Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2022**
Sponsored by **SonicWall**

How to Deal with Business Email Compromise

Executive Summary

Business email compromise (BEC) attacks have not engendered the same level of notoriety as ransomware attacks, but rank in combination as one of the most financially devastating and common types of cybercrimes against organizations. Many organizations are ill-prepared to address the threat of BEC and lack sufficient protections across people, process, and technology factors. This white paper reports on an in-depth survey exploring current readiness and confidence to deal with the threat of BEC, highlights solutions that have been specifically designed to counteract BEC threats, and outlines a series of best practices to strengthen defenses against BEC threats.

KEY TAKEAWAYS

- **Most organizations are already subject to BEC attacks**
  80% of organizations have experienced BEC attacks over the last year. The most common type of BEC attack involves impersonating a senior executive.
- **BEC attacks are a costly form of cybercrime**
  In the United States alone, almost 20,000 BEC attacks were reported to the FBI in 2020, with a cumulative loss of $1.8 billion. Countless other BEC attacks are not reported to the FBI.
- **Organizations are ill-prepared to deal with BEC attacks**
  Many organizations lack confidence in their ability to safeguard funds targeted by a BEC attack, get help from law enforcement or insurance providers for BEC losses, or even stop BEC threats from reaching highly targeted users. Current cybersecurity protections are ineffective, with many organizations relying on technologies that were not designed to counteract BEC threats.
- **Low preparedness equals ample opportunity for more BEC threats**
  Threat actors are likely to step up the frequency and cost of BEC attacks. It is unlikely that we have seen the peak of BEC attacks yet, either in number of incidents, business impact or overall losses to the economy.
- **Organizations need modern technology to counteract BEC threats**
  Technologies that specifically counteract BEC threats include anti-impersonation protections, contextual warnings on messages, and training focused specifically on identifying BEC threats. Solutions that address account compromise, such as strong multi-factor authentication, are also helpful.
- **Harden organizational processes targeted by BEC threats**
  Invoicing and payroll processes are commonly targeted by BEC attempts, and organizations should take appropriate action to reduce the threat scope.

Organizations are ill-prepared to address the threat of BEC and lack sufficient protections across people, process, and technology factors.

ABOUT THIS WHITE PAPER

This white paper is sponsored by SonicWall. Information about SonicWall is provided at the end of this paper.

This white paper references data from an in-depth survey conducted in November and December 2021 of 119 professionals in IT, cybersecurity, risk, and compliance roles. Respondents work for mid-sized and large organizations (average employees 14,388, median 1,599) across multiple industries. All respondents know how their organization is addressing or planning to address the threat of BEC.

What is BEC?

In this section, we explore the nature of the BEC threat, profile several successful BEC attacks, and look at the cost of BEC incidents.

WHAT IS BEC?

BEC attacks are a specific type of phishing attack. They rely on targeting (i.e., going after a specific person or role type in an organization) and normally seek monetary payment as a direct outcome. Types of BEC attacks include diverting payment on a valid invoice to a fraudulent bank account, submitting a fake invoice for payment, diverting employee payroll to a fraudulent bank account, and using impersonation of senior executives to lend credibility to plausible but irregular requests (i.e., paying a large sum to a new bank account to secure a merger or acquisition target). BEC also includes gift card fraud and romance scams. BEC types of attack have also been called man-in-the-email attacks, email account compromise (EAC), and wire fraud. Employees at all levels of an organization are targeted by BEC attacks.

BEC attacks differ from many other forms of cyberthreats, relying almost entirely on social engineering to trigger human susceptibility to plausible requests. Social engineering tricks include establishing rapport (pretexting), promising personal benefit, and invoking urgency. BEC attacks do not generally carry malware, include weaponized links, or seek to compromise email account credentials. By definition, BEC attacks rely on the compromise of business email—a normal and highly used channel for business communication—by inserting fraudulent email messages into a stream of regular ones. Examples of different types of BEC attacks include:

- **An impersonated email account**
  A threat actor finds out the name of the CFO at your organization from LinkedIn and registers a personal email account in their name with Google or Microsoft. Email messages can then be sent to your accounts department from your.CFOs.name@gmail.com, beginning with a plausible explanation, such as "I'm travelling and don't have access to my corporate email, but could you please wire an urgent payment to XYZ Corp who we are trying to buy."
- **An impersonated domain**
  A threat actor registers a domain name that looks like the domain name of the targeted company or one of their trusted vendors. While the text of the domain is clearly different, many people miss the subtle differences in lookalike domains—microsoft.com versus microsofl.com or amazon.com vs amazom.com. Lookalike domain name variants are hard to spot with only a cursory glance and it is unsurprising that people regularly miss the differences.
- **A compromised email account (the EAC variant of BEC attacks)**
  A senior executive at a vendor company is the victim of a phishing attack that results in the compromise of his or her email account credentials. Until the credential compromise is detected, the threat actor can send email messages impersonating the senior executive—such as new messages requesting payment to a different bank account or re-submitting invoices already sent with new payment details. For organizations using Microsoft 365 or Google Workspace for email, the compromise of account credentials also gives access to the user's documents in OneDrive/SharePoint or Google Drive, which can include invoices or invoice templates that can be altered before sending.

BEC attacks differ from many other forms of cyberthreats, relying almost entirely on social engineering to trigger human susceptibility to plausible requests.

EXAMPLES OF BEC INCIDENTS

There are tens of thousands of successful BEC attacks every year. A minority of these are publicly disclosed and covered in media channels. Three examples are:

- **One Treasure Island**
  The charity in San Francisco paid $625,000 into the wrong bank account after hackers gained access to the bookkeeper's email account and changed the payment details on one invoice and submitted two additional fake invoices.[1] The money was intended to be a loan to a partner to enable a new building project to start for combatting homelessness. The misdirected payments were not detected for a month, the FBI declined to investigate, and One Treasure Island did not recover the funds. For a charity with revenue of only $2.4 million in 2019, the lost payments represent a sizeable proportion of overall revenue.

- **Scott County Schools**
  The school district paid $3.7 million into a cybercriminal's bank account after receiving change of bank account details by email. The incorrect payment was discovered two weeks after the fact when the vendor who should have been paid asked why their payment was overdue.[2]

- **America's Cup Event Limited**
  The event arm of Team New Zealand paid $2.8 million NZD (about $1.85 million USD) into a cybercriminal's bank account in Hungary. The threat actor used an email address from a lookalike domain name to request that the payment on an invoice due to the real contractor in Europe be paid to a new bank account.[3]

Several companies have lost tens of millions of dollars to BEC scams, including Scoular Corporation ($17.2 million in 2014),[4] Ubiquiti Networks ($46.7 million in 2015),[5] and Xoom Corporation ($30.8 million in 2015).[6] One of the most expensive—and extensive—BEC scams cost Google and Facebook a combined $120 million.[7] Advanced BEC attacks often rely on extensive attempts at obfuscation, including the use of a network of fake companies and multiple bank accounts.[8]

THE COST OF BEC ATTACKS: A CUMULATIVE VIEWPOINT

Wider research beyond our survey offers evidence for the generalized high cost of BEC attacks. For example:

- **Almost 20,000 complaints in the United States in 2020 costing $1.8 billion**
  In the United States, BEC attacks rank at the most expensive type of the 33 categories of internet crime tracked by the FBI.[9] For 2020 (the latest year for which full data is available), the FBI received almost 20,000 complaints of successful BEC scams, with losses of more than $1.8 billion. This was 43% of the total cost for all internet crime types reported to the FBI, and over three times more costly than the second most expensive type of internet crime. The average direct cost of each BEC attack was $96,372, or around 85% higher than the direct cost estimated from our survey (see page 6). The 2020 numbers were up significantly from the $215 million in losses and 2,126 incidents recorded by the FBI from October 2013 to December 2014.[10]

- **95% of BEC attacks cost between $250 and $984,855**
  Drawing on a global data set, Verizon's Data Breach Investigations Report for 2021 found that 95% of BEC attacks cost between $250 and $984,855 per incident.[11] That means 2.5% of incidents cost less than $250, and 2.5% cost more than $984,855 per incident.

In the United States, BEC attacks rank as the most expensive type of the 33 categories of internet crime tracked by the FBI.

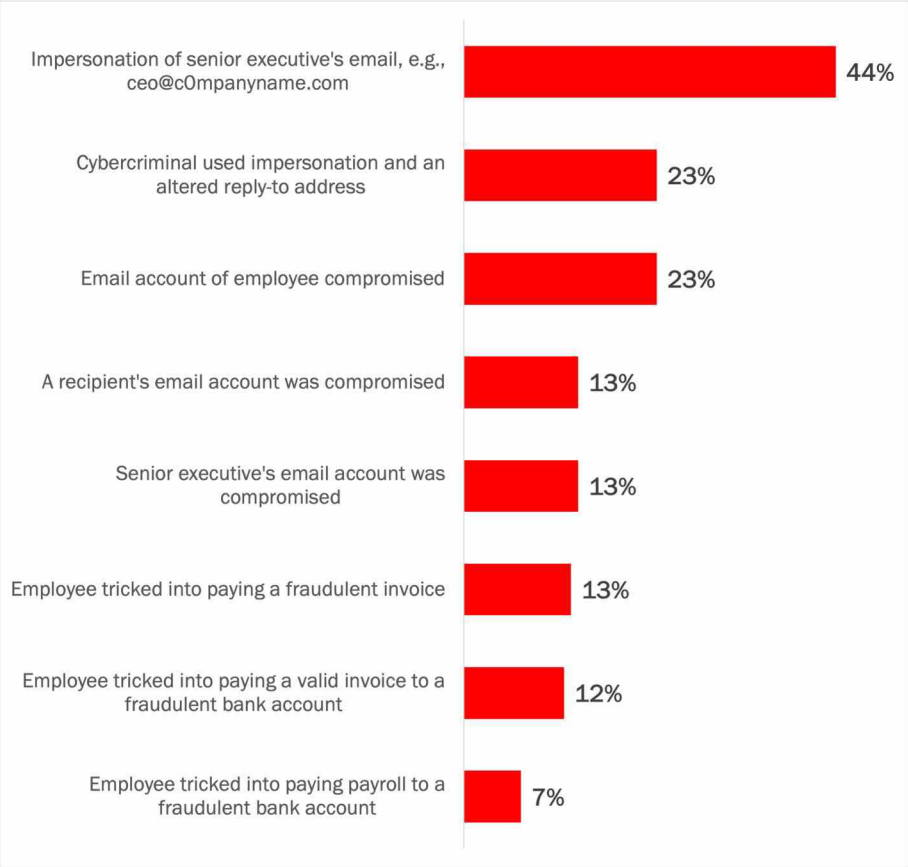
Organizations Are Ill-Prepared for BEC

BEC is a threat to many organizations, yet most are ill-prepared to deal with it. In this section we investigate the evidence.

