Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **March 2023**
Commissioned by **IRONSCALES**

Defending the Enterprise: The Latest Trends and Tactics in BEC Attacks

Executive Summary

In our research last year on the business cost of phishing, commissioned by IRONSCALES, we found that IT and security teams spent an average of 27.5 minutes dealing with a single phishing email.[1] In this research, also commissioned by IRONSCALES, we dug deeper into business email compromise (BEC), an extremely costly type of phishing attack. We found that organizations see BEC as twice the problem of phishing in general, and among large organizations, concern with BEC attacks will increase by 43.3% over the next 12 months. Many organizations are over-reliant on technologies with questionable efficacy at addressing the threat of BEC attacks. Confidence in the ability of executives and employees to detect BEC attacks remains low, and new channels are being used as precursors to BEC attacks—increasing the risk footprint. Organizations must re-examine their anti-BEC approach, re-balance their technology strategy, and leverage better signals on BEC threats to target training at the most frequently attacked people and groups.

KEY TAKEAWAYS

The key takeaways from this research are:

- **The threat of BEC is growing year on year and is twice as high as the threat of phishing in general**
  Large organizations anticipate a 43.3% increase in the threat created by BEC attacks in the next 12 months. The threat created by BEC attacks is twice as high as the threat created by phishing attacks in general.
- **Finance employees and C-level executives receive the most BEC attacks**
  At more than half of organizations, finance employees and C-level executives are subject to BEC attacks daily, weekly, or monthly.
- **Fake invoices, data theft, and account takeover are the most common types of BEC attacks**
  One in five organizations have experienced these types of BEC attacks in the past 12 months. Two in three organizations have faced three or more types of BEC attacks over this time. Data theft attacks occur with the highest frequency.
- **Organizations are placing the highest reliance on technologies and solutions with questionable efficacy for protecting against BEC attacks**
  Security awareness training, secure email gateways, and multi-factor authentication are the technologies that organizations rely on the most to protect against BEC attacks. However, each suffer from significant shortcomings that undermine their efficacy at counteracting BEC threats.
- **More organizations should be using AI-powered anti-phishing tools to protect against BEC attacks**
  The technology with the most to offer for detecting and remediating BEC attacks is AI-powered anti-phishing tools, although only 55% of organizations are currently using such tools.
- **Beware emerging precursors to BEC attacks**
  Threat actors are leveraging new channels ("precursors") to engage with executives and employees to set up a BEC attack. Organizations with strong BEC protections that work only in email will be blind to the use of newer precursor attack channels.

Large organizations anticipate a 43.3% increase in the threat of BEC attacks in the next 12 months.

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by IRONSCALES. Information about IRONSCALES and details on the survey methodology are provided at the end of the paper.

The Cost and Variants of BEC Attacks

We look at the cost of BEC attacks in this section, along with the growing number of variants used by threat actors.

BEC ATTACKS ARE VERY COSTLY

BEC attacks have consistently topped the list of most costly crimes in the United States reported to the FBI, even though other types of crimes are more common:

- In 2020, there were 19,369 complaints of BEC schemes that cost $1.8 billion. On average, that's $92,932 per incident. This represented 44% of total crime losses, yet just 2.4% of the total number of crime complaints to the FBI.[2]
- In 2021, the number of complaints about BEC remained about the same (19,954), but the cost increased to $2.4 billion (and the average to $120,276). This represented 35% of total crime losses, and 2.4% of total crime complaints.[3]
- In 2022, both complaints (21,832) and losses ($2.7 billion) from BEC increased compared to 2021. The average cost increased to $125,611 per incident. BEC represented 2.7% of complaints, and 26% of total crime losses.[4]
- In November 2022, the FBI presented a congressional report on BEC and real estate wire fraud.[5] The report was prepared because "BEC is one of the fastest growing and most financially damaging crimes" in the United States, and while addressing BEC is a priority to the FBI, there are several systemic vulnerabilities that make it a difficult crime for the FBI to disrupt.

BEC attacks have consistently topped the list of most costly crimes reported to the FBI.

