Business Email Compromise

Survival Guide

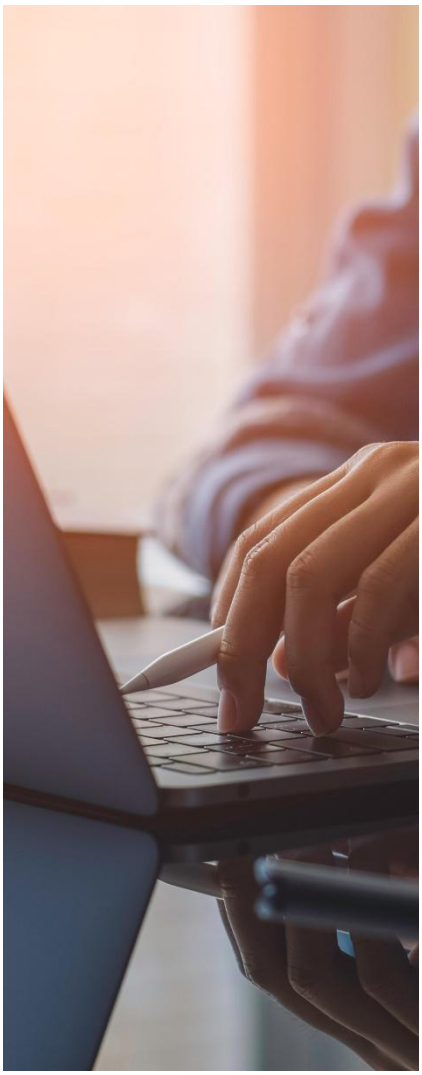
Provided by: Barnard Donegan Insurance

BDI Barnard Donegan Insurance
Since 1911

Table of Contents

This guide is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.
© 2023 Zywave, Inc. All rights reserved.

Introduction



Cybercriminals continue to become more sophisticated, leveraging a wide range of tactics in order to attack their targets. One tactic that has increased in frequency, complexity and resulting losses over the past few years is the use of business email compromise (BEC) scams. A BEC scam entails a cybercriminal impersonating a seemingly legitimate source, such as a senior-level employee, supplier, vendor, business partner or other organization, via email. The cybercriminal uses these emails to gain the trust of their target, thus tricking them into believing they are communicating with a genuine sender. From there, the cybercriminal convinces their target to wire money, share sensitive information (e.g., customer and employee data, proprietary knowledge or trade secrets) or engage in other compromising activities.

BEC scams can lead to numerous consequences for businesses of all sizes and sectors, including financial losses, stolen or damaged data, and potentially severe reputational damages. What's more, these scams are among the costliest cyberattacks. According to technology corporation IBM, BEC scams are the second most expensive type of data breach, costing targets an average of $4.9 million per incident. Making matters worse, these scams have become an increasingly prevalent threat. In fact, the FBI's Internet Crime Complaint Center (IC3) recently reported that BEC scams have jumped by 65% since 2019, contributing to $2.7 billion in losses across the United States during 2022 alone. In total, the FBI confirmed that global losses stemming from these scams have already surpassed $43 billion.

With this in mind, it's crucial for businesses across industry lines to have a better understanding of BEC scams and associated prevention and response measures. That's where this guide can help. This resource provides an overview of how BEC scams work, explains common scam techniques, identifies key targets of such scams, outlines effective mitigation strategies, and describes effective response and recovery methods. By utilizing this guide, businesses can equip themselves with the information needed to combat BEC scams and minimize potential losses if these incidents occur.

This guide is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Businesses should contact legal counsel or an insurance professional for appropriate advice. Reach out to Barnard Donegan Insurance today for further risk management guidance and insurance solutions.

How BEC Scams Work

Essentially, BEC scams consist of cybercriminals impersonating individuals or entities within their targets' trusted networks for malicious gains. These scams are categorized as a form of social engineering, which refers to a broader cyberattack method that preys on key human behaviors (e.g., trust of authority, fear of conflict and promise of rewards) to obtain unwarranted access to organizational systems, funds or data. While the specific methods utilized for executing BEC scams can vary, these incidents often follow the same general framework. Here are the main steps a cybercriminal takes when deploying a BEC scam.