MOST ORGANIZATIONS ARE ALREADY SUBJECT TO BEC ATTACKS

An average of four out of five organizations have experienced one or more types of BEC-related security incidents during the previous 12 months, with almost 90% of mid-size organizations (500 to 2500 email users) experiencing or more incidents. The most common incident is a BEC attack against the organization that uses an email account impersonating a senior executive, for example, ceo@c0mpanyname.com or ceo1@gmail.com. These attacks rely on impersonation using either freely available email services (e.g., Gmail) or easily obtainable lookalike domain names. BEC attacks that originated from a senior executive's actual email account due to compromised credentials occurred much less frequently (at 13% of organizations compared to 44% of organizations for an impersonated address), reflecting the reality that an impersonated address is much easier to obtain than a compromised account. Out of three types of BEC attacks that resulted in funds being paid on a fraudulent basis, the two types of invoice fraud occurred about twice as often as payroll fraud. See Figure 1.

Figure 1
Cybersecurity Incidents in 2021
Percentage of respondents experiencing each type of BEC attack



Source: Osterman Research (2022)

BEC attacks that rely on an impersonated address for a senior executive are much more common than attacks relying on the use of compromised credentials.

MANY ORGANIZATIONS ARE LOSING MONEY DUE TO BEC ATTACKS

Almost three-fifths of organizations reported being victims of a successful or almost successful BEC attack. On average, the number of BEC attacks that reached one of three states at these organizations over the past 12 months were:

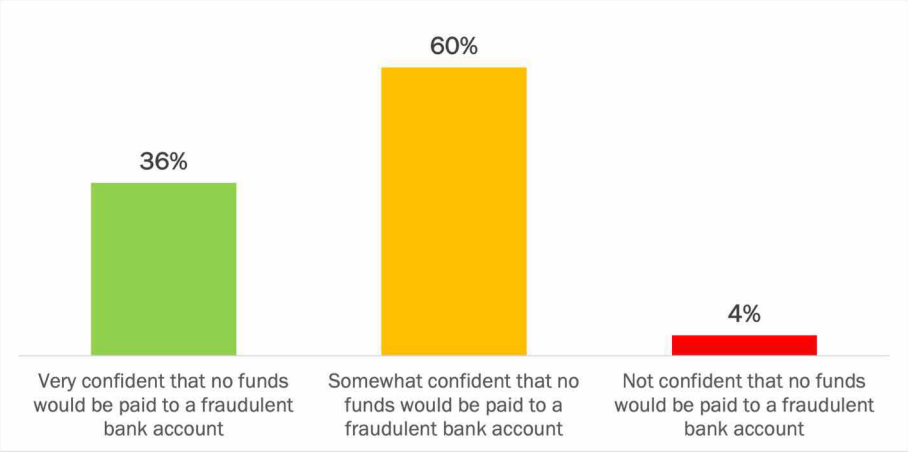
- **Number of attacks that were almost successful**
  7.4 attacks per organization—an employee almost sent funds after getting tricked by a BEC attack, but the incident was caught within the organization before the funds were sent.
- **Number of attacks that failed due to luck**
  4.5 attacks per organization—an employee was tricked, the funds were sent, but the funds were returned by a lucky chance, such as the criminal's bank account being flagged for fraud or closed.
- **Number of attacks that succeeded and the funds were not recovered**
  2.2 attacks per organization—an employee was tricked, the funds were sent, and the funds were not recovered.

Two-fifths of organizations reported that no BEC attacks reached any of these three states (36%) or gave no response to this question (6%). With the prevalence of BEC attacks across organizations and industries, we are inclined to interpret these answers as non-disclosure rather than zero incidents.

MOST ORGANIZATIONS ARE UNSURE OF THEIR ABILITY TO SAFEGUARD FUNDS AFTER A BEC ATTACK

Two-thirds of organizations do not have high confidence that a BEC attack "tomorrow" would result in no funds being paid to a fraudulent bank account. The majority of this grouping have a "somewhat" level of confidence, and the remainder have no confidence. See Figure 2.

Figure 2
Confidence that a BEC Attack Would Not Result in Funds Being Paid to a Fraudulent Bank Account
Percentage of respondents



Source: Osterman Research (2022)

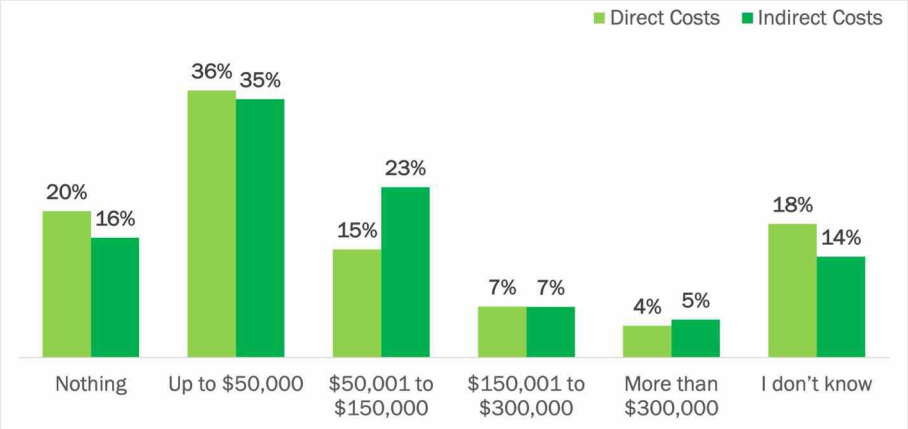
64%

Organizations that are at best only somewhat confident that a BEC attack would not result in funds being paid to a fraudulent bank account

BEC ATTACKS INCUR A PESKY LEVEL OF COST

Organizations anticipate the indirect costs of a successful BEC attack would outstrip the direct costs of an invoice being paid to a fraudulent bank account. The direct cost is the amount of the lost funds, while indirect costs include post-mortem incident response, lost productivity, and compliance violation penalties. Over a third of respondents expect direct and indirect costs to be up to $50,000. In comparison to direct costs, more respondents expect indirect costs to be in the $50,001 to $150,000 and more than $300,000 cost brackets, and fewer expect indirect costs to be nothing or unknown. See Figure 3.

Figure 3
Estimated Direct and Indirect Costs of a Successful BEC Incident
Percentage of respondents



Source: Osterman Research (2022)

This distribution of expectations gives a conservative weighted average of $52,115 of direct costs and $62,607 of indirect costs per incident, or a total of $114,762 per successful BEC incident. Based on the average distribution of incidents per year, therefore, the average amount at risk from BEC attacks per organization is $1.6 million per year. This is comprised of:

- **Cost at risk from attacks that were almost successful**
  $849,239 for 7.4 attacks per organization that were caught by organizational processes.
- **Cost at risk from attacks that failed due to a lucky chance**
  $516,429 for 4.5 attacks per organization that were paid but the money was returned by a lucky chance. When the lucky chance fails, however, these funds are more likely to be lost too.
- **Cost of attacks that succeeded and the funds were not recovered**
  $252,476 for 2.2 attacks per organization that were paid, and the funds were not recovered.

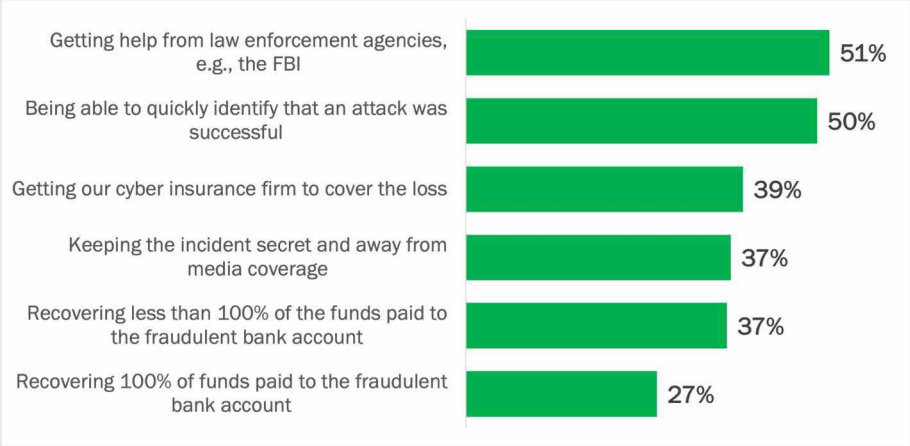
This level of cost is pesky in the sense that individual incidents may cost too little to trigger help from law enforcement agencies and insurance companies, but multiple attacks in combination represent a costly incursion on corporate funds.

Individual BEC incidents often cost too little to trigger help from law enforcement agencies and insurance companies.