NEW VARIANTS OF BEC ATTACKS

Fake invoices were the predominant variant of early BEC attacks. Additional variants such as gift card scams and payroll diversion have proliferated over time as threat actors have expanded their toolkits to steal funds in complementary and specialized attacks. This research investigated the following variants of BEC attacks (in alphabetical order):

- **Account takeover**
  A threat actor attempts to gain access to an email account for an employee or executive at a given company.
- **Attorney impersonation**
  A threat actor uses an email account that impersonates an attorney to request fraudulent payments.
- **CEO fraud**
  A threat actor uses an email account that impersonates a senior executive to send emails requesting fraudulent payments.
- **Data theft**
  A threat actor uses email to request access to data they are not authorized to view, resulting in a data breach or data exposure.
- **Fake invoices**
  A threat actor submits a fraudulent invoice for payment or attempts to fraudulently change the payment details on a valid invoice.
- **Gift card scams**
  A threat actor uses an email account that impersonates a manager or executive to request the purchase of gift cards.
- **Payroll diversion**
  A threat actor attempts to submit new payment details to divert an employee's payroll to a fraudulent bank account.

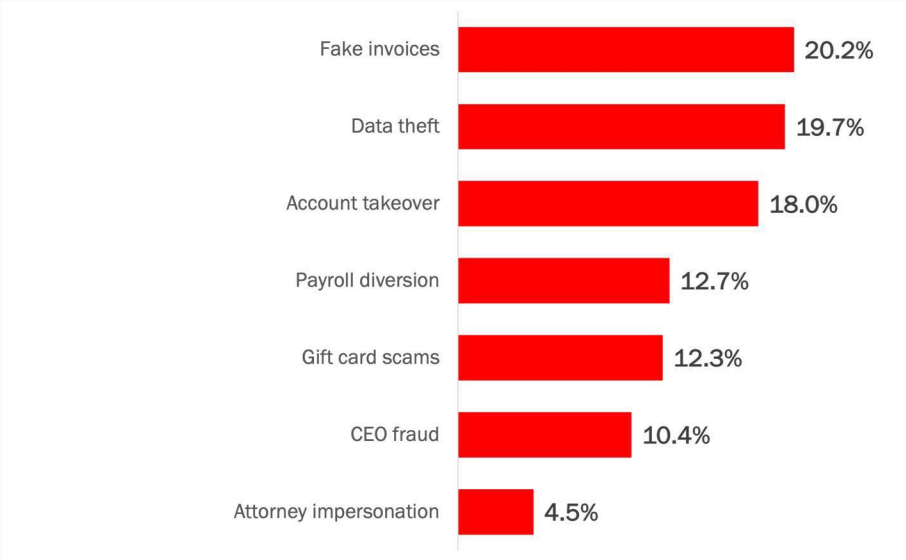
Profile of BEC Attacks

In this section, we investigate what BEC attacks look like for organizations.

ORGANIZATIONS ARE SEEING NEW VARIANTS OF BEC ATTACKS

The organizations in this research indicated that fake invoices are the most common variant of BEC attacks seen during the previous 12 months (at 20.2% of organizations), followed closely by the variants of data theft (19.7%) and account takeover (18.0%). See Figure 1. Over 93% of organizations experienced one or more of the BEC attack variants in the previous 12 months, with 62% facing three or more attack variants over this time. See Figure 2. Increasing variation in BEC attacks requires stronger detection mechanisms.

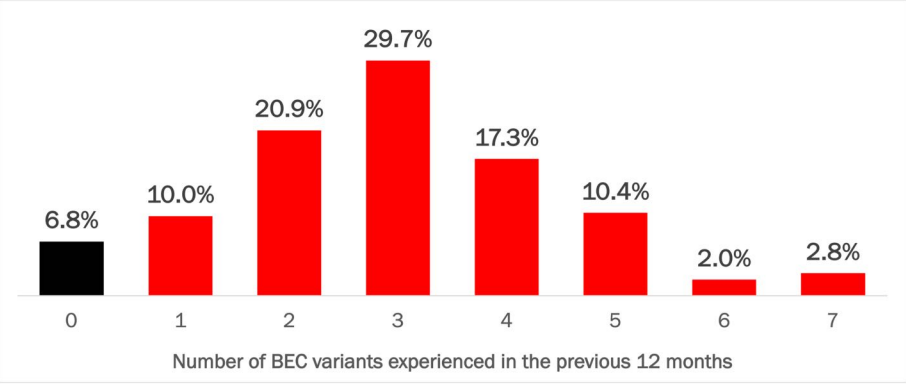
Figure 1
Variants of BEC Attacks in Previous 12 Months
Percentage of respondents



Source: Osterman Research (2023)

62% of organizations have been subjected to three or more BEC attack variants during the previous 12 months.