Researching the Organization

First, a cybercriminal selects an organization to launch their BEC scam against. From there, the cybercriminal will conduct a range of research on the organization to help them develop a detailed profile of the company and its executives, create convincing emails and gain their target's trust during the attack. This research may include activities such as the following:

- Analyzing the company's website and LinkedIn page to understand its organizational hierarchy (e.g., members of the senior leadership team, primary department roles and reporting structures)
- Finding and examining individual employees' social media profiles and professional platforms to learn more about their interests, job responsibilities and workplace connections
- Reviewing any other information available on the company (e.g., industry news articles, public records and press releases) to identify key organizational issues and developments

Selecting the Target

After researching the organization, cybercriminals will use the information they collected to prepare for their attack. At this point, the cybercriminal picks a specific individual within the organization as their main target for the incident, likely someone who has access to critical company funds and data.

Launching the Attack

Once they choose their target, the cybercriminal will deploy malicious software (also called malware) to access their target's email account, monitoring the target's digital interactions for days or weeks without their knowledge. Doing so allows the cybercriminal to see who the target frequently interacts with, what their conversations typically look like and the types of activities they conduct via email (e.g., paying invoices or sharing sensitive company files). The cybercriminal can then use this information to better impersonate a trusted sender and manipulate the target.

What's more, the cybercriminal may also hack into the email account of another individual in the target's organizational network, inserting themselves directly into legitimate conversations and further convincing the target to engage in compromising activities. Here are some other common attack strategies the cybercriminal may use:

- **Utilizing fake accounts or websites**—If the cybercriminal opts not to hack into the target's or a trusted sender's email account, they will likely rely on fraudulent accounts or websites to launch their attack. For example, the cybercriminal may send emails using false domain names that appear genuine or direct the target to seemingly legitimate websites (also known as domain spoofing). Similarly, the cybercriminal may utilize lookalike domains, which almost exactly match the actual source, to deceive their target into performing certain actions.
- **Creating confusing variations**—In an attempt to convince their target that they are a trusted source, the cybercriminal may create an email address that is nearly identical to the source they are impersonating, with the exception of a few characters (e.g., altering the email address "janedoe@samplecompany.com" to "janedoee@samplecompanyy.com").
- **Using spear-phishing techniques**—The cybercriminal may engage in spear-phishing by conducting additional, personalized research on their target and leveraging any extra details they discover to further motivate the target to believe their false identity. When spear-phishing, a cybercriminal will often impersonate a source who is more directly connected to their target (e.g., a close colleague or department leader).
- **Deploying additional malware**—When sending fraudulent emails, a cybercriminal may encourage their target to download harmful attachments or click on deceptive links in an effort to launch additional malware. Once activated, this harmful software can help the cybercriminal more easily gain access to their target's systems, funds and data.

Manipulating the Target

Once the cybercriminal convinces their target that they are engaging in a genuine business interaction, they will conclude the attack by manipulating the target into wiring company funds to the cybercriminal's personal bank account or a bank account controlled by a large-scale organized crime group; sharing sensitive organizational details, intellectual property, supply chain information or workplace documentation; providing account credentials; or disclosing confidential employee or customer data.

Common Types of BEC Scams

The FBI identifies five primary types of BEC scams, including the following:

1. **False invoice scheme**—In such a scheme, a cybercriminal impersonates an organizational supplier to trick their target into paying fraudulent invoices or transferring funds to a phony account.

2. **CEO fraud**—This scam method entails a cybercriminal impersonating a senior-level employee or executive and requesting that their target conduct a wire transfer to a fake account. The request is often demanding in nature, threatening the target with work-related consequences or other punishments for failing to comply.

3. **Account compromise**—With this scam tactic, a cybercriminal hacks into an employee or executive's actual email account and distributes messages to various contacts, attempting to fool these recipients into paying fraudulent invoices.

4. **Attorney impersonation**—This scam technique refers to a cybercriminal impersonating a lawyer or other legal representative and requesting a payment be made to a phony account in order to handle an organizational matter deemed "sensitive" or "pressing."

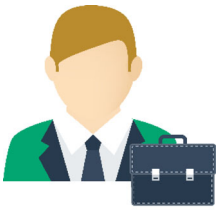
5. **Data theft**—In such a scam method, a cybercriminal impersonates an HR professional to trick their target into sharing personal information about employees or executives. The cybercriminal can then leverage this sensitive data during future attacks.