MOST ORGANIZATIONS ARE NOT CONFIDENT IN RECOVERY OUTCOMES

Organizations do not expect much good news if they were hit with a successful BEC attack "tomorrow" that resulted in funds being paid to a fraudulent bank account. In general, organizations have a low level of confidence in their ability to achieve a range of satisfactory outcomes following a successful attack. The two outcomes that garnered the highest levels of confidence were discovery outcomes—i.e., getting help from law enforcement agencies (51% of respondents were "confident" or "highly confident") and being able to quickly identify that the attack was successful (50%). Organizations had a lower level of confidence in outcomes focused on recovering from the attack, such as the return of the lost funds or cyber insurance coverage for the loss. Between two-thirds and three-quarters of organizations expect to be on their own following a successful BEC attack. See Figure 4.

Figure 4
Confidence in Achieving Discovery and Recovery Outcomes After a BEC Attack
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2022)

The ability to recover 100% of funds paid to a fraudulent bank account is the outcome with the lowest confidence level. Only one in four believe they could recover 100% of funds. For the others, there is a foreboding sense of "the money is gone and not coming back." This is consistent with several of the examples quoted above, e.g., One Treasure Island, Scoular. Some organizations have been successful in recovering a portion of the lost funds, e.g., Ubiquiti Networks was able to quickly recover $8.1 million of the $46.7 million and had another $6.8 million under protection, but did not know how it would recover the final $31.8 million.

73%

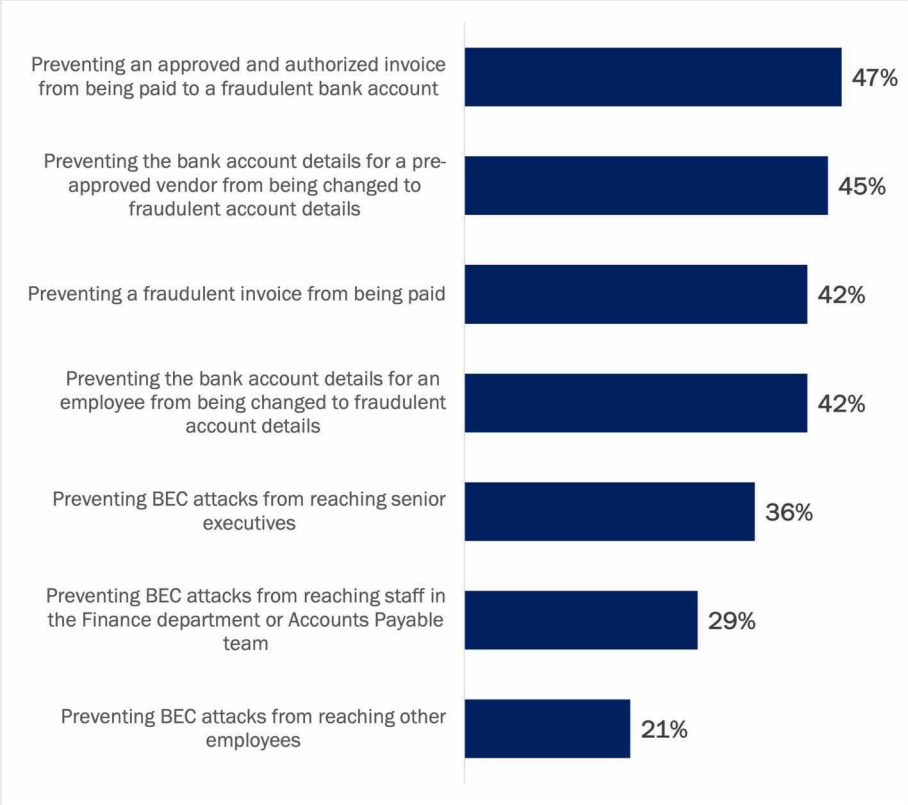
Organizations that are not confident in their ability to recover 100% of funds paid to a fraudulent bank account after a BEC attack

ORGANIZATIONS ARE RELYING ON INSUFFICIENT CYBERSECURITY PROTECTIONS

Cybersecurity solutions and approaches provide protections to organizations against BEC threats. The use of appropriate cybersecurity solutions should enable organizations, in turn, to achieve a range of beneficial outcomes, including safeguarding funds, preventing potential human error, reducing the number of threats being presented to employees, and assuring the integrity of other organizational processes.

Organizations have a low level of confidence that their current cybersecurity protections can achieve the seven beneficial outcomes about which we queried in the survey. Between one-half and four-fifths of organizations lack confidence in the current protections to offer safeguards against BEC attacks. The outcomes that combine people, process, and technology factors achieved the highest levels of confidence (albeit low) among the seven outcomes we asked about—e.g., 47% of respondents were "confident" or "highly confident" that an approved and authorized invoice would not be paid to a fraudulent bank account. The outcomes that rely on technology alone received the lowest levels of confidence. See Figure 5.

Figure 5
Confidence in the Sufficiency of Current Cybersecurity Protections
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2022)

71%

Organizations that cannot rely on current technology solutions to stop BEC attacks from reaching Finance and Accounts Payable staff

The last three items in Figure 5 indicate that the traditional technical solutions organizations are currently relying on are insufficient in the fight against BEC attacks. For instance:

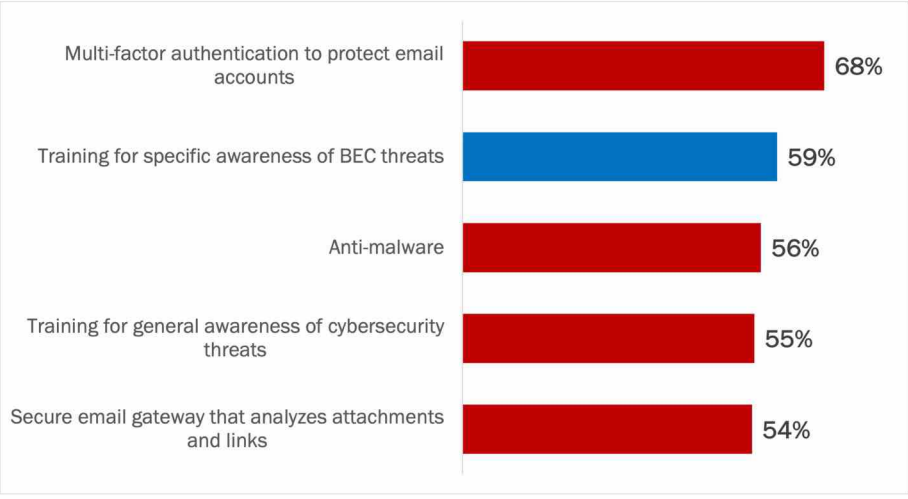
- **BEC attacks against senior executives**
  Only 36% of respondents believe they can stop BEC attacks from reaching senior executives—i.e., that currently deployed traditional technical protections can identify, block, or quarantine BEC threats arriving by email.
- **BEC attacks against finance and Accounts Payable staff**
  Only 29% can stop BEC attacks from reaching staff in the Finance department or Accounts Payable team who are commonly targeted by BEC attacks.
- **BEC attacks against employees in general**
  Only 21% can stop the flow of BEC threats against employees in general.

These data points in combination present a concerning situation.

The traditional technical solutions that are currently deployed are insufficient because organizations are relying on cybersecurity solutions and approaches that are ineffective against BEC attacks. Two of the top five protections rated highly for effectiveness offer little to no value in protecting against BEC. Both anti-malware (rated by respondents as 56% effective, in third place) and a secure email gateway (54%, fifth place) focus on identifying and blocking malicious content and code in messages, attachments, and links rather than identifying malicious intent. Both protections are essential components in a wider cybersecurity posture for addressing other types of email-borne threats, but are ineffective against BEC attacks specifically. The only approach in the top five that specifically focuses on addressing BEC threats is employee training (which 59% of respondents say is "effective" or "extremely effective")—which is an essential component of an anti-BEC security posture but does not enact any effective technical protections to reduce the number of BEC threats from getting through to employees. See Figure 6.

Organizations are relying on cybersecurity solutions and approaches that are ineffective against BEC attacks.

Figure 6
Efficacy of Solutions and Approaches in Protecting Against BEC Attacks: Top Five
Percentage of respondents indicating "effective" or "extremely effective"

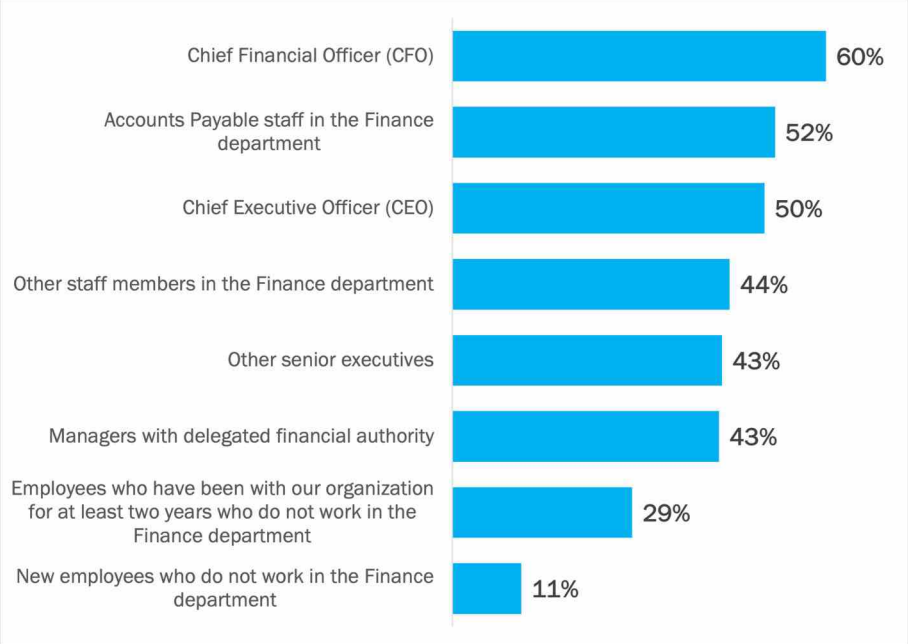


Source: Osterman Research (2022)

ORGANIZATIONS CANNOT RELY ON KEY PEOPLE OR GROUPS TO RECOGNIZE BEC ATTACKS

Three-fifths of respondents are "confident" or "highly confident" that their CFO could recognize a BEC attempt, and one half have the same confidence that accounts payable staff in the finance department could do the same. These are the two most likely individuals or groups to receive a BEC attempt—directly from a threat actor or indirectly from another employee who was originally targeted by the threat actor—that could result in a payment on a fraudulent basis. While these levels of confidence are higher than for the other individuals and groups we asked about, it reflects that many organizations lack such confidence in these key players. Preparedness of the human shield against BEC attacks is lacking. See Figure 7.