Figure 2
Variants of BEC Attacks: Count of Variants in Previous 12 Months
Percentage of respondents

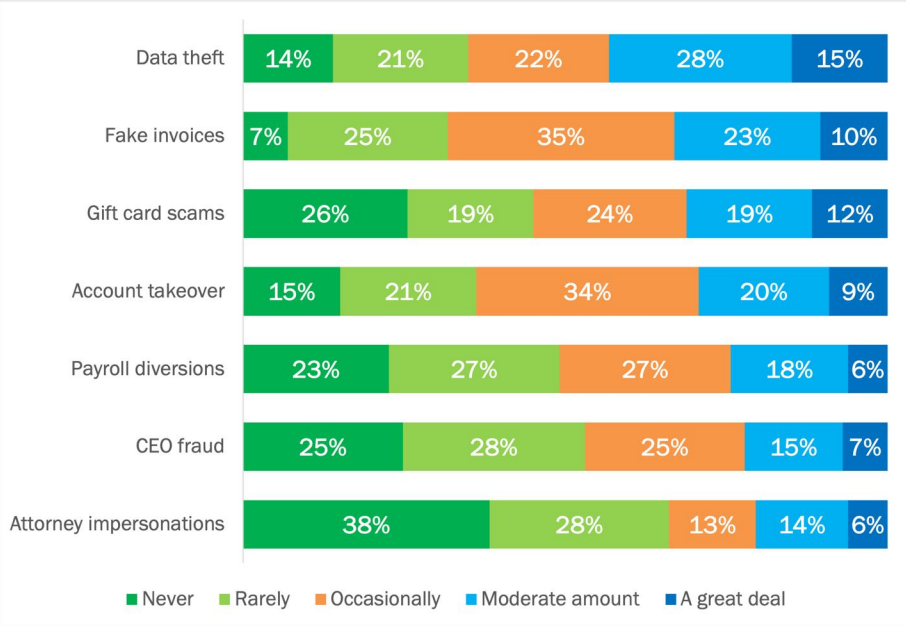


Source: Osterman Research (2023)

BEC ATTACK VARIANTS ARE EXPERIENCED REGULARLY

All BEC attack variants are experienced regularly by roughly a quarter to a half of organizations (where "regularly" is the combination of "moderate amount" and "a great deal"). BEC attacks that result in data theft occur with the highest frequency, followed by fake invoices and gift card scams. See Figure 3.

Figure 3
Variants of BEC Attacks: Frequency
Percentage of respondents



Source: Osterman Research (2023)

Data theft is the most common result from BEC attacks.

CONSEQUENCES OF NOT DETECTING BEC ATTACKS

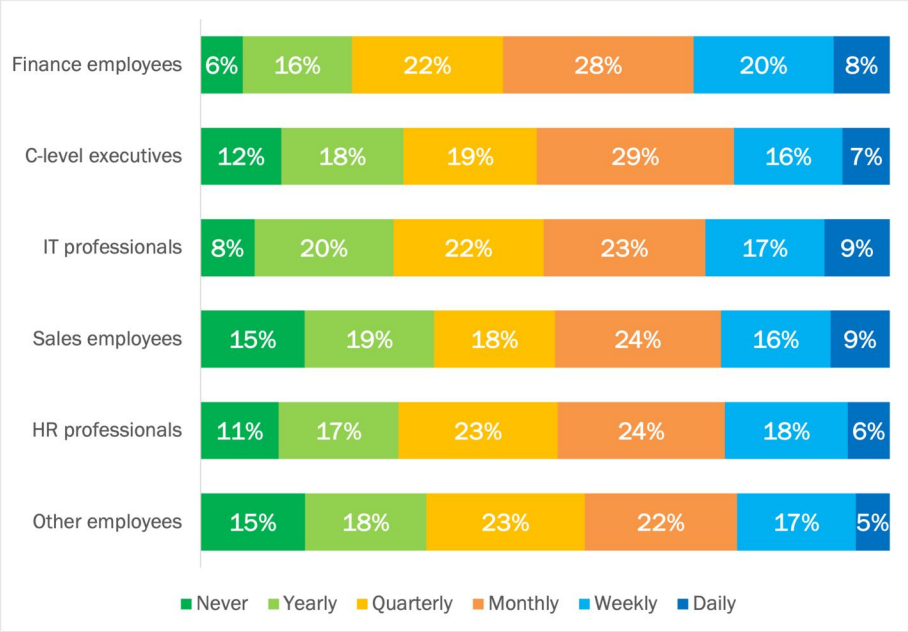
The consequences of not detecting BEC attacks differ by variant. For example:

- **Data theft**
  High-value data such as company strategy details, new product development plans, and other intellectual property can reduce profitability for years. Data covered by regulatory requirements, such as privacy regulations in the United States, Europe, and elsewhere, can trigger data breach notification processes (and associated costs) and regulatory fines.
- **Fake invoices**
  Loss of funds is the direct result of paying a fake invoice (or a valid invoice to the wrong bank account after details have been maliciously changed). The average loss amount varies widely—Verizon says 95% of BEC scams cost the organization between $250 and $984,885[5]—but the outliers can be extremely expensive (e.g., Xoom's loss of $30.8 million to a BEC attack in 2015)[6].
- **Account takeover**
  Account credentials are compromised for theft of valuable data, phishing from trusted accounts that leverages existing relationships, and lateral movement to take over additional accounts. For organizations using Microsoft 365 or Google Workspace, account credentials give access to a whole suite of tools and data, not just email.

MOST EMPLOYEES AND EXECUTIVES EXPERIENCE BEC ATTACKS DAILY, WEEKLY, OR MONTHLY

Finance employees and C-level executives are the two groups subject to the most frequent BEC attacks (manifesting the different variants of BEC attacks noted above), and around half of all groups experience BEC attacks daily, weekly, or monthly. Finance employees are targeted because they have direct access to the systems that can initiate a monetary payment and change bank account details for payroll and vendors. C-level executives are targeted because they have the authority to order a finance employee to make a payment to a specified account, and hence if a threat actor can trick a C-level executive, there is an increased likelihood of receiving a monetary payment. See Figure 4.

Figure 4
Groups Targeted by BEC Attacks: Frequency Distribution
Percentage of respondents



Source: Osterman Research (2023)

Half of all groups experience BEC attacks daily, weekly, or monthly.

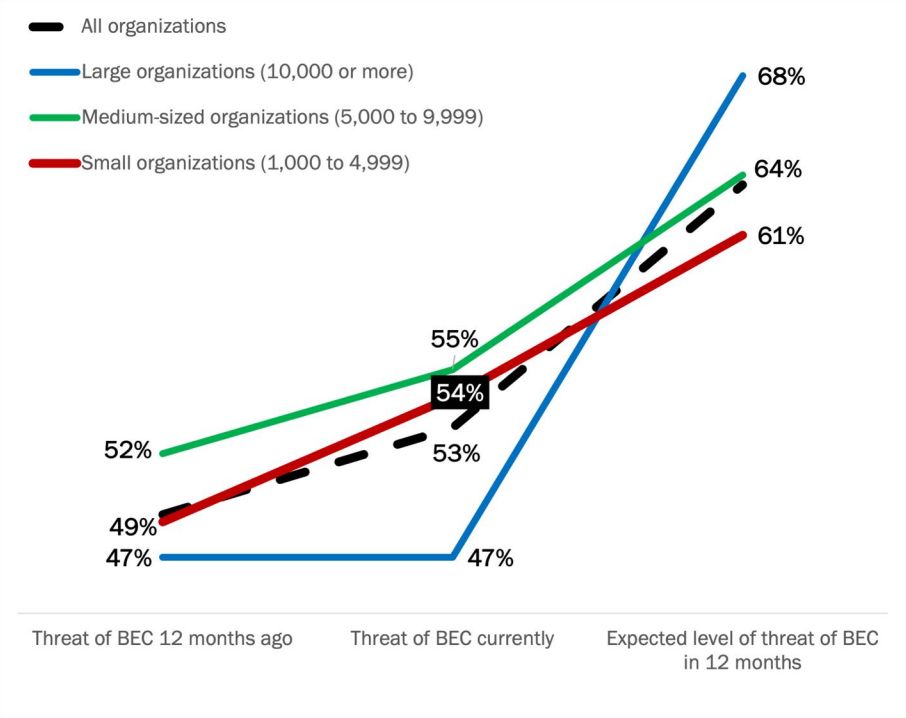
Organizations face the risk of costly consequences from BEC attacks irrespective of the frequency of attacks. That is:

- **Frequent attacks (daily, weekly, or monthly) provide regular exposure to malicious threats and increase the likelihood that one will slip through**
  Employees and executives subject to frequent attacks will ideally develop a sense of what seems out of place by repeated exposure. By observing that attacks happen regularly, employees and executives should be on higher alert for the different variants of BEC attacks. But attacks can still slip through.
- **Less frequent attacks (quarterly or yearly) seek to capitalize on novelty and dulled awareness**
  Employees and executives who are targeted by BEC attacks on a less frequent cadence have fewer opportunities to tune their efficacy at detecting out-of-place messages. They are also more likely to fall for well-crafted BEC attacks that threat actors have taken the time to personalize for the intended victim and sanitized of malicious signals—increasingly with the aid of AI, e.g., ChatGPT.