Key Targets of BEC Scams

Businesses of any size or industry may experience BEC scams. Yet, certain organizations, such as large-scale corporations, government entities, nonprofits and educational institutions, may be more susceptible to these incidents due to the amount of resources, funds and information they have access to. In the same vein, any employee can be targeted in a BEC scam; nevertheless, some employees may be more likely to encounter these attacks than others. Specifically, cybercriminals generally view the following types of employees as attractive targets in BEC scams:

- **New or entry-level employees**—These employees could be considered ideal targets for BEC scams due to their limited training or experience, potential lack of cybersecurity knowledge, and relative unfamiliarity with applicable organizational protocols (e.g., email verification requirements, data-sharing standards and invoice payment procedures).

- **Mid-level HR or finance employees**—Such employees may also be perceived as top targets for BEC scams because of their ability to access confidential company data, including corporate banking details and account numbers, tax statements, contact information and employment records. Furthermore, mid-level employees are inclined to comply with their managers' requests and often possess the authority to conduct activities such as paying invoices or sharing files, thus making them more prone to perform these tasks for cybercriminals disguised as their senior-level counterparts.



- **Company leaders and executives**—These employees could be preferred targets for BEC scams because of their expansive access to organizational funds and data. Additionally, key details about such employees are usually publicly available on company websites and platforms, making it easier for cybercriminals to learn more about them and pretend to know these individuals during email interactions. While company leaders may seem less likely to be fooled by these scams, the reality is quite the opposite; recent research from software company KnowBe4 found that 50% of business executives have fallen for phishing attacks, which are often the first step in BEC scams.

BEC Prevention Measures

There are several steps businesses can take to help establish a layered defense against BEC scams and reduce related losses. In particular, here are some effective measures for companies to consider:

- **Educate employees.** Minimizing losses from BEC scams starts with training employees to identify common attack scenarios and help detect and prevent such incidents. During this training, businesses should equip staff with the following best practices:

  - Refrain from sharing personal or work-related information on social media platforms, as cybercriminals could use those details to help launch BEC scams.
  - Avoid opening or responding to emails from individuals or organizations you don't know. If an email claims to be from a trusted source, be sure to verify the source's identity by double-checking the domain name.
  - Monitor emails for key signs of BEC scams, such as unusual questions from managers or executives, requests that bypass typical channels or workflows, demands to avoid communicating with others or phrasing that deploys an extreme sense of urgency. Also, be especially wary of emails that lack personalization, contain spelling and grammatical errors, or use threatening language.
  - Don't divulge financial information or share confidential data over email. Further, never click on suspicious links contained in emails. Similarly, avoid downloading email attachments or from unknown sources.
  - Contact your manager or the IT department immediately for additional guidance if you suspect a BEC scam.

  Because BEC scams continue to evolve, this training shouldn't be a one-time occurrence. Businesses should provide cybersecurity training regularly and update it when needed to reflect the latest threats, attack trends and workplace changes.

- **Implement effective payment protocols.** Having safe and secure payment procedures can help put a stop to BEC scams before any money is lost. As such, businesses should instruct employees who handle financial operations to carefully analyze invoices and fund transfer requests to ensure their validity. When possible, these requests should be discussed in person before moving forward, especially if they involve alternative payment procedures or changes in account numbers. Businesses may also consider utilizing several verification methods to confirm payment requests.

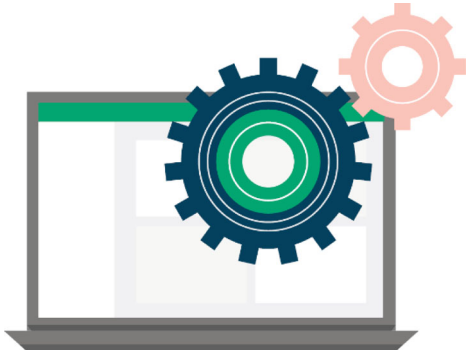
- **Leverage access control policies.** Businesses should only provide employees with access to sensitive organizational data as needed. Some of the most valuable access control policies include the following:
    - **The principle of least privilege (POLP)**—POLP is a cybersecurity concept that refers to allowing employees access to only the networks, data and technology necessary for performing their job duties. By implementing POLP, businesses can ensure cybercriminals won't receive full access to all company assets by compromising a single employee's account, therefore limiting available resources to leverage in a BEC scam.
    - **Multifactor authentication (MFA)**—On the other hand, MFA is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login. This additional login hurdle means that cybercriminals will have a harder time hacking into employees' accounts to execute BEC scams. It's best practice for businesses to enable MFA for remote access to their networks, administrative functions within their networks and any enterprise-level cloud applications.
- **Perform frequent data backups.** By keeping sensitive data secure, businesses can make it increasingly difficult for cybercriminals to access this information amid BEC scams. One of the best ways to do this is by conducting frequent and secure data backups. First, businesses should determine safe locations to store their critical data, whether it's within cloud-based applications, on-site hard drives or external data centers. From there, businesses should establish concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber incidents.
- **Utilize security features.** Businesses should make sure all organizational devices, networks and systems possess adequate security features to help deter BEC scams, including antivirus and malware prevention programs, virtual private networks, and firewalls. In addition, businesses may want to consider the following advanced security features:
    - **Email authentication technology**—This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards that businesses have in place. There are several different verification standards that businesses can choose from, but the most common is sender policy framework (SPF), which focuses on verifying senders' IP addresses and domains.

