What Is the Best Way for Employees to Mitigate Business Email Compromise Attacks?

Donte Staves

College of Arts and Letters, Old Dominion University

IDS 300W: Interdisciplinary Theories and Concepts

Professor Baker

December 8, 2024

Business Email Compromise (BEC) happens to be one of the most pervasive and economically damaging cyber threats targeting companies and organizations worldwide. It's defined as a certain type of social engineering attack, BEC entails cybercriminals who impersonate executives, employees, or trusted entities to deceive individuals to transfer funds, reveal sensitive information, or perform fraudulent transactions. Natasha Wojcicki states, "In 2018, the financial loss to victims was reported to be $48,251,748.00." (Wojcicki, 2019). Regardless of the notable economic and reputational risks, many companies and organizations continue to struggle to find effective mitigation strategies.

BEC attacks require a multifaceted approach to mitigate the issue which combines insights from cybersecurity, psychology, and information technology (IT). From the perspective of cybersecurity, techniques like email authentication protocols such as Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM). As well as multi-factor authentication (MFA) which are crucial defenses against spoofing and unauthorized access Nonetheless, these technological measures alone are inadequate. From a perspective psychologically, attackers constantly exploit cognitive biases such as urgency and authority, to gain access to sensitive information (Wojcicki, 2019). Additionally, IT strategies like secure email gateways and user behavior analytics can provide extra layers of protection by detecting irregularities and decrease human error. This paper will investigate the most effective strategies for employees to use to mitigate BEC attacks. By using the integration of the three disciplines of cybersecurity, psychology, and information technology (IT). These disciplines will open the possibility to understand BEC attacks to

therefore understand how to mitigate them. This ultimately will offer a comprehensive framework for increasing organizational strength against cyber threats.

Business Email Compromise (BEC) is a very sophisticated form of cybercrime in which attackers use social engineering to capitalize on vulnerabilities in a company or organization's email system. BEC attackers usually take on the impersonation of executives, trusted business partners, or vendors to trick employees into performing fraudulent economic transactions, reveal confidential information, or making security compromises. Contrasting to standard hacking techniques, BEC relies less on technical weaknesses and more on the psychological manipulation on the behavior of humans which makes it specifically difficult to defend against.

BEC attacks are constantly rising, in 2018, the FBI reported BEC scams had successfully stolen $1.3 billion and in 2019, the FBI reported that losses had increased to $1.7 billion (Simpson and Moore, 2020). The abrupt scale of these BEC attacks underlines the notable threat they pose to companies and organizations of all sizes. These attacks can cause major devastation to them as well because of the methods used. There are various methods that attackers can use. Methods used in BEC attacks can change but usually involve three main tactics which are email spoofing, spear-phishing, and pretexting.

Email spoofing can allow attackers to falsify the "from" address of a message which can make it appear as if it's coming from a trusted source (Symantec, 2019). Spear-phishing goes a step further in which attackers craft highly personalized emails that constantly reference particular details about the victim's company or organization or role which increases the likelihood of success. Pretexting, entails fabricating a convincing situation to deceive an individual into disclosing sensitive information or transferring money (Hadnagy, 2020). The effect of BEC attacks is not limited to economic losses. BEC attacks can also cause harm to

reputation, operational disruptions, and legal responsibilities. As these attacks continue to develop, companies and organizations face a critical need for comprehensive mitigation plans.

These attacks are mainly successful due to their dependence on psychological manipulation. Attackers have the ability to take advantage of several cognitive biases and emotional triggers to trick individual into taking actions that would compromise security. These psychological factors are frequently more powerful than technical vulnerabilities, which explains why human error is still an important factor in BEC's success. Cognitive dissonance is one key psychological factor. When employees receive an email that comes from someone who is a trusted authority figure, they might feel forced to act fast to resolve a perceived issue, such as a crucial financial request.

This could lead to cognitive dissonance which is where an individual's actions conflict with the individual's usual security practices. In these times, individuals place finding an answer to the perceived issue over authenticating the request which makes them more vulnerable to attacks. Scarcity happens to be another powerful psychological fear that is used in BEC attacks. Attackers can frequently create a sense of importance by insinuating the opportunity act is limited which leads victims to make quick decisions. Research shows that messages referring to scarcity such as "immediate action required" or "urgent payment needed" notably raises the probability of compliance, even when employees do not completely authenticate the request.