UNSURPRISINGLY, ORGANIZATIONS SEE BEC ATTACKS BECOMING A MORE SIGNIFICANT THREAT

The perceived threat level of BEC attacks is growing year on year. Large organizations (with 10,000 or more employees) anticipate a 43.3% increase in the threat of BEC attacks in the next 12 months. The overall expected threat level of BEC attacks in the next 12 months is 64%. See Figure 5. This is twice as high as the expected threat level of all types of phishing in 12 months that we found in our research on the cost of phishing last year (34%).[7]

Figure 5
Perceived Threat of BEC Attacks to Organizations
Percentage of respondents indicating BEC attacks "a threat" or "an extreme threat"



Source: Osterman Research (2023)

Respondents at large organizations anticipate the largest overall elevation of threat level over the coming 12 months (with growth from 47% to 68%). Large organizations have the greatest number of variables to control, and thus the greatest likelihood of chaotic results and costly consequences from BEC attacks.

Respondents from small and medium-sized organizations see a lower change in the threat level of BEC over time in comparison to respondents at larger organizations. Costly BEC incidents will still wreak financial havoc and disruption on small organizations, but the amount of money at risk is less than for much larger organizations, thus decreasing the relative attractiveness of small organizations as of financial interest to threat actors. There are also fewer executives and employees in finance roles that need to be on high alert against BEC attacks, compared to medium-sized and large organizations.

The expected threat level of BEC attacks in 12 months is twice as high as the expected threat level of phishing in general in 12 months.

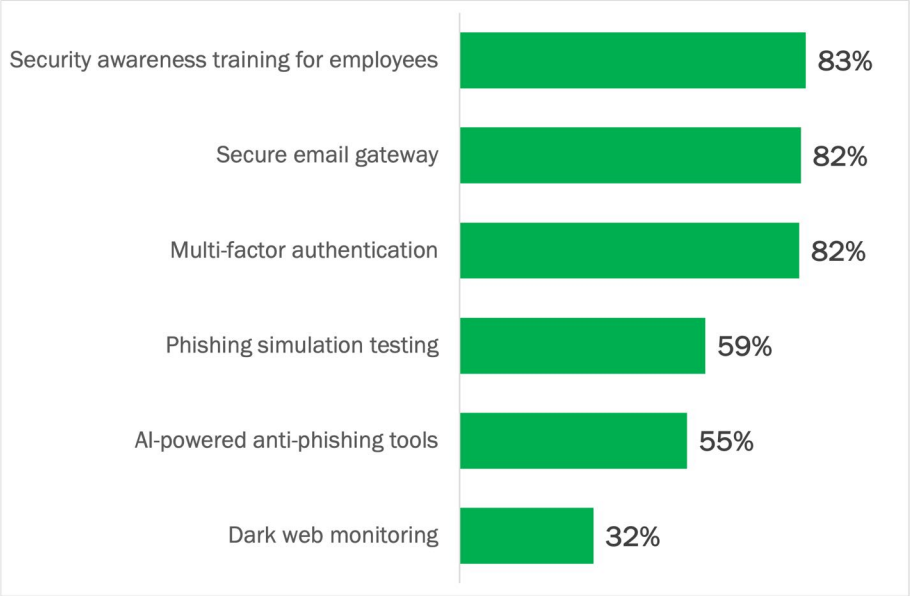
Shortcomings with How Organizations Are Protecting Themselves Against BEC

Current approaches in how organizations are protecting themselves against BEC threats are often ineffective and hampered by systemic shortcomings.

ORGANIZATIONS ARE RELYING ON TECHNOLOGIES AND SOLUTIONS WITH QUESTIONABLE EFFICACY FOR PROTECTING AGAINST BEC

The three most common technologies used for detecting and remediating BEC attacks are security awareness training for employees, a secure email gateway, and multi-factor authentication. In combination, these are used at more than 80% of organizations. See Figure 6. Of the tools below, 87% of organizations are using three or more to protect against BEC attacks, and 59% are using four or more.

Figure 6
Technologies Used for Detecting and Remediating BEC Attacks
Percentage of respondents



Source: Osterman Research (2023)

Organizations are placing the highest reliance on technologies and solutions with questionable efficacy for protecting against BEC attacks.