Figure 7
Confidence in the Ability of Groups and Individuals to Recognize BEC Attacks
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2022)

48%

Organizations that are not confident that Accounts Payable staff in the Finance department can recognize a BEC attack

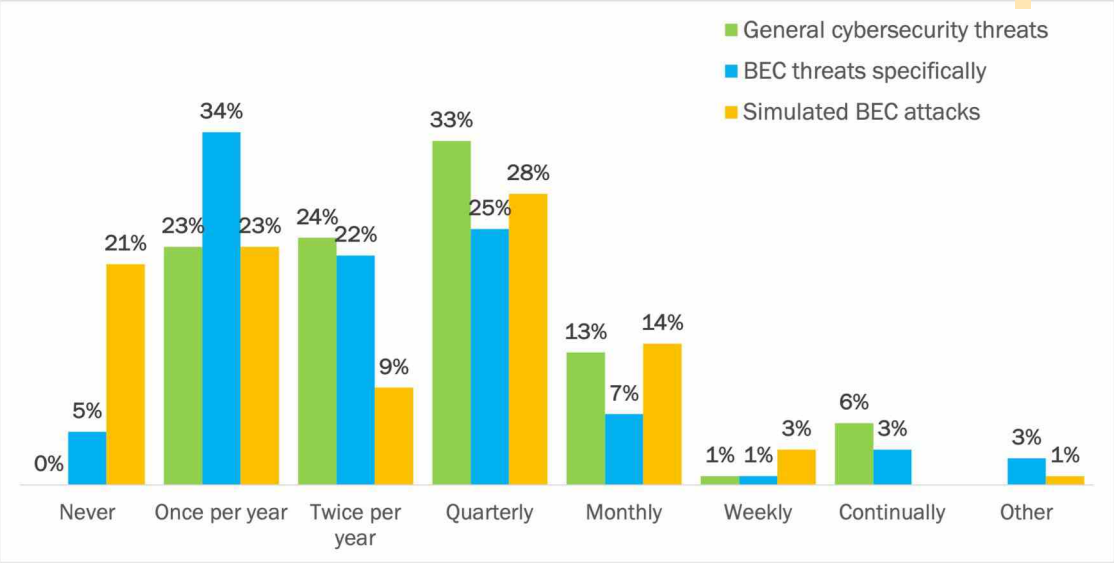
While some BEC attacks can be easily identified through poor spelling, bad grammar, and other visual indications that the message does not come from the person who claims to have sent it, other BEC attacks include none of these easy signals. For example, it is more difficult to identify a BEC threat when a threat actor has compromised a vendor's email account and replies to a current conversation about payment of an invoice. Likewise, BEC threats that come from lookalike domains hosted on highly reputable email infrastructures, such as Microsoft 365 and Google Workspace, are difficult to identify with only a cursory glance, especially if the message has been written by a native language speaker.

In addition to reliance on ineffective cybersecurity tools, there are two reasons why organizations appear to be unable to rely on key people and groups to recognize and prevent BEC attacks:

- **Current training is too infrequent**
  Four-fifths of organizations offer training on general cybersecurity threats only quarterly or less frequently. Training specifically for BEC threats and the use of simulated BEC attacks to gauge anti-BEC efficacy is offered even less frequently. See Figure 8.
- **Current training is ineffective**
  Three-fifths of organizations say their current training approaches for general cybersecurity threats and BEC specifically are at best only somewhat effective. See Figure 9.

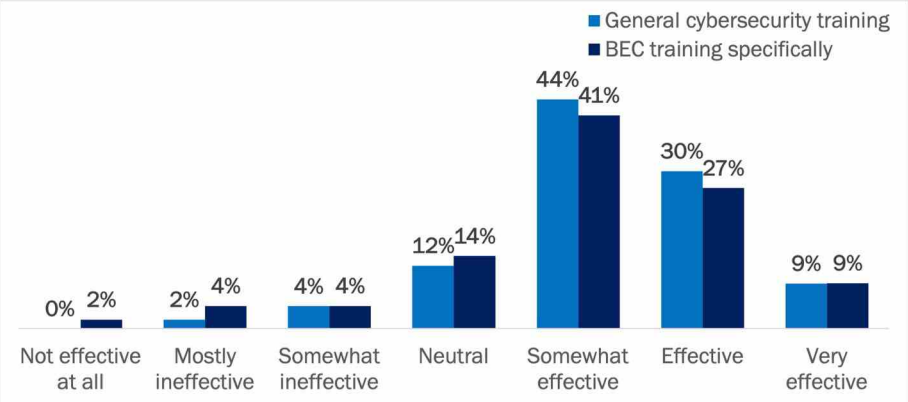
Organizations are not training employees frequently or effectively enough on BEC threats.

Figure 8
Frequency of Offering Employee Training on Cybersecurity in General and BEC Threats Specifically
Percentage of respondents



Source: Osterman Research (2022)

Figure 9
Effectiveness of Current Employee Training on Cybersecurity in General and BEC Threats Specifically
Percentage of respondents



Source: Osterman Research (2022)

The Outlook for BEC

Being able to merely ask for funds has proven to be a financially lucrative strategy for cybercriminals to earn a fast payback for their malicious deeds. Social engineering requests for funds bypass the need to develop malware, keyloggers, ransomware, and other examples in the cyberthreat arsenal. In this section, we look at how BEC is expected to change over the next two years.

LOW PREPAREDNESS EQUALS AMPLE OPPORTUNITY

Our survey results have shown that organizations are ill-prepared to meet the threat of BEC attacks. This is shown in the following:

- **Low readiness across many dimensions**
  Organizations lack strong confidence in their ability to safeguard funds after a BEC attack or to achieve discovery and recovery outcomes. Traditional technology solutions that are currently deployed are viewed as ineffective in stopping BEC attacks from getting through to the key people and groups targeted by many BEC attacks.
- **Reliance on ineffective tools that cannot address BEC attacks**
  Many organizations claim that several cybersecurity solutions and approaches are highly effective against BEC attacks and yet indicate low confidence in the ability of their currently deployed traditional solutions to protect against BEC attacks. There appears to be a misplaced reliance on more general cybersecurity solutions that by design are not intended to protect against BEC threats, such as anti-malware tools and secure email gateways that analyze links and attachments for evidence of malicious code.
- **Low confidence in enlisting help from law enforcement**
  Only half of organizations have high confidence in their ability to enlist help from law enforcement agencies after succumbing to a BEC attack (whether this is an accurate assessment or misplaced confidence is questionable). One Treasure Island, the charity in San Francisco mentioned earlier, was unable to secure help from the FBI, despite repeated requests and despite the amount of the funds at stake representing 15% of the value of their monetary assets. If law enforcement agencies are unwilling to help with lower-value BEC attacks—which will often be the case given insufficient staffing for the volume of incidents—then organizations are left to their own devices to fend off attackers leveraging BEC attacks for quick financial gain.
- **Low confidence to receive insurance coverage for BEC losses**
  Three-fifths of organizations are not confident in their ability to secure insurance coverage for losses due to a BEC incident. In the wider context, insurance coverage is increasingly difficult to secure, especially due to the growing incidence of costly ransomware attacks.[12] Insurance companies are increasing premium rates and decreasing coverage maximums.

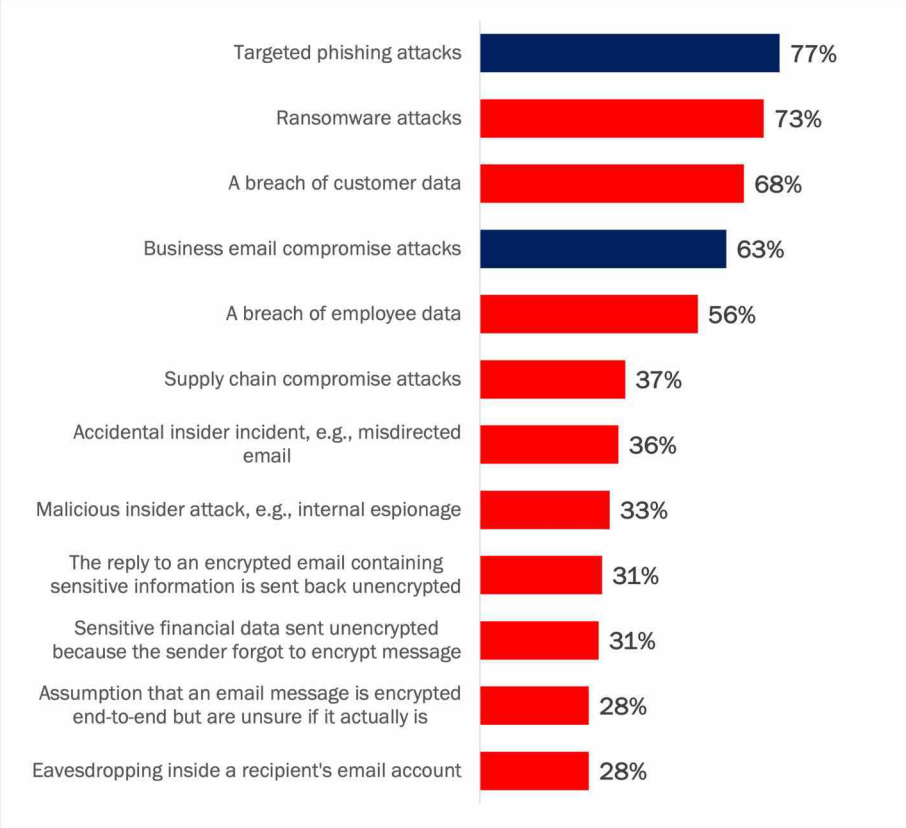
The conflation of these factors creates a perfect storm where threat actors are likely to step up the frequency and cost of BEC attacks. It is unlikely that we have seen the peak of BEC attacks yet, either in number of incidents or overall losses to the economy.

