-based-data

[4] Johnson, A. (2022) Vulnerabilities and Financial Losses in Small and Medium Enterprises: A Study of Limited Resources and Cybersecurity Investments. *Journal of Business Security*, **8**, 45-62.

[5] Cybersecurity Ventures (2021) The Official Annual Cybercrime Report. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[6] FBI (2020) FBI Internet Crime Report 2019.

https://www.fbi.gov/news/press-releases/fbi-releases-2019-incident-crime-report

[7] Proofpoint (n.d.) Business Email Compromise. https://www.proofpoint.com/us/threat-reference/business-email-compromise

[8] Cybersecurity Insiders (2023) Email Security in 2023—Your Cybersecurity Insiders Guide to Email Security Best Practices & Top Vendors. https://www.cybersecurity-insiders.com/email-security-in-2023-cybersecurity-insiders-guide-best-practices-top-email-security-vendors/