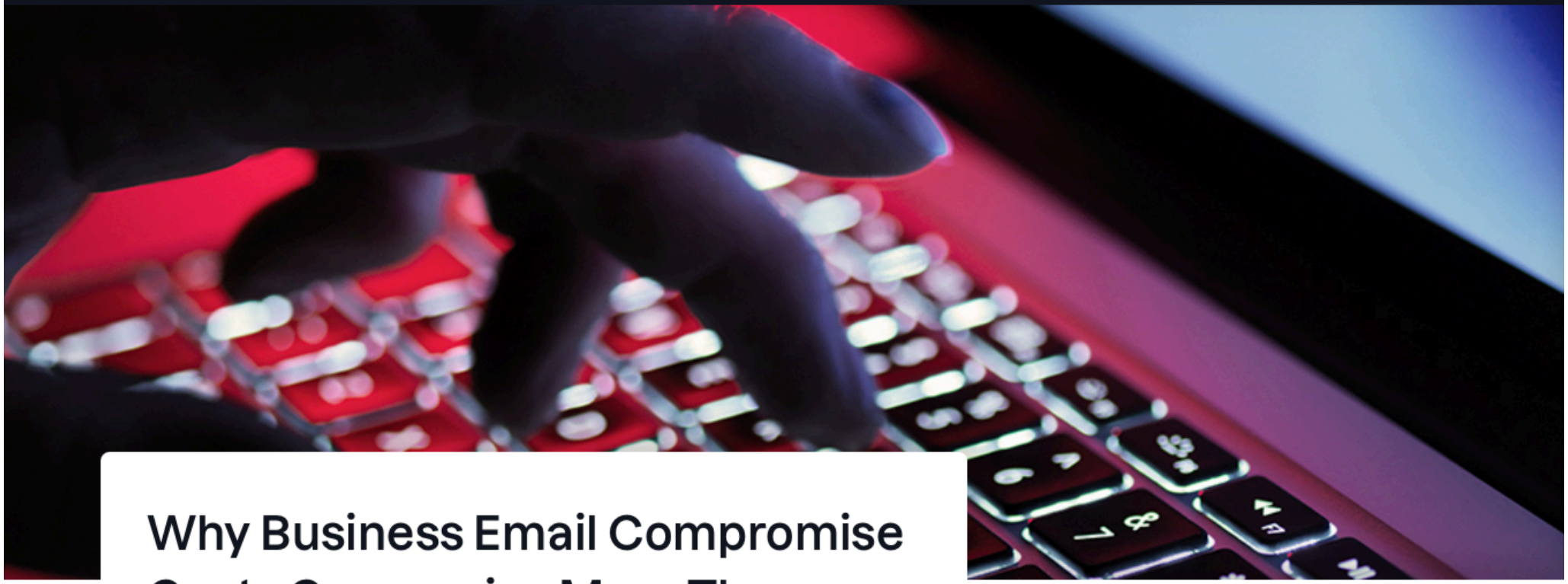

Why Business Email Compromise Costs Companies More Than Ransomware Attacks

Hackers love to trick employees into wiring them money. Here's how to stop them.

Perspective

NOVEMBER 10, 2022

Last fall, a newly hired administrative assistant for a prestigious East Coast law firm received three emails over six months from a partner asking her to wire a total of $240,000 to an outside consultant.

Not wanting to displease one of her superiors, the admin made the transfers. All seemed fine—until a few months later, when it turned out a cyber thief had impersonated the partner and hijacked the money. The firm filed a cyber insurance claim for its losses, but was denied because its employee had not followed an internal dual authentication policy requiring multiple stakeholders to review large transfers.

"New-employee business email compromises like this are unfortunately becoming all too common," says Kirsten Bay, CEO of Cysurance, a cyber insurance agency. "Attackers often watch for new corporate email addresses or social media postings about people starting new jobs. They then digitally impersonate corporate executives, capitalizing on employee reluctance to question the legitimacy of emails from senior staff."