Being able to merely ask for funds has proven an effective strategy for cybercriminals to earn a fast payback for their malicious deeds.

ORGANIZATIONS ARE CONCERNED ABOUT BEC ATTACKS

Two of the top four types of cyberattacks that organizations are most concerned about involve targeted attacks by email, with targeted phishing attacks ranking first (77% of respondents are "concerned" or "extremely concerned") and business email compromise attacks ranking fourth (63%). Ransomware ranks in second place (73%), and a breach of customer data in third place (68%). The level of concern felt for targeted phishing and business email compromise attacks is higher than supply chain compromise attacks (e.g., SolarWinds-style attacks), two types of insider attacks, and several issues related to the use or non-use of email encryption. See Figure 10.

Figure 10
Level of Concern About Types of Cyberattacks
Percentage of respondents indicating "concerned" or "extremely concerned"



Source: Osterman Research (2022)

Phishing attacks have been widely implicated as the initial threat vector for a range of subsequent cyberattacks, including ransomware[13] and breaches of customer and employee data (e.g., through account credential compromise providing access to email accounts, confidential files, and cloud services). BEC attacks are a subset of targeted phishing attacks that focus on direct theft of financial resources.

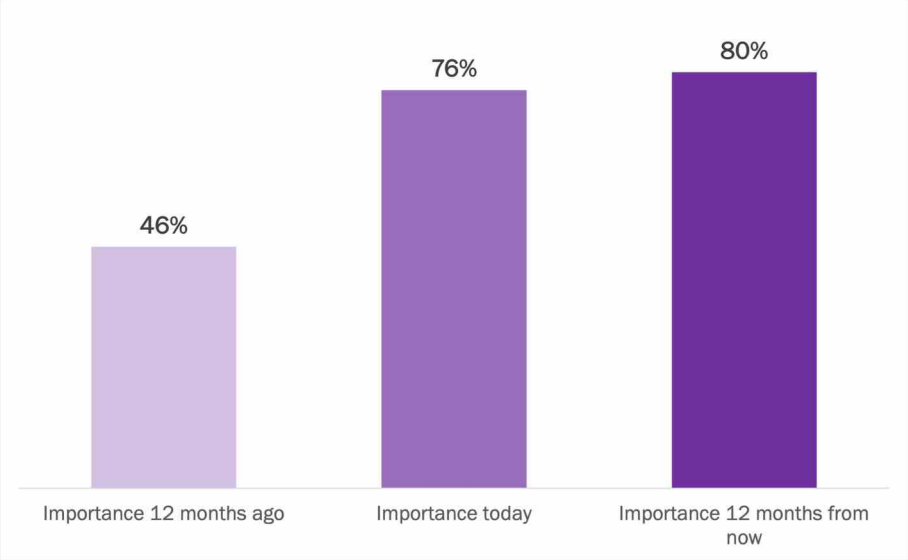
2/4

Two of the top four types of cyberattacks that organizations are most concerned about involve targeted attacks by email.

ORGANIZATIONS VIEW PROTECTING AGAINST BEC ATTACKS AS INCREASINGLY IMPORTANT

Respondents see an increasing need to protect their organization against BEC attacks, with the importance of these protections almost doubling over a two-year timeframe. The largest stepwise change in importance has been from 12 months ago (46% of respondents said such protections are "important" or "extremely important") to the level of importance today (76%). A further small change in importance is expected over the next 12 months (to 80%). See Figure 11.

Figure 11
Importance of Protecting Against BEC Attacks: Three Year View
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2022)

This elevation in importance is to be expected given the growing frequency and cost of BEC attacks, along with the overall poor state of preparedness to counteract such attacks.

80%

Organizations indicating that protecting against BEC attacks in 2022 is of high importance

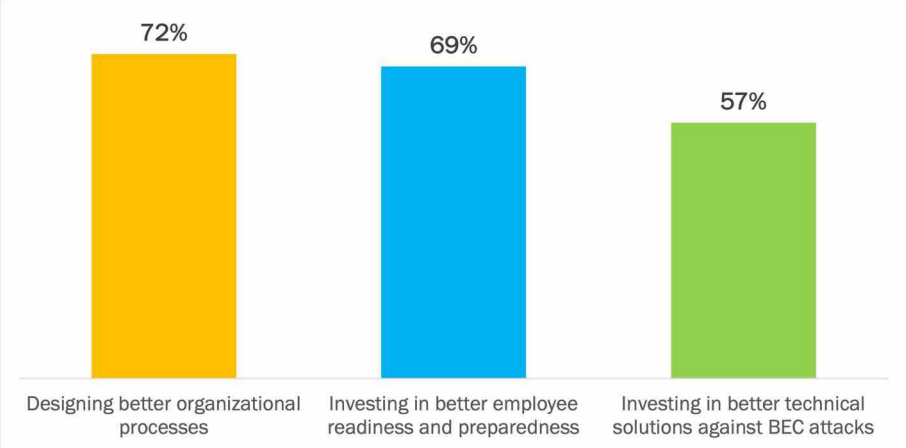
Solutions to Protect Against BEC

Deploying the right cybersecurity protections against BEC is essential. In this section, we look at solutions to protect against BEC threats.

IMPORTANCE OF THREE CATEGORIES OF PROTECTIONS

Protecting against BEC attacks relies on three categories of protections: people, process, and technology. Respondents see organizational processes as the most important category of protections (72% said such protections were "important" or "extremely important"), followed closely by employee readiness and preparedness (69%). Technical solutions were in third place (57%). See Figure 12.

Figure 12
Relative Importance of People, Process, and Technology in BEC Protections
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2022)

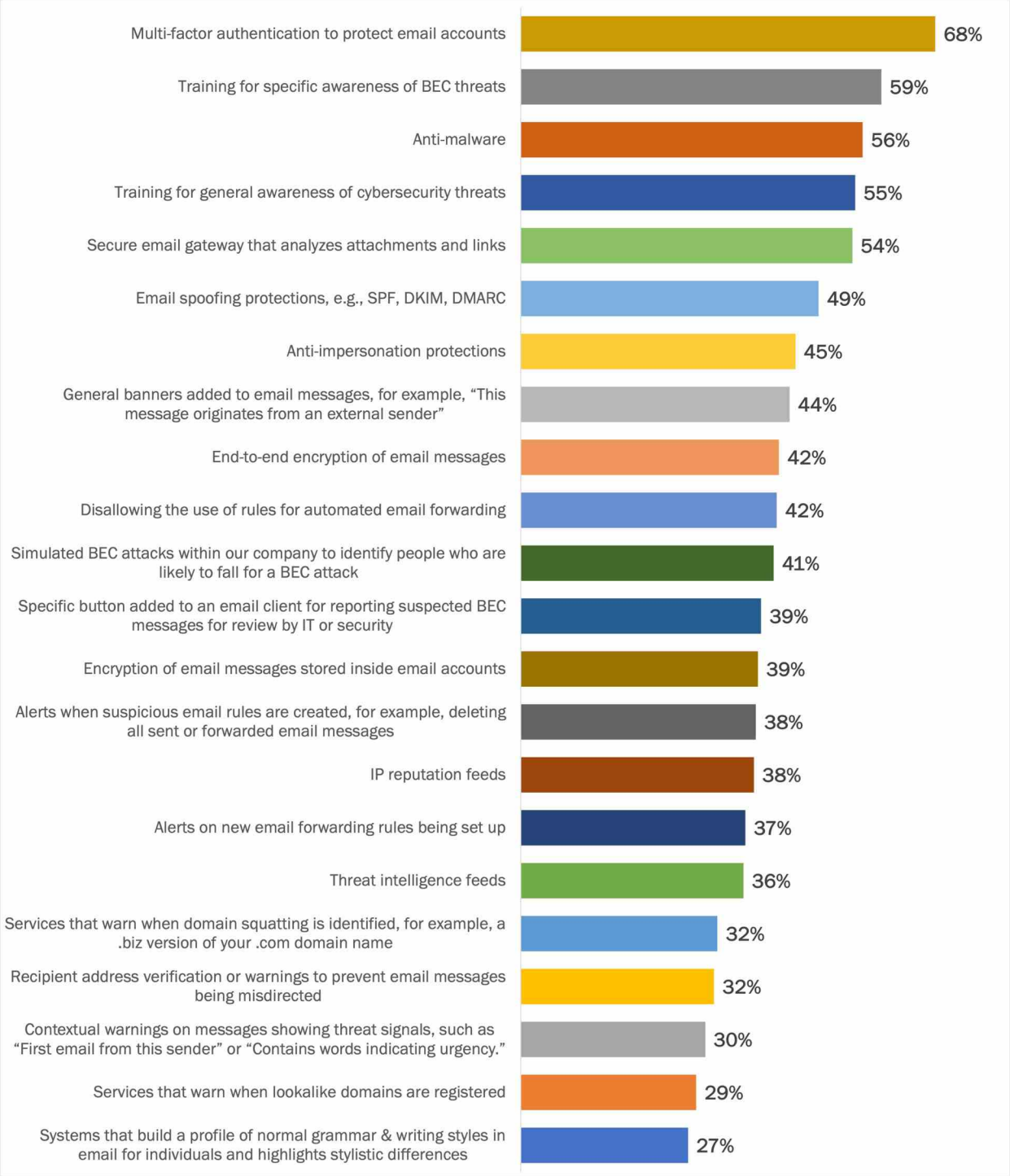
While the relative importance weighting varies between the three categories, none stand alone. Technical solutions that block or identify BEC attacks provide signals to employees who need to be trained to look for highlighted and other hidden signals, and both culminate in how organizational processes are designed to function. When great technology is used by well-trained people according to optimal process designs, the likelihood of identifying and defeating BEC attacks is high. When any category is operating below standard, the other two must work much harder to achieve the same level of efficacy, if that is even possible.