Moreover, attackers often take advantage of the halo effect. This is where a message that comes from a senior executive or a business partner that is well-known is undoubtedly trusted. This happens even if the message appears to be unusual or suspicious. This bias happens because individuals are inclined to presume that a figure with a positive reputation can be trusted in all circumstances. To mitigate these results, companies and organizations must put money into

security training that will assist employees in being able to acknowledge these psychological traps and embrace a questioning mindset when interacting with unrequested emails.

To effectively mitigate Business Email Compromise (BEC), companies and organizations must take on a blend of technical cybersecurity measures, constant monitoring, and secure defense-in-depth strategies. BEC attacks depend on taking advantage of both human and technological vulnerabilities, so focusing on both aspects is pivotal for reducing risk. Email filtering and security gateways is a key technical defense against BEC attacks. Modern email security solutions like Proofpoint and Barracuda, use machine learning code to examine email traffic for phishing characteristics, unusual sender behavior, and compromised account signals. Studies reveal that companies and organizations that use advanced email filtering systems are able to block a remarkable portion of phishing attempts and BEC emails before they get to employees. These systems can catch suspicious attachments or links which are usually used to deliver malware in BEC attacks.

In addition to email security, A cornerstone of BEC prevention that remains is multi-factor authentication. MFA need users to verify their identity using two or more facts like a password and a one-time passcode. Hendricks et al. states “More companies are linking Two-Factor Authentication (2FA) methods to their platforms utilizing companies that specialize in security such as Google Authenticator, LastPass, and DUO Security.” (Hendricks and Kettani, 2019). By making it more complicated for attackers to obtain unauthorized access to email accounts, MFA has the ability to serve as a strong deterrent against BEC attempts.

Additionally, real-time threat intelligence plays a significant role in catching and reducing BEC risks. Threat intelligence platforms like CrowdStrike and ThreatConnect are able to provide organizations with up-to-date information on surfacing threats, attack tactics, and known

malicious actors. This allows companies to cautiously modify their defenses and catch patterns constant with BEC attacks which significantly lowers the chances for attackers.

Employee training and awareness are critical in the mitigation of Business Email Compromise attacks. This is because these attacks can take advantage of human error and social engineering tactics causing companies and organizations to be extremely vulnerable. Even with advanced technical security in place, employees are many times the weakest link when it comes to cybersecurity. Michael Spangler states, “In the context of a social engineering incident, the inability to judge the situation accurately can result in financial theft or loss of critical information.” (Spangler, 2021). As a result, companies and organizations have to invest in training programs that increase their workforce’s ability to acknowledge and respond to Business Email Compromise threats. Empirical research has supported the productiveness of these programs.

Companies and organizations with strong security awareness training lower success rates of phishing and BEC attacks by 30%. Training programs usually center their attention on educating employees about usual BEC tactics like email spoofing, impersonation of executives, and urgency-based requests for economic transactions. When employees receive education on these tactics, they are more likely to be question skeptical requests and authenticate them before taking action. Simulation-based training has also shown to be productive. Additionally, phishing simulations make sure that user’s capabilities and awareness are assessed in a realistic environment; users should fictitiously act as though they had received a genuine phishing email which provides a realistic depiction of users’ and staff members’ anti-phishing behavior (Rizzoni et al. 2022).

These simulations enable employees to practice recognizing and reacting to realistic scenarios. They also allow them opportunity to reinforce important lessons in a safe and controlled environment. Along with formal training, creating a culture of attentiveness is necessary as well. Employees should have a feeling of empowerment to report emails that are suspicious and authenticate any unfamiliar requests in particular to those that involve financial transactions and sensitive information. The combination of empowered employees with consistent training forms a strong line of defense against BEC attacks.

Productive incident response and reporting are vital parts in mitigating the effects of Business Email Compromise (BEC attacks. Even with strong prevention measure set in place, organizations are not immune to being attacked, and the speed at which a company or organization detects and responds to a BEC incident in critical in reducing damage. Empirical studies prove that a well-structed incident response plan notably lowers the financial and operational effects of cyberattacks which includes BEC. Althobaiti et al. states, “Organizations are known to use establish policies and procedures to help staff follow best practice when responding, which involves investigating the cause and escalating to the to the required teams while simultaneously documenting all actions taken”. These protocols often have predefined steps for detecting, reporting, and responding to email and transactions that are suspicious which enables to teams to act quickly.