Compare and prescriptively improve your IT risk metrics against your industry peers.

While many organizations today view **ransomware as their chief concern**, business email compromise (BEC) attacks, which have been around far longer, are growing in frequency, complexity, and severity.

"Ransomware gets all the attention because it's sexier, cooler, cloak-and-dagger types of attacks," says Eric Gyasi, vice president of engagement management and an attorney at Stroz Friedberg, an Aon company. "Business email compromise, on the other hand, isn't something people like to talk about. It often happens when they've been conned, and they therefore feel foolish. So the public does not hear as much about them. However, it's just as pervasive a problem in terms of volume as **ransomware attacks**—if not more so."

65%

The increased surge in BEC and EAC attacks between July 2019 and December 2021

A quietly growing threat

Indeed, the FBI's Internet Crime Complaint Center (IC3) lists BEC as the most financially damaging internet crime. In 2021, BEC and EAC (email account compromise) scams led to roughly **$2.4 billion in global cyber losses**, compared to $49.2 million from ransomware, according to the FBI. What's more, between July 2019 and December 2021, BEC/EAC attacks surged 65% and have cost organizations **approximately $43.3 billion since 2016**, the FBI says.

> **Ransomware gets all the attention because it's sexier, cooler, cloak-and-dagger types of attacks.**
>
> Eric Gyasi, vice president of engagement management, Stroz Friedberg

David Rand

David Rand is a business and technology reporter whose work has appeared in major publications around the world. He specializes in spotting and digging into what's coming next – and helping executives in organizations of all sizes know what to do about it.

Key takeaways

- Ransomware is top of mind for many, but business email compromise (BEC) is a more prevalent threat.
- Companies that ignore BEC, an increasingly troubling problem, do so at their financial and reputational peril.
- Enterprises should implement safeguards, from training programs to multifactor authentication and zero trust.

Focal Point

Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.

BEC typically targets businesses that regularly conduct wire transfers. Scammers gain access to an email account belonging to an employee to learn about the business's vendors. They then send a fraudulent request for a wire transfer payment to a vendor. The vendor is then tricked into sending money to an account controlled by the perpetrator.

At one time, these things were fairly easy to spot. The user could look for **horribly reproduced brand logos**, broken English, or ludicrous come-ons in emails and assume they were phishing attempts. But cybercriminals are more effective at covering their tracks these days. They are spoofing CEO and CFO email addresses and sending bogus communications to recipients that are indistinguishable from the true article.

[Read also: Cyber con artists are also keeping up with current events and attuned to what's trending, as in this heart-tugging Ukraine-related crypto scam]

They are also studying businesses and employee activities to seamlessly inject themselves into key conversations at critical moments. If they learn about a merger, for example, they might use that knowledge to represent themselves as part of the deal and con people into sending them money.

It happens more often than organizations like to let on in almost every industry, including:

- **Real estate,** where scammers have been diverting hundreds of thousands of dollars in seller and buyer funds. As Tyler Adams, co-founder and CEO of the Texas-based SaaS platform CertifID told **Dark Reading**, all it takes is a simple search to see every house that's for sale, who the real estate agents are, and the names of the supporting title and escrow companies. With additional light investigation, they can find email addresses of the parties dealing with the transactions and then pose as those parties to pilfer money. **About 13,638 people** were victims of real estate wire fraud in 2020, with losses totaling more than $213 million, the FBI says. BEC caused a huge chunk of that.
- **Healthcare,** where cybercriminals have been launching BEC attacks against payment processors to redirect victim payments. In April, for example, a healthcare company with more than 175 medical providers discovered that someone posing as an employee had changed automated clearing house (ACH) instructions for one of their payment processing vendors in order to direct about $840,000 to the robber rather than the intended providers, according to the FBI.
- **Philanthropy,** where cybercriminals have pilfered funds meant to help people around the world. During the holidays in 2020, for example, hackers dummied-up a legitimate-looking invoice, sent it to **One Treasure Island**, a San Francisco nonprofit benefiting the homeless, and convinced someone to send $650,000 to a bank account in Odessa, Texas, in three different payments. The organization recovered $37,000 from a frozen account but lost the rest.