Organizations are placing the highest reliance on technologies and solutions with questionable efficacy for protecting against BEC attacks. While many of the technologies in Figure 6 offer some level of protection against BEC attacks—and all organizations should be using them in an orchestrated approach—individually, most suffer from shortcomings that undermine anti-BEC protections:

- **Security awareness training: infrequent and ineffective**
  The ability of security awareness training to help executives and employees identify BEC attacks relies on how often the training is conducted and how well it teaches general security principles that enable people to recognize the particular BEC threats. Too many organizations offer security awareness training too infrequently to be of much value, and infrequency also means that examples of current BEC threats are not used to inform the training curriculum.

Executives and employees may be empowered to identify attacks that were in common use three to six months previously, but not current attack patterns.

- **Secure email gateway (SEG): ineffective at detecting malicious intent**
  SEGs have been at the forefront of stopping traditional phishing attacks with malicious content in the form of embedded links, attachments, and code from getting through to inboxes. Stopping these types of threats is critically important, but BEC attacks weaponize intent, not code, attachments, or links. Many BEC emails contain nothing that the detection engines in most SEGs have been programmed to identity.
- **Multi-factor authentication (MFA): beware MFA-aware phishing kits**
  MFA solutions can thwart a threat actor attempting to use compromised credentials to gain malicious access to an account. However, there has been a significant increase in the number of phishing kits available to threat actors that include mechanisms for circumventing MFA, which reduces their systemic efficacy.[8] In addition, if a BEC attack succeeds in tricking an employee to initiate a fraudulent funds transfer, the employee is taking the action and will therefore have access to the required MFA tokens, authenticators, or biometrics—without the threat actor having to compromise them.
- **Phishing simulation testing: signals not certainty**
  Phishing simulations quantify which people and groups remain susceptible to phishing attacks. It shows where more and better training—or technology—is required. However, the efficacy of phishing simulations for BEC attacks depends on the security group acting on the quantified results and offering new training that is effective at upskilling detection abilities (i.e., who needs more testing and training). At minimum, organizations must ensure phishing simulation testing goes beyond general phishing messages to specific BEC simulations for the groups facing the highest frequency of attack. However, competence at detecting phishing simulations is no guarantee that an executive or employee will be able to detect a specific future BEC attack. Phishing simulations offer signals of competence in identifying test messages, not certainty of detection efficacy for real BEC attacks.
- **Artificial intelligence (AI)-powered anti-phishing tools: not used enough**
  The technology with the most to offer for detecting and remediating BEC attacks is AI-powered anti-phishing tools, although only 55% of organizations are currently using these. This type of technology looks for malicious intent hidden in messages that SEGs miss or classify as benign. AI models detect, highlight, and learn subtle discrepancies in communication patterns, language usage, and mail flows, along with the presence of malicious inbox rules and other suspicious activity that triggers elevated warning levels for individual messages. AI models leverage continuous learning from all organizations and environments in which they are used, exponentially improving their ability to detect advanced BEC attacks in any given organization. Organizations using AI can see who is being targeted by BEC threats and customize security awareness training and phishing simulations to match those real-world current threats.
- **Dark web monitoring: susceptibility not specifics**
  Monitoring the dark web can offer early warning signals of an upcoming attack to raise the alert level, but not the specifics of what the attack will look like. Message titles, people being targeted, and date ranges for an attack are less available.

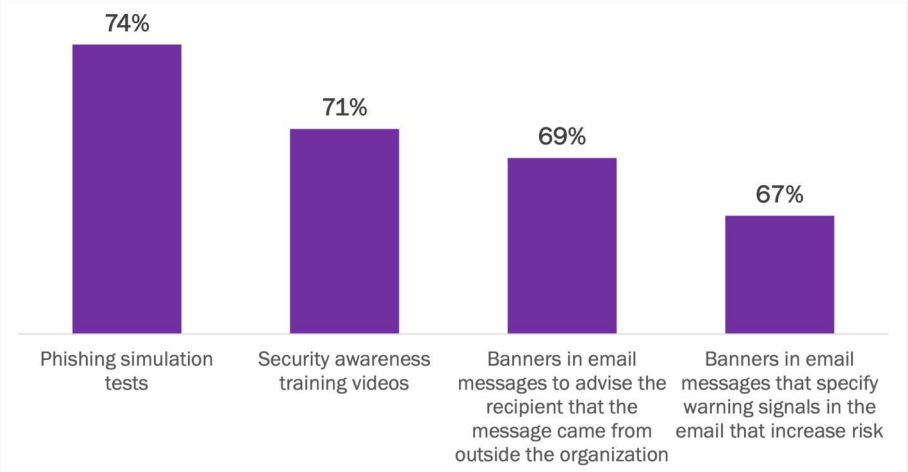
Orchestration and integration across these technologies are key in elevating protections against BEC attacks. From the list above, more organizations should be using AI-powered anti-phishing tools while also improving the efficacy of the others.