When great technology is used by well-trained people according to optimal process designs, the likelihood of identifying and defeating BEC attacks is high.

EFFICACY OF SOLUTIONS AND APPROACHES TO PROTECT AGAINST BEC

Figure 13 shows how respondents ranked the efficacy of the various solutions and approaches they are currently using in counteracting BEC attacks.

Figure 13
Efficacy of Solutions and Approaches in Protecting Against BEC Attacks
Percentage of respondents indicating "effective" or "extremely effective"



Source: Osterman Research (2022)

LOW EFFECTIVENESS VERSUS LOW ADOPTION?

Several newer types of solutions and approaches that offer specific and targeted protections against BEC attacks received low ratings for effectiveness in Figure 13. We see two potential explanations:

1. **Newer solutions are ineffective**
   Newer solutions have been widely adopted and respondents have found these to be ineffective against BEC attacks.
2. **Newer solutions are not widely adopted**
   Newer solutions have not yet been widely adopted, and therefore the level of experience with these newer solutions is low.

While both explanations could be true, the wider survey data indicates the second is more likely to be correct. Throughout the survey, respondents repeatedly said that their current technical solutions were ineffective against a variety of BEC attack types, and have rated both anti-malware and a secure email gateway as two of the most effective protections against BEC. This does not make sense. These protections by design cannot provide high efficacy against BEC attacks.

IDENTIFYING MALICIOUS INTENT THROUGH ANTI-IMPERSONATION, EMAIL SPOOFING, AND OTHER CONTEXTUAL ABNORMALITIES

BEC messages do not usually include strong threat signals such as malicious code, weaponized documents, or nefarious links. Instead, they seek to hide malicious intent within benign requests. Counteracting BEC threats requires solutions that can aggregate and correlate weak threat signals from multiple systems. These include:

- Anti-impersonation protections for identifying masquerade attempts.
- Checking for misalignment in underlying email settings to identify spoofing attempts. SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting and Conformance) are three basic controls for increasing the authenticity of email. SPF defines trusted email hosts, DKIM uses cryptography for signing messages, and DMARC defines what organizations should do when receiving email with suspicious authentication attributes. Email messages that exhibit inconsistencies between these three controls are more likely to be fraudulent.
- Technologies that can analyze the authenticity of the sender, message content and attachments, and authorship.
- Systematic alerting of untimely or abnormal email forwarding and auto-filing rules. Such rules are frequently created when an email account is compromised and thus provides signaling of nefarious activity.
- Capabilities which identify abnormalities in conversational tone, historical communication patterns, and underlying network usage.
- Brand monitoring services that warn of domain squatting and the registration of lookalike domain names.
- Services that check the age and provenance of a domain to identify risky domains.

The aggregation and correlation of these individual weak threat signals enables greater accuracy in identifying and neutralizing BEC attempts.

Counteracting BEC threats requires solutions that can aggregate and correlate weak threat signals from multiple systems.

GRAMMATICAL ANALYSIS AND DETECTION OF STYLISTIC VARIATIONS

While some phishing and BEC messages give off easy warning signals by using poor spelling and grammar, more advanced BEC threats are carefully crafted to align with the normal writing style of the compromised user. This makes it increasingly difficult for people to distinguish valid from fake email messages. Some vendors offer technology that builds a baseline pattern of language, grammar, writing style, and spelling usage per individual that is applied to current and future messages to highlight the anomalies.

CONTEXTUAL WARNINGS ON MESSAGES SHOWING THREAT SIGNALS

An in-line warning in an email message that tells the recipient a message originated from outside their organization is a common example of surfacing hidden technical attributes about the message in a user-friendly way. For counteracting BEC attacks, however, this warning is insufficient. Since almost all valid vendor email originates from outside the organization, the inclusion of this general warning does not help an employee targeted by a BEC attack to differentiate a valid vendor email from an impersonated one.

Some vendors include more advanced in-line warnings in email messages that surface insights on communication patterns and message construction that are better designed to warn employees of BEC threats. Examples include:

- **Warning when an email message has unusual address characteristics**
  BEC attacks can include abnormal address characteristics, such as when a cybercriminal alters the reply-to address of an email message so it will be sent to a different address than the address it purports to come from. An in-line warning such as “this email will be sent to someone you have never communicated with before” alerts the recipient to exercise caution.
- **Warning when an email is received from a new sender**
  Masquerade attempts that combine a sender’s name that the recipient normally interacts with and an impersonated address can be detected through in-line warnings, e.g., “this is the first email received from this sender.”
- **Warning when an email message includes common social engineering tricks**
  Requests for urgency and secrecy are two frequently used social engineering tricks. In-line coaching and awareness on the presence of such tricks in an email message can be signaled through warnings such as “this message contains words that indicate urgency.”

Vendors that can detect multiple warning signals and abnormalities in an email message can automatically quarantine suspected BEC messages before they reach a user’s inbox.

End-to-end encryption implements security controls on messages and attachments during both transmission and storage.

END-TO-END ENCRYPTION OF EMAIL MESSAGES

End-to-end encryption implements security controls on messages and attachments during both transmission and storage, as well as offering identity verification of the sender. Email messages with end-to-end encryption are unreadable by threat actors if an email server is hacked or accessed through a vulnerability, or if an email administrator’s account is compromised and used for lateral movement attempts. End-to-end-encryption solutions also provide senders with the option of enforcing encryption at rest for messages they send to ensure lifecycle protections, so that confidential and sensitive data remains encrypted while in the recipient’s inbox.

SPECIFIC TRAINING FOR EMPLOYEES FOR AWARENESS OF BEC THREATS

Many BEC threats use a set of social engineering levers that are different to other types of cyberattacks. While general cybersecurity awareness training helps create a general climate of security preparedness—and is an essential cybersecurity strategy for all organizations—people and groups most targeted by BEC attacks require regular training on the specific characteristics and nuances of BEC. Training interventions specifically focused on BEC should also encompass simulated BEC attacks to assess competence.

TAKE A LAYERED SECURITY APPROACH TO PROTECTING AGAINST BEC THREATS

Protecting against BEC threats requires a layered approach. Multiple layers of BEC protections work in combination to stop threats from reaching end users. Attacks that are not caught by one layer of protection—for example, an anti-impersonation check—can be caught by another layer of protection—for example, new sender or new recipient alert warnings. Layering technical solutions with ongoing training specifically on BEC threats for the people and groups who face a high likelihood of attack—as well as a layer of hardened organizational processes as we discuss in the next section—offers a set of strong protections that are unachievable using traditional technical solutions and general cybersecurity training.

WIDER CYBERSECURITY PROTECTIONS HELP TOO

Protecting against BEC attacks benefits from specific people, process, and technology interventions, as we have discussed. However, wider cybersecurity protections at an organization helps too. Create an overall cybersecurity posture that elevates protections in general and contributes to reducing the threat of BEC. Two wider cybersecurity protections that specifically benefit BEC are:

- **Protect email account credentials with strong multi-factor authentication**
  Gaining access to email account credentials through password-spray attacks, brute force password attacks, phishing attacks, or keyloggers provides a cybercriminal with an initial foothold for launching BEC attacks. This can include conversation hijacking, altering previously sent invoices, or submitting fake invoices from the compromised account. Reliance on only a username and password for accessing an email account is an invitation for compromise, and newer, modern forms of strong authentication should be preferred. This includes the stronger forms of multi-factor authentication (e.g., authenticator apps, secure hardware tokens), biometrics, and passwordless authentication. Reducing the ease of compromising account credentials increases protections against a range of cyberattacks, including BEC.
- **Monitor for abnormal patterns of login, geography, and network usage**
  Use security monitoring tools to highlight deviations from normal login patterns by users, such as out-of-hours logins, logins from geographical regions where the user is not located nor visiting, and usage of dark web networks. Login attempts with abnormal attributes can give early warning of targeted attacks against individuals, attempts to break into accounts, or compromised account credentials.

Reliance on only a username and password for accessing an email account is an invitation for compromise.

