# Opportunity Knocks: Modern Trends with Business Email Compromise in a Changing Cyber World

*New Jersey Law Journal*
November 27, 2024
By David J. Shannon and Jeremy J. Zacharias

Imagine the following scenario: On a busy Monday morning at a major law firm, an associate attorney receives an email from a senior partner asking for his thoughts on a legal brief that must be filed that morning. This request is odd, because the associate has never spoken to or worked with this partner. However, wanting to appear capable and helpful, the associate opens the link attached to the email to reveal a blank document. Little does he know that he just made the entire firm vulnerable to a business email attack by a threat actor. His actions will lead to potential encryption of firm data, a high ransom demand and public professional embarrassment.

In the current new age of technology and capability, threat actors are cashing in by using various tools in their arsenal, including generative artificial intelligence (gen AI), to penetrate security safeguards in place by businesses. Threat actors, once embedded in a compromised computer system by way of some vulnerability, are learning patterns and structures of the computer system host and wait until a financial opportunity, such as a large wire payment, arises. Gen AI and other modern cyber tools make it increasingly difficult to detect breaches and leave businesses vulnerable to wire fraud, data encryption and ransomware, among other threats.

## Current Trends With BEC

According to a recent Arctic Wolf market survey, Business Email Compromise (BEC) is the top method of cyberattack that businesses face. In a BEC scheme, threat actors utilize a vulnerability in a business email system to access the email account to create a scam campaign for financial gain. This has become the fastest moving trend for global cyberattacks. Nearly 70% of organizations were the targets of attempted BEC attacks in 2023, with almost 30% of these businesses becoming victims of successful BEC occurrences. With the growing number of attacks, threat actors are becoming increasingly successful in penetrating an organization's security measures, which inevitably leads to financial harm.

One reason for the increasing occurrence of successful BEC attacks has to do, in large part, to the rise of gen AI, which can be used as both a helpful tool and a dangerous weapon. A large percentage of organizations globally have implemented adoption and usage policies pertaining to the use of gen AI to aid day-to-day business.

Threat actors are currently utilizing gen AI as a weapon to carry out their BEC pursuits. Gen AI can create realistic fraudulent emails, text messages, life-like audio and realistic deep fake videos to trick employees into divulging sensitive information, such as banking information or sensitive client data.

Current trends with gen AI include voice cloning, deep fake video cloning and mirroring email vernacular of the person the threat actor seeks to impersonate. Even if security measures are in place to verify the fraudulent request received, depending on how deep the threat actor is embedded into a business server, there is not much the company can do at that time to prevent a larger breach.

A very common practice utilized by threat actors stems from robust phishing campaigns, which are bolstered by the use of gen AI. Organizations that use cloud-based email servers make it difficult to detect phishing attempts, especially with unsuspecting and over-worked employees.

Even if an organization has invested in the most effective security tools available, the human element is still the largest threat. With BEC attacks launched daily, a company's least security aware employee can make the entire organization susceptible to a threat actor's infiltration.

## Measures That Can Be Taken to Mitigate BEC Attacks

Multi-Factor Authentication (MFA) is one of the best tools a business can utilize to prevent or mitigate the risk of a BEC attack. Threat actors, by entering into a BEC campaign, try to evade traditional cyber defenses such as firewalls and anti-malware protections. Organizations should have measures in place to detect these attacks and to gain an understanding of vulnerabilities in the system to prevent future attacks from occurring. Even if a threat actor successfully infiltrates the business server, the use of MFA can limit the scope of the threat actor's contagion in the business environment.

Businesses must make data security a priority by incorporating the use of MFA, among other security tools, into daily practice. Security-savvy organizations will mandate that all employees use MFA when using company technology. The mandate is imperative because while most businesses have the capabilities to use MFA as a security measure, there are employees who are not security aware or do not care to take the time for added security protocols.

Additionally, organizations must practice heightened security awareness and take extra precautions as part of their daily practice. Employee error, which is always a factor, could be lessened by implementing routine training and awareness of common traps used by threat actors in gaining sensitive information. For example, employees should be educated on how to review an email sender's address to ensure accuracy and trained to never open random links from unknown senders. Organizations should train employees to assume all incoming emails and links are untrustworthy until proven otherwise. With rising BEC claims, these actions also apply to phone calls or text messages requesting the dissemination of confidential information or money.

Threat actors are utilizing modern advancements with gen AI to cash in when penetra-

ting vulnerable businesses in a BEC. Once a threat actor finds an opening in an unsecured business server, it patiently waits to strike until discovering an opportunity for financial gain or stealing sensitive company or client data in a ransomware attack. When each employee is vigilant about security risks and vulnerabilities, the fight against cybercrime is on a more level playing field. With the rise of gen AI technology and how it is being used for harm, it is more important than ever that employees consistently question and remain skeptical of attempts to gain sensitive data.

*David J. Shannon chairs both the privacy and data security, and the intellectual property, technology and medial litigation practice groups in the Philadelphia office of Marshall Dennehey. He concentrates a substantial portion of his practice on privacy law, data breaches, intellectual property, copyright and trademark infringement, as well as trade secret, trade dress technology and media related litigation. He may be reached at djshannon@mdwcg.com.*

*Jeremy J. Zacharias is a shareholder in the professional liability department in Marshall Dennehey's Mount Laurel office. A member of the firm's privacy and data security practice group, he represents a broad spectrum of clients in privacy and data breach matters. He additionally handles cases involving the defense of attorneys, accountants, insurance producers, corporate directors and officers, and financial institutions, when claims are brought against them. He may be reached at jjzacharias@mdwcg.com.*