Orchestration and integration across technologies are key in elevating protections against BEC attacks. More organizations should be using AI-powered anti-phishing tools while also improving the efficacy of the others.

EDUCATIONAL APPROACHES ARE NOT WORKING WELL

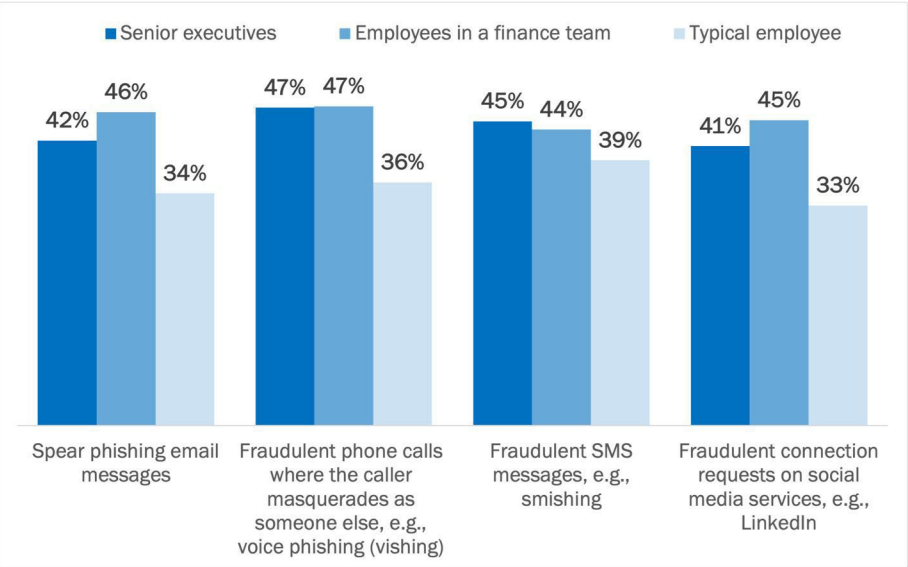
More than two out of three respondents say that multiple educational approaches are highly important for educating employees to detect BEC attacks, with phishing simulation tests rated the most important (74%). See Figure 7. However, despite the importance of these approaches, their usage is not flowing through to high levels of confidence in the detection ability of executives and employees. In no cases are confidence levels for the groupings of executives or employees more than 50%, and for the "typical employees" group, confidence in detection is only 35% on average. See Figure 8.

Figure 7
Importance of Educational Approaches
Percentage of respondents indicating "important" or "extremely important"



Source: Osterman Research (2023)

Figure 8
Confidence in Ability of Executives and Employees to Detect BEC Attacks
Percentage of respondents indicating "confident" or "highly confident"



Source: Osterman Research (2023)

Although organizations are embracing multiple approaches to educate executives and employees on how to detect BEC attacks, confidence in their ability to do so remains low.

THREAT ACTORS ARE WEAPONIZING NEW CHANNELS FOR BEC ATTACKS

Threat actors are leveraging new channels ("precursors") to engage with executives and employees to set up a BEC attack. Spear phishing email messages remain the most used channel for setting up a BEC attack (40% of respondents indicate these are used "almost every time" or "every time"), and fraudulent SMS messages (36%) are not far behind. Interestingly, more than one quarter (28%) of respondents already say that fraudulent connection requests on social media are used frequently during the setup for a BEC attack, and the use of fraudulent phone calls is not far behind (22%). See Figure 9.

Figure 9
Threat Types Used as a Precursor to BEC Attacks: Frequency
Percentage of respondents

Source: Osterman Research (2023)

Organizations with strong BEC protections that work only in email will be blind to the use of newer precursor attack channels. Fraudulent SMS messages, connection requests on social media, and phone calls bypass most of the technology that is used currently to protect against phishing and BEC attacks. This includes bypassing MFA protections, either because the targeted employee falls for the attack and carries out the requested action and meeting the MFA challenges, or because the attackers bombard the employee with MFA prompts which the employee interprets as a system malfunction (as happened at Uber last year).[9] These precursor channels are more personal in nature, precisely targeted at specific individuals, and highlight the importance of training executives and employees to detect such precursors. Relevant security awareness training can certainly help, but ultimately, simulation testing must be extended to incorporate these precursors, something which organizations must address in parallel as vendors uplevel their technology solutions to protect these newer channels.