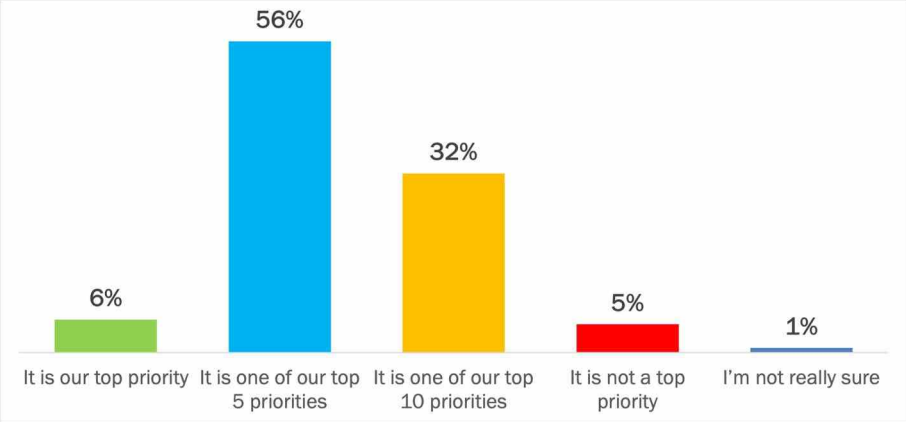
Best Practices Against BEC Attacks

In this section, we look at several best practices for protecting against BEC attacks.

ACT ON THE PRIORITY OF PROTECTING AGAINST BEC ATTACKS

Three-fifths of organizations view protecting against BEC attacks as one of their top five priorities relative to all other security priorities, and another third place it in their top-10 list. See Figure 14.

Figure 14
Priority of Protecting Against BEC Attacks Relative to All Security Priorities
Percentage of respondents



Source: Osterman Research (2022)

In other recent surveys by Osterman Research, respondents have assigned high priority to implementing zero trust,[14] discovering sensitive data,[15] preventing data exfiltration,[16] and assessing the extended cybersecurity threat surface for organizations with subsidiaries.[17] Across multiple separate surveys, therefore, respondents are indicating heightened focus on initiatives to improve baseline cybersecurity protections.

Given the commonality of BEC attacks and the cumulative number and cost of incidents seen each year, including protecting against BEC threats as a top-10 priority appears a fair response. In addition, given the general low state of current preparedness across multiple dimensions, a specific focus on BEC is more than appropriate. We encourage organizations to act on the heightened priority assigned to protecting against BEC attacks.

62%

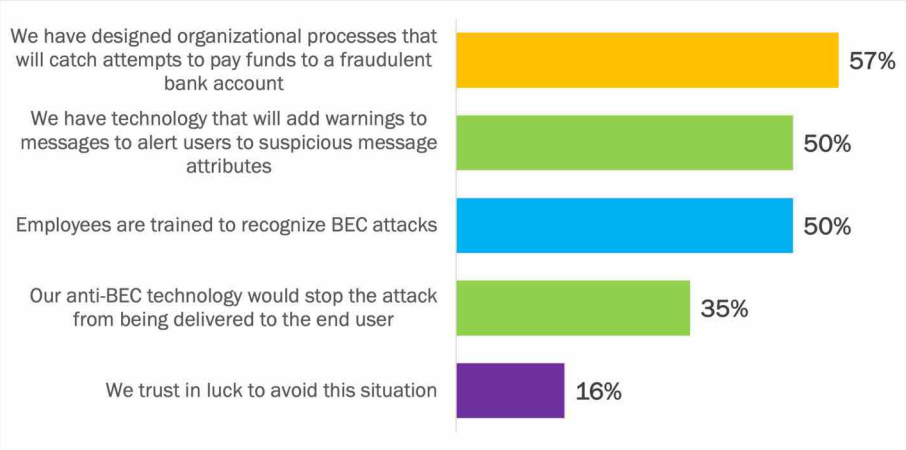
Organizations ranking protections against BEC attacks as one of their top five priorities.

STRENGTHEN INEFFECTIVE PROTECTIONS

Many of the traditional technology protections and financial process designs organizations are using against BEC threats fail to inspire confidence in their ability to identify and prevent BEC threats from becoming costly incidents. Organizations need to strengthen protections that are currently ineffective.

For example, respondents indicated that designing organizational processes to catch attempts to pay funds to a fraudulent bank account, using methods such as pre-authorized banking details for vendors or a multi-person review of requests to change bank account details, is currently the single most influential factor in ensuring that no funds would be paid. Warnings added to messages to alert users of suspicious message attributes and training employees to recognize BEC attacks rated in second equal place for influence. Organizations that cannot rank these factors as highly influential have more work to do. See Figure 15.

Figure 15
Relative Influence of Various Factors in Safeguarding Funds in a BEC Attack
Percentage of respondents indicating "influential" or "extremely influential"



Source: Osterman Research (2022)

Only 35% of respondents indicated that the anti-BEC technology they are currently using for stopping BEC attacks from being delivered to end users would be "influential" or "extremely influential" in preventing the payment of funds to a fraudulent bank account. This reflects the challenge of accurately identifying malicious intent in messages that do not include attachments or links with malicious content, code, or behavioral attributes. For many organizations, the anti-BEC technology they are currently using for stopping the delivery of BEC attacks is insufficient, and any BEC threats that are delivered to an inbox must then rely on people or process for identification and neutralization. We have already explored the need for organizations to select and deploy much more effective anti-BEC technology to protect against BEC attacks, and organizations that lack sufficient protections need to address this shortcoming.

65%

Organizations where currently used anti-BEC technology would probably not stop a BEC attack from being delivered to an end user

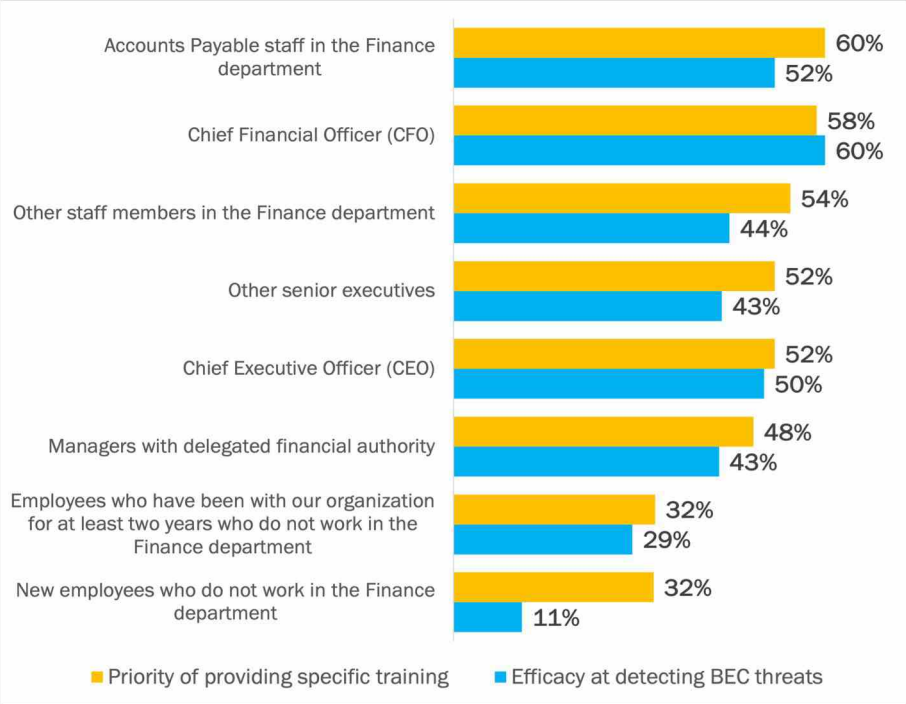
ELEVATE EMPLOYEE PREPAREDNESS

Individuals in a small range of job roles are likely to be targeted by a disproportionate share of BEC attacks because they are high-value targets for a threat actor. This includes employees who have authorization to change bank account details for vendors, and employees or managers who can approve invoices for payment. Accounts and identities belonging to senior executives are also of high value for initiating attacks with higher-value compromise. On the other hand, smaller BEC attacks can be initiated against any manager or employee with a corporate credit card, e.g., the gift card BEC scam where an employee is asked to buy gift cards on behalf of a manager and send the gift card numbers by email. Not providing targeted training on BEC threats increases the likelihood of BEC attacks being successful, and in some cases, the lack of training has shifted the balance of blame from the employee to the employer.[18]

Figure 16 compares the priority of providing training to various people and groups specifically on BEC threats with their corresponding efficacy at detecting BEC attempts. Except for the CFO role, efficacy always trails priority by a few percentage points, indicating that increasing the priority (proxied by frequency and intensity of effective training) has a flow-on effect to efficacy at detecting BEC. The other takeaway from Figure 16 is that the efficacy of employees at detecting BEC based on currently used training approaches is not as high as it needs to be. Organizations should evaluate alternative training approaches to increase detection efficacy.

Targeted training for employees and managers on BEC attacks strengthens the organization's defenses against the threat of BEC.

Figure 16
Priority on Providing Cybersecurity Training Specifically on BEC Threats to Various People and Groups and Efficacy at Detecting BEC Threats
Percentage of respondents indicating "priority" or "essential priority" and percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2022)

Training approaches that increase detection efficacy are likely to have the following characteristics:

- **More than only infrequent classroom training or on-demand online training**
  Both classroom training (which has become more difficult to offer during the pandemic and with remote and hybrid work designs) and online training are helpful for establishing the context of BEC threats and the types of incidents commonly seen within a given organization. However, such training can only be offered infrequently and outside normal routines of communication. More effective training approaches complement these baseline modes with newer approaches to elevating employee preparedness.
- **Add alerts to suspicious email messages to provide in-context warnings**
  The concept of people, process, and technology offering protections against BEC attacks is best understood in complementary and interrelated terms, rather than as standalone and isolated protections. Adding alerts to suspicious email messages is an example of technology and people factors complementing each other—potential threat signals identified by anti-BEC technology are surfaced to the end user to provide a context warning and in-the-moment coaching. Alerts of this nature translate the concepts of BEC protections into specific instances within normal routines of communication.
- **Test at-risk groups and individuals through simulated BEC attacks**
  Simulated BEC attacks provide an opportunity to assess the efficacy of different groups and individuals at detecting and neutralizing BEC attacks. Low efficacy scores indicate the need for additional interventions such as more training, enhanced in-context warnings, and additional hardening of key processes.