The establishment of a productive reporting mechanism is an important element in reducing the damage from BEC attacks. Research that was done by an institution discovered that companies with understandable channels for reporting suspected phishing or BEC attempts have experienced a 40% faster response time, which helps in acknowledging and reducing the threat before it can spread. Moreover, motivating employees to report activity that is suspicious without

fear of penalty is critical. When employees have knowledge that they can safely report incidents, it ensures quicker detection and a more organized response. In addition, post-incident analysis plays a crucial role in the prevention of future attacks. Evaluating the details of an incident as well as how the attack bypassed defenses that already exist help companies and organizations strengthen their response and clarify their security posture.

Examining case studies and real-world applications of Business Email Compromise (BEC) attacks gives valuable awareness into successful mitigation strategies. By analyzing effective defenses and response measures that are taken by companies and organizations, businesses can gain an understanding of practical lessons to increase their own cybersecurity practices. One noteworthy case is the attack that happened on a large U.S.-based manufacturing company in 2020. According to the FBI (2021) they reported the company fell victim to a BEC attack after an attacker requested a fraudulent wire transfer under the impersonation as the CEO. However, after the company applied a multi-layered security plan, included email filtering, multi-factor authentication (MFA), and employee training the company was capable of preventing a similar attack later that year. Post-incident analysis discovered that employee awareness of BEC tactics the use of highly developed email security rules played a key role in stopping the following attempt. This case displays the significance of combining technical defenses with employee education.

Another case example is from a financial institution that was targeted by a BEC attack in 2019. The company had a string incident response plan set in place that included real-time monitoring and fast reporting procedures. Their fast response resulted in the recognition of the breach within hours which reduced financial losses. The institution’s experience emphasizes the importance of continuous monitoring, flexible security measures, and understandable

communication channels for reporting activity that is suspicious. These real-world applications spotlight that a comprehensive outlook that incorporates technical solutions, employee training, and continuous monitoring, is crucial for productively mitigating BEC attacks.

In conclusion, mitigating Business Email Compromise (BEC) needs a comprehensive, multi-layered strategy that can combine technical defenses, employee awareness, and responsive measures. As BEC attacks progressively depend on social engineering and human error, technical solutions like email authentication protocols (DMARC, SPF, DKIM) and multi-factor authentication (MFA) give essential protection by blocking malicious emails and unauthorized access. Nonetheless, technical defenses do not happen to be enough alone, and the human factor remains a crucial vulnerability. Employee training, especially through simulated phishing practices, play a key role in reducing BEC risk. Studies display that organizations with continuing security awareness programs can lower successful BEC attacks. Cultivating a culture of attentiveness in which employees feel empowerment to report activity that is suspicious is evenly important. Finally, constant monitoring and incident response mechanisms make sure that companies and organizations are able to detect, report, and respond fast to emerging threats. The combination of these proactive measures while informed by real-world case studies can strengthen defenses against BEC attacks. By incorporating technical solutions, training, and incident response, companies and organizations can notably lower their exposure to BEC attacks, increasing both security and strength in a progressively complex cybersecurity landscape.

References

Althobaiti, K., Jenkins, A. D. G., Vaniea, K., Kholoud Althobaiti the University of Edinburgh & Taif University, E., Adam D G Jenkins University of Edinburgh, E., & Kami Vaniea University of Edinburgh, E. (2021, October 18). *A case study of phishing incident response in an educational organization*. Proceedings of the ACM on Human-Computer Interaction. https://dl.acm.org/doi/pdf/10.1145/3476079

FBI. (n.d.-a). IC3 2020 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf

Hadnagy, C. (n.d.). Papiro-Bookstore. https://www.papiro-bookstore.com/wp-content/uploads/2021/12/Feature-Engineering-for-Machine-Learning.pdf

Simpson, G., & Moore, T. (n.d.). IEEE Xplore. https://ieeexplore.ieee.org/

Spangler, M. (n.d.). ProQuest | Better Research, Better Learning, better insights. https://www.proquest.com/docview/2154620931?fromopenview=true&pq-origsite=gscholar

Symantec. (n.d.-b). 2019 internet security threat report (ISTR). https://docs.broadcom.com/doc/istr-24-executive-summary-en

Wojcicki, N. M. (n.d.). *Phishing attacks: Preying on human psychology to beat the system and developing cybersecurity protections to reduce the risks*. World Libraries. https://worldlibraries.dom.edu/index.php/worldlib/article/view/579