In Figure 3 (see page 5), an average of one in five respondents indicated they never see the different types of the BEC attack variants at their organization, which could be due to any number of reasons. One possibility is that the organization is not targeted by those attack variants, or alternatively, that the organizations have very high detection efficacy. More likely reasons, however, are to do with a lack of optics to identify attack variants or a lack of disclosure on what is experienced. If lack of optics is the cause, how will organizations detect BEC attacks that leverage newer precursor channels, such as social media and phone calls?

Organizations with strong BEC protections that work only in email will be blind to the use of newer precursor attack channels.

Conclusion

BEC attacks are expected to become much more of a problem over the next 12 months. Newer variants of BEC attacks threaten havoc on organizations and threat actors are leveraging new precursor attack channels to bypass current technology defenses. Organizations must do everything possible to stop BEC attacks from reaching executives and employees because unidentified BEC attacks result in lost data and high financial costs. To get there, organizations must re-examine their anti-BEC approach, re-balance their technology strategy, ensure they are integrated and orchestrated, and leverage better signals on BEC threats to target training at the most frequently attacked people and groups.

About IRONSCALES

IRONSCALES is the leading cloud email security platform for the enterprise that uses machine learning and AI to stop advanced phishing attacks that bypass traditional security solutions. Its award-winning self-learning platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO) and more. As the most powerfully simple email security platform, IRONSCALES helps enterprises reduce risk, boost security team efficiency, and build a culture of cybersecurity awareness.

IRONSCALES is headquartered in Atlanta, Georgia and is proud to support more than 10,000 customers globally.

Visit www.ironscales.com or @IRONSCALES to learn more.

www.ironscales.com

@IRONSCALES

Methodology

This white paper was commissioned by IRONSCALES. Osterman Research surveyed 249 IT and security professionals in the United States in January 2022 on how their organization handled the threat of phishing.

SIZE OF ORGANIZATION

1,000 to 4,999 employees (average 2,058 employees)	53.2%
5,000 to 9,999 employees (average 6,442 employees)	22.6%
10,000 or more employees (average 49,347 employees)	24.2%
Average number of employees across all organizations	14,077

ROLES

IT manager or IT team lead	62%
IT security manager or IT security team lead	20%
Email security manager or email security team lead	9%
Security manager	5%
Email security administrator	2%
SOC analyst	0.8%
SOC manager or SOC team lead	0.4%

INDUSTRY

Financial Services	24%
Computer Hardware or Computer Software	13%
Industrials (Manufacturing, Construction, etc.)	12%
Healthcare	10%
Professional Services (Law, Consulting, etc.)	8%
Retail / eCommerce	7%
Transport, Logistics	6%
Data Infrastructure, Telecom	5%
Education	4%
Energy, Utilities	3%
Public Service, Social Service	3%
Life Sciences	1.2%
Media, Creative Industries	1.2%
Hospitality, Food, Leisure Travel	0.8%
Agriculture, Forestry, Mining	0.4%
Business Services	0.4%
Engineering	0.4%
Accounting	0.4%
Technology	0.4%

---

[1] Osterman Research, The Business Cost of Phishing, October 2022, at https://ostermanresearch.com/2022/10/21/business-cost-phishing-ironscales/

[2] 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

[3] FBI, Internet Crime Report 2021, March 2022, at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[4] FBI, Internet Crime Report 2022, March 2023, at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[5] FBI, FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud, November 2022, at https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view

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

[7] 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

[8] Osterman Research, The Business Cost of Phishing, October 2022, at https://ostermanresearch.com/2022/10/21/business-cost-phishing-ironscales/

[9] Catalin Cimpanu, More than 1,200 phishing toolkits capable of intercepting 2FA detected in the wild, December 2021, at https://therecord.media/more-than-1200-phishing-toolkits-capable-of-intercepting-2fa-detected-in-the-wild/

[10] Jessica Lyons Hardcastle, Uber explains how it was pwned this month, points finger at Lapsus$ gang, September 2022, at https://www.theregister.com/2022/09/19/uber_admits_breach/