      Upon verifying emails, email authentication technology permits them to pass through organizations' IT infrastructures and into employees' inboxes. When emails can't be authenticated, they will either appear as flagged in employees' inboxes or get blocked from reaching inboxes altogether. With SPF, unauthenticated emails may even be filtered directly into employees' spam folders. Ultimately, email authentication technology can make all the difference in keeping dangerous emails out of employees' inboxes and putting a stop to cybercriminals' BEC scams before they can begin.
    - **Endpoint detection and response (EDR) solutions**—Businesses can use EDR solutions to continuously monitor security-related threat information across their systems and devices in

order to better detect and respond to BEC scams, particularly those involving malware. These solutions offer advanced threat detection, investigation and response capabilities—including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment—by constantly analyzing network events to identify suspicious activity.

- **Patch management plans**—Patch management refers to the process of acquiring and applying software updates, called patches, at various endpoints, such as smartphones, desktop computers, laptops, tablets and other devices that communicate back and forth with the networks in which they are connected. Patches modify operating systems and software to enhance security, fix bugs and improve performance. They are created by vendors and address key vulnerabilities cybercriminals may target, including those used in BEC scams.



The patch management process can be carried out by organizations' IT departments, automated tools or a combination of both. Steps in the patch management process include identifying IT assets and their locations, assessing critical systems and vulnerabilities, testing and applying patches, tracking progress and maintaining records of such progress. As it pertains to limiting their BEC exposures, businesses should be sure to establish patch management plans that include frameworks for prioritizing, testing and deploying software updates.

- **Have a plan.** In the event that a BEC scam is suspected or detected, it's essential for businesses to have dedicated cyber incident response plans in place that outline steps to ensure timely remediation and keep damages to a minimum. These response plans should address a variety of possible attack scenarios and be communicated to all applicable parties. Both the Cybersecurity &

Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have resources available to help businesses create such plans. At a glance, a solid response plan should outline:

- Who is part of the cyber incident response team (e.g., company executives, IT specialists, legal experts, media professionals and HR leaders)
- What roles and responsibilities each member of the response team must uphold during an incident
- What the company's key functions are, and how these operations will continue throughout an incident
- How critical workplace decisions will be made during an incident
- When and how stakeholders and the public (if necessary) should be informed of an incident
- Which federal, state and local regulations the company must follow when responding to an incident (e.g., reporting protocols)
- When and how the company should seek assistance from additional parties to help recover from an incident (e.g., law enforcement and insurance professionals)
- How an incident will be investigated, and what forensic activities will be leveraged to identify the cause and prevent future incidents

- **Conduct tabletop exercises and penetration testing.** It's not enough for businesses to simply create cyber incident response plans. Rather, they should routinely assess these plans for ongoing security gaps and make changes as needed to ensure maximum protection amid BEC scams. Common assessment techniques include:
  - **Penetration testing**—Such testing consists of an IT professional mimicking the actions of a cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and is able to withstand attack efforts. This testing usually targets a specific type of workplace technology and may leverage various attack vectors.
  - **Tabletop exercises**—A tabletop exercise is an activity that allows an organization to simulate a realistic cyberattack scenario for the purpose of testing its incident response plan's efficiency. In other words, this exercise serves as a cyberattack drill, giving participants (typically members of the incident response team) the opportunity to practice responding to an attack.

- **Foster a strong cybersecurity culture.** For organizational cybersecurity measures to be effective, businesses must properly enforce them and ensure employees of all levels and departments—whether they are new to the workforce, tenured employees or experienced executives—take these measures seriously. By doing so, businesses can effectively establish cybersecurity as a top priority, give employees the tools and knowledge to fight against digital threats with confidence, and promote a culture of compliance.