Finding new targets

Earlier this year, the **FBI warned** that scammers are extending their BEC attacks beyond traditional platforms. Whereas social engineering has typically relied on some combination of telephone and email exchanges, the technique has now extended to include **virtual meeting platforms**, as people have worked remotely since the pandemic began.

> **Human nature being what it is, these scams are easier to execute than you might think.**
>
> Frank Dickson, group vice president and security and trust analyst, IDC

The thieves compromise a senior leader's email address and then use that to ask employees to attend a virtual call. In the meeting, the scammer inserts a still picture of the CEO with no audio, or a deepfake audio, and claims their audio or video is not properly working. The scammer then tells employees to initiate wire transfers to fraudulent bank accounts.

With the level of sophistication hackers are reaching, it is clear BEC attacks are not going away. If anything, advances in automated technologies like artificial intelligence (AI) and machine learning (ML), as well as the continued evolution of deepfake audio and video, are accelerating their efforts.

[Read also: It's not just BEC attacks that are on the rise. Enterprise leaders must also be alert to this activity with the funny name—and, no, it's not phishing]

But, more than that, BEC continues to succeed because it plays on the trusting nature of human beings. Most people aren't comfortable questioning emails that appear to come from senior execs, valued partners, customers, or the media. And they do not always scrutinize every email address to verify it is written in the proper company format because, let's face it, they don't have time—and they likely never will.

Crucial countermeasures

Observers say organizations need to offset human tendencies by implementing the following technological and procedural best practices:

Invest in education and awareness. According to the Verizon 2022 Data Breach Investigations Report, **82% of data breaches** "involved the human element," including social attacks, errors, and misuse. In fact, unlike ransomware or other attacks, BEC doesn't even need malware to succeed, says Frank Dickson, group vice president and security and trust analyst with research firm IDC. "Human nature being what it is, these scams are easier to execute than you might think," he says.

82%

of data breaches involve the "human element," including social attacks, errors, and misuse

Dickson says investing in training programs to help employees spot and respond to possible BEC attempts is essential. The FBI recommends taking basic precautions, including:

- **Be careful** with what information employees share online or in social media.
- **Don't click** on anything in an unsolicited email or text message. If a company says you have a problem, go to their website to check it out.
- **Carefully examine** email addresses and URLs to see if anything looks unusual. An additional number on an email or a URL hyperlink with words that do not go along with the company's name or mission can be signs something is wrong.
- **Exercise extreme caution** when downloading and never open attachments from unknown sources.
- **Verify payment and purchase requests** in person, if possible, rather than digitally or by telephone.

Implement multifactor authentication (MFA). Multifactor authentication has helped minimize ransomware attacks and is now a basic requirement in cyber insurance policies. That's for a reason: Having extra checks and balances before someone can access a network, email, or financial account can stop a BEC attempt cold. Conversely, not having MFA can lead to disaster. In fact, of all the BEC cases security monitoring company Arctic Wolf tracked in the first part of the year, **80% of affected organizations** had no MFA.

Embrace a layered defense. While BEC attacks aren't necessarily technologically sophisticated, deploying basic security countermeasures and regularly updating IT systems can help. Analysts recommend using spam filters, implementing secure file-sharing processes, and embracing **zero-trust approaches**, in which every person or machine trying to access a network is considered suspicious until proven otherwise.

While ransomware continues to capture world attention, observers say organizations cannot take business email compromise too lightly. This unsung threat is not going away. If anything, it's growing in frequency, complexity, and severity. It's vital to address it now.

Related

RSAC 2023 Preview: What CISOs (Need to) Know About Board Accountability

Report: Last Year's Top Finserv Cyber Threats to Intensify in 2023

What the Tech Sector Can Learn From TikTok: Trust Is Everything