BUILD THE CULTURAL SUPPORT FOR CONFIRMING REQUESTS WITH EXECUTIVES

It is important that the corporate culture of an organization does not magnify the problem of BEC. For example, if senior management discourages any sort of pushback on their orders, a CFO or HR clerk might be less likely to question a request for a wire transfer or provision of confidential records received in a BEC attempt purporting to come from the CEO. Building the cultural support for assessing the validity of messages that could be valid or a BEC attack includes:

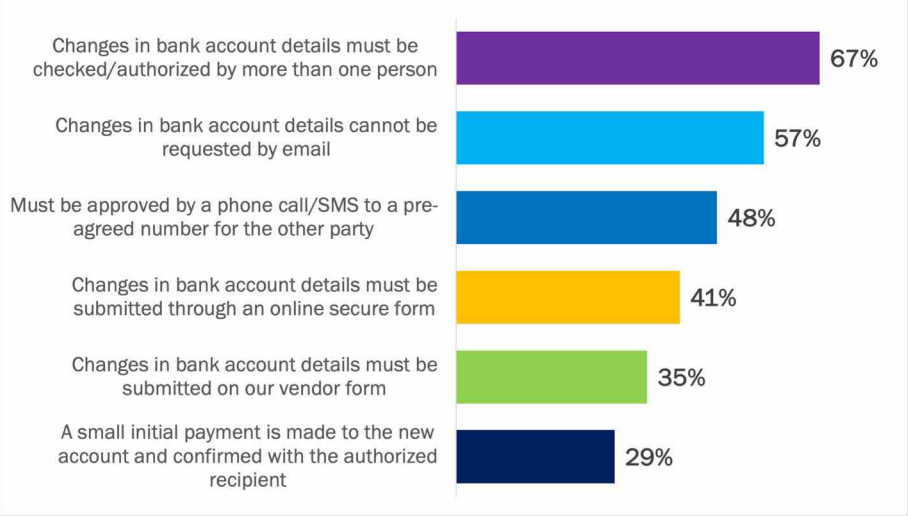
The corporate culture of an organization can magnify the problem of BEC.

- **Document expectations for confirming requests in the employee handbook**
  Designing strong financial processes is an essential task in safeguarding funds, reducing fraud, and establishing normal operating parameters for an organization. The employee handbook should explain how financial controls are implemented within the organization and include details on how requests can be confirmed. It is beneficial if the employee handbook also states that senior executives will never request urgent transfers from personal email accounts, only their official business email account.
- **Executive assistants need to be part of the solution**
  Senior executives face a deluge of requests by email and phone, and many rely on an executive assistant to triage their email inbox and incoming calls to identify priority issues, handle routine requests, and schedule meetings. When an employee seeks confirmation of an out-of-the-ordinary request that feels to them like a BEC attack, it is likely to be handled by an executive assistant first. The cultural fiber is weakened if employees are made to feel stupid for asking for confirmation of an abnormal request.

HARDEN ORGANIZATIONAL PROCESSES THAT ARE WEAPONIZED FOR INVOICE FRAUD

Organizations have taken several actions to harden processes for changing bank account details for invoices due, with internal multi-person review for any changes the most common action taken (at 67% of organizations), followed by disallowing the use of email for changing bank account details (57%), and approval via phone call or SMS to a pre-agreed number for the other party (48%). Three-fifths of organizations have taken two or three actions in combination to harden invoice payment processes and reduce the likelihood of these being compromised through a BEC attack. See Figure 17.

Figure 17
Actions Taken to Harden Processes for Changes to Invoices Due
Percentage of respondents



Source: Osterman Research (2022)

Respondents had the option of noting other actions taken as well. Two respondents left notes about other actions, and both focused on identity verification.

However, many organizations have not taken enough actions to harden invoicing processes. Those that lack the more widely adopted safeguards outlined in Figure 17 would be well-advised to step up current protections.

There are also other ways of strengthening internal process controls for financial transactions, but many organizations have shied away from implementing these. For example, requiring alignment between a quote issued by a vendor, a purchase order and number issued by the organization, and the invoice issued by the vendor decreases the likelihood that fake invoices will be authorized and paid. The trifecta benefits internal financial planning and protections, and is also a strong practice for reducing the threat of BEC attacks.

Three-fifths of organizations have taken two or three actions to harden invoicing processes against BEC threats.

HARDEN ORGANIZATIONAL PROCESSES FOR EMPLOYEE PAYROLL

Organizations have also hardened processes for changing bank account details for employees, and the relative ordering of the actions for employees is the same as the vendor list except for the one item. Approval of a change by phone call or SMS to a pre-agreed number for the other party was the third most commonly used approach when dealing with vendors, but is in sixth place for the employee list of actions. Three-fifths of organizations have taken two or three actions in combination to harden employee payroll processes. See Figure 18.

Figure 18
Actions Taken to Harden Processes for Changes to Employee Payroll
Percentage of respondents

Source: Osterman Research (2022)

Respondents had the option of noting other actions taken as well. Two respondents left notes about other actions. The first said that any change "must be done in person," and the second was verification of the request was required but "specifically not [by] phone call or SMS."

As with our recommendation for hardening processes against invoice fraud, organizations still relying on email for changing employee payroll details should adopt several of the more widely used safeguards in Figure 18 above.

Organizations still relying on email for changing employee payroll details should adopt newer anti-BEC safeguards.

Conclusion

BEC is a costly cyberthreat for organizations around the world, and many are ill-prepared with their current people, process, and technology posture to fend off attacks. Many organizations appear to be relying on technology that was not designed to identify and protect against BEC attacks, have people who lack training to recognize and counteract BEC threats, and use weak processes that enable BEC threats to become incidents. Except for BEC incidents at the more costly end of the spectrum, confidence in securing help from law enforcement is low, and gaining insurance coverage for losses is equally problematic. Organizations need to take urgent action to strengthen current processes targeted by BEC, deploy new technology that specifically identifies and neutralizes BEC attacks, and elevate preparedness of executives, managers, and employees to stop BEC in its tracks.

Sponsored by SonicWall

SonicWall is well known for its market-changing Boundless Cybersecurity vision. This approach safeguards organizations with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. Boundless Cybersecurity upends traditional thinking by empowering organizations to know the unknown, unify visibility and control, and disrupt TCO expectations. SonicWall has nurtured a reputation of professionalism, innovation and integrity that spans nearly three decades. SonicWall has helped protect and secure more than 500,000 customers in 215 countries and territories.

Learn more at www.sonicwall.com.

www.sonicwall.com

@SonicWall

+1 888 557 6642

Contact us

---

[1] James Rundle, Hackers Stole $650,000 From Nonprofit and Got Away, Showing Limits to Law Enforcement's Reach, June 2021, at https://www.wsj.com/articles/hackers-stole-650-000-from-nonprofit-and-got-away-showing-limits-to-law-enforcements-reach-11623058201

[2] WKYT News Staff, Scott County Schools Victim of $3.7 Million Scam, April 2019, at https://www.wkyt.com/content/news/Scott-County-Schools-victim-of-37-million-scam-509017341.html

[3] Todd Niall, America's Cup: How Team New Zealand Was Scammed out of $2.8m in Hungarian Fraud, August 2020, at https://www.stuff.co.nz/sport/americas-cup/122595362/americas-cup-how-team-new-zealand-was-scammed-out-of-28m-in-hungarian-fraud

[4] Maria Korolov, Omaha's Scoular Co. loses $17 million after spearphishing attack, February 2015, at https://www.csoonline.com/article/2884339/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html

[5] Krebs on Security, Tech Firm Ubiquiti Suffers $46M Cyberheist, August 2015, at https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

[6] Therese Poletti, The strange case of a money-transfer firm's missing millions, January 2015, at https://www.marketwatch.com/story/the-strange-case-of-a-money-transfer-firms-missing-millions-2015-01-07

[7] FBI, Leader of Fraud Ring Sentenced: Protect Yourself from Business Email Compromise Schemes, January 2020, at https://www.fbi.gov/news/stories/ringleader-of-business-email-compromise-scheme-sentenced-012820

[8] Phil Muncaster, Spanish Police Arrest Three in €10m BEC Bust, October 2019, at https://www.infosecurity-magazine.com/news/spanish-police-arrest-three-in-10m/

[9] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[10] FBI, Business E-mail Compromise, January 2015, at https://www.ic3.gov/Media/PDF/Y2015/PSA150122.pdf

[11] Verizon, 2021 Data Breach Investigations Report, May 2021, at https://www.verizon.com/business/resources/reports/dbir/

[12] Aon, 2021 Cyber Security Risk Report, at https://www.aon.com/2021-cyber-security-risk-report/

[13] Osterman Research, How to Reduce the Risk of Phishing and Ransomware, March 2021, at https://ostermanresearch.com/2021/03/17/orwp_0336/

[14] Osterman Research, Why Zero Trust is Important, November 2021, at https://ostermanresearch.com/2021/11/10/orwp_0348/

[15] Osterman Research, Sensitive Data Discovery Rises as a Top Concern for Organizations, September 2021, at https://ostermanresearch.com/2021/09/22/activenav-sensitive-data-discovery/

[16] Osterman Research, Preventing Data Exfiltration: Introducing Anti-Data Exfiltration (ADX), October 2021, at https://ostermanresearch.com/2021/10/26/orwp_0347/

[17] Osterman Research, Managing Risk from Subsidiaries: Goals, Friction, and Failure, September 2021, at https://ostermanresearch.com/2021/09/23/cycognito-subsidiary-risk/

[18] Ry Crozier, BOQ Tries to Pin BEC Blame on a Branch Manager, February 2021, at https://www.itnews.com.au/news/boq-tries-to-pin-bec-blame-on-a-branch-manager-560557