- **Consult trusted experts and professionals.** Businesses don't have to navigate and address their BEC exposures alone. Instead, they can seek assistance and supplement their existing resources with guidance from a wide range of trusted external parties, including insurance professionals, legal counsel, cybersecurity firms, law enforcement and government agencies (e.g., CISA and NIST).
- **Purchase sufficient coverage.** It's critical for businesses to purchase adequate cyber insurance to secure ample financial protection against potential losses that may arise from BEC scams. Businesses should consult trusted insurance professionals to discuss their specific coverage needs.

BEC Response and Recovery Steps

Even with effective prevention measures in place, some businesses may still be targeted in BEC scams. Yet, how they respond to and recover from these incidents can make all the difference in keeping related disruptions and damages to a minimum. As such, businesses should consider the following BEC response and recovery protocols:

- **Activate the response plan.** As soon as a potential BEC scam has been reported, a business should assess the associated report and determine whether the incident is a genuine threat. If the attack can be validated, the business should coordinate with the cyber incident response team and execute the response plan. In the scope of a BEC scam, specific procedures outlined in the response plan will likely include the following:

  - Analyzing which systems (including email and banking accounts), funds and data have been affected by the incident and informing employees to ensure they avoid further engagement with cybercriminals
  - Consulting the IT department to take impacted systems offline and disable compromised email accounts and contacting financial institutions to freeze affected banking accounts, thus limiting additional losses
  - Accessing backups of any impacted data (if possible) and keeping this information in a secure, offline location
  - Documenting as many details as possible about the incident and related losses in order to provide ample information to insurers, forensic investigators and law enforcement
  - Utilizing offline communication methods (e.g., phone calls) to discuss future steps with the response team to prevent cybercriminals from intercepting any important conversations
  - Reporting the incident to the local FBI field office and logging the scam with the IC3

- **Notify applicable parties.** Depending on the nature and severity of a BEC scam, there are various parties a business will need to inform about the attack—whether it's for the purpose of ensuring financial protection, getting additional remediation assistance, discussing legal ramifications or notifying impacted individuals (i.e., those who may have had their data exposed). These parties may include:
  - Insurers, brokers and risk management professionals
  - IT experts and cybersecurity firms

- HR, communications and media professionals
- Law enforcement and forensic investigators
- Government agencies and legal counsel
- Stakeholders (e.g., customers, investors and suppliers)

In any case, communication is key both during and after a BEC scam. If a business fails or neglects to inform necessary parties of an attack, it could face substantially higher losses, regulatory penalties and widespread reputational damage.

- **Restore affected systems and data.** After a BEC scam, it's vital for a business to restore all impacted systems and data. This may include wiping any devices of malware, taking affected systems back online, and enabling or unfreezing compromised accounts. In some cases, this could also entail opening new accounts or purchasing additional technology or software to replace any severely damaged assets.
- **Perform a post-incident analysis.** To properly assess how a BEC scam was handled and identify any shortcomings, it's best for a business to conduct a post-incident analysis. Specifically, this analysis should focus on where the attack originated; how the attack was detected (as well as how quickly such detection occurred); how effective the incident response plan was in handling the attack; and the different technical, operational and financial impacts of the attack. Depending on the attack's origin and the overall damages, it may also be worthwhile to evaluate whether employee training (or lack thereof), software vulnerabilities or data backup processes played a role in the incident.

- **Identify weaknesses and fill any gaps.** Based on the results of the post-incident analysis, a business should point out its cybersecurity weaknesses and make an effort to fill possible gaps with bolstered defenses. Doing so is critical to help prevent future incidents and minimize associated damages. Necessary adjustments may include modifying the cyber incident response plan, enhancing employee training, updating or introducing new software, improving data backup protocols and implementing stricter security policies.

Conclusion

BEC scams have become a pressing concern for all businesses, regardless of size or industry. With these incidents on the rise, businesses simply can't afford to ignore their BEC exposures. Nonetheless, by implementing effective prevention, response and recovery procedures, businesses can not only limit their likelihood of experiencing such incidents but also mitigate possible losses when attacks arise.

Above all, it's crucial for businesses to understand that they aren't alone in managing their cyber risks and safeguarding against BEC scams. There is a wide range of resources and guidance available from trusted experts and professionals. For more information, contact Barnard Donegan Insurance today.